On Topics Related to Sum Systems

Ambrose David Law

This thesis is submitted in partial fulfilment of the requirement
for the degree of Doctor of Philosophy

School of Mathematics

Cardiff University

December 2023

CARDIFF
UNIVERSITY

PRIFYSGOL
CAERDYDD

DECLARATION

This thesis is the result of my own independent work, except where otherwise stated, and the views expressed are my own. Other sources are acknowledged by explicit references. The thesis has not been edited by a third party beyond what is permitted by Cardiff University's Use of Third Party Editors by Research Degree Students Procedure.

Signed .... (candidate) Date ....

STATEMENT 1

This thesis is being submitted in partial fulfilment of the requirements for the degree of PhD.

Signed .... (candidate) Date ....

STATEMENT 2

This work has not been submitted in substance for any other degree or award at this or any other university or place of learning, nor is it being submitted concurrently for any other degree or award (outside of any formal collaboration agreement between the University and a partner organisation).

Signed .... (candidate) Date ....

STATEMENT 3

I hereby give consent for my thesis, if accepted, to be available in the University's Open Access repository (or, where approved, to be available in the University's library and for inter-library loan), and for the title and summary to be made available to outside organisations, subject to the expiry of a University-approved bar on access if applicable.

Signed .... (candidate) Date ....

Summary

For $m \in \mathbb{N}$, we say that the m integer sets $A_1, \ldots, A_m \subset \mathbb{N}_0$, form an *m-part sum system* if their *sumset* is the target set

$$\sum_{j=1}^{m} A_j = \Big\{ a_1 + \cdots + a_m : a_j \in A_j,\ j \in \{1, \ldots, m\} \Big\} = \Big\{ 0, 1, 2, \ldots, \prod_{j=1}^{m} |A_j| - 1 \Big\}.$$

That is to say, the sum over each element of the sets $A_1, \ldots, A_m$ uniquely generates the consecutive integers from 0 to $\prod_{j=1}^{m} |A_j| - 1$ with each integer appearing exactly once.

Huxley, Lettington and Schmidt, in 2018, established a bijection between sum systems and sum-and-distance systems, utilising *joint ordered factorisations*, a specific form of ordered multi-factorisations, historically considered by MacMahon. They proved that for each m-part sum system there exists a corresponding m-part *sum-and-distance system* which generates the centro-symmetric set of consecutive (half) integers symmetric around the origin

$$\Big\{ -\frac{1}{2}\Big(\prod_{j=1}^{m} |A_j| - 1 \Big), \ldots, \frac{1}{2}\Big(\prod_{j=1}^{m} |A_j| - 1 \Big) \Big\}.$$

In this thesis, we extend the results of Huxley, Lettington and Schmidt to obtain a unifying theory underpinning sum-and-distance systems, expressing their structures in terms of joint-ordered-factorisations, thus enabling explicit construction formulae to be established via these factorisations.

This unifying theory occurs when one allows consecutive half integers in the target set, when at least one component sum-and-distance set has even cardinality, leading to an invariance in the sum over weighted averages of the sum of squares across the sum-and-distance system component sets to be deduced.

Further results include the application of associated divisor functions and Stirling numbers of the second kind, to enumerate all m-part joint ordered factorisations $\mathcal{N}_m(N)$ for a given positive integer $N = n_1 \times n_2 \times \ldots n_m$. We go on to show that the counting function $\mathcal{N}_m(N)$ satisfies an implicit three term recurrence relation proving an important relation in additive combinatorics.

Additionally, sum systems $\pmod{N + z}$, are considered, as well as orbit structures arising from very simple joint ordered factorisations. The latter leads to connections with cyclotomy.

Acknowledgments

First and foremost, thank you Dr Matthew Lettington. You have been supervising my work since I took that summer research internship back in 2016, and I owe where I am today to your support. Our mutual passion for the wide variety of topics we have shared, discussed and investigated will always be remembered. You have been an amazing mentor.

Secondly, thank you Prof Karl Michael Schmidt. As my tutor during my undergrad, and now my supervisor, you have been helping me along my journey, and your expertise and knowledge has been invaluable. You always kept me on my toes in meetings, and I appreciated your rigorous eye for detail (usually telling me some equation of mine made no sense – which was often true).

Thank you to Cardiff University, who has undertook my academic career from undergraduate degree to my PhD. I am glad I was able to stick around until the promised new building was finally a reality. I acknowledge the financial support given to me by EPSRC.

Thank you mum, for being a beacon of love, to whom I could always turn to. Your encouragement and logic have gotten me to who I am today.

Dad, you told me the story that you once read that a "Möbius strip can be explained using higher mathematics" and it was your hope that I would be able to explain it to you. It took 3 years and a module in Topology, but you finally got that explanation.

Thank you to my twin Oscar for always being at the other end of the phone and for world-building the Projective with me. Thank you Theo, for your unending hilarity and entertainment, your wit never seizes to amaze me.

Thank you to the Oborne family for housing me throughout my PhD, and a special thanks to Doris the cat (Lady Snu) for educating me on the fact I am a cat person.

To Sh'kyra my skeleton key, Fionn my arch-nemesis, Oska and Glenn World, to Tom my king, Grace and your care, Amy your endless tolerance, Amelia my neurospicy counterpart, James with your enthusiasm, my magic groups, my friend network, Brighton, my piano (always a welcomed distraction) and to all those who have contributed to my development and life; I love you all and thank you.

Contents

Notation

Notation	Name	Definition
$\mathbb{N}$	The natural numbers	$\{1, 2, 3, \dots\}$
$\mathbb{N}_0$	The non-negative integers	$\{0, 1, 2, \dots\}$
$\mathbb{N}_2$	The natural numbers ≥ 2	$\{2, 3, 4, \dots\}$
$\frac{1}{2}\mathbb{N}$	The half integers	$\{\frac{1}{2}, 1, \frac{3}{2}, 2, \frac{5}{2}, 3, \dots\}$
$\mathbb{Z}$	The integers	$\{\dots, -2, -1, 0, 1, 2, \dots\}$
$\emptyset$	The empty set	$\{\}$
$\big(a_1 \ \dots \ a_n\big)$	Cycle permutation notation	Permutes the value a_i to a_{i+1} and a_n to a_1, for $i \in \{1, \dots, n\}$.
$\delta_{\cdot,\cdot}$	The Kronecker delta function	For $m, n \in \mathbb{N}$ $$\delta_{m,n} = \begin{cases} 1, & \text{if } m = n \\ 0, & \text{if } m \neq n \end{cases}$$
$\cdot \mid \cdot$	Divides	For $m, n \in \mathbb{N}$, $m \mid n$ means m *divides* n
$\lfloor \cdot \rfloor$	The floor function	For $x \in \mathbb{R}$, $\lfloor x \rfloor = \max\{m \in \mathbb{Z} : m \leq x\}$
$\lceil \cdot \rceil$	The ceiling function	For $x \in \mathbb{R}$, $\lceil x \rceil = \min\{n \in \mathbb{Z} : x \leq n\}$
$\omega(\cdot)$, $\Omega(\cdot)$	Prime omega functions	For $n \in \mathbb{N}$, $\omega(n)$ counts the number of distinct prime factors of n, and $\Omega(n)$ counts the total number of prime factors of n, counting multiplicity. If $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, then $\omega(n) = k$ and $\Omega(n) = a_1 + \dots + a_k$.
$\gcd(\cdot, \cdot)$	Greatest common divisor	For $m, n \in \mathbb{N}$, $$\gcd(m, n) = \max\{d \in \mathbb{N} : d \mid m, \text{ and } d \mid n\}.$$ If $\gcd(m, n) = 1$ we say m and n are *coprime.*

$\varphi(\cdot)$	Euler's totient function	For $n \in \mathbb{N}_0$, $\varphi(n)$ counts the number of coprime positive integers up to n, i.e. $\varphi(n) = \big\lvert\{m \in \mathbb{N} : m < n,\ \gcd(m,n) = 1\}\big\rvert$
$\mu(\cdot)$	The Möbius function	For $n \in \mathbb{N}$, $\mu(n) = \begin{cases} (-1)^{\Omega(n)}, & \text{if } n \text{ is square-free} \\ 0, & \text{if } n \text{ is not square-free} \end{cases}$
$\lambda(\cdot)$	Liouville lambda function	For $n \in \mathbb{N}$, $\lambda(n)$ is $+1$ if n has an even number of prime factors, and -1 if n has an odd number of prime factors, given by $\lambda(n) = (-1)^{\Omega(n)}.$
$\operatorname{ord}_{\cdot}(\cdot)$	Multiplicative order	For $n \in \mathbb{N}$, $k \geq 2$ with n and k are coprime, $\operatorname{ord}_k(n) \in \mathbb{N}$ is the smallest integer such that $n^{\operatorname{ord}_k(n)} \equiv 1 \pmod{k}.$
	Multi-index notation	An m-dimensional multi-index is an m-tuple $n = (n_1, \ldots, n_m) \in \mathbb{N}^m$.
	Partial order	For multi-indices $n, k \in \mathbb{N}^m$, their partial order is given by $k \leq n \iff k_j \leq n_j$, for $j \in \{1, \ldots, m\}$.
$0_{\cdot}$ and $1_{\cdot}$		For $m \in \mathbb{N}$, let $0_m = (0, \ldots, 0) \in \mathbb{N}_0^m$ and $1_m = (1, \ldots, 1) \in \mathbb{N}^m$.

$\bar{e}_\cdot$	Unit vector	For $m \in \mathbb{N}$ and $j \in \{0, \dots, m-1\}$ $\bar{e}_j = (0, \dots, 0, 1, 0, \dots, 0) \in \mathbb{N}_0^m$, with 1 in the j-th position.
$\cdot \oplus \cdot$	Direct sum of vectors	For $m \in \mathbb{N}$ and vectors $v, w \in \mathbb{N}_0^m$, such that $v = (v_1, \dots, v_m), \quad \text{and} \quad w = (w_1, \dots, w_m)$, then $v \oplus w = (v_1, \dots, v_m, w_1, \dots, w_m)$.
π	Circular shift permutation	For $m \in \mathbb{N}$ and $v = (v_1, \dots, v_m) \in \mathbb{N}_0^m$, then $\pi v = (v_m, v_1, \dots, v_{m-1})$ and $\pi^i v = (v_{m-i+1}, \dots, v_m, v_1, \dots, v_{m-i})$.
$\langle \cdot \rangle$	Arithmetic progression	For any $N, s, r \in \mathbb{N}$, $\langle N \rangle = \{0, 1, \dots, N-1\}$, and the arithmetic progression with start value r, step size s and N terms can be expressed as $s\langle N \rangle + r = \{r, r+s, r+2s, \dots, r+(N-1)s\}$.

Chapter 1

Introduction

For a collection of m finite integer sets $A_1, \ldots, A_m \subset \mathbb{Z}$, each with cardinality $|A_j| \geq 2$ for $j \in \{1, \ldots, m\}$ (i.e. non-empty and non-singleton), we are interested in their *sumset* (or *Minkowski sum*) defined by

$$\sum_{j=1}^{m} A_j := \left\{ \sum_{j=1}^{m} a_j : a_j \in A_j \right\}. \tag{*}$$

We say these sets form an m-dimensional additive system for a given non-empty target set of integers $T \subseteq \mathbb{Z}$ if their sumset satisfies

$$T = \sum_{j=1}^{m} A_j.$$

The cardinalities of the sets satisfy the equation $|T| = |A_1||A_2| \ldots |A_m|$ if and only if each element $t \in T$ is represented uniquely in this sumset.

The study of additive systems dates back to de Bruijn's paper [7] in 1950 on (possibly infinite) sets of non-negative integers A_j, with $|A_j| \neq 0$ and $0 \in A_j$, for $T = \mathbb{N}_0$. He referred to such an additive system as a *number system*, and paid particular interest to the *awkward* British Imperial number systems historically employed in weights, measures and currency.

Subsequently, number systems became known as complementing set systems [84, 53], the latter paper focusing on uniquely representing the first N non-negative consecutive integers, $T = \{0, 1, 2, \ldots, N-1\}$, generated by the sumset of two integer sets, i.e. the case $m = 2$ above (*). More recently an exhaustive construction of complementing set systems, generalised to consisting of $m \in \mathbb{N}_2$ sets, called *sum systems*, based on integer factorisations of the cardinalities $|A_1|, \ldots, |A_m|$ with $|A_j| \geq 2$, was given by Huxley, Lettington and Schmidt [42]. The enumeration of two-dimensional sum systems was first attempted by Long in the $m = 2$ case [53] but contained an error. Some 42 years later Lettington and Schmidt, for a given vector $(n_1, \ldots, n_m)$, with $N = n_1 n_2 \ldots n_m$, $n_j \geq 2$ and $|A_j| = n_j$, enumerated the number of m-part sum systems [51]. In this present work, amongst other results, we extend this to enumerating all m-part sum systems for a given integer N, bypassing the need to consider given m-part vectors individually. The results incorporate the Stirling numbers of the second kind.

A question posed by de Bruijn in the closing remarks of [8] refers to an earlier publication of his [7], concerning the analogous problem for number systems representing uniquely all integers in $T = \mathbb{Z}$. Of this de Bruijn says “That problem is much more difficult than the one dealt with above, and it is still far from a complete solution.”

This question was considered in 1974 by Swenson [79], with a survey of results collected by Tijdeman in 1998 [82], at which point the topic of *direct sum decompositions of the integers* started to gain more interest [43, 18, 24, 17]. Results indicated that the additive systems for $T = \mathbb{N}$ could be characterised concisely, whereas the systems for $T = \mathbb{Z}$ could not [79]. To address this, *tiling* sets were introduced that considered writing $\mathbb{Z}$ as a disjoint union of translations of some given set. These results provide an answer to de Bruijn's problem in the infinite case but cannot be applied to the restricted problem where the integer set T may contain both positive and negative integers.

A modern contextualisation of this question was proposed in [42, 40, 39] that looked to re-frame the question of summing m-part finite additive systems to consider the difference between the component sets as well, naturally integrating negative integers into the target sets. To help facilitate approaching this generalised problem, these papers introduced *sum-and-distance systems*, which have the centro-symmetric target set

$$T = \left\{ -\frac{N-1}{2}, -\frac{N-3}{2}, \ldots, \frac{N-3}{2}, \frac{N-1}{2} \right\},$$

providing a partial answer to de Bruijn's question in the finite case. This present work is thus partially motivated by understanding further the concept of sum-and-distance systems, their construction and enumeration, and their underpinning structures. The following example is given to introduce these additive systems.

Example 1.0.1. Consider the 3 integer sets

$$\begin{aligned} A_1 &= \{0, 1, 2, 6, 7, 8\}, \\ A_2 &= \{0, 3, 12, 15\}, \\ A_3 &= \{0, 24\}. \end{aligned}$$

The cardinality of these sets are $|A_1| = 6$, $|A_2| = 4$ and $|A_3| = 2$, which we can represent by the tuple $n = (6, 4, 2)$. For the sumsets we have

$A_1 + A_2 + \{0\} =$

+0	0	1	2	6	7	8
0	0	1	2	6	7	8
3	3	4	5	9	10	11
12	12	13	14	18	19	20
15	15	16	17	21	22	23

$A_1 + A_2 + \{24\} =$

+24	0	1	2	6	7	8
0	24	25	26	30	31	32
3	27	28	29	33	34	35
12	36	37	38	42	43	44
15	39	40	41	45	46	47

and the collection of these two number grids comprises the consecutive integers from 0 to 47. As $|A_1||A_2||A_3| = 48$, we can write

$$\sum_{j=1}^{3} A_j = \langle 48 \rangle,$$

so by Definition 2.2.1 the sets A_1, A_2, A_3 form a sum system. We refer to an individual set A_j as a *sum system component set.*

To allow for subtraction within our integer systems, we construct associated sets via operations on sum systems, which generates sum-and-distance system [39]. To do this, we take half the internal difference between terms in symmetric positions within a sum system component set around the central term. For A_1, we define the associated sum-and-distance system component B_1 such that

$$B_1 = \frac{1}{2}\{6-2, 7-1, 8-0\} = \{2, 3, 4\}.$$

Similarly, we find that $B_2 = \frac{1}{2}\{9, 15\}$ and $B_3 = \{12\}$. For set differences, we consider the union of B_j with its negative $-B_j$ (for more details, see Theorem 2.2.5) as depicted in the following table

$$B_1 \cup (-B_1) + B_2 \cup (-B_2) + \{-12\} =$$

-12	-4	-3	-2	2	3	4
$-\frac{15}{2}$	$-\frac{47}{2}$	$-\frac{45}{2}$	$-\frac{43}{2}$	$-\frac{35}{2}$	$-\frac{33}{2}$	$-\frac{31}{2}$
$-\frac{9}{2}$	$-\frac{41}{2}$	$-\frac{39}{2}$	$-\frac{37}{2}$	$-\frac{29}{2}$	$-\frac{27}{2}$	$-\frac{25}{2}$
$\frac{9}{2}$	$-\frac{23}{2}$	$-\frac{21}{2}$	$-\frac{19}{2}$	$-\frac{11}{2}$	$-\frac{9}{2}$	$-\frac{7}{2}$
$\frac{15}{2}$	$-\frac{17}{2}$	$-\frac{15}{2}$	$-\frac{13}{2}$	$-\frac{5}{2}$	$-\frac{3}{2}$	$-\frac{1}{2}$

$$B_1 \cup (-B_1) + B_2 \cup (-B_2) + \{-12\} =$$

+12	-4	-3	-2	2	3	4
$-\frac{15}{2}$	$\frac{1}{2}$	$\frac{3}{2}$	$\frac{5}{2}$	$\frac{13}{2}$	$\frac{15}{2}$	$\frac{17}{2}$
$-\frac{9}{2}$	$\frac{7}{2}$	$\frac{9}{2}$	$\frac{11}{2}$	$\frac{19}{2}$	$\frac{21}{2}$	$\frac{23}{2}$
$\frac{9}{2}$	$\frac{25}{2}$	$\frac{27}{2}$	$\frac{29}{2}$	$\frac{37}{2}$	$\frac{39}{2}$	$\frac{41}{2}$
$\frac{15}{2}$	$\frac{31}{2}$	$\frac{33}{2}$	$\frac{35}{2}$	$\frac{43}{2}$	$\frac{45}{2}$	$\frac{47}{2}$

The resulting component set of these number grids generate the consecutive half integers from $-\frac{47}{2}$ to $\frac{47}{2}$, the required target set for a sum-and-distance system when $|A_1||A_2||A_3|$ is even.

By considering the sum system component sets, we can determine an ordering on the appearance of the next smallest integer across each set. This ordering encodes the structure of these sets, facilitating further analysis.

The three smallest integers are the consecutive terms 0, 1 and 2 within A_1, which we can write as the pair $(1, 3)$, where 1 denotes the set under consideration, and 3 the cardinality of the set $\{0, 1, 2\}$. The next smallest integer is 3 contained in A_2, which we denote by the pair $(2, 2)$, where the second 2 is the cardinality of the set so far, namely $\{0, 3\}$.

We return to A_1 for the next smallest integers, which are 6, 7 and 8. Importantly, these terms are a translation of the initial three terms $0, 1, 2$ by adding $+6$. Thus we could write this set as $A_1 = \{0, 1, 2\} + \{0, 6\}$. We denote the return to this direction with the pair $(1, 2)$, where the 2 corresponds to the cardinality of the set $\{0, 6\}$ now added.

The next smallest integer is found again in A_2, for which we have the terms 12 and 15. These terms are the translation of the initial set $\{0, 3\}$ by adding $+12$, such that $A_2 = \{0, 3\} + \{0, 12\}$, and we similarly denote this order by the pair $(2, 2)$.

Lastly, 24 is found in A_3. Since $A_3 = \{0, 24\}$, we write the next ordering as the pair $(3, 2)$, which finalises our ordering.

Collecting these pairs together, we have a linear chain of pairs which encodes the set under consideration and the terms contained in that set. In this case, our chain is the tuple

$$\Big((1, 3), (2, 2), (1, 2), (2, 2), (3, 2)\Big).$$

This combinatorial object is known as a *joint ordered factorisation* of $(6, 4, 2)$, which describes the ordered factors of the cardinality of each sum system component set. That is to say, the product over the second term of each pair which corresponds to the 1st set is $3 \times 2 = 6 = |A_1|$. Similarly for $2 \times 2 = |A_2|$ and $3 = |A_3|$. A formal definition is as follows.

Definition 1.0.2. Let $m, L \in \mathbb{N}$ and $n = (n_1, \ldots, n_m) \in \mathbb{N}_2^m$, where $\mathbb{N}_2 = \{2, 3, \ldots\}$. Then we call

$$\mathcal{J} = \Big(\big(j_1, f_1\big), \big(j_2, f_2\big), \ldots, \big(j_L, f_L\big)\Big) \in \big(\{1, 2, \ldots, m\} \times \mathbb{N}_2\big)^L,$$

a *joint ordered factorisation of* n if $j_\ell \neq j_{\ell-1}$ for $\ell \in \{2, \ldots, L\}$ and, for $j \in \{1, \ldots, m\}$,

$$\prod_{\ell \in \mathcal{L}_j} f_\ell = n_j,$$

where

$$\mathcal{L}_j := \big\{\ell : j_\ell = j\big\} = \Big\{\ell_1^{(j)}, \ldots, \ell_{k_j}^{(j)}\Big\} \subset \big\{1, 2, \ldots, L\big\},$$

with suitable $k_j \in \mathbb{N}$.

Hence, a joint ordered factorisation of an m-tuple of natural numbers $(n_1, \ldots, n_m)$ arises from writing each of these numbers as a product of factors ≥ 2, and then arranging all factors in a linear chain such that no two adjacent factors arise from the factorisation of the same n_j factor. It is important to note that all factors are non-trivial, i.e. $f_\ell \geq 2$, and we could not allow the pair $(j,1)$. Furthermore, repeated factors from different n_i are allowed, for example $(j_\ell,5)(j_{\ell+1},5)$ could be consecutive pairs in a joint ordered factorisations, but $(j,5)(j,5)$ could not.

These objects lie at the heart of our investigations, underpinning all the additive system structures considered here. To perform concise analysis on additive systems, we utilise the one-to-one correspondence both sum systems and sum-and-distance systems have with joint ordered factorisation (see Theorem 2.2.5 and [42, Theorem 6.7]).

In number theory, many problems require the interplay of addition and multiplication to be understood in order for a solution to be deduced. The classical example of this is Euclid's algorithm which uses repeated division with remainder to determine the highest common factor of two integers. Sum systems are an elegant example of this naturally occurring interplay, where a multi-factorisation structure ensures multiset addition properties.

Before proceeding further we give the reader an outline of the structure of this work. As a whole, this study falls into two parts. Chapters 2 to 5 detail and investigate properties of sum systems and sum-and-distance systems, using joint ordered factorisations to deduce and retrieve these results. Chapters 6 to 8 consider how comparing different internal structures of these additive systems correspond to an ordered framework from which numerical patterns are observed and proved.

Chapter 2 uses the established bijections between joint ordered factorisations and both sum systems and sum-and-distance systems to write an explicit construction formula for the latter systems in terms of these factorisation. This expression is then used to prove numerical properties of these systems, as well as deducing invariant properties that these additive systems possess. The main result of this chapter is the generalisation an invariant result of Hill [39], given by Eq. (2.18) of Corollary 2.4.12, which states that *for $m \in \mathbb{N}$, $n \in \mathbb{N}_2^m$ and $N = \prod_{j=1}^m n_j$, all sum-and-distance systems, $B_1, \dots, B_m$, with target set $\big\{-\frac{1}{2}(N-1), \dots, \frac{1}{2}(N-1)\big\}$ (when also considering set difference operation) satisfy*

$$\sum_{j=1}^{m} \frac{1}{n_j} \sum_{b \in B_j} b^2 = \frac{1}{24}\big(N^2-1\big).$$

Conceptually this result proves that any sum-and-distance system with this target set satisfies an invariance in the sum over weighted averages of the sum of squares across the sum-and-distance system component sets.

In Chapter 3 we introduce divisor functions which are used in many enumerations across this work. We prove Theorem 3.2.1 which provides an enumeration for the number of joint ordered factorisations for a given integer $N \in \mathbb{N}$, and therefore the number of sum systems with the target set $\langle N \rangle = \{0, \ldots, N-1\}$. Theorem 3.2.1 states that *for $m, N \in \mathbb{N}$, the number of m-part sum systems generating the target set $\langle N \rangle$ is equal to*

$$\mathcal{N}_m(N) = \sum_{L=0}^{\infty} m!\, S(L,m)\, (e-\mu)^{*L}(N) = \sum_{L=0}^{\infty} m!\, S(L,m)\, c_L^{(-L)}(N),$$

where $S(L,m)$ are the Stirling numbers of the second kind, and $c_L^{(-L)}(N)$ is the associated divisor function. We go on to show that this counting function satisfies an implicit three term recurrence relation in Theorem 3.3.1, which establishes that *for $m \in \mathbb{N}$ and $N \in \mathbb{N}_2$ with $\mathcal{N}_m(N)$ our counting function for the number of m-part sum systems with target set $\langle N \rangle$, then $\mathcal{N}_m(N)$ obeys the sum over divisors relations*

$$\begin{aligned} \mathcal{N}_m(N) &= \sum_{\substack{d \mid N \\ d<N}} \Big((m-1)\mathcal{N}_m(d) + m\mathcal{N}_{m-1}(d) \Big) \\ &= -\, m \sum_{\substack{d \mid N \\ d<N}} \mu\left(\frac{N}{d}\right) \Big(\mathcal{N}_m(d) + \mathcal{N}_{m-1}(d) \Big). \end{aligned}$$

Historically, this result, as far as the author is aware, remained undiscovered and provides a much-needed result to fill a long-standing gap in the literature.

Chapter 4 combines the focus of Chapters 2 and 3 to enumerate an invariance property observed within sum-and-distance systems with components' cardinality equalling powers of two. Across all joint ordered factorisations corresponding of 2^t, for $t \in \mathbb{N}_2$, and their associated m-part sum-and-distance systems, if we consider the sum over each component set, these values occur multiple times. It is this property that we derive an enumeration for. A conjecture is stated for systems of odd powers.

Chapter 5 is the last chapter in the first part of this work. Here we generalise the sumset operation to work under modular arithmetic, considering sum systems modulo $N + z$, for

$z \in \mathbb{N}_0$. In Theorem 5.2.6, we establish a modular transformation that maps any collection of sum system components, which have the subset target set $\{0, \ldots, N-1\}$, into another collection of additive systems which has a different target set. Theorem 5.2.6 states that *for $m \in \mathbb{N}$, $n \in \mathbb{N}_2^m$, with $N = \prod_{j=1}^m n_j$, and $z \in \mathbb{N}$, let $u, t_j \in \{0, 1, \ldots, N+z-1\}$ for $j \in \{1, \ldots, m\}$, with gcd$(N+z, u) = 1$ and set $\tilde{t} \equiv \sum_{j=1}^m t_j \pmod{N+z}$. For a sum system $A_1, \ldots, A_m$ with target set $\langle N \rangle$, let $D_1, \ldots, D_m$ be the modular system modulo $N+z$ such that $D_j \equiv u(A_j + t_j) \pmod{N+z}$, for $j \in \{1, \ldots, m\}$. Then $D_1, \ldots, D_m$ is an additive system modulo $N+z$ with target set*

$$\sum_{j=1}^m D_j \equiv \big\{0, 1, \ldots, N+z-1\big\} \Big\backslash u\big(\{0, 1, \ldots, z-1\} + \tilde{t} - z\big) \pmod{N+z}.$$

A natural question that arises is whether all these systems of transformed sets account for all additive systems with this new target set, or if there exists a collection of sets which are not transforms of sum systems and yet still has this new target set. When $z = 0$ the answer to this question is no, there does exist unaccounted for additive systems. When $z > 0$ we state a conjecture that all such sets are accounted for.

We start part 2 of this work with Chapter 6, where we set up the motivational framework and establish the required notation to discuss the second half of this study. Usually there are two or more ways to write an m-part sum system with target set $\{0, \ldots, N-1\}$. If we take two of these systems and compare how the component sets differ as a result in the difference between the corresponding joint ordered factorisations, we can investigate how the internal structures of arithmetic progressions and numerical patterns that build these systems might also differ. These differences are represented by permutations in the ordering of their generated set, and we can retrieve a system of equations to describe them. The resulting structures are called *orbits*.

Chapter 7 concerns the orbits between the two simplest expressions the joint ordered factorisations can be written in for 2 dimensions; $\big((1, n_1), (2, n_2)\big)$ and $\big((2, n_2), (1, n_1)\big)$. The emergent patterns are ordered and concise, and the resulting orbits are linked to objects found in coding theory, with connections to other fields such as Lie groups via a well known polynomial function. We deduce an enumeration for the number of two-system orbits of this structure in Theorem 7.2.16, which says that *for $n_1, n_2 \in \mathbb{N}$, let $\Theta(n_1, n_2)$ enumerate the* *number of distinct cyclic orbits between the joint ordered factorisations* $\mathcal{J}_1 = \big((1, n_1), (2, n_2)\big)$ *and* $\mathcal{J}_2 = \big((2, n_2), (1, n_1)\big)$*. Then* $\Theta(n_1, n_2)$ *is given by*

$$\Theta(n_1, n_2) = 1 + \sum_{k|(n_1 n_2 - 1)} \frac{\varphi(k)}{ord_k(n_1)},$$

where φ *is Euler's totient function.*

In Chapter 8, the final chapter in this thesis, we continue our study into orbits between two-dimensional systems for more generalised joint ordered factorisations. If two joint ordered factorisations share common terms in their tuple expressions, we identify an underpinning pattern to their orbit structures corresponding to the orbits between the two systems resulting from removing these common terms. We finish by constructing equivalent frameworks found in Chapter 7 for special cases of joint ordered factorisations, wherein we notice the increasing complexity of the governing equations resulting from more general joint ordered factorisations.

Chapter 2

On Sum-and-Distance Systems

Huxley, Lettington and Schmidt, in their 2018 paper [42], introduced the additive objects *sum systems* and *sum-and-distance systems*, with the former shown to be constructed via arithmetic progressions and joint ordered factorisations in Theorem 9 of the same paper. The latter was shown to result from a transformation of the former using internal differences, which we demonstrate in Example 1.0.1.

This chapter shall focus initially on the construction of sum-and-distance system, defined in Definition 2.2.1, via arithmetic progressions and joint. Once obtained, we perform a range of analyses on these systems to retrieve arithmetic properties concerning sums of terms and sum of squares. In particular we identify an invariant property for both systems which generalises the final result in [40]. First we shall consider some of the context that the underlying operation considered throughout this study are found in.

2.1 Minkowski sum and sumset

For two sets A and B, the resultant set $A + B := \{a + b : a \in A, b \in B\}$ is known as either a *Minkowski sum* or *sumset* depending on the context of use - primarily based upon what A and B are sets of.

The Minkowski sum was named after Hermann Minkowski, Albert Einstein's former professor. In reaction to the revolutionary theory of special relativity in 1905, Minkowski pondered on the geometric implications of Einstein's work. In 1908 he realised that combining the three dimensions of space with the dimension of time into a four dimensional vector space allowed for easier computations of transforming frames of references. The resulting model is known today as *Minkowski Spacetime*.

Although the Minkowski sum does not make an appearance in this formulation of spacetime, it does concern itself with vector spaces. The definition of the Minkowski sum asks that A and B are two sets of position vectors in n-dimensional Euclidean space, with $A+B$ the set formed by adding each vector in A to each vector in B.

For example, in two-dimensional space, let

$$A = \{(0,0),(1,0),(0,1),(1,1)\}, \quad \text{and} \quad B = \{(1,1),(2,1),(1,2),(2,2)\}.$$

Here A is the set of vertices of a unit square with its bottom left corner at the origin, and B is the set of vertices of a unit square with its bottom left corner the upper right corner of A. Then

$$\begin{aligned} A+B = \big\{\, & (1,1),(2,1),(1,2),(2,2),(2,1),(3,1),(2,2),(3,2), \\ & (1,2),(2,2),(1,3),(2,3),(2,2),(3,2),(2,3),(3,3)\big\}, \end{aligned}$$

which constitutes the 9 internal points of a square with sides of length 2, with the bottom left corner the same as the bottom left corner of B. In the two-dimensional integer lattice this set represents the convex hull of the square with four corners $(1,1)$, $(3,1)$, $(1,3)$ and $(3,3)$.

By using the terminology of the Minkowski sum in additive systems, we are considering sets of vector positions in one-dimensional Euclidean space. This supports the idea of additive systems forming a *basis* to some target set $T \subset \mathbb{N}$.

The definition of a sumset has the two sets A and B be subsets of an abelian group G. In our context we have only required $A, B \subset \langle N \rangle$, and will consider modular arithmetic inherited from the abelian group in Chapter 5. Sumsets are thus a more pure interpretation of adding sets together, with many problems in additive combinatorics and additive number theory using this terminology. Although similar disciplines, both these fields are considered a part of combinatorial number theory and their literature is expansive.

The k-fold sum of a set A with itself is a topic of considerable interest in additive number theory, which is defined by

$$kA := \underbrace{A + \cdots + A}_{k}.$$

Here A is a subset of an abelian group. Problems often ask which elements can be created by the sum kA. Three famous questions that fall under additive number theory are Goldbach's conjecture (1742) (for which [87] provides a version using sumset notation), Waring's problem (1770) and Erdös-Turán conjecture on additive bases (1941) [27].

The name "additive combinatorics" was first used by Terence Tao and Van H. Vu in their book of the same name in 2006. It is typically concerned with bounds for $|A + B|$, and in particular the *inverse problem*; what can we tell about the structure of A and B if $|A + B|$ is small?

Despite being relatively new, the field holds a theorem of Augustin Cauchy dating back to 1813 [11] as one of the most important theorems of the field. Davenport rediscovered Cauchy's proof in 1947 [19], and the theorem is hence named after these two.

Theorem: *(Cauchy–Davenport theorem)* Suppose that A and B are subsets of the prime order cyclic group $\mathbb{Z}/p\mathbb{Z}$ for a prime p. Then we have that

$$\min\{p, |A| + |B| - 1\} \leq |A + B|,$$

where $A + B$ is taken modulo p.

Also of interest is the *restricted sumset*, given by

$$S = \{a_1 + \cdots + a_m : a_j \in A_j \text{ and } P(a_1, \ldots, a_m) \neq 0\},$$

where $A_1, \ldots, A_m$ are finite nonempty subsets of a field F and $P(a_1, \ldots, a_m)$ is a polynomial over F. This framework can often be more fruitful than using standard sumsets. Erdös gave the Erdös-Heilbronn conjecture [26] in 1980, which was proven in 1994 [20], and again in 1995 [2], which considered restricted sumsets. The latter proof developed the *polynomial method* (also known as *Combinatorial Nullstellensatz*), which has been used to prove multiple longstanding conjectures (including, unsurprisingly, an Erdös problem).

If $P(a_1, \ldots, a_m) = 1$ for all a_i, then S is just the sumset, as is the case for our additive systems.

Another overlapping area of interest between these two studies is the *doubling constant*, which is defined as $K = \frac{|A+A|}{|A|}$, which sees how the 2-fold sum of A grows and what that can tell us about the structure of A.

Throughout this study we shall use *sumset*. The decision to do so is based on the more algebraic context this operation is found in, with considerations for modular arithmetic found in Chapter 5. This work of sum systems falls into an intersection between additive combinatorics and number theory. There has been some recent development within the field in the 2010s by work of Hill, Huxley, Law, Lettington and Schmidt [42, 51, 40, 39, 49], whose work this study builds upon.

Considering that sumsets modulo N are abelian groups, the question arises regarding their relevance to the factorisation of abelian groups.

In their book [80], Szabó and Sands investigate numerous ways to factorise abelian groups into collections of subsets and subgroups. This area was considered by Hajós, reformulating (1938 [34]) and proving (1941 [35]) a geometric conjecture of Minkowski [62], using factors of finite abelian groups and subsets. At the core of this solution is the theorem that if a finite abelian group is factored into cyclic subsets, then it must be that at least one of these subsets is itself a subgroup. Consequently factoring these groups gained wide spread interest. Over the years, there has been much work on classifying these factors with respect to their properties (see [45, 72, 73, 80, 81] for some examples of these). Some relevant theory to this study is as follows.

Consider the abelian group $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$ under addition modulo N. For two subsets $A, B \subset \mathbb{Z}_N$, we say A, B *factorises* $\mathbb{Z}_N$ if $A + B \equiv \mathbb{Z}_N \pmod{N}$. If $A + B$ factorises $\mathbb{Z}_N$ without using modular arithmetic, we say $A + B = \mathbb{Z}_N$ is a *Krasner factorisation.* It can be seen that a Krasner factorisation is functionally the same as a 2-part sum system. However, Krasner factorisations appear to be considered as a subset of the larger study of the factorisation of groups. Szabó and Sands provide an existence theorem for Krasner factorisation, and gave construction formulae [80][Section 4.3].

2.2 Definitions and constructions

We begin by introducing the following object, which we use extensively throughout this work. For any $n, s, r \in \mathbb{N}$, denote the consecutive integers from 0 to $n-1$ by

$$\langle n \rangle := \{0, 1, \ldots, n-1\}.$$

Then the arithmetic progression with start value r, step size s, with n terms is expressed by

$$s\langle n \rangle + r = \{r, r+s, r+2s, \ldots, r+(n-1)s\}.$$

Two important relations satisfied by the arithmetic progression $\langle n \rangle$ are

$$\langle n \rangle = n - 1 - \langle n \rangle, \tag{2.1}$$

and, for $m \in \mathbb{N}$,

$$\langle mn \rangle = \langle n \rangle + n\langle m \rangle = \langle m \rangle + m\langle n \rangle. \tag{2.2}$$

Note that these sets are not distributive, nor linear in addition. That is,

$$(a+b)\langle n \rangle \neq a\langle n \rangle + b\langle n \rangle, \quad \text{and} \quad \langle n \rangle - \langle n \rangle \neq 0.$$

Individual elements of these sets, such as $\ell \in \langle n \rangle = \{0, \ldots, n-1\}$, will be referred to frequently to detail what integers a variable may take.

We now define the central objects of this work.

Definition 2.2.1. Let $m \in \mathbb{N}$. We call a collection of m distinct non-empty finite sets of non-negative integers $A_1, A_2, \ldots, A_m \subset \mathbb{N}_0$ an *m-part sum system* if

$$\sum_{j=1}^{m} A_j = \left\langle \prod_{j=1}^{m} |A_j| \right\rangle.$$

We refer to $N := \prod_{j=1}^{m} |A_j|$ as the *target value*, and $\langle N \rangle = \left\langle \prod_{j=1}^{m} |A_j| \right\rangle$ as the *target set.*

We also associate a collection of m distinct non-empty finite sets of (half) integers $B_1, \ldots, B_m$, with $B_j \subset \mathbb{N}$ if n_j odd and $B_j \subset \frac{1}{2}\mathbb{N}$ if n_j even, to the sum system $A_1, \ldots, A_m$ satisfying

$$J_e := \{j : |A_j| \text{ even}\} \subset \{1, \ldots, m\}, \quad \text{if} \quad |A_j| = 2|B_j|,$$

$$J_o := \{j : |A_j| \text{ odd}\} \subset \{1, \ldots, m\}, \quad \text{if} \quad |A_j| = 2|B_j| + 1,$$

where $|J_e|+|J_o|=m$. We call $B_1,\dots,B_m$ an *m-part sum-and-distance system* which satisfies

$$\sum_{j\in J_e}\Big(B_j\cup\big(-B_j\big)\Big)+\sum_{j\in J_o}\Big(B_j\cup\{0\}\cup\big(-B_j\big)\Big)=\langle N\rangle-\frac{N-1}{2}.$$

For $j\in\{1,\dots,m\}$, we call the set A_j a *sum system component (set)*, and B_j a *sum-and-distance system component (set)*.

Initially, the authors of [42] classified sum-and-distance systems into two types; *non-inclusive* and *inclusive*, where non-inclusive systems generated a centro-symmetric set around zero of consecutive odd integers, and inclusive sum-and-distance systems generated a central-symmetric set around zero of consecutive integers. The terminology of *non-inclusive* and *inclusive* pertains respectively to whether the target set is generated solely by the sums and differences of elements between the different sets or whether the elements of the individual sets themselves are also required.

However, there is no reason to require the components have all odd or all even cardinalities, and a sum system with mixed parity component set cardinalities will correspond to a hybrid inclusive/non-inclusive sum-and-distance system, as stated in Definition 2.2.1. The definitions of inclusive and non-inclusive sum-and-distance systems found in [42] can be retrieved if $J_e=\emptyset$ and $J_o=\emptyset$ respectively, that is, if n_j is odd or even for all $j\in\{1,\dots,m\}$.

Theorem 3.4 and Theorem 3.5 of [42] establishes a bijection between sum systems and the sum-and-distance systems that shows the distinction between inclusive and non-inclusive sum-and-distance systems resolves into the simple dichotomy between odd and even cardinality of the related sum system component. This process constructs a sum-and-distance systems component set via the internal difference between terms in symmetric positions within the sum system component set around the central term, dividing by two for strictly odd cardinality systems (see Example 1.0.1 for this process).

This method of deriving a sum-and-distance system requires a sum system already calculated, and is inconvenient to perform any analysis on to obtain properties about the system. Furthermore the two stated theorems required the cardinalities of the sum-and-distance system components to be purely odd or even. To achieve a direct construction of a sum-and-distance system we need to first consider the bijection between these additive systems and joint ordered factorisations.

The concept of an ordered multi-factorisation has been around for over a century, with much of the early work attributed to MacMahon [57]. His ideas have been expanded upon since, though of particular interest to us are results relating to the non-trivial divisor function $c_j(n)$, discussed in Chapter 3, which counts the number of ways of writing $n = n_1 \dots n_j$ as an ordered product of factors, with each factor $n_k \geq 2$, $1 \leq k \leq j$.

Although ordered factorisations have been studied extensively with [47] being a noteworthy survey of these objects in the literature, the concept of a *joint* ordered factorisation is far less documented, with the two-dimensional case considered by Ollerenshaw and Brëe in [68]. Since then, Webb [86] used a rudimentary notion of a joint ordered factorisation to construct complementing sets, and Munagi [65, 64] employed this technique in their formulations.

The modern concise notation presented for a joint ordered factorisation was established in [42, 40], which we previously stated in Definition 1.0.2. We introduce below additional notation used throughout this work based on the tuple expression of a joint ordered factorisation.

Definition 2.2.2. Let $m, L \in \mathbb{N}$, $n = (n_1, \dots, n_m) \in \mathbb{N}_2^m$, with $\mathcal{J} = \big((j_1, f_1), \dots, (j_L, f_L)\big)$ a joint ordered factorisation of n, as given in Definition 1.0.2. Then for each such joint ordered factorisation we define the partial products of factors, and of the factors with index class j, as

$$F(\ell) = \prod_{s=1}^{\ell-1} f_s, \quad \text{and} \quad P_j(\ell) = \prod_{\substack{q \in \mathcal{L}_j \\ q < \ell}} f_q,$$

so that

$$N = \prod_{j=1}^{m} n_j = F(L+1), \quad \text{and} \quad F(\ell) = \prod_{j=1}^{m} P_j(\ell).$$

We refer to (j_ℓ, f_ℓ) as the *pair in position* ℓ, and call j_ℓ a *j-value*, with f_ℓ an *f-value.*

When notation may be confused, we will also refer to the j-value as the *j-th coordinate axis.* This occurs when we consider the j-th sum system component set A_j for some $j \in \{1, \dots, m\}$. We will use phrases like "pair with j-value", "pair corresponding to the j-th component axis", and " pair corresponding to the j-th sum system component" interchangeably through out this work. Then we can describe $\mathcal{L}_j := \big\{\ell : j_\ell = j\big\}$ as the set which contains the positions of each pair in $\mathcal{J}$ corresponding to the j-th sum system component.

For reference purposes we define $\mathcal{L}_j$ to be the set of position indices for the pairs in the joint ordered factorisation $\mathcal{J}$ corresponding to A_j.

We will see that the underpinning structure of a sum-and-distance system component will depend on the parity of the cardinality of the associated sum system component. In particular, the position of pairs in $\mathcal{J}$ with an even f-value is important. As such, we define $\ell_{e_j} := \max\big\{\ell \in \mathcal{L}_j : f_\ell \text{ even}\big\}$ to be the position in $\mathcal{J}$ of the last pair corresponding to the j-th sum system component with an even f-value (reading $\mathcal{J}$ from left to right). Additionally, define the j-th index subset $\mathcal{L}'_j := \big\{\ell : j_\ell = j, \ell > \ell_{e_j}\big\}$ to be the positions of all pairs with j-value $j_\ell = j$ after the pair $(j, f_{\ell_{e_j}})$. If n_j is odd, then set $e_j = 0$, $\mathcal{L}'_j = \mathcal{L}_j$ and we say $\ell_{e_j} = f_{\ell_{e_j}} = 0$.

Joint ordered factorisations are important objects which underpin many results found within this study. Often properties of additive systems are proven via analysis of the joint ordered factorisations. It was proven in [42, Theorem 6.7] that given a joint ordered factorisation $\mathcal{J} = \big((j_1, f_1), \ldots, (j_L, f_L)\big)$, for $j \in \{1, \ldots, m\}$, the sets

$$A_j = \sum_{\ell \in \mathcal{L}_j} F(\ell)\langle f_\ell \rangle = \sum_{\substack{\ell \in \{1,\ldots,L\} \\ j_\ell = j}} \left(\prod_{s=1}^{\ell-1} f_s \right) \{0, \ldots, f_\ell - 1\} \tag{2.3}$$

form a sum system, and that conversely any sum system arises from some joint ordered factorisation of the product of cardinalities of its component sets. Hence, a bijection was established between sum systems and joint ordered factorisations.

Remark 2.2.3. For a given joint ordered factorisation $\big((j_1, f_1), \ldots, (j_L, f_L)\big)$, since no $f_\ell = 1$, by Eq. (2.3) there can never be a sum system that contains the component set $\{0\}$.

While complementing sets were the additive systems of interest in the literature for the better part of 80 years, various construction formulae and processes were given for the component sets in the infinite target set case [7, 84, 8, 66, 67], and finite consecutive integer case [53, 86]. The closest such expressions to Eq. (2.3) was given by Webb [86] and Munagi [65]. However, the notation employed here is unwieldly compared with that used for joint ordered factorisations and arithmetic progressions, as established in [42]. In the words of Professor Martin Neil Huxley "Notions are more important than notations, but bad notation can hold you back, whilst good notation can suggest connections with other problems".

Similar to the definition of consecutive sum-and-distance systems, we update Theorem 3.4 and Theorem 3.5 of [42] to now accommodate a mixed parity of component set cardinality. To do this, we require the following result, which is Theorem 3.3 of [42].

Proposition 2.2.4. Let $m \in \mathbb{N}$. Suppose the sets $A_1, \dots, A_m \subset \mathbb{N}_0$ form an m-part sum system. Then, for each $j \in \{1, \dots, m\}$, we have

$$A_j = (\max A_j) - A_j,$$

i.e. $a \in A_j$ if and only if $(\max A_j - a) \in A_j$. We refer to this property as A_j having *palindromic symmetry.*

Theorem 2.2.5. Let $m \in \mathbb{N}_2$, $n \in \mathbb{N}_2^m$ and let the sets $B_1, \dots, B_m \subset \frac{1}{2}\mathbb{N}$ form an m-part consecutive sum-and-distance system. Let J_e and J_o be defined as in Definition 2.2.1. For $j \in J_e$, let

$$A_j := \max B_j + \big(B_j \cup (-B_j)\big), \tag{2.4}$$

and for $j \in J_o$, let

$$A_j := \max B_j + \big(B_j \cup \{0\} \cup (-B_j)\big). \tag{2.5}$$

Then $A_1, \dots, A_m$ form an m-part sum system.

Conversely, let the sets $A_1, \dots, A_m \subset \mathbb{N}_0$ form an m part sum system with $|A_j| = n_j$. For $j \in \{1, \dots, m\}$ and $l \in \langle n_j \rangle$, let $a_l \in A_j$ be the l-th element in A_j. For $\nu_j = \lceil \frac{n_j}{2} \rceil$ and $\tau_j = \lfloor \frac{n_j}{2} \rfloor$, define the integer sets

$$B_j := \big\{ \tfrac{1}{2}(a_{\nu_j + k} - a_{\tau_j - 1 - k}) : k \in \langle \tau_j \rangle \big\}. \tag{2.6}$$

Then $B_1, \dots, B_m$ forms an m part consecutive sum-and-distance system.

Proof. Set $N := \prod_{j=1}^m |A_j| = \prod_{j=1}^m n_j$. We find the sumset

$$\begin{aligned}\sum_{j \in J_e} A_j + \sum_{j \in J_o} A_j &= \sum_{j=1}^m \max B_j + \sum_{j \in J_e} \big(B_j \cup (-B_j)\big) + \sum_{j \in J_o} \big(B_j \cup \{0\} \cup (-B_j)\big) \\ &= \frac{N-1}{2} + \langle N \rangle - \frac{N-1}{2} = \langle N \rangle,\end{aligned}$$

where we use the fact that the sum of the largest elements of the component sets of a sum-and-distance system gives the largest element of its target set, which is $(N-1)/2$.

Conversely, we know sum system component sets have palindromic symmetry from Proposition 2.2.4. For sum system components with even cardinality, i.e. $|A_j| = n_j$ is even, the palindromic symmetry satisfies

$$a_{\frac{n_j}{2}+k} + a_{\frac{n_j}{2}-1-k} = a_{n_j-1},$$

with $a_{n_j-1} = \max A_j$. Then we can write

$$\frac{1}{2}\Big(a_{\frac{n_j}{2}+k} - a_{\frac{n_j}{2}-1-k}\Big) = \frac{1}{2}\Big(a_{\frac{n_j}{2}+k} - \big(a_{n_j-1} - a_{\frac{n_j}{2}+k}\big)\Big) = a_{\frac{n_j}{2}+k} - \frac{1}{2}a_{n_j-1},$$

and similarly

$$\begin{aligned}-\frac{1}{2}\Big(a_{\frac{n_j}{2}+k} - a_{\frac{n_j}{2}-1-k}\Big) &= \tfrac{1}{2}a_{n_j-1} - a_{\frac{n_j}{2}+k}\\ &= \tfrac{1}{2}a_{n_j-1} - \Big(a_{n_j-1} - a_{\frac{n_j}{2}-1-k}\Big)\\ &= a_{\frac{n_j}{2}-1-k} - \tfrac{1}{2}a_{n_j-1}.\end{aligned}$$

Hence we have

$$B_j \cup (-B_j) = \{a_{\frac{n_j}{2}+k} - \tfrac{1}{2}a_{n_j-1} : k \in \langle\tau\rangle\} \cup \{a_{\frac{n_j}{2}-1-k} - \tfrac{1}{2}a_{n_j-1} : k \in \langle\tau\rangle\} = A_j - \tfrac{1}{2}\max A_j.$$

For sum system components with odd cardinality, i.e. $|A_j| = n_j$ is odd, the palindromic symmetry satisfies

$$a_{\frac{n_j-1}{2}+k} + a_{\frac{n_j-1}{2}-k} = a_{n_j-1}.$$

Then we can write

$$\frac{1}{2}\Big(a_{\frac{n_j-1}{2}+1+k} - a_{\frac{n_j-1}{2}-1-k}\Big) = \frac{1}{2}\Big(a_{\frac{n_j-1}{2}+1+k} - \big(a_{n_j-1} - a_{\frac{n_j-1}{2}+1+k}\big)\Big) = a_{\frac{n_j-1}{2}+1+k} - \tfrac{1}{2}a_{n_j-1},$$

and similarly

$$\begin{aligned}-\frac{1}{2}\Big(a_{\frac{n_j-1}{2}+1+k} - a_{\frac{n_j-1}{2}-1-k}\Big) &= \tfrac{1}{2}a_{n_j-1} - a_{\frac{n_j-1}{2}+1+k}\\ &= \tfrac{1}{2}a_{n_j-1} - \Big(a_{n_j-1} - a_{\frac{n_j-1}{2}-1-k}\Big)\\ &= a_{\frac{n_j-1}{2}-1-k} - \tfrac{1}{2}a_{n_j-1}.\end{aligned}$$

Hence we have

$$\begin{aligned}B_j \cup \{0\} \cup (-B_j) &= \{a_{\frac{n_j-1}{2}+1+k} - \tfrac{1}{2}a_{n_j-1} : k \in \langle\tau\rangle\} \cup \{0\} \cup \{a_{\frac{n_j-1}{2}-1-k} - \tfrac{1}{2}a_{n_j-1} : k \in \langle\tau\rangle\}\\ &= A_j - \tfrac{1}{2}\max A_j.\end{aligned}$$

Then taking the sum over the parity partition on the indices, J_e and J_o, we find that

$$\sum_{j\in J_e} B_j \cup (-B_j) + \sum_{j\in J_o} B_j \cup \{0\} \cup (-B_j) = \sum_{j=1}^{m} A_j - \frac{1}{2}\sum_{j=1}^{m} \max A_j = \langle N\rangle - \frac{N-1}{2},$$

as required. □

Lemma 2.2.6. Let $m \in \mathbb{N}_2$, $n \in \mathbb{N}_2^m$ and $\mathcal{J}$ be a joint ordered factorisation of n. For $j \in \{1,\dots,m\}$, sum system components, A_j, and sum-and-distance system components, B_j, have the following properties.

$$\max A_j = \sum_{\ell\in\mathcal{L}_j} F(\ell)(f_\ell - 1), \qquad \min A_j = 0, \qquad \max B_j = \frac{1}{2}\max A_j,$$

$$\min B_j = \begin{cases} F(\ell_1), & \nexists \ell_{e_j} \in \boldsymbol{\mathcal{L}}_j \\ \frac{1}{2}\Big(F\big(\ell_{e_j}\big) - \sum\limits_{\substack{p\in\mathcal{L}_j \\ p<\ell_{e_j}}} F(p)\big(f_p - 1\big)\Big), & \exists\ \ell_{e_j} \in \boldsymbol{\mathcal{L}}_j \end{cases} \tag{2.7}$$

Proof. By considering Eq. (2.3) we have

$$\max A_j = \sum_{\ell\in\mathcal{L}_j} F(\ell)\max\langle f_\ell\rangle = \sum_{\ell\in\mathcal{L}_j} F(\ell)(f_\ell - 1).$$

As $0 \in A_j$ and $A_j \subset \mathbb{N}_0$, for all $j \in \{1,\dots,m\}$, then $\min A_j = 0$. We can use Eq. (2.6) to write

$$\max B_j = \tfrac{1}{2}(\max A_j - \min A_j) = \tfrac{1}{2}\max A_j.$$

The parity of n_j dictates the centre two values in A_j. Let $A_j = \{a_0,\dots,a_{n_j-1}\}$, with $a_i \in \mathbb{N}_0$.

Case 1 $\nexists\ \ell_{e_j} \in \boldsymbol{\mathcal{L}}_j$: The central position in A_j, $\nu = \frac{n_j-1}{2}$, is not considered, instead we start with the two terms either side of it, $a_\nu \pm F(\ell_1)$, which enables us to write

$$\frac{1}{2}\Big(a_\nu + F(\ell_1) - \big(a_\nu - F(\ell_1)\big)\Big) = F(\ell_1).$$

Case 2 $\exists\ \ell_{e_j} \in \boldsymbol{\mathcal{L}}_j$: The two centre positions in A_j are $\nu_0 = \frac{n_j}{2} - 1$ and $\nu_1 = \frac{n_j}{2}$ with corresponding terms

$$a_{\nu_0} = F\big(\ell_{e_j}\big)\left(\frac{1}{2}f_{\ell_{e_j}} - 1\right) + \sum_{\substack{p\in\mathcal{L}_j \\ p<\ell_{e_j}}} F(p)\big(f_p - 1\big) + \frac{1}{2}\sum_{p\in\mathcal{L}'_j} F(p)\big(f_p - 1\big),$$

$$a_{\nu_1} = \frac{1}{2}\left(F\big(\ell_{e_j}\big)f_{\ell_{e_j}} + \sum_{p\in\mathcal{L}'_j} F(p)(f_p - 1)\right).$$

Taking their difference and dividing by 2 yields the desired result. □

2.3 Constructions from factorisations

The construction presented in Eq. (2.6), though streamlined, requires the sum system component sets to be established. To bypass this requirement we now establish a direct construction formula for sum-and-distance systems in terms of their corresponding joint ordered factorisations. We begin by first defining three arithmetic progressions which underpin the structure of sum-and-distance system components.

Definition 2.3.1. Let $m \in \mathbb{N}_2$, $n \in \mathbb{N}_2^m$ and $\mathcal{J}$ be a joint ordered factorisation of n with $L \in \mathbb{N}_m$ pairs. For $\ell \in \{1, \dots, L\}$ we define

$$H_\ell := F(\ell)\bigg(\langle f_\ell \rangle - \frac{f_\ell - 1}{2}\bigg),$$

which is symmetric around the origin, i.e. $H_\ell = -H_\ell$. For fixed $j \in \{1, \dots, m\}$, if $\ell = \ell_{e_j}$ we define

$$E_{\ell_{e_j}} := F(\ell_{e_j})\Bigg(\bigg\langle \frac{f_{\ell_{e_j}}}{2} \bigg\rangle + \frac{1}{2}\Bigg).$$

For $\ell \neq \ell_{e_j}$ we define

$$G_\ell := F(\ell)\Bigg(\bigg\langle \frac{f_\ell - 1}{2} \bigg\rangle + 1\Bigg).$$

These sets have the following properties.

$$H_\ell = \begin{cases} E_{\ell_{e_j}} \cup (-E_{\ell_{e_j}}) \text{ if } \ell = \ell_{e_j}, \\ G_\ell \cup \{0\} \cup (-G_\ell) \text{ otherwise,} \end{cases} \tag{2.8}$$

$$\max G_\ell = \max E_\ell = \max H_\ell = -\min H_\ell = \frac{1}{2}F(\ell)(f_\ell - 1),$$
$$\min G_\ell = F(\ell), \qquad \min E_{\ell_{e_j}} = \frac{1}{2}F(\ell_{e_j}).$$

Lemma 2.3.2. Let $m \in \mathbb{N}_2$, $n \in \mathbb{N}_2^m$, $N = \prod_{j=1}^m n_j$, and $\mathcal{J}$ be a joint ordered factorisation of n with corresponding sum-and-distance system $B_1, \dots, B_m$. For $j \in \{1, \dots, m\}$, if n_j is even then

$$B_j \cup (-B_j) = \sum_{\ell \in \mathcal{L}_j} H_\ell. \tag{*}$$

If n_j is odd then

$$B_j \cup \{0\} \cup (-B_j) = \sum_{\ell \in \mathcal{L}_j} H_\ell. \tag{**}$$

Moreover, we have that

$$\sum_{\ell=1}^{L} H_\ell = \langle N\rangle - \frac{N-1}{2}. \tag{2.9}$$

Proof. For Eq. (*), we use Eq. (2.4), Eq. (2.7), and Theorem 6.7 in [42], to obtain

$$\begin{aligned} B_j \cup (-B_j) = A_j - \max B_j &= \sum_{\ell\in\mathcal{L}_j} F(\ell)\langle f_\ell\rangle - \sum_{\ell\in\mathcal{L}_j} F(\ell)\left(\frac{f_\ell - 1}{2}\right) \\ &= \sum_{\ell\in\mathcal{L}_j} F(\ell)\left(\langle f_\ell\rangle - \frac{f_\ell-1}{2}\right) = \sum_{\ell\in\mathcal{L}_j} H_\ell, \end{aligned}$$

as required. Eq. (**) follows from the same argument, but considering expression (2.5) instead. For Eq. (2.9), we take the sum over all $j \in J_e$ and $j \in J_o$, with J_e and J_o as defined in Definition 2.2.1, such that

$$\langle N\rangle - \frac{N-1}{2} = \sum_{j\in J_e}\Big(B_j \cup \big(-B_j\big)\Big) + \sum_{j\in J_o}\Big(B_j\cup\{0\}\cup\big(-B_j\big)\Big) = \sum_{j=1}^{m}\sum_{\ell\in\mathcal{L}_j} H_\ell = \sum_{\ell=1}^{L} H_\ell,$$

as required. □

The construction detailed below gives an explicit formula for the unique component sets of a sum-and-distance system, derived from a given joint ordered factorisation.

Theorem 2.3.3. Let $m \in \mathbb{N}_2$, $n \in \mathbb{N}_2^m$ and $\mathcal{J}$ be a joint ordered factorisation of n with sum-and-distance system $B_1, \ldots, B_m$. For fixed $j \in \{1, \ldots, m\}$, B_j is given by

$$B_j = \Bigg(E_{\ell_{e_j}} + \sum_{\substack{p\in\mathcal{L}_j\\ p<\ell_{e_j}}} H_p\Bigg) \cup \bigcup_{\ell\in\mathcal{L}'_j}\Bigg(G_\ell + \sum_{\substack{p\in\mathcal{L}_j\\ p<\ell}} H_p\Bigg). \tag{2.10}$$

Proof. Fix $j \in \{1, \ldots, m\}$. We shall prove this theorem in two parts.

(a) Assume $\exists\ \ell_{e_j} = \ell_e \in \mathcal{L}_j$. For $\ell \in \mathcal{L}_j$, let $\mathcal{H}_\ell = \sum_{\substack{p\in\mathcal{L}_j\\ p<\ell}} H_p$ and when $\ell \in \mathcal{L}'_j$ we have

$$\mathcal{H}_\ell = \mathcal{H}_{\ell_e+1} + \sum_{\substack{p\in\mathcal{L}'_j\\ p<\ell}} H_p.$$

Taking the right hand side of (2.10) union with its negative we get

$$\big(E_{\ell e} + \mathcal{H}_{\ell e}\big) \cup \bigcup_{\ell\in\mathcal{L}'_j}\big(G_\ell + \mathcal{H}_\ell\big) \cup \big(-E_{\ell e} + \mathcal{H}_{\ell e}\big) \cup \bigcup_{\ell\in\mathcal{L}'_j}\big(-G_\ell + \mathcal{H}_l\big)$$

$$
\begin{aligned}
&= \big(E_{\ell e} + \mathcal{H}_{\ell e}\big) \cup \big(-E_{\ell e} + \mathcal{H}_{\ell_e}\big) \cup \bigcup_{\ell \in \mathcal{L}'_j} \Big(\big(G_\ell + \mathcal{H}_\ell\big) \cup \big(-G_\ell + \mathcal{H}_\ell\big)\Big) \\
&= \Big(\mathcal{H}_{\ell_e} + \underbrace{E_{\ell_e} \cup \big(-E_{\ell_e}\big)}_{=H_{\ell_e}}\Big) \cup \bigcup_{\ell \in \mathcal{L}'_j} \Big(G_\ell \cup \big(-G_\ell\big) + \mathcal{H}_\ell\Big) \\
&= \mathcal{H}_{\ell_e+1} \cup \bigcup_{\ell \in \mathcal{L}'_j} \Big(G_\ell \cup \big(-G_\ell\big) + \mathcal{H}_{\ell_e+1} + \sum_{\substack{p \in \mathcal{L}'_j \\ p<\ell}} H_p\Big) \\
&= \big(\mathcal{H}_{\ell_e+1} + \{0\}\big) \cup \Bigg(\mathcal{H}_{\ell_e+1} + \bigcup_{\ell \in \mathcal{L}'_j} \Big(G_\ell \cup \big(-G_\ell\big) + \sum_{\substack{p \in \mathcal{L}'_j \\ p<\ell}} H_p\Big)\Bigg) \\
&= \mathcal{H}_{\ell_e+1} + \bigcup_{\ell \in \mathcal{L}'_j} \Big(G_\ell \cup \big(-G_\ell\big) + \sum_{\substack{p \in \mathcal{L}'_j \\ p<\ell}} H_p\Big) \cup \{0\},
\end{aligned}
$$

where we have applied Corollary 2.2.6 in the final step. We continue via proof by induction, noting that for $i \in \{1, \ldots, |\mathcal{L}'_j|\}$ then $\ell_{e_j+i} \in \mathcal{L}'_j$.

Claim $\mathcal{P}(\Lambda)$: We claim that for $\Lambda \in \{1, \ldots, |\mathcal{L}'_j|\}$ then

$$
\mathcal{P}(\Lambda) = \{0\} \cup \bigcup_{i=1}^{\Lambda} \Big(G_{\ell_{e+1}} \cup \big(-G_{\ell_{e+1}}\big) + \sum_{\substack{p \in \mathcal{L}'_j \\ p<\ell_{e+i}}} H_p\Big) = \sum_{i=1}^{\Lambda} H_{\ell_{e+i}}.
$$

Base Step $\mathcal{P}(1)$: Take $\Lambda \in \{1\}$. Then the sum over $p \in \mathcal{L}'_j$ with $p < \ell_{e+1}$ is the empty sum, such that

$$
\mathcal{P}(1) = \{0\} \cup \Big(G_{\ell_{e+1}} \cup \big(-G_{\ell_{e+1}}\big) + \overbrace{\sum_{\substack{p \in \mathcal{L}'_j \\ p<\ell_{e+1}}} H_p}^{=0}\Big) = \{0\} \cup G_{\ell_{e+1}} \cup \big(-G_{\ell_{e+1}}\big) = H_{\ell_{e+1}},
$$

as required.

Induction Step $\mathcal{P}(\Lambda+1)$: We assume for $\Lambda \in \{1, \ldots, |\mathcal{L}'_j| - 1\}$ that $\mathcal{P}(\Lambda)$ is true. We now prove $\mathcal{P}(\Lambda+1)$, noting that $\mathcal{P}(\Lambda) = \mathcal{P}(\Lambda) + \{0\}$. Then

$$\begin{aligned}\mathcal{P}(\Lambda+1) =&\mathcal{P}(\Lambda) \cup \Bigg(G_{\ell_{e+\Lambda+1}} \cup \big(-G_{\ell_{e+\Lambda+1}}\big) + \overbrace{\sum_{\substack{p\in\mathcal{L}'_j\\ p<\ell_{e+\Lambda+1}}} H_p}^{\sum_{i=1}^{\Lambda} H_{\ell_{e+i}}}\Bigg)\\ =&\Bigg(\sum_{i=1}^{\Lambda} H_{\ell_{e+i}} + \{0\}\Bigg) \cup \Bigg(G_{\ell_{e+\Lambda+1}} \cup \big(-G_{\ell_{e+\Lambda+1}}\big) + \sum_{i=1}^{\Lambda} H_{\ell_{e+i}}\Bigg)\\ =&\sum_{i=1}^{\Lambda} H_{\ell_{e+i}} + \{0\} \cup G_{\ell_{e+\Lambda+1}} \cup (-G_{\ell_{e+\Lambda+1}}) = \sum_{i=1}^{\Lambda+1} H_{\ell_{e+i}},\end{aligned}$$

as required, proving the claimed statement.

Continuing the proof, we find that

$$\mathcal{H}_{\ell_e+1} + \bigcup_{\ell\in\mathcal{L}'_j}\Bigg(G_\ell \cup \big(-G_\ell\big) + \sum_{\substack{p\in\mathcal{L}'_j\\ p<\ell}} H_p\Bigg) \cup \{0\} = \mathcal{H}_{\ell_e+1} + \mathcal{P}\big(|\mathcal{L}'_j|\big) = \mathcal{H}_{\ell_e+1} + \sum_{\ell\in\mathcal{L}'_j} H_\ell = \sum_{\ell\in\mathcal{L}_j} H_\ell.$$

By Lemma 2.3.2, we have therefore shown that the right hand side of (2.10), union its negative, is equal to $B_j \cup (-B_j)$.

(b) If $\nexists\ \ell_e \in \mathcal{L}_j$, the argument is similar, except that the first bracket of (2.10) is the empty set (see Eq. (2.11)), and we take the remaining term union the negative of itself and $\{0\}$, which results in there being no $\mathcal{H}_{\ell_e+1}$ term. In the proof by induction $\ell_{e+i} \in \mathcal{L}'_j$ is replaced by $\ell_i \in \mathcal{L}_j$. The result is $B_j \cup \{0\} \cup (-B_j)$.

Taking the sum over all $j \in J_e$ and $j \in J_o$ of these unions gives us Eq. (2.9), which proves that (2.10) forms a sum-and-distance system component set. □

Remark 2.3.4. If $\nexists\ \ell_{e_j} \in \mathcal{L}_j$, i.e. n_j is odd, then the explicit form of B_j is given by

$$B_j = \bigcup_{\ell\in\mathcal{L}_j}\Bigg(G_\ell + \sum_{\substack{p\in\mathcal{L}_j\\ p<\ell}} H_p\Bigg). \tag{2.11}$$

Example 2.3.5. Let $n = (18, 25, 8)$ with the joint ordered factorisation

$$\mathcal{J} = \big((1,3),(2,5),(1,2),(3,4),(1,3),(3,2),(2,5)\big).$$

The set B_1 corresponds to $\mathcal{L}_1 = \{1,3,5\}$ with $\ell_{e_1} = 3$. Using expression (2.10) we have

$$B_1 = (E_3 + \sum_{\substack{p\in\{1,3,5\}\\ p<\ell_{e_1}}} H_p) \cup \bigcup_{l\in\{5\}}\Bigg(G_\ell + \sum_{\substack{p\in\{1,3,5\}\\ p<\ell}} H_p\Bigg) = \big(E_3 + H_1\big) \cup \big(G_5 + H_3 + H_1\big),$$

with

$$\begin{aligned}
E_3 &= F(3)\Big(\langle \tfrac{f_3}{2} \rangle + \tfrac{1}{2}\Big) = 15 \times \Big(\langle 1 \rangle + \tfrac{1}{2}\Big) = \tfrac{1}{2}\{15\},\\
G_5 &= F(5)\Big(\langle \tfrac{f_5-1}{2} \rangle + 1\Big) = 120 \times \Big(\langle 1 \rangle + 1\Big) = \{120\},\\
H_1 &= F(1)\Big(\langle f_1 \rangle - \tfrac{f_1-1}{2}\Big) = 1 \times \Big(\langle 3 \rangle - 1\Big) = \{-1, 0, 1\},\\
H_3 &= F(3)\Big(\langle f_3 \rangle - \tfrac{f_3-1}{2}\Big) = 15 \times \Big(\langle 2 \rangle - \tfrac{1}{2}\Big) = \tfrac{1}{2}\{-15, 15\}.
\end{aligned}$$

Substituting for these values we obtain

$$\begin{aligned}
B_1 =& \Big(\tfrac{1}{2}\{15\} + \{-1,0,1\}\Big) \cup \Big(\{120\} + \tfrac{1}{2}\{-15,15\} + \{-1,0,1\}\Big)\\
=& \tfrac{1}{2}\{13, 15, 17, 223, 225, 227, 253, 255, 257\}.
\end{aligned}$$

The set B_2 corresponds to $\mathcal{L}_2 = \{2, 7\}$. As n_2 is odd, we can use expression (2.11) to write

$$B_2 = \bigcup_{\ell \in \{2,7\}} \Bigg(G_\ell + \sum_{\substack{p \in \{2,7\} \\ p < \ell}} H_p\Bigg) = (G_2) \cup (G_7 + H_2),$$

with $G_2 = \{3, 6\}$, $G_7 = \{720, 1440\}$ and $H_2 = \{-6, -3, 0, 3, 6\}$. Then we have

$$\begin{aligned}
B_2 &= \{3, 6\} \cup \big(\{720, 1440\} + \{-6, -3, 0, 3, 6\}\big)\\
&= \{3, 6, 718, 719, 720, 721, 722, 1438, 1439, 1440, 1441, 1442\}.
\end{aligned}$$

Finally, set B_3 corresponds to $\mathcal{L}_3 = \{4, 6\}$ and $\ell_{e_3} = 6$. Since $\ell_{e_3} = \max \mathcal{L}_3$, the union over $\ell \in \mathcal{L}'_3$ in (2.10) is the empty set. Then

$$B_3 = E_{\ell_{e_3}} + \sum_{\substack{p \in \{4,6\} \\ p < \ell}} H_p = E_6 + H_4,$$

with $E_6 = \{180\}$ and $H_4 = \{-45, -15, 15, 45\}$. Hence

$$B_3 = \{180\} + \{-45, -15, 15, 45\} = \{135, 165, 195, 225\},$$

and B_1, B_2 and B_3 is the unique sum-and-distance system corresponding to the joint ordered factorisation $\mathcal{J}$.

2.4 Invariant properties of additive systems

The paper [40] concludes by noting that for $m = 2$, and $|B_1| = |B_2|$, inclusive and non-inclusive sum-and-distance systems have the general property that the sum of squares of all entries of their component sets is invariant, determined only by the cardinality $|B_j|$, as stated in the following proposition.

Proposition 2.4.1. Let $n \in \mathbb{N}$ and $\{\{a_1, \dots, a_n\}, \{b_1, \dots, b_n\}\}$ be a (non-inclusive or inclusive) sum-and-distance system. Then we have that

$$\sum_{j=1}^{n}(a_j^2 + b_j^2) = \begin{cases} \quad \frac{1}{3!}\,(2n)((2n)^4 - 1) & \textit{in the non-inclusive case,} \\ \frac{1}{4!}\,(2n+1)((2n+1)^4 - 1) & \textit{in the inclusive case.} \end{cases}$$

Irrespective of our updated terminology of sum-and-distance systems, the results presented in Proposition 2.4.1 demonstrate an invariant sums of squares property for 2-part sum-and-distance systems. This invariant property implies that the n elements for each sum-and-distance system component set can be viewed as comprising the coordinates of lattice points on a sphere centred at the origin of an n-dimensional Euclidean space, with radius given by the cases present in the theorem, emphasising the geometric interpretation of the Minkowski sum.

As this was proven in the case of $m = 2$, the remainder of this section is dedicated to generalising this invariant sum of squares to m-part sum-and-distance systems.

As a by-product of our investigations we will deduce three additional invariant properties inherent in additive systems, as well as other related properties, such as the sum of elements in sum system components and sum-and-distance system components, the latter invariant property being discussed in Chapter 4.

The first two of these invariant properties are results from [49], of which this study's author is a co-author.

We begin with the following useful lemma.

Lemma 2.4.2. Let A and B be two disjoint sets with elements a and b respectively, satisfying the set cardinality condition $|A||B| = |A + B|$, so that $a_i + b_j \neq a_u + a_v$, for all index pairs satifying $(i, j) \neq (u, v)$. Furthermore, let B be symmetric around the origin. Then we have

$$\sum_{c\in(A+B)} c = |B| \sum_{a\in A} a, \quad \text{and} \quad \sum_{c\in(A+B)} c^2 = |B| \sum_{a\in A} a^2 + |A| \sum_{b\in B} b^2.$$

Proof. We have $A+B = \{a_1+B, a_2+B, \ldots, a_{|A|}+B\}$, and taking the sum over all elements in $A+B$, in conjunction with $\sum_{b\in B} b = 0$, gives us

$$\sum_{c\in(A+B)} c = (a_1+B) + \cdots + (a_{|A|}+B) = \sum_{i=1}^{|A|}\sum_{j=1}^{|B|}(a_i+b_j) = |B|\sum_{i=1}^{|A|} a_i + |A|\sum_{i=1}^{|B|} b_i = |B|\sum_{a\in A} a,$$

and for the sum of elements squared we have

$$\begin{aligned}\sum_{c\in(A+B)} c^2 =&(a_1+B)^2 + \cdots + (a_{|A|}+B)^2 = \sum_{i=1}^{|A|}\sum_{j=1}^{|B|}(a_i^2 + a_ib_j + b_j^2)\\ =&|B|\sum_{i=1}^{|A|} a_i^2 + \sum_{i=1}^{|A|}\sum_{i=1}^{|B|} a_ib_j + |A|\sum_{i=1}^{|B|} b_i^2 = |B|\sum_{a\in A} a^2 + |A|\sum_{b\in B} b^2,\end{aligned}$$

as the sum of the cross-terms is zero, and hence the result. □

We first establish the summation invariances for the elements of sum system component sets, detailed in the below lemma.

Lemma 2.4.3. Let $m \in \mathbb{N}_2$, $n \in \mathbb{N}_2^m$, and $A_1, \ldots, A_m$ an m-part sum system with $|A_j| = n_j$ and $\sum\limits_{j=1}^{m} A_j = \langle N\rangle$. Then

$$\sum_{s\in\langle N\rangle} s = T_{N-1} = \frac{(N-1)N}{2}, \tag{2.12}$$

where T_i is the i-th triangular number for $i \in \mathbb{N}$. Furthermore, for $j \in \{1, \ldots, m\}$, we have

$$\sum_{a\in A_j} a = \frac{n_j}{2}\max A_j. \tag{2.13}$$

Proof. The target set of any sum system is the consecutive integers from 0 to $N-1$. Summing over these integers equates to the $(N-1)$-th triangular number, and thus Eq. (2.12). We know from Proposition 2.2.4 that each sum system component set A_j is palindromic, centred about $(\max A_j)/2$, with $a_i + a_{n_j-1-i} = \max A_j$. When summing over A_j, we can pair palindromic elements together to obtain

$$\sum_{a\in A_j} a = \frac{|A_j|}{2}\max A_j = \frac{n_j}{2}\max A_j,$$

and hence Eq. (2.13). □

Corollary 2.4.4. Let $m \in \mathbb{N}_2$, $n \in \mathbb{N}_2^m$, $N = \prod_{j=1}^m n_j$ and let $\mathcal{J}$ be a joint ordered factorisation of n with $A_1, \ldots, A_m$ the corresponding sum system. Set $n_{j_0} = n_{j_{L+1}} = 0$. Then the sum over each element across all component sets is given by

$$\sum_{j=1}^m \sum_{a \in A_j} a = \frac{1}{2} \sum_{\ell=1}^{L+1} F(\ell)\big(n_{j_{\ell-1}} - n_{j_\ell}\big). \tag{*}$$

If $n_j = \bar{n} \in \mathbb{N}_2$ for all $j \in \{1, \ldots, m\}$, then

$$\sum_{j=1}^m \sum_{a \in A_j} a = \frac{\bar{n}}{2}(N-1). \tag{**}$$

Proof. The partial product F satisfies the relation $F(\ell)f_\ell = F(\ell+1)$. Combining this with Eq. (2.13), we find that

$$\begin{aligned}\sum_{j=1}^m \sum_{a \in A_j} a = \frac{1}{2}\sum_{j=1}^m n_j \max A_j &= \frac{1}{2}\sum_{j=1}^m \left(n_j \sum_{\ell \in \mathcal{L}_j} F(\ell)(f_\ell - 1)\right) \\ &= \frac{1}{2}\sum_{\ell=1}^{L} n_{j_\ell} F(\ell)(f_\ell - 1) \\ &= \frac{1}{2}\sum_{\ell=1}^{L} n_{j_\ell} F(\ell+1) - \frac{1}{2}\sum_{\ell=1}^{L} n_{j_\ell} F(\ell) \\ &= \frac{1}{2}\sum_{\ell=2}^{L+1} n_{j_{\ell-1}} F(\ell) - \frac{1}{2}\sum_{\ell=1}^{L} n_{j_\ell} F(\ell),\end{aligned}$$

and collecting like terms, we deduce Eq. (*).

Eq. (**) follows by setting $n_{j_{\ell-1}} = n_{j_\ell} = \bar{n}$ in Eq. (*), for all $\ell \in \{2, \ldots, L\}$, where all terms cancel except $-F(1) = -1$ and $F(L+1) = N$. □

We now give our first invariant quantity, $\sigma_A(N)$, that considers the weighted sum of terms across a sum system.

Corollary 2.4.5. Let $m \in \mathbb{N}_2$, $n \in \mathbb{N}_2^m$ and $N = \prod_{j=1}^m n_j$. Then all sum systems, $A_1, \ldots, A_m$, with target set $\langle N \rangle$ satisfy

$$\frac{1}{N}\sigma_A(N) := \sum_{j=1}^m \frac{1}{n_j} \sum_{a \in A_j} a = \frac{N-1}{2}. \tag{2.14}$$

Proof. Using Eq. (2.13), we can write

$$\sum_{j=1}^{m}\frac{1}{n_j}\sum_{a\in A_j}a=\frac{1}{2}\sum_{j=1}^{m}\max A_j=\frac{N-1}{2},$$

as required. □

It is Eq. (2.14) that establishes an invariant property for sum systems; for a fixed $N\in\mathbb{N}$, the sum over weighted sums of sum system component sets, which have target set $\langle N\rangle$, is constant. It is independent of our choice of the number of m-parts and the joint ordered factorisation.

Furthermore, we can write Eq. (2.14) in terms of Eq. (2.12) such that

$$\sigma_A(N):=\sum_{s\in\langle N\rangle}s=N\sum_{j=1}^{m}\frac{1}{n_j}\sum_{a\in A_j}a=T_{N-1}.$$

The presence of the $\frac{1}{N}$ factor in Eq. (2.14) is consistent with the approach used in [49].

The following result involves our next invariant property, $\tau_C(N)$, that considers the sum over the target set for a sum-and-distance system.

Theorem 2.4.6. Let $N\in\mathbb{N}$. Then

$$\tau_C(N):=\sum_{s\in\langle N\rangle-\frac{N-1}{2}}s^2=\frac{1}{12}N(N^2-1).$$

Proof. As $\big\langle N\big\rangle-\frac{N-1}{2}$ is symmetric around the origin, it is sufficient to find twice the sum of squares for just the positive half of the component set. That is to say,

$$\sum_{s\in\langle N\rangle-\frac{N-1}{2}}s^2=2\sum_{s\in\{\delta,\dots,\frac{N-1}{2}\}}s^2=\begin{cases}\frac{1}{2}\sum\limits_{i=1}^{\frac{N}{2}}\big(2i-1\big)^2, & \text{if } N \text{ even},\\ 2\sum\limits_{i=1}^{\frac{N-1}{2}}i^2, & \text{if } N \text{ odd},\end{cases}$$

where $\delta=1$ if N is odd and $\delta=\frac{1}{2}$ if N is even. We evaluate this expression using the identities

$$\sum_{i=1}^{x}(2i-1)^2=\frac{x(4x^2-1)}{3},\quad\text{and}\quad\sum_{i=1}^{x}i^2=\frac{x(x+1)(2x+1)}{6},$$

so that

$$\sum_{s\in\langle N\rangle-\frac{N-1}{2}}s^2=\begin{cases}\frac{1}{2}\times\frac{\frac{N}{2}\left(4\left(\frac{N}{2}\right)^2-1\right)}{3}=\frac{N(N^2-1)}{12}, & (N \text{ even}),\\ 2\frac{\left(\frac{N-1}{2}\right)\left(\frac{N-1}{2}+1\right)\left(2N-1\right)}{6}=\frac{N(N^2-1)}{12}, & (N \text{ odd}),\end{cases}$$

as required. □

Remark 2.4.7. Theorem 2.4.6 is Theorem 1 of [49], in which *centred sum systems* are considered instead of sum-and-distance systems. A centred sum system $C_1, \ldots, C_m \subset \mathbb{Z}$ satisfies $\sum_{j=1}^{m} C_j = \langle N \rangle - \frac{N-1}{2}$, and Lemma 1 of the same paper proves that the component sets are $C_j = (B_j) \cup (-B_j)$ $(j \in J_e)$ and $C_j = (B_j) \cup \{0\} \cup (-B_j)$ $(j \in J_o)$. Within this context, Theorem 2.4.6 establishes our second invariant property on N, where the weighted sum of squares of centred sum system components is constant and independent of our choice for joint ordered factorisation. As centred sum systems components exist as unions of sum-and-distance systems, Theorem 2.4.6 partially answers the motivational interest of generalising Proposition 2.4.1 to $m > 2$. Additionally we have the relation

$$\tau_C(N) = \frac{N+1}{6} \sigma_A(N).$$

Before considering further invariant properties of sum-and-distance systems we introduce the following useful identities. Recall the arithmetic progressions H_ℓ, E_ℓ and G_ℓ from Definition 2.3.1. For $j \in \{1, \ldots, m\}$ and $\ell \in \mathcal{L}_j = \{\ell_1, \ldots, \ell_{k_j}\}$, for suitable $k_j \in \mathbb{N}$, we have

$$\prod_{\substack{p \in \mathcal{L}_j \\ p < \ell}} |H_p| = \prod_{\substack{p \in \mathcal{L}_j \\ p < \ell}} f_p = P_j(\ell). \tag{2.15}$$

For $\ell_i \in \mathcal{L}_j$, with $i \in \{1, \ldots, k_j\}$, we have

$$f_{\ell_i} P_j(\ell_i) = f_{\ell_i} \prod_{\substack{p \in \mathcal{L}_j \\ p < \ell_i}} f_p = \prod_{\substack{p \in \mathcal{L}_j \\ p \leq \ell_i}} f_p = P_j(\ell_i + 1) = P_j(\ell_{i+1}),$$

and if $i = k_j$ then $P_j(\ell_{k_j} + 1) = P_j(\ell_{k_j+1}) = n_j$. To streamline notation, let

$$\sum_{\substack{p \in \mathcal{L}_j \\ p < \ell}} H_p = \mathcal{H}_\ell.$$

Theorem 2.4.8. Let $m \in \mathbb{N}_2$, $n \in \mathbb{N}_2^m$, and let $\mathcal{J}$ be a joint ordered factorisation of n with $B_1, \ldots, B_m$ the corresponding m-part sum-and-distance system. Then, for $j \in \{1, \ldots, m\}$, the sum of elements in a component set, ΣB_j, is given by

$$\Sigma B_j = \sum_{b \in B_j} b = \frac{1}{8} \left(F(\ell_{e_j}) P_j(\ell_{e_j}) f_{\ell_{e_j}}^2 + \sum_{\ell \in \mathcal{L}'_j} P_j(\ell) F(\ell) (f_\ell^2 - 1) \right). \tag{2.16}$$

Proof. We fix $j \in \{1, \ldots, m\}$ and assume $\exists\ \ell_{e_j} = \ell_e \in \mathcal{L}_j$. Theorem 2.3.3 implies B_j is the union of disjoint sets, so that summing over B_j sums over each disjoint set gives us

$$\Sigma B_j = \sum_{b\in B_j} b = \sum_{g\in(E_{\ell_e}+\mathcal{H}_{\ell_e})} g + \sum_{\ell\in\mathcal{L}'_j} \sum_{g\in(G_\ell+\mathcal{H}_\ell)} g = P_j(\ell_e) \sum_{g\in E_{\ell_e}} g + \sum_{\ell\in\mathcal{L}'_j} P_j(\ell) \sum_{g\in G_\ell} g,$$

where we have used Lemma 2.4.2 and Eq. (2.15). Evaluating the sums over E_{ℓ_e} and G_ℓ respectively yields

$$\sum_{g\in E_{\ell_e}} g = \frac{1}{2}F(\ell_e) \sum_{\substack{\alpha\in\langle f_{\ell_e}\rangle \\ \alpha \text{ odd}}} \alpha = \frac{1}{2}F(\ell_e)\left(\frac{f_{\ell_e}}{2}\right)^2 = \frac{1}{8}F(\ell_e)f_{\ell_e}^2,$$

and

$$\sum_{g\in G_\ell} g = F(\ell) \sum_{\alpha\in\left\langle \frac{f_\ell-1}{2}\right\rangle+1} \alpha = F(\ell)\, T_{\frac{f_\ell-1}{2}} = F(\ell)\frac{\left(\frac{f_\ell-1}{2}\right)\left(\frac{f_\ell-1}{2}+1\right)}{2} = \frac{1}{8}F(\ell)(f_\ell-1)^2.$$

Substituting these expressions into the first equation above yields the desired result. □

Remark 2.4.9. If $\nexists\ \ell_{e_j} \in \mathcal{L}_j$, i.e. n_j is odd, then

$$\Sigma B_j = \sum_{b\in B_j} b = \frac{1}{8}\sum_{\ell\in\mathcal{L}_j} P_j(\ell)F(\ell)(f_\ell^2-1).$$

Theorem 2.4.10. Let $m \in \mathbb{N}$, $n \in \mathbb{N}_2^m$, and let $\mathcal{J}$ be a joint ordered factorisation of n with sum-and-distance system $B_1, \ldots, B_m$. Then for $j \in \{1, \ldots, m\}$, the sum of elements squared in B_j is given by

$$\sum_{b\in B_j} b^2 = \frac{n_j}{24}\sum_{\ell\in\mathcal{L}_j} F(\ell)^2(f_\ell^2-1). \tag{2.17}$$

Proof. Fix $j \in \{1, \ldots, m\}$ and assume $\exists\ \ell_{e_j} = \ell_e \in \mathcal{L}_j$. As Theorem 2.3.3 implies B_j is the union of disjoint sets, then summing over B_j sums over each disjoint set as follows

$$\begin{aligned}\sum_{b\in B_j} b^2 &= \sum_{g\in(E_{\ell_e}+\mathcal{H}_{\ell_e})} g^2 + \sum_{\ell\in\mathcal{L}'_j}\sum_{g\in(G_\ell+\mathcal{H}_\ell)} g^2 \\ &= P_j(\ell_e)\sum_{g\in E_{\ell_e}} g^2 + \left|E_{\ell_e}\right| \sum_{h\in\mathcal{H}_{\ell_e}} h^2 + \sum_{\ell\in\mathcal{L}'_j}\left(P_j(\ell)\sum_{g\in G_\ell} g^2 + \left|G_\ell\right|\sum_{h\in\mathcal{H}_\ell} h^2\right),\end{aligned}$$

using Lemma 2.4.2 and Eq. (2.15). The sums of squares over E_{ℓ_e} and G_ℓ are given by

$$\sum_{g\in E_{\ell_e}} g^2 = F(\ell_e)^2\frac{1}{4}\sum_{i=1}^{\frac{f_{\ell_e}}{2}}(2i-1)^2 = \frac{1}{24}F(\ell_e)^2 f_{\ell_e}(f_{\ell_e}^2-1),$$

$$\sum_{g\in G_\ell} g^2 = F(\ell)^2 \sum_{i=1}^{\frac{f_\ell-1}{2}} i^2 = \frac{1}{24}F(\ell)^2 f_\ell(f_\ell^2-1).$$

By repeatedly applying Lemma 2.4.2, along side the second expression in Eq. (2.8) (since the sum of squares over E_{ℓ_e} and G_ℓ are equal when $\ell = \ell_e$), we can write

$$\sum_{h\in\mathcal{H}_\ell} h^2 = \sum_{\substack{p\in\mathcal{L}_j\\ p<\ell}} \left(\frac{2P_j(\ell)}{f_p}\sum_{g\in G_p} g^2\right) = 2P_j(\ell)\sum_{\substack{p\in\mathcal{L}_j\\ p<\ell}}\left(\frac{1}{f_p}\sum_{g\in G_p} g^2\right) = \frac{P_j(\ell)}{12}\sum_{\substack{p\in\mathcal{L}_j\\ p<\ell}} F(p)^2(f_p^2-1).$$

Substituting these results into the first equation returns

$$\begin{aligned}\sum_{g\in(E_{\ell_e}+\mathcal{H}_{\ell_e})} g^2 &= P_j(\ell_e)\sum_{g\in E_{\ell_e}} g^2 + \left|E_{\ell_e}\right| \sum_{h\in\mathcal{H}_{\ell_e}} h^2\\ &= \frac{P_j(\ell_e)f_{\ell_e}}{24}F(\ell_e)^2(f_{\ell_e}^2-1) + \frac{P_j(\ell_e)f_{\ell_e}}{24}\sum_{\substack{p\in\mathcal{L}_j\\ p<\ell_e}} F(p)^2(f_p^2-1)\\ &= \frac{P_j(\ell_{e+1})}{24}\sum_{\substack{p\in\mathcal{L}_j\\ p<\ell_{e+1}}} F(p)^2(f_p^2-1).\end{aligned}$$

and, for $\ell_i \in \mathcal{L}'_j = \{\ell_{e+1},\ldots,\ell_{k_j}\}$, then

$$\begin{aligned}\sum_{g\in(G_{\ell_i}+\mathcal{H}_{\ell_i})} g^2 &= P_j(\ell_i)\sum_{g\in G_{\ell_i}} g^2 + \left|G_{\ell_i}\right| \sum_{h\in\mathcal{H}_{\ell_i}} h^2\\ &= \frac{P_j(\ell_i)f_{\ell_i}}{24}F(\ell_i)^2(f_{\ell_i}^2-1) + \frac{P_j(\ell_i)(f_{\ell_i}-1)}{24}\sum_{\substack{p\in\mathcal{L}_j\\ p<\ell_i}} F(p)^2(f_p^2-1)\\ &= \frac{P_j(\ell_{i+1})}{24}\sum_{\substack{p\in\mathcal{L}_j\\ p<\ell_{i+1}}} F(p)^2(f_p^2-1) - \frac{P_j(\ell_i)}{24}\sum_{\substack{p\in\mathcal{L}_j\\ p<\ell_i}} F(p)^2(f_p^2-1)\end{aligned}$$

which becomes a telescoping sum when summed over $\ell_i \in \mathcal{L}'_j$. After cancellation, the two remaining terms are

$$\begin{aligned}\sum_{\ell\in\mathcal{L}'_j}\sum_{g\in(G_{\ell_i}+\mathcal{H}_{\ell_i})} g^2 &= \frac{P_j(\ell_{k_j+1})}{24}\sum_{\substack{p\in\mathcal{L}_j\\ p<\ell_{k_j+1}}} F(p)^2(f_p^2-1) - \frac{P_j(\ell_{e+1})}{24}\sum_{\substack{p\in\mathcal{L}_j\\ p<\ell_{e+1}}} F(p)^2(f_p^2-1)\\ &= \frac{n_j}{24}\sum_{\ell\in\mathcal{L}_j} F(\ell)^2(f_\ell^2-1) - \sum_{g\in(E_{\ell_e}+\mathcal{H}_{\ell_e})} g^2.\end{aligned}$$

Eq. (2.17) then follows from rearranging the above equation. If $\nexists\ \ell_e \in \mathcal{L}_j$, then $\mathcal{L}'_j = \mathcal{L}_j$, the set of $p \in \mathcal{L}_j$ with $p < \ell_1$ is empty, and the sum over $E_{\ell_e} + \mathcal{H}_{\ell_e}$ is zero. This leaves only

$$\sum_{b\in B_j} b^2 = \frac{n_j}{24}\sum_{\ell\in\mathcal{L}_j} F(\ell)^2(f_\ell^2-1),$$

as required. □

Corollary 2.4.11. Let $m \in \mathbb{N}$, $n \in \mathbb{N}_2^m$, $N = \prod_{j=1}^m n_j$, and let $\mathcal{J}$ be a joint ordered factorisation of n with the sum-and-distance system $B_1, \ldots, B_m$. Set $n_{j_0} = n_{j_{L+1}} = 0$. Then the sum of elements squared across all component sets is given by

$$\sum_{j=1}^{m} \sum_{b \in B_j} b^2 = \frac{1}{24} \sum_{\ell=1}^{L+1} F(\ell)^2 \big(n_{j_{\ell-1}} - n_{j_\ell}\big). \tag{*}$$

If $n_j = \bar{n} \in \mathbb{N}$ for all $j \in \{1, \ldots, m\}$, then

$$\sum_{j=1}^{m} \sum_{b \in B_j} b^2 = \frac{\bar{n}}{24} \big(N^2 - 1\big). \tag{**}$$

Proof. Eq. (*) is achieved by applying the same arguments present in the proof of Corollary 2.4.4 to the double sum

$$\sum_{j=1}^{m} \sum_{b \in B_j} b^2 = \frac{1}{24} \sum_{j=1}^{m} \left(n_j \sum_{\ell \in \mathcal{L}_j} F(\ell)^2 (f_\ell^2 - 1) \right).$$

Eq. (**) follows by setting $n_{j_{\ell-1}} = n_{j_\ell} = \bar{n}$ in Eq. (*), for all $\ell \in \{2, \ldots, L\}$, where all terms cancel except $-F(1)^2 = -1$ and $F(L+1)^2 = N^2$. □

The following result is the third invariant invariant property established in this chapter. Given by $\sigma_B(N)$, it relates to sum-and-distance systems.

Corollary 2.4.12. Let $m \in \mathbb{N}$, $n \in \mathbb{N}_2^m$ and $N = \prod_{j=1}^m n_j$. Then all sum-and-distance systems, $B_1, \ldots, B_m$, with target set $\langle N \rangle - \frac{N-1}{2}$ satisfy

$$\sigma_B(N) := \sum_{j=1}^{m} \frac{1}{n_j} \sum_{b \in B_j} b^2 = \frac{1}{24} \big(N^2 - 1\big). \tag{2.18}$$

Proof. By multiplying Eq. (2.17) by $\frac{1}{n_j}$ and summing over j from 1 to m, we obtain the telescoping sum

$$\begin{aligned} \sigma_B(N) = \sum_{j=1}^{m} \frac{1}{n_j} \sum_{b \in B_j} b^2 &= \frac{1}{24} \sum_{j=1}^{m} \sum_{\ell \in \mathcal{L}_j} F(\ell)^2 \big(f_\ell^2 - 1\big) \\ &= \frac{1}{24} \sum_{\ell=1}^{L} \Big(F(\ell+1)^2 - F(\ell)^2\Big) = \frac{1}{24} \Big(N^2 - 1\Big), \end{aligned}$$

as required. □

It is Eq. (2.18) that generalises the invariant sum of squares of Proposition 2.4.1, as found in [40], to an arbitrary dimension $m \in \mathbb{N}$. The right hand side of this expression is constant. It is independent of how many m-parts the system is comprised of, as well as the choice of joint ordered factorisation used. Therefore, any sum-and-distance system with target set $\langle N \rangle - \frac{N-1}{2}$ satisfies this identity and is thus invariant. The notation $\sigma_B(N)$ brings this result in line with that used in [49].

Remark 2.4.13. Geometrically, Eq. (2.18) establishes a constraint on the shape of the resulting integer lattice which sum-and-distance systems are associated to. If we label the j-th axis of an m-dimensional lattice in $\mathbb{Z}^m$ with the elements from B_j, the resulting N (half) integer lattice points form an ellipsoid in N-dimensional Euclidean space. The term $\frac{1}{n_j}$ is thus an axis normalisation factor that transform these (half) integer lattice points on the ellipsoid into (half) integer lattice points on an N-dimensional sphere, centred at the origin, with radius

$$\sqrt{\sigma_B(N)} = \sqrt{\frac{1}{24}\big(N^2 - 1\big)}.$$

Given that the Minkowski sum is inherently a geometric operation (see Section 2.1 for more) this interpretation provides a limitation on these additive structures.

Example 2.4.14. Let $m = 3$, $n = (18, 25, 8)$ and consider the joint ordered factorisation $\mathcal{J} = \big((1,3),(2,5),(1,2),(3,4),(1,3),(3,2),(2,5)\big)$, with $\mathcal{L}_1 = \{1,3,5\}$, $\ell_{e_1} = 3$, $\mathcal{L}_2 = \{2,7\}$, $\ell_{e_2} = 0$, $\mathcal{L}_3 = \{4,6\}$ and $\ell_{e_3} = 6$. The sum-and-distance system component sets are

$$\begin{aligned} B_1 =& \tfrac{1}{2}\{13,15,17,223,225,227,253,255,257\},\\ B_2 =& \{3,6,718,719,720,721,722,1438,1439,1440,1441,1442\},\\ B_3 =& \{135,165,195,225\}. \end{aligned}$$

By Theorem 2.4.8, the sum over the terms of each set above are as follows.

$$\begin{aligned} \sum_{b\in B_1} b =& \frac{1}{8}\Big(F(\ell_{e_1})P_1(\ell_{e_1})f_{\ell_{e_1}}^2 + \sum_{\ell\in\{5\}} F(\ell)P_1(\ell)(f_\ell^2 - 1)\Big)\\ =& \frac{1}{8}\Big(15 \times 3 \times 4 + 120 \times 6 \times (9-1)\Big) = 742.5, \end{aligned}$$

and likewise $\sum_{b\in B_2} b = 10809$ and $\sum_{b\in B_3} b = 720$. The target set of this sum-and-distance system is $\frac{1}{2}\{-3599, -3597, \ldots, 3597, 3599\}$, and by Theorem 2.4.6 we have

$$\tau_C(3600) = \tfrac{1}{12}3600(3600^2 - 1) = 3\,887\,999\,700.$$

By Theorem 2.4.10, the sum of the square of each component set is

$$\begin{aligned}\sum_{b\in B_1} b^2 =&\frac{1}{24}n_1 \sum_{\ell\in\{1,3,5\}} F(\ell)^2(f_\ell^2-1)\\ =&\frac{1}{24}18\Big(1\times(9-1)+15^2\times(4-1)+120^2\times(9-1)\Big)=86912.25,\end{aligned}$$

and likewise $\sum_{b\in B_2} b^2 = 12960225$ and $\sum_{b\in B_3} b^2 = 134100$. Finally, we have the invariant property

$$\sigma_B(3600) = \tfrac{1}{24}(3600^2-1) = 539999.958\dot{3},$$

which is invariant of our choice of joint ordered factorisations $\mathscr{J}$ of $n = (18, 25, 8)$. Indeed, if we take the sum-and-distance systems corresponding to $\big((2,5),(1,3),(3,8),(1,6),(2,5)\big)$ and $\big((1,18),(2,25),(3,8)\big)$, we find the same evaluation also yields $539999.958\dot{3}$.

2.5 Conclusion

We modified the definition of a sum-and-distance system such that they no longer require that the cardinality of each component sets have the same parity, allowing a hybrid of odd and even set sizes. This extension then completes the picture of additive systems, associating every integer with a host of sum systems and now sum-and-distance systems, relying only on how we factorise said integer.

As there is a bijection between joint ordered factorisations and a sum-and-distance systems, we have been able to find a closed form that constructs the latter via the former, akin to Theorem 6.7 of [42].

With this explicit formula we are then able to perform arithmetic analysis on these additive systems. In particular, we generalised the invariant sum of squares property in Proposition 2.4.1 to allow for any number of sets. Additionally, we found the weighted sum over a sum system component set constituted its own invariant property for sum systems. We will see that the sum over sum-and-distance system components have an invariant property also, though only in cases where their cardinalities are prime powers (see Chapter 4 for more).

Chapter 3

On the Number of Factorisation Classes

3.1 Enumeration functions

In number theory and combinatorics the question is often to count the number of solutions or configurations for a given object type, establishing connecting relationships and identities where possible. In this chapter, for given natural numbers m and N, our focus is to count the number of m-part sum systems with target set $\langle N \rangle = \{0, 1, \ldots, N-1\}$, which we denote $\mathcal{N}_m(N)$. We deduce a formula for $\mathcal{N}_m(N)$, employing the Stirling numbers of the second kind $S(k, n)$, and go on to show that this counting function satisfies an implicit three term recurrence relation, thus correcting in the two-dimensional case the results of C. T. Long, and in the general m-dimensional case, providing deeper insights into recurrence relations for the number of multi-factorisations.

By extension, $\mathcal{N}_m(N)$ also counts the number of joint ordered factorisations of $n \in \mathbb{N}_2^m$ such that $\prod_{j=1}^{m} n_j = N$. As such, this enumeration considers the ordering of component sets to be important. This is because the enumeration on joint ordered factorisations will consider $\big((1, f), (2, g)\big)$ to be different from $\big((2, f), (1, g)\big)$, even though their resulting sum systems will be identical up to a change of indices. To retrieve the enumeration for the number of sum systems with order unimportant, one would consider $\mathcal{N}_m(N)/m!$, which might feel more natural when considering sum systems.

The enumeration of these objects uses the following function.

Proposition 3.1.1. Let $n \in \mathbb{N}$ and $1 \leq j \leq \Omega(n)$. We define $c_j(n)$ to be the *j-th non-trivial divisor function* which counts the number of ordered non-trivial factorisations of n into j factors, so that that each factor ≥ 2. If $n = p_1^{a_1} \dots p_{\omega(n)}^{a_{\omega(n)}}$ then

$$c_j(n) = \sum_{k=0}^{j} (-1)^k \binom{j}{k} \prod_{l=1}^{\omega(n)} \binom{a_l + j - k - 1}{a_l}, \tag{3.1}$$

where $\omega(n)$, the prime counting function, counts the number of distinct prime factors of n.

Proof. See [57]. □

Example 3.1.2. Let $n = 12$ and $j = 2$. The number of ways to write 12 as 2 non-trivial factors is

$$\begin{aligned} c_2(12) &= \sum_{k=0}^{2} (-1)^k \binom{2}{k} \prod_{l=1}^{2} \binom{a_l + 1 - k}{a_l} = \sum_{k=0}^{2} (-1)^k \binom{2}{k} \binom{3-k}{2} \binom{2-k}{1} \\ &= \binom{2}{0}\binom{3}{2}\binom{2}{1} - \binom{2}{1}\binom{2}{2}\binom{1}{1} + \binom{2}{2}\binom{1}{2}\binom{0}{1} \\ &= 6 - 2 + 0 = 4, \end{aligned}$$

which are 2 × 6, 3 × 4, 4 × 3 and 6 × 2.

The initial discovery of this closed form for $c_j(n)$ is attributed to MacMahon [57] in 1892, where he counted *multipartite numbers*, which were ordered multi-factorisations of integers.

The summatory function $\sum_{j=1}^{\Omega(n)} c_j(n)$ has since gained a great deal more attention. The asymptotic behaviour of this summation had been pioneered by Kalmár [46] in 1931, and been mentioned on page 7 of the second edition of [83] in 1951. A comprehensive survey of modern (2012) studies is given in [47], with [78] (2016) detailing further works on the topic.

Interestingly, Long [53] used this function to enumerate all complementing subsets (which are now known as 2-part sum systems) of the set $\langle n \rangle$, bridging the theory between additive systems and ordered factorisations back in 1967. Unfortunately there was an error in his count, which we correct in this work. In the 2000s, Munagi [64] also made the connection between this function and k-complementing subsets (k-part sum systems), as well as establishing the bijection between these systems and ordered factorisations [65].

It is works [51, 40] that are most relevant to this study, published in the 2019 and 2020 respectively. In the former, Lettington and Schmidt introduce generalised results of concepts explored in [78, 28, 77] by way of the *associated* (j,r)*-divisor function* $c_j^{(r)}(n)$, for $r \in \mathbb{Z}$.

It was demonstrated in [51] that this arithmetic function counts the ordered factorisations of n into $j+r$ factors, of which the first j must be ≥ 2. This function appears to be new to the field, seamlessly incorporating itself into various previously well-known relations as a natural extension of these identities (such as Theorem 2 in [51] extending Corollary 2.1, Eq. (2.12) and Eq. (2.13) in [78]).

When $r < 0$, the associated divisor function involves factorising n into $\max\{j, -r\}$ factors of which at least j must be non-trivial, and at least $-r$ factors must be square-free [49]. We shall give reasoning why in Section 3.2.

Proposition 3.1.3. Let $n \in \mathbb{N}$, $1 \leq j \leq \Omega(n)$ and $r \in \mathbb{Z}$. The associated divisor function has the explicit form

$$c_j^{(r)}(n) = \sum_{k=0}^{j} (-1)^k \binom{j}{k} \prod_{l=1}^{\omega(n)} \binom{a_l + j + r - k - 1}{a_l}. \tag{3.2}$$

Proof. See Theorem 1 in [51] or Lemma 11 in [40]. □

We see that Eq. (3.2) introduces an addition term in the inner binomial coefficient in MacMahon's expression, Eq. (3.1). This substitution of j for $j+r$ imbalances the alternating binomial coefficients of the sum, subtly altering what is being enumerated. We retrieve Eq. (3.1) by setting $r = 0$ in Eq. (3.2), i.e. $c_j^{(0)} = c_j$.

The most relevant occurrence of this function is found in Theorem 4 of [51], where the authors proved the following enumeration. We use a multinomial coefficient in the result, namely for $\ell \in \mathbb{N}_0^m$, with $|\ell| = \ell_1 + \cdots + \ell_m$, we use $\binom{|\ell|}{\ell_1, \ldots, \ell_m}$, which has the combinatorial interpretation of the number of ways to put $|\ell|$ distinct objects into m groupings, with ℓ_1 objects in the first grouping, ℓ_2 objects in the second groupings, and so on. The multinomial coefficient is given by

$$\binom{|\ell|}{\ell_1, \ldots, \ell_m} = \frac{|\ell|!}{(\ell_1!)(\ell_2!) \ldots (\ell_m!)},$$

and we note, for a given $L \in \mathbb{N}$, we have the following identity

$$\sum_{\substack{\ell \in \mathbb{N}_0^m \\ |\ell| = L}} \binom{L}{\ell_1, \dots, \ell_m} x_1^{\ell_1} x_2^{\ell_2} \dots x_m^{\ell_m} = (x_1 + x_2 + \cdots + x_m)^L,$$

for any variable $x_1, \dots, x_m \in \mathbb{N}$. We shall use the special case when $x_1 = x_2 = \cdots = x_m = 1$ for which we have

$$\sum_{\substack{\ell \in \mathbb{N}_0^m \\ |\ell| = L}} \binom{L}{\ell_1, \dots, \ell_m} 1^{\ell_1} 1^{\ell_2} \dots 1^{\ell_m} = m^L. \tag{3.3}$$

Proposition 3.1.4. Let $m \in \mathbb{N}$, and $n = (n_1, \dots, n_m) \in \mathbb{N}_2^m$. Then the number of different joint ordered factorisations (and hence sum systems) of n is given by

$$N_m(n) = \sum_{\ell \in \mathbb{N}^m} \binom{|\ell|}{\ell} \prod_{j=1}^{m} c_{\ell_j}^{(-\ell_j)}(n_j), \tag{3.4}$$

where $\binom{|\ell|}{\ell}$ is a multinomial coefficient.

Like many important functions in number theory, $c_j(n)$ concerns itself with the prime signature of n rather than the prime factors themselves.

Lemma 3.1.5. Let $p, t \in \mathbb{N}$ with p prime, and $1 \leq j \leq t$. Then

$$c_j(p^t) = \binom{t-1}{j-1}. \tag{3.5}$$

Proof. This follows from setting $r = 0$ in Lemma 5 of [40]. □

Example 3.1.6. Let $p = 3$, $t = 5$ and $j = 3$. The number of ways to write 243 as 3 non-trivial factors is

$$c_3(3^5) = \binom{4}{2} = 6,$$

which are $3 \times 3 \times 3^3$, $3 \times 3^3 \times 3$, $3^3 \times 3 \times 3$, $3 \times 3^2 \times 3^2$, $3^2 \times 3 \times 3^2$ and $3^2 \times 3^2 \times 3$.

In consideration of m-part sum systems whose component sets have prime power cardinality, we find that $N_m(n)$ simplifies considerably, as detailed in the following corollary to Proposition 3.1.4.

Corollary 3.1.7. Let $m \in \mathbb{N}$, and $n = (p_1^{t_1}, \ldots, p_m^{t_m}) \in \mathbb{N}_2^m$, for p_j prime and $t_j \in \mathbb{N}$, for $j \in \{1, \ldots, m\}$. Then the number of different joint ordered factorisations of n is given by

$$N_m(n) = \begin{pmatrix} \sum\limits_{j=1}^{m} t_j \\ t_1, \ldots, t_m \end{pmatrix}, \tag{3.6}$$

where we use the multinomial coefficient notation.

Proof. By lemma 5 of [40], we can write $N_m(n)$ as

$$N_m(n) = \sum_{\ell \in \mathbb{N}^m} \binom{|\ell|}{\ell} \prod_{j=1}^{m} \binom{t_j - \ell_j - 1}{-1}.$$

The binomial coefficient is 0 for all $\ell_j \in \mathbb{N}$ except when $\ell_j = t_j$, such that $\binom{t_j - \ell_j - 1}{-1} = \binom{-1}{-1} = 1$. This occurs only when $\ell = (t_1, \ldots, t_m)$, which enables us to write

$$N_m(n) = \begin{pmatrix} \sum\limits_{j=1}^{m} t_j \\ t_1, \ldots, t_m \end{pmatrix} \prod_{j=1}^{m} 1,$$

as required. □

The following two sections are the latter two sections of [49], of which this work's author is a co-author.

3.2 Divisor functions and the number of m-part sum systems

In this section we enumerate all m-part joint ordered factorisations for a given natural number N, and hence all m-part sum systems with target set $\langle N \rangle$. To simplify our calculations it is convenient to work in the commutative Dirichlet convolution algebra of arithmetic functions, where the convolution of arithmetic functions $f_1, f_2, \ldots, f_j$ of $n \in \mathbb{N}$ is given by

$$(f_1 * f_2 * \cdots * f_j)(n) = \sum_{n_1 n_2 \cdots n_j = n} f_1(n_1) f_2(n_2) \cdots f_j(n_j),$$

summing over all ordered factorisations of n into j factors. We denote the j-th convolution power as $f^{*j} := f * f * \cdots * f$, where the right-hand side has j repetitions of f. By the usual convention, $f^{*0} = e$, where the function $e(n) = \delta_{n,1}$ is the neutral element of the Dirichlet convolution product, and $\delta_{n,1}$ is the Kronecker delta function. The convolution inverse of the constant function 1 is the well-known Möbius function μ. In order to state our results we first need to introduce some arithmetic divisor functions.

The j-th convolution of the constant function 1 is more generally known as the classical j-th divisor function $d_j = 1^{*j}$ [75, p. 9], which counts the ordered factorisations of its argument into j positive integer factors. For $n, j \in \mathbb{N}$, it can be shown (see section 2 of [40]) that d_j satisfies the sum-over-divisors recurrence relation

$$d_{j+1}(n) = (d_j * 1)(n) = \sum_{m|n} d_j(m) = 1^{*j+1}(n),$$

and has the Dirichlet series

$$\sum_{n=1}^{\infty} \frac{d_j(n)}{n^s} = \zeta(s)^j, \quad \text{where} \quad \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

for $\Re(s) > 1$. In contrast, the jth non-trivial divisor function c_j, only counts ordered factorisations in which all factors are greater than 1. It can be expressed as the j-fold Dirichlet convolution $c_j = (1-e)^{*j}$, and so satisfies the slightly different sum-over-divisors recurrence relation

$$c_{j+1}(n) = (c_j * (1-e))(n) = \sum_{m|n} c_j(m)\,(1-e)\left(\frac{n}{m}\right) = \sum_{m|n, m<n} c_j(m).$$

As the Dirichlet series for $1-e$ is $\zeta(s)-1$, the non-trivial divisor function c_j has the Dirichlet series

$$\sum_{n=1}^{\infty} \frac{c_j(n)}{n^s} = (\zeta(s)-1)^j\,.$$

These formulae extend to $j = 0$ when we set $c_0 = e\ = d_0$. It is important to note that c_j, unlike d_j, is *not* a multiplicative arithmetic function.

Combining these two functions yields the *associated* (j, r)*-divisor function*, defined for non-negative integers r, j as $c_j^{(r)} = (1-e)^{*j} * 1^{*r}$.

Moreover, as the constant function 1 has a convolution inverse, this definition extends naturally to negative upper indices, giving the associated $(j,-r)$-divisor function the form $c_j^{(-r)} = (1-e)^{*j} * \mu^{*r}$. Here μ is the well known Möbius function, returning $+1$ or -1 when n is square-free with respectively an even or odd number of prime factors, and 0 otherwise. (We note that $(1-e)$ does not have a convolution inverse, as $(1-e)(1) = 0$, so there is no analogous extension to negative lower indices). Popovici [69] studied the functions $c_0^{(-r)} = \mu^{*r}$. For $n \in \mathbb{N}$, in the associated $(j,-r)$-divisor functions, for the *modified Möbius function* we have that

$$(\mu - e)(n) = \begin{cases} (-1)^{\Omega(n)} & \text{if } n \text{ is square-free} \\ 0 & \text{otherwise (including the case } n = 1) \end{cases}$$

where $\Omega(n)$ is the number of prime factors of n, appears naturally. It was also shown in [51] that if $j \geq r$, then

$$c_j^{(-r)} = (1-e)^{*j-r} * ((1-e)*\mu)^{*r} = (-1)^r (1-e)^{*j-r} * (\mu - e)^{*r};$$

if $j < r$, then

$$c_j^{(-r)} = ((1-e)*\mu)^{*j} * \mu^{*r-j} = (-1)^j (\mu - e)^{*j} * \mu^{*r-j},$$

so that $c_j^{(r)}(n)$ involves factorisation of n into $\max\{j,-r\}$ factors if $r < 0$, of which at least j must be non-trivial. Also for $r < 0$, at least $-r$ factors must be square-free, and for $r \geq 0$ it follows that $c_j^{(r)}(n) = 0$ if $j > \Omega(n)$.

Also shown in [51] and [40], for $n \in \mathbb{N}$, the special case $j = -r$,

$$c_j^{(-j)}(n) = (-1)^j \sum_{n_1 n_2 \cdots n_j = n} (\mu - e)(n_1)\,(\mu - e)(n_2) \cdots (\mu - e)(n_j) = (e - \mu)^{*j}(n), \tag{3.7}$$

turns out to be particular interesting and can be interpreted as $(-1)^{\Omega(n)+j}$ times the number of ordered factorisations of n into j non-trivial, square-free factors.

If $j > \Omega(n)$, then we have $c_j^{(-j)}(n) = 0$ as we are trying to factor n into more factors than it has.

We are now in a position to state our main result of this section which gives an explicit formula for the number of m-part sum systems in terms of the modified Möbius function and the Stirling numbers of the second kind, which count the number of ways to partition a set of n objects into k non-empty subsets ($n, k \in \mathbb{N}_0$).

Theorem 3.2.1. Let $m, N \in \mathbb{N}$. Then the number of m-part sum systems generating the target set $\langle N\rangle = \{0, \ldots, N-1\}$, with component set ordering important, is equal to

$$\mathcal{N}_m(N) = m! \sum_{L=m}^{\Omega(N)} S(L, m)\, (e-\mu)^{*L}(N) = m! \sum_{L=m}^{\Omega(N)} S(L, m)\, c_L^{(-L)}(N),$$

where $S(L, m)$ are the Stirling numbers of the second kind, and $c_L^{(-L)}(N)$ is the associated divisor function.

To aid us in the proof of this result we first require a lemma.

Lemma 3.2.2. Let $(a_j)_{j\in\mathbb{N}_0}$ and $(b_j)_{j\in\mathbb{N}_0}$ be number sequences. If

$$a_j = \sum_{i=0}^{j} \binom{j}{i} b_i,$$

then

$$b_j = \sum_{i=0}^{j} (-1)^{j-i} \binom{j}{i} a_i,$$

and vice versa.

Proof. For any $j \in \mathbb{N}_0$, we have

$$\begin{aligned}\sum_{i=0}^{j}(-1)^{j-i}\binom{j}{i}\sum_{\ell=0}^{i}\binom{i}{\ell}b_\ell &= \sum_{\ell=0}^{j}\left(\sum_{i=\ell}^{j}(-1)^{j-i}\binom{j}{i}\binom{i}{\ell}\right)b_\ell\\ &= \sum_{\ell=0}^{j}\left(\sum_{k=0}^{j-\ell}(-1)^{k}\binom{j}{j-k}\binom{j-k}{\ell}\right)b_\ell,\end{aligned}$$

after the change of variables $k = j - i$. The claimed formula now follows by observing that

$$\begin{aligned}\sum_{k=0}^{j-\ell}(-1)^{k}\binom{j}{j-k}\binom{j-k}{\ell} &= \sum_{k=0}^{j-\ell}(-1)^{k}\frac{j!\,(j-k)!}{k!\,(j-k)!\,\ell!\,(j-k-\ell)!}\\ &= \binom{j}{\ell}\sum_{k=0}^{j-\ell}(-1)^{k}\binom{j-\ell}{k} = \binom{j}{\ell}(1-1)^{j-\ell} = \delta_{j,\ell}.\end{aligned}$$

The converse follows by an almost identical calculation. □

Example 3.2.3. As a sample application, using the above lemma on Lemma 4 of [40], which, for $j \in \mathbb{N}$ and $r \in \mathbb{N}_0$, states that

$$c_j^{(r)} = \sum_{i=0}^{r} \binom{r}{i} c_{j+i},$$

we immediately obtain the following expression of the non-trivial divisor function in terms of associated divisor functions, such that for $j \in \mathbb{N}$ and $i \in \mathbb{N}_0$, we have

$$c_{j+i} = \sum_{r=0}^{i} (-1)^{i-r} \binom{i}{r} c_j^{(r)}.$$

Proof of Theorem 3.2.1. Bearing in mind the definition of Dirichlet convolution, summing over all possible m-tuples, and then applying Proposition 3.1.4, we have that

$$\begin{aligned}\mathcal{N}_m(N) = \sum_{\substack{n\in\mathbb{N}_2^m \\ n_1\ldots n_m=N}} N_m(n) &= \sum_{\substack{n\in\mathbb{N}_2^m \\ n_1\ldots n_m=N}} \sum_{\ell\ \in\mathbb{N}^m} \binom{|\ell|}{\ell} \prod_{j=1}^{m} (e-\mu)^{*\ell_j}(n_j) \\ &= \sum_{\ell\in\mathbb{N}^m} \binom{|\ell|}{\ell} \sum_{\substack{n\in\mathbb{N}_2^m \\ n_1\ldots n_m=N}} \prod_{j=1}^{m} (e-\mu)^{*\ell_j}(n_j) \\ &= \sum_{\ell\in\mathbb{N}^m} \binom{|\ell|}{\ell} \left(\mathop{*}_{j=1}^{m} (e-\mu)^{*\ell_j} \right)(N) \\ &= \sum_{\ell\in\mathbb{N}^m} \binom{|\ell|}{\ell} (e-\mu)^{*|\ell|}(N) \\ &= \sum_{\ell\in\mathbb{N}^m} \binom{|\ell|}{\ell} c_{|\ell|}^{-|\ell|}(N),\end{aligned}$$

where we use Eq. (3.7) in the final line. For the fixed integer N, we consider the sequence $(\mathcal{N}_m(N))_{m\in\mathbb{N}}$. Also define

$$\tilde{\mathcal{N}}_m(N) = \sum_{\ell\in\mathbb{N}_0^m} \binom{|\ell|}{\ell} c_{|\ell|}^{-|\ell|}(N) = \sum_{L=0}^{\Omega(N)} \left(c_L^{-L}(N) \sum_{\substack{\ell\in\mathbb{N}_0^m \\ |\ell|=L}} \binom{L}{\ell} 1^{\ell_1} \ldots 1^{\ell_m} \right) = \sum_{L=0}^{\Omega(N)} m^L c_L^{-L}(N),$$

where we use Eq. (3.3) in the last equality. Also consider the sequence $(\tilde{\mathcal{N}}_m(N))_{m\in\mathbb{N}}$, where we note that

$$
\begin{aligned}
\tilde{\mathcal{N}}_m(N) &= \binom{m}{m}\sum_{\ell\in\mathbb{N}^m}\binom{|\ell|}{\ell}c_{|\ell|}^{-|\ell|}(N) + \binom{m}{m-1}\sum_{\ell\in\mathbb{N}^{m-1}}\binom{|\ell|}{\ell}c_{|\ell|}^{-|\ell|}(N) \\
&\qquad + \binom{m}{m-2}\sum_{\ell\ \in\mathbb{N}^{m-2}}\binom{|\ell|}{\ell}c_{|\ell|}^{-|\ell|}(N) + \cdots + \binom{m}{0}\sum_{\ell\in\mathbb{N}^0}\binom{|\ell|}{\ell}c_{|\ell|}^{-|\ell|}(N) \\
&= \sum_{k=0}^{m}\binom{m}{k}\mathcal{N}_k(N).
\end{aligned}
$$

We apply Lemma 3.2.2 and shift the the indices to start at $k=1$, since $\tilde{\mathcal{N}}_0(N)=0$ for all $N\in\mathbb{N}$, to obtain

$$
\mathcal{N}_m(N) = \sum_{k=1}^{m}(-1)^{m-k}\binom{m}{k}\tilde{\mathcal{N}}_k(N) = \sum_{L=0}^{\Omega(N)}\left(\sum_{k=1}^{m}(-1)^{m-k}k^L\binom{m}{k}\right)c_L^{-L}(N).
$$

Using the the identity

$$
S(L,m) = \sum_{k=1}^{m}(-1)^{m-k}k^{L-1}\frac{1}{(k-1)!(m-k)!},
$$

and Eq. (3.7), we can write

$$
\begin{aligned}
\mathcal{N}_m(N) &= \sum_{L=0}^{\Omega(N)}\left(\sum_{k=1}^{m}(-1)^{m-k}k^L\binom{m}{k}\right)c_L^{-L}(N) \\
&= \sum_{L=0}^{\Omega(N)}\left(\sum_{k=1}^{m}(-1)^{m-k}k^L\frac{m!}{k!(m-k)!}\right)c_L^{-L}(N) \\
&= m!\sum_{L=0}^{\Omega(N)}\left(\sum_{k=1}^{m}(-1)^{m-k}k^{L-1}\frac{1}{(k-1)!(m-k)!}\right)c_L^{-L}(N) \\
&= m!\sum_{L=0}^{\Omega(N)}S(L,m)c_L^{-L}(N),
\end{aligned}
$$

as required. □

Example 3.2.4. The first values of $\mathcal{N}_m(N)$ for $N\in\{1,\dots,32\}$, with $1\le m\le 4$, are

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathcal{N}_1(N)$	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
$\mathcal{N}_2(N)$	0	0	0	2	0	4	0	6	2	4	0	14	0	4	4	14
$\mathcal{N}_3(N)$	0	0	0	0	0	0	0	6	0	0	0	18	0	0	0	36
$\mathcal{N}_4(N)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	24

N	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$\mathcal{N}_1(N)$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
$\mathcal{N}_2(N)$	0	14	0	14	4	4	0	38	2	4	6	14	0	24	0	30
$\mathcal{N}_3(N)$	0	18	0	18	0	0	0	126	0	0	6	18	0	36	0	150
$\mathcal{N}_4(N)$	0	0	0	0	0	0	0	96	0	0	0	0	0	0	0	240

We note that $\mathcal{N}_1(1) = 0$. This is because we do not consider $A_1 = \{0\}$ to be a sum system, since the corresponding joint ordered factorisation is $\big((1,1)\big)$ and we require all f-values to be ≥ 2. Hence there is no sum system.

When $N = p$, a prime number, there exists only one sum system of dimension 1 corresponding to the component set $\{0, 1, 2, 3, \ldots, p-1\}$, with joint ordered factorisation $\big((1,p)\big)$. When $N = p^2$, with $m = 2$, so $(n_1, n_2) = (p, p)$, we find that there exist two joint ordered factorisations $\big((1,p),(2,p)\big)$ and $\big((2,p),(1,p)\big)$ and no others.

However when N has a greater number of prime factors there are a greater number of possible ordered factorisations. For example, when $N = 6 = n_1 \times n_2$, for $m = 2$, we find that we have the four 2-part sum systems, with associated joint ordered factorisations and (n_1, n_2) tuples

A_1	A_2	Joint Ordered Factorisation	(n_1, n_2)
$\{0,1,2\}$	$\{0,3\}$	$\big((1,3),(2,2)\big)$	$(3,2)$
$\{0,2,4\}$	$\{0,1\}$	$\big((2,2),(1,3)\big)$	$(3,2)$
$\{0,1\}$	$\{0,2,4\}$	$\big((1,2),(2,3)\big)$	$(2,3)$
$\{0,3\}$	$\{0,1,2\}$	$\big((2,3),(1,2)\big)$	$(2,3)$

Although the sum systems $A_1 = \{0,2,4\}, A_2 = \{0,1\}$ and $\tilde{A}_1 = \{0,1\}, \tilde{A}_2 = \{0,2,4\}$ appear to be the same, we count them as two distinct systems for the purpose of this enumeration.

For $N = 12 = n_1 \times n_2$, so again $m = 2$, we find that we have the fourteen 2-part sum systems corresponding to the 7 joint ordered factorisations and (n_1, n_2) tuples

Joint Ordered Factorisation	(n_1, n_2)
$\big((1,2),(2,6)\big)$	$(2,6)$
$\big((1,6),(2,2)\big)$	$(6,2)$
$\big((1,3),(2,4)\big)$	$(3,4)$
$\big((1,4),(2,3)\big)$	$(4,3)$
$\big((1,2),(2,3),(1,2)\big)$	$(4,3)$
$\big((1,3),(2,2),(1,2)\big)$	$(6,2)$
$\big((1,2),(2,2),(1,3)\big)$	$(6,2)$

where the remaining 7 possibilities are obtained by swapping the j-values of each pair in the above joint ordered factorisations.

In [51] the number of two-dimensional joint ordered factorisation $M_{(n,n)}$, corresponding to the tuple (n, n), where in our notation $N = n^2$, was calculated to be

$$\frac{1}{2}\mathcal{N}_2(N) = M_{(n,n)} = \sum_{j=1}^{\infty} \big(c_j(n)c_j(n) + c_j(n)c_{j+1}(n)\big) = \sum_{j=1}^{\Omega(n)} c_j^{(1)}(n)c_j^{(0)}(n). \tag{3.8}$$

Unlike the case $m = 1$, when $N = n^2$ and $m = 2$ there always exists at least one joint ordered factorisation, ignoring permutations of axes.

In the next section we derive sums over divisor relations for our counting function $\mathcal{N}_2(N)$.

3.3 Sums over divisors relations

In [53] the complementing set system

$$C = A + B = \{x : x = a + b,\ a \in A,\ b \in B\}$$

was considered for all complementing subsets of $\langle N\rangle = \{0, 1, 2 \ldots, N-1\}$. In Theorem 2 they state that the number $C(N)$ of complementing subsets of $\langle N\rangle$, is given by

$$C(N) = \frac{1}{2}\sum_{\substack{d|N \\ d<N}} C(d). \tag{3.9}$$

The paper [53] would have benefited from some examples to demonstrate how this sum over divisors relates to the above tables given in Example 3.2.4. Using our counting function, such that $\mathcal{N}_2(N) = C(N)$, it stands to reason this relation should generalise to m dimensions. However, it has been remarked that Long's enumeration contained an error [47], which we correct. To help clarify this matter we now develop the sum over divisors relation for our counting function $\mathcal{N}_m(N)$, as stated below.

Theorem 3.3.1. Let $m \in \mathbb{N}$ and $N \in \mathbb{N}_2$. Then our counting function $\mathcal{N}_m(N)$ obeys the sum over divisors relations

$$\begin{aligned}\mathcal{N}_m(N) &= \sum_{\substack{d|N \\ d<N}} \Big((m-1)\mathcal{N}_m(d) + m\mathcal{N}_{m-1}(d)\Big) \\ &= -m \sum_{\substack{d|N \\ d<N}} \mu\left(\frac{N}{d}\right)\Big(\mathcal{N}_m(d) + \mathcal{N}_{m-1}(d)\Big).\end{aligned}$$

Proof. We begin by summing $\mathcal{N}_m(N)$ given in Theorem 3.2.1 over divisors of N, to give

$$\begin{aligned}\sum_{d|N} \mathcal{N}_m(d) &= \sum_{L=0}^{\Omega(N)} m!\, S(L,m) \sum_{d|N} c_L^{(-L)}(d) \\ &= \sum_{L=0}^{\Omega(N)} m!\, S(L,m)\, c_L^{(-L+1)}(N),\end{aligned}$$

using the sum over divisor relation identity from [40]

$$c_j^{(r)}(N) = \sum_{d|N} c_j^{(r-1)}(d).$$

Theorem 1(a) of [51] gives a three term recurrence relation for the associated divisor function, stated here as

$$c_{j+1}^{(r)} = c_j^{(r+1)} - c_j^{(r)}.$$

Setting $r = -L+1$ and $j = L-1$, we obtain as operators

$$c_{L-1}^{(-L+1)} = c_{L-1}^{(-L+2)} - c_{L-1}^{(-L+1)} = \sum_{d|N} c_{L-1}^{(-(L-1))} - c_{L-1}^{(-(L-1))}.$$

Combining these results gives us

$$\sum_{d|N} \mathcal{N}_m(d) = \sum_{L=0}^{\Omega(N)} m!\, S(L,m) \left(\sum_{d|N} c_{L-1}^{(-(L-1))}(d) - c_{L-1}^{(-(L-1))}(N)\right).$$

We now substitute for the well known three-term recurrence relation for the Stirling numbers of the second kind

$$S(L,m) = m\,S(L-1,m) + S(L-1,m-1),$$

along with the fact that $S(0,m) = 0$ for $m \geq 1$ to obtain

$$\begin{aligned}\sum_{d|N} \mathcal{N}_m(d) &= \sum_{L=1}^{\Omega(N)} m! \Big(m\,S(L-1,m) + S(L-1,m-1)\Big) \left(\sum_{d|N} c_{L-1}^{(-(L-1))}(d) - c_{L-1}^{(-(L-1))}(N)\right) \\ &= \sum_{L=0}^{\Omega(N)} m! \Big(m\,S(L,m) + S(L,m-1)\Big) \left(\sum_{d|N} c_{L}^{(-L)}(d) - c_{L}^{(-L)}(N)\right).\end{aligned}$$

Expanding out the right hand side, we have

$$\begin{aligned}\sum_{d|N} \mathcal{N}_m(d) = &-m \sum_{L=0}^{\Omega(N)} m!\,S(L,m) c_L^{(-L)}(N) - m \sum_{L=0}^{\Omega(N)} (m-1)!\,S(L,m-1) c_L^{(-L)}(N) \\ &+ \sum_{d|N} \sum_{L=0}^{\Omega(N)} m! \Big(m\,S(L,m) c_L^{(-L)}(d) + S(L,m-1) c_L^{(-L)}(d)\Big) \\ = &-m\mathcal{N}_m(N) - m\mathcal{N}_{m-1}(N) + \sum_{d|N} \Big(m\mathcal{N}_m(d) + m\mathcal{N}_{m-1}(d)\Big).\end{aligned}$$

Collecting $d = N$ terms, we have

$$\sum_{d|N} \mathcal{N}_m(d) = m \sum_{\substack{d|N \\ d<N}} \Big(\mathcal{N}_m(d) + \mathcal{N}_{m-1}(d)\Big).$$

By writing the left hand side as $\mathcal{N}_m(N)$ and a sum over divisors for $d < N$, we can rearrange to

$$\begin{aligned}\mathcal{N}_m(N) &= m \sum_{\substack{d|N \\ d<N}} \Big(\mathcal{N}_m(d) + \mathcal{N}_{m-1}(d)\Big) - \sum_{\substack{d|N \\ d<N}} \mathcal{N}_m(d) \\ &= \sum_{\substack{d|N \\ d<N}} \Big((m-1)\mathcal{N}_m(d) + m\mathcal{N}_{m-1}(d)\Big),\end{aligned}$$

as required. □

Corollary 3.3.2. Let $m \in \mathbb{N}$ and $N \in \mathbb{N}_2$ with $\mathcal{N}_m(N)$ our counting function introduced in Theorem 3.2.1 for the number of m-part sum systems with target set $\langle N \rangle$. When $m = 2$, the formula for $\mathcal{N}_2(N)$ simplifies to

$$\mathcal{N}_2(N) = \sum_{\substack{d|N \\ d<N}} \Big(\mathcal{N}_2(d) + 2\mathcal{N}_1(d)\Big),$$

and using $\mathcal{N}_1(d) = 1$ for $d > 1$, we have

$$\mathcal{N}_2(N) = 2d_2(N) - 4 + \sum_{\substack{d|N \\ d<N}} \mathcal{N}_2(d),$$

with $d_2(N)$ the number-of-divisor function, counting the number of divisors of N.

Example 3.3.3. When $N = 12$, we find that $\mathcal{N}_2(12) = 14$, whereas $2d_2(12) - 4 = 8$, and

$$\sum_{\substack{d|12 \\ d<12}} \mathcal{N}_2(12) = 0 + 0 + 0 + 2 + 4 = 6,$$

so that as predicted by the formula $14 = 8 + 6$.

For $N = p$ a prime number, we have that $2d_2(p) - 4 = 4 - 4 = 0 = \mathcal{N}_2(p) = \mathcal{N}_2(1)$, and both sides equate to zero.

Remark 3.3.4. We note that the formula given in Corollary 3.3.2 has the additional term of $2d_2(N) - 4$ compared with Eq. (3.9) as stated in [53]. It is understood that the enumeration by Long contained an error, which our counting function $\mathcal{N}_2(N)$ corrects.

Chapter 4

Prime Powers and an Invariance Property

We established the underpinning arithmetic structures for sum-and-distance system components in Chapter 2. With this expression, along with Eq. (2.3), we deduced various summation properties, including the two invariant properties conveyed by Eq. (2.14) and Eq. (2.18). Chapter 3 introduced the first major enumeration of this work in the form of the counting function $\mathcal{N}_m(N)$ and its three-term recurrence relations. In this chapter we shall investigate an enumeration that pertains to an additional invariance property for sum-and-distance systems. Where Eq. (2.18) concerned the weighted sum of squares over component sets, this enumeration based observation uses the sum of elements of a given sum-and-distance system component found by Eq. (2.16) in Theorem 2.4.8.

4.1 Powers of 2 systems

This new invariant property is most clearly seen when we set the cardinality of the sum-and-distance system components to be powers of 2. Although each component may have different powers, to introduce this observation let us consider the two-dimensional case with equal component cardinalities. That is, let $m = 2$, $n = (2^t, 2^t) \in \mathbb{N}_2^m$, for $t \in \mathbb{N}$, and let $\mathcal{J} = \big((j_1, f_1), \dots, (j_L, f_L)\big)$ be a joint ordered factorisation of n, with sum-and-distance system B_1 and B_2.

As $n_j = 2^t$, we are considering only the even case across the various properties beholden to the parity conditions, which simplifies many of our previous results.

Recall from Definition 1.0.2 the position set

$$\mathcal{L}_j := \big\{\ell : j_\ell = j \text{ in } \mathcal{J}\big\},$$

that tracks the position of which pairs in $\mathcal{J}$ correspond to the j-th component set.

Recall from Definition 2.2.2 the term $\ell_{e_j} := \max\big\{\ell \in \mathcal{L}_j : f_\ell \text{ even}\big\}$ which is the position of the last pair in $\mathcal{J}$ (reading left to right) corresponding to the j-th component set which has an even f-value. We further defined the restricted position set

$$\mathcal{L}'_j := \big\{\ell : j_\ell = j,\ \ell > \ell_{e_j}\big\},$$

that detailed the position of all pairs corresponding to the j-th component set after this last even parity pair.

Returning to our context, by restricting the component sets to powers of 2 we will have $\mathcal{L}'_j = \emptyset$, the empty set, since every pair in $\mathcal{J}$ will have an even f-value (some power of 2). This simplifies any expression that this set appears in.

Of particular interest is Eq. (2.16). Since $\mathcal{L}'_1 = \mathcal{L}'_2 = \emptyset$ we can ignore the summation altogether. Then, for $j \in \{1, 2\}$, we have

$$\Sigma B_j = \sum_{b \in B_j} b = \frac{1}{8} F(\ell_{e_j} + 1) P_j(\ell_{e_j} + 1) = \begin{cases} \frac{(2^{t-1})^3}{f_L}, & j \neq j_L \\ (2^{t-1})^3, & j = j_L. \end{cases} \tag{4.1}$$

This illustrates that, for all joint ordered factorisations $\mathcal{J}$ of $n = (2^t, 2^t)$, there is an invariance on ΣB_j which depends only on the last f-value in $\mathcal{J}$. In the cases that f_L remains the same across different joint ordered factorisations, then these systems share an invariance in both sums.

To demonstrate this, the tables below detail half of all joint ordered factorisations of $n = (2^t, 2^t)$ for $t = 2$ and $t = 3$, the corresponding sum-and-distance components B_j, and ΣB_j, for $j = 1, 2$. The other half is found by swapping the j-values in each pair between 1 and 2, which would swap the sum-and-distance component sets and their sums.

$\mathcal{J}$	B_1	B_2	ΣB_1	ΣB_2
$\big((1,2),(2,2),(1,2),(2,2)\big)$	$\{\frac{3}{2},\frac{5}{2}\}$	$\{3,5\}$	4	8
$\big((2,2),(1,4),(2,2)\big)$	$\{1,3\}$	$\{\frac{7}{2},\frac{9}{2}\}$	4	8
$\big((1,4),(2,4)\big)$	$\{\frac{1}{2},\frac{3}{2}\}$	$\{2,6\}$	2	8

$\mathcal{J}$	B_1	B_2	ΣB_1	ΣB_2
$\big((1,2),(2,2),(1,2),(2,2),(1,2),(2,2)\big)$	$\{\frac{11}{2},\frac{13}{2},\frac{19}{2},\frac{21}{2}\}$	$\{11,13,19,21\}$	32	64
$\big((2,2),(1,2),(2,2),(1,4),(2,2)\big)$	$\{3,5,11,13\}$	$\{\frac{27}{2},\frac{29}{2},\frac{35}{2},\frac{37}{2}\}$	32	64
$\big((2,2),(1,4),(2,2),(1,2),(2,2)\big)$	$\{5,7,9,11\}$	$\{\frac{23}{2},\frac{25}{2},\frac{39}{2},\frac{41}{2}\}$	32	64
$\big((1,2),(2,2),(1,4),(2,4)\big)$	$\{\frac{3}{2},\frac{5}{2},\frac{11}{2},\frac{13}{2}\}$	$\{7,9,23,25\}$	16	64
$\big((1,4),(2,2),(1,2),(2,4)\big)$	$\{\frac{5}{2},\frac{7}{2},\frac{9}{2},\frac{11}{2}\}$	$\{6,10,22,26\}$	16	64
$\big((1,2),(2,4),(1,4),(2,2)\big)$	$\{\frac{7}{2},\frac{9}{2},\frac{23}{2},\frac{25}{2}\}$	$\{13,15,17,19\}$	32	64
$\big((1,4),(2,4),(1,2),(2,2)\big)$	$\{\frac{13}{2},\frac{15}{2},\frac{17}{2},\frac{19}{2}\}$	$\{10,14,18,22\}$	32	64
$\big((2,2),(1,8),(2,4)\big)$	$\{1,3,5,7\}$	$\{\frac{15}{2},\frac{17}{2},\frac{47}{2},\frac{49}{2}\}$	16	64
$\big((2,4),(1,8),(2,2)\big)$	$\{2,6,10,14\}$	$\{\frac{29}{2},\frac{31}{2},\frac{33}{2},\frac{35}{2}\}$	32	64
$\big((1,8),(2,8)\big)$	$\{\frac{1}{2},\frac{3}{2},\frac{5}{2},\frac{7}{2}\}$	$\{4,12,20,28\}$	8	64

For $t \in \{2,3\}$, by tallying the occurrence of each ΣB_j we find that each value appears as a sequence of simplicial numbers. For $t = 2$ this sequence is the natural numbers, and for $t = 3$ it is the triangular numbers. Because ΣB_j depends only on the last pair of the corresponding $\mathcal{J}$, the occurrence rate of each value is then the number of joint ordered factorisations that have $(2, 2^{\xi})$ as the last pair, for some $\xi \in \{0, \ldots, t\}$. Technically the case when $\xi = 0$ leads to the joint ordered factorisation containing the final pair $(2,1)$ which we normally would not allow. However, it is convenient to allow this setting for the parameter, as by ignoring the resultant pair we obtain the second half of the joint ordered factorisations for $(2^t, 2^t)$, all of which end with a pair with j-value 1. Note that we would actually find twice these numbers since these tables only list half the number of possible joint ordered factorisations, with the other half yielding the same sums but for the other coordinate axis.

To enumerate how many sum-and-distance system components are invariant under this sum of elements, we will fix the value of this sum and then work out how many joint ordered factorisations will provide this answer.

Let $m \in \mathbb{N}$, $n = (2^{t_1}, \ldots, 2^{t_m}) \in \mathbb{N}$ for $t_j \in \mathbb{N}$, and $\mathcal{J}$ be a joint ordered factorisation of n with $B_1, \ldots, B_m$ a corresponding sum-and-distance system. For $j \in \{1, \ldots, m\}$, we have that $\ell_{e_j} = \max \mathcal{L}_j$, i.e. ℓ_{e_j} is the position of the last pair in $\mathcal{J}$ that corresponds to the j-th component set. Let us label this pair (j, g) (where $g = f_{\ell_{e_j}}$).

Each f-value in $\mathcal{J}$ will be some power of 2. Let $\xi \in \mathbb{N}_0$ be the exponent in the product

$$\prod_{s=1}^{L-\ell_{e_j}} f_{\ell_{e_j}+s} = 2^{\xi}.$$

This product is over the f-values of each pair after (j, g). The sum of elements of B_j is thus given by

$$\Sigma B_j = \sum_{b \in B_j} b = \frac{1}{8} F(\ell_{e_j} + 1) P_j(\ell_{e_j} + 1) = \frac{1}{8} \frac{2^{\sum_{s=1}^{m} t_s}}{f_{\ell_{e_j}+1} \cdots f_L} 2^{t_j} = 2^{\sum_{s=1}^{m} t_s + t_j - 3 - \xi},$$

This implies that ΣB_j depends only on ξ, and not on how the pairs that are used to define ξ are laid out in $\mathcal{J}$.

For example, ΣB_1 for the joint ordered factorisations

$$\big((2,2),(1,2),(3,2),(2,2^2),(3,2),(2,2)\big) \quad \text{and} \quad \big((2,2),(1,2),(3,2^2),(2,2^3)\big)$$

will be the same since $\xi = 5$ in both tuples. We can use this to define the set

$$D(n, j, \xi) = \Big\{ \big(d_1, \ldots, d_{j-1}, 0, d_{j+1}, \ldots, d_m\big) : 0 \le d_i \le t_i,\ \sum_{i=1}^{m} d_i = \xi \Big\}. \tag{4.2}$$

Then $D(n, j, \xi)$ is the set of all m-tuples which has an entry of 0 in the j-th position, and, for $i \in \{1, \ldots, m\}$ and $i \neq j$, the i-th entry is the exponent in the product over f-values that come after (j, g) and have the j-value i, i.e.

$$\prod_{\substack{\ell \in \mathcal{L}_i \\ \ell > \ell_{e_j}}} f_\ell = d_i.$$

The i-th component set, for $i \in \{1, \ldots, m\}$ and $i \neq j$, will hence commit d_i factors of 2^{t_i} to appear after (j, g). This leaves $t_i - d_i$ factors to come before (j, g). Therefore, for $d \in D(n, j, \xi)$ we define the $(m-1)$-tuple

$$\Delta(n, d, j) := \Big(t_1 - d_1, \ldots, t_{j-1} - d_{j-1},\ t_{j+1} - d_{j+1}, \ldots, t_m - d_m\Big), \tag{4.3}$$

to be the pair-wise difference between t_i and d_i excluding the j-th term.

Example 4.1.1. Let $m = 4$, $n = (2^3, 2^2, 2^1, 2^2)$ and $\chi = 4$. Then

$$\begin{aligned}
D(n,1,4) &= \Big\{ (0,2,1,1),(0,2,0,2),(0,1,1,2)\Big\},\\
D(n,2,4) &= \Big\{ (3,0,1,0),(3,0,0,1),(2,0,1,1),(2,0,0,2),(1,0,1,2)\Big\},\\
D(n,3,4) &= \Big\{ (3,1,0,0),(3,0,0,1),(2,2,0,0),(2,1,0,1),\\
&\qquad (2,0,0,2),(1,2,0,1),(1,1,0,2),(0,2,0,2)\Big\},\\
D(n,3,4) &= \Big\{ (3,1,0,0),(3,0,1,0),(2,2,0,0),(2,1,1,0),(1,2,1,0)\Big\}.
\end{aligned}$$

For $d \in D(n,1,4)$ we have

$$\begin{aligned}
\Delta\big(n,(0,2,1,1),1\big) &= \big(2-2,1-1,2-1\big) = (0,0,1),\\
\Delta\big(n,(0,2,0,2),1\big) &= \big(2-2,1-0,2-2\big) = (0,1,0),\\
\Delta\big(n,(0,1,1,2),1\big) &= \big(2-1,1-1,2-2\big) = (1,0,0).
\end{aligned}$$

Remark 4.1.2. Traditionally, for $m \in \mathbb{N}$, we require that $n = (n_1, \ldots, n_m) \in \mathbb{N}_2^m$. However, if $n_j = 1$, for some $j \in \{1, \ldots, m\}$, then by Eq. (3.2), for $\ell \in \mathbb{N}$, we have that

$$c_\ell^{(r)}(1) = \sum_{k=0}^{\ell} (-1)^k \binom{\ell}{k} \prod_{l=1}^{0} \binom{0+\ell+r-k-1}{0} = \sum_{k=0}^{\ell}(-1)^k\binom{\ell}{k} = 0,$$

using identity (1.5) of [33]. Then by using Eq. (3.4) we conclude that

$$N_m(n) = \sum_{\ell\in\mathbb{N}^m} \binom{|\ell|}{\ell} \prod_{s=1}^{m} c_{\ell_s}^{(-\ell_s)}(n_s) = 0.$$

However, the closed form for the enumeration of sum-and-distance system components with invariant ΣB_j will contain the term $N_m\big((2^{t_1-d_1}, \ldots, 2^{t_m-d_m})\big)$. When $t_i = d_i$ (implying the i-th element of $\Delta(n,d,j)$ will be 0) then this argument will contain the term $2^{t_i-d_i} = 2^0 = 1$, which makes $N_m\big((2^{t_1-d_1}, \ldots, 2^{t_m-d_m})\big) = 0$. Although technically correct, this rigid expression does not allow for cases where we might wish to ignore a coordinate axis, by setting $n_j = 1$ for example. To account for this, let $\tilde{n}$ equal n with any entries of 1 omitted, and define the enumeration function

$$N_m^r(n) := N_m(\tilde{n}).$$

This function is used only as a mathematical counting trick to account for instances where $n_j = 1$ in the following theorem's proof. It should not be interpreted in the same way that $N_m(n)$ is.

Theorem 4.1.3. Let $m \in \mathbb{N}$, $n = (2^{t_1}, \dots, 2^{t_m}) \in \mathbb{N}_2^m$, for $t_1, \dots, t_m \in \mathbb{N}$, and consider all joint ordered factorisations of n. Let $N = \prod_{j=1}^m n_j$, such that $\Omega(N) = \sum_{j=1}^m t_j$. For some fixed $\xi \in \{0, \dots, \Omega(N) - 1\}$ and some $j \in \{1, \dots, m\}$, let $D(n, j, \xi)$ be defined by expression (4.2), and let $\Delta(n, d, j)$ be defined by expression (4.3) (for $d \in D(n, j, \xi)$). Then, across all joint ordered factorisations of n, the number of sum-and-distance system components that are invariant under the summation property $\Sigma B_j = 2^{\Omega(N)+t_j-3-\xi}$ is given by

$$\Sigma_2(m, n, \xi) = \sum_{j=1}^{m} \left(\binom{\Omega(N) - \xi - 1}{t_j - 1} \sum_{d \in D(n,j,\xi)} \binom{\xi}{d} \binom{\Omega(N) - t_j - \xi}{\Delta(n, d, j)} \right)$$

where $\binom{\xi}{d}$ and $\binom{\Omega(N)-t_j-\xi}{\Delta(n,d,j)}$ are multinomial coefficients.

Proof. We will construct and enumerate a generalised form that a joint ordered factorisation of n must take to satisfy the summation condition $\Sigma B_j = 2^{\Omega(N)+t_j-3-\xi}$.

Let $j \in \{1, \dots, m\}$. Recall $\mathcal{L}_j = \{\ell_1, \dots, \ell_{e_j}\}$ to be the positions of the pairs with j-value $j_\ell = j$ in the joint ordered factorisation to be constructed. Denote the last pair corresponding to the j-th coordinate axis by (j, g), for $g \mid n_j$ to be determined later. This pair is in position $\ell_{e_j} = \max \mathcal{L}_j$. We are interested in the pairs after (j, g), which will correspond to each axis aside from the j-th, and the pairs before (j, g), which will contain pairs from every axes.

So that the summation condition is satisfied, Eq. (2.16) requires

$$\Sigma B_j = \sum_{b \in B_1} b = \frac{1}{8} F(\ell_{e_j} + 1) P_1(\ell_{e_j} + 1) = \frac{1}{2^3} \times \frac{2^{\Omega(N)}}{2^\xi} \times 2^{t_j}.$$

This implies that the product over the f-values of the pairs after (j, g) must satisfy

$$\prod_{\ell > \ell_{e_j}} f_\ell = 2^\xi.$$

For $i = \{1, \dots, m\}$ with $i \neq j$, let the product over the f-values of pairs with j-value $j_\ell = i$ after (j, g) be given by

$$\prod_{\substack{\ell > \ell_{e_j} \\ j_\ell = i}} f_\ell = 2^{d_i}.$$

Collecting these values, letting $d_j = 0$, we have the tuple $d = (d_1, \dots, d_{j-1}, 0, d_{j+1}, \dots, d_m)$ with $\sum_{i=1}^m d_i = \xi$. Let $D(n, j, \xi)$ be the set of all possible tuples d, which align with the definition given in expression (4.2). The pairs that come after (j, g) can be written in any order, implying every distinct arrangement of these pairs (adhering to the conditions of consecutive pairs in a joint ordered factorisation) will correspond to a different joint ordered factorisation to be counted. For $d \in D(n, j, \xi)$, these end pairs will form a joint ordered factorisations of $2^d := (2^{d_1}, \dots, 2^{d_m})$. Using Remark 4.1.2 and Eq. (3.6), the number of configurations these end pairs can take is the multinomial coefficient

$$N^r_m\big((2^{d_1}, \dots, 2^{d_m})\big) = \begin{pmatrix} \sum\limits_{i=1}^{m} d_i \\ d \end{pmatrix} = \binom{\xi}{d}.$$

The number of ways the pairs before (j, g) can be written also depends on which pairs came after it. Excluding the j-th coordinate axis, the pairs that will occur before (j, g) will form a joint ordered factorisation of the tuple

$$\delta = (2^{t_1 - d_1}, \dots, 2^{t_{j-1} - d_{j-1}}, 2^{t_{j+1} - d_{j+1}}, \dots, 2^{t_m - d_m}).$$

The $(m-1)$-tuple $\Delta(n, d, j)$ is the exponents in δ. Then using Remark 4.1.2 and Eq. (3.6) again gives us the multinomial expression

$$N^r_m(\delta) = \begin{pmatrix} \sum\limits_{\substack{i=1 \\ i \neq j}}^{m} (t_i - d_i) \\ \Delta(n, d, j) \end{pmatrix} = \binom{\Omega(N) - t_j - \xi}{\Delta(n, d, j)}.$$

We must now add the j-th coordinate axis into the pairs before (j, g).

For $i \in \{1, \dots, m\}$ and $i \neq j$, the f-values of the pairs corresponding to the i-th component set that occur before (j, g) will be factors of $2^{t_i - d_i}$. Write these pairs as a maximal chain of prime factors, i.e. $(i, 2), \dots, (i, 2)$, where there would be $t_i - d_i$ pairs. Repeating this for each i, we obtain $\sum_{i=1}^{m} (t_i - d_i) - t_j$ pairs. To add the j-th coordinate axis, we must insert new pairs between the pairs present in the maximal chain. Say we add s pairs, for $s \in \{0, \dots, t_j - 1\}$. We must add these new pairs either before the first pair, or between any two consecutive pairs, but not after the final pair (as then we would have consecutive pairs for the j-th axis). Then there are $\sum_{i=1}^{m} (t_i - d_i) - t_j$ choose s ways to place these pairs.

Once we have added these pairs, we must assign their f-values. This is how many ways can we write 2^{t_j} as $s + 1$ non-trivial factors, for which we have $c_{s+1}(2^{t_j}) = \binom{t_j - 1}{s}$, by Eq. (3.5) (note that we have $s + 1$ to account for the pair (j, g) already present). Summing over

s from 0 to $t_j - 1$ we get

$$\sum_{s=0}^{t_j-1} c_{s+1}(2^{t_j}) \binom{\sum_{i=1}^{m}(t_i - d_i) - t_j}{s} = \sum_{s=0}^{t_j-1} \binom{t_j - 1}{s} \binom{\Omega(N) - \xi - t_j}{s} = \binom{\Omega(N) - \xi - 1}{t_j - 1},$$

using identity (3.20) in [33]. Altogether, we sum from $j = 1$ to m, over all $d \in D(n, j, \xi)$, to get

$$\begin{aligned}\Sigma_2(m, n, \xi) &= \sum_{j=1}^{m} \sum_{d \in D(n,j,\xi)} N_m^r(2^d) N_m^r(\delta) \binom{\Omega(N) - \xi - 1}{t_j - 1} \\ &= \sum_{j=1}^{m} \sum_{d \in D(n,j,\xi)} \binom{\xi}{d} \binom{\Omega(N) - t_j - \xi}{\Delta(n, d, j)} \binom{\Omega(N) - \xi - 1}{t_j - 1},\end{aligned}$$

as required. □

Remark 4.1.4. In the special case $n = (2^t, \ldots, 2^t) \in \mathbb{N}_2^m$, for $t \in \mathbb{N}$, then $\Sigma_2(m, n, \xi)$ simplifies. For $j = 1$ and some $d = (0, d_2, d_3, \ldots, d_m) \in D(n, 1, \xi)$, we can write the tuple

$$\Delta(n, d, 1) = (t - d_2, t - d_3, \ldots, t - d_m).$$

Now, for $j = 2$ we take $d' = (d_2, 0, d_3, \ldots, d_m) \in D(n, 1, \xi)$ such that

$$\Delta(n, d', 2) = (t - d_2, t - d_3, \ldots, t - d_m) = \Delta(n, d, 1).$$

Indeed, we find that $\Delta(n, d^{(1)}, 1) = \cdots = \Delta(n, d^{(m)}, m)$, for some $d^{(i)} \in D(n, i, \chi)$. Then we can remove the sum over j from 1 to m and only sum over $d \in D(n, 1, \xi)$ by accounting for the fact we get m repeat of each element of $D(n, j, \xi)$. Removing the outer sum, changing the variables in the inner sum, and multiplying through by m, we obtain the reduced expression

$$\Sigma_2(m, n, \xi) = m\binom{mt - \xi - 1}{t - 1} \sum_{d \in D(n,1,\xi)} \binom{\xi}{d} \binom{(m-1)t - \xi}{\Delta(n, d, 1)}.$$

Additionally, if we set $m = 2$, then we find that $D(2, 1, \xi) = \{(0, \xi)\}$ and $D(2, 2, \xi) = \{(\xi, 0)\}$. Thus the summation over $D(m, 1, \xi)$ in $\Sigma_2(2, n, \xi)$ contains only one term, simplifying $\Sigma_2(2, n, \xi)$ to

$$\begin{aligned}\Sigma_2(2, n, \xi) &= 2\binom{2t - \xi - 1}{t - 1} \binom{\xi}{(0, \xi)} \binom{t - \xi}{\Delta(n, (0, \xi), 1)} \\ &= 2\binom{2t - \xi - 1}{t - 1} \binom{\xi}{\xi} \binom{t - \xi}{t - \xi} = 2\binom{2t - \xi - 1}{t - 1}.\end{aligned}$$

Example 4.1.5. Let $n = (2^3, 2^3)$, and fix $\xi \in \{0, 1, 2, 3\}$. Using Remark 4.1.4, for $m = 2$, the number of sum-and-distance system components that are invariant under the summation property $\Sigma B_j = 2^{6-\xi}$ is given by

$$\frac{1}{2}\Sigma_2(2, n, \xi) = \binom{5-\xi}{2} = \frac{(5-\xi)!}{2 \times (3-\xi)!} = \frac{(4-\xi)(5-\xi)}{2} = T_{4-\xi},$$

where T_i is the i-th triangular number, which confirms the observation made earlier. For any $t \in \mathbb{N}$ this binomial coefficient represents the $(t-1)$-simplex numbers, retrieving the simplicial number generalisation observed earlier.

4.2 Odd prime powers

If $n = (p^t, p^t)$ with p an odd prime then we would not observe this invariance for ΣB_j. One reason why is that Eq. (2.16) will have a summation over the set $\mathcal{L}'_j$, which is $\mathcal{L}'_j = \mathcal{L}_j$ when n_j is odd. The invariant property for $p = 2$ occurred due to the fact this set was the empty set, removing the summation. In fact, this leads to the following conjecture that states the opposite of the powers of 2 invariant property.

Conjecture 4.2.1. Let $t \in \mathbb{N}$ and p be an odd prime. Let $\mathcal{J}_1, \mathcal{J}_2$ be distinct joint ordered factorisations of (p^t, p^t), with the sum-and-distance systems $B_{(1,1)}$, $B_{(1,2)}$ and $B_{(2,1)}$, $B_{(2,2)}$ respectively. Then

$$\Sigma B_{(1,1)} \neq \Sigma B_{(2,1)} \quad \text{and} \quad \Sigma B_{(1,2)} \neq \Sigma B_{(2,2)}.$$

Example 4.2.2. Let $n = (3^3, 3^3)$. Below is a table detailing all possible joint ordered factorisations for n and the sum over their sum-and-distance system components.

$\mathcal{J}$	ΣB_1	ΣB_2
$\big((1,3),(2,3),(1,3),(2,3),(1,3),(2,3)\big)$	757	2271
$\big((2,3),(1,3),(2,3),(1,3),(2,3),(1,3)\big)$	2271	757
$\big((2,3),(1,3),(2,3),(1,9),(2,3)\big)$	813	2215
$\big((2,3),(1,9),(2,3),(1,3),(2,3)\big)$	759	2269
$\big((1,3),(2,3),(1,3),(2,9),(1,3)\big)$	2215	813
$\big((1,3),(2,9),(1,3),(2,3),(1,3)\big)$	2269	759
$\big((1,3),(2,3),(1,9),(2,9)\big)$	271	2433
$\big((1,9),(2,3),(1,3),(2,9)\big)$	253	2439
$\big((1,3),(2,9),(1,9),(2,3)\big)$	811	2217
$\big((1,9),(2,9),(1,3),(2,3)\big)$	739	2277
$\big((2,3),(1,3),(2,9),(1,9)\big)$	2433	271
$\big((2,9),(1,3),(2,3),(1,9)\big)$	2439	253
$\big((2,3),(1,9),(2,9),(1,3)\big)$	2217	811
$\big((2,9),(1,9),(2,3),(1,3)\big)$	2277	739
$\big((2,3),(1,27),(2,9)\big)$	273	2431
$\big((2,9),(1,27),(2,3)\big)$	819	2197
$\big((1,3),(2,27),(1,9)\big)$	2431	273
$\big((1,9),(2,27),(1,3)\big)$	2197	819
$\big((1,27),(2,27)\big)$	91	2457
$\big((2,27),(1,27)\big)$	2457	91

We can see that no two summations of sum-and-distance system components in the same column are the same. However, we note that there are equalities when considering sums between the two columns. This is due to the fact half the joint ordered factorisations can be retrieved by swapping their j-values between 1 and 2, which corresponds to swapping the sum-and-distance system components.

Letting $n = (p_1^t, \dots, p_m^t)$, with p an odd prime number, and considering ΣB_j, then the generalisation of $\Sigma_2(m,t,\xi)$ to $\Sigma_p(m,t,\xi)$ is not straight forward. To date, this enumeration is still outstanding. However, we can provide a counter example to a generalised Conjecture

4.2.1 that considers $m > 2$.

Example 4.2.3. For $n = (3^2, 3^2, 3^2)$, consider the sum-and-distance systems for the joint ordered factorisations $\mathcal{J}_1 = \big((3,3),(1,9),(2,9),(3,3)\big)$ and $\mathcal{J}_2 = \big((2,3),(1,9),(2,3),(3,9)\big)$, denoted $B_{1,j}$ and $B_{2,i}$ respectively. The first sum-and-distance system component of both factorisations have that $\Sigma B_{1,1} = 30$ and $\Sigma B_{2,1} = 30$ respectively. Therefore there is equality between these two sums, and a generalised version of Conjecture 4.2.1 is not present.

Additionally, this invariant property will be present for $n \in \mathbb{N}_2^m$ where n_j is even, for any $j \in \{1, \ldots, m\}$. Any joint ordered factorisation of n which has that $\ell_{e_j} = \max \mathcal{L}_j$, i.e. the last pair corresponding to the j-th coordinate axis has an even f-value, will have that ΣB_j depends only on the pairs after (j, ℓ_{e_j}), i.e. $\frac{F(L+1)}{F(\ell_k)} = \frac{N}{F(\ell_{e_j})}$. Hence, any two joint ordered factorisations of n that has the parity of the last pair corresponding to the j-th coordinate axis is even, and which satisfies this product, will have the same ΣB_j and thus is invariant. An enumeration for how many sum-and-distance systems have this invariant property is possible, but is also an outstanding problem.

4.3 Conclusion

Sum-and-distance systems which have components of prime power cardinality contain an invariant property pertaining to the sum of their elements across various choices of joint ordered factorisations. In the case that the cardinalities are powers of 2 we have obtained an enumeration for how many component sets have this equality between systems.

The odd prime power case in two-dimensions does not hold this invariance property, but is given as a conjecture. Along side a generalisation of this enumeration for m-dimensions, as well as mixed parity cardinalities, there is still a plethora of enumerations to be obtained.

Chapter 5

Sum System Modulo $N + z$

5.1 Transforms of sum systems and cryptography

As discussed in Chapter 2, the sumset operation is generally defined for two subsets A and B of an abelian group G. So far, we have considered the system $A_1, \ldots, A_m \subset \mathbb{N}_0$ without requiring any additional structure beyond that of the ring of integers. The arithmetic progression $\langle N \rangle = \{0, \ldots, N-1\}$ can be viewed as considering the sumset of the sum system modulo N, just without any sum actually surpassing $N - 1$, i.e.

$$\sum_{j=1}^{m} A_j \equiv \langle N \rangle \pmod{N}.$$

With this relaxation on how we compute the sumset operation, now considering modular arithmetic, it stands to reason to ask whether there are any other sets that satisfy this equation. This question is the focus of this chapter, and to study these sets we require the following definition, which generalise our notions of sum systems into the context of modular arithmetic.

Definition 5.1.1. Let $m \in \mathbb{N}$, $z \in \mathbb{N}_0$, $n = (n_1, \ldots, n_m) \in \mathbb{N}_2^m$ and $N = \prod_{j=1}^{m} n_j$. The collection of m sets $A_1, \ldots, A_m \subset \mathbb{N}_0$, with $|A_j| = n_j$, form an *m-part sum system modulo* $N + z$ if

$$\sum_{j=1}^{m} A_j \equiv \langle N \rangle \pmod{N + z}.$$

Naturally, any traditional sum system is a sum system modulo $N+z$ since for $a^{(j)} \in A_j$, for $j \in \{1, \ldots, m\}$, we have that

$$\sum_{j=1}^{m} a^{(j)} < N,$$

and thus are never reduced modulo $N+z$.

De Bruijn initiated the studies of additive systems, proposing multiple types of problems based on which target set was the goal. Generally, modern literature is concerned with the target set $T = \mathbb{Z}$, and we have previously discussed the few who continued research into the target set $T = \langle N \rangle$ (through complementing sets). However, only Webb [86] seems to have considered a variant of this problem using modular arithmetic and taking transforms of sum systems. Though appearing to be a natural consideration given that the sumset operation is defined for subsets of an abelian group, this overlooked framework proves to be a powerful generalisation.

In 1992, Webb had implemented this idea in his construction for a cryptographic key, that used complementing sets (an earlier name for sum systems) to encode and decode messages [86]. He used the additive system to generate an asymmetric cryptosystem which uses a public and private key, also known as a *public key cryptosystem*.

Public key cryptosystems were first published by Diffie and Hellman [22] in 1976, with the RSA cryptosystem published a year later using this method. Merkle and Hellman published their *Merkle–Hellman knapsack cryptosystem* a year later.

There are various types of knapsack problems, but a knapsack cryptosystem considers specifically the *subset sum problem*, which generally asks; given a multiset of integers S and some target value t, can you find a subset $S' \subset S$ such that $\sum\limits_{s \in S'} s = t$?

The Merkle–Hellman system took a sequence $W = (w_1, \ldots, w_n)$, such that $w_i > \sum_{j=1}^{i-1} w_j$ (this property is known as *superincreasing*), and use it to encode a message. In 1982, two algorithms (known as *attacks*) were developed that rendered the Merkle–Hellman cryptosystem broken, and considered insecure [76, 1], both requiring only the public key to decipher. The superincreasing sequence proves to be the Achilles' heel of the system, being easily exploited. Furthermore, Lagarias and Odlyzko [48] constructed a lattice out of the elements of the knapsack problem and defines a special vector corresponding to the target value. For systems with a low *density*, a metric on the complexity of the underlying knapsack problem, Lagarias and Odlyzko pointed out that that this special vector often has the shortest length out of vectors in the system, and is therefore easy to attack.

There has been a long list of knapsack cryptosystems which have all fallen to either the low density method above, or specialised attacks on their construction and parameters.

However, when the system is not based on a superincreasing sequence, or has high density, these cryptosystems are harder to break. Usually only being solvable by a brute-force checking method, many variants of these systems are NP-complete. The trade-off appears to be in the size of the key, or the heavy computation required to construct the systems. But despite this, the more complicated knapsack cryptosystems are thought to be strong candidates for post quantum cryptography [21], in which possible quantum computers could break the RSA cryptosystem in seconds but would still have to brute force knapsack cryptosystems.

One such system was developed by Chor and Rivest [13] in 1988, which considers the knapsack problem over finite fields. They computed logarithms of translations of roots to minimal polynomials over the field, randomised their order and added in noise to the data. Multiple attacks are known that break these systems, including a broadly reaching algorithm by Vaudenay [85] that recognised that any private key also corresponds to numerous other equivalent keys. However, all these attacks only broke Chor and Rivest's system under their original parameters, more than 30 years ago. Since then, safe parameters that are resilient against these attacks have been established, but the size of the public key is often in the kilobytes, or even megabytes.

The system Webb developed is similar in design to that of Chor and Rivest. He generated an m-part sum system with target set $\langle N \rangle$, which he then linearly transformed under modular arithmetic twice to make new additive systems. These sets formed the public key, with the information on these transforms acting as the private key.

Webb used a rudimentary construction process to generate his m-part sum system which, like Munagi afterwards [65, 64], lacked the powerfully concise notation for the joint ordered factorisation that was established in [42]. Nevertheless, his transforms are a novel idea that seems unexplored in literature. To illustrate Webb's idea, we will use the example he provided in [86] alongside explaining the algorithm used. It has been found that his framework and example contains some labeling errors which makes his calculations unclear, which we clarify below.

Example 5.1.2. For $m \in \mathbb{N}$, $n \in \mathbb{N}_2^m$, $N = \prod_{j=1}^m n_j$, and consider a m-part sum system $A_1, \dots, A_m$, recalling that $|A_j| = n_j$ and index $A_j = \{a_0^{(j)}, \dots, a_{n_j-1}^{(j)}\}$. Choose some value $s_1 > N$, and pick parameters $u_1, t_1, \dots, t_m \in \mathbb{N}_0$ such that $\gcd(s_1, u_1) = 1$ (with no restraint on t_j). Then choose $s_2 > ms_1$ with $u_2 \in \mathbb{N}$ such that $\gcd(s_2, u_2) = 1$. Then we can perform two transformations on $A_1, \dots, A_m$ under modular arithmetic to arrive at a seemingly random set of integers, with which we can encode a number.

For our working example, let $m = 2$, $n = (4, 3)$, $N = 12$ and consider $A_1 = \{0, 1, 6, 7\}$ and $A_2 = \{0, 2, 4\}$. Set the parameters $s_1 = 13$, $s_2 = 29$, $u_1 = 3$, $u_2 = 5$, $t_1 = 4$ and $t_2 = 6$ to be used for our calculations.

First, calculate the sets $D_j \equiv u_1\big(A_j + t_j\big) \pmod{s_1}$. In our example we have

$$D_1 \equiv 3\big(A_1 + 4\big) \equiv \{12, 2, 4, 7\} \pmod{13},$$
$$D_2 \equiv 3\big(A_2 + 6\big) \equiv \{5, 11, 4\} \pmod{13}.$$

Note that we do not reorder the set, preserving the placement found in A_j.

Secondly, calculate the sets $E_j \equiv u_2 D_j \pmod{s_2}$. In our example we have

$$E_1 \equiv 5D_1 \equiv \{2, 10, 20, 6\} \pmod{29},$$
$$E_2 \equiv 5D_2 \equiv \{25, 26, 20\} \pmod{29},$$

again preserving the original order of elements. In general we let $E_j = \{e_0^{(j)}, \dots, e_{n_j-1}^{(j)}\}$. These sets form the *public key.*

From here we can encode any integer in $\langle N \rangle = \{0, \dots, N-1\}$. To encode $c \in \langle N \rangle$ we need to satisfy the equation

$$c = x_0 + n_1 x_1 + n_1 n_2 x_2 + \cdots + x_{m-1} \prod_{j=1}^{m-1} n_j,$$

solving for $0 \leq x_j < n_{j+1}$. Once we find the unique values that satisfies this expression, we compute $c_1 = \sum_{j=1}^m e_{x_{j-1}}^{(j)}$ for $e_{x_{j-1}}^{(j)} \in E_j$. In our example we have

$$2 = x_0 + n_1 x_1 = x_0 + 4x_1 \implies x_0 = 2, x_1 = 0.$$

Then our encoded message is $e^{(1)}_{x_0} + e^{(2)}_{x_1} = 20 + 25 = 45$. We note that Webb's labeling convention causes him issue in the case that $x_j = 0$ since he indexed his sets to start at 1. In his example he encodes the integer 7 by finding $7 = 3 + 4(1)$ with $x_0 = 3$ and $x_1 = 1$, which with his index corresponds to 20 and 25. However, if we set $c = 2$ with his labelling, we would have $x_0 = 2$ and $x_1 = 0$, but his set E_2 has no 0th indexed element. Thus we have chosen to use $c = 2$ to align with the numbers he used.

For anyone to decode this message using the public key alone, they would need to find which values across E_1 to E_m summed to make c_1. In our example it is trivial to spot that the two such values, but with say 100 sets each with 100 elements this problem becomes far more exhaustive.

The *private key* consists of $A_1, \dots, A_m$ and $s_1, s_2, u_1, u_2, t_1, t_2$. To decode the message c_1, we find $u_1^{-1} \pmod{s_1}$ and $u_2^{-1} \pmod{s_2}$, which we use to solve $c_2 \equiv u_2^{-1} c_1 \pmod{s_2}$, and then $c_3 \equiv u_1^{-1} c_2 - \sum_{j=1}^{m} t_j \pmod{s_1}$. Then we find which values satisfy $c_3 = \sum_{j1}^{m} a^{(j)}_{x_{j-1}}$ for $a^{(j)}_{x_{j-1}} \in A_j$.

In our example, we have $u_1^{-1} \equiv 9 \pmod{13}$ and $u_2^{-1} \equiv 6 \pmod{29}$. Then we have

$$c_2 \equiv 6 \times 45 \equiv 9 \pmod{29},$$

and

$$c_3 \equiv 9 \times 9 - t_1 - t_2 \equiv 71 \equiv 6 \pmod{13}.$$

Since $6 = 6 + 0 = a^{(1)}_2 + a^{(2)}_0$, we retrieve that $x_0 = 2$ and $x_1 = 0$, and thus $x_0 + x_1 n_1 = 2$, which was our original message.

Webb's example is inconsistent with which u_j^{-1} is used where, with even his generalised algorithm swapping them within the same sentence. This example corrects his errors in the set index, as well as provides the correct equations to be used.

5.2 Modular systems

We will use the additive systems Webb had constructed for his cryptosystems, though with the cryptography context removed [86, p.179]. These sets are transforms of a sum system under modular arithmetic which appears to be a new idea in the literature of additive systems. We give a revised version of this system below.

Definition 5.2.1. Let $m \in \mathbb{N}_2$, $n = (n_1, \ldots, n_m) \in \mathbb{N}_2^m$, $N = \prod_{j=1}^{m} n_j$, and let $\mathcal{J}$ be a joint ordered factorisation of n, with the sum system $A_1, \ldots, A_m \subset \mathbb{N}_0$. Let $z \in \mathbb{N}_0$, and choose $u \in \langle N+z \rangle$ with $\gcd(N+z, u) = 1$. For each $j \in \{1, \ldots, m\}$, let $t_j \in \langle N+z \rangle$ and define the set

$$D_j \equiv u\big(A_j + t_j\big) \pmod{N+z},$$

which we call a *modular system component (set)*. We call the collection of sets $D_1, \ldots, D_m$ a *modular system*, and refer to $u, t_1, \ldots, t_m$ as the *parameters*.

Remark 5.2.2. It is convention that elements in A_j are written in increasing order. The elements in $u(A_j + t_j) \pmod{N+z}$ will often not be in increasing order. As such, we will permute them so that the elements in D_j are also in increasing order.

As the multiplier parameter $u \in \langle N+z \rangle$ is coprime to $N+z$, it will be a unit of the group $\Big(\mathbb{Z}_{N+z}, \times \pmod{N+z}\Big)$. For any two $j, i \in \{1, \ldots, m\}$, the terms t_j and t_i may be different or the same, but u will remain the same. Either way, we do not require t_j and $N+z$ to be coprime.

In a more geometric frame of reference, we can consider t_j to be a translation on the sum system component set A_j, which itself is the coordinate axis of an integer lattice. Then u dilates the component set, which we then reduce modulo $N+z$.

Example 5.2.3. Let $m = 3$, $n = (6, 3, 4)$, with $N = 72$, and consider the joint ordered factorisation $\mathcal{J} = \big((1,3), (3,2), (2,3), (1,2), (3,2)\big)$ with sum system $A_1 = \{0, 1, 2, 18, 19, 20\}$, $A_2 = \{0, 6, 12\}$ and $A_3 = \{0, 3, 36, 39\}$.

Let $z = 4$, meaning we are working modulo $N + z = 76$. Take $u = 5$ such that $\gcd(76, 5) = 1$, and $(t_1, t_2, t_3) = (15, 9, 20)$ with $\tilde{t} \equiv 15 + 9 + 20 \equiv 44 \pmod{76}$. Then the corresponding modular system is

$$D_1 \equiv 5\{15, 16, 17, 33, 34, 35\} \equiv \{75, 80, 85, 165, 170, 175\} \equiv \{4, 9, 13, 18, 23, 75\} \pmod{76},$$

$$D_2 \equiv 5\{9, 15, 21\} \equiv \{45, 75, 105\} \equiv \{29, 45, 75\} \pmod{76},$$

$$D_3 \equiv 5\{20, 23, 56, 59\} \equiv \{100, 115, 280, 295\} \equiv \{24, 39, 52, 67\} \pmod{76}.$$

By performing set addition under modulo 76 we retrieve the target set

$$\sum_{j=1}^{3} D_j \equiv \langle 76 \rangle \backslash \{48, 53, 58, 63\} \pmod{76},$$

which are the consecutive integers from 0 to 75, excluding 48, 53, 58 and 63.

Remark 5.2.4. In terms of distinct sums, a modular system will only ever generate N integers modulo $N+z$. This resulting target set will be a subset of $\langle N+z \rangle$, excluding z integers. This invokes the following questions. First, can we consider this modular system as a form of additive system under modular arithmetic? Second, is there a way to understand which z elements are omitted in the target set of the modular system? The answer to both of these is yes, motivating the following definition of a modular additive system and the ensuing theorem, detailing which z elements are omitted.

Definition 5.2.5. Let $m, q \in \mathbb{N}$, and consider some integer set $T \subset \mathbb{Z}$. We call the collection of m sets $A_1, \ldots, A_m \subset \mathbb{Z}$ an *m-dimensional additive system modulo q of T* if

$$T \equiv \sum_{j=1}^{m} A_j \pmod{q}.$$

Each $t \in T$ appears once if and only if $|T| = |A_1| \ldots |A_m|$.

The map in Definition 5.2.1 transforms a traditional sum system into an additive system modulo $N+z$, which we prove in the following theorem and lemma when $z > 0$ and $z = 0$ respectively. For this reason, we will often refer to a modular system modulo $N+z$ as a *transform* of some sum system.

Theorem 5.2.6. Let $m \in \mathbb{N}_2$, $n = (n_1, \ldots, n_m) \in \mathbb{N}_2^m$, with $N = \prod_{j=1}^m n_j$, and $z \in \mathbb{N}$. Let $u, t_1, \ldots, t_m \in \langle N+z \rangle$ with $\gcd(N+z, u) = 1$, and set $\tilde{t} \equiv \sum_{j=1}^m t_j \pmod{N+z}$. For a sum system $A_1, \ldots, A_m$ with target set $\langle N \rangle$, let $D_1, \ldots, D_m$ be the modular system modulo $N+z$ such that $D_j \equiv u(A_j + t_j) \pmod{N+z}$, for $j \in \{1, \ldots, m\}$. Then $D_1, \ldots, D_m$ is an additive system modulo $N+z$ with target set

$$\sum_{j=1}^{m} D_j \equiv \langle N+z \rangle \Big\backslash u\big(\langle z \rangle + \tilde{t} - z\big) \pmod{N+z},$$

where the set difference $X \backslash Y$ is the set of all elements that belong to set X but not set Y.

Proof. The sumset of the modular system will generate the same number of terms as the sumset of the sum system, which will be N integers. Because we are working modulo $N+z$, the target set of the modular system must be a subset of $\langle N+z\rangle$. Hence the sumset of the modular system will be missing z integers from $\langle N+z\rangle$, and is given by

$$\sum_{j=1}^{m} D_j \equiv \sum_{j=1}^{m} u\big(A_j+t_j\big) \equiv u\left(\sum_{j=1}^{m} A_j + \sum_{j=1}^{m} t_j\right)$$
$$\equiv u\big(\langle N\rangle + \tilde{t}\big) \equiv u\big\{\tilde{t},\dots,\tilde{t}+N-1\big\} \pmod{N+z}.$$

The set $\langle N\rangle+\tilde{t}$ is a subset of $\langle N+z\rangle+\tilde{t}$, where the integers missing are

$$\big\{\tilde{t}+N,\tilde{t}+N+1,\dots,\tilde{t}+N+z-1\big\} \equiv \big\{\tilde{t}-z,\dots,\tilde{t}-1\big\} \equiv \tilde{t}-1-\langle z\rangle \pmod{N+z}.$$

By Identity 2.1, we can write $\langle z\rangle = z-1-\langle z\rangle$ such that

$$\tilde{t}-1-\langle z\rangle = \tilde{t}-1-z+1+\langle z\rangle = \langle z\rangle+\tilde{t}-z,$$

which we can use to write

$$\sum_{j=1}^{m} D_j \equiv u\big\{\tilde{t},\dots,\tilde{t}+N-1\big\} \equiv \big\langle N+z\big\rangle \Big\backslash u\big(\langle z\rangle+\tilde{t}-z\big) \pmod{N+z},$$

as required. □

Explicitly, this target set is

$$\big\langle N+z\big\rangle \Big\backslash u\big(\langle z\rangle+\tilde{t}-z\big) \equiv \big\{0,\dots,N+z-1\big\} \Big\backslash u\big\{\tilde{t}-z,\dots,\tilde{t}-1\big\} \pmod{N+z}.$$

Alternatively, we can write

$$u\big(\langle z\rangle+\tilde{t}-z\big) \equiv u\big(\langle z\rangle+\tilde{t}+N\big) \equiv u\big\{N+\tilde{t},N+\tilde{t}+1,\dots,N+z+\tilde{t}-1\big\}.$$

Lemma 5.2.7. Let $m \in \mathbb{N}_2$, $n=(n_1,\dots,n_m)\in\mathbb{N}_2^m$, with $N=\prod\limits_{j=1}^{m} n_j$. Let $z=0$ and $D_1,\dots,D_m$ be a modular system modular N. Then this modular system forms a sum system modulo N.

Proof. A collection of sets forms a sum system modulo $N+z$ if their sumset is the target set $\langle N\rangle$. We observe that $\langle N\rangle+\tilde{t}\equiv\langle N\rangle \pmod N$ and $u\langle N\rangle\equiv\langle N\rangle \pmod N$ since $\gcd(N,u)=1$. Then $\sum\limits_{j=1}^{m} D_j \equiv u\big(\langle N\rangle+\tilde{t}\big)\equiv\langle N\rangle \pmod N$. □

When $z > 0$, a sum system may be transformed into a particular modular system via two different set of values for the parameters considered.

Example 5.2.8. Continuing from Example 5.2.3, we had used the parameters $u = 5$ and $(t_1, t_2, t_3) = (15, 9, 20)$. If we consider the parameters $\hat{u} = 71$ and $(\hat{t}_1, \hat{t}_2, \hat{t}_3) = (41, 55, 17)$, the corresponding modular system, $\hat{D}_1, \hat{D}_2, \hat{D}_3$, is in fact $\hat{D}_j = D_j$ for $j \in \{1, 2, 3\}$, implying two different transforms of this sum system results in the same modular system. It turns out that for any choice of parameters we take, we can find another set of parameters which will correspond to the same modular system, which we state in the following lemma.

Lemma 5.2.9. Let $m \in \mathbb{N}_2$, $n = (n_1, \ldots, n_m) \in \mathbb{N}_2^m$, with $N = \prod_{j=1}^{m} n_j$, and $z \in \mathbb{N}_0$. Let $u, t_1, \ldots, t_m \in \langle N + z \rangle$ such that $\gcd(N + z, u) = 1$. Let $A_1, \ldots, A_m$ be a sum system with target set $\langle N \rangle$. Then the parameters u and t_j, for $j \in \{1, \ldots, m\}$, and the parameters $N + z - u$ and $-\max A_j - t_j$ result in the same modular system, i.e.

$$u(A_j + t_j) \equiv (N + z - u)(A_j - \max A_j - t_j) \pmod{N + z}.$$

Proof. Because $N + z - u \equiv -u \pmod{N + z}$, the result follows directly from

$$(N + z - u)(A_j - \max A_j - t_j) \equiv -u(-A_j - t_j) \equiv u(A_j + t_j) \pmod{N + z},$$

as required. □

Note that if $z = 0$, then Lemma 5.2.9 still holds true, except there will also be other parameters that can also correspond to the same modular system. These additional parameters are not as concise to state, and thus are excluded from this study.

5.3 Missing sum systems

With Definition 5.2.1 and Theorem 5.2.6 established, we can now ask the following question: let $m \in \mathbb{N}$, $n \in \mathbb{N}^m$, $N = \prod_{j=1}^{m} n_j$, $z \in \mathbb{N}_0$, and $u, \tilde{t} \in \langle N + z \rangle$ with $\gcd(N + z, u) = 1$. Do we retrieve all additive systems modulo $N + z$ with target set $\langle N + z \rangle \backslash u\big(\langle z \rangle + \tilde{t} - z\big)$ via transforms of sum systems, i.e. modular systems? By extension this question asks whether there is a bijection between joint ordered factorisations and all such additive systems modulo $N+z$.

The answer to this question falls into two cases. Firstly, when $z=0$ the answer is no, there exists additive systems modulo N that are not modular systems, and hence not a transform of a sum system. This is explored via the works of Szabó and Sands concerning factorising abelian groups into subsets [80].

When $z>0$, we conjecture that all such additive systems modulo $N+z$ are in fact modular systems.

Case 1: $z=0$

Let us illustrate this case with an example when $z=0$.

Example 5.3.1. Let $m=2$ and $n=(5,2)$ with $N=10$. We have the two traditional 2-part sum systems

$$A_1=\{0,1,2,3,4\}, \quad \text{and} \quad A_2=\{0,5\},$$
$$\tilde{A}_1=\{0,2,4,6,8\}, \quad \text{and} \quad \tilde{A}_2=\{0,1\}.$$

Let us select the pair $\tilde{A}_1$ and A_2 and consider their sumset modulo 10, given below in the table

	0	2	4	6	8
0	0	2	4	6	8
5	5	7	9	1	3

The consecutive integers from 0 to 9 occur once each within this table, and thus the collection of sets $\tilde{A}_1, A_2$ form a sum system modulo 10 (i.e. $\tilde{A}_1+A_2\equiv\langle 10\rangle \pmod{10}$).

However, there exists no $u, t_1, t_2 \in \langle 10\rangle$, with $\gcd(10,u)=1$, such that we can transform the sum systems A_1, A_2 or $\tilde{A}_1, \tilde{A}_2$ into the system $\tilde{A}_1, A_2$, i.e.

$$u(A_1+t_1)\not\equiv\tilde{A}_1 \pmod{10}, \quad \text{and} \quad u(A_2+t_2)\not\equiv A_2 \pmod{10},$$
$$\text{and} \quad u(\tilde{A}_1+t_1)\not\equiv\tilde{A}_1 \pmod{10}, \quad \text{and} \quad u(\tilde{A}_2+t_2)\not\equiv A_2 \pmod{10}.$$

In this case we can retrieve these sets by considering the expression

$$\langle 10\rangle \equiv \underbrace{2\langle 5\rangle}_{=\tilde{A}_1}+\underbrace{5\langle 2\rangle}_{=A_2} \pmod{10}.$$

Similarly, consider the sets

$$C_1 = \{0, 1, 2, 4, 8\}, \quad \text{and} \quad A_2 = \{0, 5\},$$

with their sumset modulo 10

	0	1	2	4	8
0	0	1	2	4	8
5	5	6	7	9	3

Again we find that $C_1 + A_2 \equiv \langle 10 \rangle \pmod{10}$, and this time there exists no parameters that map either A_1 or $\tilde{A}_1$ to C_1. Hence we have a sum system modulo 10 that we cannot retrieve via transforms of a sum system.

The essence of these additional sets can be understood through group theory. In their book Factoring Groups into Subsets [80], Szabó and Sands consider how to generate an abelian group G from subsets of that group. Although their theory works with a generalised G, we may restrict it to considering the abelian group of the integers modulo N, under modular arithmetic mod N, i.e. $\Big(\mathbb{Z}_N, + \pmod{N}\Big)$.

For $m \in \mathbb{N}_2$ and some non-empty subsets $A_1, \ldots, A_m$ of $\mathbb{Z}_N$, we say the sum $A_1 + \cdots + A_m$ is *direct* if, for $a_j, a'_j \in A_j$ for $j \in \{1, \ldots, m\}$, we have that

$$a_1 + \cdots + a_m = a'_1 + \cdots + a'_m$$

implies $a_j = a'_j$. If the direct sum $A_1 + A_2 + \cdots + A_m \equiv \mathbb{Z}_N \pmod{N}$, we call this a *factorisation* of $\mathbb{Z}_N$. If the identity element is in each A_j, in this case 0, we say A_j is *normalized*, and if $0 \in A_j$ for all j then we say the $A_1 + \cdots + A_m$ is a *normalized factorisation.*

It is known, from [16, Lemma 4], that for some subsets A, B of $\mathbb{Z}_N$ and $g \in \mathbb{Z}_N$, if $A + B$ is direct, then so is $(A + g) + B$. This can be generalised to say that for $g_i \in \mathbb{Z}_N$, if $\mathbb{Z}_N \equiv A_1 + A_2 + \cdots + A_m \pmod{N}$ is direct and a factorisation, then so is $\mathbb{Z}_N \equiv (A_1 + g_1) + (A_2 + g_2) + \cdots + (A_m + g_m) \pmod{N}$. Therefore we can always consider A_j to be normalized by applying this shift such that the resulting set contains 0.

A subset A of $\mathbb{Z}_N$ is λ-*simulated* if $|A| \geq 3$, and there exists a subgroup H of $\mathbb{Z}_N$ such that $|A| = |H|$ and we have the compliment $|A \backslash H| \leq \lambda$, i.e. A disagrees with H in at most λ elements. Usually we consider only when $\lambda = 1$ for which we say A is *simulated* by H.

If A isn't a subgroup but is simulated by one, say H, then there exists some $h \in H$, $g \in \mathbb{Z}_N \backslash \{0\}$ such that $A = \big(H \backslash \{h\}\big) \cup \{g + h\}$. We call g the *distorting element* of A.

From [16, Lemma 1], we have the following result. Let $C = \{0, a, a^2, \ldots, a^{r-1}\}$ be a cyclic subset of $\mathbb{Z}_N$, and $A = \{0, a, \ldots, a^{i-1}, a^i + g, a^{i+1}, \ldots, a^{r-1}\}$ simulated by C. If $r \geq 4$, then in the normalized factorisation $\mathbb{Z}_N \equiv A + B \pmod N$, we can replace A with C.

Lemma 6.9 in [80] says let $A_1, \ldots, A_m$ be subsets of, and factorise $\mathbb{Z}_N$. If each A_j are $(p_j - 1)$-simulated sets, with p_j the least prime factor of $|A_j|$, of a subgroup H_j, then any A_j can be replaced with H_j in the factorisation of $\mathbb{Z}_N$.

This theory of simulated subsets provides the answer to our missing sum systems. In Example 5.3.1 the sets $C_1 = \{0, 1, 2, 4, 8\}$ and $A_2 = \{0, 5\}$ formed a sum system modulo 10, but we could not generate C_1 from any known joint ordered factorisation. As we are working under the group $\mathbb{Z}_{10}$, if we consider the subgroup $H = \{0, 2, 4, 6, 8\}$, we see that $|C_1| = |H| = 5$ and $|C_1 \backslash H| = 1$, thus C_1 is simulated by H. In this case, the differing term is $1 \in A$ and $6 \in H$, with distorting element $g = 5$.

There are three results in [74] that are relevant to our study, which we now outline. Lemma 1 says; for A, B subsets of $\mathbb{Z}_N$, with A simulated with distorting element g, if $\mathbb{Z}_N \equiv A + B \pmod N$ is a factorisation, then $g + B \equiv B \pmod N$. Lemma 2 states; if $\mathbb{Z}_N$ is factorised by $A_1, \ldots, A_m$, and each A_j is either a simulated subset or a subset with prime cardinality, then one of these subsets is a subgroup of $\mathbb{Z}_N$.

Theorem 1 says let $A_1, \ldots, A_m$ be simulated subsets, but not subgroups, of $\mathbb{Z}_N$. If $A \equiv A_1 + \cdots + A_m \pmod N$ is direct and A has prime index of $\mathbb{Z}_N$ (i.e. $|\mathbb{Z}_N|/|A|$ is prime), then there exists at most one subset B of $\mathbb{Z}_N$ such that $\mathbb{Z}_N \equiv A + B \pmod N$ is a factorisation. Also, B is a subgroup of $\mathbb{Z}_N$ generated by the distorting element of one of these simulated subsets, i.e. $B = \{i * g : i \in \mathbb{N}_0\}$.

We now consider these results in the context of our example, with $C_1 = \{0, 1, 2, 4, 8\}$ and $A_2 = \{0, 5\}$. As $|C_1| = 5$ and $|A_2| = 2$ are both prime, along with the fact that C_1 is a simulated subset, by Lemma 2 one of these two sets is a subgroup of $\mathbb{Z}_{10}$. As C_1 is simulated, it follows that A_2 is a subgroup of $\mathbb{Z}_{10}$. By Lemma 1 we note that, with the distorting element $g = 5$, we have $A_2 + 5 \equiv A_2 \pmod{10}$. In fact, by Theorem 1 above we know that A_2 is generated by this distorting element.

We note that there is a similar result to Lemma 2 of [74], given by Theorem 1 of [15], which is as follows. Let $\mathbb{Z}_N \equiv A_1 + \cdots + A_m \pmod{N}$ be a factorisation, where for each j there is a subgroup H_j of $\mathbb{Z}_N$ such that $|A_j| = |H_j|$ and $|A_j \backslash H_j| \leq 1$. Then $A_j = H_j$ for some j, i.e. some of the factorising subsets are subgroups.

We conclude this literature review with a result from [12] which defines a factorisation $\mathbb{Z}_N \equiv A_1 + \cdots + A_m \pmod{N}$ to be *complete* if $A_i \cap A_j = \emptyset$ for all $i, j \in \{1, \ldots, m\}$ and $i \neq j$. Theorem 2.9 of [12] states; let $n_1, \ldots, n_m \in \mathbb{N}_2$ such that $N = \prod_{j=1}^{m} n_j$ and consider $\mathbb{Z}_N$. Then there exists a complete factorisation $A_1, \ldots, A_m$ of $\mathbb{Z}_N$ with $|A_j| = n_j \iff m \geq 3$.

In our example, we had that $C_1 \cap A_2 = \{0\} \neq \emptyset$, which agrees with the above theorem since here we had $m = 2$.

This additional theory goes some way in explaining these "missing" sum systems, though to address our transformations under modular arithmetic we require the following lemma.

Lemma 5.3.2. Let $N \in \mathbb{N}_2$, $\mathbb{Z}_N$ be the finite cyclic group of integers modulo N, with addition $\pmod{N}$, and H a subgroup of $\mathbb{Z}_N$. For $u \in \langle N \rangle$ with $\gcd(N, u) = 1$, then

$$u \times H \equiv H \pmod{N}$$

where we work $\pmod{N}$.

Proof. By the Fundamental Theorem of Cyclic Groups, any subgroup of $\mathbb{Z}_N$ is cyclic and has an order that divides N (additionally, there is at most one subgroup with this order). Let $d \mid N$ and assign H to be the subgroup of order d. As H is cyclic, it is generated by a single element, which is N/d. Hence we have

$$H = \{i \times \tfrac{N}{d} : i \in \langle d \rangle\} = \frac{N}{d} \langle d \rangle.$$

Now consider $a, b, c \in \langle d \rangle$. If $ua \equiv ub \equiv c \pmod{d}$, by dividing through by u (which is allowed since $\gcd(N, u) = \gcd(d, u) = 1$) we have $a \equiv b \pmod{d}$. If $c \equiv ua \pmod{d}$, then $a \equiv u^{-1}c \pmod{d}$. Let $u^{-1}c = xd + y$ for $x \in \mathbb{N}_0$ and $y \in \langle d \rangle$. Then we can write

$a \equiv u^{-1}c \equiv xd + y \equiv y \pmod{d}$. Hence we have shown that $u\langle d\rangle \pmod{d}$ is a bijective mapping to $\langle d\rangle$, and thus $u\langle d\rangle \equiv \langle d\rangle \pmod{d}$. Multiplying through by $\frac{N}{d}$ we get

$$u\frac{N}{d}\langle d\rangle \equiv \frac{N}{d}\langle d\rangle \pmod{N},$$

and therefore $uH \equiv H \pmod{N}$ as required. □

Given a simulated set that factorises $\mathbb{Z}_N$ of the given form $A = (H\backslash\{h\}) \cup \{g+h\}$, with g the distorting element, if we consider u times this set, we get

$$uA \equiv (uH\backslash\{uh\}) \cup \{u(g+h)\} \equiv (H\backslash\{uh\}) \cup \{ug+uh\} \pmod{N}.$$

This can be read as uA is simulated by the subgroup H, where we have replaced the term $uh \pmod{N}$ with $ug + uh \pmod{N}$, with ug being the distorting element.

As we know that $A + t$ factorises $\mathbb{Z}_N$, for some $t \in \mathbb{Z}_N$, together with the result above, it follows that $u(A + t)$ factorises $\mathbb{Z}_N$ and is a simulated set.

Hence, in Example 5.3.1 with the sum system $C_1 = \{0, 1, 2, 4, 8\}$ and $A_2 = \{0, 5\}$, the resulting system $u(C_1+t_1)$ and $u(A_2+t_2)$ under addition modulo 10 will also form a modular system.

The question regarding how many modular systems are accounted for under the transforms of these simulated sets is still open. Thus, to date, there exists no enumeration for the number of sum systems modulo N.

Case 2: $z > 0$

When $z > 0$, it seems likely that only modular systems, found via transforms of sum systems, have the sumset $\langle N + z\rangle\backslash u\big(\langle z\rangle + \tilde{t} - z\big)$, as stated in the following conjecture.

Conjecture 5.3.3. Let $m, N, z \in \mathbb{N}$, and consider a collection of sets $D_1, \ldots, D_m \subset \mathbb{N}_0$. If

$$\sum_{j=1}^{m} D_j \equiv \langle N + z\rangle\backslash u\big(\langle z\rangle + \tilde{t} - z\big) \pmod{N + z},$$

for some $u, \tilde{t} \in \langle N + z\rangle$ with $\gcd(N + z, u) = 1$, then $D_1, \ldots, D_m$ forms a modular system with

$$D_j \equiv u\big(A_j + t_j\big) \pmod{N + z},$$

for all $j \in \{1, \ldots, m\}$ and $\sum\limits_{j=1}^{m} t_j \equiv \tilde{t} \pmod{N+z}$, where A_j is a sum system component of a given sum system $A_1, \ldots, A_m$ with target set $\langle N \rangle$.

Remark 5.3.4. Although a conjecture, we can reduce this problem to the following. The sumset modulo $N + z$ of $D_1, \ldots, D_m$ generates the consecutive integers from 0 to $N + z - 1$ excluding z terms. We can write these "missing" integers as

$$u\big(\langle z \rangle + \tilde{t} - z\big) \equiv u\big(\langle z \rangle + N + \tilde{t}\big) \equiv u\big\{N + \tilde{t}, N + 1 + \tilde{t}, \ldots, N + z - 1 + \tilde{t}\big\} \pmod{N+z}.$$

We can rearrange the set $\langle N+z \rangle \backslash u\big(\langle z \rangle + \tilde{t} - z\big) \pmod{N+z}$ such that the difference between consecutive terms is u with final term $u(N + \tilde{t} - 1) \pmod{N+z}$. The first term in this rearrangement will be $u(N + \tilde{t} - 1) - u(N - 1) \equiv u\tilde{t} \pmod{N+z}$, which is the next integer u distance from the last term in the missing set. Thus we can write

$$\begin{aligned} \langle N + z \rangle \backslash u\big(\langle z \rangle + \tilde{t} - z\big) &\equiv \big\{u\tilde{t}, u\tilde{t} + u, u\tilde{t} + 2u, \ldots, u(\tilde{t} + N - 1)\big\} \\ &\equiv u\big\{\tilde{t}, \tilde{t} + 1, \tilde{t} + 2, \ldots, \tilde{t} + N - 1\big\} \pmod{N+z}. \end{aligned}$$

Dividing through by u and subtracting $\tilde{t}$ yields

$$\frac{1}{u}\Big(\langle N + z \rangle \backslash u\big(\langle z \rangle + \tilde{t} - z\big)\Big) - \tilde{t} \equiv \sum_{j=1}^{m} \left(\frac{1}{u} D_j - t_j\right) \equiv \langle N \rangle \pmod{N+z}.$$

This implies that the sumset of $\frac{1}{u} D_j - t_j$ modulo $N + z$, from $j = 1$ to m, generates the consecutive integers 0 to $N - 1$, i.e. $\langle N \rangle$. By Definition 5.1.1 these sets form an m-part sum system modulo $N + z$. We know that we can find a sum system $A_1, \ldots, A_m$, with $|A_j| = n_j$, with target set $\langle N \rangle$, i.e.

$$\sum_{j=1}^{m} A_j = \langle N \rangle.$$

Hence we can write

$$\sum_{j=1}^{m} \left(\frac{1}{u} D_j - t_j\right) \equiv \sum_{j=1}^{m} A_j \pmod{N+z}.$$

Since

$$\left|\frac{1}{u} D_j - t_j\right| = |A_j| = n_j,$$

it appears that we can pair sets according to their cardinalities, but it is no simple task to prove their equivalence. Example 5.3.5 illustrates how this process translates to an explicit case.

We can continue using the theory found in Section 3 of [42], in particular Lemma 3.2 and the proof of Theorem 3.3. For $j \in \{1, \dots, m\}$, let $\frac{1}{u}D_j - t_j := B_j = \{b_0^{(j)}, \dots, b_{n_j-1}^{(j)}\}$, and define the polynomial

$$p_{B_j}(x) := 1 + x^{b_1^{(j)}} + \cdots + x^{b_{n_j-1}^{(j)}}.$$

A polynomial p of degree d is *palindromic* if it is equal to its reciprocal polynomial, i.e. $p(x) = x^d p(\frac{1}{x})$. We can write

$$\begin{aligned} \prod_{j=1}^{m} p_{B_j}(x) &= \left(\sum_{k_1=0}^{n_1-1} x^{b_{k_1}^{(1)}}\right)\left(\sum_{k_2=0}^{n_2-1} x^{b_{k_2}^{(2)}}\right)\dots\left(\sum_{k_m=0}^{n_m-1} x^{b_{k_m}^{(m)}}\right) \\ &= \sum_{k_1=0}^{n_1-1}\sum_{k_2=0}^{n_2-1}\cdots\sum_{k_m=0}^{n_m-1} x^{b_{k_1}^{(1)}+b_{k_2}^{(2)}+\cdots+b_{k_m}^{(m)}}. \end{aligned}$$

As we are working modulo $N+z$ in the conjecture, let us consider this polynomial modulo $x^{N+z}-1$. Since we know $\sum_{j=1}^{m} B_j \equiv \langle N \rangle \pmod{N+z}$, we can write

$$\begin{aligned} \prod_{j=1}^{m} p_{B_j}(x) &= \sum_{k_1=0}^{n_1-1}\sum_{k_2=0}^{n_2-1}\cdots\sum_{k_m=0}^{n_m-1} x^{b_{k_1}^{(1)}+b_{k_2}^{(2)}+\cdots+b_{k_m}^{(m)}} \\ &\equiv \sum_{h=0}^{N-1} x^h = \frac{1-x^N}{1-x} \pmod{x^{N+z}-1}. \end{aligned}$$

Following the same arguments found in the proof of Theorem 3.3 of [42] we find that $p_{B_j}(x)$ is palindromic, and thus B_j satisfies the expression

$$B_j = \max B_j - B_j.$$

This property requires $\min B_j = 0$, since the only way to retrieve $\max B_j$ must be $\max B_j - 0$. Furthermore, Theorem 3.3 of [42] tells us that B_j satisfies $b_k^{(j)} + b_{n_j-1-k}^{(j)} = \max B_j$, and hence

$$\begin{aligned} \langle N \rangle \equiv \sum_{j=1}^{m} B_j = \sum_{j=1}^{m}\Big(\max B_j - B_j\Big) &= \sum_{j=1}^{m} \max B_j - \sum_{j=1}^{m} B_j \\ &\equiv \sum_{j=1}^{m} \max B_j - \langle N \rangle \\ &\equiv \sum_{j=1}^{m} \max B_j + \langle N \rangle - N + 1 \pmod{N+z}, \end{aligned}$$

which implies

$$\sum_{j=1}^{m} \max B_j \equiv N - 1 \pmod{N+z}.$$

Additionally, we know that $\max B_j < N-1$ since if we take all $B_i = 0$, for $i \in \{1,\dots,m\}$ with $i \neq j$, then $\sum_{h=1}^{m} B_h = B_j$ and if $B_j > N-2$ then we have a contradiction.

Hence we know that B_j has palindromic structure (i.e. $b_k^{(j)} + b_{n_j-1-k}^{(j)} = \max B_j$), $\min B_j = 0$, $\max B_j < N-1$ and $\sum_{j=1}^{m} \max B_j \equiv N-1 \pmod{N+z}$, with $|B_j| = n_j$. Both B_j and A_j share these properties, except that we have the stronger requirement that $\sum_{j=1}^{m} A_j = N-1$. It is here that additional theory is required to prove that $B_j \equiv A_j \pmod{N+z}$, or even to provide a counterexample.

Example 5.3.5. let us continue Example 5.2.3, with $m = 3$, $n = (6,3,4)$, $N = 72$ and $z = 4$. We had the modular system

$$\begin{aligned} D_1 &= \{4, 9, 13, 18, 23, 75\},\\ D_2 &= \{29, 45, 75\},\\ D_3 &= \{24, 39, 52, 67\}, \end{aligned}$$

which generated the set

$$\sum_{j=1}^{3} D_j \equiv \langle 76\rangle \backslash \{48, 53, 58, 63\} \pmod{76},$$

with the parameters $u = 5$, $(t_1, t_2, t_3) = (15, 9, 20)$ and $\tilde{t} \equiv 15 + 9 + 20 \equiv 44 \pmod{76}$.

We can rearrange the set $\langle 76\rangle \backslash \{48, 53, 58, 63\}$ such that consecutive terms have a difference of $u = 5$ modulo 76, i.e.

$$\langle 76\rangle \backslash \{48, 53, 58, 63\} = \{68, 73, 2, 7, 12, \dots, 62, 67, 72, 1, 6, 11, \dots, 33, 38, 43\},$$

with the next four terms in the sequence the "missing" terms $\{48, 53, 58, 63\}$.

Working modulo 76, we can start this rearranged set with $68 \equiv 220 \pmod{76}$, followed by $73 \equiv 225 \pmod{76}$, then $2 \equiv 230 \pmod{76}$ and so on, until the final term $43 \equiv u(N + \tilde{t} - 1) \equiv 5(72 + 44 - 1) \equiv 575 \pmod{76}$. Now this set takes the form

$$\begin{aligned} \langle 76\rangle \backslash \{48, 53, 58, 63\} &\equiv \{220, 225, 230, \dots, 565, 570, 575\}\\ &\equiv 5\{44, 45, 46, \dots, 113, 114, 115\}\\ &\equiv 5\big(\{0, 1, 2, \dots, 69, 70, 71\} + 44\big) \equiv 5\big(\langle 72\rangle + 44\big) \pmod{76}. \end{aligned}$$

Dividing by $u = 5$ and subtracting $\tilde{t} = 44$, the rearranged set can be written as

$$\frac{1}{5}\Big(\langle 76\rangle \backslash \{48, 53, 58, 63\}\Big) - 44 \equiv \{0, 1, \ldots, 71\} = \langle 72\rangle.$$

Therefore we can write

$$\begin{aligned}\langle 72\rangle \equiv \frac{1}{5}\Big(\langle 76\rangle \backslash \{48, 53, 58, 63\}\Big) - 44 &\equiv \frac{1}{5}\sum_{j=1}^{3} D_j - 44 \\ &\equiv \tfrac{1}{5}D_1 - 15 + \tfrac{1}{5}D_2 - 9 + \tfrac{1}{5}D_3 - 20 \\ &\equiv \sum_{j=1}^{3}\Big(\tfrac{1}{5}D_j - t_j\Big) \pmod{76}.\end{aligned}$$

We can find a sum system $A_1, \ldots, A_m$ with target set $\langle 72\rangle$ and $|A_j| = n_j$, such that

$$\sum_{j=1}^{3}\Big(\tfrac{1}{5}D_j - t_j\Big) \equiv \sum_{j=1}^{3} A_j \pmod{76}.$$

Indeed, we find that

$$\tfrac{1}{5}D_1 - 15 \equiv \{0, 1, 2, 18, 19\} \equiv A_1 \pmod{76},$$

and like wise for $j = 2$ and $j = 3$. Therefore D_1, D_2, D_3 is a modular system (which we had already previously shown).

The additional theory in Remark 5.3.4 concerning Theorem 3.3 of [42] is enough to prove the conjecture to be true when $m = 2$, as stated in the following theorem.

Theorem 5.3.6. Let $N, z \in \mathbb{N}$, and consider the collection of sets $D_1, D_2 \subset \mathbb{N}_0$. If

$$D_1 + D_2 \equiv \langle N + z\rangle \backslash u\big(\langle z\rangle + \tilde{t} - z\big) \pmod{N + z},$$

for some $u, \tilde{t} \in \langle N + z\rangle$ with $\gcd(N + z, u) = 1$, then D_1, D_2 forms a modular system with

$$D_j \equiv u\big(A_j + t_j\big) \pmod{N + z},$$

for all $j \in \{1, 2\}$ and $t_1 + t_2 \equiv \tilde{t} \pmod{N + z}$, where A_j is a sum system component of a given sum system A_1, A_2 with target set $\langle N\rangle$.

Proof. We use the arguments present in Remark 5.3.4, using $\frac{1}{u}D_j - t_j = B_j$ for $j \in \{1, 2\}$, to arrive at $\min B_j = 0$, $\max B_j < N - 1$ and $\max B_1 + \max B_2 \equiv N - 1 \pmod{N + z}$. We can hence write

$$\max B_1 + \max B_2 < 2N - 2 < 2N + z - 2 = N - 2 + (N + z) < N - 1 + (N + z),$$

which implies we must have $\max B_1 + \max B_2 = N - 1$. Since no sum $b_{k_1}^{(1)} + b_{k_2}^{(2)}$ can be more than the sum of $\max B_1 + \max B_2$, we must generate the set $\langle N\rangle$ without requiring any modular arithmetic. Therefore $B_1 + B_2 = \langle N\rangle$ and B_1, B_2 form a traditional sum system. □

For $m > 2$, if this conjecture turns out to be false then there will exist sum systems modulo $N + z$ that are not transforms of traditional sum systems, as with the case of $z = 0$. These sets will thus not be directly associated with joint ordered factorisations, and an enumeration of how many such sets exist would be of great interest.

If this conjecture is true (which is the belief of this work's author) then we have shown that the consecutive integers from 0 to $N + z$ with z missing terms forming an arithmetic progression has to be generated by a transform of a sum system. There will exist no other collection of sets that form this target set.

If the missing terms do not form an arithmetic progression, or if $\gcd(N + z, u) \neq 1$, there may exist a collection of sets with the given target set that are not transforms of sum systems.

Remark 5.3.7. When $z = 1$, the missing term $u(\tilde{t} - 1) \pmod{N + 1}$ always forms an arithmetic progression, even if $\gcd(N+1, u) \neq 1$. If we set $u = 1$, then the set $\langle N+1\rangle\backslash(\tilde{t}-1)$ can be generated by a transform of a sum system.

If $z = 2$, then the missing terms $\{u(t-1), u(t-2)\} \pmod{N+2}$ will always form an arithmetic progression, but we will require that $\gcd(N + 2, u) = 1$. For example, let $N = 14$ and consider $\langle 16\rangle\backslash\{0, 4\}$. Then $\{0, 4\} \equiv 4\langle 2\rangle \pmod{16}$ for $t \in \{0, 4, 8, 12\}$. Since $\gcd(16, 4) > 1$, there exists no modular system D_1, D_2 such that $D_1 + D_2 \equiv \langle 16\rangle\backslash\{0, 4\} \pmod{16}$. However, there will exist some collection of sets that have the target set $\langle 16\rangle\backslash\{0, 4\}$, such as $\tilde{D_1} = \{1, 2, 3, 8, 9, 10, 11\}$ and $\tilde{D_2} = \{0, 4\}$. These sets are not transforms of any sum system for the same parameter u.

Once again we apply the theory of factorising abelian groups to gain some insight into this problem.

For two A, B subsets of $\mathbb{Z}_N$, (A, B) form a *near-factorisations* of $\mathbb{Z}_N$ if $A + B \equiv \mathbb{Z}_N \backslash \{g\}$ (mod $N + 1$), for some $g \in \mathbb{Z}_N$. The element g is known as the *uncovered element.* If $0 \leq a + b \leq N$, for all $a \in A$ and $b \in B$, we call (A, B) a *Krasner near-factorisation.*

Near-factorisations are of particular interest to the field of graph theory due to the fact they can be used to generate Cayley graphs, and are connected to the Strong Perfect Graph Conjecture (which was stated in 1961 and proven in 2006). Cean et al [9] presented this connection in 1990 and formulated numerous results regarding near-factors.

Sakuma and Shinohara considered three transformations of near-factorisations (A, B) [71], which they state results in near-factorisations. They are as follows;

- *Shifting:* $(A + t_1, B + t_2)$ for $t_1, t_2 \in \mathbb{Z}_N$.
- *Scaling:* (uA, uB) for $u \in \langle N + 1\rangle$ with $\gcd(N + 1, u) = 1$.
- *Swapping:* taking $(-A, B)$.

Any near-factorisations constructed by the above methods is known as a degenerate British number systems (DBNS) near-factorisations (named by de Bruijn [8]).

In 1984 Grinstead conjectured that all near-factorisations of a finite cyclic group are DBNS near-factorisations [31]. Szabó and Sands proposed the problem to classify all Krasner near-factorisations [80]. Sakuma and Shinohara proved that all Krasner near-factors were DBNS near-factors in 2013 [71, Theorem 3.1], thus classifying these factors and proving a positive answer for the simplest case of Grinstead's conjecture.

In the context of this chapter, near-factorisations are 2-part modular systems modulo $N + 1$. In fact, Theorem 3.1 of [71] is a special case of Conjecture 5.3.3 and Theorem 5.3.6, where we set $z = 1$ and $m = 2$.

5.4 Conclusions

This chapter introduced the notion of generalising sum systems to consider sumset addition with modular arithmetic. Initially, Webb constructed a cryptographic key by transforming sum systems under addition and multiplication modulo some value [86]. These were used to form public keys and private keys to encode and decode messages respectively. However, it is the idea of transforming these sets, only once, that spurred the study of this chapter.

For $N \in \mathbb{N}$ and $z \in \mathbb{N}_0$, we transform a sum system with target set $\langle N \rangle$ by adding some integers to the component sets and multiplying the result by another parameter under modulo $N+z$. We labelled the collection of sets resulting from this process *modular systems*. By performing a sumset modulo $N+z$ on the modular system, we obtain the consecutive integers from 0 to $N+z-1$ excluding z terms, which form an arithmetic progression. We have a lot of control over which integers we wish to omit from the generated target set.

We stated an important conjecture concerning whether we account for all possible additive systems with a given target set modulo $N+z$ via modular systems, or if there exists some collections of sets that can not be transformed to via sum systems. We have proven this conjecture to be true when considering $m = 2$, i.e. two dimensional systems.

In the case that $z = 0$, we have shown that the conjecture does not hold. We gave a counterexample showing that there exist a collection of sets with the target set $\langle N \rangle$ under sumset modulo $N+z$ addition, but which are not modular systems.

If the conjecture is true for $z > 0$, we will be able to generate any set of consecutive integers with z missing terms via modular systems. This is a very general and strong result, which may have important uses in forming cryptography systems in the future.

Chapter 6

Orbits and Index Systems

For some target value $N \in \mathbb{N}$, as a sum system generates consecutive integers, without repeats, from 0 to $N-1$, which is to say $\langle N \rangle = \{0, \ldots, N-1\}$, an integer $M \in \langle N \rangle$ is uniquely represented by a sum incorporating one element from each sum system component. Each of these elements have a position within these ordered sets, for which we can assign a coordinate to. Collating these positions associates M with a unique identifier that details which elements of the sum system component sets sum to M. We call this the *address of M* (see Definition 6.2.1), which describes M as a multi-indexed element associated to the sum system.

As $\langle N \rangle$ is usually the target set to multiple sum system, an integer M will have different addresses for each of these systems. By comparing these differences, we can construct a mapping for describing the discrepancies between two given joint ordered factorisations. Said mapping will detail how M is represented with respect to both sum systems, and it is this notion we will focus on in this chapter and the next.

6.1 Principal reversible cuboids

Ollerenshaw and Brée published the book *Most-Perfect Pandiagonal Magic Squares* [68] which contained an enumeration of a class of $4k \times 4k$ matrices they called *principal reversible matrices*. Hill [39] employed a block representation technique for constructing these matrices and use them to enumerate the number of 2-part sum-and-distance systems.

These matrices have been the focal point of some recent papers [39, 37, 50, 38, 52] which have them as elements of a $\mathbb{Z}_2$ graded algebra known as a *superalgebra*, where the *super* prefix comes from how they form a framework for formulating models of supersymmetry in theoretical physics.

It was noticed in the 2010s by Huxley, Lettington and Schmidt [42], that these matrices contained 2-part sum systems as their first row and column. They generalised these matrices to order m tensors which they called *principal reversible cuboids*. In section 6 of [42], these tensors were constructed via an ordered chain of *building operators* that followed a joint ordered factorisations to detail said order. Theorem 4.5 of the same paper stated that the collection of coordinate axes of a principal reversible cuboid formed a sum system. The definition of these arrays are given below, after the following reminder and remark.

Recall the partial ordering of multiindicies is given as follows. Let $m \in \mathbb{N}$ and $c, n \in \mathbb{N}^m$. We write $c \leq n$ to mean for all $j \in \{1, \ldots, m\}$ that $c_j \leq n_j$, for $c_j \in c$ and $n_j \in n$.

Remark 6.1.1. It is convention in the sum system literature that $(c_1, c_2) \in \mathbb{N}^2$ corresponds to the c_1-th column and c_2-th row, opposed to the standard interpretation which has the converse orientation. This is due to the decision to label the *1st coordinate axis* of a tensor as the first row.

Definition 6.1.2. Let $m \in \mathbb{N}$ and $n \in \mathbb{N}^m$. Then $\mathcal{M} \in \mathbb{N}_0^n$ is called an *order m tensor* (of dimensions $n_1, \ldots, n_m$). The entries of $\mathcal{M}$ are called *components*, which we denote $\mathcal{M}_c = \mathcal{M}_{(c_1,\ldots,c_m)} \in \mathbb{N}_0$, for $0_m \leq c \leq n - 1_m$. The index 0_m is the *root component* of a given tensor.

Furthermore, we say that $\mathcal{M}$ has the *vertex cross sum property (V)* if and only if, for $0 \leq c_j \leq n_j - 1$ for all $j \in \{1, \ldots, m\}$, and some $0 \leq c'_j \leq n_j - 1$ and $0 \leq c'_i \leq n_i - 1$, for $i \in \{1, \ldots, j-1\}$, the tensor $\mathcal{M}$ has the property

$$\mathcal{M}_{(c_1,\ldots,c_i,\ldots,c_j,\ldots,c_m)} + \mathcal{M}_{(c_1,\ldots,c'_i,\ldots,c'_j,\ldots,c_m)} = \mathcal{M}_{(c_1,\ldots,c_i,\ldots,c'_j,\ldots,c_m)} + \mathcal{M}_{(c_1,\ldots,c'_i,\ldots,c_j,\ldots,c_m)}.$$

Finally, we call an order m tensor $\mathcal{M} \in \mathbb{N}_0^n$ a *principal reversible m-cuboid* if $\mathcal{M}$ has property (V), its set of components is $\{\mathcal{M}_c : c \in \mathbb{N}_0^m, 0_m \leq c \leq n - 1_m\} = \langle N \rangle$, and every row in the j-th direction is arranged in strictly increasing order, for $j \in \{1, \ldots, m\}$.

If we are considering two-dimensional sum systems (i.e. $m = 2$), we may refer to the principal reversible 2-cuboid as the principal reversible matrix, as Ollerenshaw and Brée did.

Principal reversible cuboids provide a convenient way to visualise an m-part sum system. The elements of A_1 are the first row, the elements of A_2 form the first column, and any subsequent set A_j forms the j-th coordinate axis, hence why we use this label. They all intersect in the root position 0_m with the component 0. The component in position c is found by the sum of the c_1-th component in the first row, c_2-th component in the first column, up to the c_m-th component in the m-th axis. That is to say

$$\mathcal{M}_c = \mathcal{M}_{(c_1,0,\dots,0)} + \mathcal{M}_{(0,c_2,\dots,0)} + \cdots + \mathcal{M}_{(0,0,\dots,c_m)} = \sum_{j=1}^{m} \mathcal{M}_{c_j \bar{e}_j},$$

where $\bar{e}_j$ is the unit vector with 1 in the j-th position.

Example 6.1.3. Consider the sum system $A_1 = \{0, 1, 12, 13\}$, $A_2 = \{0, 2, 4\}$ and $A_3 = \{0, 6\}$. The corresponding principal reversible cuboid is

$$\mathcal{M} = \left(\begin{pmatrix} 0 & 1 & 12 & 13 \\ 2 & 3 & 14 & 15 \\ 4 & 5 & 16 & 17 \end{pmatrix}, \quad \begin{pmatrix} 6 & 7 & 18 & 19 \\ 8 & 9 & 20 & 21 \\ 10 & 11 & 22 & 23 \end{pmatrix} \right),$$

where we note that A_3 is the vector that intersects the root position, 0, and 6, which forms the 3rd coordinate axis. The component in position $c = (2, 1, 1)$ is

$$\mathcal{M}_{(2,1,1)} = \mathcal{M}_{(2,0,0)} + \mathcal{M}_{(0,1,0)} + \mathcal{M}_{(0,0,1)} = 12 + 2 + 6 = 20.$$

If we take the components $\mathcal{M}_{(2,1,1)} = 20$ and $\mathcal{M}_{(1,0,1)} = 7$, we can write

$$\mathcal{M}_{(2,1,1)} + \mathcal{M}_{(1,0,1)} = 20 + 7 = 27 = 9 + 18 = \mathcal{M}_{(1,1,1)} + \mathcal{M}_{(2,0,1)},$$

demonstrating that $\mathcal{M}$ has property (V).

For $m \in \mathbb{N}$ and $n \in \mathbb{N}_2^m$, we shall investigate how two additive systems of different joint ordered factorisations of n relate via their principal reversible cuboids, and study the group behaviour that emerges. To do this, consider the following motivational problem.

Let $\mathcal{J}_1, \mathcal{J}_2$ be two joint ordered factorisations, and let $\mathcal{M}, \mathcal{N} \in \mathbb{N}_0^n$ be their respective principal reversible cuboids. Since $\mathcal{J}_1$ and $\mathcal{J}_2$ are joint ordered factorisations of n, then $\mathcal{M}$ and $\mathcal{N}$ will have the same dimensions.

The component in the root position is 0 in both tensors, i.e. $\mathcal{M}_{0_m} = \mathcal{N}_{0_m} = 0$. The component in position $c = n - 1_m$ is $N - 1$ also in both, i.e. $\mathcal{M}_{n-1_m} = \mathcal{N}_{n-1_m} = N - 1$. Hence there is a notion of an invariance of the position of these two values between $\mathcal{M}$ and $\mathcal{N}$.

Now consider the component 1. By design, 1 is uniquely an element in one sum system component set for both $\mathcal{J}_1$ and $\mathcal{J}_2$, which depends on the first j-value in both tuples, denoted $j_1^{(1)}$ in $\mathcal{J}_1$ and $j_1^{(2)}$ in $\mathcal{J}_2$. Without loss of generality, let $j_1^{(1)} = 1$ such that $\mathcal{M}_{\bar{e}_1} = 1$. If we let $j_1^{(2)} = 2$, then $\mathcal{N}_{\bar{e}_2} = 1$, which means 1 is in a different position between $\mathcal{M}$ and $\mathcal{N}$.

For $M \in \langle N \rangle$ we can associate two positions $0_m \leq c^{(1)}, c^{(2)} \leq n - 1_m$, such that $M = \mathcal{M}_{c^{(1)}} = \mathcal{N}_{c^{(2)}}$. So what about $\mathcal{N}_{c^{(1)}}$? Let $\tilde{M} = \mathcal{N}_{c^{(1)}}$, so that $\tilde{M} = \mathcal{M}_{c^{(3)}}$ for some $0_m \leq c^{(3)} \leq n - 1_m$. We can now ask what value does $\mathcal{N}_{c^{(3)}}$ take?

By repeating this process, due to the pigeon-hole principle, we will inevitably return to our starting value M. Say this takes $d \in \mathbb{N}$ steps. We call this sequence of d terms that M moves the *cyclic orbit of* M. If $d = 1$ then M is invariant under this process and we call M a *fixed point*, such as $M = 0$ or $N - 1$.

It is answering this question which prompts the following chapters. The emergent structure of comparing component positions overlaps with many areas of mathematics, from finite field theory and coding theory, to a shared enumeration function that is connected to free groups on Lie algebras and more (see Section 7.2.4 for more).

We begin by setting up the required multi-index notation in order to describe the nested sum systems in the principal reversible cuboids.

6.2 Addresses and orbits

Let $m \in \mathbb{N}$, $n \in \mathbb{N}_2^m$, $m \leq L \leq \Omega(N)$ and $\mathcal{J} = \big((j_1, f_1), \ldots, (j_L, f_L)\big)$ a the joint ordered factorisation of n, with sum system $A_1, \ldots, A_m \subset \mathbb{N}_0$. For $j \in \{1, \ldots, m\}$, we write $A_j = \{a_0^{(j)}, a_1^{(j)}, \ldots, a_{n_j-1}^{(j)}\}$ and denote the position of pairs in $\mathcal{J}$ with j-value $j_\ell = j$ by

$\mathcal{L}_j = \{\ell_1, \dots, \ell_{k_j}\}$. For the partial products $F(\ell) = \prod_{s=1}^{\ell-1} f_s$ and $P_j(\ell) = \prod_{\substack{s\in\mathcal{L}_j \\ s<\ell}} f_s$, we define the following column vectors:

$$\vec{F} := \begin{pmatrix} F(1) \\ F(2) \\ \vdots \\ F(L) \end{pmatrix}, \qquad \vec{P} := \begin{pmatrix} P_{j_1}(1)\bar{e}_{j_1} \\ P_{j_2}(2)\bar{e}_{j_2} \\ \vdots \\ P_{j_L}(L)\bar{e}_{j_L} \end{pmatrix}.$$

By definition, each $M \in \langle N\rangle$ can be uniquely written as a sum of one element of each sum system component, i.e. $M = \sum\limits_{j=1}^{m} a^{(j)}$, for $a^{(j)} \in A_j$. As $A_j = \sum\limits_{\ell\in\mathcal{L}_j} F(\ell)\langle f_\ell\rangle$, then $a^{(j)}$ is uniquely represented by the sum of $F(\ell)\alpha_\ell$ for $\ell \in \mathcal{L}_j$ and some $\alpha_\ell \in \langle f_\ell\rangle$. Together, M can be represented by a multi-index that details these alpha values, as we formally state in the following definition.

Definition 6.2.1. Let $m \in \mathbb{N}$, $n \in \mathbb{N}_2^m$, $N = \prod_{j=1}^m n_j$, and $\mathcal{J} = \big((j_1, f_1), \dots, (j_L, f_L)\big)$ a joint ordered factorisation of n, for $L \in \{m, \dots, \Omega(N)\}$. For $M \in \{0, \dots, N-1\} = \langle N\rangle$, we define the *address of M (in $\mathcal{J}$)* to be the L-tuple

$$\alpha(M) := (\alpha_1, \dots, \alpha_L) \in \langle f_1\rangle \times \langle f_2\rangle \times \cdots \times \langle f_L\rangle = \bigtimes_{\ell=1}^{L} \langle f_\ell\rangle,$$

that satisfies the equality

$$M = (\alpha_1, \dots, \alpha_L) \begin{pmatrix} F(1) \\ \vdots \\ F(L) \end{pmatrix} = \alpha(M)\vec{F}. \tag{6.1}$$

We let $\alpha(M)_\ell = \alpha_\ell$ denote the ℓ-th term in $\alpha(M)$. Additionally, for $j \in \{1, \dots, m\}$ and $\mathcal{L}_j = \{\ell_1, \dots, \ell_{k_j} : j_\ell = j \text{ in } \mathcal{J}\}$, with suitable $k_j \in \mathbb{N}$, we define the *j-address of M* to be the k_j-tuple

$$\alpha(M; j) = \big(\alpha_{j,\ell_1}, \alpha_{j,\ell_2}, \dots, \alpha_{j,\ell_{k_j}}\big) \in \bigtimes_{\ell\in\mathcal{L}_j} \langle f_\ell\rangle,$$

which implies $\alpha(M) = \big(\alpha_{j_1,\ell_1}, \alpha_{j_2,\ell_1}, \dots, \alpha_{j_L,\ell_{k_{j_L}}}\big)$.

Example 6.2.2. Let $n = (12, 6)$ with $\mathcal{J} = \big((1,3), (2,2), (1,2), (2,3), (1,2)\big)$ a joint ordered factorisation of n, with the sum system $A_1 = \{0, 1, 2, 6, 7, 8, 36, 37, 38, 42, 43, 44\}$ and

$A_2 = \{0, 3, 12, 15, 24, 27\}$. We can compute $M = 32$ with the expression

$$32 = (2, 0, 1, 2, 0) \begin{pmatrix} 1 \\ 3 \\ 6 \\ 12 \\ 36 \end{pmatrix},$$

which implies the address of 32 is given by

$$\alpha(32) = (\alpha_{1,1}, \alpha_{2,1}, \alpha_{1,2}, \alpha_{2,2}, \alpha_{1,3}) = (2, 0, 1, 2, 0).$$

Remark 6.2.3. The address of M in $\mathcal{J}$ is non-linear, i.e. for $M, M_1, M_2 \in \langle N \rangle$, in general we have that $\alpha(M_1 + M_2) \neq \alpha(M_1) + \alpha(M_2)$ and $\lambda\alpha(M) \neq \alpha(\lambda M)$. However, for $a^{(j)} \in A_j$, the address of $a^{(j)}$ in $\mathcal{J}$ follows addition, i.e. $\alpha\big(a^{(i)} + a^{(j)}\big) = \alpha\big(a^{(i)}\big) + \alpha\big(a^{(j)}\big)$. To see why, for $\ell \in \mathcal{L}_j$ we have $\alpha\big(a^{(j)}\big)_\ell \in \langle f_\ell \rangle$, with $\alpha\big(a^{(i)}\big)_\ell = 0$, and so

$$\alpha\big(a^{(i)} + a^{(j)}\big)_\ell = \alpha\big(a^{(i)}\big)_\ell + \alpha\big(a^{(j)}\big)_\ell = \alpha\big(a^{(i)}\big)_\ell + 0 \in \langle f_\ell \rangle.$$

Example 6.2.4. In Example 6.2.2, we find that $\alpha(8) = (2, 0, 1, 0, 0)$ and $\alpha(24) = (0, 0, 0, 2, 0)$. Therefore $\alpha(32) = (2, 0, 1, 0, 0) + (0, 0, 0, 2, 0) = (2, 0, 1, 2, 0)$.

The address of M not only encodes the unique sum that makes M from a sum system, but also the coordinates for the position of M in the corresponding principal reversible cuboid.

Definition 6.2.5. Let $m \in \mathbb{N}$, $n \in \mathbb{N}_2^m$, $N = \prod_{j=1}^m n_j$, and $\mathcal{J} = \big((j_1, f_1), \dots, (j_L, f_L)\big)$ a joint ordered factorisation of n, for $L \in \{m, \dots, \Omega(N)\}$, with principal reversible cuboid $\mathcal{M}$. Let $M \in \langle N \rangle$ have address $\alpha(M) = (\alpha_1, \dots, \alpha_L)$. The *coordinate map of M (in $\mathcal{M}$)* is defined to be

$$C_{\mathcal{J}}(M) := \sum_{\ell=1}^{L} \alpha(M)_\ell P_{j_\ell}(\ell) \bar{e}_{j_\ell} = \alpha(M)\vec{P}, \tag{6.2}$$

such that

$$\mathcal{M}_{C_{\mathcal{J}}(M)} = M.$$

Example 6.2.6. Continuing Example 6.2.2, we can use the address $\alpha(32) = (2, 0, 1, 2, 0)$ to write

$$C_{\mathcal{J}}(32) = \alpha(32)\overrightarrow{P} = (2, 0, 1, 2, 0)\begin{pmatrix} 1\bar{e}_1 \\ 1\bar{e}_2 \\ 3\bar{e}_1 \\ 2\bar{e}_2 \\ 6\bar{e}_1 \end{pmatrix} = (5, 4).$$

It can be seen in Example 6.2.8 that $\mathcal{M}_{(5,4)} = 32$.

Let $\mathcal{J}_1, \mathcal{J}_2$ be joint ordered factorisations of n, with principal reversible cuboid $\mathcal{M}, \mathcal{N}$ respectively. For some $M \in \langle N \rangle$, as $C_{\mathcal{J}_1}(M)$ is the coordinates for the position of M in $\mathcal{M}$, then we can restate the motivational problem to this chapter as asking what value $\mathcal{N}_{C_{\mathcal{J}_1}(M)}$ take. Say that $\mathcal{N}_{C_{\mathcal{J}_1}(M)} = M^{(1)}$. Then we want to know what value $\mathcal{N}_{C_{\mathcal{J}_1}(M)}$ takes. We can repeat this process and, by the pigeon hole principle, will eventually return to M, i.e. $\mathcal{N}_{C_{\mathcal{J}_1}(M^{(d-1)})} = M$ for some $d \in \mathbb{N}$. It is the set $\{M, M^{(1)}, \ldots, M^{(d-1)}\}$ we are interested in, which we label as the *cyclic orbit* of M and formally define in the following definition.

Definition 6.2.7. Let $m \in \mathbb{N}$, $n \in \mathbb{N}_2^m$, $N = \prod_{j=1}^m n_j$, and $\mathcal{J}_1, \mathcal{J}_2$ be two joint ordered factorisations, with principal reversible cuboids $\mathcal{M}$ and $\mathcal{N}$ respectively. We define the *raising operator* for $M \in \langle N \rangle$ to be

$$O_{\mathcal{J}_1,\mathcal{J}_2}(M) := \mathcal{N}_{C_{\mathcal{J}_1}(M)}.$$

The inverse raising operator, which we call the *lowering operator*, is defined to be

$$(O_{\mathcal{J}_1,\mathcal{J}_2})^{-1}(M) := \mathcal{M}_{C_{\mathcal{J}_2}(M)},$$

and thus the raising operator is a bijection. Let $M^{(t)} = (O_{\mathcal{J}_1,\mathcal{J}_2})^t(M)$ denote t applications of the raising operator to M, for some $t \in \mathbb{N}$.

Furthermore, define the *cyclic orbit of M (between $\mathcal{J}_1$ and $\mathcal{J}_2$)* as the ordered set

$$\mathcal{O}_{\mathcal{J}_1,\mathcal{J}_2}(M) := \left\{(O_{\mathcal{J}_1,\mathcal{J}_2})^t(M) : t \in \langle d \rangle\right\} = \left\{M^{(0)}, M^{(1)}, \ldots, M^{(d-1)}\right\},$$

for some $d \in \mathbb{N}$. We say that M has *orbit of length* d and set

$$(O_{\mathcal{J}_1,\mathcal{J}_2})^d(M) = M^{(d)} := M^{(0)} = M,$$

which implies $|\mathcal{O}_{\mathcal{J}_1,\mathcal{J}_2}(M)| = d$. If $d = 1$, then M is invariant under $O_{\mathcal{J}_1,\mathcal{J}_2}$ and we call M a *fixed point.*

The choice for the naming of "raising" and "lowering" operators comes from the fact $O_{\mathcal{J}_1,\mathcal{J}_2}(M^{(t)}) = M^{(t+1)}$ and $(O_{\mathcal{J}_1,\mathcal{J}_2})^{-1}(M^{(t+1)}) = M^{(t)}$ respectively. When $\mathcal{J}_1$ and $\mathcal{J}_2$ are fixed or clearly stated in context, we may omit subscripts so that $O_{\mathcal{J}_1,\mathcal{J}_2} = O$ and $\mathcal{O}_{\mathcal{J}_1,\mathcal{J}_2} = \mathcal{O}$. Since $M^{(0)} = (O_{\mathcal{J}_1,\mathcal{J}_2})^0(M) = M$ we may use $M^{(0)}$ and M interchangeably.

We will be letting $t \in \langle d \rangle$, and note that

$$M^{(d+t)} = (O_{\mathcal{J}_1,\mathcal{J}_2})^{d+t}(M) = (O_{\mathcal{J}_1,\mathcal{J}_2})^{t}\big((O_{\mathcal{J}_1,\mathcal{J}_2})^{d}(M)\big) = (O_{\mathcal{J}_1,\mathcal{J}_2})^{t}(M) = M^{(t)}.$$

For $M^{(t)}, M^{(t+1)} \in \mathcal{O}_{\mathcal{J}_1,\mathcal{J}_2}(M)$, we have that $C_{\mathcal{J}_1}\big(M^{(t)}\big) = C_{\mathcal{J}_2}\big(M^{(t+1)}\big)$. If M is a fixed point, then $C_{\mathcal{J}_1}(M) = C_{\mathcal{J}_2}(M)$.

For $M_1, M_2 \in \langle N \rangle$, if $M_2 \notin \mathcal{O}_{\mathcal{J}_1,\mathcal{J}_2}(M_1)$, then $\mathcal{O}_{\mathcal{J}_1,\mathcal{J}_2}(M_1) \cap \mathcal{O}_{\mathcal{J}_1,\mathcal{J}_2}(M_2) = \emptyset$.

We call the set of minimum representatives $\mathcal{T} := \big\{ \min \mathcal{O}_{\mathcal{J}_1,\mathcal{J}_2}(M) \,:\, M \in \langle N \rangle \big\}$ the *transversal (between $\mathcal{J}_1$ and $\mathcal{J}_2$)*, which satisfies

$$\langle N \rangle = \bigcup_{M \in \mathcal{T}} \mathcal{O}_{\mathcal{J}_1,\mathcal{J}_2}(M).$$

Therefore, the cyclic orbits between $\mathcal{J}_1$ and $\mathcal{J}_2$ partitions $\langle N \rangle$, and the lengths of the orbits form an integer partition of N, i.e. $N = \sum\limits_{M \in \mathcal{T}} |\mathcal{O}_{\mathcal{J}_1,\mathcal{J}_2}(M)|$.

We associate the cyclic orbit $\mathcal{O}_{\mathcal{J}_1,\mathcal{J}_2}(M) = \big\{M^{(0)},\ \ldots,\ M^{(d-1)}\big\}$ with the permutation, written in cycle notation, given by

$$\varsigma(M) := \Big(M^{(0)}\ \ M^{(1)}\ \ \ldots\ \ M^{(d-1)}\Big).$$

For $M \in \mathcal{T}$, we define the *full orbit permutation (between $\mathcal{J}_1$ and $\mathcal{J}_2$)* to be the permutation

$$\sigma_{\mathcal{J}_1,\mathcal{J}_2} := \varsigma(0)\,\varsigma(1)\ \ldots\ \varsigma(M)\ \ldots\ \varsigma(N-1).$$

We note that $\sigma^{-1}_{\mathcal{J}_1,\mathcal{J}_2} = \sigma_{\mathcal{J}_2,\mathcal{J}_1}$. We also direct attention to the fact that the elements of $\varsigma(M)$ will not appear as multiple permutations as we consider only cyclic orbits for $M \in \mathcal{T}$.

Example 6.2.8. Continuing Example 6.2.2, the principal reversible matrix of the joint ordered factorisation $\mathcal{J}_1 = \big((1,3),(2,2),(1,2),(2,3),(1,2)\big)$ is

$$\mathcal{M} = \begin{pmatrix} 0 & 1 & 2 & 6 & 7 & 8 & 36 & 37 & 38 & 42 & 43 & 44 \\ 3 & 4 & 5 & 9 & 10 & 11 & 39 & 40 & 41 & 45 & 46 & 47 \\ 12 & 13 & 14 & 18 & 19 & 20 & 48 & 49 & 50 & 54 & 55 & 56 \\ 15 & 16 & 17 & 21 & 22 & 23 & 51 & 52 & 53 & 57 & 58 & 59 \\ 24 & 25 & 26 & 30 & 31 & 32 & 60 & 61 & 62 & 66 & 67 & 68 \\ 27 & 28 & 29 & 33 & 34 & 35 & 63 & 64 & 65 & 69 & 70 & 71 \end{pmatrix}.$$

Let us also consider $\mathcal{J}_2 = \big((1,6),(2,2),(1,2),(2,3)\big)$ with principal reversible cuboid

$$\mathcal{N} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 12 & 13 & 14 & 15 & 16 & 17 \\ 6 & 7 & 8 & 9 & 10 & 11 & 18 & 19 & 20 & 21 & 22 & 23 \\ 24 & 25 & 26 & 27 & 28 & 29 & 36 & 37 & 38 & 39 & 40 & 41 \\ 30 & 31 & 32 & 33 & 34 & 35 & 42 & 43 & 44 & 45 & 46 & 47 \\ 48 & 49 & 50 & 51 & 52 & 53 & 60 & 61 & 62 & 63 & 64 & 65 \\ 54 & 55 & 56 & 57 & 58 & 59 & 66 & 67 & 68 & 69 & 70 & 71 \end{pmatrix}.$$

Let $M = 32$. We wish to detail $\mathcal{O}(32)$. Initially, we have

$$O(32) = \mathcal{N}_{C_{\mathcal{J}_1}(32)} = \mathcal{N}_{(5,4)} = 53 = (2,1,0,1,1)\vec{F}.$$

The position of 53 in $\mathcal{M}$ is $C_{\mathcal{J}_1}(53) = (2,1,0,1,1)\vec{P} = (8,3)$, and thus the raising operator of 53 is

$$O(53) = \mathcal{N}_{C_{\mathcal{J}_1}(53)} = \mathcal{N}_{(8,3)} = 44 = (2,0,1,0,1)\vec{F}.$$

The position of 44 in $\mathcal{M}$ is $C_{\mathcal{J}_1}(44) = (2,0,1,0,1)\vec{P} = (11,0)$, and thus the raising operator of 44 is

$$O(4) = \mathcal{N}_{C_{\mathcal{J}_1}(44)} = \mathcal{N}_{(11,0)} = 17 = (2,1,0,1,0)\vec{F}.$$

The position of 17 in $\mathcal{M}$ is $C_{\mathcal{J}_1}(17) = (2,1,0,1,0)\vec{P} = (2,3)$, and thus the raising operator of 17 is

$$O(17) = \mathcal{N}_{C_{\mathcal{J}_1}(17)} = \mathcal{N}_{(2,3)} = 32.$$

Then 32 is mapped to 53, which is mapped to 44, which is mapped to 17, which is mapped back to 32. Hence the cyclic orbit of 32 is

$$\mathcal{O}_{\mathcal{J}_1,\mathcal{J}_2}(32) = \{32, 53, 44, 17\},$$

which has length $d = 4$. We would usually refer to this set by the minimum representative which is 17, opposed to 32. By considering each $M \in \langle 72 \rangle$, the transversal between $\mathcal{J}_1$ and $\mathcal{J}_2$ is

$$\begin{aligned} \mathcal{T} = \{&0, 1, 2, 3, 4, 5, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, \\ &19, 20, 21, 22, 23, 60, 61, 62, 63, 64, 65, 69, 70, 71\}, \end{aligned}$$

and the full orbit permutation between $\mathcal{J}_1$ and $\mathcal{J}_2$ is

$$\begin{aligned} \sigma_{\mathcal{J}_1,\mathcal{J}_2} = &(0)\ (1)\ (2)\ (3\ \ 6)\ (4\ \ 7)\ (5\ \ 8)\ (9)\ (10)\ (11)\ (12\ \ 24\ \ 48\ \ 36)\ (13\ \ 25\ \ 49\ \ 37)\ (14\ \ 26\ \ 50\ \ 38) \\ &(15\ \ 30\ \ 51\ \ 42)\ (16\ \ 31\ \ 52\ \ 43)\ (17\ \ 32\ \ 53\ \ 44)\ (18\ \ 27\ \ 54\ \ 39)\ (19\ \ 28\ \ 55\ \ 40) \\ &(20\ \ 29\ \ 56\ \ 41)\ (21\ \ 33\ \ 57\ \ 45)\ (22\ \ 34\ \ 58\ \ 46)\ (23\ \ 35\ \ 59\ \ 47) \\ &(60)\ (61)\ (62)\ (63\ \ 66)\ (64\ \ 67)\ (65\ \ 68)\ (69)\ (70)\ (71). \end{aligned}$$

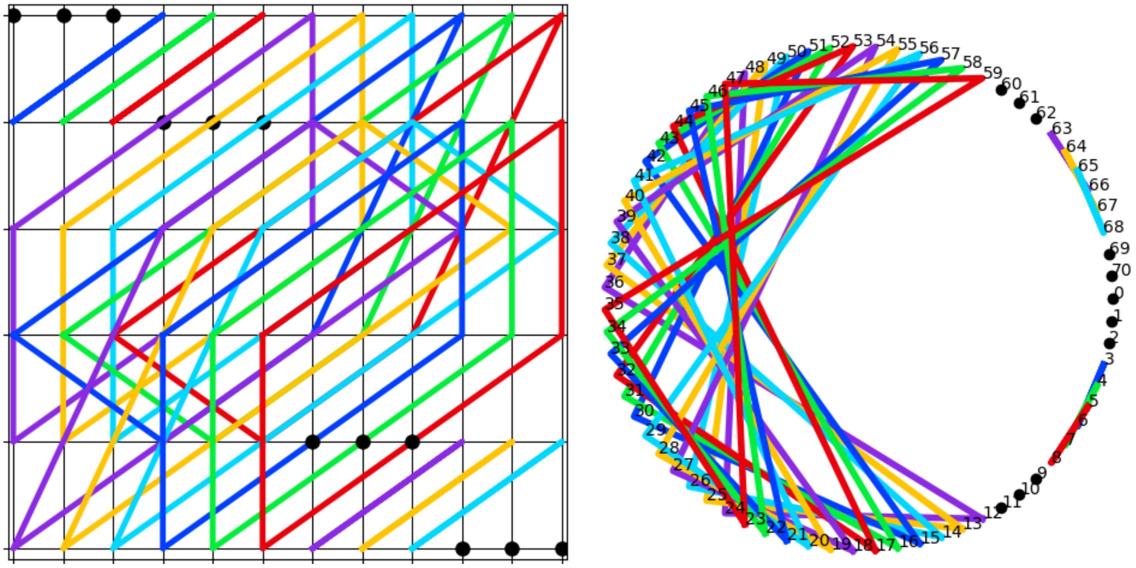
We now give two geometric visualisation for the permutation $\sigma_{\mathcal{J}_1,\mathcal{J}_2}$.

Cuboid Geometry: We write either tensor $\mathcal{M}$ or $\mathcal{N}$, and draw a line between each component in the order they appear in their orbit, drawing a dot for fixed points. When $m > 3$ these lines might be difficult to draw, and the full geometry of these orbits might be lost as a result. But for the two or three dimensional case (i.e. $m = 2$ or 3) this diagram is easily understood.

Ring Geometry: Put $N - 2$ points equidistant on a circle and label them 0 to $N - 2$. Then draw lines between the points corresponding to elements in the order they appear in their orbits, with dots representing fixed points. Though we lose the block structuring of the principal reversible cuboids, we can compactly show the orbits for any $m \in \mathbb{N}$.

We use $N - 2$ due to the modulo $N - 1$ behaviour these orbits obey which we discuss in future sections. This second approach parallels the notion of the $N - 2$-th roots of unity, and indeed we will see that the cyclic orbit sets are in fact objects called *cyclotomic cosets*, which are used in factorising the function $x^{N-1} - 1$.

Example 6.2.9. Continuing Example 6.2.8, the cuboid and ring geometries are



Note that two cyclic orbits having the same colour does not indicate any relation between those sets.

In the next section we will investigate how a full orbit permutation $\sigma_{\mathcal{J}_1,\mathcal{J}_2}$ can contain nested orbits between reduced versions of $\mathcal{J}_1$ and $\mathcal{J}_2$. This property arises when $\mathcal{J}_1$ and $\mathcal{J}_2$ share the same first and last few pairs. By removing these pairs from these joint ordered factorisation, we are left with a system of cyclic orbits that will form the canonical orbit pattern of $\sigma_{\mathcal{J}_1,\mathcal{J}_2}$.

To understand the structure of a cyclic orbit, we require explicit forms for $\mathcal{J}_1$ and $\mathcal{J}_2$. This leads to us considering two-dimensional expressions when $\mathcal{J}_1$ has L_1 pairs and $\mathcal{J}_2$ has L_2 pairs, for examples when $L_1 \in \{3,4\}$ and $L_2 \in \{2,3\}$. When $L_1 = L_2 = 3$ we will demonstrate that the identities we find are not complete enough to fully describe the cyclic orbits. Similarly for $L_1 = 4$ and $L_2 = 3$, but not if $L_1 = 4$ and $L_2 = 2$.

In the next chapter we consider the special case $L_1 = L_2 = 2$, with $\mathcal{J}_1 = \big((1,n_1),(2,n_2)\big)$ and $\mathcal{J}_2 = \big((2,n_2),(1,n_1)\big)$, for $n_1, n_2 \in \mathbb{N}$. In this special case, the formulae found are sufficient to completely detail the full orbit permutation $\sigma_{\mathcal{J}_1,\mathcal{J}_2}$.

6.3 Orbits of length d

Given two joint ordered factorisations $\mathcal{J}_1$ and $\mathcal{J}_2$, in order to formulate a system of equations that represents the cyclic orbit $\mathcal{O}_{\mathcal{J}_1,\mathcal{J}_2}$ we need to find an explicit expression for the raising operator $O_{\mathcal{J}_1,\mathcal{J}_2}$. This can be achieved by equating raising operators for elements in $\mathcal{M}$ and $\mathcal{N}$, as well as a recurrence relation with their coordinate maps.

In what follows, let $m \in \mathbb{N}$, $n \in \mathbb{N}_2^m$, $m \leq L_1, L_2 \leq \Omega(N)$, and let $\mathcal{J}_1$ and $\mathcal{J}_2$ be joint ordered factorisations of n with L_1 and L_2 pairs respectively, and with $\mathcal{M}$ and $\mathcal{N}$ their corresponding principal reversible cuboids. For $M \in \langle N\rangle$, with cyclic orbit $\mathcal{O}(M) = \{M^{(0)}, \dots, M^{(d-1)}\}$ of length $d \in \mathbb{N}$, we denote the address of $M^{(t)}$ in $\mathcal{J}_1$ as $\alpha\big(M^{(t)}\big) = \big(\alpha_1^{(t)}, \dots, \alpha_{L_1}^{(t)}\big)$ and the address of $M^{(t)}$ in $\mathcal{J}_2$ as $\beta\big(M^{(t)}\big) = \big(\beta_1^{(t)}, \dots, \beta_{L_2}^{(t)}\big)$.

For $\kappa \in \{1, 2\}$ and $j \in \{1, \dots, m\}$, define the partial products

$$F(\kappa;\ell) = \prod_{s=1}^{\ell-1} f_\ell^{(\kappa)}, \quad \text{and} \quad P_j(\kappa;\ell) = \prod_{\substack{p\in\mathcal{L}_j^\kappa \\ p<\ell}} f_p^{(\kappa)},$$

where $f_\ell^{(\kappa)}$ is the f-value of the ℓ-th pair in $\mathcal{J}_\kappa$, and $\mathcal{L}_j^\kappa = \{\ell : j_\ell = j \text{ in } \mathcal{J}_\kappa\}$ the positions of pairs corresponding to the j-th coordinate axis in $\mathcal{J}_\kappa$. We further define the column vectors

$$\overrightarrow{F(\kappa)} := \begin{pmatrix} F(\kappa;1) \\ \vdots \\ F(\kappa;L) \end{pmatrix}, \qquad \overrightarrow{P_j(\kappa)} := \begin{pmatrix} P_j(\kappa;\ell_1) \\ \vdots \\ P_j(\kappa;\ell_{k_j}) \end{pmatrix}.$$

Recall the j-address of M, which in $\mathcal{J}_1$ we denote $\alpha\big(M^{(t)};j\big) = \big(\alpha_{\ell_1}^{(t)}, \dots, \alpha_{\ell_u}^{(t)}\big)$ (for $\ell_i \in \mathcal{L}_j^1$), and in $\mathcal{J}_2$ we denote $\beta\big(M^{(t)};j\big) = \big(\beta_{\ell'_1}^{(t)}, \dots, \beta_{\ell'_v}^{(t)}\big)$ (for $\ell'_i \in \mathcal{L}_j^2$).

For $t \in \langle d\rangle$, we wish to investigate the system of linear Diophantine equations:

$$\alpha\big(M^{(t)}\big)\overrightarrow{F(1)} = M^{(t)} = \beta\big(M^{(t)}\big)\overrightarrow{F(2)},$$

$$C_{\mathcal{J}_1}\big(M^{(t)}\big) = C_{\mathcal{J}_2}\big(M^{(t+1)}\big).$$

These equations equate the address of $M^{(t)}$ in $\mathcal{J}_1$ and $\mathcal{J}_2$, and the position of $M^{(t)}$ in $\mathcal{J}_1$

with the position of $M^{(t+1)}$ in $\mathscr{J}_2$. When written explicitly, we get the system of equations

$$\begin{aligned}
\alpha_1^{(t)} F(1;1) + \cdots + \alpha_{L_1}^{(t)} F(1;L_1) = M^{(t)} &= \beta_1^{(t)} F(2;1) + \cdots + \beta_{L_2}^{(t)} F(2;L_2),\\
\alpha\big(M^{(t)};1\big)\overrightarrow{P_1(1)} &= \beta\big(M^{(t+1)};1\big)\overrightarrow{P_1(2)},\\
\alpha\big(M^{(t)};2\big)\overrightarrow{P_2(1)} &= \beta\big(M^{(t+1)};2\big)\overrightarrow{P_2(2)},\\
&\vdots\\
\alpha\big(M^{(t)};m\big)\overrightarrow{P_m(1)} &= \beta\big(M^{(t+1)};m\big)\overrightarrow{P_m(2)}.
\end{aligned} \tag{6.3}$$

If $t = d-1$, then we take $\alpha\big(M^{(d-1)};j\big)\overrightarrow{P_j(1)} = \beta\big(M^{(0)};j\big)\overrightarrow{P_j(2)}$.

If $d = 1$, i.e. M is a fixed point, then these systems of equations simplify to

$$\begin{aligned}
\alpha(M)\overrightarrow{F(1)} = M &= \beta(M)\overrightarrow{F(2)},\\
\alpha(M;j)\overrightarrow{P_j(1)} &= \beta(M;j)\overrightarrow{P_j(2)},
\end{aligned}$$

for $j \in \{1, \dots, m\}$.

To analyse these identities further, an explicit expression for $\mathscr{J}_1$ and $\mathscr{J}_2$ must be given. For the next two chapters we will focus on the two-dimensional case, when $m = 2$.

In the next chapter we consider the joint ordered factorisations $\big((1,n_1),(2,n_2)\big)$ and $\big((2,n_2),(1,n_1)\big)$, for $n_1, n_2 \in \mathbb{N}_2$. These forms are the simplest two joint ordered factorisations can take. Due to this, the raising operators and cyclic orbits can be entirely described in terms of n_1 and n_2, with any address terms vanishing when we consider congruence relations. We will see that there are close links in the structure and enumeration of these cyclic orbits to the theory of cyclotomic cosets from coding theory.

In the following chapter we will consider joint ordered factorisations containing more than two pairs. The orbit structure between these principal reversible cuboids will mimic the orbit structure of simpler systems, repeating and stretching the cyclic orbits. We will then attempt to construct similar arguments used in the next chapter on these longer tuples, which will highlight just how complicated these structures get beyond the simplest cases.

6.4 Conclusion

It has been understood since 2019 that sum systems can be found embedded into matrices and tensors as their coordinate axes [42]. Hence a comparison between two of these structures will outline discrepancies in their building blocks, which can be traced to how the corresponding two joint ordered factorisations differ.

Any value in the system can be assigned a unique multi-index tuple, their address, which identifies which arithmetic contributions generate the term. These addresses can be used to retrieve which element of each sum system component is used in its unique sum. If two joint ordered factorisations are different, then so will be the addresses of the same value.

Since these addresses also inform us of the position in the principal reversible cuboids said value appears, we can compare pair-wise components in these tensors at the same coordinate.

By carrying out this comparison check for all integers in the system, we can identify which values occupy the same coordinates as one another, and collecting this information gives us the cyclic orbit of the value.

With this setup, establishing the core ideas behind this notion of orbits between principal reversible cuboids, we are now able to investigate specific cases, and attain some global patterns nested within these structures.

Chapter 7

The Number of Two-Dimensional Orbits and Cyclotomy

As outlined in the previous chapter, the discrepancies between two principal reversible cuboids resolves to a matter of differences between the corresponding joint ordered factorisations. The longer the tuples are, the more complicated their structure, and the less wieldy the theory of orbits become. Therefore, in this chapter we shall investigate the orbit between two joint ordered factorisations which both consist of only two pairs, in two-dimensions.

That is to say, let $n_1, n_2 \in \mathbb{N}$ and consider the joint ordered factorisations $\big((1, n_1), (2, n_2)\big)$ and $\big((2, n_2), (1, n_1)\big)$. For an integer $M \in \langle n_1 n_2 \rangle = \{0, 1, \ldots, n_1 n_2 - 1\}$, we will see that its cyclic orbit between these two joint ordered factorisations will take the form

$$\begin{aligned}\mathcal{O}(M) &\equiv \big\{n_1^d M,\ n_1^{d-1} M,\ n_1^{d-2} M,\ \ldots, n_1 M\big\} \pmod{n_1 n_2 - 1}\\ &\equiv \big\{M,\ n_2 M,\ n_2^2 M,\ \ldots, n_2^{d-1} M\big\} \pmod{n_1 n_2 - 1},\end{aligned}$$

with orbit length $d \mid \varphi(n_1 n_2 - 1)$, where φ is Euler's totient function, as shown by Eq. (7.11).

These forms are then shown to be cyclotomic cosets, objects that naturally arise in coding theory which, for $n, q \in \mathbb{N}$ such that $\gcd(n, q) = 1$ and $s \in \langle n \rangle$, take the form

$$\mathcal{C}(n, q, s) = \big\{s, sq, sq^2, \ldots, sq^{d-1}\big\} \pmod{n},$$

and s is said to have order $d \mid \varphi(n)$ (akin to the length of a cyclic orbit being d). This connection provides a well known enumeration function to count the number of cyclic orbits between the two restricted joint ordered factorisations $\big((1,\eta^{u-t}),(2,\eta^{t})\big)$ and $\big((2,\eta^{t}),(1,\eta^{u-t})\big)$, with $\eta, t, u \in \mathbb{N}$.

This chapter concludes by establishing an enumeration for orbits between the two generalised joint ordered factorisations $\big((1,n_1),(2,n_2)\big)$ and $\big((2,n_2),(1,n_1)\big)$.

Theorem 7.2.14, Theorem 7.2.16 and Theorem 7.3.2 are the important results of this section.

7.1 Orbits between $\big((1,n_1),(2,n_2)\big)$ and $\big((2,n_2),(1,n_1)\big)$

In the lemmas and theorems throughout this section, we will use the following hypothesis.

Hypothesis statement 1 (H1): Let $n = (n_1, n_2) \in \mathbb{N}_2^2$, $N = n_1 n_2$, and consider the two two-dimensional joint ordered factorisations $\mathcal{J}_1 = \big((1,n_1),(2,n_2)\big)$ and $\mathcal{J}_2 = \big((2,n_2),(1,n_1)\big)$. Let $\mathcal{M}$ and $\mathcal{N}$ be the principal reversible cuboids of $\mathcal{J}_1$ and $\mathcal{J}_2$ respectively.

For integer $M \in \langle N\rangle = \{0,1,\ldots,N-1\}$, the cyclic orbit of M is given by

$$\mathcal{O}_{\mathcal{J}_1,\mathcal{J}_2}(M) = \mathcal{O}(M) = \Big\{M^{(0)},\ M^{(1)},\ \ldots,\ M^{(d-1)}\Big\}$$

with length $d \in \mathbb{N}$. For $t \in \langle d\rangle$, let $M^{(t)} \in \mathcal{O}(M)$ be the t-th term in the cyclic orbit of M, where we set $M^{(d)} = M^{(0)} = M$. Furthermore, the raising operator is given by

$$O_{\mathcal{J}_1,\mathcal{J}_2}\big(M^{(t)}\big) = O\big(M^{(t)}\big) = \mathcal{N}_{C_{\mathcal{J}_1}(M^{(t)})} = M^{(t+1)},$$

where $C_{\mathcal{J}_1}\big(M^{(t)}\big)$ is the coordinate map of M in $\mathcal{J}_1$ (see Definition 6.2.5). Furthermore, for some $s \in \{-d+1,\ldots,d-1\}$, let $O^{s}\big(M^{(t)}\big) = M^{(t+s)}$ denote s applications of the raising operator to $M^{(t)}$. See Definition 6.2.7 for more on cyclic orbits and raising operators.

The address of $M^{(t)}$ in $\mathcal{J}_1$ is $\alpha\big(M^{(t)}\big) = \big(\alpha_1^{(t)}, \alpha_2^{(t)}\big) \in \langle n_1\rangle \times \langle n_2\rangle$. Note that we will not be considering addresses in $\mathcal{J}_2$ (aside from the first proof below). See Definition 6.2.1 for more on addresses.

Lemma 7.1.1. Assume (H1). The raising operator of M is given by

$$O(M) = n_2\alpha_1 + \alpha_2. \tag{7.1}$$

Additionally, M and $O(M)$ relate by the following recursive relations;

$$n_1 O(M) = M + \alpha_1 (N-1), \tag{7.2}$$

$$O(M) = n_2 M - \alpha_2 (N-1). \tag{7.3}$$

Proof. Let the address of $O(M)$ in $\mathcal{J}_2$ be $\beta\big(O(M)\big) = \big(\beta_1^{(1)}, \beta_2^{(1)}\big) \in \langle n_2 \rangle \times \langle n_1 \rangle$. The first equation in (6.3) can be written as

$$\alpha_1^{(1)} + n_1 \alpha_2^{(1)} = O(M) = n_2 \beta_1^{(1)} + \beta_2^{(1)}.$$

The second equation in (6.3) informs us that we can write $\beta_\kappa^{(1)} = \alpha_\kappa$, for $\kappa \in \{1, 2\}$, with the address of M in $\mathcal{J}_1$ as $\alpha(M) = (\alpha_1, \alpha_2)$. After this substitution we have Eq. (7.1). By considering $M + \alpha_1(n_1 n_2 - 1)$ we can write

$$M + \alpha_1(n_1 n_2 - 1) = \alpha_1 + n_1 \alpha_2 + \alpha_1(n_1 n_2 - 1) = n_1(n_2 \alpha_1 + \alpha_2) = n_1 O(M),$$

deducing Eq. (7.2). By considering the equation $n_2 M - \alpha_2(n_1 n_2 - 1)$, we can write

$$n_2 M - \alpha_2(n_1 n_2 - 1) = n_2 \alpha_1 + n_1 n_2 \alpha_2 - \alpha_2(n_1 n_2 - 1) = n_2 \alpha_1 + \alpha_1 = O(M),$$

which is Eq. (7.3). □

The equations in Lemma 7.1.1 gives a complete description for each cyclic orbit $\mathcal{O}(M)$, since $O(M)$ needs only information about M to calculate it - a problem we will encounter with joint ordered factorisations with more than 2 pairs.

We can generalise Eq. (7.1), Eq. (7.2) and Eq. (7.3) to considering the t-th term in a cyclic orbit for M. That is to say, given the cyclic orbit $\mathcal{O}(M) = \big\{M^{(0)}, M^{(1)}, \ldots, M^{(d-1)}\big\}$, consecutive terms satisfy

$$O\big(M^{(t)}\big) = M^{(t+1)} = n_2 \alpha_1^{(t)} + \alpha_2^{(t)},$$

$$n_1 M^{(t+1)} = M^{(t)} + \alpha_1^{(t)}(N-1), \tag{7.4}$$

$$M^{(t+1)} = n_2 M^{(t)} - \alpha_2^{(t)}(N-1). \tag{7.5}$$

Remark 7.1.2. We can write Eq. (7.4) and Eq. (7.5) as the congruence relations

$$n_1 M^{(t+1)} \equiv M^{(t)} \pmod{N-1}, \tag{7.6}$$

$$M^{(t+1)} \equiv n_2 M^{(t)} \pmod{N-1}. \tag{7.7}$$

These two congruence relations do not rely on the address of $M^{(t)}$, and thus give a straightforward approach to calculate the raising operator $O\big(M^{(t)}\big) = M^{(t+1)}$. By multiplying $M^{(t)}$ by n_2 modulo $N-1$, we calculate the next term, $M^{(t+1)}$, in the orbit (applying the raising operator), whereas multiplying by n_1 modulo $N-1$ gives the prior term, $M^{(t-1)}$ (applying the lowering operator). These equations are the the quickest, and most direct, way to generate a cyclic orbit.

Corollary 7.1.3. Assume (H1) and consider $M \in \{0, \ldots, N-2\}$. Then $\alpha(M^{(t)}) = (\alpha_1^{(t)}, \alpha_2^{(t)})$, the address of $M^{(t)}$, satisfies

$$\alpha_1^{(t)} = \left\lfloor \frac{n_1 M^{(t+1)}}{N-1} \right\rfloor, \qquad \text{and} \qquad \alpha_2^{(t)} = \left\lfloor \frac{n_2 M^{(t)}}{N-1} \right\rfloor.$$

Proof. For $x, y \in \mathbb{N}$, the modulo operation gives the remainder of x divided by y, which can be written as $x \pmod{y} = x - y\left\lfloor \frac{x}{y} \right\rfloor$. Then the congruence relations Eq. (7.6) and Eq. (7.7) can be respectively written as

$$n_1 M^{(t+1)} \pmod{N-1} = n_1 M^{(t+1)} - (N-1)\left\lfloor \frac{n_1 M^{(t+1)}}{N-1} \right\rfloor,$$

$$n_2 M^{(t)} \pmod{N-1} = n_2 M^{(t)} - (N-1)\left\lfloor \frac{n_2 M^{(t)}}{N-1} \right\rfloor.$$

Equating these expression to Eq. (7.4) and Eq. (7.5), we deduce that

$$\alpha_1^{(t)} = \left\lfloor \frac{n_1 M^{(t+1)}}{N-1} \right\rfloor, \qquad \text{and} \qquad \alpha_2^{(t)} = \left\lfloor \frac{n_2 M^{(t)}}{N-1} \right\rfloor,$$

as required. □

Note that when $M = N-1$, Corollary 7.1.3 tells us that the address of M is

$$\alpha(N-1) = \left(\left\lfloor \frac{n_1(N-1)}{N-1} \right\rfloor, \left\lfloor \frac{n_2(N-1)}{N-1} \right\rfloor \right) = (n_1, n_2),$$

but since $\alpha(M) \in \langle n_1 \rangle \times \langle n_2 \rangle$ this can not occur, hence its omission in the assumption.

Lemma 7.1.4. Assume (H1). We can express $M^{(t)}$ and $M^{(d-t)}$ in terms of $M = M^{(0)}$ by the equations

$$O^{-t}\big(M^{(0)}\big) = M^{(d-t)} = n_1^t M^{(0)} - (N-1)\sum_{j=0}^{t-1} n_1^j \alpha_1^{(d-t+j)}, \tag{7.8}$$

$$O^{t}\big(M^{(0)}\big) = M^{(t)} = n_1^{d-t} M^{(0)} - (N-1)\sum_{j=0}^{d-t-1} n_1^j \alpha_1^{(t+j)}, \tag{7.9}$$

$$O^{t}\big(M^{(0)}\big) = M^{(t)} = n_2^{t} M^{(0)} - (N-1)\sum_{j=0}^{t-1} \alpha_2^{(j)} n_2^{t-j-1}. \tag{7.10}$$

Proof. We use proof by induction to prove the statements

$$\mathcal{P}_1(t): \quad M^{(d-t)} + (N-1)\sum_{j=0}^{t-1} n_1^j \alpha_1^{(d-t+j)} = n_1^t M^{(0)},$$

$$\mathcal{P}_2(t): \quad M^{(t)} + (N-1)\sum_{j=0}^{t-1} \alpha_2^{(j)} n_2^{t-j-1} = n_2^t M^{(0)},$$

is true for $t \in \langle d \rangle$.

Base Step: For $\mathcal{P}_1(0)$ and $\mathcal{P}_2(0)$ we have

$$\mathcal{P}_1(0): \quad M^{(d)} + (N-1)\sum_{j=0}^{-1} n_1^j \alpha_1^{(d+j)} = M^{(0)},$$

$$\mathcal{P}_2(0): \quad M^{(0)} + (N-1)\sum_{j=0}^{-1} \alpha_2^{(j)} n_2^{-j-1} = M^{(0)},$$

as $M^{(d)} = M^{(0)}$ by definition, and the summation is from $j = 0$ to -1 which is the empty sum and thus equals 0.

Induction Step: We now assume that $\mathcal{P}_1(t)$ and $\mathcal{P}_2(t)$ are true for $t \in \langle d \rangle$. We show $\mathcal{P}_1(t+1)$ holds true by writing

$$\begin{aligned}
M^{(d-t-1)} &+ (N-1)\sum_{j=0}^{t} n_1^j \alpha_1^{(d-t-1+j)} \\
&= M^{(d-t-1)} + (N-1) n_1^0 \alpha_1^{(d-t-1)} + (N-1)\sum_{j=1}^{t} n_1^j \alpha_1^{(d-t-1+j)} \\
&= n_1 M^{(d-t)} + (N-1)\sum_{j=0}^{t-1} n_1^{j+1} \alpha_1^{(d-t+j)} \\
&= n_1\Big(M^{(d-t)} + (N-1)\sum_{j=0}^{t-1} n_1^j \alpha_1^{(d-t+j)}\Big) = n_1^{t+1} M^{(0)}
\end{aligned}$$

where we have used Eq. (7.4) and shifted the index of summation from $j = 1$ to $j = 0$ in the third line, applying $\mathcal{P}_1(t)$ in the last. This deduces Eq. (7.8).

To show $\mathcal{P}_2(t+1)$ is true, we have that

$$\begin{aligned} M^{(t+1)} + (N-1)\sum_{j=0}^{t} \alpha_2^{(j)} n_2^{t-j} \\ &= n_2 M^{(t)} - \alpha_2^{(t)}(N-1) + (N-1)\alpha_2^{(t)} n_2^{t-t} + (N-1)n_2 \sum_{j=0}^{t-1} \alpha_2^{(j)} n_2^{t-j-1} \\ &= n_2\Big(M^{(t)} + (N-1)\sum_{j=0}^{t-1} \alpha_2^{(j)} n_2^{t-j-1}\Big) = n_2^{t+1} M^{(0)}, \end{aligned}$$

where we use Eq. (7.5) and $\mathcal{P}_2(t)$ in the last line. This proves Eq. (7.10). Finally, we shift the index of summation in Eq. (7.8) from t to $d-t$ to deduce Eq. (7.9). □

Remark 7.1.5. Normally Eq. (7.8), Eq. (7.9) and Eq. (7.10) would not prove efficient to calculate $M^{(t)}$ since the summation requires the address of each subsequent term before for. However, by writing these formulae as congruence relations modulo $N-1$, we remove this summation and are left with

$$M^{(d-t)} \equiv n_1^t M^{(0)} \pmod{N-1},$$

$$M^{(t)} \equiv n_1^{d-t} M^{(0)} \pmod{N-1},$$

$$M^{(t)} \equiv n_2^t M^{(0)} \pmod{N-1}.$$

This enables us to express the cyclic orbit of M modulo $N-1$ as

$$\begin{aligned} \mathcal{O}(M) &\equiv \big\{n_1^d M,\, n_1^{d-1} M,\, n_1^{d-2} M,\, \ldots, n_1 M\big\} \pmod{N-1} \\ &\equiv \big\{M,\, n_2 M,\, n_2^2 M,\, \ldots, n_2^{d-1} M\big\} \pmod{N-1}, \\ &\equiv M\big\{1,\, n_2,\, n_2^2,\, \ldots, n_2^{d-1}\big\} \pmod{N-1} \\ &\equiv M\mathcal{O}(1) \pmod{N-1}. \end{aligned} \tag{7.11}$$

These objects are in fact *cyclotomic cosets*, an important object in coding theory. We will explore this connection further in Section 7.2.

Setting $t = d$, we obtain the identity

$$M n_1^d \equiv M n_2^d \equiv M \pmod{N-1},$$

and with $\gcd(N-1, M) = \delta_M$, we have that

$$n_1^d \equiv n_2^d \equiv 1 \left(\bmod \frac{N-1}{\delta_M}\right). \tag{7.12}$$

By considering the equations in (7.11), we can write

$$n_1 n_2 M \equiv n_2(n_2^{d-1}M) \equiv n_2^d M \equiv M \pmod{N-1},$$

which can be reduced to

$$n_1 n_2 \equiv 1 \left(\bmod \frac{N-1}{\delta_M}\right).$$

Therefore n_1 and n_2 are multiplicative inverses modulo $\frac{N-1}{\delta_M}$, with d their *multiplicative order*.

Corollary 7.1.6. Assume (H1) and consider $M \in \{0, \ldots, N-2\}$. Then addresses of $M^{(t)}$ satisfies the following relations.

$$\sum_{j=0}^{d-t-1} n_1^j \alpha_1^{(t+j)} = \left\lfloor \frac{n_1^{d-t} M^{(0)}}{N-1} \right\rfloor,$$

$$\sum_{j=0}^{t-1} n_1^j \alpha_1^{(d-t+j)} = \left\lfloor \frac{n_1^t M^{(0)}}{N-1} \right\rfloor,$$

$$\sum_{j=0}^{t-1} \alpha_2^{(j)} n_2^{t-j-1} = \left\lfloor \frac{n_2^t M^{(0)}}{N-1} \right\rfloor.$$

Proof. This proof is identical to the proof of Corollary 7.1.3 except we consider the congruence relations in Remark 7.1.5 and compare them to Eq. (7.8), Eq. (7.9) and Eq. (7.10). □

Corollary 7.1.7. Assume (H1). Then the sum over the addresses of elements in a cyclic orbit obey the equality

$$(n_2 - 1)\sum_{t=0}^{d-1} \alpha_1^{(t)} = (n_1 - 1)\sum_{t=0}^{d-1} \alpha_2^{(t)}. \tag{7.13}$$

Furthermore, the sum over the elements in a cyclic orbit obey the equalities

$$(n_1 - 1)\sum_{t=0}^{d-1} M^{(t)} = (N-1)\sum_{t=0}^{d-1} \alpha_1^{(t)}, \quad \text{and} \quad (n_2 - 1)\sum_{t=0}^{d-1} M^{(t)} = (N-1)\sum_{t=0}^{d-1} \alpha_2^{(t)}. \tag{7.14}$$

Proof. The system of equations in (6.3) reduces to three equations, which when summed from t from 0 to $d-1$ gives us

$$\sum_{t=0}^{d-1} \alpha_1^{(t)} + n_1 \sum_{t=0}^{d-1} \alpha_2^{(t)} = n_2 \sum_{t=0}^{d-1} \beta_1^{(t)} + \sum_{t=0}^{d-1} \beta_2^{(t)},$$

$$\sum_{t=0}^{d-1} \alpha_1^{(t)} = \sum_{t=0}^{d-1} \beta_1^{(t)}, \quad \text{and} \quad \sum_{t=0}^{d-1} \alpha_2^{(t)} = \sum_{t=0}^{d-1} \beta_2^{(t)}.$$

Eq. (7.13) comes from substituting the summations with β terms in the first equation with the corresponding summations with α terms. Multiplying Eq. (7.13) by either n_1 or n_2 and rearranging yields Eq. (7.14). □

We can express Eq. (7.13) and Eq. (7.14) as the congruence relation

$$(n_1 - 1)\sum_{t=0}^{d-1} M^{(t)} \equiv (n_2 - 1)\sum_{t=0}^{d-1} M^{(t)} \equiv 0 \pmod{N-1}.$$

Letting $\gcd(N-1, n_\kappa - 1) = \delta$ for either $\kappa \in \{1,2\}$, we have the identity

$$\sum_{t=0}^{d-1} M^{(t)} \equiv 0 \left(\mathrm{mod}\ \frac{N-1}{\delta}\right).$$

Corollary 7.1.8. Assume (H1) and let $n_2 = sn_1 + r$, for $s \in \mathbb{N}$ and $r \in \langle n_1 \rangle$. Then consecutive terms in a cyclic orbit have the three term recurrence relation

$$sM^{(t)} + rM^{(t+1)} + (N-1)\big(s\alpha_1^{(t)} - \alpha_2^{(t+1)}\big) = M^{(t+2)},$$

which gives rise to the congruence relation

$$sM^{(t)} + rM^{(t+1)} \equiv M^{(t+2)} \pmod{N-1}.$$

Proof. Substituting Eq. (7.4) into $sM^{(t)} + rM^{(t+1)}$ and applying Eq. (7.5) leads to

$$\begin{aligned} s\Big(n_1 M^{(t+1)} - \alpha_1^{(t)}(N-1)\Big) + rM^{(t+1)} &= n_2 M^{(t+1)} - s\alpha_1^{(t)}(N-1) \\ &= M^{(t+2)} + (N-1)\Big(\alpha_2^{(t+1)} - s\alpha_1^{(t)}\Big), \end{aligned}$$

and by rearranging we deduce the desired result. □

Example 7.1.9. Let $n = (3,5)$, and consider the two joint ordered factorisations of n $\mathcal{J}_1 = \big((1,3),(2,5)\big)$ and $\mathcal{J}_2 = \big((2,5),(1,3)\big)$. We have $N = 15$, and thus we work modulo 14. The value $M = 0$ has the trivial cyclic orbit $\mathcal{O}(0) = \{0\}$. The first interesting case is when $M = 1$. From Eq. (7.7) we have

$$\begin{aligned} M^{(1)} &\equiv 5 \times 1 \equiv 5 \pmod{14}, \\ M^{(2)} &\equiv 5 \times 5 \equiv 11 \pmod{14}, \\ M^{(3)} &\equiv 5 \times 11 \equiv 13 \pmod{14}, \\ M^{(4)} &\equiv 5 \times 13 \equiv 9 \pmod{14}, \\ M^{(5)} &\equiv 5 \times 9 \equiv 3 \pmod{14}, \\ M^{(6)} &\equiv 5 \times 3 \equiv 1 \pmod{14}. \end{aligned}$$

Therefore we have

$$\mathcal{O}(1) = \big\{1, 5, 11, 13, 9, 3\big\} \equiv \big\{1, 5, 5^2, 5^3, 5^4, 5^5\big\} \pmod{14}. \tag{7.15}$$

Next we choose the next smallest integer not in the above orbit, which in this case is when $M = 2$. Again we apply Eq. (7.11) to obtain

$$\mathcal{O}(2) \equiv 2\mathcal{O}(1) \equiv \{2, 10, 22, 26, 18, 6\} \equiv \{2, 10, 8, 12, 4, 6\} \pmod{14}.$$

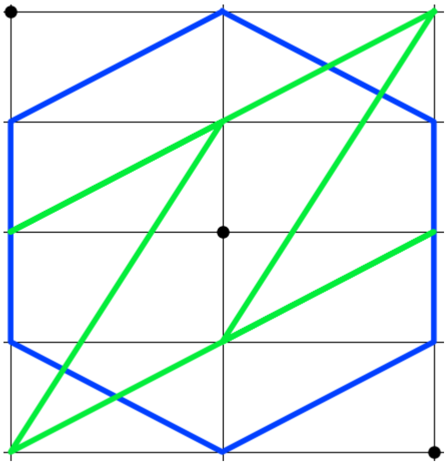
The next value to consider is $M = 7$, where we find that

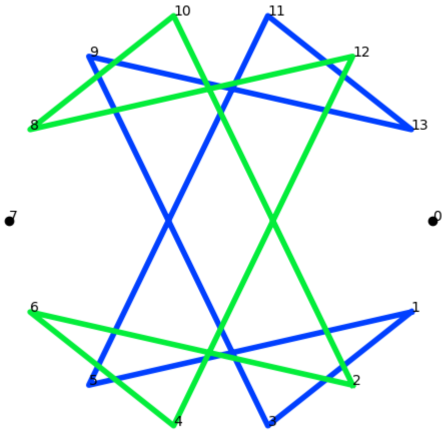
$$\mathcal{O}(7) \equiv \{7, 35, 77, 91, 63, 21\} \equiv \{7, 7, 7, 7, 7, 7\} \equiv \{7\} \pmod{14},$$

and thus 7 is a fixed point. The last value to consider is $M = 14$ which is also simply $\mathcal{O}(14) = \{14\}$. Putting these orbits together, we can write the full orbit permutation between $\mathcal{J}_1$ and $\mathcal{J}_2$ as

$$\sigma_{\mathcal{J}_1,\mathcal{J}_2} = (0)\,(1\ \ 5\ \ 11\ \ 13\ \ 9\ \ 3)\,(2\ \ 10\ \ 8\ \ 12\ \ 4\ \ 6)\,(7)\,(14).$$

Two geometric visualisations are depicted below





7.2 Cyclotomic cosets

Let $n = (n_1, n_2) \in \mathbb{N}_2^2$, with $N = n_1 n_2$, and consider the cyclic orbits between the two joint ordered factorisations $\mathcal{J}_1 = \big((1, n_1), (2, n_2)\big)$ and $\mathcal{J}_2 = \big((2, n_2), (1, n_1)\big)$. We concluded Remark 7.1.5 by stating that the cyclic orbit $\mathcal{O}(M)$, for $M \in \langle N \rangle$, were, when considered modulo $N-1$, equivalent to objects known as cyclotomic cosets. In this section we formally define these objects and discuss properties they hold that will translate to our cyclic orbits. They are often found in the literature of coding theory (see Section 7.2.3 for details), and are connected to a well known, and mysterious, counting function that links multiple fields of mathematics together, including Lie Algebras and Lyndon words.

7.2.1 Cyclotomic cosets and orbits

We begin by introducing the group structures that the cyclotomic cosets are apart of.

Definition 7.2.1. Let $\big(G, \cdot\big)$ be a group. For $g \in G$, let g^i denote i applications of the binary operation $\cdot$ on g. We call the subgroup generated by g, $\{g^0,\ g^1,\ \ldots,\ g^{d-1}\}$, a *cyclic subgroup* of G, with d the *order*. G is a *(finite) cyclic group* if it equals one of these cyclic subgroups.

Definition 7.2.2. For $n \in \mathbb{N}$, let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\} = \langle n\rangle$ denote the set of integers modulo n. The pair $\big(\mathbb{Z}_n, + \pmod{n}\big)$ forms a finite cyclic group.

Furthermore, let $\mathbb{Z}_n^* = \big\{a \in \langle n\rangle : \gcd(a, n) = 1\big\}$ denote the set of integers modulo n that are coprime to n. The pair $\big(\mathbb{Z}_n^*, \times \pmod{n}\big)$ is the group known as the *multiplicative group of integers modulo n*.

Remark 7.2.3. The triple $\big(\mathbb{Z}_n, + \pmod{n}, \times \pmod{n}\big)$ forms a ring, and $\mathbb{Z}_n^*$ is the group of units of this ring. Alternative notation for $\mathbb{Z}_n$ is $\mathbb{Z}/n\mathbb{Z}$, and alternative notation for $\mathbb{Z}_n^*$ is $\mathbb{U}(\mathbb{Z}_n)$ or $\big(\mathbb{Z}/n\mathbb{Z}\big)^*$.

The set $\mathbb{Z}_n^*$ is a fundamental object across many fields in mathematics, from abstract algebra to number theory. Two noteworthy properties this set has are $|\mathbb{Z}_n^*| = \varphi(n)$, with φ being Euler's totient function, and that $\mathbb{Z}_n^*$ is *cyclic* if n is $1, 2, 4, p^k$ or $2p^k$, where p is an odd prime and $k > 0$.

We will formally define the cyclotomic cosets with respect to the equivalence class of the following relation.

Lemma 7.2.4. Let $a, b, n, q \in \mathbb{N}$ such that $\gcd(n, q) = 1$ and d is the smallest integer such that $sq^d \equiv s \pmod{n}$. We say $a \sim b$ is true if $b \equiv aq^i \pmod{n}$ for some $i \in \langle d \rangle$. Then the binary operation $\sim$ is an equivalence relation.

Proof. Reflexivity: it is always true that $a \equiv aq^0 \pmod{n}$. Symmetric: as $b \equiv aq^i \pmod{n}$, we can multiply through by q^{d-i} to get $bq^{d-i} \equiv a \pmod{n}$ which implies $b \sim a$. Transitivity: if $a \sim b$ and $b \sim c$, then $c \equiv bq^{i_1} \equiv aq^{i_1+i_2} \pmod{n}$. If $i_1 + i_2 \geq d$ then we can write $i_1 + i_2 = d + i$ such that $c \equiv aq^d q^i \equiv aq^i \pmod{n}$. □

Definition 7.2.5. For $n, q \in \mathbb{N}$, such that $\gcd(n, q) = 1$, the *q-ary cyclotomic cosets modulo n* are the equivalence classes of $s \in \langle n \rangle$ with respect to $\sim$. These cosets take the form

$$\mathcal{C}(n, q, s) = [s] = \{s, sq, sq^2, \ldots, sq^{d-1}\} \pmod{n},$$

where d is the smallest integer such that $sq^d \equiv s \pmod{n}$ which we call the *order*.

The smallest entries of the cyclotomic cosets are call *coset representatives*. The set of all coset representatives for modulo n is called the *transversal*, denoted $\mathcal{T}$.

Lemma 7.2.6. The pair $\big(\mathcal{C}(n, q, s), \circ\big)$, with the binary operation $sq^i \circ sq^j \equiv sq^{i+j} \pmod{n}$ for $sq^i, sq^j \in \mathcal{C}(n, q, s)$ and $i + j \pmod{d}$ for $i, j \in \langle d \rangle$, forms a cyclic group.

Proof. Closure: because $sq^i \circ sq^j \equiv sq^{i+j} \pmod{n}$ then $sq^{i+j} \in \mathcal{C}(n, q, s)$ for $i + j < d$. Otherwise, we can write $i + j = d + k$ with $k \in \langle d \rangle$ such that $sq^{i+j} \equiv sq^d q^k \equiv sq^k \pmod{n}$ with $sq^k \in \mathcal{C}(n, q, s)$.

Associativity: this follows from

$$\big(sq^i \circ sq^j\big) \circ sq^k \equiv sq^{i+j} \circ sq^k \equiv sq^{i+j+k} \equiv sq^i \circ sq^{k+j} \equiv sq^i \circ \big(sq^j \circ sq^k\big) \pmod{n}.$$

Identity: the identity element is $sq^0 = s$, such that

$$sq^i \circ s \equiv sq^i \equiv s \circ sq^i \pmod{n}.$$

Inverse: the inverse of the element sq^i is sq^{d-i}, such that

$$sq^i \circ sq^{d-i} \equiv sq^d \equiv s \equiv sq^{d-i} \circ sq^i \pmod{n}.$$

Therefore we have shown $\big(\mathcal{C}(n,q,s),\circ\big)$ is a group. We can write $sq^i = \overbrace{sq\circ\cdots\circ sq}^{i\text{ times}}$. Then sq generates $\mathcal{C}(n,q,s)$, which is to say $\mathcal{C}(n,q,s)$ equals a cyclic subgroup, and thus is a cyclic group. □

Lemma 7.2.7. Let $n, q \in \mathbb{N}$, such that $\gcd(n,q) = 1$. For $s_1, s_2 \in \langle n\rangle$, if $t \in \mathcal{C}(n,q,s_1)$ and $t \in \mathcal{C}(n,q,s_2)$ then $s_1 \sim s_2$ modulo n.

Proof. If $t \in \mathcal{C}(n,q,s_1)$ and $t \in \mathcal{C}(n,q,s_2)$ then $t \equiv s_1q^i \equiv s_2q^j \pmod{n}$. Multiplying through by q^{d-j} gives us $s_2 \equiv s_1q^{d+i-j} \equiv s_1q^{i-j} \pmod{n}$ and this is $s_1 \sim s_2$ by definition. □

If $t \in \mathcal{C}(n,q,s_1)\cap\mathcal{C}(n,q,s_2)$, then we can write $t \equiv s_1q^i \equiv s_2q^j \pmod{n}$, which Lemma 7.2.7 implies

$$\begin{aligned}\mathcal{C}(n,q,s_2) &= \big\{s_2, s_2q, s_2q^2, \ldots, s_2q^{d-1}\big\}\\ &\equiv \big\{s_1q^{i-j}, s_1q^{i-j+1}, \ldots, \underbrace{s_1q^{i-j+d-1}}_{\equiv s_1q^{i-j-1}}\big\} = \pi^{i-j}\mathcal{C}(n,q,s_1),\end{aligned}$$

where π is the circular shift permutation (see notation table). Furthermore, if $r_1, r_2 \in \mathcal{T}$ with $r_1 \neq r_2$, then $\mathcal{C}(n,q,r_1)\cap\mathcal{C}(n,q,r_2) = \emptyset$.

Theorem 7.2.8. Let $n, q \in \mathbb{N}$, such that $\gcd(n,q) = 1$. Let $\mathcal{T}^* \subset \mathbb{Z}_n^*$ be the transversal of $\mathbb{Z}_n^*$. Then $\mathcal{C}(n,q,r)$ partitions $\mathbb{Z}_n^*$ and $\mathbb{Z}_n$, splitting the groups by

$$\mathbb{Z}_n^* = \bigcup_{r\in\mathcal{T}^*}\mathcal{C}(n,q,r),$$

and

$$\mathbb{Z}_n = \bigcup_{r\in\mathcal{T}}\mathcal{C}(n,q,r).$$

We set $\mathbb{Z}_1^* := \{0\}$ since $\gcd(1,0) = 1$.

Proof. As $\gcd(n,q) = 1$, then $q^i \pmod{n} \in \mathbb{Z}_n^*$ for $i \in \langle d\rangle$ with d the smallest integer such that $q^d \equiv 1 \pmod{n}$. This implies that $\mathcal{C}(n,q,1) \subset \mathbb{Z}_n^*$.

For $z \in \mathbb{Z}_n^*$, we can write $z \equiv q^i + x \pmod{n}$ for $i \in \langle d\rangle$, $0 < x < n$ and $\gcd(n, q^i + x) = 1$, i.e. z is some element in $\mathcal{C}(n,q,1)$ plus a constant x. We can write $x \equiv xq^d \pmod{n}$ which implies

$$z \equiv q^i + x \pmod{n} \equiv q^i + xq^d \equiv \big(1 + xq^{d-i}\big)q^i \pmod{n},$$

where $(1+xq^{d-i})q^i \in \mathcal{C}\big(n,q,1+xq^{d-i}\big)$. This implies all $z \in \mathbb{Z}_n^*$ can be written in the form of an element of some cyclotomic coset. Letting $\mathcal{T}^* = \{\min \mathcal{C}(n,q,z) \,:\, z \in \mathbb{Z}_n^*\}$ denote the transversal of $\mathbb{Z}_n^*$, then the cyclotomic cosets with representatives from the transversal partition $\mathbb{Z}_n^*$.

Consider the splitting

$$\mathbb{Z}_n = \bigcup_{e|n} \left(\tfrac{n}{e}\mathbb{Z}_e^*\right),$$

where $\frac{n}{e}\mathbb{Z}_e^* = \frac{n}{e}\{a \in \langle e\rangle : \gcd(a,e)=1\}$. We want to show that each number from 1 to $n-1$ occurs once within one of these sets, and thus the union across them all covers $\mathbb{Z}_n$.

Let $e \mid n$ with $e \neq 1$. If $a \in \mathbb{Z}_e^*$, then letting $x = \left(\frac{n}{e}\right)a$ we have

$$\gcd(x,n) = \gcd\left(\frac{n}{e}a, n\right) = \frac{n}{e}\gcd(a,e) = \frac{n}{e}.$$

Conversely, for $1 \le x \le n-1$ and $\gcd(x,n) = \frac{n}{e}$, then $x = \left(\frac{n}{e}\right)a$ such that $\gcd(a,e)=1$.

If $\gcd(x,n) = d$, then x will occur in the set corresponding to $e = \frac{n}{d}$, as the element corresponding to $a = \frac{x}{d}$. Therefore, you get each $1 \le x \le n-1$ exactly once. If $e=1$, then $\mathbb{Z}_1^* := \{0\}$ and we choose $x=0$. Altogether, we have accounted for all $x \in \{0,\ldots,n-1\} = \mathbb{Z}_n$. □

Lemma 7.2.9. Let $n, q \in \mathbb{N}$, such that $\gcd(n,q)=1$, and $s \in \langle n+1\rangle$. Then

$$\mathcal{C}(n,q,s) \equiv s\,\mathcal{C}\left(\frac{n}{\gcd(n,s)}, q, 1\right) \quad \left(\mathrm{mod}\ \frac{n}{\gcd(n,s)}\right),$$

and $\mathcal{C}(n,q,s) = s\,\mathcal{C}(n,q,1)$ if $\gcd(n,s)=1$.

Proof. If $\gcd(n,s)=1$ then

$$\mathcal{C}(n,q,s) = \left\{sq^0, sq^1, sq^2, \ldots, sq^{d-1}\right\} = s\left\{q^0,q^1,q^2,\ldots,q^{d-1}\right\} = s\,\mathcal{C}(n,q,1).$$

If $\gcd(n,s) = \delta > 1$ then

$$\begin{aligned}\mathcal{C}(n,q,s) &= \left\{sq^0, sq^1, sq^2, \ldots, sq^{d-1}\right\} \pmod{n}\\ &\equiv \left\{q^0,q^1,q^2,\ldots,q^{d_s-1}\right\} \pmod{\tfrac{n}{\delta}} = s\,\mathcal{C}(\tfrac{n}{\delta},q,1),\end{aligned}$$

where $d_s = \mathrm{ord}_{\frac{n}{\delta}}(q)$ such that $q^{d_s} \equiv 1 \pmod{\frac{n}{\delta}}$. □

Lemma 7.2.9 implies that the greatest common divisor across all elements in $\mathcal{C}(n, q, s)$ is $\gcd(n, s)$.

Lemma 7.2.10. Let $n, q \in \mathbb{N}$, such that $\gcd(n, q) = 1$, and let $\mathcal{T}^*$ be the transversal of $\mathbb{Z}_n^*$. Then, for $r_1, r_2 \in \mathcal{T}^*$ we have

$$\big|\mathcal{C}(n, q, r_1)\big| = \big|\mathcal{C}(n, q, r_2)\big| = \operatorname{ord}_n(q).$$

Proof. By definition $\gcd(n, r_1) = \gcd(n, r_2) = 1$. Then, using Lemma 7.2.9, we find that

$$\big|\mathcal{C}(n, q, r_1)\big| = \big|r_1\, \mathcal{C}(n, q, 1)\big| = \operatorname{ord}_n(q) = \big|r_2\, \mathcal{C}(n, q, 1)\big| = \big|\mathcal{C}(n, q, r_2)\big|,$$

as required. □

Remark 7.2.11. Lemma 7.2.10 implies that all integers $z \in \mathbb{Z}_n^*$ have the same order.

As we have now formally defined cyclotomic cosets, we are now in a position to return to cyclic orbits. Eq. (7.11) can now be written as

$$\begin{aligned}\mathcal{O}(M) \equiv& \big\{n_1^d M,\ n_1^{d-1} M,\ n_1^{d-2} M,\ \ldots, n_1 M\big\} \pmod{N-1} = \mathcal{C}(N-1, n_1, M)^{-1}\\ \equiv& \big\{M,\ n_2 M,\ n_2^2 M,\ \ldots, n_2^{d-1} M\big\} \pmod{N-1} = \mathcal{C}(N-1, n_2, M),\end{aligned}$$

where $\mathcal{C}(N-1, n_1, M)^{-1}$ is the reversed ordering of $\mathcal{C}(N-1, n_1, M)$.

Example 7.2.12. Let $\mathcal{J}_1 = \big((1, 3), (2, 4)\big)$ and $\mathcal{J}_2 = \big((2, 4), (1, 3)\big)$. Then the full orbit permutation between $\mathcal{J}_1$ and $\mathcal{J}_2$ is given by

$$\sigma_{\mathcal{J}_1, \mathcal{J}_2} = \big(0\big)\ \big(1\ \ 4\ \ 5\ \ 9\ \ 3\big)\ \big(2\ \ 8\ \ 10\ \ 7\ \ 6\big)\ \big(11\big).$$

Since $4^5 \equiv 3^5 \equiv 1 \pmod{11}$, we know the order of 3 and 4 modulo 11 is 5. Then we can write the cyclotomic cosets

$$\mathcal{C}(11, 4, 1) = \{4^0, 4^1, 4^2, 4^3, 4^4\} \equiv \{1, 4, 5, 9, 3\} \pmod{11} \equiv \mathcal{O}(1),$$

$$\mathcal{C}(11, 4, 2) = \{2 \times 4^0, 2 \times 4^1, 2 \times 4^2, 2 \times 4^3, 2 \times 4^4\} \equiv \{2, 8, 10, 7, 6\} \pmod{11} \equiv \mathcal{O}(2).$$

Note that since $\gcd(11, 4) = 1$, and $\gcd(11, 1) = \gcd(11, 2) = 1$, Lemma 7.2.9 implies $\mathcal{C}(11, 4, 2) = 2\mathcal{C}(11, 4, 1)$, which confirms equations (7.11).

Traditionally, cyclotomic cosets are restricted to considering finite fields of prime power order in the literature of coding theory. However, for $N = n_1n_2 \in \mathbb{N}$, we are working modulo $N-1$. Then the properties of cyclotomic cosets found in this section will translate to cyclic orbits between the two joint ordered factorisations $\big((1, n_1), (2, n_2)\big)$ and $\big((2, n_2), (1, n_1)\big)$. In particular, we have that $\mathcal{O}(M)$ forms a cyclic subgroup structure of $\mathbb{Z}^*_{N-1}$, and $\mathbb{Z}_{N-1}$ is partitioned by $\mathcal{O}(M)$ for $M \in \mathcal{T}$.

7.2.2 Enumeration of cyclic orbits

Let $n_1, n_2 \in \mathbb{N}_2$. We are now in a position to enumerate how many distinct cyclic orbits occur between the two joint ordered factorisations $\big((1, n_1), (2, n_2)\big)$ and $\big((2, n_2), (1, n_1)\big)$, which we denote $\Theta(n_1, n_2)$.

By this, letting $N = n_1n_2$, we mean how many $M \in \langle N\rangle = \{0, \dots, N-1\}$ correspond to cyclic orbits that shares no elements with any other cyclic orbits. Recall that the set

$$\mathcal{T} = \big\{ \min \mathcal{O}(M) : M \in \langle N\rangle \big\}$$

is the transversal of $\langle N\rangle$. Since, for $r_1, r_2 \in \mathcal{T}$, we have $\mathcal{O}(r_1) \cap \mathcal{O}(r_2) = \emptyset$, for $\emptyset$ the empty set, then we wish to calculate $\Theta(n_1, n_2) = |\mathcal{T}|$. Alternatively, we can state $\Theta(n_1, n_2)$ is the number of cyclic orbits in the full orbit permutation $\sigma_{\mathcal{J}_1,\mathcal{J}_2}$.

For $r \in \mathcal{T}$ we let $\delta_r = \gcd(N-1, r)$, we define $d_r > 0$ to be the smallest integer to satisfy

$$n_1^{d_r} \equiv n_2^{d_r} \equiv 1 \left(\bmod\ \frac{N-1}{\delta_r}\right).$$

Then, for $\kappa \in \{1, 2\}$, d_r is the *order* of n_κ modulo $\frac{N-1}{\delta_r}$, which we denote $d_r := \operatorname{ord}_{\frac{N-1}{\delta_r}}(n_\kappa)$. We set $d_0 := 1$. Eq. (7.12) implies that

$$d_r = \big|\mathcal{C}(n_1n_2 - 1, n_2, r)\big| = \big|\mathcal{C}(n_1n_2 - 1, n_1, r)^{-1}\big| = \big|\mathcal{O}(r)\big| = \operatorname{ord}_{\frac{N-1}{\delta_r}}(n_\kappa),$$

which means that d_r is the length of the cyclic orbit of r.

To continue, we will need the following lemma.

Lemma 7.2.13. Let $a, d, m \in \mathbb{N}$ with $\gcd(a, dm) = 1$. Let $g = \operatorname{ord}_{dm}(a)$ and $f = \operatorname{ord}_m(a)$. Then $f \mid g$.

Proof. We can write $a^g \equiv 1 \pmod{dm} = 1 + kdm \equiv 1 \pmod{m}$, for $k \in \mathbb{Z}$. Then it is well known that if $a^g \equiv 1 \pmod{m}$ then $f \mid g$. □

Theorem 7.2.14. Let $n = (n_1, n_2) \in \mathbb{N}_2$, $N = n_1 n_2$ and consider the two joint ordered factorisations $\mathcal{J}_1 = \big((1, n_1), (2, n_2)\big)$ and $\mathcal{J}_2 = \big((2, n_2), (1, n_1)\big)$. Let $\mathcal{T}$ be the transversal of $\langle N \rangle$. Then the length of all cyclic orbits must divide the cyclic orbit with the longest length, which occurs for $\big|\mathcal{O}(1)\big|$. That is, for all $r \in \mathcal{T}$, we have

$$\big|\mathcal{O}(r)\big| \;\Bigg|\; \big|\mathcal{O}(1)\big|.$$

Proof. Let $d_r = \big|\mathcal{O}(r)\big|$, for $r \in \mathcal{T}$. For $\kappa \in \{1, 2\}$, by Eq. (7.12) with $M = 1$ we know $n_\kappa^{d_1} \equiv 1 \pmod{N-1}$. For no $r \in \mathcal{T}$ can d_r be greater than d_1 since $N - 1 \geq \frac{N-1}{\delta_r}$, for $\delta_r = \gcd(N-1, r)$. We can write $n_\kappa^{d_1} \equiv 1 \pmod{\frac{N-1}{\delta_r}}$, which Lemma 7.2.13 then implies

$$\big|\mathcal{O}(r)\big| = d_r = \operatorname{ord}_{\frac{N-1}{\delta_r}}(n_\kappa) \;\Bigg|\; d_1 = \big|\mathcal{O}(1)\big|,$$

as required. □

Remark 7.2.15. There can be more than one orbit with length d_1. This occurs whenever $r \in \mathcal{T}$ satisfies $\gcd(N-1, r) = 1$. Furthermore, we have the chain of divisions

$$d_r \mid d_1 \mid \lambda(N-1) \mid \varphi(N-1),$$

where λ is Carmichael's function, and φ is Euler's totient function [10, pp.47]. This result implies that all cyclic orbit lengths divide a common divisor, namely the Carmichael's function, thus limiting what orbit lengths are possible.

Theorem 7.2.16. For $n_1, n_2 \in \mathbb{N}$, let $\Theta(n_1, n_2)$ enumerate the number of distinct cyclic orbits between the joint ordered factorisations $\mathcal{J}_1 = \big((1, n_1), (2, n_2)\big)$ and $\mathcal{J}_2 = \big((2, n_2), (1, n_1)\big)$. Then $\Theta(n_1, n_2)$ is given by

$$\Theta(n_1, n_2) = 1 + \sum_{k \mid (n_1 n_2 - 1)} \frac{\varphi(k)}{\operatorname{ord}_k(n_1)}, \tag{7.16}$$

where φ is Euler's totient function.

Remark 7.2.17. Since $\operatorname{ord}_k(n_1) = \operatorname{ord}_k(n_2)$ in these systems, we can replace n_1 in the fraction with n_2.

Proof. Let $N = n_1 n_2$, and let $\mathcal{T}$ be the transversal of $\mathbb{Z}_{N-1}$ (recall Definition 7.2.5). From Theorem 7.2.8, we can partition $\langle N \rangle$ into the union

$$\mathbb{Z}_{N-1} = \langle N \rangle = \bigcup_{k|(N-1)} \tfrac{N-1}{k}\mathbb{Z}_k^* = \bigcup_{r \in \mathcal{T}} \mathcal{C}(N-1, n_2, r) = \bigcup_{r \in \mathcal{T}} \mathcal{O}(r).$$

For $k \mid (N-1)$, let $\mathcal{T}^*$ be the transversal of $\mathbb{Z}_k^*$. Then we can partition $\mathbb{Z}_k^*$ into the union

$$\mathbb{Z}_k^* = \bigcup_{r \in \mathcal{T}_k^*} \mathcal{C}(N-1, n_2, r) = \bigcup_{r \in \mathcal{T}_k^*} \mathcal{O}(r).$$

Therefore, the number of cyclic orbits in the full orbit permutation $\sigma_{\mathcal{J}_1,\mathcal{J}_2}$ is equal to the size of its transversal, $|\mathcal{T}|$. Then we need to work out $|\mathcal{T}_k^*|$ such that $|\mathcal{T}| = \sum_{k|(n_1n_2-1)} |\mathcal{T}_k^*|$.

We know $|\mathbb{Z}_k^*| = \varphi(k)$. By Remark 7.2.11 we know that each $z \in \mathbb{Z}_k^*$ has the same order, and by Lemma 7.2.10 we know $|\mathcal{O}(r)| = \mathrm{ord}_k(n_1)$ for all $r \in \mathcal{T}_k^*$. Then we can split $\mathbb{Z}_k^*$ into $\frac{\varphi(k)}{\mathrm{ord}_k(n_1)}$ groupings of numbers, each corresponding to an orbit. Collecting the minimums of these groupings gives us $\mathcal{T}_k^*$. Therefore

$$|\mathcal{T}_k^*| = \frac{\varphi(k)}{\mathrm{ord}_k(n_1)}, \quad \text{and} \quad |\mathcal{T}| = \sum_{k|(n_1n_2-1)} \frac{\varphi(k)}{\mathrm{ord}_k(n_1)}.$$

All $M \in \{0, \dots, N-2\}$ are accounted for in one of the sets $\mathbb{Z}_k^*$, for $k \mid (N-1)$, except for the integer $N-1$, which has the cyclic orbit $\mathcal{O}(N-1) = \{N-1\}$, and thus we add 1 to complete our enumeration. □

Considering the enticingly natural look of Eq. (7.16), it would feel surprising if this enumeration function has not occurred in literature. However, after extensive searches, the author has to date not been able to locate such an article describing $\Theta(n_1, n_2)$.

Example 7.2.18. Let $n_1 = 5$, $n_2 = 8$, with $N = 5 \times 8 = 40$, and consider the joint ordered factorisations $\mathcal{J}_1 = \big((1,5),(2,8)\big)$ and $\mathcal{J}_2 = \big((2,8),(1,5)\big)$. The full orbit permutation between $\mathcal{J}_1$ and $\mathcal{J}_2$ is given by

$$\begin{aligned}\sigma_{\mathcal{J}_1,\mathcal{J}_2} =&(0)\ (1\ \ 8\ \ 25\ \ 5)\ (2\ \ 16\ \ 11\ \ 10)\ (3\ \ 24\ \ 36\ \ 15)\ (4\ \ 32\ \ 22\ \ 20)\ (6\ \ 9\ \ 33\ \ 30)\\ &(7\ \ 17\ \ 19\ \ 35)\ (12\ \ 18\ \ 27\ \ 21)\ (13\ \ 26)\ (14\ \ 34\ \ 38\ \ 31)\ (23\ \ 28\ \ 29\ \ 37)\ (39).\end{aligned}$$

By using Eq. (7.16), the number of cyclic orbits in $\sigma_{\mathcal{J}_1,\mathcal{J}_2}$ is

$$\begin{aligned}\Theta(5,8) = 1 + \sum_{k|39} \frac{\varphi(k)}{\mathrm{ord}_k(5)} &= 1 + \frac{\varphi(39)}{\mathrm{ord}_{39}(5)} + \frac{\varphi(13)}{\mathrm{ord}_{13}(5)} + \frac{\varphi(3)}{\mathrm{ord}_3(3)} + \frac{\varphi(1)}{\mathrm{ord}_1(1)}\\ &= 1 + \frac{24}{4} + \frac{12}{4} + \frac{2}{2} + \frac{1}{1} = 12,\end{aligned}$$

which we can count is true using $\sigma_{\mathcal{J}_1,\mathcal{J}_2}$.

Theorem 7.2.19. Let $n_1, n_2 \in \mathbb{N}$, and consider cyclic orbits between the two joint ordered factorisations $\mathcal{J}_1 = \big((1, n_1), (2, n_2)\big)$ and $\mathcal{J}_2 = \big((2, n_2), (1, n_1)\big)$. Let $d \mid \varphi(n_1 n_2 - 1)$, where φ is Euler's totient function, such that $\mathrm{ord}_{n_1 n_2 - 1}(n_1) = \mathrm{ord}_{n_1 n_2 - 1}(n_2) = d$. Then $\Theta(n_1, n_2)$, the number of distinct cyclic orbits between $\mathcal{J}_1$ and $\mathcal{J}_2$, is alternatively given by

$$\Theta(n_1, n_2) = 1 + \sum_{e \mid d} \frac{1}{e} \sum_{\substack{k \mid (n_1 n_2 - 1) \\ \mathrm{ord}_k(n_1) = e}} \varphi(k). \tag{7.17}$$

Proof. Let $N = n_1 n_2$. For $e \mid d$ and $k_1, k_2 \mid (N-1)$ such that $\mathrm{ord}_{k_1}(n_1) = \mathrm{ord}_{k_2}(n_1) = e$, we can split all divisors of $N - 1$ into the sets $E(e) := \big\{k \mid (N-1) : \mathrm{ord}_k(n_1) = e\big\}$. Then

$$\sum_{k \mid (N-1)} \frac{\varphi(k)}{\mathrm{ord}_k(n_1)} = \sum_{e \mid d} \sum_{k \in E(e)} \frac{\varphi(k)}{\mathrm{ord}_k(n_1)} = \sum_{e \mid d} \frac{1}{e} \sum_{k \in E(e)} \varphi(k) = \sum_{e \mid d} \frac{1}{e} \sum_{\substack{k \mid (n_1 n_2 - 1) \\ \mathrm{ord}_k(n_1) = e}} \varphi(k).$$

Adding 1 yields the desired result. □

Corollary 7.2.20. For $n_1, n_2 \in \mathbb{N}$, the enumeration Θ has the symmetric property

$$\Theta(n_1, n_2) = \Theta(n_2, n_1).$$

Proof. Because $\mathrm{ord}_k(n_1) = \mathrm{ord}_k(n_2)$ for $k \mid (n_1 n_2 - 1)$, then

$$\Theta(n_1, n_2) = 1 + \sum_{k \mid (n_1 n_2 - 1)} \frac{\varphi(k)}{\mathrm{ord}_k(n_1)} = 1 + \sum_{k \mid (n_1 n_2 - 1)} \frac{\varphi(k)}{\mathrm{ord}_k(n_2)} = \Theta(n_2, n_1),$$

as required. □

7.2.3 Coding theory

Coding theory is an expansive field which concerns the study of *codes*; strings of symbols that represent a message. Claude Shannon generated the interest in studying codes in 1948, [25], with Richard Hamming pioneering the field of *error-correcting codes* by considering the objects *Hamming codes* in 1950, [36].

Hamming codes allowed algorithms to detect and correct one or two errors. Blahut, [5, Theorem 5.5.1], proved these codes were equivalent to *cyclic codes* - a particularly useful type of code due to their ease of implantation and connections to a wide range of important codes.

A code is cyclic if the circular shift permutation (see notation table) of that code remains a code. By restricting elements of our code to symbols over a finite field of order p^m, for p prime, also known as a Galois field $GF(p^m)$, these cyclic codes can be expressed as polynomials modulo $x^{p^m-1}-1$.

Using Fermat's little theorem [5, Corollary 4.6.5] [4, pp. 102, 156] [58, pp. 96, Corollary 3, pp. 99], and considering monic polynomials $M(x)$ with various properties [5, pp. 105] [58, pp. 105, Property M7], we can factorise the polynomial

$$x^{p^m-1}-1=\prod_{r\in\mathcal{T}} M(x),$$

where $\mathcal{T}$ is the transversal of $\{1,\ldots,p^m-1\}$. For $g\in GD(p^m)$, the polynomials $M(x)$, known as minimal polynomials, are irreducible over a given polynomial field, and have the closed form

$$M(x)=\prod_{i\in\mathcal{C}}(x-g^i),$$

where $\mathcal{C}\subset\{0,\ldots,p^m-1\}$.

These sets $\mathcal{C}$ are *cyclotomic cosets* [58, pp.104], [70, pp.13], [32, pp.413]. In literature, these sets are also referred to as the *sets of conjugates* [5, pp.108] [4, pp.101], or q-ary conjugates [6, pp.35]. These sets are also referred to as *Galois Orbits* [6, pp.35], which appears to be generalisations of the above argument for minimal polynomials over finite fields, and is linked to *resolvents* in Galois Theory. This is not to be confused with *conjugate classes*, which are equivalence classes, also known as *orbits*, of a group acting on itself [23, pp.123] [41, pp.89].

Though restricted to powers of primes, this is the natural occurrence for cyclotomic cosets in applications. They are important tools when partitioning these finite fields and factorising minimal polynomials over them, and are considered alongside many type of codes.

7.2.4 Necklace polynomials

For $n, k \in \mathbb{N}$, consider the polynomial

$$M(k,n) = \frac{1}{n}\sum_{d|n} \mu\Big(\frac{n}{d}\Big)k^d,$$

where μ is the Möbius function. This function is known as the *necklace polynomial* and satisfies

$$k^n = \sum_{d|n} d\, M(k,d).$$

Furthermore, the *general necklace polynomial* (or *general necklace-counting function*) is defined as

$$N(k,n) = \sum_{d|n} M(k,d) = \frac{1}{n}\sum_{d|n} \varphi\Big(\frac{n}{d}\Big)k^d, \tag{7.18}$$

where φ is Euler's totient function.

Famously, these polynomials connect seemingly disconnected areas of mathematics, with $N(k,n)$ enumerating various characteristics of interest across the fields. Here are some examples.

A cyclically ordered set of n beads, chosen from k colours, is called a *k-ary necklace of length n*. A necklace which is asymmetric under rotation is *aperiodic* (also known as *primitive* [60]). An aperiodic necklace is also an equivalence class of circular shifts on a necklace. Then $M(k,n)$ counts the number of k-ary aperiodic necklaces of length n, and $N(k,n)$ counts the total number of necklaces of length n with k colours, and hence their namesake. Both Lucas [54] and Metropolis and Rota [60] attribute $N(k,n)$ to the French colonel Moreau, who proved the result in 1872 [63].

A k-ary Lyndon word of length n is an n-character string over an alphabet of size k that is strictly smaller in lexicographic order than all of its rotations. There is a bijection between aperiodic necklaces and Lyndon words, and therefore the number of Lyndon words of length n formed from k letters is $M(k,n)$. MacMahon stated this result in 1892, [56] and $N(k,n)$ is named after him in [30].

Witt [88] showed that $M(k,n)$ is the dimension of the degree n homogeneous component of the free Lie algebra on k generators. In [55], $N(k,n)$ is called Witt's formula.

Furthermore, $M(k,n)$ appears as an exponent in the *cyclotomic identity*

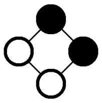
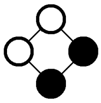
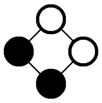
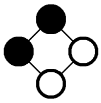
$$\frac{1}{1-kz} = \prod_{j=1}^{\infty} \left(\frac{1}{1-z^j} \right)^{M(k,j)},$$

credited to be proven by Metropolis and Rota [61] and a specific case for $k = p^t$, p prime, in [4, Theorem 3.32, pp. 78].

Finally, if $k = p$ is a prime, then $M(p,t)$ is the number of irreducible minimal monic polynomials of degree t over the a finite field with p^t elements that divides $x^{p^t-1} - 1$, and $N(p,t)$ is the number of powers of these polynomials. As we saw in the previous subsection, these polynomials also correspond to p-ary cyclotomic cosets [58, Theorem 15] and are enumerated by $N(p,t)$. This has been attributed to Gauss [29] and called Gauss' Formula by Jacobson [44].

The far reaching influences of $M(k,n)$ and $N(k,n)$ is evident alone by the fact they are named after four noteworthy individuals. The underlying connections between these counted fields is still considered a bit of a mystery, though insight into why they are all enumerated by the same function has surfaced over time.

In his thesis [70, Example 2.5.3] Rebenich provides an excellent illustration for how the aperiodic necklaces and cyclotomic cosets are connected. If we write the elements of the cyclotomic cosets modulo p^t as t-digit string in base p, they have a one-to-one correspondence to the aperiodic p-ary necklaces of length t. The cyclotomic cosets are thus the equivalence classes of circular shifts of distinct ways to write a necklace, and enumerated by $N(p,t)$.

Example 7.2.21. Consider the necklace  consisting of 2 white beads and 2 black beads, with length 4. Assign the white beads the value 0 and black beads the value 1. Starting at the top and going clockwise, this necklace can be written as the string 1100. By rotating the necklace 90 degrees we obtain , which can be written as the string 0110. Note that 0110 is the circular shift of 1100. Rotating twice more, we obtain the necklaces  and , with stings 0011 and 1001.

Then each string is the circular shift on the digits of a previous string. Collating these strings, and considering the equivalence relation based on circular shifts, the collection of these strings form an equivalence class on the necklace written as 0011, i.e. $[0011] = \{0011, 0110, 1100, 1001\}$. Since we have two colours of beads, this implies these strings are numbers in base 2, which we can convert into base 10. Then 0011=3, 0110=6, 1100=12 and 1001=9, such that $[0011] = \{3, 6, 12, 9\}$.

Now, consider the 2-ary cyclotomic coset modulo 15 of 3, given by

$$\mathcal{C}(15, 2, 3) \equiv \big\{3,\ 3 \times 2,\ 3 \times 2^2,\ 3 \times 2^3\big\} \equiv \big\{3, 6, 12, 9\big\} \pmod{15}.$$

Then we see $\mathcal{C}(15, 2, 3) = [0011]$, and thus we see the link between these objects.

In total, let $q = 2$, and $t = 4$. The transversal of $\langle 2^4 \rangle$ is $\mathcal{T} = \{0, 1, 3, 5, 7, 15\}$. For $r \in \mathcal{T}$, the cyclotomic coset $\mathcal{C}(15, 2, r)$, alongside their 4-digit string in base 2, are

$r \in \mathcal{T}$	$\mathcal{C}(15, 2, r)$	base 2
0	$\{0\}$	$\{0000\}$
1	$\{1, 2, 4, 8\}$	$\{0001, 0010, 0100, 1000\}$
3	$\{3, 6, 12, 9\}$	$\{0011, 0110, 1100, 1001\}$
5	$\{5, 10\}$	$\{0101, 1010\}$
7	$\{7, 14, 13, 11\}$	$\{0111, 1110, 1101, 1011\}$
15	$\{15\}$	$\{1111\}$

This table accounts for all possible ways to write equivalence classes for necklaces with 4 beads and 2 colours. Hence the cyclotomic cosets $\mathcal{C}(15, 2, r)$ correspond to these necklaces. Then we can use the general necklace polynomial to enumerate how many sets there are, which we get

$$N(2, 4) = \frac{1}{4}\sum_{d|4} \varphi\Big(\frac{4}{d}\Big)2^d = \frac{1}{4}\big(\varphi(4)2^1 + \varphi(2)2^2 + \varphi(1)2^4\big) = \frac{1}{4}\big(2 \times 2 + 4 + 16\big) = 6,$$

and indeed there are 6 such sets considered.

Because the general necklace polynomials counts cyclotomic cosets, then it also counts distinct cyclic orbits between two joint ordered factorisations. Therefore, we may add these cyclic orbits to the long list of characteristics that the general necklace polynomials count, though with less mystery due to the clear nature of their connection to cyclotomic cosets.

Interestingly, we already have an enumeration function for these distinct cyclic orbits, and thus the general necklace polynomials and our counting function must be equal for certain values. In the following section, we will formally state and prove this connection.

7.3 Integer powers and necklace polynomials

Let $n, u \in \mathbb{N}$ with $v \in \langle u \rangle$, and consider the cyclic orbits between $\mathscr{J}_1 = \big((1, n^{u-v}), (2, n^v)\big)$ and $\mathscr{J}_2 = \big((2, n^v), (1, n^{u-v})\big)$.

Since, for $M \in \langle n^u \rangle$, we can write $\mathcal{O}(M) = \mathcal{C}(n^u - 1, n^{u-v}, M)$, The general necklace polynomial $N(n, u)$ enumerates these cyclotomic cosets, and thus enumerates the cyclic orbits $\mathcal{O}(M)$. Then Eq. (7.18) enumerates the number of distinct cyclic orbits between $\mathscr{J}_1$ and $\mathscr{J}_2$. To prove this, we require the following Lemma.

Lemma 7.3.1. Let $n, u \in \mathbb{N}$, $v \in \langle u \rangle$ with $s = \gcd(u, v)$, and consider the two couples of joint ordered factorisations $\mathscr{J}_1 = \big((1, n^{u-v}), (2, n^v)\big)$ with $\mathscr{J}_2 = \big((2, n^v), (1, n^{u-v})\big)$, and $\mathscr{J}_3 = \big((1, n^{u-s}), (2, n^s)\big)$ with $\mathscr{J}_4 = \big((2, n^s), (1, n^{u-s})\big)$. Then $\Theta\big(n^{u-v}, n^v\big)$, the number of distinct cyclic orbits between $\mathscr{J}_1$ and $\mathscr{J}_2$, equals $\Theta\big(n^s, n^{u-s}\big)$, the number of distinct cyclic orbits between $\mathscr{J}_3$ and $\mathscr{J}_4$, i.e.

$$\Theta\big(n^{u-v}, n^v\big) = \Theta\big(n^s, n^{u-s}\big).$$

Proof. Proposition 5, page 57, of [23] provides the expression

$$\mathrm{ord}_N(a^k) = \frac{\mathrm{ord}_N(a)}{\gcd(\mathrm{ord}_N(a), k)}.$$

Let $\eta = n^s$, $e \mid \frac{u}{s}$, and $k \mid (n^u - 1)$ such that $\mathrm{ord}_k(\eta) = e$. We can write $\frac{u}{s} = ex$, such that

$$\gcd\big(\mathrm{ord}_k(\eta), \tfrac{u-t}{s}\big) = \gcd(e, \tfrac{u-v}{s}) = \gcd(e, ex - \tfrac{v}{s}) = \gcd(e, \tfrac{v}{s}) = 1.$$

Then we have

$$\mathrm{ord}_k\Big(\eta^{\frac{u-v}{s}}\Big) = \frac{\mathrm{ord}_k(\eta)}{\gcd\Big(\mathrm{ord}_k(\eta), \frac{u-v}{s}\Big)} = \mathrm{ord}_k(\eta) = e,$$

which enables us to write

$$\begin{aligned}\Theta\bigl(n^{u-v}, n^{v}\bigr) = \Theta\Bigl(\eta^{\frac{u-v}{s}}, \eta^{\frac{v}{s}}\Bigr) &= 1 + \sum_{k|(n^u-1)} \frac{\varphi(k)}{\operatorname{ord}_k(\eta^{\frac{u-v}{s}})} \\ &= 1 + \sum_{k|(n^u-1)} \frac{\varphi(k)}{\operatorname{ord}_k(\eta)} = \Theta\Bigl(\eta, \frac{n^u}{\eta}\Bigr) = \Theta\Bigl(n^s, n^{u-s}\Bigr),\end{aligned}$$

as required. □

This implies, for $v_1, v_2 \in \langle u \rangle$ and $s = \gcd(u, v_1, v_2) = 1$, that $\mathcal{J}_1 = \bigl((1, n^{u-v_1}), (2, n^{v_1})\bigr)$ with $\mathcal{J}_2 = \bigl((2, n^{v_1}), (1, n^{u-v_1})\bigr)$, and $\mathcal{J}_3 = \bigl((1, n^{u-v_2}), (2, n^{v_2})\bigr)$ with $\mathcal{J}_4 = \bigl((2, n^{v_2}), (1, n^{u-v_2})\bigr)$ have the same number of cyclic orbits between them.

Theorem 7.3.2. Let $n, u \in \mathbb{N}$, with $v \in \langle u \rangle$ and consider the cyclic orbits between the joint ordered factorisations $\mathcal{J}_1 = \bigl((1, n^{u-v}), (2, n^{v})\bigr)$ and $\mathcal{J}_2 = \bigl((2, n^{v}), (1, n^{u-v})\bigr)$. Let $s = \gcd(u, v)$. Then $\Theta\bigl(n^{u-v}, n^{v}\bigr)$, the number of distinct cyclic orbits between $\mathcal{J}_1$ and $\mathcal{J}_2$, and the general necklace polynomial given in Eq. (7.18) relate by the equality

$$\Theta\bigl(n^{u-v}, n^{v}\bigr) = N\bigl(n^s, \tfrac{u}{s}\bigr) = \frac{s}{u} \sum_{e|\frac{u}{s}} \varphi\biggl(\frac{u}{es}\biggr) n^{es},$$

where φ is Euler's totient function.

Proof. Set $\eta = n^s$. Using Eq. (7.18) we can write

$$N\bigl(\eta, \tfrac{u}{s}\bigr) = \sum_{e|\frac{u}{s}} M\bigl(\eta, e\bigr) = \sum_{e|\frac{u}{s}} \frac{1}{e} \sum_{g|e} \mu\biggl(\frac{e}{g}\biggr) \eta^{g}.$$

By Lemma 7.3.1 we can write $\Theta\bigl(n^{u-v}, n^{v}\bigr) = \Theta\bigl(\eta, \eta^{\frac{u}{s}-1}\bigr)$. Using Eq. (7.17), with the set $E(e) = \{k|(\eta^{\frac{u}{s}} - 1) : \operatorname{ord}_k(\eta) = e\}$ we have

$$\Theta\bigl(\eta, \eta^{\frac{u}{s}}\bigr) = 1 + \sum_{e|\frac{u}{s}} \frac{1}{e} \sum_{k \in E(e)} \varphi(k).$$

If $k|(\eta^{\frac{u}{s}} - 1)$ and $\operatorname{ord}_k(\eta) = e$, then $\eta^e \equiv 1 \pmod{k}$ which implies $k|(\eta^e - 1)$. But if $k|(\eta^g - 1)$ for $g|e$, then $\eta^g \equiv 1 \pmod{k}$ which implies $\operatorname{ord}_k(\eta) = g \neq e$ unless $g = e$. Then we can express the set

$$E(e) = \bigl\{k|(\eta^{\frac{u}{s}} - 1) : \operatorname{ord}_k(\eta) = e\bigr\} = \bigl\{k|(\eta^{e} - 1) : \operatorname{ord}_k(\eta) = e\bigr\},$$

and for $g \mid e$ we can write

$$E(g) = \big\{k|(\eta^e - 1) : \mathrm{ord}_k(\eta) = g\big\}.$$

To find $\sum_{k\in E(e)} \varphi(k)$, we will apply the Möbius inversion formula to the following expression

$$\begin{aligned}\sum_{g|e}\sum_{k\in E(g)} \varphi(k) &= \sum_{g|e}\sum_{\substack{k|(\eta^e-1)\\ \mathrm{ord}_k(\eta)=g}} \varphi(k)\\ &= \sum_{g|e}\sum_{k|(\eta^e-1)} \varphi(k)\delta_{\mathrm{ord}_k(\eta),g}\\ &= \sum_{k|(\eta^e-1)}\Bigg(\varphi(k)\sum_{g|e}\delta_{\mathrm{ord}_k(\eta),g}\Bigg)\\ &= \sum_{k|(\eta^e-1)} \varphi(k) = \eta^e - 1,\end{aligned}$$

since for $k \mid (\eta^e - 1)$ has $\mathrm{ord}_k(\eta) = e$ and thus $\delta_{e,g} = 1$ only when $g = e$, and we use the identity $\sum_{d|n}\varphi(d) = n$ in the final line. Taking the Möbius inversion of the above expression, along with the identity $\sum\limits_{k|e}\mu\big(\frac{e}{k}\big) = \delta_{e,1}$ [3, Theorem 2.1, pp 25], we have

$$\sum_{k\in E(e)}\varphi(k) = \sum_{g|e}\mu\left(\frac{e}{g}\right)(\eta^g - 1) = \sum_{g|e}\mu\left(\frac{e}{g}\right)\eta^g - \sum_{g|e}\mu\left(\frac{e}{g}\right) = \sum_{g|e}\mu\left(\frac{e}{g}\right)\eta^g - \delta_{e,1}.$$

Now we can substitute this expression back into $\Theta\big(\eta, \eta^{\frac{u}{s}}\big)$ to find

$$\begin{aligned}\Theta\big(\eta, \eta^{\frac{u}{s}}\big) &= 1 + \sum_{e|\frac{u}{s}}\frac{1}{e}\sum_{k\in E(e)}\varphi(k) = 1 + \sum_{e|\frac{u}{s}}\frac{1}{e}\Bigg(\sum_{g|e}\mu\left(\frac{e}{g}\right)\eta^g - \delta_{e,1}\Bigg)\\ &= 1 + \sum_{e|\frac{u}{s}}\frac{1}{e}\sum_{g|e}\mu\left(\frac{e}{g}\right)\eta^g - \sum_{e|\frac{u}{s}}\frac{1}{e}\delta_{e,1} = \sum_{e|\frac{u}{s}}\frac{1}{e}\sum_{g|e}\mu\left(\frac{e}{g}\right)\eta^g = N(\eta, \tfrac{u}{s}),\end{aligned}$$

as required. □

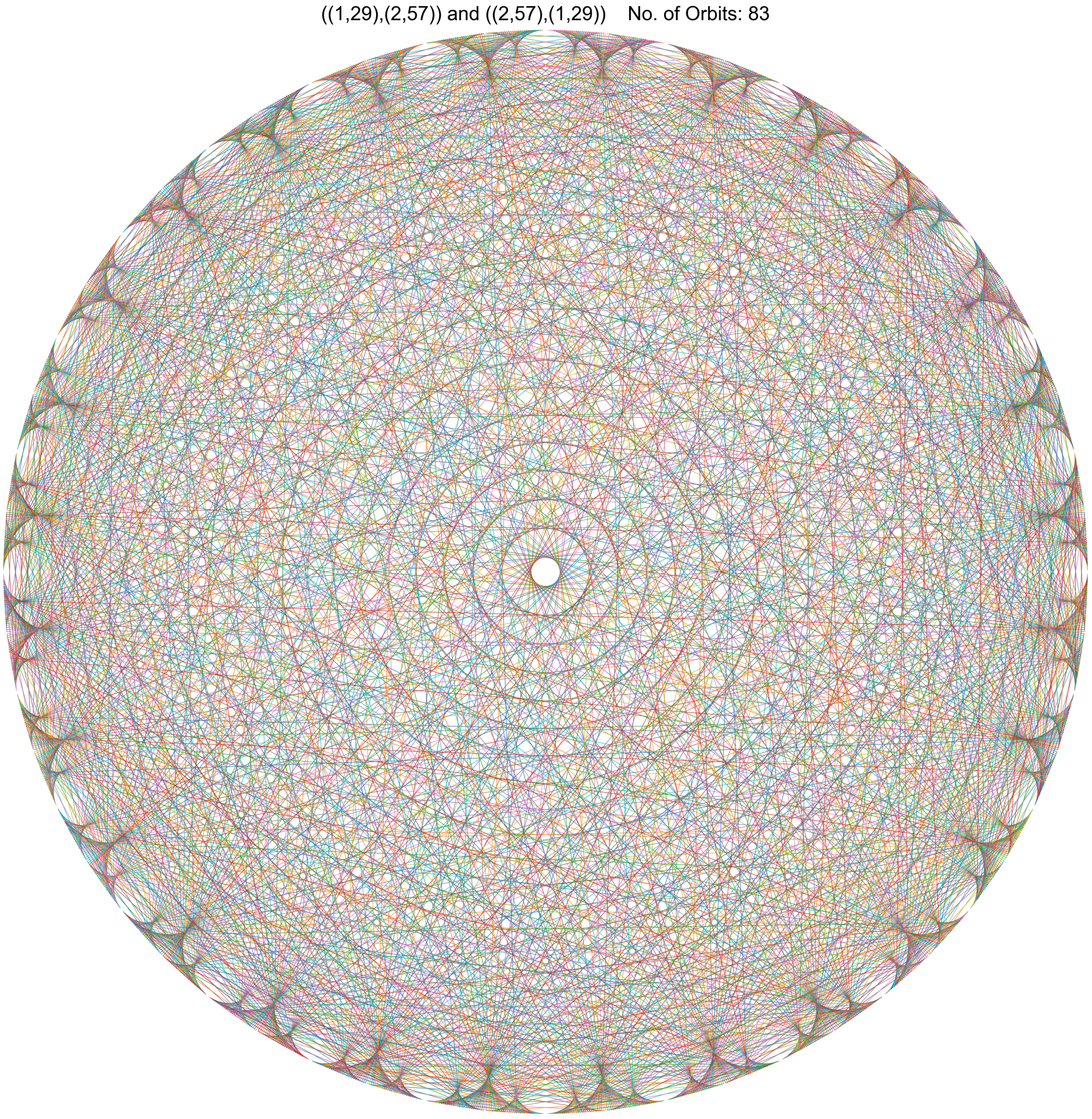
If $s = \gcd(u, v) = 1$ then $\Theta(n^{u-v}, n^v)$ can be simplified to

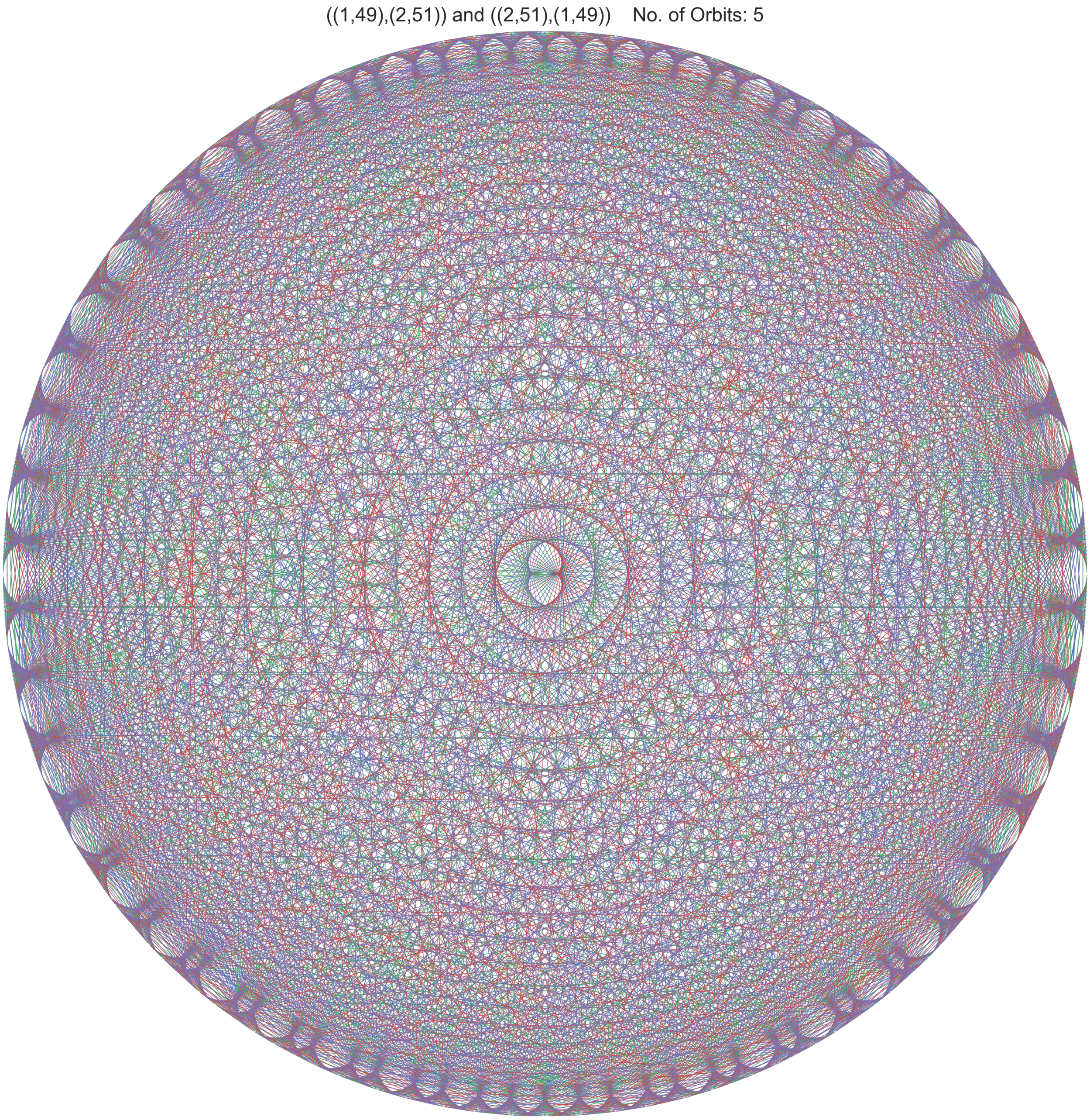
$$\Theta(n^{u-v}, n^v) = N(n, u) = \frac{1}{u}\sum_{e|u}\varphi\left(\frac{u}{e}\right)n^e.$$

7.4 Cyclic orbit examples

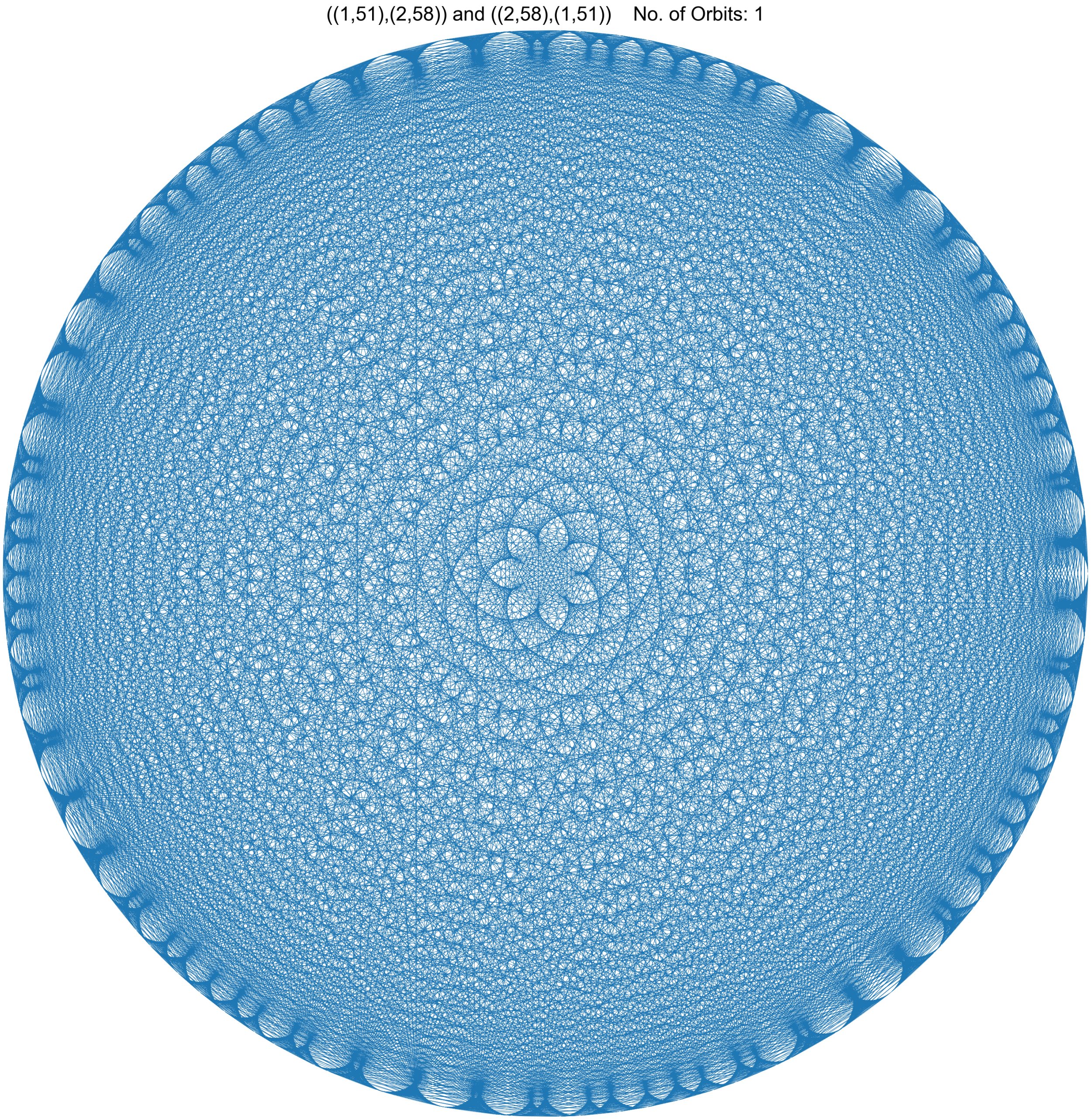
So far, we have used relatively small numbers for our examples of cyclic orbits. The cyclic orbit between $\big((1,n_1),(2,n_2)\big)$ and $\big((2,n_2),(1,n_1)\big)$ will require n_1n_2-1 terms in total. Once this value is larger than 50, the numbers becomes cumbersome.

However, at such low values the full display of the ring geometry's structure and symmetry are lost. We provided a few examples of these ring geometries without listing all the cyclic orbits. We note that the number of Orbits measure used does not include the orbit of 0 or n_1n_2-1 (so we add 2 to retrieve $\Theta(n_1,n_2)$).

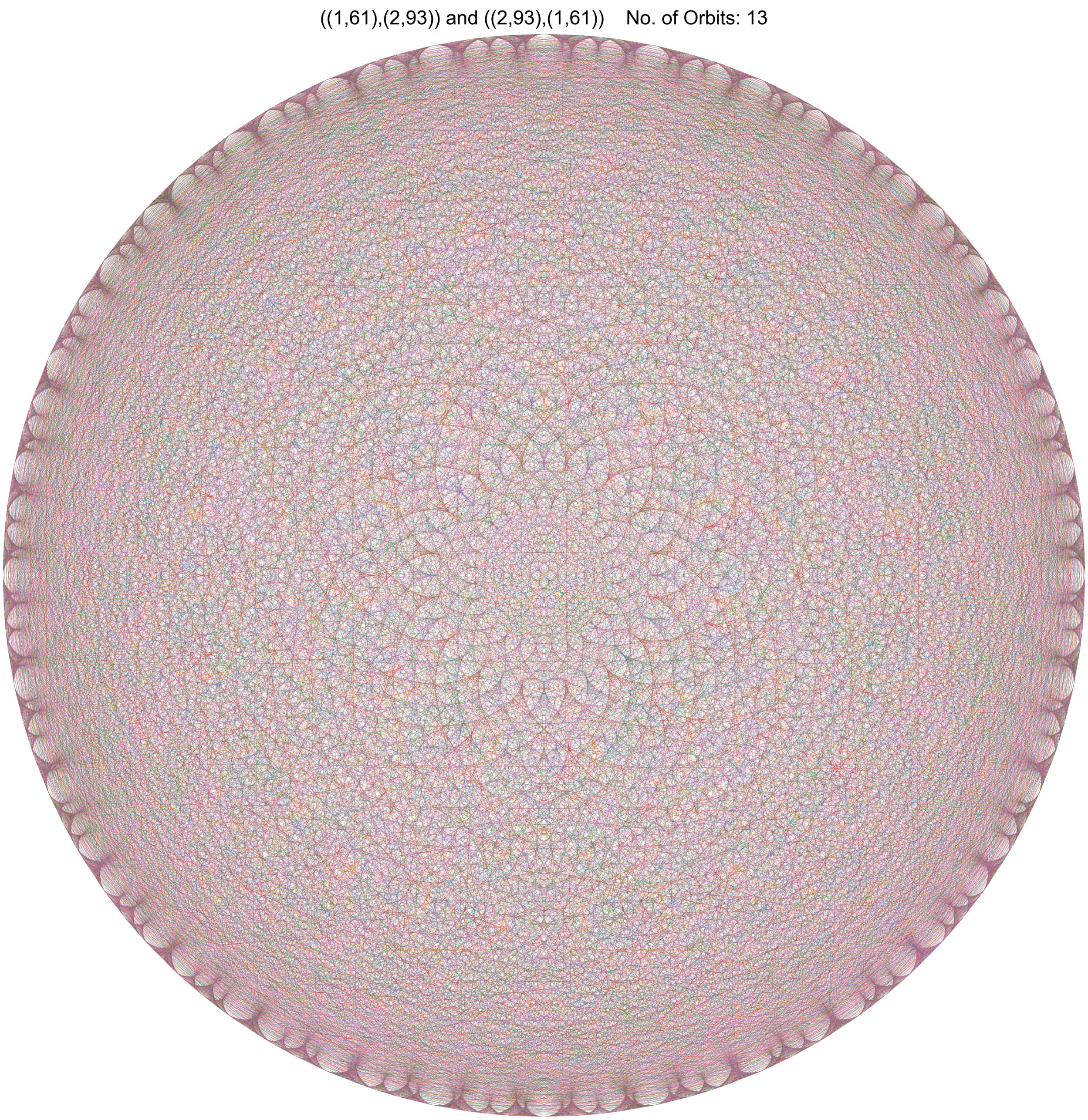




The above geometric construction employs straight lines, and so any curved line patterns are the result of overlapping these straight lines. In this case, there are 5 distinct cyclic orbits that, when overlapped, produces the above image. Each cyclic orbit has a different colour. The transversal is $\mathcal{T} = \{1, 2, 7, 14, 1249\}$ with 1249 a fixed point.

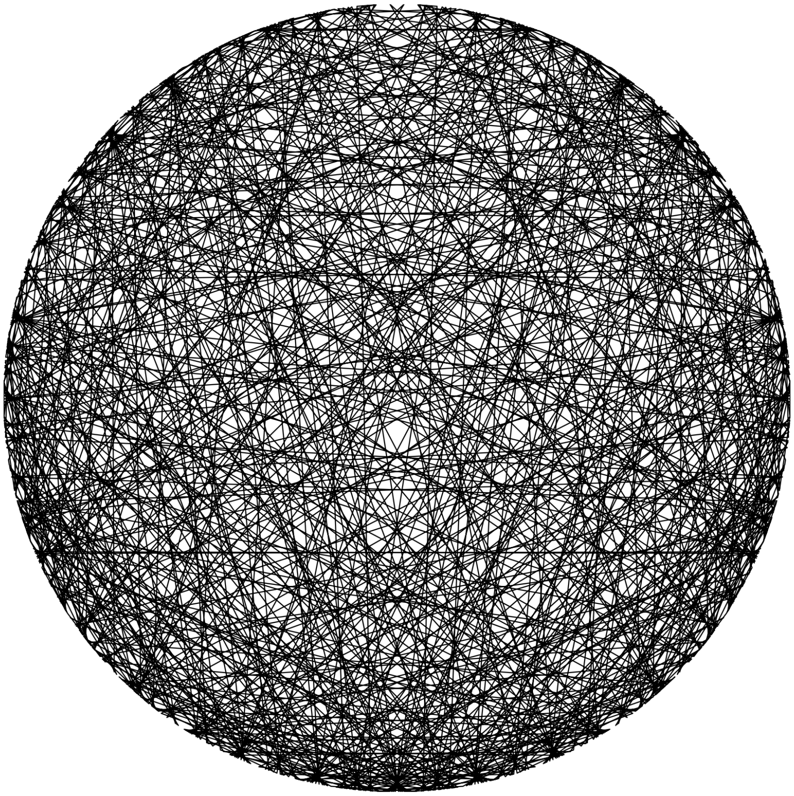


In this case, there is only one cyclic orbit, that of 1, which visits every integer between 1 and 2956.

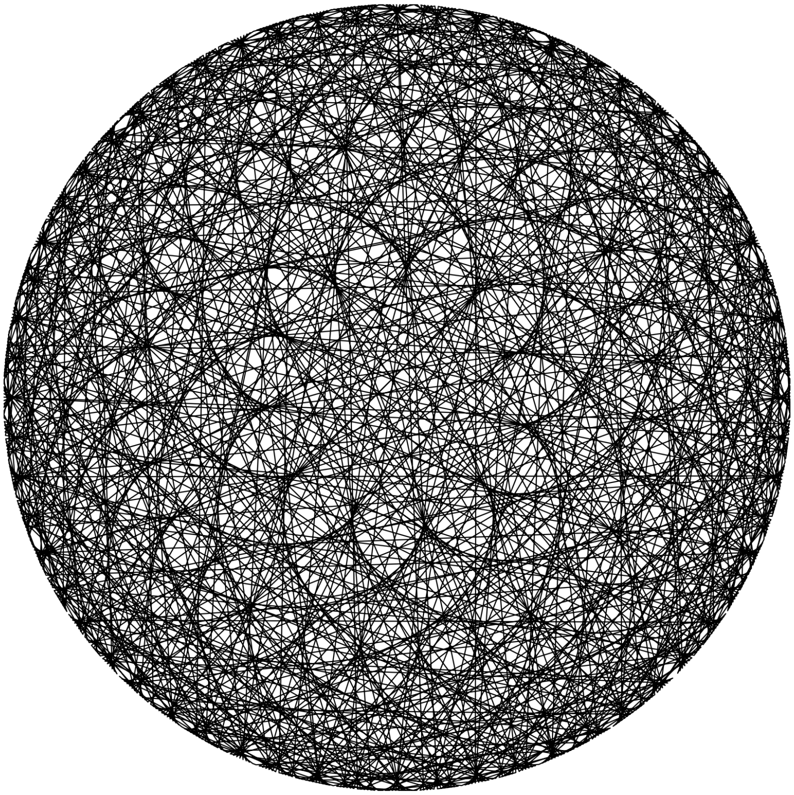


The above image is the composition of the following two cyclic orbits rotated four times by 90 degrees, as well as two cyclic orbits with only two elements (i.e. a straight line), and 3 fixed points. The four numbers that the rotations of the first image are cyclic orbits of are 1, 3, 5, 7. The four numbers that the rotations of the second image are cyclic orbits of are 2, 4, 6, 8. The two straight lines are the cyclic orbits of 709 and 2127. The three fixed points are 1418, 2836 and 4254.

((1,61),(2,93)) and ((2,93),(1,61))   Cyclic Orbit of 1



((1,61),(2,93)) and ((2,93),(1,61))   Cyclic Orbit of 2



7.5 Conclusion

In Chapter 6 we formulated the framework of notation needed to describe orbits between two joint ordered factorisations, and concluding by stating that a full description required an explicit form for the two factorisations.

When we focus on the orbits between two joint ordered factorisations written in their simplest forms (two-dimensional with only two pairs in each expressions), we found that these systems were completely described by concise operations and expressions. Their structures were compact enough to formulate multiple identities and properties that the orbits satisfied, providing insight into the structure of these simplest case.

Additionally, the emergent structures of these orbits turned out to be objects known as cyclotomic cosets. These cosets are naturally found in the literature of coding theory and are cyclic groups, which connects orbits to both these fields.

This in turn also established the link between orbits and a well known counting function; general necklace polynomials. This enumeration function is often regarded as quite mysterious due to the fact it counts a wide selection of properties that appear to have little to do with each other, from minimal polynomials and Lyndon words, to Lie algebras and necklaces. To this exclusive list we can now include the number of orbits between two certain joint ordered factorisations.

This enumeration could be generalised too. We found an equation for the number of orbits between two general joint ordered factorisations of two-dimensions and with only two pairs each. This counting function can be considered as the last piece to understanding these particular orbits; we can detail what each orbit looks like, as well as how many there are.

Chapter 8

Orbit Structures

Using the framework outlined in Chapter 6, we established a complete description for cyclic orbits in two dimensions between two joint ordered factorisations written in their simplest form in Chapter 7.

Naturally we may extend our investigation to joint ordered factorisations with m dimensions and with more than two pairs.

To explicitly write the orbit structures pertaining to this generalisation will prove to be far more complex than the simplest case studied previously. Even restricting ourselves to the 2-dimensional cases yields raising operators that require information about its output in order to compute said output - which implies an *incompleteness* of these system's operators to fully describe their structure. We will demonstrate this at the end of the chapter where we consider special cases of 2-dimensional joint ordered factorisations with fairly low number of pairs.

However, this is not to say we cannot obtain more global patterns and properties these systems have. In the next section we shall see how the orbit structure between two m-dimensional joint ordered factorisations with an arbitrary number of pairs mimics the orbit structures between two different, but related, joint ordered factorisations. The cyclic orbits are repeated and stretched based upon commonly shared pairs between the joint ordered factorisations' tuple expressions (recall Definition 1.0.2 for these tuples).

8.1 Repeating orbits

If two joint ordered factorisations are similar in their ordering, then the orbits between their corresponding principal reversible cuboids will mirror orbits found between smaller principal reversible cuboids (smaller in reference to their component axis lengths). These smaller tensors are associated to joint ordered factorisations found by removing the initial similar ordering.

In particular, if the first number of pairs between two joint ordered factorisations are the same, then the orbit structures will mimic the orbit structure of the joint ordered factorisations which result from removing these equivalent pairs. The same is true if the last number of pairs are the same.

To demonstrate what we mean by "first/last number of pairs," consider, for $f_1, f_2, f_3 \in \mathbb{N}_2$, the two joint ordered factorisations $\mathcal{J}_1 = \big((1, f_1), (2, f_2), (1, f_3)\big)$ and $\mathcal{J}_2 = \big((1, f_1 f_3), (2, f_2)\big)$. If we were to write $\mathcal{J}_2$ as $\big((1, f_1), (1, f_3), (2, f_2)\big)$, although technically this is not a joint ordered factorisation due to two consecutive pairs having the same j-value, it is now correct to say that the first pair in both $\mathcal{J}_1$ and the alternative $\mathcal{J}_2$ are the same, namely $(1, f_1)$. To represent this we introduce the following definition and lemma.

Definition 8.1.1. Let $m \in \mathbb{N}$, $n \in \mathbb{N}_2^m$, $N = \prod_{j=1}^m n_j$, and $\mathcal{J} = \big((j_1, f_1), \ldots, (j_L, f_L)\big)$ a joint ordered factorisation on n, for $L \in \{m, \ldots, \Omega(N)\}$. We call the $\Omega(N)$-tuple of pairs

$$\mathcal{F} := \Big(\big(j_1, p_1\big), \big(j_2, p_2\big), \ldots, \big(j_{\Omega(N)}, p_{\Omega(N)}\big)\Big) \in \big(\{1, 2, \ldots, m\} \times \mathbb{N}_2\big)^{\Omega(N)},$$

where p_l is prime for $l \in \{1, \ldots, \Omega(N)\}$, a *full joint ordered factorisations of* n if, for $j \in \{1, \ldots, m\}$,

$$\prod_{j=j_l} p_l = n_j.$$

We say $\mathcal{F}$ is an *extension of* $\mathcal{J}$ if the joint ordered factorisation resulting from replacing consecutive pairs with the same j-value in $\mathcal{F}$ to form a single pair, with the same j-value and which the f-value is the product of the primes removed, is the same as $\mathcal{J}$.

This definition differs from the definition for joint ordered factorisations in two ways. Firstly, consecutive pairs in $\mathcal{F}$ can have the same j-value (i.e. $j_l = j_{l+1}$ is permitted).

Secondly, the second value of each pair must be prime. When referring to the position of a pair in $\mathcal{J}$ we continue to use the variable ℓ, and will use the variable l for the position in $\mathcal{F}$.

Often this coalescing of pairs process implies there is multiple ways to write the extension of a joint ordered factorisations $\mathcal{J}$. For each pair (j_ℓ, f_ℓ) in $\mathcal{J}$, the number of ways to write the corresponding pairs in $\mathcal{F}$ is equal to the number of ways to uniquely write all the prime factors of f_ℓ as a chain of primes, for which there are $c_{\Omega(f_\ell)}(f_\ell)$ ways to do so.

Lemma 8.1.2. Let $m \in \mathbb{N}$, $n \in \mathbb{N}_2^m$, $\mathcal{J}$ be a joint ordered factorisation of n and let $\mathcal{F}$ be an extension of $\mathcal{J}$. Then the sum system and sum-and-distance system that arises from $\mathcal{F}$ is identical to those found from $\mathcal{J}$.

Proof. Let us write $\mathcal{J} = \big((j_1, f_1), \ldots, (j_L, f_L)\big)$ and $\mathcal{F} = \big((j_1, p_1), \ldots, (j_{\Omega(N)}, p_{\Omega(N)})\big)$. For $j \in \{1, \ldots, m\}$ and $\ell \in \{1, \ldots, L\}$, let $(j, f_1 f_2)$ be the pair in position ℓ in $\mathcal{J}$. The construction formula for the j-th sum system component set, Eq. (2.3), contains the term $F(\ell)\langle f_1 f_2 \rangle$. Using identity (2.2), we can write

$$F(\ell)\langle f_1 f_2 \rangle = F(\ell)\Big(\langle f_1 \rangle + f_1 \langle f_2 \rangle\Big) = F(\ell)\langle f_1 \rangle + F(\ell + 1)\langle f_2 \rangle.$$

Hence, writing the single pair $(j, f_1 f_2)$ as $(j, f_1), (j, f_2)$ does not change the terms in the sumset of Eq. (2.3). Then expanding each pair into a chain of prime factors will not alter the construction of the sum system components, and thus $\mathcal{F}$ generates the same sum system as $\mathcal{J}$. By the bijection in Theorem 2.2.5, the sum-and-distance system will remain unchanged also. □

In what follows we let $m \in \mathbb{N}$, $\kappa \in \{1, 2\}$, $n \in \mathbb{N}_2^m$, $N = \prod_{j=1}^m n_j$, and $\mu, \nu \in \mathbb{N}_0$.

Consider two joint ordered factorisations of n, $\mathcal{J}_1$ and $\mathcal{J}_2$, such that for at least one extension each, $\mathcal{F}_1$ and $\mathcal{F}_2$, the first μ pairs or last $\Omega(N) + 1 - \nu$ pairs are the same in both extensions. Explicitly, let (j_l, p_l) and (i_l, q_l) be the l-th pair in $\mathcal{F}_1$ and $\mathcal{F}_2$ respectively. Then we want $(j_l, p_l) = (i_l, q_l)$ for $l \leq \mu$ or $l \geq \nu$.

For example, for the two joint ordered factorisations

$$\mathcal{J}_1 = \big((1,6), (2,9), (1,5)\big), \quad \text{and} \quad \mathcal{J}_2 = \big((1,3), (2,3), (1,2), (2,3), (1,5)\big),$$

we can choose the extensions

$$\mathcal{F}_1 = \big((1,3), (1,2), (2,3), (2,3), (1,5)\big), \quad \text{and} \quad \mathcal{F}_2 = \big((1,3), (2,3), (1,2), (2,3), (1,5)\big).$$

In this case, the first pair in both extensions are equal (i.e. $\mu = 1$) and the last two pairs are equal (i.e. $\nu = 4$).

If $\mu \geq 0$ and $\nu \leq \Omega(N)$, the full orbit permeation $\sigma_{\mathcal{J}_1,\mathcal{J}_2}$ exhibits repeating cyclic orbit structure based on the full orbit between joint ordered factorisations that result by removing these equal pairs.

For $\kappa \in \{1, 2\}$, by Lemma 8.1.2 both $\mathcal{F}_\kappa$ and $\mathcal{J}_\kappa$ share the same sum system, and thus the same principal reversible cuboid. As such, there is no ambiguity when considering coordinates between these systems, i.e. $C_{\mathcal{F}_\kappa}(M) = C_{\mathcal{J}_\kappa}(M)$. Likewise, the raising operator and cyclic orbit remains the same when considering either expression such that $O_{\mathcal{J}_1,\mathcal{J}_2}(M) = O_{\mathcal{F}_1,\mathcal{F}_2}(M)$ and $\mathcal{O}_{\mathcal{J}_1,\mathcal{J}_2}(M) = \mathcal{O}_{\mathcal{F}_1,\mathcal{F}_2}(M)$. Therefore we will be only considering $\mathcal{F}_\kappa$ for this section.

Before continuing, we recall the following operation that shall make appearance within this section. For $m \in \mathbb{N}$ and vectors $v, w \in \mathbb{N}_0^m$, such that

$$v = (v_1, \ldots, v_m), \quad \text{and} \quad w = (w_1, \ldots, w_m),$$

then we define the *direct sum (of these vectors)* to be

$$v \oplus w := (v_1, \ldots, v_m, w_1, \ldots, w_m).$$

8.1.1 Case 1: first μ pairs equal

Let $1 \leq \mu \leq \Omega(N)$ and $\nu > \Omega(N)$, such that only the first μ pairs for the fixed extensions $\mathcal{F}_1$ and $\mathcal{F}_2$ are equal. In the lemmas and theorem of this subsection, we will refer to the following hypothesis statement.

Hypothesis statement 2 (H2): Let $m \in \mathbb{N}$, $n \in \mathbb{N}_2^m$ and $N = \prod_{j=1}^m n_j$. Let $\mathcal{F}_1$ and $\mathcal{F}_2$ be two full joint ordered factorisations of n, such that the first $1 \leq \mu \leq \Omega(N)$ pairs are the same in both tuples. Let $\mathcal{M}$ and $\mathcal{N}$ denote the principal reversible cuboids of $\mathcal{F}_1$ and $\mathcal{F}_2$ respectively. For $\kappa \in \{1, 2\}$, we let $M \in \langle N \rangle$ be an element from the target set for the sum system of $\mathcal{F}_\kappa$, and denote the address of M in $\mathcal{F}_\kappa$ by $\alpha(M)$.

Let us write

$$\mathcal{F}_\kappa = \Big((j_1^{(\kappa)}, p_1^{(\kappa)}), \ldots, (j_{\Omega(N)}^{(\kappa)}, p_{\Omega(N)}^{(\kappa)}) \Big),$$

such that $\big(j_l^{(1)}, p_l^{(1)}\big) = \big(j_l^{(2)}, p_l^{(2)}\big)$ for $1 \leq l \leq \mu$. For $l \in \{1, \ldots, \Omega(N)\}$ and $j \in \{1, \ldots, m\}$, associate to $\mathcal{F}_\kappa$ the partial products

$$F(\kappa; l) = \prod_{h=1}^{l-1} p_h^{(\kappa)}, \quad \text{and} \quad P_j(\kappa; l) = \prod_{\substack{h \in \mathcal{L}_j(\kappa) \\ h<l}} p_h^{(\kappa)},$$

where $\mathcal{L}_j(\kappa) = \{l : j_l^{(\kappa)} = j \text{ in } \mathcal{F}_\kappa\}$. We associate to these partial products the column vectors

$$\overrightarrow{F(\kappa)} := \begin{pmatrix} F(\kappa; 1) \\ \vdots \\ F(\kappa; L) \end{pmatrix}, \qquad \overrightarrow{P(\kappa)} := \begin{pmatrix} P_{j_1}(\kappa; 1)\bar{e}_{j_1} \\ \vdots \\ P_{j_L}(\kappa; L)\bar{e}_{j_L} \end{pmatrix}.$$

Additionally, define the constants

$$^{\mu}F := F(\kappa; \mu+1), \quad \text{and} \quad {}^{\mu}P_j := P_j(\kappa; \mu+1)$$

which are independent of κ.

Then let us define

$$^{\mu}\mathcal{F}_\kappa := \Big(\big(j_{\mu+1}^{(\kappa)}, p_{\mu+1}^{(\kappa)}\big), \ldots, \big(j_{\Omega(N)}^{(\kappa)}, p_{\Omega(N)}^{(\kappa)}\big) \Big)$$

to be the full joint ordered factorisation that results from removing the first μ pairs in $\mathcal{F}_\kappa$. We let $\mathcal{M}^\mu$ and $\mathcal{N}^\mu$ denote the principal reversible cuboids of ${}^{\mu}\mathcal{F}_1$ and ${}^{\mu}\mathcal{F}_2$ respectively. The target set of the sum system associated to ${}^{\mu}\mathcal{F}_\kappa$ is $\langle \frac{N}{{}^{\mu}F} \rangle$. We use $\tilde{M} \in \langle \frac{N}{{}^{\mu}F} \rangle$ to denote an element from this system, with the address of $\tilde{M}$ in ${}^{\mu}\mathcal{F}_\kappa$ given by $\beta(\tilde{M}) = (\beta_1, \ldots, \beta_{\Omega(N)-\mu})$.

For $\mu + 1 \leq l \leq \Omega(N)$ and $j \in \{1, \ldots, m\}$, over ${}^{\mu}\mathcal{F}_\kappa$ we define the partial products

$$F^\mu(\kappa; l) = \prod_{h=\mu+1}^{l-1} p_h^{(\kappa)} = \frac{\prod_{h=1}^{l-1} p_h^{(\kappa)}}{\prod_{h=1}^{\mu} p_h^{(\kappa)}} = \frac{F(\kappa; l)}{{}^{\mu}F},$$

$$P_j^\mu(\kappa; l) = \prod_{\substack{h \in \mathcal{L}_j(\kappa) \\ \mu<h<l}} p_h^{(\kappa)} = \frac{\prod_{\substack{h \in \mathcal{L}_j(\kappa) \\ h<l}} p_h^{(\kappa)}}{\prod_{\substack{h \in \mathcal{L}_j(\kappa) \\ h<\mu+1}} p_h^{(\kappa)}} = \frac{P_j(\kappa; l)}{{}^{\mu}P_j},$$

which we can write in terms of partial products over $\mathcal{F}_\kappa$. We associate to $F^\mu(\kappa; l)$ the column vector

$$\overrightarrow{F^\mu(\kappa)} = \begin{pmatrix} F^\mu(\kappa; \mu+1) \\ \vdots \\ F^\mu(\kappa; \Omega(N)) \end{pmatrix}.$$

Remark 8.1.3. When removing pairs for ${}^\mu\mathcal{F}_\kappa$, if all pairs with a specific j-value are removed, say $j = \delta$, then we set the δ-th value in $C_{{}^\mu\mathcal{F}_\kappa}\big(\tilde{M}\big)$ to be 0. Another way to say this is that we still consider $\mathcal{M}^\mu$ and $\mathcal{N}^\mu$ to be order m tensors even if the δ-th coordinate axis was removed. In such a case we set the δ-th sum system component set of ${}^\mu\mathcal{F}_\kappa$ to be $\{0\}$.

Example 8.1.4. Let $n = (6, 6)$, with $N = 36$, and consider the two full joint ordered factorisations

$$\mathcal{F}_1 = \big((1,2),(2,3),(1,3),(2,2)\big), \quad \text{and} \quad \mathcal{F}_2 = \big((1,2),(2,3),(2,2),(1,3)\big),$$

with the principal reversible matrices

$$\mathcal{M} = \begin{pmatrix} 0 & 1 & 6 & 7 & 12 & 13 \\ 2 & 3 & 8 & 9 & 14 & 15 \\ 4 & 5 & 10 & 11 & 16 & 17 \\ 18 & 19 & 24 & 25 & 30 & 31 \\ 20 & 21 & 26 & 27 & 32 & 33 \\ 22 & 23 & 28 & 29 & 34 & 35 \end{pmatrix}, \quad \text{and} \quad \mathcal{N} = \begin{pmatrix} 0 & 1 & 12 & 13 & 24 & 25 \\ 2 & 3 & 14 & 15 & 26 & 27 \\ 4 & 5 & 16 & 17 & 28 & 29 \\ 6 & 7 & 18 & 19 & 30 & 31 \\ 8 & 9 & 20 & 21 & 32 & 33 \\ 10 & 11 & 22 & 23 & 34 & 35 \end{pmatrix}.$$

The first two pairs, $(1,2),(2,3)$, are the same, thus $\mu = 2$. Removing these pairs leaves us the full joint ordered factorisations

$${}^\mu\mathcal{F}_1 = \big((1,3),(2,2)\big), \quad \text{and} \quad {}^\mu\mathcal{F}_2 = \big((2,2),(1,3)\big).$$

with the principal reversible matrices

$${}^\mu\mathcal{M} = \begin{pmatrix} 0 & 1 & 2 \\ 3 & 4 & 5 \end{pmatrix}, \quad \text{and} \quad {}^\mu\mathcal{N} = \begin{pmatrix} 0 & 2 & 4 \\ 1 & 3 & 5 \end{pmatrix}.$$

For either $\kappa \in \{1, 2\}$, we have the constants

$${}^\mu F := F(\kappa; 3) = 6, \qquad {}^\mu P_1 := P_1(\kappa; 3) = 2, \quad \text{and} \quad {}^\mu P_2 := P_2(\kappa; 3) = 3.$$

Lemma 8.1.5. Assume (H2). For $\kappa \in \{1,2\}$, let $\tilde{M} \in \langle \frac{N}{{}^{\mu}F} \rangle$ be an integer from the target set of the sum system corresponding to ${}^{\mu}\mathcal{F}_{\kappa}$. Additionally, let ${}^{\mu}F\tilde{M}, M \in \langle N \rangle$ be integers from the target set of the sum system corresponding to $\mathcal{F}_{\kappa}$. Then the address of $\tilde{M}$ in ${}^{\mu}\mathcal{F}_{\kappa}$ and the address of ${}^{\mu}F\tilde{M}$ in $\mathcal{F}_{\kappa}$ are related by

$$\alpha({}^{\mu}F\tilde{M}) = 0_{\mu} \oplus \beta(\tilde{M}) = (0, \ldots, 0, \beta_1, \ldots, \beta_{\Omega(N)-\mu}),$$

where $\oplus$ is the direct sum of two vectors. Furthermore, we can associate each $M \in \langle N \rangle$ with a unique pair $(\tilde{M}, r)$, for $r \in \langle {}^{\mu}F \rangle$, such that

$$M = {}^{\mu}F\tilde{M} + r.$$

Proof. We can write $\tilde{M} = \beta(\tilde{M})\overrightarrow{F^{\mu}(\kappa)}$ using Eq. (6.1), which we multiply by ${}^{\mu}F$ and expand to get

$$\begin{aligned}
{}^{\mu}F\tilde{M} = {}^{\mu}F\beta(\tilde{M})\overrightarrow{F^{\mu}(\kappa)} &= {}^{\mu}F\Big(\beta_1 F^{\mu}(\kappa;1) + \cdots + \beta_{\Omega(N)-\mu}F^{\mu}(\kappa;\Omega(N)-\mu)\Big) \\
&= {}^{\mu}F\left(\beta_1 \frac{F(\kappa;\mu+1)}{{}^{\mu}F} + \cdots + \beta_{\Omega(N)-\mu}\frac{F(\kappa;\Omega(N))}{{}^{\mu}F}\right) \\
&= \beta_1 F(\kappa;\mu+1) + \cdots + \beta_{\Omega(N)-\mu}F(\kappa;\Omega(N)) \\
&= \big(0, \ldots, 0, \beta_1, \ldots, \beta_{\Omega(N)-\mu}\big)\overrightarrow{F(\kappa)} \\
&= 0_{\mu} \oplus \beta(\tilde{M})\overrightarrow{F(\kappa)} = \alpha({}^{\mu}F\tilde{M})\overrightarrow{F(\kappa)},
\end{aligned}$$

where we use Eq. (6.1) again in the final line with ${}^{\mu}F\tilde{M} = \alpha({}^{\mu}F\tilde{M})\overrightarrow{F(\kappa)}$. By equating tuples in the final line we retrieve $\alpha({}^{\mu}F\tilde{M}) = 0_{\mu} \oplus \beta(\tilde{M})$.

The first μ pairs in both $\mathcal{F}_1$ and $\mathcal{F}_2$ are the same and thus the first ${}^{\mu}F$ integers are in the same position in both $\mathcal{M}$ and $\mathcal{N}$. Therefore each $r \in \langle {}^{\mu}F \rangle$ is a fixed point which means $C_{\mathcal{F}_1}(r) = C_{\mathcal{F}_2}(r)$. Because $F(1;l) = F(2;l)$, for $1 \leq l \leq \mu$, we can write

$$r = \alpha(r)\overrightarrow{F(\kappa)} = (\alpha_1, \ldots, \alpha_{\mu}, 0, \ldots, 0)\overrightarrow{F(\kappa)} = \alpha_1 F(\kappa;1) + \alpha_2 F(\kappa;2) + \cdots + \alpha_{\mu}F(\kappa;\mu).$$

For $M \in \langle N \rangle$, using Eq. (6.1) we can express M as

$$\begin{aligned} M &= \alpha(M)\overrightarrow{F(\kappa)} \\ &= \underbrace{\alpha_1 F(\kappa;1) + \cdots + \alpha_\mu F(\kappa;\mu)}_{=\text{ some } r\in\langle {}^\mu F\rangle} + \alpha_{\mu+1} \underbrace{F(\kappa;\mu+1)}_{={}^\mu F} + \cdots + \alpha_{\Omega(N)} F\big(\kappa;\Omega(N)\big) \\ &= r + {}^\mu F\left(\alpha_{\mu+1} + \alpha_{\mu+2}\frac{F(\kappa;\mu+2)}{{}^\mu F} + \cdots + \alpha_{\Omega(N)}\frac{F\big(\kappa;\Omega(N)\big)}{{}^\mu F}\right) \\ &= r + {}^\mu F \underbrace{\left(\alpha_{\mu+1} + \alpha_{\mu+2}F^\mu(\kappa;\mu+2)\cdots + \alpha_{\Omega(N)}F^\mu\big(\kappa;\Omega(N)\big)\right)}_{=\text{ some } \tilde{M}\in\langle \frac{N}{{}^\mu F}\rangle \text{ from the system } {}^\mu\mathcal{F}_\kappa} \\ &= r + {}^\mu F\tilde{M}, \end{aligned}$$

where we set $\beta_l = \alpha_{\mu+l}$ in $\alpha({}^\mu F\tilde{M}) = (0,\ldots,0,\beta_1,\ldots,\beta_{\Omega(N)-\mu})$. □

Lemma 8.1.6. Assume (H2). Let $\tilde{M} \in \langle \frac{N}{{}^\mu F}\rangle$ be an integer from the target set of the sum system corresponding to ${}^\mu\mathcal{F}_1$ and ${}^\mu\mathcal{F}_2$, which have the principal reversible cuboids $\mathcal{M}^\mu$ and $\mathcal{N}^\mu$ respectively. Additionally, let ${}^\mu F\tilde{M}, M \in \langle N\rangle$ be integers from the target set of the sum system corresponding to $\mathcal{F}_1$ and $\mathcal{F}_2$, which have the principal reversible cuboids $\mathcal{M}$ and $\mathcal{N}$ respectively. Then the position of $\tilde{M}$ in $\mathcal{M}^\mu$ and $\mathcal{N}^\mu$ is related to the position of ${}^\mu F\tilde{M}$ in $\mathcal{M}$ and $\mathcal{N}$ by the transform

$$C_{\mathcal{F}_\kappa}\big({}^\mu F\tilde{M}\big) = C_{{}^\mu\mathcal{F}_\kappa}\big(\tilde{M}\big)\begin{pmatrix} {}^\mu P_1 & 0 & \ldots & 0 \\ 0 & {}^\mu P_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & {}^\mu P_m \end{pmatrix}, \tag{8.1}$$

for $\kappa \in \{1,2\}$. Furthermore, for some $r \in \langle {}^\mu F\rangle$, the position of $M = {}^\mu F\tilde{M} + r \in \langle N\rangle$ in either $\mathcal{M}$ and $\mathcal{N}$ can be expressed as

$$C_{\mathcal{F}_\kappa}(M) = C_{\mathcal{F}_\kappa}\big({}^\mu F\tilde{M}\big) + C_{\mathcal{F}_\kappa}(r). \tag{8.2}$$

Proof. The address of $\tilde{M}$ in ${}^\mu\mathcal{F}_\kappa$ is given by $\beta(\tilde{M}) = (\beta_1,\ldots,\beta_{\Omega(N)-\mu})$. Using Eq. (6.2), we can write the coordinate map of $\tilde{M}$ in ${}^\mu\mathcal{F}_\kappa$ as

$$C_{{}^\mu\mathcal{F}_\kappa}(\tilde{M}) = \beta(\tilde{M})\begin{pmatrix} P^\mu_{j_{\mu+1}}(\kappa;\mu+1)\bar{e}_{j_{\mu+1}} \\ \vdots \\ P^\mu_{j_{\Omega(N)}}(\kappa;\Omega(N))\bar{e}_{j_{\Omega(N)}} \end{pmatrix} = \sum_{l=\mu+1}^{\Omega(N)} \beta_{l-\mu}P^\mu_{j_l}(\kappa;l)\bar{e}_{j_l}.$$

Using Lemma 8.1.5, with $P^{\mu}_{j}(\kappa;l) = \frac{P_j(\kappa;l)}{{}^{\mu}P_j}$ and Eq. (6.2) again, Eq. (8.1) follows from

$$\begin{aligned}
C_{\mathcal{F}_\kappa}({}^{\mu}F\tilde{M}) = \alpha({}^{\mu}F\tilde{M})\overrightarrow{P(\kappa)} &= 0_\mu \oplus \beta(\tilde{M})\overrightarrow{P(\kappa)} \\
&= \sum_{l=1}^{\mu} \underbrace{\alpha_l}_{=0} P_{j_l}(\kappa;l)\bar{e}_{j_l} + \sum_{l=\mu+1}^{\Omega(N)} \beta_l P_{j_l}(\kappa;l)\bar{e}_{j_l} \\
&= \sum_{l=\mu+1}^{\Omega(N)} {}^{\mu}P_{j_l}\beta_l \frac{P_{j_l}(\kappa;l)}{{}^{\mu}P_{j_l}}\bar{e}_{j_l} \\
&= \underbrace{\left(\sum_{l=\mu+1}^{\Omega(N)} \beta_{l-\mu} P^{\mu}_{j_l}(\kappa;l)\bar{e}_{j_l}\right)}_{=C_{{}^{\mu}\mathcal{F}_\kappa}(\tilde{M})} \begin{pmatrix} {}^{\mu}P_1 & 0 & \dots & 0 \\ 0 & {}^{\mu}P_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & {}^{\mu}P_m \end{pmatrix},
\end{aligned}$$

as required.

Because $\alpha\big({}^{\mu}F\tilde{M}\big) = (0,\dots,0,\alpha_{\mu+1},\dots,\alpha_{\Omega(N)})$ and $\alpha(r) = (\alpha_1,\dots,\alpha_\mu,0,\dots,0)$ then

$$\alpha\big({}^{\mu}F\tilde{M} + r\big) = (\alpha_1,\dots,\alpha_\mu,\alpha_{\mu+1},\dots,\alpha_{\Omega(N)}) = \alpha\big({}^{\mu}F\tilde{M}\big) + \alpha(r).$$

Eq. (8.2) then follows from

$$C_{\mathcal{F}_\kappa}(M) = C_{\mathcal{F}_\kappa}\big({}^{\mu}F\tilde{M}+r\big) = \alpha\big({}^{\mu}F\tilde{M}+r\big)\overrightarrow{P(\kappa)} = \big(\alpha\big({}^{\mu}F\tilde{M}\big)+\alpha(r)\big)\overrightarrow{P(\kappa)} = C_{\mathcal{F}_\kappa}\big({}^{\mu}F\tilde{M}\big)+C_{\mathcal{F}_\kappa}(r).$$

□

Lemma 8.1.7. Assume (H2). Let $\tilde{M} \in \langle \frac{N}{{}^{\mu}F} \rangle$ be an integer from the target set of the sum system corresponding to ${}^{\mu}\mathcal{F}_\kappa$, for $\kappa \in \{1,2\}$. For $r \in \langle {}^{\mu}F \rangle$, let $M = {}^{\mu}F\tilde{M} + r \in \langle N \rangle$ be an integer from the target set of the sum system corresponding to $\mathcal{F}_\kappa$. Then the raising operator of M between $\mathcal{F}_1$ and $\mathcal{F}_2$ is related to the raising operator of $\tilde{M}$ between ${}^{\mu}\mathcal{F}_1$ and ${}^{\mu}\mathcal{F}_2$ by the identity

$$O_{\mathcal{F}_1,\mathcal{F}_2}(M) = M^{(1)} = {}^{\mu}F\, O_{{}^{\mu}\mathcal{F}_1,{}^{\mu}\mathcal{F}_2}(\tilde{M}) + r = {}^{\mu}F\tilde{M}^{(1)} + r.$$

Proof. By definition $O_{\mathcal{F}_1,\mathcal{F}_2}(M) = M^{(1)} = \mathcal{N}_{C_{\mathcal{F}_1}(M)}$, with the reverse map $M = \mathcal{M}_{C_{\mathcal{F}_2}(M^{(1)})}$. Likewise, $\tilde{M} = \mathcal{M}^{\mu}_{C_{{}^{\mu}\mathcal{F}_2}(\tilde{M}^{(1)})}$. Furthermore, for $0 \le c \le n - 1_m$, we have $C_{\mathcal{F}_1}(\mathcal{M}_c) = c$, and $C_{{}^{\mu}\mathcal{F}_1}(\mathcal{M}^{\mu}_{\tilde{c}}) = \tilde{c}$ for $\tilde{c}_j < \frac{n_j}{{}^{\mu}P_j}$. Let $[P_\mu]$ denote the matrix in Eq. (8.1). Then we have

$$C_{\mathcal{F}_1}({}^{\mu}F\tilde{M}) = C_{{}^{\mu}\mathcal{F}_1}(\tilde{M})[P_\mu] = C_{{}^{\mu}\mathcal{F}_1}\Big(\mathcal{M}^{\mu}_{C_{{}^{\mu}\mathcal{F}_2}(\tilde{M}^{(1)})}\Big)[P_\mu] = C_{{}^{\mu}\mathcal{F}_2}(\tilde{M}^{(1)})[P_\mu] = C_{\mathcal{F}_2}({}^{\mu}F\tilde{M}^{(1)}),$$

which enables us to write

$$M^{(1)} = \mathcal{N}_{C_{\mathcal{F}_1}(M)} = \mathcal{N}_{C_{\mathcal{F}_1}({}^{\mu}F\tilde{M})} + \mathcal{N}_{C_{\mathcal{F}_2}(r)} = \mathcal{N}_{C_{\mathcal{F}_2}({}^{\mu}F\tilde{M}^{(1)})} + r = {}^{\mu}F\tilde{M}^{(1)} + r,$$

where we have used Lemma 8.1.5 for $C_{\mathcal{F}_1}(r) = C_{\mathcal{F}_2}(r)$. □

Theorem 8.1.8. Assume (H2). Let $\tilde{M} \in \langle \frac{N}{{}^{\mu}F} \rangle$ be an integer from the target set of the sum system corresponding to ${}^{\mu}\mathcal{F}_{\kappa}$, for $\kappa \in \{1, 2\}$. For $r \in \langle {}^{\mu}F \rangle$, let $M = {}^{\mu}F\tilde{M} + r \in \langle N \rangle$ be an integer from the target set of the sum system corresponding to $\mathcal{F}_{\kappa}$. Then the cyclic orbit of M between $\mathcal{F}_1$ and $\mathcal{F}_2$ is related to the cyclic orbit of $\tilde{M}$ between ${}^{\mu}\mathcal{F}_1$ and ${}^{\mu}\mathcal{F}_2$ by the identity

$$\mathcal{O}_{\mathcal{F}_1,\mathcal{F}_2}(M) = {}^{\mu}F\, \mathcal{O}_{{}^{\mu}\mathcal{F}_1,{}^{\mu}\mathcal{F}_2}\big(\tilde{M}\big) + r.$$

Proof. For $t \in \langle d \rangle$, after t applications of Lemma 8.1.7 to $O_{\mathcal{F}_1,\mathcal{F}_2}(M)$, we get

$$M^{(t)} = (O_{\mathcal{F}_1,\mathcal{F}_2})^t(M) = {}^{\mu}F\tilde{M}^{(t)} + r,$$

which enables us to write

$$\begin{aligned}
\mathcal{O}_{\mathcal{F}_1,\mathcal{F}_2}(M) &= \Big\{M^{(0)}, M^{(1)}, \dots, M^{(d-1)}\Big\} \\
&= \Big\{{}^{\mu}F\tilde{M}^{(0)} + r,\ {}^{\mu}F\tilde{M}^{(1)} + r,\ \dots,\ {}^{\mu}F\tilde{M}^{(d-1)} + r\Big\} \\
&= {}^{\mu}F\Big\{\tilde{M}^{(0)}, \tilde{M}^{(1)}, \dots, \tilde{M}^{(d-1)}\Big\} + r \\
&= {}^{\mu}F\mathcal{O}_{{}^{\mu}\mathcal{F}_1,{}^{\mu}\mathcal{F}_2}\big(\tilde{M}\big) + r,
\end{aligned}$$

as required. □

This relation effectively takes each orbit between ${}^{\mu}\mathcal{F}_1$ and ${}^{\mu}\mathcal{F}_2$, and copies it in the j_l-th coordinate axis direction p_l times and scales the orbit by ${}^{\mu}F$, where (j_l, p_l) is the l-th pair in $\mathcal{F}_{\kappa}$, for $l \leq \mu$. There are ${}^{\mu}F$ copies of each orbit.

Example 8.1.9. Let us continue Example 8.1.4, with $\mathcal{F}_1 = \big((1,2),(2,3),(1,3),(2,2)\big)$ and $\mathcal{F}_2 = \big((1,2),(2,3),(2,2),(1,3)\big)$. Here we had $\mu = 2$ such that ${}^{\mu}\mathcal{F}_1 = \big((1,3),(2,2)\big)$ and ${}^{\mu}\mathcal{F}_2 = \big((2,2),(1,3)\big)$. Note that $N = 36$ and ${}^{\mu}F = 6$.

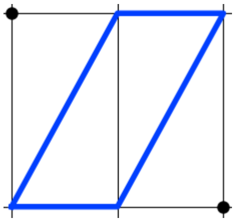
By Theorem 8.1.5 we can write $M \in \langle 36 \rangle$ as $M = 6\tilde{M} + r$, for some $\tilde{M} \in \langle \frac{N}{{}^{\mu}F} \rangle = \langle 6 \rangle$ and $r \in \langle {}^{\mu}F \rangle = \langle 6 \rangle$, and by Theorem 8.1.8 we have $\mathcal{O}_{\mathcal{F}_1,\mathcal{F}_2}(M) = 6\ \mathcal{O}_{{}^{\mu}\mathcal{F}_1,{}^{\mu}\mathcal{F}_2}(\tilde{M}) + r$. For example, let $M = 25 = 6(4) + 1$, and by Eq. (8.2) we can write

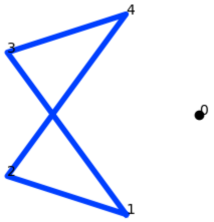
$$C_{\mathcal{F}_1}(25) = C_{\mathcal{F}_1}(24) + C_{\mathcal{F}_1}(1) = \ C_{{}^{\mu}\mathcal{F}_1}(4)\begin{pmatrix}2 & 0\\ 0 & 3\end{pmatrix} + (1,0) = (1,1)\begin{pmatrix}2 & 0\\ 0 & 3\end{pmatrix} + (1,0) = (3,3).$$

Using Theorem 8.1.8 we have

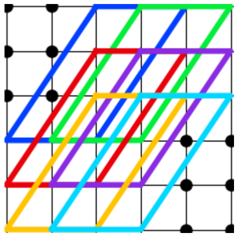
$$\mathcal{O}_{\mathcal{F}_1,\mathcal{F}_2}(25) = 6\mathcal{O}_{{}^{\mu}\mathcal{F}_1,{}^{\mu}\mathcal{F}_2}(4) + 1 = 6\{1,2,4,3\} + 1 = \{7,13,25,19\}.$$

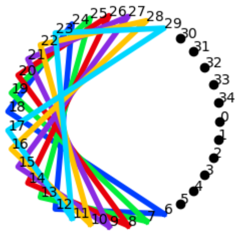
We can write the full orbit permutation $\sigma_{{}^{\mu}\mathcal{F}_1,{}^{\mu}\mathcal{F}_2} = (0)\,(1\ 2\ 4\ 3)\,(5)$ which have the cuboid and ring geometries





The full orbit permutation $\sigma_{\mathcal{F}_1,\mathcal{F}_2}$ has the cuboid and ring geometries





The orbits within $\sigma_{{}^{\mu}\mathcal{F}_1,{}^{\mu}\mathcal{F}_2}$ can be seen within the orbits of $\sigma_{\mathcal{F}_1,\mathcal{F}_2}$, copied and stretched. We make ${}^{\mu}F = 6$ copies of each cyclic orbit in $\sigma_{{}^{\mu}\mathcal{F}_1,{}^{\mu}\mathcal{F}_2}$. Each copy is multiplied by 6, and there are $p_1 = 2$ copies in the $j_1 =$ 1-st coordinate axis direction (going right), and $p_2 = 3$ copies in the $j_2 =$ 2-nd coordinate axis direction (going down), with each copy placed in consecutive positions. Note that $\mathcal{O}_{\mathcal{F}_1,\mathcal{F}_2}(25)$ is depicted by the green line in the cuboid and ring geometries of $\sigma_{\mathcal{F}_1,\mathcal{F}_2}$.

8.1.2 Case 2: last $\Omega(N) + 1 - \nu$ pairs equal

Now we will investigate the case of $\mu = 0$ and $1 \leq \nu \leq \Omega(N)$, such that only the last $\Omega(N) + 1 - \nu$ pairs for the fixed extensions $\mathcal{F}_1$ and $\mathcal{F}_2$ are equal. In the lemmas and theorem of this subsection, we will refer to the following hypothesis statement.

Hypothesis statement 3 (H3): Let $m \in \mathbb{N}$, $n \in \mathbb{N}_2^m$ and $N = \prod_{j=1}^m n_j$. Let $\mathcal{F}_1$ and $\mathcal{F}_2$ be two full joint ordered factorisations of n, such that the last $\Omega(N)+1-\nu$ pairs are the same in both tuples, for $1 \leq \nu \leq \Omega(N)$. Let $\mathcal{M}$ and $\mathcal{N}$ denote the principal reversible cuboids of $\mathcal{F}_1$ and $\mathcal{F}_2$ respectively. For $\kappa \in \{1, 2\}$, we let $M \in \langle N \rangle$ be an element from the target set for the sum system of $\mathcal{F}_\kappa$, and denote the address of M in $\mathcal{F}_\kappa$ by $\alpha(M)$.

Let us write

$$\mathcal{F}_\kappa = \Big(\big(j_1^{(\kappa)}, p_1^{(\kappa)}\big), \ldots, \big(j_{\Omega(N)}^{(\kappa)}, p_{\Omega(N)}^{(\kappa)}\big) \Big),$$

such that $\big(j_l^{(1)}, p_l^{(1)}\big) = \big(j_l^{(2)}, p_l^{(2)}\big)$ when $\nu \leq l \leq \Omega(N)$. For $l \in \{1, \ldots, \Omega(N)\}$ and $j \in \{1, \ldots, m\}$, associate to $\mathcal{F}_\kappa$ the partial products

$$F(\kappa; l) = \prod_{h=1}^{l-1} p_h^{(\kappa)}, \quad \text{and} \quad P_j(\kappa; l) = \prod_{\substack{h \in \mathcal{L}_j(\kappa) \\ h<l}} p_h^{(\kappa)},$$

where $\mathcal{L}_j(\kappa) = \{l : j_l^{(\kappa)} = j \text{ in } \mathcal{F}_\kappa\}$. We associate to these partial products the column vectors

$$\overrightarrow{F(\kappa)} := \begin{pmatrix} F(\kappa; 1) \\ \vdots \\ F(\kappa; L) \end{pmatrix}, \qquad \overrightarrow{P(\kappa)} := \begin{pmatrix} P_{j_1}(\kappa; 1)\bar{e}_{j_1} \\ \vdots \\ P_{j_L}(\kappa; L)\bar{e}_{j_L} \end{pmatrix}.$$

Additionally, define the constants

$$F^\nu := F(\kappa; \nu), \quad \text{and} \quad P_j^\nu := P_j(\kappa; \nu),$$

which are independent of κ.

Then let us define

$$\mathcal{F}_\kappa^\nu := \Big(\big(j_1^{(\kappa)}, p_1^{(\kappa)}\big), \ldots, \big(j_{\nu-1}^{(\kappa)}, p_{\nu-1}^{(\kappa)}\big) \Big)$$

to be the full joint ordered factorisation that results from removing the last $\Omega(N)+1-\nu$ pairs in $\mathcal{F}_\kappa$. We let $\mathcal{M}^\nu$ and $\mathcal{N}^\nu$ denote the principal reversible cuboids of $\mathcal{F}_1^\nu$ and $\mathcal{F}_2^\nu$ respectively. The target set of the sum system associated to $\mathcal{F}_\kappa^\nu$ is $\langle \frac{N}{\mu F} \rangle$. We use $\hat{M} \in \langle F^\nu \rangle$ to denote an element from this system, with the address of $\hat{M}$ in $\mathcal{F}_\kappa^\nu$ given by $\gamma(\hat{M}) = \big(\gamma_1, \ldots, \gamma_\nu\big)$.

For $1 \leq l \leq \nu - 1$ and $j \in \{1, \ldots, m\}$, over $\mathcal{F}_\kappa^\nu$ we define the partial products

$$F^\nu(\kappa; l) = \prod_{h=1}^{l-1} p_h^{(\kappa)} = F(\kappa; l), \quad \text{and} \quad P_j^\nu(\kappa; l) = \prod_{\substack{h \in \mathcal{L}_j(\kappa) \\ h<l}} p_h^{(\kappa)} = P_j(\kappa; l),$$

which we can write in terms of partial products over $\mathcal{F}_\kappa$.

Remark 8.1.10. When removing pairs for $\mathcal{F}_\kappa^\nu$, if all pairs with a specific j-value are removed, say $j = \delta$, then we set the δ-th value in $C_{\mathcal{F}_\kappa^\nu}\big(\hat{M}\big)$ to be 0. Another way to say this is that we still consider $\mathcal{M}^\nu$ and $\mathcal{N}^\nu$ to be order m tensors even if the δ-th coordinate axis was removed. In such a case we set the δ-th sum system component set of $\mathcal{F}_\kappa^\nu$ to be $\{0\}$.

Example 8.1.11. Let $n = (6, 6)$, with $N = 36$, and consider the two full joint ordered factorisations

$$\mathcal{F}_1 = \big((1,3),(2,2),(1,2),(2,3)\big), \quad \text{and} \quad \mathcal{F}_2 = \big((2,2),(1,3),(1,2),(2,3)\big),$$

with the principal reversible matrices

$$\mathcal{M} = \begin{pmatrix} 0 & 1 & 2 & 6 & 7 & 8 \\ 3 & 4 & 5 & 9 & 10 & 11 \\ 12 & 13 & 14 & 18 & 19 & 20 \\ 15 & 16 & 17 & 21 & 22 & 23 \\ 24 & 25 & 26 & 30 & 31 & 32 \\ 27 & 28 & 29 & 33 & 34 & 35 \end{pmatrix}, \quad \text{and} \quad \mathcal{N} = \begin{pmatrix} 0 & 2 & 4 & 6 & 8 & 10 \\ 1 & 3 & 5 & 7 & 9 & 11 \\ 12 & 14 & 16 & 18 & 20 & 22 \\ 13 & 15 & 17 & 19 & 21 & 23 \\ 24 & 26 & 28 & 30 & 32 & 34 \\ 25 & 27 & 29 & 31 & 33 & 35 \end{pmatrix}.$$

The last two pairs, $(1,2),(2,3)$, are the same, thus $\nu = \Omega(36) + 1 - 2 = 3$. Removing these pairs leaves us the full joint ordered factorisations

$$\mathcal{F}_1^\nu = \big((1,3),(2,2)\big), \quad \text{and} \quad \mathcal{F}_2^\nu = \big((2,2),(1,3)\big).$$

with the principal reversible matrices

$$\mathcal{M}^\nu = \begin{pmatrix} 0 & 1 & 2 \\ 3 & 4 & 5 \end{pmatrix}, \quad \text{and} \quad \mathcal{N}^\nu = \begin{pmatrix} 0 & 2 & 4 \\ 1 & 3 & 5 \end{pmatrix}.$$

For either $\kappa \in \{1, 2\}$, we have the constants

$$F^\nu := F(\kappa; 3) = 6, \qquad P_1^\nu := P_1(\kappa; 3) = 3 \quad \text{and} \quad P_2^\nu := P_2(\kappa; 3) = 2.$$

Lemma 8.1.12. Assume (H3). Let $\hat{M} \in \langle F^\nu \rangle$ be an integer from the target set of the sum system correspond to $\mathcal{F}_\kappa^\nu$, for $\kappa \in \{1, 2\}$. Then the address of $\hat{M}$ in $\mathcal{F}_\kappa$ and $\mathcal{F}_\kappa^\nu$ are related by

$$\alpha(\hat{M}) = \gamma(\hat{M}) \, \oplus \, 0_{\Omega(N)+1-\nu} = (\gamma_1, \ldots, \gamma_\nu, 0, \ldots, 0),$$

where $\oplus$ is the direct sum of two vectors. Furthermore, we can associate each $M \in \langle N \rangle$ with a unique pair $(\hat{M}, s)$, for $s \in \langle \frac{N}{F^\nu} \rangle$, such that

$$M = \hat{M} + F^\nu s.$$

Proof. The $\Omega(N)+1-\nu$ pairs removed in $\mathcal{F}_\kappa^\nu$ form their own joint ordered factorisation, with the target set $\langle \frac{N}{F^\nu} \rangle$. We can alternatively state that this new joint ordered factorisation is the result of removing the first ν pairs, akin to how we formulated ${}^\mu\mathcal{F}_\kappa$, which we denote ${}^\nu\mathcal{F}_\kappa$. An important difference is that ${}^\nu\mathcal{F}_1 = {}^\nu\mathcal{F}_2$ since the last $\Omega + 1 - \nu$ pairs are equal between $\mathcal{F}_1$ and $\mathcal{F}_2$. Nevertheless, we can use the same argument for the proof of Lemma 8.1.5 with $\tilde{M} = s$ and F^ν instead of ${}^\mu F$ to show that $\alpha(F^\nu s) = 0_\nu \oplus \beta(s) = (0, \ldots, 0, \beta_1, \ldots, \beta_{\Omega(N)+1-\nu})$.

Using Eq. (6.1) on $\hat{M}$ in $\mathcal{F}_\kappa^\nu$, we can write

$$\begin{aligned}
\hat{M} = \gamma(\hat{M}) \begin{pmatrix} F(\kappa;1) \\ \vdots \\ F(\kappa;\nu) \end{pmatrix} &= \gamma_1 F^\nu(\kappa;1) + \cdots + \gamma_\nu F^\nu(\kappa;\nu) \\
&= \gamma_1 F(\kappa;1) + \cdots + \gamma_\nu F(\kappa;\nu) + 0F(\kappa;\nu+1) + \cdots + 0F(\kappa;\Omega(N)) \\
&= (\gamma_1, \ldots, \gamma_\nu, 0, \ldots, 0)\overrightarrow{F(\kappa)} \\
&= \gamma(\hat{M}) \ \oplus \ 0_{\Omega(N)+1-\nu} \ \overrightarrow{F(\kappa)} = \alpha(\hat{M})\overrightarrow{F(\kappa)}.
\end{aligned}$$

By equating address tuples in the final line we deduce $\alpha(\hat{M}) = \gamma(\hat{M}) \ \oplus \ 0_{\Omega(N)+1-\nu}$.

Therefore, we can write $\alpha(\hat{M} + F^\nu s) = \alpha(\hat{M}) + \alpha(F^\nu s)$ which we use to write

$$\begin{aligned}
M = \alpha(M)\overrightarrow{F(\kappa)} &= (\alpha_1, \ldots, \alpha_\nu, \alpha_{\nu+1}, \ldots, \alpha_{\Omega(N)})\overrightarrow{F(\kappa)} \\
&= \Big((\alpha_1, \ldots, \alpha_\nu) \oplus 0_{\Omega(N)+1-\nu} + 0_\nu \oplus (\alpha_{\nu+1}, \ldots, \alpha_{\Omega(N)})\Big)\overrightarrow{F(\kappa)} \\
&= \big(\alpha(\hat{M}) + \alpha(F^\nu s)\big)\overrightarrow{F(\kappa)} = \hat{M} + F^\nu s,
\end{aligned}$$

as required. □

Lemma 8.1.13. Assume (H3). Let $\mathcal{F}_1$ and $\mathcal{F}_2$ have the principal reversible cuboids $\mathcal{M}$ and $\mathcal{N}$. Let $\hat{M} \in \langle F^\nu \rangle$ be an integer from the target set of the sum system corresponding to $\mathcal{F}_1^\nu$ and $\mathcal{F}_2^\nu$, which have the principal reversible cuboids $\mathcal{M}^\nu$ and $\mathcal{N}^\nu$. Let $s \in \langle \frac{N}{F^\nu} \rangle$. Then $F^\nu s \in \langle N \rangle$ is a fixed point between $\mathcal{F}_1$ and $\mathcal{F}_2$, such that

$$C_{\mathcal{F}_1}\big(F^\nu s\big) = C_{\mathcal{F}_2}\big(F^\nu s\big).$$

Furthermore, for $\kappa \in \{1,2\}$, the position of $M = \hat{M} + F^n us \in \langle N \rangle$ in either $\mathcal{M}$ and $\mathcal{N}$ can be expressed as

$$C_{\mathcal{F}_\kappa}(M) = C_{\mathcal{F}_\kappa}\big(\hat{M}\big) + C_{\mathcal{F}_\kappa}\big(F^\nu s\big).$$

Proof. As the last $\Omega(N) + 1 - \nu$ pairs in $\mathcal{F}_1$ and $\mathcal{F}_2$ are the same, for $0 \leq l \leq \Omega(N) - \nu$ we have

$$P_j(1; \nu + l) = \prod_{\substack{h \in \mathcal{L}_j(1) \\ h < \nu + l}} p_h^{(1)} = P_j^\nu \prod_{\substack{h \in \mathcal{L}_j(1) \\ \nu < h < \nu + l}} p_h^{(1)} = P_j^\nu \prod_{\substack{h \in \mathcal{L}_j(2) \\ \nu < h < \nu + l}} p_h^{(2)} = P_j(2; \nu + l).$$

Therefore, we can write

$$\begin{aligned} C_{\mathcal{F}_1}(F^\nu s) = \alpha(F^\nu s)\overrightarrow{P(1)} &= \alpha_\nu P_{j_\nu}(1;\nu)\bar{e}_{j_\nu} + \cdots + \alpha_{\Omega(N)} P_{j_{\Omega(N)}}(1;\Omega(N))\bar{e}_{j_{\Omega(N)}} \\ &= \alpha_\nu P_{j_\nu}(2;\nu)\bar{e}_{j_\nu} + \cdots + \alpha_{\Omega(N)} P_{j_{\Omega(N)}}(2;\Omega(N))\bar{e}_{j_{\Omega(N)}} \\ &= \alpha(F^\nu s)\overrightarrow{P(2)} = C_{\mathcal{F}_2}(F^\nu s). \end{aligned}$$

We deduce that $F^\nu s$ is a fixed point since

$$O_{\mathcal{F}_1,\mathcal{F}_2}(F^\nu s) = \mathcal{N}_{C_{\mathcal{F}_1}(F^\nu s)} = \mathcal{N}_{C_{\mathcal{F}_2}(F^\nu s)} = F^\nu s.$$

Furthermore, we can write

$$\begin{aligned} C_{\mathcal{F}_\kappa}(M) = C_{\mathcal{F}_\kappa}\big(\hat{M} + F^\nu s\big) &= \alpha\big(\hat{M} + F^\nu s\big)\overrightarrow{P(\kappa)} \\ &= \Big(\alpha\big(\hat{M}\big) + \alpha\big(F^\nu s\big)\Big)\overrightarrow{P(\kappa)} = C_{\mathcal{F}_\kappa}(\hat{M}) + C_{\mathcal{F}_\kappa}(F^\nu s), \end{aligned}$$

as required. □

Lemma 8.1.14. Assume (H3). Let $\hat{M} \in \langle F^\nu \rangle$ be an integer from the target set of the sum system corresponding to $\mathcal{F}_\kappa^\nu$, for $\kappa \in \{1,2\}$. For $s \in \langle \frac{N}{F^\nu} \rangle$, let $M = \hat{M} + F^\nu s \in \langle N \rangle$ be an integer from the target set of the sum system corresponding to $\mathcal{F}_\kappa$. Then the raising operator of M between $\mathcal{F}_1$ and $\mathcal{F}_2$ is related to the raising operator of $\hat{M}$ between $\mathcal{F}_1^\nu$ and $\mathcal{F}_2^\nu$ by the identity

$$O_{\mathcal{F}_1,\mathcal{F}_2}(M) = M^{(1)} = O_{\mathcal{F}_1^\nu,\mathcal{F}_2^\nu}(\hat{M}) + F^\nu s = \hat{M}^{(1)} + F^\nu s.$$

Proof. Because the first F^ν integers form cyclic orbits between $\mathcal{F}_1^\nu$ and $\mathcal{F}_2^\nu$, then it must be true that $O_{\mathcal{F}_1^\nu,\mathcal{F}_2^\nu}(\hat{M}) \in \langle F^\nu \rangle$. Adding the removed pairs back on to the end of $\mathcal{F}_\kappa^\nu$ will not change the positions of these first F^ν integers, nor their cyclic orbits, and therefore

$\hat{M}^{(1)} = O_{\mathcal{F}_1^\nu,\mathcal{F}_2^\nu}(\hat{M}) = O_{\mathcal{F}_1,\mathcal{F}_2}(\hat{M})$. This has the inverse map $\hat{M} = \mathcal{M}_{C_{\mathcal{F}_2}(\hat{M}^{(1)})}$ which enables us to write $C_{\mathcal{F}_1}(\hat{M}) = C_{\mathcal{F}_1}\big(\mathcal{M}_{C_{\mathcal{F}_2}(\hat{M}^{(1)})}\big) = C_{\mathcal{F}_2}\big(\hat{M}^{(1)}\big)$. Therefore

$$M^{(1)} = O_{\mathcal{F}_1,\mathcal{F}_2}(M) = \mathcal{N}_{C_{\mathcal{F}_1}(M)} = \mathcal{N}_{C_{\mathcal{F}_1}(\hat{M})} + \mathcal{N}_{C_{\mathcal{F}_1}(F^\nu s)} = \mathcal{N}_{C_{\mathcal{F}_2}(\hat{M}^{(1)})} + F^\nu s = \hat{M}^{(1)} + F^\nu s,$$

as required. □

Theorem 8.1.15. Assume (H3). Let $\hat{M} \in \langle F^\nu \rangle$ be an integer from the target set of the sum system corresponding to $\mathcal{F}_\kappa^\nu$, for $\kappa \in \{1,2\}$. For $s \in \langle \frac{N}{F^\nu} \rangle$, let $M = \hat{M} + F^\nu s \in \langle N \rangle$ be an integer from the target set of the sum system corresponding to $\mathcal{F}_\kappa$. Then the cyclic orbit of M between $\mathcal{F}_1$ and $\mathcal{F}_2$ is related to the cyclic orbit of $\hat{M}$ between $\mathcal{F}_1^\nu$ and $\mathcal{F}_2^\nu$ by the identity

$$\mathcal{O}_{\mathcal{F}_1,\mathcal{F}_2}(M) = \mathcal{O}_{\mathcal{F}_1^\nu,\mathcal{F}_2^\nu}(\hat{M}) + F^\nu s.$$

Proof. For $t \in \langle d \rangle$, after t applications of Lemma 8.1.14 to $O_{\mathcal{F}_1,\mathcal{F}_2}(M)$, we get

$$M^{(t)} = (O_{\mathcal{F}_1,\mathcal{F}_2})^t(M) = \hat{M}^{(t)} + F^\nu s,$$

which enables us to write

$$\begin{aligned}\mathcal{O}_{\mathcal{F}_1,\mathcal{F}_2}(M) =& \Big\{M^{(0)}, M^{(1)}, \dots, M^{(d-1)}\Big\}\\ =& \Big\{\hat{M}^{(0)} + F^\nu s,\ \hat{M}^{(1)} + F^\nu s,\ \dots,\ \hat{M}^{(d-1)} + F^\nu s\Big\}\\ =& \Big\{\hat{M}^{(0)},\ \hat{M}^{(1)},\ \dots,\ \hat{M}^{(d-1)}\Big\} + F^\nu s = \mathcal{O}_{\mathcal{F}_1^\nu,\mathcal{F}_2^\nu}(\hat{M}) + F^\nu s,\end{aligned}$$

as required. □

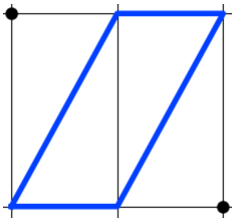
This relation effectively takes the cyclic orbit structure between $\mathcal{F}_1^\nu$ and $\mathcal{F}_2^\nu$ and copies it in the j_ℓth coordinate axis direction p_l times, for (j_l, p_l) in $\mathcal{F}_\kappa$ for $l \geq \nu$.

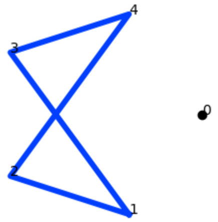
Example 8.1.16. Let us continue Example 8.1.11, with $\mathcal{F}_1 = \big((1,3),(2,2),(1,2),(2,3)\big)$ and $\mathcal{F}_2 = \big((2,2),(1,3),(1,2),(2,3)\big)$. Here we had $\nu = 3$ such that $\mathcal{F}_1^\nu = \big((1,3),(2,2)\big)$ and $\mathcal{F}_2^\nu = \big((2,2),(1,3)\big)$, the same as found in Example 8.1.9. Note that $N = 36$ and $F^\nu = 6$.

By Theorem 8.1.12 we can write $M \in \langle 36 \rangle$ as $M = \hat{M} + 6s$, for some $\hat{M} \in \langle F^\nu \rangle = \langle 6 \rangle$ and $s \in \langle \frac{N}{F^\nu} \rangle = \langle 6 \rangle$, and by Theorem 8.1.15 we have $\mathcal{O}_{\mathcal{F}_1,\mathcal{F}_2}(M) = \mathcal{O}_{\mathcal{F}_1^\nu,\mathcal{F}_2^\nu}(\tilde{M}) + 6s$. For example, letting $M = 19 = 1 + 6 \times 3$ and using Theorem 8.1.15, we have

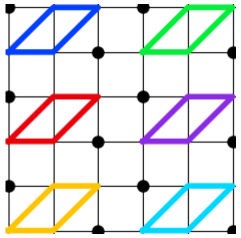
$$\mathcal{O}_{\mathcal{F}_1,\mathcal{F}_2}(19) = \mathcal{O}_{\mathcal{F}_1^\nu,\mathcal{F}_2^\nu}(1) + 18 = \{1,2,4,3\} + 18 = \{19,20,22,21\}.$$

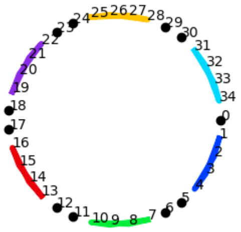
We can write the full orbit permutation $\sigma_{\mathcal{F}_1^\nu,\mathcal{F}_2^\nu} = (0)\,(1\;2\;4\;3)\,(5)$ which have the cuboid and ring geometries





The full orbit permutation $\sigma_{\mathcal{F}_1,\mathcal{F}_2}$ has the cuboid and ring geometries





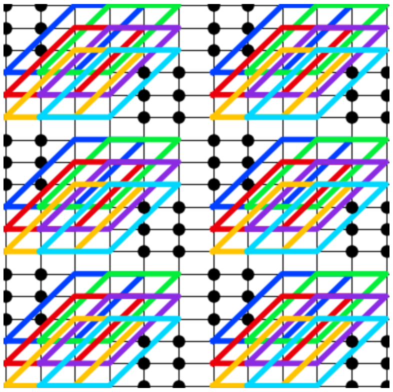
The orbits within $\sigma_{\mathcal{F}_1^\nu,\mathcal{F}_2^\nu}$ can be seen within the orbits in $\sigma_{\mathcal{F}_1,\mathcal{F}_2}$. We make $F^\nu = 6$ copies of each cyclic orbit in $\sigma_{\mathcal{F}_1^\nu,\mathcal{F}_2^\nu}$. There are $f_3 = 2$ copies in the $j_3 = 1$st coordinate axis direction (going right), and $f_4 = 3$ copies in the $j_4 = 2$nd coordinate axis direction (going down). Note that $\mathcal{O}_{\mathcal{F}_1,\mathcal{F}_2}(19)$ is depicted as the purple line in the cuboid and ring geometries of $\sigma_{\mathcal{F}_1,\mathcal{F}_2}$

8.1.3 Case 3: $1 \leq \mu < \nu \leq \Omega(N)$

If $1 \leq \mu < \nu \leq \Omega(N)$, then the first μ pairs and last $\Omega(N) + 1 - \nu$ pairs in $\mathcal{F}_1$ and $\mathcal{F}_2$ will be the same. In this case we have a combination of both Theorem 8.1.8 and Theorem 8.1.15 where we consider ${}^\mu\mathcal{F}_\kappa^\nu$ to be the resulting joint ordered factorisation after removing the first μ, and last $\Omega(N) + 1 - \nu$, pairs of $\mathcal{F}_\kappa$, such that

$${}^\mu\mathcal{F}_\kappa^\nu = \Big(\big(j_{\mu+1}^{(\kappa)}, p_{\mu+1}^{(\kappa)}\big), \ldots, \big(j_{\nu-1}^{(\kappa)}, p_{\nu-1}^{(\kappa)}\big)\Big).$$

Example 8.1.17. By considering a combination of Example 8.1.9 and Example 8.1.16, take the full joint ordered factorisations $\mathcal{F}_1 = \big((1,2),(2,3),(2,2),(1,3),(1,2),(2,3)\big)$ and $\mathcal{F}_2 = \big((1,2),(2,3),(1,3),(2,2),(1,2),(2,3)\big)$. In this case, we have $\mu = 2$ and $\nu = 5$, such that ${}^\mu\mathcal{F}_1^\nu = \big((2,2),(1,3)\big)$ and ${}^\mu\mathcal{F}_2^\nu = \big((1,3),(2,2)\big)$. The full orbit permutation $\sigma_{\mathcal{F}_1,\mathcal{F}_2}$ has the geometric representation



which is fundamentally the full orbit permutation from Example 8.1.9, repeated 6 times as in Example 8.1.16.

8.2 Specific examples of orbit structure

Because an explicit expression for a cyclic orbit depends so heavily on the given joint ordered factorisations, we are unable to retrieve many general properties about the raising operators used in such a description. The remainder of this chapter shall detail the orbit structure between two generalised joint ordered factorisations with a certain number of pairs in either expression, but once again in 2-dimensions.

In Chapter 7 we saw how the cyclic orbits between two joint ordered factorisations written in their most simplest form was entirely described via their raising operators. We shall see that once these joint ordered factorisations contain more than 2 pairs, the raising operator is no longer enough to fully predict the cyclic orbits.

For two joint ordered factorisation $\mathcal{J}_1$ and $\mathcal{J}_2$, we denote the number of pairs in their tuples by L_1 and L_2 respectively. In the previous chapter we had $L_1 = L_2 = 2$. We shall consider the select cases

$$(L_1, L_2) \in \big\{(3,2),\ (3,3),\ (4,2),\ (4,3)\big\}.$$

Note that $(L_1, L_2) = (X, Y)$ will correspond to the same system as $(L_1, L_2) = (Y, X)$, for $X, Y \in \mathbb{N}$.

No additional cases are presented, such as $L_1 = L_2 = 4$, because, as we will see, the systems become less and less wieldy, describing less and less of the structure.

8.2.1 $L_1 = 3$ and $L_2 = 2$

Let $n = (f_1 f_3, f_2) \in \mathbb{N}_2^2$ with $\mathcal{J}_1$ and $\mathcal{J}_2$ joint ordered factorisations of n with 3 pairs and 2 pairs respectively. There are only two configurations that $\mathcal{J}_1$ and $\mathcal{J}_2$ can each take, which are

$$\mathcal{J}_1 : \quad \big((1, f_1), (2, f_2), (1, f_3)\big) \quad \text{or} \quad \big((1, f_3), (2, f_2), (1, f_1)\big),$$

$$\mathcal{J}_2 : \quad \big((1, f_1 f_3), (2, f_2)\big) \quad \text{or} \quad \big((2, f_2), (1, f_1 f_3)\big).$$

For all four combinations of $\mathcal{J}_1$ and $\mathcal{J}_2$ we have that either $\mu = 1$ or $\nu = 3$, i.e. the first pair or last pair are the same. By Theorem 8.1.8 and Theorem 8.1.15, we know these systems mimic the orbit between reduced joint ordered factorisations with length 2.

For example, let $\mathcal{J}_1 = \big((1, f_1), (2, f_2), (1, f_3)\big)$ and $\mathcal{J}_2 = \big((1, f_1 f_3), (2, f_2)\big)$. Then $\mu = 1$ and $\sigma_{\mathcal{J}_1, \mathcal{J}_2}$ mimics the full orbit permutation $\sigma_{{}^{\mu}\mathcal{J}_1, {}^{\mu}\mathcal{J}_2}$ where we have ${}^{\mu}\mathcal{J}_1 = \big((2, f_2), (1, f_3)\big)$ and ${}^{\mu}\mathcal{J}_2 = \big((1, f_3), (2, f_2)\big)$.

As these structures were analysed in Chapter 7, we need not repeat the findings here. Though it is noteworthy that all length 3 and length 2 joint ordered factorisations reduce to this case.

8.2.2 $L_1 = L_2 = 3$

There are two pairs of joint ordered factorisations such that $L_1 = L_2 = 3$, $\mu = 0$ and $\nu > 3$. For $f_1, f_2, f_3, f_4 \in \mathbb{N}$, these pairs are

$$\mathcal{J}_1 = \big((1, f_1), (2, f_2), (1, f_3)\big) \qquad \text{and} \qquad \mathcal{J}_2 = \big((1, f_3), (2, f_2), (1, f_1)\big),$$

and

$$\mathcal{J}_3 = \big((1, f_1), (2, f_2 f_4), (1, f_3)\big) \qquad \text{and} \qquad \mathcal{J}_4 = \big((2, f_2), (1, f_1 f_3), (2, f_4)\big).$$

Any other $\mathcal{J}$ with 3 pairs can be described as either a permutation of the j-values, the f-values, or both, in the above configurations. We first consider $\mathcal{J}_1$ and $\mathcal{J}_2$.

Case 1: $\mathcal{J}_1$ and $\mathcal{J}_2$

With the explicit expressions given for $\mathcal{J}_1$ and $\mathcal{J}_2$, we are able to find a closed form for the raising operator and cyclic orbit set. In what follows, we will assume the following hypothesis statement.

Hypothesis statement 4 (H4): Let $n = (f_1 f_3, f_2) \in \mathbb{N}_2^2$ with $\gcd(f_1, f_3) = 1$, $N = f_1 f_2 f_3$, and consider the joint ordered factorisations of n of the form

$$\mathcal{J}_1 = \big((1, f_1), (2, f_2), (1, f_3)\big), \quad \text{and} \quad \mathcal{J}_2 = \big((1, f_3), (2, f_2), (1, f_1)\big).$$

Let $M \in \langle N \rangle$ have the cyclic orbit $\mathcal{O}_{\mathcal{J}_1,\mathcal{J}_2}(M) = \mathcal{O}(M)$ of length $d \in \mathbb{N}$. For $t \in \langle d \rangle$, denote the t-th element of $\mathcal{O}(M)$ with $M^{(t)}$, and note that we use $M = M^{(0)}$ interchangeably. Let the raising operator be given by $O_{\mathcal{J}_1,\mathcal{J}_2}\big(M^{(t)}\big) = O\big(M^{(t)}\big) = M^{(t+1)}$.

We write the address of $M^{(t)}$ with respect to $\mathcal{J}_1$ as $\alpha(M^{(t)}) = \big(\alpha_{1,1}^{(t)}, \alpha_2^{(t)}, \alpha_{1,2}^{(t)}\big)$, and with respect to $\mathcal{J}_2$ as $\beta(M^{(t)}) = \big(\beta_{1,1}^{(t)}, \beta_2^{(t)}, \beta_{1,2}^{(t)}\big)$. Note that we have opted to write $\alpha_2^{(t)}$ instead of $\alpha_{2,1}^{(t)}$ to reduce notation, and likewise for $\beta_2^{(t)}$.

Lemma 8.2.1. Assume (H4). The raising operator of $M^{(t)}$ is given by

$$\begin{aligned} O\big(M^{(t)}\big) = M^{(t+1)} &= \alpha_{1,1}^{(t)} + f_3 \alpha_2^{(t)} + f_1 \alpha_{1,2}^{(t)} + f_3(f_2 - 1)\beta_{1,2}^{(t+1)} && (8.3) \\ &= f_2 \alpha_{1,1}^{(t)} + f_3 \alpha_2^{(t)} + f_1 f_2 \alpha_{1,2}^{(t)} - (f_2 - 1)\beta_{1,1}^{(t+1)} && (8.4) \\ &= (f_2 + 1)\alpha_{1,1}^{(t)} + f_3 \alpha_2^{(t)} + f_1(f_2 + 1)\alpha_{1,2}^{(t)} - \big(f_2 \beta_{1,1}^{(t+1)} + f_3 \beta_{1,2}^{(t+1)}\big). && (8.5) \end{aligned}$$

Proof. The system of questions in (6.3) reduces to

$$\alpha_{1,1}^{(t)} + f_1 \alpha_2^{(t)} + f_1 f_2 \alpha_{1,2}^{(t)} = M^{(t)} = \beta_{1,1}^{(t)} + f_3 \beta_2^{(t)} + f_2 f_3 \beta_{1,2}^{(t)},$$

$$\alpha_{1,1}^{(t)} + f_1 \alpha_{1,2}^{(t)} = \beta_{1,1}^{(t+1)} + f_3 \beta_{1,2}^{(t+1)},$$

$$\alpha_2^{(t)} = \beta_2^{(t+1)}.$$

Eq. (8.3) follows by substituting the latter two equations into the left hand side of the first equation and rearranging. Eq. (8.4) follows from substituting $f_3 \beta_{1,2}^{(t+1)} = \alpha_{1,1}^{(t)} + f_1 \alpha_{1,2}^{(t)} - \beta_{1,1}^{(t+1)}$ into Eq. (8.3). Eq. (8.5) follows from summing the Eq. (8.3) and Eq. (8.4). □

We are unable to remove all terms corresponding to either α or β in the equations of Lemma 8.2.1, which means $O\big(M^{(t)}\big)$ depends on the address of $M^{(t)}$ in both $\mathcal{J}_1$ and $\mathcal{J}_2$.

Lemma 8.2.2. Assume (H4). Then the raising operator of $M^{(t)}$ follows the recurrence relation

$$\begin{aligned} O\big(M^{(t)}\big) = M^{(t+1)} &= M^{(t)} + (f_3 - f_1)\alpha_2^{(t)} + (f_2 - 1)\Big(f_3\beta_{1,2}^{(t+1)} - f_1\alpha_{1,2}^{(t)}\Big) \\ &= M^{(t)} + (f_3 - f_1)\alpha_2^{(t)} + (f_2 - 1)\Big(\alpha_{1,1}^{(t)} - \beta_{1,1}^{(t+1)}\Big) \\ &= M^{(t)} + f_2\alpha_{1,1}^{(t)} + (f_3 - f_1)\alpha_2^{(t)} + f_1\alpha_{1,2}^{(t)} - \big(f_2\beta_{1,1}^{(t+1)} + f_3\beta_{1,2}^{(t+1)}\big). \end{aligned}$$

Proof. These equations follow from factoring out the terms $\alpha_{1,1}^{(t)} + f_1\alpha_2^{(t)} + f_1f_2\alpha_{1,2}^{(t)} = M^{(t)}$ in each of the equations in Lemma 8.2.1 and rearranging. □

The equations of Lemma 8.2.2 introduces an additional variable to those in Lemma 8.2.1. Though the equations in Lemma 8.2.1 will be quicker to calculate, the equations of Lemma 8.2.2 enables us to compare two consecutive terms in $\mathcal{O}\big(M\big)$.

Importantly, in any of these formulae for $O\big(M^{(t)}\big) = M^{(t+1)}$ we are unable to remove all terms with index $t+1$. This implies $O\big(M^{(t)}\big)$ requires information about $M^{(t+1)}$ to calculate $M^{(t+1)}$. Therefore, these equations are unable to give a complete description of the cyclic orbit $\mathcal{O}\big(M\big)$.

A tool we will find useful in analysing cyclic orbits is to turn the raising operator into a congruence relation. We can express Eq. (8.3) as

$$\begin{aligned} O\big(M^{(t)}\big) = M^{(t+1)} &\equiv \alpha_{1,1}^{(t)} + f_3\alpha_2^{(t)} + f_1\alpha_{1,2}^{(t)} \pmod{f_3(f_2 - 1)} \\ &\equiv M^{(t)} + (f_3 - f_1)\alpha_2^{(t)} - f_1(f_2 - 1)\alpha_{1,2}^{(t)} \pmod{f_3(f_2 - 1)}. \end{aligned} \tag{8.6}$$

These equations have removed all terms with index $t + 1$, which implies we can describe $O(M^{(t)}) = M^{(t+1)}$ without needing information on $M^{(t+1)}$ itself. Unfortunately, any value $M > f_3(f_2-1)$ will be incorrectly reduced, and thus this congruence relation will not provide a full descriptor for $\mathcal{O}(M)$. However, we may introduce a process to generate the orbit by calculating Eq. (8.6) and checking the result against Eq. (8.5).

The following lemma establishes an algorithm that generates the cyclic orbit of some integer $M \in \langle N\rangle$ when the number of pairs in the two given joint ordered factorisations is more than 2.

Lemma 8.2.3 (Algorithm)**.** Assume (H4). We can generate the raising operator $O(M^{(t)})$ using the following process:

1. Compute the term

$$M_a \equiv \alpha_{1,1}^{(t)} + f_3\alpha_2^{(t)} + f_1\alpha_{1,2}^{(t)} \pmod{f_3(f_2-1)}.$$

2. Substitute $\alpha(M^{(t)}) = \big(\alpha_{1,1}^{(t)}, \alpha_2^{(t)}, \alpha_{1,2}^{(t)}\big)$ and $\beta(M_a) = \big(\beta_{1,1}^{(t+1)}, \beta_2^{(t+1)}, \beta_{1,2}^{(t+1)}\big)$ into

$$M_a = (f_2+1)\alpha_{1,1}^{(t)} + f_3\alpha_2^{(t)} + f_1(f_2+1)\alpha_{1,2}^{(t)} - \big(f_2\beta_{1,1}^{(t+1)} + f_3\beta_{1,2}^{(t+1)}\big).$$

3. If this equality is not satisfied, return to step 2 and use $M_a = M_a + f_3(f_2-1)$.

4. Otherwise, $M_a = M^{(t+1)} = O\big(M^{(t)}\big)$.

Note that $\beta(M_a)$ is the address of M_a with respect to $\mathcal{J}_2$.

Proof. For the algorithm to give a false positive, i.e. $M_a \neq M^{(t+1)}$ but the algorithm identified $M_a = O(M^{(t)})$, then Eq. (8.5) must be satisfied. This can only occur when

$$\beta(M_a) = \big(\beta_{1,1}^{(t+1)}, \tilde{\beta}_2^{(t+1)}, \beta_{1,2}^{(t+1)}\big), \qquad \text{and} \qquad \beta\big(M^{(t+1)}\big) = \big(\beta_{1,1}^{(t+1)}, \beta_2^{(t+1)}, \beta_{1,2}^{(t+1)}\big).$$

But because $\beta_2^{(t+1)} = \alpha_2^{(t)} = \tilde{\beta}_2^{(t+1)}$, then the address of M_a and $M^{(t+1)}$ in $\mathcal{J}_2$ are the same, and thus $M_a = M^{(t+1)}$. □

Example 8.2.4. Let $\mathcal{J}_1 = \big((1,3),(2,3),(1,5)\big)$ and $\mathcal{J}_2 = \big((1,5),(2,3),(1,3)\big)$ be two joint ordered factorisations. We can write Eq. (8.5) as

$$O\big(M^{(t)}\big) = M^{(t+1)} = 4\alpha_{1,1}^{(t)} + 5\alpha_2^{(t)} + 12\alpha_{1,2}^{(t)} - \big(3\beta_{1,1}^{(t+1)} + 5\beta_{1,2}^{(t+1)}\big). \tag{8.7}$$

The first non-fixed point is $M = M^{(0)} = 3$.

To continue we use the algorithm outlined in Lemma 8.2.3, with the congruence relation

$$M_a \equiv \alpha_{1,1}^{(t)} + 5\alpha_2^{(t)} + 3\alpha_{1,2}^{(t)} \pmod{10}.$$

Starting with $M = 3$, we have $\alpha(3) = (0,1,0)$, which step 1 gives us $M_a \equiv 0+5\times1+3\times0 \equiv 5 \pmod{10}$, with $\beta(5) = (0,1,0)$. For step 2, plugging these addresses into Eq. (8.7), we calculate $0+5+0-(0+0) = 5 = M_a$, and thus $M_a = M^{(1)} = 5$.

Next, with $\alpha(5) = (2,1,0)$, step 1 gives us $M_a \equiv 2 + 5 \times 1 + 3 \times 0 \equiv 7 \pmod{10}$, with $\beta(7) = (2,1,0)$. For step 2, plugging these addresses into Eq. (8.7), we calculate $8 + 5 + 0 - (6+0) = 7 = M_a$, and thus $M_a = M^{(2)} = 7$.

With $\alpha(7) = (1,2,0)$, step 1 gives us $M_a \equiv 1 + 5 \times 2 + 3 \times 0 = 11 \equiv 1 \pmod{10}$, with $\beta(1) = (1,0,0)$. For step 2, plugging these addresses into Eq. (8.7), we calculate $4 + 10 + 0 - 3 = 11 \neq M_a$, and thus $M^{(3)} \neq 1$. Adding 10, we have $M_a = 11$, with $\beta(11) = (1,2,0)$. Evaluating step 2 again returns $4 + 10 + 0 - 3 = 11 = M_a$ and so step 4 informs us that $M^{(3)} = 11$.

Continuing with $\alpha(11) = (2,0,1)$, step 1 gives $M_a \equiv 2 + 0 + 3 \equiv 5 \pmod{10}$. As 5 is already part of the orbit and is not the starting term, we can move to step 3 and add 10, such that $M_a = 5 + 10 = 15$. We then evaluate Eq. (8.7) with $\beta(15) = (0,0,1)$ which is satisfied, and thus $M^{(4)} = 15$.

Next, with $\alpha(15) = (0,2,1)$ we find $M_a \equiv 0 + 10 + 3 = 13 \equiv 3 \pmod{10}$. It is possible that this value is true, which implies the orbit ends here with order 4. But computing step 2, with $\beta(3) = (3,0,0)$, tells us that $0 + 10 + 12 - (9+0) = 13 \neq M_a$, thus is it not correct and the orbit carries on. Adding 10 and repeating, we confirm that $M^{(5)} = 13$.

The next term is $M^{(6)} = 9$, and then $M^{(7)} \equiv 9 + 0 - 6 = 3 \pmod{10}$. By carrying out the algorithm we can confirm that $M^{(7)} = 3$, and thus the cyclic orbit ends with length 7.

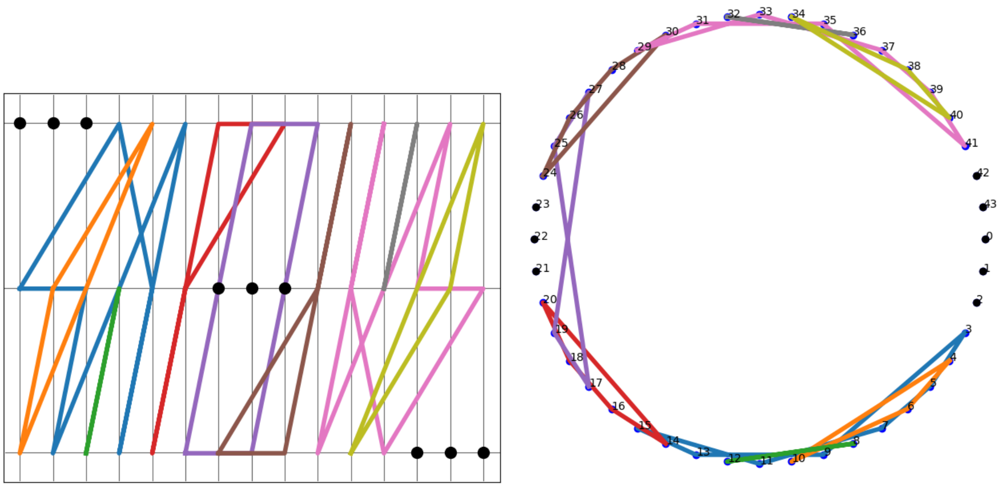
The full cyclic orbit is $\mathcal{O}(3) = \{3, 5, 7, 11, 15, 13, 9\}$. The address of each term in $\mathcal{J}_1$ and $\mathcal{J}_2$ is found in the table below.

$M^{(t)}$	3	5	7	11	15	13	9
$\alpha(M^{(t)})$	$(0,1,0)$	$(2,1,0)$	$(1,2,0)$	$(2,0,1)$	$(0,2,1)$	$(1,1,1)$	$(0,0,1)$
$\beta(M^{(t)})$	$(3,0,0)$	$(0,1,0)$	$(2,1,0)$	$(1,2,0)$	$(0,0,1)$	$(3,2,0)$	$(4,1,0)$

The full orbit permutation $\sigma_{\mathcal{J}_1,\mathcal{J}_2}$ is given by

$$\begin{aligned}\sigma_{\mathcal{J}_1,\mathcal{J}_2} = {} & (0)\,(1)\,(2)\,(3\;\;5\;\;7\;\;11\;\;15\;\;13\;\;9)\,(4\;\;6\;\;10)\,(8\;\;12)\,(14\;\;20\;\;18\;\;16)\,(17\;\;25\;\;27\;\;19)\\ & (21)\,(22)\,(23)\,(24\;\;26\;\;28\;\;30)\,(29\;\;31\;\;35\;\;41\;\;39\;\;37\;\;33)\\ & (32\;\;36)\,(34\;\;40\;\;38)\,(42)\,(43)\,(44),\end{aligned}$$

and has the geometric visualisations



where we can see that $\mathcal{O}(3)$ is the blue line.

Case 2: $\mathcal{J}_3$ and $\mathcal{J}_4$

Now let $n = (f_1f_3, f_2f_4) \in \mathbb{N}_2^2$ and consider the remaining two joint ordered factorisations of n

$$\mathcal{J}_3 = \big((1, f_1), (2, f_2f_4), (1, f_3)\big), \quad \text{and} \quad \mathcal{J}_4 = \big((2, f_2), (1, f_1f_3), (2, f_4)\big).$$

We will see that this case is remarkably similar to Case 1.

Lemma 8.2.5. Let $n = (f_1f_3, f_2f_4) \in \mathbb{N}_2^2$, with $N = f_1f_2f_3f_4$, and consider the two joint ordered factorisations $\mathcal{J}_3 = \big((1, f_1), (2, f_2f_4), (1, f_3)\big)$ and $\mathcal{J}_4 = \big((2, f_2), (1, f_1f_3), (2, f_4)\big)$. Let $M \in \langle N\rangle$ have the cyclic orbit $\mathcal{O}_{\mathcal{J}_3,\mathcal{J}_4}(M) = \mathcal{O}(M)$ of length $d \in \mathbb{N}$, and let $M^{(t)} \in \mathcal{O}(M)$ be the t-th element, for $t \in \langle d\rangle$, with $O_{\mathcal{J}_3,\mathcal{J}_4}\big(M^{(t)}\big) = O\big(M^{(t)}\big) = M^{(t+1)}$ be the raising operator. We write the address of $M^{(t)}$ with respect to $\mathcal{J}_3$ as $\alpha\big(M^{(t)}\big) = \big(\alpha^{(t)}_{1,1}, \alpha^{(t)}_{2,1}, \alpha^{(t)}_{1,2}\big)$, and with respect to $\mathcal{J}_4$ as $\beta\big(M^{(t)}\big) = \big(\beta^{(t)}_{2,1}, \beta^{(t)}_{1,1}, \beta^{(t)}_{2,2}\big)$.

Then the raising operator of $M^{(t)}$ is given by

$$\begin{aligned} O\big(M^{(t)}\big) = M^{(t+1)} &= f_2\alpha^{(t)}_{1,1} + \alpha^{(t)}_{2,1} + f_1f_2\alpha^{(t)}_{1,2} + f_2(f_1f_3 - 1)\beta^{(t+1)}_{2,2} && (*) \\ &= f_2\alpha^{(t)}_{1,1} + f_1f_3\alpha^{(t)}_{2,1} + f_1f_2\alpha^{(t)}_{1,2} - (f_1f_3 - 1)\beta^{(t+1)}_{2,1} && (**) \\ &= f_2\alpha^{(t)}_{1,1} + (f_1f_3 + 1)\alpha^{(t)}_{2} + f_1f_2\alpha^{(t)}_{1,2} - \big(f_1f_3\beta^{(t+1)}_{2,1} + f_2\beta^{(t+1)}_{2,2}\big). && (8.8) \end{aligned}$$

Proof. The system of questions in (6.3) reduces to

$$\alpha^{(t)}_{1,1} + f_1\alpha^{(t)}_{2,1} + f_1f_2f_4\alpha^{(t)}_{1,2} = M^{(t)} = \beta^{(t)}_{2,1} + f_2\beta^{(t)}_{1,1} + f_1f_2f_3\beta^{(t)}_{2,2},$$

$$\alpha^{(t)}_{1,1} + f_1\alpha^{(t)}_{1,2} = \beta^{(t+1)}_{1,1},$$

$$\alpha^{(t)}_{2,1} = \beta^{(t)}_{2,1} + f_2\beta^{(t)}_{2,2}.$$

Eq. (*) follows from substituting the latter two equations into the left hand side of the first equation and rearranging. Eq. (**) comes from substituting the identity $f_2\beta^{(t+1)}_{2,2} = \alpha^{(t)}_{2,1} - \beta^{(t+1)}_{2,1}$ into Eq. (*). Eq. (8.8) is found by summing Eq. (*) and Eq. (**). □

As with the case for $\mathcal{J}_1$ and $\mathcal{J}_2$ in the last subsection, we are unable to remove all terms with the index $t+1$ from $O_{\mathcal{J}_3,\mathcal{J}_4}(M^{(t)})$. However, we may consider the congruence relation

$$M^{(t+1)} \equiv f_2\alpha^{(t)}_{1,1} + \alpha^{(t)}_{2,1} + f_1f_2\alpha^{(t)}_{1,2} \pmod{f_2(f_1f_3-1)},$$

and use the algorithm in Lemma 8.2.3 to generate $\mathcal{O}_{\mathcal{J}_3,\mathcal{J}_4}(M)$. We use the congruence relation above in step 1, Eq. (8.8) in step 2, and add $f_2(f_1f_3-1)$ for step 3 instead.

8.2.3 $L_1 = 4$ and $L_2 = 2$

Let $n = (f_1f_3, f_2f_4) \in \mathbb{N}_2^2$ with $N = f_1f_2f_3f_4$, and consider the joint ordered factorisations of n

$$\mathcal{J}_1 = \big((1, f_1), (2, f_2), (1, f_3), (2, f_4)\big), \quad \text{and} \quad \mathcal{J}_2 = \big((2, f_2f_4), (1, f_1f_3)\big).$$

Any other joint ordered factorisations of n with $L_1 = 4$ and $L_2 = 2$ will just be a permutation of f-values or swapping of j-values in the above. Hence we need only consider this case.

Lemma 8.2.6. Let $n = (f_1f_3, f_2f_4) \in \mathbb{N}_2^2$ with $N = f_1f_2f_3f_4$, and consider the two joint ordered factorisations $\mathcal{J}_1 = \big((1, f_1), (2, f_2), (1, f_3), (2, f_4)\big)$ and $\mathcal{J}_2 = \big((2, f_2f_4), (1, f_1f_3)\big)$. Let $M \in \langle N\rangle$ have the cyclic orbit $\mathcal{O}_{\mathcal{J}_1,\mathcal{J}_2}(M) = \mathcal{O}(M)$ of length $d \in \mathbb{N}$, and let $M^{(t)} \in \mathcal{O}(M)$ be the t-th element, for $t \in \langle d\rangle$, with $O_{\mathcal{J}_1,\mathcal{J}_2}\big(M^{(t)}\big) = O\big(M^{(t)}\big) = M^{(t+1)}$ the raising operator. We write the address of $M^{(t)}$ with respect to $\mathcal{J}_1$ as $\alpha\big(M^{(t)}\big) = \big(\alpha^{(t)}_{1,1}, \alpha^{(t)}_{2,1}, \alpha^{(t)}_{1,2}, \alpha^{(t)}_{2,2}\big)$, and with respect to $\mathcal{J}_2$ as $\beta\big(M^{(t)}\big) = \big(\beta^{(t)}_{2,1}, \beta^{(t)}_{1,1}\big)$.

Then the raising operator of $M^{(t)}$ is given by

$$O\big(M^{(t)}\big) = M^{(t+1)} = f_2f_4\alpha^{(t)}_{1,1} + \alpha^{(t)}_{2,1} + f_1f_2f_4\alpha^{(t)}_{1,2} + f_2\alpha^{(t)}_{2,2}. \tag{8.9}$$

Furthermore, the raising operator of $M^{(t)}$ satisfy the recursive relations

$$f_1f_3M^{(t+1)} = M^{(t)} + f_1\Big((f_3-1)\alpha^{(t)}_{2,1} - (f_2-1)\alpha^{(t)}_{1,2}\Big) + (N-1)\big(\alpha^{(t)}_{1,1} + f_1\alpha^{(t)}_{1,2}\big), \tag{*}$$

$$M^{(t+1)} = f_2f_4M^{(t)} - (f_1f_2f_4 - 1)\alpha_{2,1}^{(t)} - f_1f_2f_4(f_2 - 1)\alpha_{1,2}^{(t)} - f_2(N-1)\alpha_{2,2}^{(t)}. \qquad (**)$$

Proof. The system of questions in (6.3) reduce to

$$\alpha_{1,1}^{(t)} + f_1\alpha_{2,1}^{(t)} + f_1f_2\alpha_{1,2}^{(t)} + f_1f_2f_3\alpha_{2,2}^{(t)} = M^{(t)} = \beta_{2,1}^{(t)} + f_2f_4\beta_{1,1}^{(t)}, \tag{8.10}$$

$$\alpha_{1,1}^{(t)} + f_1\alpha_{1,2}^{(t)} = \beta_{1,1}^{(t+1)},$$

$$\alpha_{2,1}^{(t)} + f_2\alpha_{2,2}^{(t)} = \beta_{2,1}^{(t+1)}.$$

Eq. (8.9) follows from substituting the latter two equations into the left hand side of Eq. (8.10) and rearranging.

For Eq. (*), we multiply Eq. (8.9) through by f_1f_3 and use Eq. (8.10) to factor out $M^{(t)}$ to get

$$\begin{aligned} f_1f_3M^{(t+1)} &= N\alpha_{1,1}^{(t)} + f_1f_3\alpha_{2,1}^{(t)} + f_1N\alpha_{1,2}^{(t)} + f_1f_2f_3\alpha_{2,2}^{(t)} \\ &= M^{(t)} + f_1\Big((f_3-1)\alpha_{2,1}^{(t)} - (f_2-1)\alpha_{1,2}^{(t)}\Big) + (N-1)\big(\alpha_{1,1}^{(t)} + f_1\alpha_{1,2}^{(t)}\big). \end{aligned}$$

For Eq. (**), we multiply Eq. (8.10) through by f_2f_4 and use Eq. (8.9) to factor out $M^{(t+1)}$ to get

$$\begin{aligned} f_2f_4M^{(t)} &= f_2f_4\alpha_{1,1}^{(t)} + f_1f_2f_4\alpha_{2,1}^{(t)} + f_1f_2^2f_4\alpha_{1,2}^{(t)} + f_2N\alpha_{2,2}^{(t)} \\ &= M^{(t+1)} + (f_1f_2f_4 - 1)\alpha_{2,1}^{(t)} + f_1f_2f_4(f_2-1)\alpha_{1,2}^{(t)} + f_2(N-1)\alpha_{2,2}^{(t)}, \end{aligned}$$

as required. □

As all the formulae in Lemma 8.2.6 are independent of any term with index of $t+1$, we have a complete description of the cyclic orbit $\mathcal{O}(M)$.

Though Eq. (8.9) provides the easiest computation for this set, we can express the recursive relations in Lemma 8.2.6 as the following congruence relations;

$$\begin{aligned} f_1f_3M^{(t+1)} &\equiv M^{(t)} + f_1\Big((f_3-1)\alpha_{2,1}^{(t)} - (f_2-1)\alpha_{1,2}^{(t)}\Big) \pmod{N-1} \\ &\equiv \alpha_{1,1}^{(t)} + f_1f_3\alpha_{2,1}^{(t)} + f_1\alpha_{1,2}^{(t)} + f_1f_2f_3\alpha_{2,2}^{(t)} \pmod{N-1}, \end{aligned}$$

$$\begin{aligned} M^{(t+1)} &\equiv f_2f_4M^{(t)} - (f_1f_2f_4 - 1)\alpha_{2,1}^{(t)} - f_1f_2f_4(f_2-1)\alpha_{1,2}^{(t)} \pmod{N-1} \\ &\equiv f_4M^{(t)} + (f_2-1)\big(f_4\alpha_{1,1}^{(t)} + \alpha_{2,2}^{(t)}\big) - (f_1f_4 - 1)\alpha_{2,1}^{(t)} \pmod{N-1}. \end{aligned}$$

As these congruence relations are modulo $N-1$, any calculations will be reduced to the correct term, unlike when $L_1 = L_2 = 3$ where we had modulo $f_3(f_2-1)$. Therefore we do not require the algorithm in Lemma 8.2.3 to compute $\mathcal{O}(M)$.

By repeated substitution, we can express $M^{(t)}$ with respect to $M^{(0)}$. Let $n_2 = f_2 f_4$, then

$$M^{(t)} \equiv n_2^t M^{(0)} - \big(f_1 n_2 - 1\big) \sum_{j=0}^{t-1} n_2^{t-1-j} \alpha_{2,1}^{(j)} - f_1 n_2 \big(f_2 - 1\big) \sum_{j=0}^{t-1} n_2^{t-1-j} \alpha_{1,2}^{(j)} \pmod{N-1}.$$

Though unwieldy, this formula demonstrates that the elements of the cyclic orbit of M are close to powers of n_2 times M. The address of each previous term that came before $M^{(t)}$ is still required to compute $M^{(t)}$, which is not convenient. This is close to the expressions found in Chapter 7 for $L_1 = L_2 = 2$, though not as concise.

Remark 8.2.7. It appears that as long as $L_2 = 2$, with $L_1 \in \mathbb{N}_2$, we will be able to retrieve a complete description of the cyclic orbits by way of raising operators that do not require information about the term they compute in order to compute said term. However, these raising operators quickly become lengthy. Nevertheless, they can be used to determine any cyclic orbit.

8.2.4 $L_1 = 4$ and $L_2 = 3$

For $n = (f_1 f_3, f_2 f_4) \in \mathbb{N}_2^2$, there are only two base configurations for two joint ordered factorisations of n we need to consider, which are

$$\mathcal{J}_1 = \big((1,f_1),(2,f_2),(1,f_3),(2,f_4)\big), \quad \text{and} \quad \mathcal{J}_2 = \big((1,f_3),(2,f_2f_4),(1,f_1)\big),$$

with $\gcd(f_1, f_3) = 1$, or

$$\mathcal{J}_1 = \big((1,f_1),(2,f_2),(1,f_3),(2,f_4)\big), \quad \text{and} \quad \mathcal{J}_3 = \big((2,f_2),(1,f_1f_3),(2,f_4)\big),$$

with $\gcd(f_2, f_4) = 1$. Any other two joint ordered factorisations of n with $L_1 = 4$ and $L_2 = 3$ will be some permutation of f-values or swapping of j-values in the above.

As with the two cases for $L_1 = L_2 = 3$, both of the configurations above correspond to a similar system of equations to describe the raising operator, and so we will only consider $\mathcal{J}_1$ and $\mathcal{J}_2$.

Lemma 8.2.8. Let $n = (n_1, n_2) = (f_1f_3, f_2f_4) \in \mathbb{N}_2^2$ with $\gcd(f_1, f_3) = 1$, $N = f_1f_2f_3f_4$, and consider $\mathcal{J}_1 = \big((1, f_1), (2, f_2), (1, f_3), (2, f_4)\big)$ and $\mathcal{J}_2 = \big((1, f_3), (2, f_2f_4), (1, f_1)\big)$, two joint ordered factorisations of n. Let $M \in \langle N\rangle$ have the cyclic orbit $\mathcal{O}(M)$ of length $d \in \mathbb{N}$, with $M^{(t)} \in \mathcal{O}(M)$ for $t \in \langle d\rangle$. Let us write the address of $M^{(t)}$ with respect to $\mathcal{J}_1$ as $\alpha\big(M^{(t)}\big) = \big(\alpha_{1,1}^{(t)}, \alpha_{2,1}^{(t)}, \alpha_{1,2}^{(t)}, \alpha_{2,2}^{(t)}\big)$, and with respect to $\mathcal{J}_2$ as $\beta\big(M^{(t)}\big) = \big(\beta_{1,1}^{(t)}, \beta_{2}^{(t)}, \beta_{1,2}^{(t)}\big)$.

Then the raising operator of $M^{(t)}$ is given by

$$\begin{aligned} O\big(M^{(t)}\big) = M^{(t+1)} &= \alpha_{1,1}^{(t)} + f_3\alpha_{2,1}^{(t)} + f_1\alpha_{1,2}^{(t)} + f_2f_3\alpha_{2,2}^{(t)} + f_3(n_2-1)\beta_{1,2}^{(t+1)} && (*) \\ &= n_2\alpha_{1,1}^{(t)} + f_3\alpha_{2,1}^{(t)} + f_1n_2\alpha_{1,2}^{(t)} + f_2f_3\alpha_{2,2}^{(t)} - (n_2-1)\beta_{1,1}^{(t+1)} && (**) \\ &= (n_2+1)\Big(\alpha_{1,1}^{(t)} + f_1\alpha_{1,2}^{(t)}\Big) + f_3\alpha_{2,1}^{(t)} + f_2f_3\alpha_{2,2}^{(t)} - n_2\beta_{1,1}^{(t+1)} - f_3\beta_{1,2}^{(t+1)}. && (8.11) \end{aligned}$$

Proof. The system of questions in (6.3) reduces to

$$\alpha_{1,1}^{(t)} + f_1\alpha_{2,1}^{(t)} + f_1f_2\alpha_{1,2}^{(t)} + f_1f_2f_3\alpha_{2,2}^{(t)} = M^{(t)} = \beta_{1,1}^{(t)} + f_3\beta_{2}^{(t)} + f_2f_3f_4\beta_{1,2}^{(t)},$$

$$\alpha_{1,1}^{(t)} + f_1\alpha_{1,2}^{(t)} = \beta_{1,1}^{(t+1)} + f_3\beta_{1,2}^{(t+1)},$$

$$\alpha_{2,1}^{(t)} + f_2\alpha_{2,2}^{(t)} = \beta_{2}^{(t+1)}.$$

Eq. (*) follows from substituting the latter two equations into the left hand side of the first equation above and rearranging. Eq. (**) comes from substituting $f_3\beta_{1,2}^{(t)} = \alpha_{1,1}^{(t)} + f_1\alpha_{1,2}^{(t)} - \beta_{1,1}^{(t+1)}$ into Eq. (*). Eq. (8.11) is found by summing Eq. (*) and Eq. (**). □

As was the case for $L_1 = L_2 = 3$, we cannot remove all terms with index $t+1$, which implies $O\big(M^{(t)}\big)$ requires information about $M^{(t+1)}$ to calculate $M^{(t+1)}$. As such, these equations cannot give a complete description of $\mathcal{O}(M)$. Again, we rely on the algorithm presented in Lemma 8.2.3, using the congruence relation

$$M^{(t+1)} \equiv \alpha_{1,1}^{(t)} + f_3\alpha_{2,1}^{(t)} + f_1\alpha_{1,2}^{(t)} + f_2f_3\alpha_{2,2}^{(t)} \pmod{f_3(f_2f_4-1)},$$

in step 1, Eq. (8.11) in step 2, and add $f_3(f_2f_4-1)$ in step 3.

8.3 Conclusion

Across Chapter 6, Chapter 7 and Chapter 8, we have studied how the discrepancies that arise between two joint ordered factorisations form a complex structure. Each integer within the systems will generate a sequence of integers, tracing a path between the principal reversible cuboids that they take when we compare the positions and values of subsequent terms against each other. These so called orbits are thus a tool to describe the emergent complexity that arise from considering these differences.

Inherently, studying the cyclic orbit of elements between two joint ordered factorisation requires an explicit expression for the raising operators that formulate the terms in the orbit. Although we were able to prove a generalised property of nested cyclic orbits for m-dimensions and any joint ordered factorisations, the raising operators are too dependent on the given joint ordered factorisations to gleam any general properties.

The cyclic orbit of an integer heavily relies on the address representation of said integer in both joint ordered factorisations. This might not be too surprising since we are functionally mapping out the discrepancies between the block structure of each principal reversible cuboid, an integer at a time.

We restricted ourselves to the 2-dimensional case and considered a selection of generic forms the two joint ordered factorisations could take, varying the number of pairs that appeared in both. Using a generalised system of equations, we were able to derive equations for the accompanying raising operators. Even for relatively simple forms, the raising operator was either incomplete, requiring information about the term it was meant to calculate in order to calculate it, or was quite complex and did not have many immediately useful properties. Nevertheless, we were able to give multiple formulae in each case. The initial such formulae were derived by considering the addresses of subsequent terms in the cyclic orbits, from which we could construct recurrence relations and congruence relations that proved useful.

When $L_2 = 3$, i.e. the second joint ordered factorisation consisted of 3 pairs, the raising operator could not fully describe the orbit by itself. However, we introduced an algorithm, Lemma 8.2.3, which used the information of the system to deduce the terms of the cyclic orbit. We gave an example for $L_1 = 3$ and $L_1 = 4$, where L_1 is the number of pairs of the first joint ordered factorisation, but this algorithm can be used for any $L_1 \in \mathbb{N}_2$.

When $L_2 = 2$ and $L_1 = 4$, the raising operator did provide a complete description of a cyclic orbit. Furthermore, we were able to express the raising operator through a recurrence relation which we then used to write a congruence relation. We used these to write any element in the cyclic orbit in terms of the beginning element, though this expression required information on all elements between the first and the given element, and so is not very concise.

We did not investigate when $L_1 = L_2 = 4$, nor any other case. This is because the raising operator starts to become less and less useful, requiring more and more information about the term it is meant to calculate to actually calculate it. Additionally, it is unknown if these results generalise to m-dimensions, for $m \in \mathbb{N}$.

For generalised joint ordered factorisation, these orbits become complicated and unwieldy fast. This is not to say that the inherent properties and patterns embedded into these orbits are not important however. Perhaps the incomplete pictures these raising operators paint are due to the limitations of the notation used for the framework. Though, perhaps the systems themselves are just not enough to explain every detail, requiring additional theory to support it. Considering the block structures of these principal reversible cuboids through the lens of tensors might be said theory.

Bibliography

[1] L. Adleman. *On breaking the titrated Merkle-Hellman public key cryptosystem.* Crypto'82, Springer (1982) 303–308. doi:10.1007/978-1-4757-0602-4

[2] N. Alon, M. B. Nathanson, I. Z. Ruzsa. *Adding distinct congruence classes modulo a prime.* Amer. Math. Monthly Vol. 102 (1995) 250-255

[3] T. M. Apostol. *Introduction to Analytic Number Theory (Undergraduate Texts in Mathematics).* Springer (1976) ISBN 978-0387901633

[4] E. R. Berlekamp. *Algebraic Coding Theory.* World Scientific, Revised Edition (2015). ISBN 978-9-814-63589-9

[5] R. Blahut. *Algebraic Codes for Data Transmission.* Cambridge Uni. Press (2003). doi:10.1017/CBO9780511800467

[6] R. Blahut. *Algebraic Codes on Lines, Planes, and Curves: An Engineering Approach.* Cambridge University Press (2008). ISBN 978-0-521-77194-8

[7] N. G. de Bruijn. *On bases for set of integers.* Publicationes Mathematicae, Debrecen I, 232-242 (1950)

[8] N. G. de Bruijn. *On number systems.* Nieuw Arch. Wisk., Vol. 4 (1956) 15-17

[9] D. De Caen, D. A. Gregory, I. G. Hughes, D. L. Kreher. *Near-factors of finite groups.* Ars Combin. Vol 29 (1990)

[10] R. D. Carmichael. *The theory of numbers.* Nabu Press (1914). ISBN 1144400341

[11] A. Cauchy. *Recherches sur les nombres.* J. Ecole Polytech Vol. 9 (1813) 99–116

[12] A. Y. M. Chin, K. L. Wang, K. B. Wong. *Complete factorisations of finite abelian groups.* Jor. of Alg. Vol 628 (2023)

[13] B. Chor, R. Rivest. *A knapsack-type public key cryptosystem based on arithmetic in finite fields.* IEEE Trans. Inform. Theor. Vol. 34, No. 5 (1988) 901–909

[14] L. Comtet. *Advanced Combinatorics.* Reidel, Dordrecht (1974)

[15] K. Corrádi, A. D. Sands, S. Szabó. *Simulated factorisations.* Jor. of Alg. Vol 151 (1992)

[16] K. Corrádi, S. Szabó. *Direct products of subsets in a finite abelian group.* Acta Math. Hungar. Vol 138, (2013), DOI: 10.1007/s10474-012-0289-1

[17] E. Coven, A. Meyrowitz. *Tiling the integers with translates of one finite set.* J. Algebra, Vol. 212 (1999) 161–174

[18] M. Dateyama, T. Kamae. *On direct sum decompostion of integers and Y. Ito's conjecture.* Tokyo J. Math., Vol. 21 (1998) 433–440

[19] H. Davenport. *A historical note.* London Math. Soc. Vol. 22 (1947) 100–101

[20] J. A. Dias da Silva, Y. O. Hamidoune. *Cyclic spaces for Grassmann derivatives and additive theory.* London Math. Soc. Vol. 26 (1994) 140-146

[21] R. D. Díaz, L. Hernández-Álvarez, L. H. Encinas, A. Queiruga-Dios. *Chor-Rivest knapsack cryptosystem in a post-quantum world.* Springer, Advances in Security, Networks, and Internet of Things, (2021) 67–83. https://doi.org/10.1007/978-3-030-71017-0

[22] W. Diffie, M. Hellman. *New directions in cryptography.* IEEE Transactions on Information Theory. Vol. 22, No. 6 (1976). doi:10.1109/TIT.1976.1055638, https://ieeexplore.ieee.org/document/1055638

[23] D. S. Dummit, R. M. Foote. *Abstract Algebra* Wiley Publishers, 3rd edition (2003). ISBN 978-0-471-43334-7

[24] S. J. Eigen. *A direct sum decomposition of the integers and a question of Y. Ito.* Tokyo J. Math., Vol. 26, No. 2, (2003)

[25] S. C. Elwood. *A mathematical theory of communication.* Bell System Technical Journal, Vol. 27 (1948) 623–666. doi:10.1002/j.1538-7305.1948.tb00917.x

[26] P. Erdös, R. L. Graham. *Old and new problems and results in combinatorial number theory.* Geneva, Switzerland: L'Enseignement Mathématique Université de Genéve, Vol. 28 (1980)

[27] P. Erdös, P. Turán. *On a problem of Sidon in additive number theory, and on some related problems.* Journal of the London Mathematical Society. Vol. 16, No. 4 (1941) 212–216. doi:10.1112/jlms/s1-16.4.212

[28] J. Friedlander, H. Iwaniec. *Opera de Cribro.* American Mathematical Society (2010). ISBN 978-0821849705

[29] C. F. Gauβ. *Allgemeine Untersuchungen über die Congruenzen. In Untersuchungen über höhere Arithmetik.* Berlin, 1st edition, (1889). Chelsea Publishing Co., New York, 2nd edition, (1965). http://eudml.org/doc/204648

[30] R. L. Graham, D. E. Knuth, O. Pataschnik. *Concrete Mathematics.* Addison-Wesley Publishing (1988). ISBN 978-0-201-14236-5

[31] C. M. Grinstead. *On circular critical graphs.* Discrete Math. Vol 51 (1984)

[32] S. W. Golomb. *Obtaining specified irreducible polynomials over finite fields.* SIAM Journal on Matrix Analysis and Applications; Philadelphia Vol. 1, No. 4 (1980)

[33] H. W. Gould. *Combinatorial Identities.* Morgantown (1972)

[34] G. Hajós. *Covering multidimensional spaces by cube lattices*, Mat. Fiz. Lapok 45 (1938)

[35] G. Hajós. *Über einfache und mehrfache Bedeckung des n-dimensionalenRaumes mit einem Würfelgitter.* Math. Zeit. Vol 47 (1942)

[36] R. W. Hamming. *Error detecting and error correcting codes.* Bell System Technical Journal, Vol. 29 (1950) 147-160. doi:10.1002/J.1538-7305.1950.TB00463.X

[37] N. J. Higham, M. C. Lettington, K. M. Schmidt. *Integer matrix factorisations, superalgebras and the quadratic form obstruction.* (2021) arXiv:2103.04149

[38] S. L. Hill, M. C. Lettington, K. M. Schmidt. *On block representations and spectral Properties of semimagic square matrices* (2016) arXiv:1605.08629

[39] S. L. Hill. *Problems related to number theory: Sum-and-distance systems, reversible square matrices and divisor functions.* PhD Thesis, Cardiff University (2018) https://orca.cardiff.ac.uk/id/eprint/111467

[40] S. L. Hill, M. N. Huxley, M. C. Lettington, K. M. Schmidt. *Some properties and applications of non-trivial divisor functions.* Ramanujan J, Vol. 51 (2020) 611–628. https://doi.org/10.1007/s11139-018-0093-9

[41] T. W. Hungerford. *Algebra (Graduate Texts in Mathematics).* Springer (1974). ISBN 0387905189

[42] M. N. Huxley, M. C. Lettington, K. M. Schmidt. *On the structure of additive systems of integers.* Periodica Mathematica Hungarica, Vol. 78 (2019) 178-199. https://doi.org/10.1007/s10998-018-00275-w

[43] Y. Ito. *Direct sum decomposition of the integers.* Tokyo J. Math., Vol. 18 (1995) 259–270

[44] N. Jacobson. *Basic Algebra I.* Dover Publications, 2nd ed (2009). ISBN 978-0-486-47189-1

[45] M. Kabenyuk. *Complete factorisations of finite groups.* ArXiv (2024) https://arxiv.org/pdf/2311.07061v2

[46] L. Kalmár (1931). *A "factorisatio numerorum" problémájáról.* Mat. Fiz. Lapok, Vol. 38, 1–15

[47] A. Knopfmacher, M. E. Mays. *A survey of factorisation counting functions.* Int. J. Number Theory 1 (2005) 563–581. doi: 10.1142/S1793042105000315

[48] J. C. Lagarias, A. M. Odlyzko. *Solving low-density subset sum problems.* J. Ass. Comput. Much., Vol. 32, No. 1 (1985) 229-246

[49] A. D. Law, M. C. Lettington, K. M. Schmidt. *On properties and enumerations of m-part Sum Systems.* ArXiv (2023) https://arxiv.org/pdf/2303.12042.pdf

[50] M. C. Lettington, K. M. Schmidt and S. Hill. *On superalgebras of matrices with symmetry properties.* Linear and Multilinear Algebra (2017) doi:10.1080/03081087.2017.1363153

[51] M. C. Lettington, K. M. Schmidt (2019). *Divisor functions and the number of sum systems.* Integers, Vol. 20, arXiv:1910.02455

[52] M. C. Lettington, K. M. Schmidt. *On the sum of left and right circulant matrices.* Linear Algebra and its Applications, Vol. 658 (2023) 62-85. https://doi.org/10.1016/j.laa.2022.10.024. (https://www.sciencedirect.com/science/article/pii/S0024379522003895)

[53] C. T. Long. *Addition theorems for sets of integers.* Pacific Journal of Mathematics, Vol. 23, No. 1 (1967)

[54] E. Lucas. *Théorie des nombres.* Gauthier-Villars (1891), reprinted by A. Blanchard (1961)

[55] M. Lothaire. *Combinatorics on words.* Encyclopedia of Mathematics and Its Applications. Vol. 17. Cambridge University Press. pp. 79, 84. ISBN 978-0-521-59924-5. MR 1475463

[56] P. A. MacMahon. *Applications of a theory of permutations in circular procession to the theory of numbers major.* (1891) https://doi.org/10.1112/plms/s1-23.1.305

[57] P. A. MacMahon. *Memoir on the composition of numbers*, Phil. Trans. R. S. (A) (1893)

[58] F. J. MacWilliams, N. J. A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland Mathematical Library (1983). ISBN 978-0-444-85193-2

[59] W. Magnus, A. Karass, D. Solitar. *Combinatorial group theory: presentation of groups in terms of generators and relations.* Dover Books (1966). ISBN 978-0-486-43830-6

[60] N. Metropolis, G. C. Rota. *Witt vectors and the algebra of necklaces.* Advances in Mathematics 50 (1983) 95–125. https://doi.org/10.1016/0001-8708(83)90035-X

[61] N. Metropolis, G. C. Rota. *The cyclotomic identity.* AMS Contemporary Mathematics, Vol. 34 (1984) 19-27

[62] H. Minkowski. *Geometrie der Zahlen.* Teubner, Leipzig, (1896)

[63] C. Moreau. *Sur les permutations circulaires distinctes (On distinct circular permutations)*, Nouvelles Annales de Mathématiques, Serie 2, Vol. 11 (1872) 309-314. http://www.numdam.org/item/NAM_1872_2_11__309_0/

[64] A. O. Munagi. *k-complementing subsets of nonnegative integers.* International Journal of Mathematics and Mathematical Sciences (2005). https://doi.org/10.1155/IJMMS.2005.215

[65] A. O. Munagi. *Labelled factorisation of integers.* The Electronic Journal of Combinatorics, Vol. 16, No. 1 (2009) https://doi.org/10.37236/139

[66] M. B. Nathanson. *Additive systems and a theorem of de Bruijn.* American Mathematical Monthly, Vol. 121 (2014) 5-7. arXiv:1301.6208

[67] M. B. Nathanson. *Limits and decomposition of de Bruijn's additive systems.* Combinatorial and Additive Number Theory II, Springer, New York (2017) 255-267. arXiv:1305.3001

[68] K .Ollerenshaw, D. Brée. *Most-perfect pandiagonal magic squares.* IMA (1998)

[69] C. P. Popovici. *O generalizare a funcţiei lui Möebius.* Acad. R. P. Romîne Stud. Cerc. Mat., Vol. 14 (1963) 493-499

[70] N. Rebenich. *Counting prime polynomials and measuring complexity and similarity of information.* University of Victoria (2016)

[71] T. Sakuma, H. Shinohara. *Krasner near-factorisations and 1-overlapped factorisations.* The Seventh European Conference on Combinatorics, Graph Theory and Applications EuroComb (2013)

[72] A. D. Sands. *Factorisation of cyclic groups*. Proc. Coll. on Abelian Groups, Tihany, Hungary (1963)

[73] A. D. Sands. *Factoring finite abelian groups*. J. of Algebra, Vol 274 (2004)

[74] A. D. Sands. *Factorisations of abelian groups involving simulated factors and one other factor*. Acta Sci. Math. Vol 73, (2007)

[75] W. Schwarz, J. Spilker. *Arithmetical functions*. LMS Lecture Note Series 184, Cambridge University Press (1994)

[76] A. Shamir. *A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystems*. Focs '82 (1982) 145–152. doi:10.1109/SFCS.1982.5

[77] A. Sklar. *On the factorisation of squarefree integers*. Proc. Amer. Math. Soc., Vol. 3 (1952) 701-705

[78] J. Sprittulla. *Ordered factorisations with k factors*. (2016) arXiv:1610.04826

[79] C. E. Swenson. *Direct sum subset decompositions of Z*. Pacific Journal of Mathematics, Vol. 53, No. 2 (1974) 629–633. doi: 10.2140/pjm.1974.53.629

[80] S. Szabó, A. D. Sands. *Factoring groups into subsets*. CRC Press, Lecture Notes in Pure and Applied Mathematics, Vol. 257, (2009). ISBN 978-1-420-09046-8

[81] S. Szabó. *Methods for constructing factorisations of Abelian groups with applications*. Serdica Mathematical Journal, Vol 43 (2017)

[82] R. Tijdeman. *Decomposition of the integers as a direct sum of two subsets*. Number theory (Paris, 1992–1993), London Math. Soc. Lecture Note Ser. 215 (1995). Cambridge Univ. Press, 261–276

[83] E. C. Titchmarsh. *The Theory of the Riemann Zeta-Function*. Oxford University Press (1951)

[84] A. M. Vaidya. *On complementing sets of nonnegative integers*. Mathematics Magazine, Vol. 39, No. 1 (1966) 43-44

[85] S. Vaudenay. *Cryptanalysis of the Chor-Rivest cryptosystem*. J. Cryptol. Vol. 14 (2001) 87–100

[86] W. A. Webb. *A public key cryptosystem based on complementing sets*. Cryptologia XVI (2) (1992) 177–181

[87] J. P. Wheeler. *The Cauchy-Davenport theorem for finite groups*. (2006) arXiv:1202.1816

[88] E. Witt. *Treue Darstellung Liescher Ringe*. Journal für die reine und angewandte Mathematik No. 177 (1937) 152-160. https://doi.org/10.1515/crll.1937.177.152