Topics Related to the Theory of Numbers

Integer Points close to Convex Hypersurfaces, Associated Magic Squares and a Zeta Identity

Matthew C. Lettington

School of Mathematics
University of Wales College of Cardiff
September 30, 2008

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

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

Summary

Let C be the boundary surface of a strictly convex d-dimensional body. Andrews obtained an upper bound in terms of M for the number of points on MC, the M-fold enlargement of C.

We consider the integer points within a distance δ of the hypersurface MC. Introducing δ requires some uniform approximability condition on the surface C, involving determinants of derivatives. To obtain an asymptotic formula (main term the volume of the search region) requires the Fourier transform with conditions up to the $6d$-th derivative.

We obtain an upper bound subject to a Curvature Condition that requires only first and second derivatives, that MC has a tangent hyperplane everywhere, and each two-dimensional normal section has radius of curvature in the range $c_0 M + 1/2 \leq \rho \leq c_1 M - 1/2$, where c_0 and c_1 are non-zero constants.

Our main result is Theorem 2.

THEOREM 2. *Let C be a strictly convex hypersurface in d-dimensional space ($d \geq 3$), satisfying the Curvature Condition at size M. Then the total number, N, of integer points lying within a distance δ of MC is bounded by the sum of two terms, one from Andrews's bound, the other from the hypervolume of the search region, with explicit constant factors involving δ, c_0 and c_1.*

In the body of the thesis, to simplify the notation, we use C for the enlarged surface called MC in this summary.

In Part II we enumerate a class of special magic squares. We observe a new identity between values of the zeta functions at even integers.

Acknowledgements

After what feels like an almost eternal effort it is with a certain joy and pride that I hand over the results of my labour. I have drawn inspiration, guidance and support from many different people during my time researching this PhD thesis and I would like to take this opportunity to thank them (be they alive or deceased) for their help in this process.

Special mention must of course go to my supervisor, Professor Martin N. Huxley, without whose guidance and support I would have struggled to achieve the breakthroughs made. His constancy of belief, unending patience and clarity of vision have been fundamental in shaping my research.

My wife Deborah has also been of crucial importance in this process as her encouragement, emotional support and pragmatic opinions in times of difficulty have been invaluable in helping me keep my focus.

Many thanks must also go to all my family, especially to my father, and to my aunt and uncle, Ann and Terry Hardie, to Dr Gert-Dieter Jakubczik of JSC Management-und Technologieberatung AG, and to Sue Thompson of Gloucestershire College, to all other friends/family not mentioned here who have helped, and to everyone in the School of Mathematics, Cardiff, who has found the time to give consideration to my questions (or just made me a cup of tea).

Contents

Notation for Part I v

Abstract 1

PART I: Integer Points Close to Convex Hypersurfaces 4

1 Jarník's Curve 5
- 1.1 Construction in Two-Dimensions 5
- 1.2 Moving Two Dimensions into d 8

2 The Integer Points Close to a Curve 10
- 2.1 Edges and Vertices 10
- 2.2 Major and Minor Arcs 15

3 Curvature, Surfaces and Polytopes in $\mathbb{E}^d$ 24
- 3.1 Convex and Affine Spaces 24
- 3.2 Parallelism and Orthogonality in $\mathbb{E}^d$ 25
- 3.3 Curvature, Shells and d-Surfaces 26
- 3.4 Convex Polytopes 32
- 3.5 Major Arcs and Lattices 42

4 Components of H 49
- 4.1 Vertex Components 49
- 4.2 Enlarged Vertex Components 52
- 4.3 Boundary Components 58

5 Integer Points Close to Convex Surfaces 59
- 5.1 Integer Points on One and d-Dimensional Boundary Components 59
- 5.2 Integer Points on Boundary Components of Dimension $d-1$. 64

5.3 The Shelling Argument in 3-Dimensions 72

6 Boundary Content, Relative Volumes and Ehrhart Theory 75
6.1 Andrews Theorem and Ehrhart Theory 75
6.2 Stirling Numbers of the First Kind 80

7 Integer Points Close to Convex Hypersurfaces 86
7.1 Girdles and Lattice Determinants 86
7.2 Summing the Boundary Components 89

PART II: Associated Magic Squares and a Zeta Identity 103

8 Overview 104
8.1 Brief History 104
8.2 Structure and Symmetry 109

9 Matrix Algebra 113
9.1 Vector Space Fundamentals. 113
9.2 Multiplication and Constructions 117
9.3 Two and Three Parameter Families 122

10 Explicit Calculations 128
10.1 Diagonal Coefficients 128
10.2 Characteristic Polynomials of $M(z, y)$ 135
10.3 Sums and Differences of Two n-th Powers 137

11 Identities and Determinants 138
11.1 Coefficients of the $b_q^{(2r+1)}$ Polynomials 138
11.2 Recurrence Determinants 143
11.3 Residues and Inverses modulo n 150

12 Addendum 157
12.1 Multinomial Identities 157
12.2 p-adic Relations 159

Notation for Part I

The lower case definitions are listed first followed by the upper case and then the Greek. Points in $\mathbf{E}^d$ are defined either by upper case letters or bold-face lower case letters as in vector notation.

c_0 = Lower bound constant in Curvature Condition.

c_1 = Upper bound constant in Curvature Condition.

d = Dimension.

f_j = Number of j-dimensional faces of convex hull H.

h = Height above hyperplane.

$\mathbf{n}$ = Normal vector to face F.

$\mathbf{v}$ = Vertex.

A = Sometimes a coefficient, otherwise area or $(d-1)$-volume in $\mathbf{E}^d$.

B = d-sphere radius $c_1 M$.

B_i = d-ball, centre W_i on B, radius $1/2\sqrt{c_0 \delta M}$.

C = Convex closed hypersurface.

C_0 = Inner boundary surface to shell E.

C_1 = Outer boundary surface to shell E.

$C(F)$ = Centroid of face F.

D = Distance or diameter.

E = Shell bounded by C_1 and C_0.

$\mathbf{E}^d$ = d-dimensional real vector space with Euclidean metric.

F, G = Face or facet of polytope $\mathcal{P}$ or convex hull H.

H = $\begin{cases} \text{Height of vector (chapters 1 and 2).} \\ \text{Convex hull of set of points S (chapters } 3-7). \end{cases}$

K = Number of integer points in a set.

L = Partition length.

$L^\star$ = Maximum component diameter.

M = Size parameter.

P, Q = Point.

$\mathcal{P}$ = Convex polygon or convex d-polytope.

R = Radius.

$R_0(V)$ = Normal projection of vertex V onto C_0.

$R_1(V)$ = Normal projection of vertex V onto C_1.

$\mathcal{R}(V)$ = The *reach* of an enlarged vertex component $S'(V)$.

$S(V)$ = Vertex component of vertex V.

S = Set of integer points in shell E.

$S(H)$ = Set of integer points on convex hull H.

$S'(V)$ = Enlarged vertex component of vertex V.

$S^\star(V)$ = Boundary component of vertex V.

S^+, S^- = Sets of primitive two-dimensional vectors.

T = Set of centroids of j-faces of d-polytope $\mathcal{P}$.

U = Convex set.

V = Vertex or Volume.

Y = Mid-point.

δ = Small distance.

ρ = Radius of curvature.

Λ = Lattice.

Π, Ψ = Plane or hyperplane.

Abstract

Let C be the boundary surface of a strictly convex bounded d-dimensional body. Strictly convex means that if P and Q are points on C, then points on the line segment PQ between P and Q lie in the convex body, but not on its boundary C. Let MC denote the dilation of C by a factor M. Andrews [1] proved that the number of points of the integer lattice on MC is

$$O\left(M^{\frac{d(d-1)}{d+1}}\right), \tag{1}$$

as M tends to infinity. Strict convexity is necessary because a part of a $(d-1)$-dimensional hyperplane in the boundary C can give as many as a constant times M^{d-1} integer points for infinitely many values of M.

We consider the integer points within a distance δ of the hypersurface MC. The two-dimensional case has been well studied [25], [8], [21], [14], [22] and [24]. Introducing δ requires some uniform approximability condition on the surface C, usually expressed in terms of upper and lower bounds for derivatives and determinants of derivatives. Let A be the $(d-1)$-dimensional volume of C. The search region has d-dimensional volume

$$\left(2A\delta + O(\delta^2)\right) M^{d-1}, \tag{2}$$

and this is known to be the number of integer points on average over translations of the surface MC. To obtain an asymptotic formula one considers the Fourier transform of the convex body, with conditions at least as far as the $6d$-th derivatives in order to estimate the multiple exponential integrals. Hlawka [20] obtained an asymptotic formula with error of size (1); see also Krätzel [27]. Under the C^∞ hypothesis of a convergent Taylor series, the error term in the asymptotic formula has been improved, most recently by Müller [33].

We derive an upper bound for the number of integer points within a distance δ of the hypersurface. We require only that C has a tangent hyperplane at every point, and that any two-dimensional cross-section through the normal at some point P consists (in a neighbourhood of P) of a plane curve C' with continuous radius of curvature bounded away from zero and infinity.

Curvature Condition (with size parameter M). For any point P on C and any two-plane Π through the normal to C at P, let $C(\Pi, P)$ be the closed plane curve $C \cap \Pi$. Then $C(\Pi, P)$ is a twice differentiable plane curve with radius of curvature ρ lying in the range

$$c_0 M + \frac{1}{2} \leq \rho \leq c_1 M - \frac{1}{2}, \tag{3}$$

where the constants c_0, c_1 and δ satisfy

$$\frac{1}{M} < c_0 \leq 1 \leq c_1, \text{ and } \delta < \frac{1}{4}. \tag{4}$$

Local Curvature Condition. There is a constant κ such that for $C(\Pi, P)$ defined as above, the points Q of $C(\Pi, P)$ with $PQ \leq \kappa M$ form a twice differentiable plane curve with radius of curvature satisfying (3).

In order to state our results, we set up some notation. Let C_0 be the locus of points at distance δ from C measured along the interior normals to C, and let C_1 be the locus of points at distance δ measured along the exterior normals. Let E be the d-dimensional shell bounded by C_0 and C_1 so that E has thickness 2δ. Let S be the set of integer points in E, and let H be the convex hull of S, so that H is a d-dimensional convex polytope. All points of S lie in H, but not all integer points on the boundary of H lie in S.
By Lemma 3.3.2, (stated in chapter 3) the boundary surfaces C_0 and C_1 of the shell E have a tangent hyperplane at each point Q, and their two-dimensional cross-sections $C(\Pi, Q)$ in planes normal to the tangent hyperplanes are twice differentiable, with radius of curvatures in the range

$$c_0 M \leq \rho \leq c_1 M. \tag{5}$$

Under the Curvature Condition, the shell E containing S, the set of integer points, lies in a d-hypersphere of radius $R = c_1 M$. The volume V_d and surface content S_d of this sphere is given by the formulae

$$V_d = \alpha_d R^d, \qquad S_d = d\alpha_d R^{d-1}. \tag{6}$$

We can now state our results.

THEOREM 1. *Suppose that C is a convex surface in 3-dimensional Euclidean space $\mathbb{E}^3$, satisfying the Curvature Condition at size M (so that C is contained in a sphere radius $c_1 M$). Then the total number, N, of integer points lying either on C, or within a distance δ of C, is bounded by*

$$\leq \left(\frac{c_1}{c_0}\right)^2 2^{16} \left((c_1 M)^{\frac{3}{2}} + 2^9 \delta (c_1 M)^2\right). \tag{7}$$

THEOREM 2. *Suppose that C is a convex hypersurface in d-dimensional Euclidean space $\mathbb{E}^d$ $(d \geq 3)$, satisfying the Curvature Condition at size M (so that C is contained in a hypersphere radius $c_1 M$). Then the total number, N, of integer points lying either on C, or within a distance δ of C, is bounded by*

$$N \leq \frac{2^{3d^2+5d-7} d!}{\alpha_{d-1}} \left(\frac{c_1}{c_0}\right)^{d-1} \left((c_1 M)^{\frac{d(d-1)}{d+1}} + 2^9 \delta (c_1 M)^{d-1}\right). \tag{8}$$

THEOREM 3. *Suppose that C is a convex hypersurface in d-dimensional Euclidean space $\mathbb{E}^d$ $(d \geq 3)$, satisfying the Local Curvature Condition at size M (so that C is contained in a hypersphere radius $c_1 M$), with*

$$M \geq \frac{100 \delta c_1}{\kappa^2}. \tag{9}$$

Then N, the total number of integer points lying either on C, or within a distance δ of C, satisfies the same bound (8) *as in Theorem* 2.

In Part II we enumerate a class of special magic squares. As a by-product we observe a new identity between values of the zeta functions at even integers

$$\zeta(2j) = (-1)^j \left(\frac{-j\pi^{2j}}{(2j+1)!} - \sum_{k=1}^{j-1} \frac{(-1)^k \pi^{2j-2k}}{(2j-2k+1)!} \zeta(2k)\right). \tag{10}$$

PART I

Integer Points Close to Convex Hypersurfaces

Chapter 1

Jarník's Curve

This chapter gives an overview of the Jarník Polygon and extends Jarník's result to a two-dimensional plane in d-dimensional space.

1.1 Construction in Two Dimensions

Jarník considered the question: how many integer points can lie on a strictly convex closed curve of bounded length? Jarník's extremal curve [25] circumscribes a convex plane polygon constructed by a "greedy algorithm", using the lists $S^+(H)$ and $S^-(H)$ of all the primitive integer vectors (a, b) corresponding to rational gradients b/a in their lowest terms of height at most H as sides of the polygon. That is

$$S^+(H) = \{(a, b) : (a, b) = 1, \quad 1 \leq a \leq H, \quad 0 \leq |b| \leq H\},$$

and

$$S^-(H) = \{(a, b) : (a, b) = 1, \quad -1 \leq a \leq -H, \quad 0 \leq |b| \leq H\},$$

so that the rationals corresponding to $S^+(H)$ and $S^-(H)$ have positive and negative denominators respectively and each set is ordered in terms of increasing gradient.

The construction starts at an integer point or lattice point in the plane and takes all of the ordered primitive integer vectors in $S^+(H)$, then the vector $(0, 1)$ with infinite gradient, then all of the ordered primitive integer vectors in $S^-(H)$ and then the vector $(0, -1)$ to complete the convex polygon.

Hence all the vertices are integer or lattice points. For example, the twenty-three primitive rational gradients corresponding to the vectors of $S^+(4)$ are

$$\left\{\frac{-4}{1}, \frac{-3}{1}, \frac{-2}{1}, \frac{-3}{2}, \frac{-4}{3}, \frac{-1}{1}, \frac{-3}{4}, \frac{-2}{3}, \frac{-1}{2}, \frac{-1}{3}, \frac{-1}{4}, \frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}, \frac{4}{3}, \frac{3}{2}, \frac{2}{1}, \frac{3}{1}, \frac{4}{1}\right\}.$$

Given that a polygon can have at most two parallel sides and that each side direction must be unique, the Jarník polygon for any fixed height H has the maximum number of sides ($f_1(H)$ say) and vertices ($f_2(H)$ say). In Jarník's construction

$$f_0(H) = f_1(H) = \frac{24H^2}{\pi^2} + O(H \log H) \tag{1.1}$$

and

$$D_H = \frac{6H^3}{\pi^2} + O(H^2 \log H),$$

where D_H is the diameter of the polygon.

Jarník's upper bound for the number N of vertices, in terms of the maximum length L of the polygon [25] *Satz 2* is

$$N \leq \frac{3}{\sqrt[3]{2\pi}} L^{2/3} + O\left(L^{1/3}\right). \tag{1.2}$$

Proofs are given in chapter 2. Figures (1.2) and (1.3) are examples of the Jarník polygons' for heights $H = 2, 3, 4, \ldots, 10$.

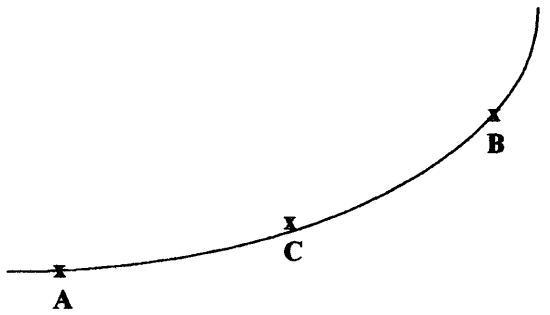

Figure 1.1: Radius of curvature bound restricts the "flatness" of the curve.

We note that Jarník uses "length $\leq x$" because the maximum number of integer points on a convex curve of length L might not be an increasing

function of L. That is, the radius of curvature in his theorem is bounded above by $7x$, so you might not be able to flatten out the curve between two points A and B, to pass through a point C say.

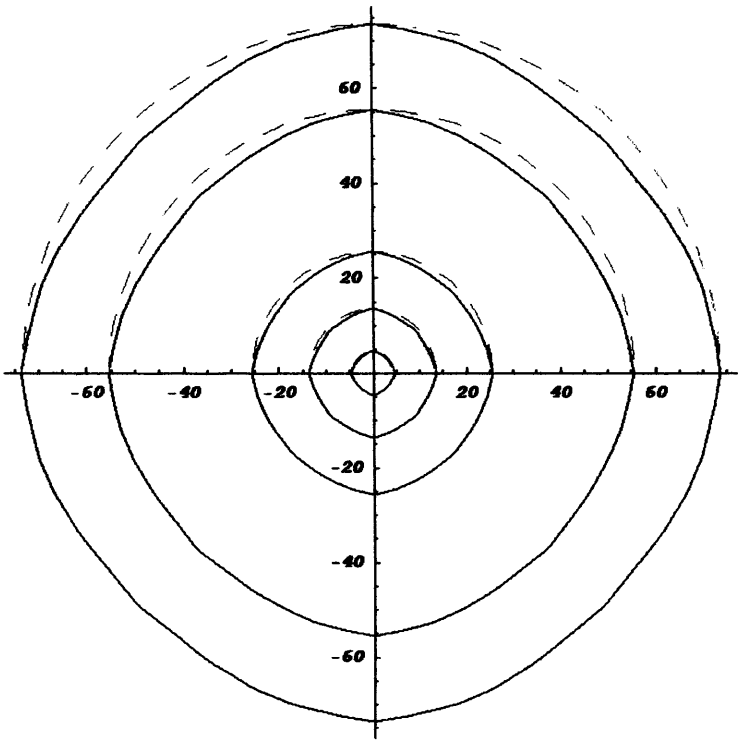

Figure 1.2: Centred Jarník polygons' of height $2, 3, 4, 5$ and 6 versus semicircles of the polygon diameters.

The expressions for $f_0(H)$ and D_H imply that if a Jarník curve of height H sits inside a circle of radius R, then $H = O(R^{1/3})$ and

$$f_0(H) = f_1(H) = O(R^{2/3}).$$

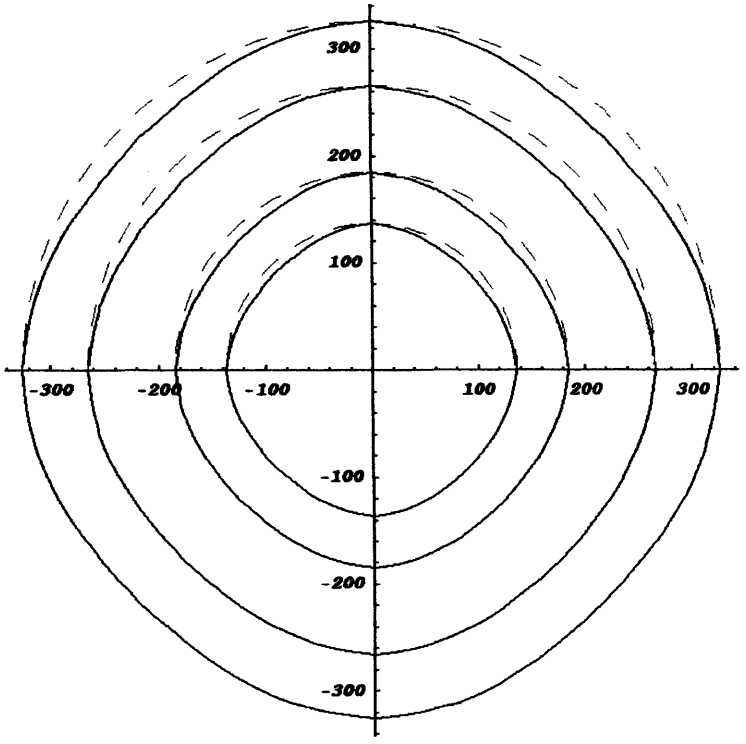

Figure 1.3: Centred Jarník polygons' of height 7, 8, 9 and 10 versus semicircles of the polygon diameters.

1.2 Moving Two-Dimensions into d Dimensions

Definition. Let $\mathbf{x} = (x_1, \ldots, x_k, \ldots, x_d)$ be a point in $\mathbb{E}^d$, let $y_i, \ldots, y_d$ represent the d co-ordinate axes and let Π be the j-dimensional plane constructed from the co-ordinate axes $y_{i_1} y_{i_2} \ldots y_{i_h} \ldots y_{i_j}$. We define the *shadow* or *projection* of the point $\mathbf{x}$ onto Π to be the point $\mathbf{x}' = (x'_1, x'_2, \ldots, x'_k, \ldots, x'_d)$, such that

$$\begin{aligned} x'_k &= x_k, \qquad k = i_h, \qquad 1 \leq h \leq j \\ x'_k &= 0, \qquad k \neq i_h, \qquad 1 \leq h \leq j. \end{aligned} \tag{1.3}$$

LEMMA 1.2.1. *Let Π be a two-dimensional plane in d-dimensional space. Let Λ be the integer lattice contained in Π with basis vectors $\mathbf{a}_1$ and $\mathbf{a}_2$ and*

let C be a Jarník curve of relative height H constructed in Λ using linear combinations of these basis vectors. That is, all edges of this Jarník curve will have vectors of the form $\lambda_1 \mathbf{a}_1 + \lambda_2 \mathbf{a}_2$, for some integers λ_1 and λ_2 with $|\lambda_1| \leq H$ and $|\lambda_2| \leq H$. If $f_0(H)$, $f_1(H)$ are the number of vertices and edges of this polygon then

$$f_0(H) = f_1(H) = \frac{24H^2(d-1)}{\pi^2} + O(H \log H).$$

Proof. The projection or shadow of a convex shape is also convex. Hence the projection of the curve C onto the two-planes y_1y_2, $y_1y_3, \ldots, y_1y_d$ yields $d-1$ convex polygons whose heights are also at most H in their respective planes. An upper bound for the maximum number of vertices and edges of each of these polygons is given in (1.1).

It only remains to check that three vertices of C that (obviously) do not lie on the same edge in Π cannot be projected into a straight line on all the planes y_1y_2, $y_1y_3, \ldots, y_1y_d$.

If this were possible, then our three vertices (under projection) would lie on the $d-1$ lines

$$\begin{aligned} y_2 &= m_2 y_1 + c_2 \\ y_3 &= m_3 y_1 + c_3 \\ &\vdots \qquad\quad \vdots \\ y_d &= m_d y_1 + c_d. \end{aligned}$$

Equating these $d-1$ equations yields

$$y_1 = \frac{y_2 - c_2}{m_2} = \frac{y_3 - c_3}{m_3} = \ldots = \frac{y_d - c_d}{m_d},$$

which is just the equation of the straight line

$$\ell = (0, c_2, c_3 \ldots, c_d) + y_1(1, m_2, m_3, \ldots, m_d)$$

in d-dimensional space contradicting our initial assumption. Therefore an upper bound for the number of edges or vertices of C is given by $d-1$ times the upper bound in (1.1) and hence the result. □

Chapter 2

The Integer Points Close to a Curve

This chapter gives a new proof of the simplest non-trivial upper bound on the number of integer points lying on or near to a convex closed curve in the plane.

2.1 Edges and Vertices

We consider the convex closed curve C, which sits in a circle of radius $c_1 M$ in the plane. We assume that C has a continuous radius of curvature ρ at each point, which remains in some range

$$0 < \rho \leq c_1 M$$

for some constant $c_1 \geq 1$.

The integer points S lying on C (if any) form a convex polygon with each side having a rational gradient as the vertices of the polygon are integer points. If the points of S lie within a distance δ of the curve with δ small, where P is a point of S and Q is the nearest point on the curve C, then for Y, the centre of curvature of C at the point Q we have

$$YQ = \rho M,$$

implying that

$$\rho M - \delta \leq YP \leq \rho M + \delta,$$

so P lies between two concentric circles centre Y, radii $\rho M + \delta$ and $\rho M - \delta$. Therefore there are two curves C_1 and C_0 with the same centres of curvature as C, distance 2δ apart measured along a common normal, and all the points of S lie between C_1 and C_0. If δ is small, then the points will all form a convex polygon. In any case, we can join up the points to obtain the smallest convex polygon that contains all of our integer points. We call this convex polygon the polygonal convex hull, $\mathcal{P}$, of the set of integer points S.

Definition (major and minor arcs).

(i) A major arc is a side of our polygonal convex hull $\mathcal{P}$ with three or more integer points lying on it.

(ii) A minor arc is a side of $\mathcal{P}$ that has only two integer points lying on it, namely its end points.

(iii) A major arc of $\mathcal{P}$ can be partitioned into components which are the parts of the side that are within a distance δ from the curve.

(iv) For a given side length $L \geq 1$, we can partition the sides of $\mathcal{P}$ into two categories such that short sides have length $\leq L$ and long sides have length $> L$.

LEMMA 2.1.1. *The number of sides of the convex polygon is*

$$\leq 15\,(c_1 M)^{2/3}.$$

Proof. Every side of $\mathcal{P}$ has a gradient, where each gradient can occur at most twice due to the nature of convex polygons.

The equation of each polygon side can be written in the form

$$ax + by = d, \qquad (a,b) = 1, \qquad \text{gradient} = -a/b.$$

If two points (x_1, y_1), (x_2, y_2) lie on such a side, then

$$ax_1 + by_1 = ax_2 + by_2 = d,$$

$$-a(x_2 - x_1) = b(y_2 - y_1),$$

$$-\frac{a}{b} = \frac{y_2 - y_1}{x_2 - x_1},$$

$$(y_2 - y_1) = -da, \qquad (x_2 - x_1) = db,$$

and this implies that consecutive integer points lying on a side of $\mathcal{P}$ are separated by the vector $(b, -a)$.

We take the convention that either $b \geq 1$ or $b = 0$ and $|a| = 1$. For short sides of $\mathcal{P}$, those with length $\leq L$, each gradient occurs at most twice with

$$1 \leq b \leq L, \qquad -L \leq a \leq L.$$

This gives at most $1 + L(2L+1)$ possible gradients of short sides so at most $2(1 + L(2L+1))$ possible short sides. Let n_s be the number of short sides and n_l the number of long sides so that

$$n_s \leq 4L^2 + 2L + 1 \leq 7L^2,$$

and for $L \geq 2$ this reduces to

$$n_s \leq 6L^2. \tag{2.1}$$

Regarding n_l, let $P_1, \cdots, P_n$ be the integer point vertices of our convex polygon with $Q_1, Q_2, \cdots, Q_n$ the integer points inside the convex hull such that $P_1Q_1P_2, P_2Q_2P_3, \cdots, P_{n-1}Q_{n-1}P_n, P_nQ_nP_1$ form n right-angled triangles whose vertices are integer points.

Repeated use of the triangle inequality yields

$$\sum_{r=1}^{n} P_rP_{r+1} \leq \sum_{r=1}^{n} P_rQ_r + \sum_{r=1}^{n} Q_rP_{r+1},$$

and relating this to the diameter of the circle gives.

$$\sum_{r=1}^{n} P_rP_{r+1} \leq 4c_1M + 4c_1M = 8c_1M.$$

Now, in the long side case we have $P_rP_{r+1} \geq L$, where P_{n+1} also denotes P_1. Hence

$$n_l < \frac{8c_1M}{L}. \tag{2.2}$$

We choose L to equate the upper bounds for the numbers of long sides and the number of short sides, so

$$\frac{8c_1M}{L} = 6L^2,$$

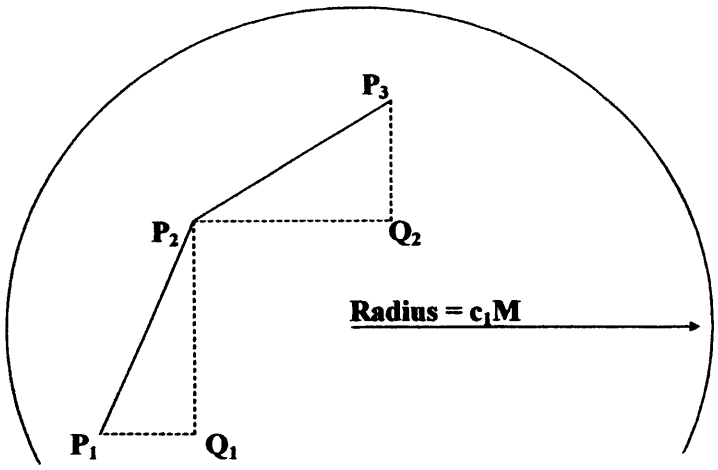

Figure 2.1:

when

$$L = \left(\frac{4c_1M}{3}\right)^{1/3}. \tag{2.3}$$

The number of vertices of the convex polygon is the same as the number of sides,

$$\leq n_s + n_l \leq 12\left(\frac{4c_1M}{3}\right)^{2/3} \leq 15(c_1M)^{2/3}.$$

□

LEMMA 2.1.2. *A set of K integer points $P_i, 1 \leq i \leq K$ that do not all lie on a straight line form $K-2$ non-overlapping triangles with integer corners.*

Proof. If $K = 3$ then we have a triangle as the three points are distinct. We now assume true for $K = t$ integer points, so that the t points form $t-2$ non-overlapping triangles. Considering $K = t+1$ points, we define the convex hull to be the smallest convex polygon which contains all of the $t+1$ points. An "outside point" is a vertex of the convex hull.

Now we re-number the points such that P_{t+1}, P_t are the two outside points that are closest together, continuing anti-clockwise with $P_{t-1}, P_{t-2}, \ldots$ around

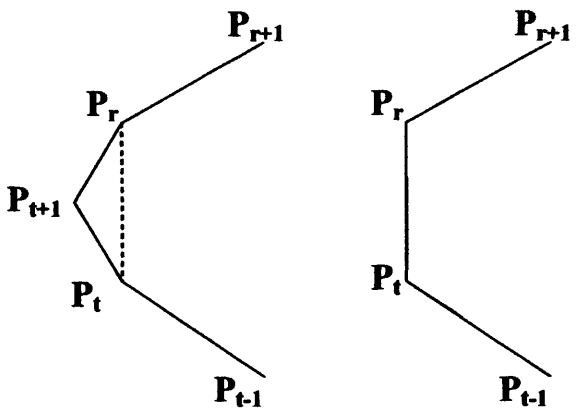

Figure 2.2:

the convex hull until the hull is re-numbered at point P_r. The "inside points" take the values $P_{r-1}, \ldots, P_1$.

If we remove the point P_{t+1} then by Figure 2.2, the convex hull gets smaller and what we lose is a triangle when we drop down to the convex hull of the other t points.

By our inductive assumption, the $t+1$ points $P_1, P_2, \cdots, P_{t+1}$ form $t-1$ non-overlapping triangles $= (t+1) - 2$. If all of the points bar one lie on a straight line then we again have $t-1$ triangles. Therefore, true for $K = t$ implies true for $K = t+1$. □

LEMMA 2.1.3. *The number of integer points lying within a short distance δ of C is*

$$\leq 8\pi\delta c_1 M. \tag{2.4}$$

Proof. Given that the integer point vertices of our convex polygon and any integer points contained within it lie within a distance δ from the closed convex curve C, we can associate a rectangle of width 2δ with each side of the polygonal convex hull where the rectangles will overlap.

Any integer points inside the polygon must lie within a distance 2δ of the nearest polygon side. For each rectangle, if L is the length of the polygon side, then either all of the integer points lie on the polygon side or there are K points forming $K-2$ triangles. The area of a triangle with integer points vertices is $\geq 1/2$. Hence in the latter case, the total area of the $K-2$

triangles satisfies

$$\frac{K-2}{2} \leq 2\delta L,$$
$$(K-2) \leq 4\delta L.$$

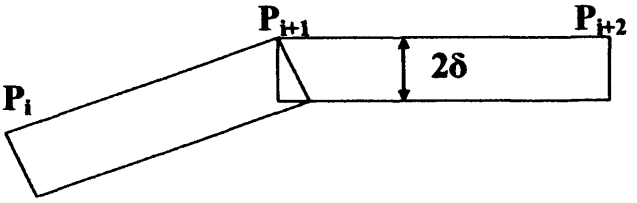

Figure 2.3:

Summing over the polygon sides we have

$$\sum_{i=1}^{n_s+n_l} P_iP_{i+1}(K-2) \leq 4\delta \sum_{i=1}^{n_s+n_l} L_i \leq 4\delta(2\pi c_1 M), \tag{2.5}$$

where $P_iP_{i+1}(K-2)$ is the number of such integer points (not including the end points) associated with the polygon side P_iP_{i+1} and L_i is the length of the side. Therefore, the total number of integer points that lie strictly inside the polygonal convex hull is $\leq 8\pi\delta c_1 M$. □

2.2 Major and Minor Arcs

As stated at the beginning of Section 2.1, a major arc can be partitioned into components, which are the parts of the side that are within a distance δ from the curve.

LEMMA 2.2.1. *A major arc of a convex curve has at most two components.*

Proof. We initially assume that a chord AB of a convex curve has three components AP_1, P_2P_3, P_4B with perpendiculars of length δ to the curve $P_1Q_1, P_2Q_2, P_3Q_3, P_4Q_4$, where $P_1 \neq P_2$, $P_3 \neq P_4$ and length $AP_1 < AP_2 < AP_3 < AP_4$. These conditions imply that the perpendicular distance from

any point P' lying between P_1 and P_2 on the chord to the curve is $> \delta$ and similarly for P'' lying between P_3 and P_4. Therefore, the line parallel to and at a distance δ from the chord AB must cut the curve twice, once between P_1 and P_2 and once between P_3 and P_4. In total, the line cuts the curve four times, which contradicts the definition of convexity. □

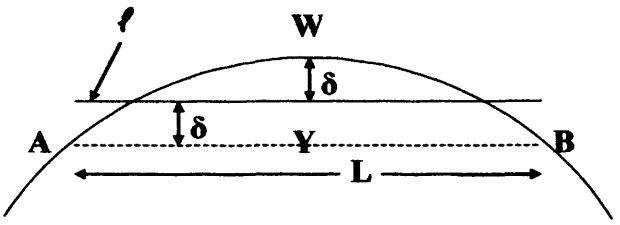

Figure 2.4:

LEMMA 2.2.2. *Let L be the length of a component of a major arc. Then*

$$L \leq L^\star = 4\sqrt{\delta c_1 M}. \tag{2.6}$$

A chord AB of C_1, tangent to C_0 has length

$$4\sqrt{\delta c_0 M} \leq AB \leq 4\sqrt{\delta c_1 M} \tag{2.7}$$

Proof. We look at a continuous part of the line ℓ that stays within a distance δ of the curve.

From Figure 2.4, we get a chord AB of the curve, equal and parallel to the segment of the line ℓ, and the curve stays within a distance 2δ from the line AB as depicted in Figure 2.5.

Applying circular geometry to the circle radius R with respect to the mid-point Y of chord AB we find that

$$-AY.YB = -WY.YX,$$

so that

$$\left(\frac{L}{2}\right)^2 = 2\delta(2R - 2\delta) \leq 4\delta R. \tag{2.8}$$

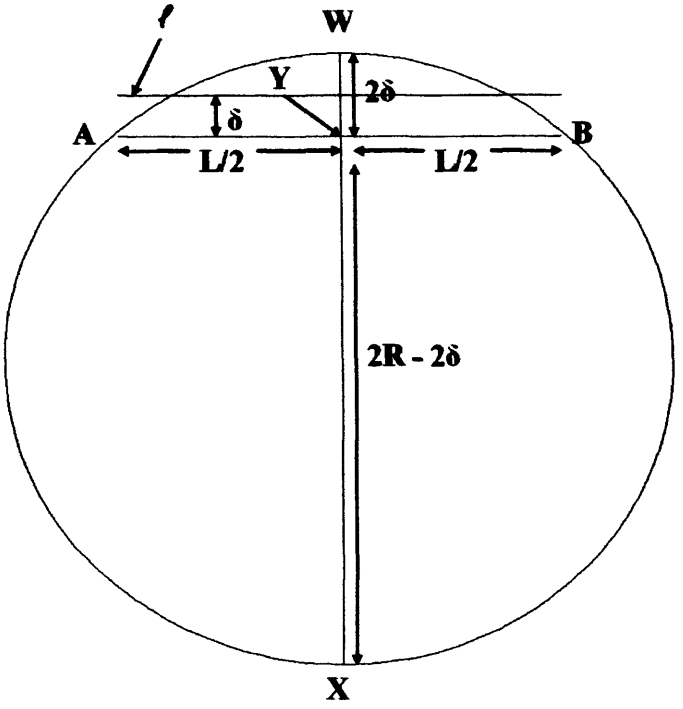

Figure 2.5:

This is maximal when the radius of curvature, R, is a large as possible, with $R = c_1 M - 1/2 < c_1 M$. Hence the maximum length, L, of a component is $\leq 4\sqrt{\delta c_1 M} = L^*$.

The lower bound in (2.7) corresponds to the case when the curve has minimal radius of curvature $R = c_0 M + 1/2$. In this instance, by (2.8)

$$AB = 2AY = 4\sqrt{\delta(R-\delta)} \geq 4\sqrt{\delta c_0 M}.$$

□

LEMMA 2.2.3. *The number of integer points lying on the sides of the major arcs of the polygon is bounded above by*

$$192\delta c_1 M. \tag{2.9}$$

Proof. The equation of each polygon side can be written in the form

$$ax + by = d, \qquad (a,b) = 1, \qquad \text{gradient} = -a/b,$$

where, by the proof of Lemma 2.1.1, consecutive integer points lying on a major arc are separated by the vector $(b, -a)$.

Let L be the length of the polygon side. The number of integer points on the side, excluding the right hand endpoint which is counted with the integer points on the following side, is

$$K = \frac{L}{\sqrt{a^2 + b^2}}. \tag{2.10}$$

Now we number the polygon sides as in Lemma 2.1.3, so that the gradient of the i-th side is $-a_i/b_i$, the length is L_i, and the number of integer points (counting P_i but not P_{i+1}) is K_i.

We recall the properties of the Farey sequence $\mathcal{F}(Q)$, which consists of those fractions c/q with $0 \le c \le q$, $1 \le q \le Q$ in lowest terms, so that $(c,q) = 1$, arranged in ascending order. The height of c/q is $\max(|c|, q) = q$, and for $q \ge 2$ the number of Farey fractions of height q is $\phi(q)$ (provided that $q \le Q$).

To allow for negative gradients, we extend the Farey sequence to allow $-q \le c \le q$. We map the gradient $-a/b$ to a fraction c/q with

$$q = \max(|a|, |b|) \le Q = [L^*],$$

$$|c| = \min(|a|, |b|), \qquad \text{sign} = \text{sign}(-a/b),$$

where L^* is the upper bound of Lemma 2.2.2. Each gradient occurs at most twice in the polygon, so at most four sides of the polygon are mapped to the same Farey fraction c/q in $[-1, 1]$.

In (2.10) we have

$$K = \frac{L}{\sqrt{c^2 + q^2}} \le \frac{L^*}{q}.$$

The polygon sides give various Farey fractions c/q. We rearrange them in increasing order, omitting repeats, as c_n/q_n, $n = 1, \ldots, N$. Then

$$2 \ge \left(\frac{c_N}{q_N} - \frac{c_1}{q_1}\right) = \sum_{n=1}^{N-1} \left(\frac{c_{n+1}}{q_{n+1}} - \frac{c_n}{q_n}\right)$$

$$\geq \sum_{n=1}^{N-1} \frac{1}{q_n q_{n+1}} \geq \sum_{n=1}^{N-1} \frac{1}{q_n L^\star},$$

since $q_{n+1} \leq L^\star$ from (2.10). Adding the term $n = N$, we deduce that

$$\sum_{n=1}^{N} \frac{1}{q_n L^\star} \leq 2 + \frac{1}{q_N L^\star} \leq 2 + \frac{1}{L^\star},$$

which yields

$$\sum_{n=1}^{N} \frac{L^\star}{q_n} \leq 2L^{\star 2} + L^\star.$$

Recalling that each Farey fraction c/q corresponds to at most four polygon sides, we see from (2.10) that the total number of integer points lying on the major arcs is

$$\leq 4 \sum_{n=1}^{N} \frac{L^\star}{q_n} \leq 8L^{\star 2} + 4L^\star \leq 12(L^\star)^2.$$

$$\leq 192 \delta c_1 M.$$

□

LEMMA 2.2.4. *The total number of integers points (excluding righthand endpoints) of "long" minor arcs, those with length at least*

$$L = \left(\frac{4c_1 M}{3}\right)^{1/3},$$

is

$$\leq 6(c_1 M)^{2/3}. \tag{2.11}$$

Proof. Each long minor arc has length $\geq L$ where

$$L = \left(\frac{4c_1 M}{3}\right)^{1/3},$$

and we only count the left hand end points so that the total number of integer points equals the total number of long minor arcs. This gives an upper bound of

$$\leq \frac{2\pi c_1 M}{L} = 2\pi c_1 M \left(\frac{3}{4c_1 M}\right)^{1/3} \leq 6(c_1 M)^{2/3}.$$

□

In the next Lemma we count all of the minor arc sides of the polygon $\mathcal{P}$ whose height, as defined in Chapter 1, is at most H. Since the length of a minor arc is at least its height, and at most $\sqrt{2}$ times its height, we can take $H = L$ to give an upper bound for the number of integer points contributed by the short minor arcs (length $\leq L$) of $\mathcal{P}$.

LEMMA 2.2.5. *Let $H \geq 2$. Let N_s be the number of integer points belonging to minor arc sides of the polygon $\mathcal{P}$ (excluding right hand end points) whose height is at most H. Then we have the bounds*

$$N_s \leq \frac{24H^2}{\pi^2} + O(H \log H),$$

and

$$N_s \leq 8H^2.$$

For

$$H = \left(\frac{4c_1 M}{3}\right)^{1/3}, \tag{2.12}$$

we have

$$N_s \leq 10\,(c_1 M)^{2/3} \tag{2.13}$$

COROLLARY 1. *The number of vertices of the Jarník polygon of height H (defined in Chapter 1) is given by*

$$4 + 4 \sum_{\substack{a=1 \\ (a,q)=1}}^{H} \sum_{q=1}^{H} 1 = \frac{24H^2}{\pi^2} + O(H \log H). \tag{2.14}$$

COROLLARY 2. *The diameter of the Jarník polygon of height H is given by*

$$\frac{6H^3}{\pi^2} + O(H^2 \log H). \tag{2.15}$$

Proof. Counting the number of points becomes counting the number of sides. Each side has a gradient a/b corresponding to a Farey Fraction of height at most H. The number of such fractions including repeat sides, extended Farey Fractions and negative gradients is eight times this.

For each height $h, 1 \leq h \leq H$, the total number of strict Farey Fractions is $\phi(h)$ and using Mobius Inversion we have

$$\phi(h) = h\sum_{d|h} \frac{\mu(d)}{d} = h\sum_{\substack{d \\ de=h}}\sum_{e} \frac{\mu(d)}{d}$$

$$= \sum_{de=h}\sum_{e} de.\frac{\mu(d)}{d} = \sum_{\substack{d \\ de=h}}\sum_{e} e\mu(d).$$

Hence by a standard computation [37] we have

$$\sum_{h=1}^{H} \phi(h) = \frac{H^2}{2}.\frac{1}{\zeta(2)} + O(H\log H)$$

$$= \frac{H^2}{2}.\frac{6}{\pi^2} + O(H\log H) = \frac{3H^2}{\pi^2} + O(H\log H).$$

Therefore, the total number of short sides or their integer point vertices is

$$\leq \frac{24H^2}{\pi^2} + O(H\log H).$$

To see that this must be $\leq 8H^2$, we consider all possible vectors of the form (e, f), with $0 \leq |e|, |f| \leq H$, for which there are $(2H+1)^2 \leq 8L^2$ $(H \geq 2)$ choices, and

$$8\left(\frac{4c_1M}{3}\right)^{2/3} \leq 10(c_1M)^{2/3}.$$

The first Corollary follows directly from Lemma 2.2.5, as the Jarník polygon incorporates every possible primitive gradient twice. To see the second Corollary we note that the height of the Jarník polygon along the y-axis has length

$$1 + 2\sum_{\substack{q=1 \\ (a,q)=1}}^{H}\sum_{a=1}^{H} a = 1 + \frac{2H(H+1)}{2}\sum_{\substack{q=1 \\ (a,q)=1}}^{H} 1$$

$$= (H(H+1)\left(\frac{6H}{\pi^2} + O(\log H)\right)$$

$$= \frac{6H^3}{\pi^2} + O(H^2\log H).$$

□

THEOREM 2.2.6. *The total number of integer points lying on or within a distance δ from a convex closed curve with a radius of curvature ρ at each point, satisfying $0 < \rho \leq R$, in the plane is*

$$\leq 16(R)^{2/3} + 200\delta R. \tag{2.16}$$

Proof. The radius R of the theorem is $c_1 M$ in the notation of Lemmas numbered 2.2.5, 2.2.4, 2.2.3 and 2.1.3. The choices of L and of H ensure that every minor arc is counted either as long in Lemma 2.2.4 or short in Lemma 2.2.5 or in both, since the length of a minor arc is at least its height, and at most $\sqrt{2}$ times its height.

Collecting together the individual upper bounds (2.13), (2.11), (2.9) and (2.4), we have.

$$\leq (10+6)(c_1 M)^{2/3} + (192+8)\delta c_1 M$$

integer points, and hence the result. □

Remark. A result due to Martin [29] proves that the fundamental arcs of the scaled Jarník polygons (diameter equal to two) converge to the arc C_J defined by

$$y = \frac{3}{4}x^2 - 1, \qquad -\frac{2}{3} \leq x \leq \frac{2}{3}, \tag{2.17}$$

and the arcs obtained by repeatedly rotating C_J by 90° about the origin. For clarity we restate Martin's definition of convergence.

Definition. Let C_H be the fundamental arc of the Jarník polygon of height H in $\mathbb{R}^2$, and for $\epsilon > 0$, let $C_J(\epsilon)$ denote the ϵ-neighbourhood of C_J, that is, the set of all points whose distance to C_J is less than ϵ. Then we say that the sequence of curves $C_1, C_2, \ldots$ converge to C_J if for every $\epsilon > 0$ there exists some integer H such that C_H is contained in $C_J(\epsilon)$ for every $H \geq H(\epsilon)$.

The scaled length, λ_H, of the scaled Jarník polygon of height H converges to four times the length of C_J, which can be calculated as

$$\theta = \frac{8\sqrt{2}}{3} + \frac{8}{3}\ln(1+\sqrt{2}),$$

$$= 6.12157\ldots = (0.974277\ldots) \times 2\pi,$$

which is less than the circumference of the unit circle.

Table 2.1: Jarník polygon dimensions (6 significant figures).

Height H	**Vertices**	**Diameter** D_H	**Length** λ_H	$\pi \times D_H$	$\lambda_H/\pi D_H$
1	8	3	9.65685	9.42477	1.0246
2	16	9	27.5454	28.2743	0.97422
3	32	27	81.688	84.823	0.963041
4	48	51	154.673	160.221	0.965373
5	80	111	336.419	348.717	0.964734
6	96	147	447.563	461.814	0.969141
7	144	273	830.372	857.655	0.968189
8	176	369	1123.73	1159.25	0.969359
9	224	531	1618.64	1668.19	0.970297
10	256	651	1987.84	2045.18	0.971963
20	1024	5235	16001.9	16446.2	0.972985

It is interesting to see how fast the Jarník polygon attains its limiting shape. In table 2.1 we have calculated values for $H = 1, \ldots 10$ and $H = 20$. Numerically we seem to have

$$0.963 < \frac{\lambda_H}{\pi D_H} < \theta, \tag{2.18}$$

for $H \geq 2$.

Chapter 3

Curvature, Surfaces and Polytopes in $\mathbb{E}^d$

This chapter underpins the structure of convex hypersurfaces and polytopes in d-dimensional Euclidean space.

3.1 Convex and Affine Spaces

We recall that an r-dimensional linear subspace in $\mathbf{E}^d$ is an r-dimensional plane through the origin, whereas an affine subspace of r-dimensions does not have to pass through the origin.

In order to rigorously work within the bounds of convex and affine Euclidean spaces we now state (without proof) some fundamental results quoted from McMullen and Shephard [30].

PROPOSITION 3.1.1. *A subset A of $\mathbf{E}^d$ is convex if and only if for all $\mathbf{x}_0, \mathbf{x}_1 \in A$, and $0 \leq \lambda \leq 1$, the point*

$$\mathbf{x} = (1 - \lambda)\mathbf{x}_0 + \lambda \mathbf{x}_1$$

also belongs to A.

Geometrically this means that A is convex if and only if it contains all the line segments whose end points lie in A.

PROPOSITION 3.1.2. *If A_1 and A_2 are affine subspaces of $\mathbf{E}^d$, then $A_1 \cap A_2$ is an affine subspace and either*

$$A_1 \cap A_2 = \phi,$$

or

$$\dim(A_1 \cap A_2) \geq \dim A_1 + \dim A_2 - d.$$

PROPOSITION 3.1.3. *If H is a convex polytope in $\mathbb{E}^d$, and A is any affine subspace of $\mathbb{E}^d$, then $A \cap H$ is also a convex polytope.*

3.2 Parallelism and Orthogonality in $\mathbb{E}^d$

To clarify the parallel condition in higher dimensions, we introduce the idea of degrees of parallelism as described in [38].

Definition (degrees of parallelism in higher dimensions). Let Π_1 and Π_2 be two planes of dimension p and q $(p \geq q)$ respectively in $\mathbb{E}^d$ that have no point in common. Let Ψ be the plane of least dimension $p + q - r$ that contains both Π_1 and Π_2. Then Π_1 and Π_2 intersect in an r-plane at infinity and we say that Π_1 and Π_2 are $(r+1)/q$ parallel.

If $p = q$ and $r = p-1$, then $p+q-r = p+1$, and Π_1 and Π_2 are contained in the $(p+1)$-plane Ψ. We say that Π_1 and Π_2 are *completely parallel.* When this occurs, then through each point O in Ψ there is a unique line in Ψ that is normal to both Π_1 and Π_2. If two normals are drawn through two points O, O', cutting Π_1 and Π_2 in A, B and A', B' then $ABB'A'$ is a rectangle and $AB = A'B'$. The distance AB is called the distance between the completely parallel p-planes.

We deduce that if two completely parallel p-planes share a common point, then they are in fact the same p-plane.

In contrast to complete parallelism, we again refer to [38] in order that we may clarify complete orthogonality in higher dimensions.

Definition (systems of d mutually orthogonal lines). Through any point O in $\mathbb{E}^d$ we can find d lines that are all mutually perpendicular. We begin with a line l_1. All lines perpendicular to l_1 through O form a $(d-1)$-plane Π_1 whose normal vector at O is l_1. Let l_2 be one of these lines and let Π_2 be the $(d-1)$-plane whose normal vector at O is l_2. Then all lines perpendicular to both l_1 and l_2 at O lie in the $(d-2)$-plane that is the intersection of Π_1 and Π_2. Let l_3 be one of these lines. Continuing in this manner we create a system of d lines $l_1, l_2, \ldots, l_d$ that are all mutually perpendicular. Any p of these lines determine a p-plane Ψ_p, and the remaining $d-p$ lines determine a $(d-p)$-plane Ψ_{d-p}. These two planes only intersect at O and have the

property that every line of Ψ_p through O is perpendicular to every line of Ψ_{d-p} through O. The two planes Ψ_p and Ψ_{d-p} are said to be *completely orthogonal*.

We deduce that for Ψ_p, defined as above and containing the point O, there exists a unique $(d-p)$-plane Ψ_{d-p} that is completely orthogonal to Ψ_p through O. Hence for a given system of d mutually orthogonal lines in $\mathbb{E}^d$ and any point O, for each partition of the lines into two sets containing p and $d-p$ lines there exists a *unique pair of completely orthogonal planes*, Ψ_p and Ψ_{d-p}, that intersect only at O,

3.3 Curvature, Shells and d-Surfaces

In 3-dimensional Euclidean space we define the normal curvature at a point on a surface C in terms of the two principal curvatures r_1 and r_2 that correspond to the principal directions $\mathbf{d}_1$ and $\mathbf{d}_2$ in which the surface torsion is zero. For a non-spherical point on a convex surface there are only two principal direction and they are orthogonal, whereas at a spherical point (locally the surface resembles that of a sphere), all orthogonal directions are principal. Hence, on a sphere, any two orthogonal directions are principal directions so that the principal curvatures are equal and the surface torsion is always zero.

If we consider a direction on the surface that makes an angle θ with the principal direction $\mathbf{d}_1$ (corresponding to principal curvature r_1) and an angle $(90° - \theta)$ with principal direction $\mathbf{d}_2$ (corresponding to principal curvature r_2), then we find that the surface normal curvature $r(\theta)$ and surface torsion $t(\theta)$ in this direction are dependant on the principal curvatures. These results can be expressed via two famous formulae attributed to Leonhard Euler and Sophie Germain respectively:

$$r(\theta) = r_1 \cos^2\theta + r_2 \sin^2\theta, \tag{3.1}$$

$$t(\theta) = (r_2 - r_1)\sin\theta\cos\theta. \tag{3.2}$$

so that r_2 and r_1 define the upper and lower bounds for the normal curvature and C has continuous radius of normal curvature ρ at each point such that

$$\rho = \left| \frac{1}{r_1 \cos^2\theta + r_2 \sin^2\theta} \right|. \tag{3.3}$$

For proofs of these results we refer the reader to [34]. We note that for a point P on a convex surface, either $r_2 \geq r_1 > 0$ or $0 > r_2 \geq r_1$, for if $r_2 > 0 > r_1$ then the point is hyperbolic and if r_2 or r_1 is equal to zero then the point is parabolic. Therefore, on a convex surface, each point is either elliptic with $r_2 \neq r_1$ or spherical with $r = r_2 = r_1$. In the latter case the radius of normal curvature ρ can be expressed simply as

$$\rho = \left|\frac{1}{r}\right|. \tag{3.4}$$

We now generalise these ideas to surfaces in higher dimensions.

Hypersurface Conditions (in $\mathbf{E}^d$).

(1) A hypersurface C is essentially an $(d-1)$-dimensional manifold embedded in d-dimensional space such as a two-dimensional surface in three-dimensional space.

(2) For a given point P on a hypersurface C in d-dimensional space there exist $(d-1)$ principal directions $\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_{d-1}$ that essentially amount to a preferred orthogonal basis for the tangent hyperplane to the hypersurface at P, where the d-th possible orthogonal direction $\mathbf{n}$ is normal to the tangent hyperplane.

(3) The normal curvatures $r_1, r_2, \ldots, r_{d-1}$ for a point P on the hypersurface C can be determined by evaluating the cross-sectional curvatures of C along the principal directions in the tangent hyperplane at P. These normal curvatures of the hypersurface in the respective principal directions $\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_{d-1}$ are called the principal curvatures.

(4) The principal curvatures $r_1, r_2, \ldots, r_{d-1}$ effectively describe the movement of the normal vector $\mathbf{n}$ to the hypersurface C at a point P via $(d-1)$ curvature elements in orthogonal directions and are also known as the extrinsic curvatures of C at P.

For a more rigorous analysis of Conditions (2), (3) and (4), the reader may refer to the bibliography [34] as a full treatise concerning the curvature of surfaces and the many ingenious methods devised for calculating the intrinsic and extrinsic curvatures and the principal directions is worthy of a long article in its own right.

We will assume from (2) that at every point P on C there exist a tangent hyperplane, and from (3), that along any direction in this hyperplane at P we can take a two-dimensional cross-section, Π of C, as clarified below in Lemma 3.3.1. This means that C will appear in Π as a closed plane curve C', where the curve C' will then have the usual measurable properties of "curvature" and "radius of curvature".

Definition. Let C be the boundary surface of a strictly convex bounded d-dimensional body, which sits in a hypersphere of radius $c_1 M$ in d-dimensional Euclidean space. At each point P on C there exists a tangent hyperplane Ψ with normal vector $\mathbf{n}$, so that $\mathbf{n}$ is the outward normal to C at P and Ψ and $\mathbf{n}$ form a completely orthogonal pair through the point P. Let C_0 be the locus of points at distance δ from C measured along the interior normals to C, and let C_1 be the locus of points at distance δ measured along the exterior normals. Let E be the d-dimensional shell bounded by C_0 and C_1 so that E has thickness 2δ. Let S be the set of integer points in E, and let H be the convex hull of S, so that H is a d-dimensional convex polytope [4], [6], [5]. All points of S lie in H, but not all integer points on the boundary of H lie in S.

LEMMA 3.3.1. *Let Π be the two-dimensional affine plane defined by the normal $\mathbf{n}$ to C at a point P and any other point inside our convex hull H that does not lie on $\mathbf{n}$. Then C_0 and C_1 will appear in Π as convex curves seperated by a distance 2δ along the normal $\mathbf{n}$ to C at point P, and H as a convex polygon whose vertices lie between these curves.*

Proof. The space bounded by the convex hull H is full d-dimensional, and applying Proposition 3.1.2, we have

$$2 \geq \dim \Pi \geq d + 2 - d,$$

yielding $\dim \Pi = 2$. Our hypersurface C also contains a portion of d-dimensional space and so by a similar argument will contain a portion of two-dimensional space in Π bounded by a convex curve C'. As Π contains a

normal, through P, common to C_0, C and C_1, the distance along this normal between C_0' and C_1' in Π must be 2δ. By Proposition 3.1.3, $\Pi \cap H$ is a convex polytope H' lying in $\Pi \cap H$, and the vertices of H' must lie between the two convex closed curves C_0' and C_1'. Hence H' is a convex polygon in Π. □

We now formulate more concisely the conditions satisfied by the hypersurface C via these plane sectional curves.

Curvature Condition (with size parameter M). For any point P on C and any two-plane Π through the normal to C at P, let $C(\Pi, P)$ be the closed plane curve $C \cap \Pi$. Then $C(\Pi, P)$ is a twice differentiable plane curve with radius of curvature ρ lying in the range

$$c_0 M + \frac{1}{2} \leq \rho \leq c_1 M - \frac{1}{2}, \tag{3.5}$$

where the constants c_0, c_1 and δ satisfy

$$\frac{1}{M} \leq c_0 \leq 1 \leq c_1, \text{ and } \delta < \frac{1}{4}. \tag{3.6}$$

Local Curvature Condition. There is a constant κ such that for $C(\Pi, P)$ defined as above, the points Q of $C(\Pi, P)$ with $PQ \leq \kappa M$ form a twice differentiable plane curve with radius of curvature satisfying (3.5).

Definition (tac-plane). Let Ψ_0 be a hyperplane and K a closed connected set in $\mathbf{E}^d$. Then Ψ_0 is called a *tac-plane* to a set K if Ψ_0 contains at least one point of K and K is contained in one of the (closed) half-spaces bounded by Ψ_0.

LEMMA 3.3.2. *The boundary surfaces C_0 and C_1 of our shell E have a tangent hyperplane at each point Q, and their two-dimensional cross-sections $C(\Pi, Q)$ in planes normal to the tangent hyperplanes are twice differentiable, with radius of curvatures in the range*

$$c_0 M \leq c_0 M + \frac{1}{2} - \delta \leq \rho \leq c_1 M - \frac{1}{2} - \delta \leq c_1 M, \tag{3.7}$$

and

$$c_0 M \leq c_0 M + \frac{1}{2} + \delta \leq \rho \leq c_1 M - \frac{1}{2} + \delta \leq c_1 M, \tag{3.8}$$

respectively.

Proof for C_0. Let the normal from Q to C meet C at a point P. Let Ψ be the tangent hyperplane to C at P. Let Ψ_0 be the hyperplane through Q parallel to Ψ. The distance from Ψ to Ψ_0 is δ. All points of C other than P lie on the same side of Ψ, so all points of C_0 other than Q lie on the opposite side of Ψ_0 to Q, so Ψ_0 is a tac-hyperplane to C_0.

Consider a two-dimensional cross-section, Π say, through PQ. The surfaces C and C_0 meet the plane in closed curves C' and C_0'. The tangent plane Ψ and tac-plane Ψ_0 meet the plane in parallel lines ℓ and m, in a direction θ to some fixed axis. Let P be the point $(x(\theta), y(\theta))$. Then Q is the point

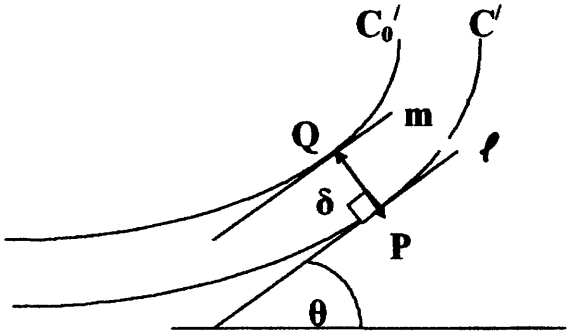

Figure 3.1:

$$(X, Y) = (x(\theta) - \delta \sin\theta, y(\theta) + \delta \cos\theta),$$

with

$$\frac{\mathrm{d}X}{\mathrm{d}\theta} = \frac{\mathrm{d}x}{\mathrm{d}\theta} - \delta\cos\theta = (\rho - \delta)\cos\theta,$$
$$\frac{\mathrm{d}Y}{\mathrm{d}\theta} = \frac{\mathrm{d}y}{\mathrm{d}\theta} - \delta\sin\theta = (\rho - \delta)\sin\theta.$$

These equations correspond to an intrinsic equation for C_0' in which there is a tangent at inclination θ, so the line m is actually tangent to C_0'. The radius of curvature of C_0' is $\rho - \delta$, which satisfies the inequalities given by (3.7) of the Lemma. Since every plane cross-section normal to Ψ_0 meets Ψ_0 in a line tangent to C_0', Ψ_0 is a tangent hyperplane to C_0 at Q, not just a tac-hyperplane. The proof for C_1 is similar. □

Remark.

(1) The parameters in (3.5) are specifically chosen so that if C is any surface satisfying the Curvature Condition, then ρ, the radius of curvature of any plane cross-sectional curve of C_0 or C_1, will obey the inequalities

$$c_0 M \leq \rho \leq c_1 M. \tag{3.9}$$

This simplifies a fundamental counting argument in following chapters where we cover the shell E, with thinner shells of thickness δ_0, and each shell will satisfy (3.9).

(2) We want to estimate the size of S in terms of δ and M, treating c_0 and c_1 as dimensionless constants.

(3) The convex hull H has hyperfaces F_i, (for facet) each with an equation of the form

$$\mathbf{n}_i.\mathbf{x}_i = D_i. \tag{3.10}$$

The hyperface or facet F_i goes through at least d integer points, so we can take $\mathbf{n}_i$ to be a primitive integer vector $(A_1, A_2, \ldots, A_d)$ and D_i to be a positive integer. Different hyperfaces F_i have different outward normal primitive integer vectors $\mathbf{n}_i$.

(4) We note that a convex hull H in two-dimensional space has the measurable quantities of one-dimensional perimeter and two-dimensional area, while in three-dimensional space, a convex hull has the measurable quantities of two-dimensional surface area and three-dimensional volume, but no measurable perimeter. Generalising to higher dimensions, we can assume that each time we step up a dimension we lose a measurable quantity from the previous dimension and gain a measurable quantity from the new dimension. Therefore we will associate two fundamental quantities with a convex hull in d-dimensional Euclidean space called the hypervolume V_d of H with dimension d and the hypersurface content S_d of H with dimension $d-1$.

LEMMA 3.3.3. *Under the Curvature Condition, the shell E containing S, the set of integer points, lies in a d-hypersphere of radius $R = c_1 M$. The volume V_d and surface content S_d of this sphere is given by the formulae*

$$V_d = \alpha_d R^d, \qquad S_d = d\alpha_d R^{d-1}, \tag{3.11}$$

where

$$\alpha_{2k} = \frac{\pi^k}{k!}, \quad \alpha_{2k+1} = \frac{2^{2k+1}\pi^k k!}{(2k+1)!}, \quad \alpha_d \leq 6, \quad \frac{\alpha_d}{\alpha_{d-1}} \leq \pi, \tag{3.12}$$

and for $d \geq 2$,

$$d\alpha_d \leq (2\pi)^{d-1}. \tag{3.13}$$

Proof. An eloquent proof of the formulaes for V_d and S_d is given in [38]. □

For example, if $d = 4$, then

$$V_4 = \alpha_4 R^4 = \frac{\pi^2}{2} R^4$$

and

$$S_4 = \beta_4 R^3 = 2\pi^2 R^3.$$

3.4 Convex Polytopes

In this section we again consider the general d-dimensional case, so that the convex hull H of the set of integer points S is a d-dimensional convex polytope $\mathcal{P}$, where $d \geq 2$.

LEMMA 3.4.1. *To each hypersurface face of the convex polytope* $\mathcal{P}$ *we assign a standard normal vector; this is the unique outward normal integer vector* $(A_1, A_2, \ldots, A_d)$, *which is primitive in the sense that* $hcf(A_1, A_2, A_3, \ldots, A_d) = 1$. *Then for each* $N \geq 1$ *there are*

$$\frac{\alpha_d N^d}{\zeta(d)} + O(N^{d-1}) \leq 3^d N^d \tag{3.14}$$

hyperfaces of $\mathcal{P}$ *whose standard normal vector has length at most* N.

Proof. Let $r_d(n)$ [16], [37] be the number of solutions to

$$A_1^2 + A_2^2 + A_3^2 + \ldots + A_d^2 = n, \tag{3.15}$$

and $S(N^2)$ the sum of all of these solutions so that

$$S(N^2) = \sum_{n=1}^{N^2} r_d(n). \tag{3.16}$$

If $(A_1, A_2, A_3 \ldots A_d)$ are integer solutions to (3.15) then they are also the co-ordinates of a lattice point on a hypersphere of radius $\sqrt{n}$. The set of all lattice points on this hypersphere correspond to the different (if not distinct) solutions to (3.15) and there number is counted exactly by $r_d(n)$.

We think of hypercubes of hypervolume 1 centred at each of these lattice points, thereby completely filling a portion of hyperspace without overlapping as each point corresponds to some solution of (3.15).

Therefore $S(N^2)$ is the volume of all these hypercubes with centres inside or on the hypersphere of radius N. The distance between the centre and vertex of a hypercube is $\sqrt{d}/2$, so that the total volume is enclosed by a hypersphere of radius

$$R = N + \frac{\sqrt{d}}{2},$$

and completely contains the sphere of radius

$$r = N - \frac{\sqrt{d}}{2},$$

so that

$$\alpha_d r^d \leq S(N^2) \leq \alpha_d R^3,$$

$$\alpha_d \left(N - \frac{\sqrt{d}}{2} \right)^d \leq S(N^2) \leq \alpha_d \left(N + \frac{\sqrt{d}}{2} \right)^d.$$

Hence

$$S(N^2) = \sum_{n=1}^{N^2} r_d(n) = \alpha_d N^d + O(N^{d-1}). \tag{3.17}$$

To obtain the average value of r_d over these N^2 values, we divide the sum by N^2 and denote this average by $\bar{r_d}$, so that

$$\bar{r_d}(N^2) = \alpha_d N^{d-2} + O(N^{d-3}). \tag{3.18}$$

If $e = hcf(A_1, A_2, A_3, \ldots, A_d)$, then there exists an integer n' such that $n^2 = (n')^2 e^2$ and

$$r_d(n) = \sum_{e^2 | n} R_d \left(\frac{n}{e^2} \right),$$

where $R_d(n)$ is the number of primitive solutions to (3.15).

Using Mobius Inversion [37] we have

$$R_d(n) = \sum_{e^2|n} \mu(e) r_d\left(\frac{n}{e^2}\right),$$

and

$$\sum_{n=1}^{N^2} R_d(n) = \sum_{n=1}^{N^2} \sum_{\substack{e=\sqrt{n} \\ \sqrt{n}\in \mathbf{N}}} \mu(e) r_d\left(\frac{n}{e^2}\right)$$

$$= \sum_{e\le N} \mu(e) \sum_{\substack{n\equiv 0 \pmod{e^2} \\ n\le N^2}} r_d\left(\frac{n}{e^2}\right) = \sum_{e\le N} \mu(e) \sum_{n\le N^2/e^2} r_d(n)$$

$$= \sum_{e\le N} \mu(e) \left\{ \frac{\alpha_d N^d}{e^d} + O\left(\frac{N^d}{e^{d-1}}\right)\right\} = \alpha_d N^d \sum_{e\le N} \frac{\mu(e)}{e^d} + O\left(N^{d-1} \sum_{e\le N} \frac{|\mu(e)|}{e^{d-1}}\right)$$

$$= \frac{\alpha_d N^d}{\zeta(d)} + O\left(\frac{N^{d-1}\zeta(d-1)}{\zeta(2d-2)}\right).$$

Hence

$$\sum_{n=1}^{N^2} R_d(n) = \frac{\alpha_d N^d}{\zeta(d)} + O(N^{d-1}).$$

To see that the constant in this order of magnitude is $\le 3^d$, we note that there are $(2N+1)$ possibilities for each vector entry so that the total possible number of vectors is

$$(2N+1)^d \le 3^d N^d. \qquad \square$$

If d=4, then we have $\le 81N^4$ facets of $\mathcal{P}$ whose standard normal vector has length at most N.

The next two results are stated without proof as their derivations are well documented [38].

LEMMA 3.4.2. *The d-dimensional hypervolume of the simplex with corners* $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \ldots, \mathbf{x}_{d+1}$, *where* $\mathbf{x}_i$ *is the row vector*

$$\mathbf{x}_i = (x_{i1}, x_{i2}, x_{i3}, \ldots, x_{id}),$$

is given by

$$V^{(d)}(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \ldots, \mathbf{x}_{d+1}) = \frac{\pm 1}{d!} \begin{vmatrix} 1 & \mathbf{x}_1 \\ 1 & \mathbf{x}_2 \\ 1 & \mathbf{x}_3 \\ \vdots & \vdots \\ 1 & \mathbf{x}_{d+1} \end{vmatrix},$$

the sign being chosen to make the right hand side non-negative.

If $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \ldots, \mathbf{x}_{d+1}$ are integer vectors not all in the same hyperplane, then

$$V^{(d)}(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \ldots, \mathbf{x}_{d+1}) \geq \frac{1}{d!}.$$

LEMMA 3.4.3. *In d-dimensional space, the perpendicular distance from the point* $\mathbf{y}$ *to the hyperplane with with equation*

$$A_1 x_1 + A_2 x_2 + A_3 x_3 + \ldots A_d x_d = E$$

is

$$D = \left| \frac{A_1 y_1 + A_2 y_2 + A_3 y_3 + \ldots A_d y_d - E}{\sqrt{(A_1^2 + A_2^2 + A_3^2 + \ldots + A_d^2)}} \right|.$$

If the point and the equation both have integer coefficients, and the point $\mathbf{y}$ does not lie on the hyperplane, then for some positive integer k

$$D = \left| \frac{k}{\sqrt{(A_1^2 + A_2^2 + A_3^2 + \ldots + A_d^2)}} \right| \geq \left| \frac{1}{\sqrt{(A_1^2 + A_2^2 + A_3^2 + \ldots + A_d^2)}} \right|. \tag{3.19}$$

LEMMA 3.4.4. *Let W be a set of distinct integer points in d-dimensional space, not all on the same hyperplane. Consider subsets K_i consisting of $d+1$ elements of W, not all on the same hyperplane. Let T_i be the convex hull of the points of K_i, a d-simplex. Let K_j be the subset for which the simplex T_j has smallest volume. Then T_j contains no other point of W besides the points in K_j.*

Proof. Suppose that K_i is the set $\{P_1, \ldots, P_{d+1}\}$, and the convex hull T_i contains another integer point Q. The point Q cannot lie on all the $d+1$ hyperplane faces of the simplex T_i. After renumbering, we can suppose that Q does not lie on the hyperplane face $P_1, P_2, \ldots P_d$. Since Q is not the vertex

P_{d+1}, the point Q is closer to this hyperplane than P_{d+1}, so the simplex $P_1P_2 \ldots P_dQ$ has integer point vertices and strictly smaller volume.

Hence the minimal set K_j is such that no other integer point lies on the convex hull T_j. □

LEMMA 3.4.5. *Let S be a set of K distinct integer points in d-dimensional space that do not all lie on a hyperplane. Then there is a simplicial complex of at least $K-d$ non-overlapping d-simplices whose vertices are the K points of S. By "non-overlapping" we mean that no two d-simplices in the complex share a portion of d-dimensional space.*

Proof.

Step 1. If $K \leq d$ then the Lemma holds. If $K \geq d+1$, then by Lemma 3.4.4, we choose the $d+1$ integer points that form the vertices of the simplex T_1 that has least possible hypervolume and so (by the same lemma) the remaining integer points all lie outside of the convex hull of T_1.

Step 2. Consider points Q which are not vertices of the minimal simplex, and the simplices T which are formed by joining Q to a face of T_1. As in Lemma 3.4.4, if T contains another point R of the set S, then there is a simplex T' of smaller volume formed by joining R to the same face of T_1. Let T_2 be a simplex of minimal volume. Then the simplicial complex $T_1 \cup T_2$ contains no $(d+3)$-rd point of S and (again by Lemma 3.4.4) the point Q cannot lie on the faces of T_1.

Step 3 (and subsequent steps). Consider points R which are not vertices of the simplicial complex J already constructed, and the simplices T formed by joining R to a face of J. Choose T_3 of minimal volume. As in Step 2, the simplicial complex $J' = T_1 \cup T_2 \cup T_3$ contains no $(d+4)$-th point of S.

This process continues until all K points of S have been used, forming a complex of $K-d$ non-overlapping simplices. □

LEMMA 3.4.6. *Let $\mathcal{P}$ be a convex polytope contained in a hypersphere radius R, whose vertices are integer points. Then the number of $(d-1)$-hyperplane faces of $\mathcal{P}$ whose standard normal vector has length greater than N is*

$$\leq \frac{\alpha_d R^{d-1} d!}{N}. \tag{3.20}$$

Proof. Consider d integer points $\mathbf{x_1}, \mathbf{x_2}, \mathbf{x_3}, \ldots, \mathbf{x_d}$ lying on a hyperplane face with primitive normal vector $(A_1, A_2, A_3, \ldots, A_d)$, where the d-integer points

form a simplex with $(d-1)$-dimensional volume $V^{(d-1)}$, and $\mathbf{x_{d+1}}$, an integer point lying off the hyperplane face. From (3.19) of Lemma 3.4.3, the perpendicular distance D from $\mathbf{x_{d+1}}$ to the hyperplane face is given by

$$D = \frac{k}{\sqrt{(A_1^2 + A_2^2 + A_3^2 + \ldots + A_d^2)}},$$

for some positive integer k. We chose $\mathbf{x}_{d+1}$ so that the distance is minimal and so $k = 1$. Theses $d+1$ points form a d-dimensional simplex whose volume, $V^{(d)}$, is calculated by multiplying the $(d-1)$-volume of the base, $V^{(d-1)}$, by the height D and then dividing by d.

Since the volume of a d-simplex whose vertices are integer points is at least $1/d!$, we have

$$\frac{1}{d!} \leq V^{(d)}(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \ldots, \mathbf{x}_{d+1}) = \frac{1}{d} D V^{(d-1)}(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \ldots, \mathbf{x}_d),$$

and so

$$V^{(d-1)}(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \ldots, \mathbf{x}_d) \geq \frac{d}{d!} \cdot \frac{1}{D} = \frac{1}{(d-1)!} \sqrt{(A_1^2 + A_2^2 + A_3^2 + \ldots + A_d^2)}$$
$$\geq \frac{N}{(d-1)!}, \tag{3.21}$$

by the conditions of the Lemma.

The $(d-1)$-dimensional hypervolume of the hyperplane faces of the convex polytope must be less than or equal to the $(d-1)$-hypervolume of the surface of the d-dimensional hypersphere enclosing it. Let A_i be the hypervolume of each hyperplane face of the polytope then by equation (3.11) we have

$$\sum A_i \leq S_d = d\alpha_d R^{d-1} = d\alpha_d R^{d-1}. \tag{3.22}$$

We obtain an upper bound for the number of large hyperplane faces of the convex polytope by dividing the lower bound (3.21) into the upper bound (3.22) to obtain

$$\leq \frac{d\alpha_d R^{d-1}(d-1)!}{N}. \tag{3.23}$$

□

THEOREM 3.4.7. *Let $\mathcal{P}$ be a convex polytope contained in a d-hypersphere radius R, whose vertices are integer points. Then the number of $(d-1)$-dimensional hyperplane faces of $\mathcal{P}$ is*

$$\leq 2\,(3\alpha_d d!)^{\frac{d}{d+1}}\, R^{\frac{d(d-1)}{d+1}}. \tag{3.24}$$

Proof. We take

$$N = \left(\frac{\alpha_d d!}{3^d}\right)^{\frac{1}{d+1}} R^{\frac{d-1}{d+1}}.$$

in (3.14) of Lemma 3.4.1 and (3.20) of Lemma 3.4.6. The total number of hyperplane faces is the sum of bounds for those with long normal vectors in (3.14) and those with short normal vectors in (3.20)

$$\leq \frac{\alpha_d (c_1 M)^{d-1} d!}{N} + (3N)^d = 2\,(3\alpha_d d!)^{\frac{d}{d+1}}\, R^{\frac{d(d-1)}{d+1}}.$$

□

LEMMA 3.4.8. *Let $\mathcal{P}$ be a convex d-polytope with vertices at integer points. From each j-face F_i of $\mathcal{P}$, we pick out $(j+1)$ vertices $\mathbf{v}_{i,1}, \mathbf{v}_{i,2}, \ldots, \mathbf{v}_{i,j+1}$ that do not all lie on a $(j-1)$-dimensional plane. Let $\mathbf{w}_i$ be the centroid of these vertices*

$$\mathbf{w}_i = \frac{1}{j+1}\left(\mathbf{v}_{i,1} + \mathbf{v}_{i,2} + \ldots + \mathbf{v}_{i,(j+1)}\right). \tag{3.25}$$

Let $T = \{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_h\}$ be the set of centroids associated with all the j-faces of $\mathcal{P}$. For a set U, let conv$\{U\}$ *denote the smallest convex set containing all the elements of U. Then the centroids $\mathbf{w}_i$ are true vertices of* conv$\{T\}$, *in the sense that for any $t = 1.\ldots, h$*

$$\text{conv}\{T \backslash \{\mathbf{w}_h\}\} \neq \text{conv}\{T\}.$$

Proof. We must rule out the possibility that

$$\mathbf{w}_i = \sum_{g=1}^{h} \lambda_g \mathbf{w}_g, \tag{3.26}$$

with

$$0 \leq \lambda_g \leq 1, \quad \sum_{g=1}^{h} \lambda_g = 1. \tag{3.27}$$

Substituting for $\mathbf{w}_g$ using (3.25) and multiplying by $(j+1)$ to clear fractions yields

$$\mathbf{v}_{i,1} + \mathbf{v}_{i,2} + \ldots + \mathbf{v}_{i,(j+1)} = \sum_{g=1}^{h} \sum_{f=1}^{j+1} \lambda_g \mathbf{v}_{g,f}. \tag{3.28}$$

Each j-face F_i is the intersection of at least $(d-j)$ hyperplane faces of $\mathcal{P}$ and our $(j+1)$ vertices of F_i are also vertices of each of these hyperplanes. We label these hyperplanes $\Pi_1, \Pi_2, \ldots, \Pi_k, \ldots \Pi_t$ with primitive integer normal vectors $\mathbf{n_k}$, so that any point $\mathbf{r}$ lying on Π_k satisfies the equation

$$\mathbf{r}.\mathbf{n}_k = D_k.$$

As $\mathcal{P}$ is convex, all the Π_k are supporting hyperplanes of $\mathcal{P}$. Hence, for any point $\mathbf{x}$ in H we have

$$\mathbf{x}.\mathbf{n}_k \leq D_k, \tag{3.29}$$

where we have assumed (using a suitable integer vector translation) that $\mathcal{P}$ contains the origin. Applying (3.29) to (3.28) yields

$$(\mathbf{v}_{i,1} + \mathbf{v}_{i,2} + \ldots + \mathbf{v}_{i,(j+1)}).\mathbf{n}_k = D_k(j+1) = \sum_{g=1}^{h}\sum_{f=1}^{j+1} \lambda_g \mathbf{v}_{g,f}.\mathbf{n}_k$$

$$\leq (j+1)\sum_{g=1}^{h} \lambda_g D_k = D_k(j+1),$$

implying that

$$D_k(j+1) = \sum_{g=1}^{h} \lambda_g \sum_{f=1}^{j+1} \mathbf{v}_{g,f}.\mathbf{n}_k = D_k(j+1). \tag{3.30}$$

This equality is only satisfied if all of the vertices $\mathbf{v}_{g,f}$ for which $\lambda_g \neq 0$ are on the hyperplanes $\Pi_k, 1 \leq k \leq t$.

Now any j-face F_i of a convex d-polytope $\mathcal{P}$ can be defined as the intersection of the q-faces that contain $F_i, j \leq q \leq (d-1)$. Therefore, as the vertices $\mathbf{v}_{g,f}$ lie on such an intersection with $q = (d-1)$, we deduce that the vertices $\mathbf{v}_{g,f}$ for which $\lambda_g \neq 0$ are all vertices of our j-face F_i. That is, $\mathbf{v}_{g,1}, \mathbf{v}_{g,2}, \ldots, \mathbf{v}_{g,j+1}$ are vertices of F_i.

This implies that for $g \neq i$ in equation (3.28) we must have $\lambda_g = 0$, as two distinct j-faces of $\mathcal{P}$ cannot share $(j+1)$ vertices. Hence there is only one term, λ_g, with $g = i$ and $\lambda_i = 1$ yielding the trivial expression, right hand side is identical to left hand side in equation (3.28).

Therefore, $\mathbf{w}_i$ has only one expression as a convex sum of

$$T = \{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_h\},$$

and thus $\mathbf{w}_i$ is not in the convex hull of $T - \mathbf{w}_i$. □

Remark. Theorem 3.4.9 is a version of Andrew's Theorem [1] (stated at the beginning of Chapter 6) with explicit constants. The second statement regarding the number of faces was not stated in [1]. McMullen [31] has upper bounds for the number of faces in terms of the vertices. These bounds can be attained by polytopes with integer vertices lying on a twisted quantic (or moment) curve, $f(t)$, defined by

$$f(t) = (t, t^2, t^3, \ldots, t^d),$$

but the parameter M is very large. The Upper-bound Theorem states:

Let $f_j(v, d)$ be the number of j-dimensional faces of a convex d-polytope $\mathcal{P}$ with v vertices, where $0 \leq j \leq d-1$. Then the following holds:

(1) If $d = 2n$, then

$$f_j(v, d) \leq \sum_{k=1}^{n} \frac{v}{v-k} \binom{v-k}{k} \binom{k}{j+1-k}.$$

(2) If $d = 2n+1$, then

$$f_j(v, d) \leq \sum_{k=0}^{n} \frac{j+2}{v-k} \binom{v-k}{k+1} \binom{k+1}{j+1-k}.$$

For $j = 0$, the above upper-bounds are exact, with $f_0(v, d) = v$, whereas, for $1 \leq j \leq d-2$, the upper bounds are $\geq O(v^2)$.

Theorem 3.4.9 (below) gives an upper-bound for the number of j-faces of a lattice d-polytope $\mathcal{P}$, lying in a hypersphere of radius R, in terms of the parameter R. Hence for a spherically contained d-polytope, there exist triples (d, f_0, j), for which the second statement of Theorem 3.4.9 is an improvement on the general Upper-bound Theorem for convex d-polytopes, proved by McMullen [30] in 1970.

THEOREM 3.4.9. *In d-dimensional space, a convex polytope $\mathcal{P}$ with f_0 vertices, all at integer points, contained in a hypersphere of radius R satisfies*

$$f_0 \leq 2\,(3\alpha_d d!)^{\frac{d}{d+1}}\,(2R)^{\frac{d(d-1)}{d+1}} \leq 36 d!(2R)^{\frac{d(d-1)}{d+1}}. \tag{3.31}$$

Let $1 \leq j \leq d-2$. Under the conditions of the theorem, the number f_j of j-faces of $\mathcal{P}$ satisfies

$$f_j \leq 2\,(3\alpha_d d!)^{\frac{d}{d+1}}\,(2(j+1)R)^{\frac{d(d-1)}{d+1}}\,. \tag{3.32}$$

Proof. Let T be the set of midpoints of edges of $\mathcal{P}$, and let $\mathcal{P}'$ be the convex hull of T. By Lemma 3.5 each point of T is a vertex of $\mathcal{P}'$. Let V be the vertex of $\mathcal{P}$ where edges $e_1, e_2, \ldots, e_r$ meet and let $W_1, W_2, \ldots, W_r$ be the respective midpoints of these edges. The $W_1, W_2, \ldots, W_r$ are all vertices of $\mathcal{P}'$ but not necessarily of the same facet.

By construction, each vertex V of $\mathcal{P}$ is truncated by a facet F of $\mathcal{P}'$ and we say that V belongs to the facet F. Geometrically we can think of V as lying above the facet F. The supporting hyperplane Π of $\mathcal{P}'$ containing F cuts $\mathcal{P}$ in a $(d-1)$-dimensional convex polytope Q. The join of V to any other vertex V' of $\mathcal{P}$ cuts Π within this convex polytope. We now show that V' cannot lie above the facet F. The vertices of Q are points $X_1, X_2, \ldots, X_r$ on $e_1, e_2, \ldots, e_r$ and X_i is either W_i, the midpoint of e_i, or between V and W_i. Therefore, if V' lies above F, then V' lies in $\mathrm{conv}(Q, V)$ and so V' lies in $\mathrm{conv}(V, X_1, X_2, \ldots, X_r)$. The only vertex of $\mathcal{P}$ in this list is V, so $V' = V$.

This implies that the number of facets of $\mathcal{P}'$ is greater than or equal to the number of vertices of $\mathcal{P}$.

Now $2\mathcal{P}'$ is a polytope with integer vertices lying in a d-sphere radius $2c_1M$, so the number of faces of $\mathcal{P}'$ is given by (3.24) of Theorem 3.4.7, but with a larger implied constant. We deduce the result (3.31).

For each j-face G of $\mathcal{P}$ we choose $j+1$ vertices that do not all lie on the same $(j-1)$-plane and construct $C(G)$, the centroid of the $j+1$ vertices. Since $C(G)$ does not lie on the $(j-1)$-dimensional boundary of G, $C(G)$ cannot lie on any other j-face. Let U be the set of centroids $C(G)$ constructed from the j-faces of $\mathcal{P}$.

By Lemma 3.4.8, U is a strictly convex set and we define $\mathcal{P}''$ to be the convex hull of the points $C(G)$ in U. Then $(j+1)\mathcal{P}''$ is a polytope with integer point vertices lying in a d-sphere radius $(j+1)R$, so that the number of vertices of $\mathcal{P}''$ is given by equation (3.31), but with a larger implied constant. Each j-face G gives a distinct point $C(G)$ in U which is a vertex of the convex polytope $\mathcal{P}''$. We deduce the result (3.32). □

3.5 Major Arcs and Lattices

Definition (major and minor arcs). It is helpful in many problems to separate "major arcs", regions where there is good Diophantine approximation, from "minor arcs", regions where there is not. In this paper a major arc can be described informally as a region U of the shell E such that the convex hull of all the integer points in U is contained in the intersection of E with some hyperplane. Hence U can be of dimension j, with $j = 1, 2, \ldots, d-1$.

For each major arc we are interested in the integer points which lie within a distance δ from the hypersurface C. In the following chapter we will show that the integer points lie in clusters around the vertices of the convex hull H, which we call components of a major arc. We saw in Lemma 2.2.1 that at most two one-dimensional components can lie on the same straight line. Higher dimensional components, are however, not as simple and for the dimensions $(d-1) \geq j \geq 2$, there can exist many j-dimensional components on the same j-dimensional plane.

By considering two-dimensional cross-sections of the shell E, we can see that each j-dimensional component of a major arc has maximum diameter equal to the maximum length of a component of a one-dimensional major arc. By Lemma 2.2.2 this is

$$\leq 4\sqrt{\delta c_1 M}. \tag{3.33}$$

Hence a j-dimensional component is contained within a j-dimensional hypercube of volume

$$\leq \left(4\sqrt{\delta c_1 M}\right)^j. \tag{3.34}$$

By the same Lemma, any major arc that is tangential to C_0, contained wholly within the shell E, and has a 2-dimensional cross-section that is chordal to C_1, must have diameter D in the range

$$4\sqrt{\delta c_0 M} \leq D \leq 4\sqrt{\delta c_1 M}. \tag{3.35}$$

LEMMA 3.5.1. *Let $R = c_1 M$ and let F be a facet or hyperplane face of H that lies in a hyperplane Ψ with outward normal* $\mathbf{n}$. *Let X be the point of C_1 at which* $\mathbf{n}$ *is the outward normal. Let h be the distance from X along the inward normal to the nearest point Y on the hyperplane Ψ. Let E' be the $(d-1)$-dimensional cross-section of E contained in Ψ, so that E' contains*

all parts of the face F that lie in the shell E. Then the $(d-1)$-dimensional volume V of E' is bounded above by

$$V \leq 2^{\frac{d+9}{2}} d\delta R^{\frac{d-1}{2}} h^{\frac{d-3}{2}}. \tag{3.36}$$

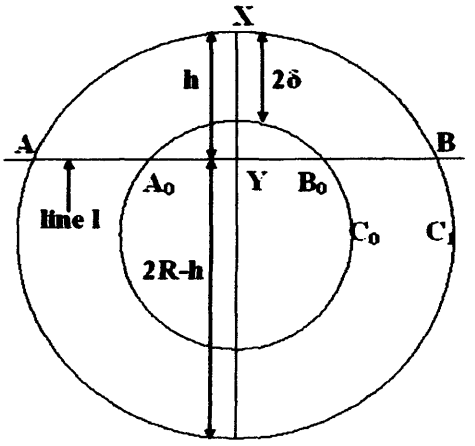

Figure 3.2: (section by 2-plane Π through l and X).

Proof. Let Π be a two-dimensional plane through XY, and let $E^\star$ be the two-dimensional cross-section of E by Π (Figure 3.2). Then Π cuts Ψ in a straight line l which meets C_1 in two distinct points A and B. The points A and B lie inside the circle radius R through X with $\mathbf{n}$ as outward normal at X. For clarity, the curves C_0 and C_1 in Figure 3.2 are drawn as circles. From (2.8) in the proof of Lemma 2.2.2 we have

$$AY \leq \sqrt{h(2R-h)} = k. \tag{3.37}$$

Hence the set $E' = E \cap \Psi$ lies within a $(d-1)$-sphere centre Y radius $\leq \sqrt{2Rh}$.

Case 1. When $h \leq 2\delta$ the plane Ψ does not cut C_0 and by (3.9), the diameter of E' satisfies (2.6). This implies that the whole of the facet F is contained within the shell E. Therefore, the $(d-1)$-dimensional volume V of E' is

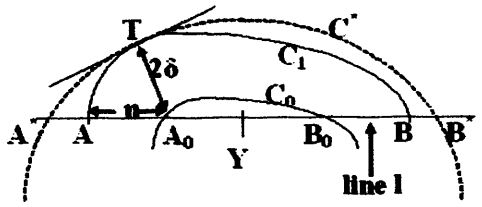

Figure 3.3: (section by 2-plane Π_1 through l and T).

less than or equal to that of a $(d-1)$-sphere radius $\sqrt{2hR}$. Applying (3.12) yields

$$V \leq \alpha_{d-1}(2hR)^{\frac{d-1}{2}} \leq 2^{\frac{d+5}{2}}(hR)^{\frac{d-1}{2}}. \tag{3.38}$$

Case 2. When $h > 2\delta$ the hyperplane Ψ meets C_0, and the line l in the two-dimensional plane Π cuts C_0 in two distinct points A_0 and B_0. Let A_0T be the normal from A_0 to C_1, so the distance A_0T is 2δ, and let C^* be the hypersphere radius R touching C_1 at T. Let Π_1 be the two-dimensional plane through the line l and the point T (Figure 3.3). Then C_1 and the shell E are contained within C^*. The line l cuts C^* at A^* and B^*, so that by the geometry of circles

$$AA_0.A_0B \leq A^*A_0.A_0B^* = 2\delta(2R-2\delta) \leq 4\delta R. \tag{3.39}$$

On the line l, the point A lies between A^* and A_0, with $AA_0 = \eta$ (say) and $\eta > 0$. Hence

$$\eta \leq A^*A_0. \tag{3.40}$$

We also have

$$A_0B^* \geq YB^* = k = \sqrt{h(2R-h)}. \tag{3.41}$$

Each point of E' lies within a distance η of the $(d-2)$-dimensional surface of $C_1 \cap \Psi$. The $(d-2)$-dimensional volume of $C_1 \cap \Psi$ is at most the surface content of a $(d-1)$-dimensional sphere radius k, which by (3.11) is equal to

$$(d-1)\alpha_{d-1}k^{d-2}.$$

Therefore, the $(d-1)$-dimensional volume V of E' satisfies

$$V \leq (d-1)\alpha_{d-1}\eta k^{d-2} \tag{3.42}$$

From (3.39), (3.40) and (3.41) we have

$$\eta k \leq A^* A_0 . A_0 B^* \leq 4\delta R. \tag{3.43}$$

Hence we can write

$$V \leq (d-1)\alpha_{d-1}(4\delta R)k^{d-3}$$

which simplifies to

$$V \leq 2^{\frac{d+7}{2}}(d-1)\delta R^{\frac{d-1}{2}} h^{\frac{d-3}{2}}. \tag{3.44}$$

Combining (3.38) and (3.44) yields

$$V \leq 2^{\frac{d+9}{2}} d\delta R^{\frac{d-1}{2}} h^{\frac{d-3}{2}},$$

and hence the result. □

LEMMA 3.5.2. *In d-dimensional space, the number of integer points of S in E that lie strictly inside the convex hull H of S is*

$$\leq 2\delta d! \alpha_d d(c_1 M)^{d-1}. \tag{3.45}$$

In particular, if $d = 3$, then the number of integer points lying within a short distance δ of the convex hull H is

$$\leq 48\pi\delta(c_1 M)^2. \tag{3.46}$$

Proof. Given that the integer point vertices of our convex hull H and any integer points contained within it lie within a distance δ from the closed convex hypersurface C, we can associate a hyperslab of width 2δ with each facet of the polytopal convex hull where the hyperslabs will overlap.

Any integer points in $H \cap E$ must lie within a distance 2δ of the nearest polytope facet F_i with hypersurface area A_i. The internal or "dihedral" angles between facets are $\leq 180°$ due to convexity. Let P be such a point with nearest hyperface F_i, so that the perpendicular from P to the hyperplane F_i actually hits F_i. If not, then some other hyperplane is nearer (F_j say depicted in Figure 3.4) under the distance equation (3.19) defined in Lemma 3.4.3.

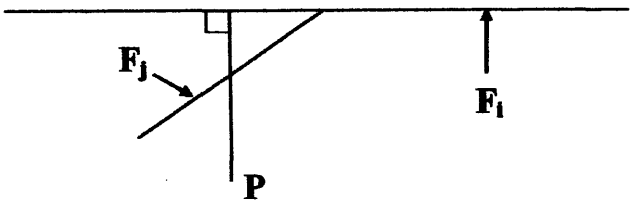

Figure 3.4:

Therefore each integer point P lying inside the convex hull can be associated uniquely with a nearest hyperface F_i.

Corresponding to each hyperface F_i we have a hyperslab S_i consisting of two completely parallel hyperfaces F_i and F_i shifted by 2δ in the normal direction to the hyperplane. The hypervolume of $S_i = 2\delta A_i$ where A_i is the hypersurface area of F_i.

We know from Lemma 3.4.5 that in d-dimensions, K points that do not all lie on the same hyperplane form a simplicial complex of $(K - d)$ non-overlapping simplices. Each simplex has hypervolume $1/d!$ multiplied by an integer so that each of these simplices has hypervolume $\geq 1/d!$.

Therefore, if K_i is the number of internal integer points associated uniquely with the hyperface F_i, which itself has at least d integer point vertices, then the total number of internal and boundary integer points of the hyperface is

$$\geq d + K_i,$$

so that we have K_i non-overlapping simplices, yielding

$$\frac{K_i}{d!} \leq 2\delta A_i,$$

so that

$$K_i \leq 2d!\delta A_i.$$

Hence the total number of integer points lying within a short distance δ of the convex hull H is

$$\leq \sum_i K_i \leq \sum_i 2d!\delta A_i.$$

The boundary content of our convex d-polytope H is less than or equal to that of the hypersphere with radius of curvature $c_1 M$ enclosing it. Therefore, using (3.11), we have

$$\sum_i K_i \leq 2d!\delta\alpha_d d(c_1 M)^{d-1}. \qquad \square$$

LEMMA 3.5.3. *Let* Π *be a hyperplane with equation*

$$\mathbf{n}.\mathbf{x} = D,$$

where $\mathbf{n}$ *is a primitive integer vector, and* D *is an integer. Then the integer points of* Π *form a lattice with determinant* $|\mathbf{n}|$.

Proof. The integer points in d dimensions with

$$\mathbf{n}.\mathbf{x} \equiv 0 \bmod |\mathbf{n}|^2$$

form a d-dimensional lattice N whose determinant is $|\mathbf{n}|^2$. Let Ψ be the hyperplane through the origin parallel to Π. The integer points on Ψ form a lattice M, a sub-lattice of N. If $\mathbf{x} \in N$, then

$$\mathbf{n}.\mathbf{x} = c|\mathbf{n}|^2,$$

for some constant c, so $\mathbf{x} - c\mathbf{n}$ is on Ψ and so in M. Hence

$$N = \text{ span} < M, \mathbf{n} > .$$

Let V be the $(d-1)$-dimensional volume of the fundamental lattice of M. Since $\mathbf{n}$ is orthogonal to the hyperplane Π, the determinant of the lattice N is $V|\mathbf{n}|$,

$$V = |\mathbf{n}|.$$

If Λ is a lattice in the hyperplane Π, then we can obtain Λ by shifting M in hyperplane Ψ by some vector $\mathbf{e}$, where $\mathbf{e}$ is a coset representative for N on the big lattice $\mathbf{Z}^d$. Thus the integer points on Π form a lattice with determinant $|\mathbf{n}|$. $\square$

LEMMA 3.5.4. *Let* Λ *be a* j*-dimensional lattice,* $1 \leq j \leq d$*, whose determinant is* n*. Let* U *be a convex set in the* j*-plane of* Λ*, with* j*-dimensional volume* V*, containing* K *points of the lattice* Λ*. Then one of the following two cases holds:*

(1) Major case. All the points of Λ *in the set* U *lie on a* $(j-1)$*-dimensional plane, or*

(2) Minor case,

$$K \leq j!\frac{V}{n} + j \leq (j+1)!\frac{V}{n}.$$

Proof. In the minor case, by Lemma 3.4.5, the convex hull H of the set U contains $K - j$ disjoint simplices with vertices at lattice points, each of volume at least $n/j!$. The union of these simplices lies inside U, so we have

$$(K-j)\frac{n}{j!} \leq V, \qquad K \leq j!\frac{V}{n} + j. \qquad \square$$

This gives the first inequality. There is at least one such simplex, so

$$V \geq \frac{n}{j!},$$

and we deduce the second inequality.

Chapter 4

Components of H

This chapter derives a method that enables the classification and enumeration of the j-dimensional major arcs of the convex hull H.

4.1 Vertex Components

For each point P in our shell E, there is a normal to the boundary C, meeting the outer boundary C_1 normally at a point R_1 and the inner boundary surface C_0 normally at a point R_0. We call R_0 and R_1 the normal projections of P onto C_0 and C_1. The vertices of our convex polytope H, must, by definition lie in E and for every other non-vertex integer point in E there must exist at least one nearest vertex. We now formalise this concept with the following definition.

Definition (vertex components). Let P be a point of S in the shell E and R_1 the normal projection of P onto C_1. Let V be a vertex of the convex hull H and E' the plane cross-sectional strip of E containing V, P and R_1. If the line segment R_1V does not cut the inner boundary surface C_0, and so lies entirely within the closed strip E', then we say that P lies in the component $S(V)$ of S.

LEMMA 4.1.1. *Every point P of S belongs to some vertex component $S(V)$.*

Proof. The line segment PR_1 cuts the boundary of the convex hull H at some point Q between P and R_1 inside E, so that Q lies in some hyperplane

face F of H. If Q is a vertex of H then P belongs to $S(Q)$ as QR_1 will lie on the line segment R_0R_1 inside E.

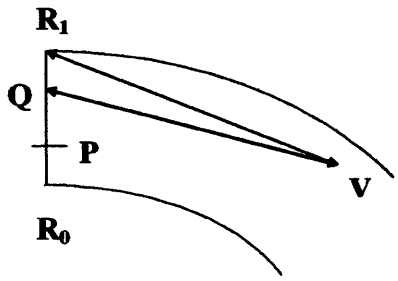

Figure 4.1:

We now assume that the point Q is not a vertex of H and triangulate the facet F of H containing Q so that Q lies in some simplex $W = V_1V_2V_3 \ldots V_d$. If the line segment QV_i does not enter the interior of the convex set bounded by C_0 then neither does R_1V_i, implying that P lies in $S(V_i)$.

If P lies in no $S(V_i)$ then each line segment QV_i on F cuts the interior of C_0 in some point Q_i also on F but not in E. The whole convex simplex $Q_1Q_2 \ldots Q_d$ therefore lies strictly inside C_0 and contains Q. Hence, Q is not in E which is impossible, since Q lies on the line segment R_0R_1, which is strictly inside E. This contradiction shows that for some i, the line segment V_iQ lies in E and so V_iR_1 lies in E and P is in the component corresponding to V_i. □

LEMMA 4.1.2 (spacing lemma). *Let V be a vertex of the convex hull H. Let P be a point of S not in the component $S(V)$ of V. Let R_1 and R_2 be the respective normal projections of P and V onto C_1. Then*

$$R_1R_2 > \sqrt{c_0\delta M}, \tag{4.1}$$

and the angle between the normals to C_1 at R_1 and R_2 is

$$> \frac{1}{c_1}\sqrt{\frac{c_0\delta}{M}}. \tag{4.2}$$

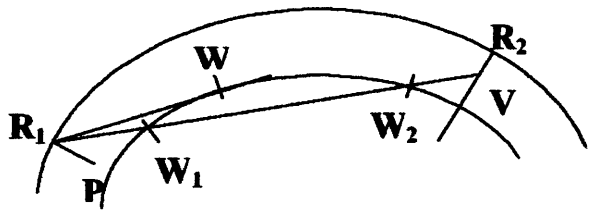

Figure 4.2:

Proof. Since P is not in the component of V, the line R_1V cuts C_0 in two points W_1 and W_2. Let E' be the plane sectional closed strip of E defined by the line R_1V and the point R_2, so that E' also contains the points W_1 and W_2. Between W_1 and W_2 on C_0 is a point W where the tanget to C_0 in E' passes through R_1. Then

$$R_1V > R_1W_2 > R_1W \geq 2\sqrt{\delta c_0 M},$$

by (3.35). Hence

$$R_1R_2 \geq R_1V - 2\delta > 2\sqrt{\delta c_0 M} - 2\delta$$
$$\geq 2\sqrt{\delta c_0 M} - \sqrt{\delta c_0 M} = \sqrt{\delta c_0 M},$$

by (3.5) and (3.6), which is (4.1).

To obtain (4.2) we consider the d-sphere B with centre on R_2V produced, radius c_1M, touching C_1 at R_2. There is a point R_1' on B where the outward normal is parallel to the outward normal to C_1 at R_1, making some angle θ with the outward normal at R_2. Since C_1 has sectional radius of curvature less than or equal to c_1M, the radius of B, we have

$$R_1R_2 \leq R_1'R_2.$$

The shortest distance from R_1' to R_2 along the surface of B is $\theta c_1 M$, so

$$\theta c_1 M \geq R_1'R_2 \geq R_1R_2 > \sqrt{c_0\delta M},$$

$$\theta > \frac{1}{c_1}\sqrt{\frac{c_0\delta}{M}},$$

as required. □

4.2 Enlarged Vertex Components

We choose a well-spaced subset of the vertices of H. As each integer point P in S belongs to at least one component $S(V)$ labelled by some vertex V of the convex hull H, components labelled by different vertices may well overlap and different vertices of the convex hull may be close together. We pick a well-spaced set of vertices of H as follows. Pick a vertex V_1, and let the enlarged component $S'(V_1)$ be the union of all components $S(V)$ with V in $S(V_1)$.

Now pick a vertex V_2 not in $S'(V_1)$, and form the enlarged component $S'(V_2)$. We pick V_{i+1} not in $S'(V_1), S'(V_2), \ldots, S'(V_i)$, and so on until all of the vertices V of the convex hull H lie in some enlarged component.

We want to discuss the spacing of the vertices V_i that label the enlarged components $S'(V_i)$. Each V_i has a normal projection R_i on C_1. Consider a d-sphere B of radius $c_1 M$. We associate R_i on C_1 with the point W_i on B where the outward normal $\mathbf{n}$ to B is parallel to the outward normal to C_1 at R_i.

Let V_i and V_j be distinct vertices labelling enlarged vertex components. Since $V_j \notin S(V_i)$, by (4.1) of Lemma 4.1.2 we have

$$R_i R_j > \sqrt{c_0 \delta M}.$$

Since C_1 has sectional radii of curvature at most $c_1 M$,

$$W_i W_j \geq R_i R_j > \sqrt{c_0 \delta M}.$$

Hence d-balls radius $\frac{1}{2}\sqrt{c_0 \delta M}$, centred on the points W_i on the surface of the d-sphere B, are disjoint.

The d-ball B_i meets the surface of the d-sphere B in a set A_i which contains the centre W_i of B_i and is a $(d-1)$-ball in spherical geometry. As the B_i are disjoint, the $(d-1)$-volumes A_i, on the surface of the d-sphere B, are also disjoint and do not overlap. Hence different sets $S'(V_i)$ correspond to disjoint sets A_i, centre W_i, on the surface of the d-sphere B. The $(d-1)$-volume of A_i is greater than the $(d-1)$-volume of the intersection of a hyperplane through W_i with B_i, which is

$$\alpha_{d-1} \left(\sqrt{\frac{c_0 \delta M}{4}} \right)^{d-1}. \tag{4.3}$$

Therefore each enlarged vertex component $S'(V_i)$ corresponds to a disjoint set A_i, centre W_i, on the surface of the d-sphere B, and the number of such sets (and so enlarged vertex components) is

$$\leq \frac{d\alpha_d (c_1 M)^{d-1}}{\alpha_{d-1} (c_0 \delta M/4)^{(d-1)/2}}. \tag{4.4}$$

LEMMA 4.2.1 (thickness lemma). *Let $S'(V)$ be an enlarged component and let R_2 be the normal projection of V onto C_1. Let P be a point in $S'(V)$. Then the distance h of P from the tangent hyperplane at R_2 satisfies*

$$h \leq \frac{52\delta c_1}{c_0}. \tag{4.5}$$

Proof. The integer point P lies in some component $S(V')$ with V' in $S'(V)$. Let R_1 and R_2' be the respective normal projections of P and V' onto C_1. The line segments R_1V' and $R_2'V$ lie inside the shell E, so by (3.33)

$$R_1V' \leq 4\sqrt{\delta c_1 M}, \quad R_2'V \leq 4\sqrt{\delta c_1 M}.$$

The distances $V'R_2'$ and VR_2 are at most 2δ, so

$$R_1R_2 \leq R_1V' + V'R_2' + R_2'V + VR_2 \leq 8\sqrt{\delta c_1 M} + 4\delta \leq 10\sqrt{\delta c_1 M}, \tag{4.6}$$

where we have used (3.5) and (3.6). Let E' be the plane cross-sectional strip

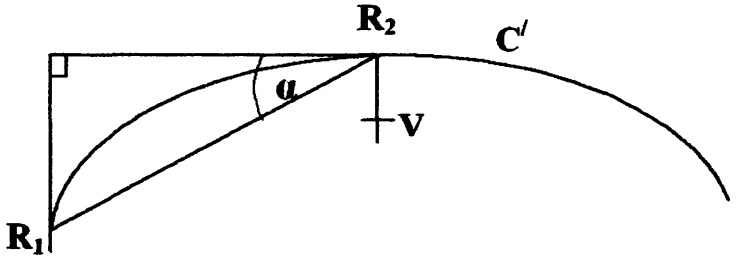

Figure 4.3:

of E defined by R_1, V and the normal projection R_2 of V onto C_1. Let C' be the convex curve defined by the intersection of C_1 and E' (Figure 4.3).

For fixed distance $R_1R_2 = D$, the distance of R_1 from the tangent line to C' at R_2 in E' is greatest when the radius of curvature is least, which is when C' is an arc of a circle radius c_0M. Let α be the angle between R_1R_2 and the tangent at R_2. In the extreme case when C' is a circle radius c_0M, the chord R_1R_2 subtends an angle 2α at the centre of the circle, so

$$D = 2c_0M \sin\alpha,$$

and by (4.6), the distance of R_1 from the tangent at R_2 is

$$D\sin\alpha = \frac{D^2}{2c_0M} \leq \frac{100\delta c_1 M}{2c_0M} = \frac{50\delta c_1}{c_0}.$$

The distance of P from the tangent hyperplane to C_1 at R_2 is therefore

$$\leq \frac{50\delta c_1}{c_0} + 2\delta \leq \frac{52\delta c_1}{c_0}. \qquad \square$$

Remark. We are ultimately working towards a shelling argument. This uses the property that if we can obtain a bound valid for δ sufficiently small, then we can deduce a possibly weaker bound for large δ by dividing the shell E into concentric shells E_r, $1 \leq r \leq R$ of thickness δ_0, bounded by shrunken copies of the exterior hypersurface C_1 of E. By inequality (3.9), we have a uniform upper bound of c_1M for the cross-sectional radius of curvature at any point on each shell E_r. Hence, when regarding maximum cross-sectional radius of curvatures, we can work within the general shell boundary C_1, whose sectional radius of curvature is also $\leq c_1M$.

LEMMA 4.2.2 (flatness lemma). *Let $S'(V)$ be an enlarged vertex component of our convex hull H. If*

$$\delta < \delta_0 = \left(\frac{c_0}{2^{2d}5^{d-1}13d!c_1}\right)^{\frac{2}{d+1}} (c_1M)^{\frac{-(d-1)}{d+1}}, \tag{4.7}$$

then all the points of $S'(V)$ lie on a hyperplane through the vertex V.

Proof. Let P be a point of $S'(V)$ and let R_1 and R_2 be the the normal projections of P and V onto C_1. All points P of $S'(V)$ lie within a distance $52\delta c_1/c_0$ from the tangent hyperplane at R_2 and by (4.6)

$$PV \leq R_1R_2 \leq 10\sqrt{\delta c_1 M}. \tag{4.8}$$

Hence, the set of integer points $S'(V)$ all lie within a rectangular box L, of d-dimensional volume

$$\text{Vol}(L) \leq \frac{52\delta c_1}{c_0}\left(20\sqrt{\delta c_1 M}\right)^{d-1} < \frac{1}{d!}, \tag{4.9}$$

where we have used the assumption (4.7). Therefore, for $\delta < \delta_0$, the enlarged vertex component cannot be full d-dimensional. Hence the major arc case holds, and all points of the enlarged vertex component $S'(V)$, including V itself, lie on a hyperplane. □

LEMMA 4.2.3 (approximate tangency). *Let $S'(V)$ be an enlarged component. Let T be the point of C_1 closest to V. Let P be another point of $S'(V)$, and let $\mathbf{g}$ be the integer vector VP. Then the angle α between VP and the normal to C_1 at T satisfies*

$$|\cos\alpha| \leq \frac{52\delta c_1}{c_0|\mathbf{g}|}. \tag{4.10}$$

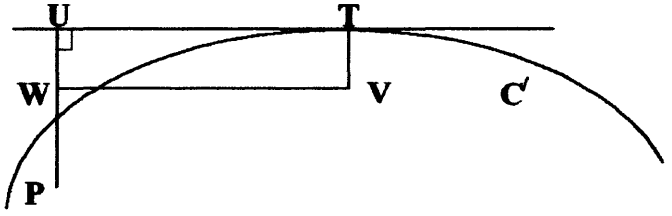

Figure 4.4:

Proof. Let Π be the 2-plane through P and the normal to C_1 at T through V. Then C_1 will appear in Π as a convex curve C'. Let l be the tanget to C' at T, and let U be the foot of the perpendicular from P to l in Π. If W is the foot of the perpendicular from V to PU then $VTUW$ is a rectangle in Π (Figure 4.4).

By Lemma 4.2.1 we have

$$PU \leq \frac{52\delta c_1}{c_0}.$$

Now if P is between W and U, then

$$VP|\cos\alpha| = PW \leq WU = VT \leq 2\delta,$$

and if W is between P and U then

$$VP|\cos\alpha| = PW \leq PU \leq \frac{52\delta c_1}{c_0}.$$

The inequality (4.10) holds in both cases. □

LEMMA 4.2.4 (sums of reciprocal vector lengths). *For $j = 1, \cdots, d-1$ we have*

$$\sum_{1\leq|\mathbf{e}|\leq E} \frac{1}{|\mathbf{e}|^j} \leq 2^{2d+j} E^{d-j}, \tag{4.11}$$

and when $d = 3$ and $j = 1$, this can be refined to

$$\sum_{1\leq|\mathbf{e}|\leq E} \frac{1}{|\mathbf{e}|} \leq 2^6 E^2. \tag{4.12}$$

Proof. Applying the Cauchy condensation method, we divide the normal vectors into ranges

$$\frac{F}{2} < |\mathbf{e}| \leq F, \quad F = 1, 2, 4, \ldots, 2^K,$$

where 2^K is the largest power of 2 less than or equal to E. The number of integer vectors in this range is

$$\leq (2F+1)^d - (F+1)^d \leq \sum_{j=0}^{d} \binom{d}{j} (2^{d-j} - 1) F^{d-j},$$

$$\leq F^3(27-8) = 19F^3,$$

when $d = 3$, and

$$\leq F^d(3^d - 2^d) \leq 2^{2d-1} F^d,$$

otherwise. Hence, in the specific case we have

$$\sum_{F/2<|\mathbf{e}|\leq F} \frac{1}{|\mathbf{e}|} \leq 19F^3 . \frac{2}{F} = 38F^2,$$

and in the general case

$$\sum_{F/2<|\mathbf{e}|\leq F} \frac{1}{|\mathbf{e}|^j} \leq 2^{2d-1}F^d.\left(\frac{2}{F}\right)^j = 2^{2d+j-1}F^{d-j}.$$

Summing over the ranges for F, gives

$$\begin{aligned}\sum \frac{1}{|\mathbf{e}|} &\leq 38(1+4+16+\ldots+2^{2K}) \\ &\leq \frac{39(2^{2K+2}-1)}{4-1} \leq 13.4(2^{2K}) \\ &\leq 2^6E^2,\end{aligned}$$

in the specific case, and

$$\begin{aligned}\sum_{1\leq|\mathbf{e}|\leq F} \frac{1}{|\mathbf{e}|^j} &\leq 2^{2d+j-1}(1+(2^1)^{d-j}+(2^2)^{d-j}+\ldots+(2^K)^{d-j}), \\ &\leq 2^{2d+j-1}\frac{(2^{d-j})^{k+1}-1}{2^{d-j}-1} \leq 2^{2d+j}2^{(d-j)K}, \\ &\leq 2^{2d+j}E^{d-j},\end{aligned}$$

in the general case, as required. □

Definition (the *reach* of an enlarged vertex component). Let R be the normal projection of V onto the outer surface C_1. We define the *reach*, $\mathcal{R}(V)$, of the enlarged vertex component $S'(V)$ to be the set of points on C_1 such that for all points $P \in \mathcal{R}(V)$ we have

$$PR \leq 10\sqrt{\delta c_1 M}. \tag{4.13}$$

By (4.6), if Q is an integer point in $S'(V)$, the normal projection R_1 of Q onto the surface C_1 lies in $\mathcal{R}(V)$, the reach of the enlarged component $S'(V)$.

LEMMA 4.2.5 (Enlarged Vertex Components and the Local Curvature Condition). *If*

$$M \geq \frac{100\delta c_1}{\kappa^2}, \tag{4.14}$$

then the Local Curvature Condition with respect to R, holds at all points R_1 in the reach of $S'(V)$.

Proof. Let P be a point of C_1 in $\mathcal{R}(V)$. By (4.13) and (4.14)

$$PR \leq 10\sqrt{\delta c_1 M} \leq \kappa M,$$

which is the threshhold for the Local Curvature Condition. □

4.3 Boundary Components

Definition. Let $S^\star(V_i)$ be the subset of $S'(V_i)$ consisting of integer points on the boundary of H. We will call this a boundary component. As $V_i \in S^\star(V_i)$ and $S^\star(V_i) \subseteq S'(V_i)$, different sets $S^\star(V_i)$ also correspond to disjoint sets A_i, centre W_i, on the surface of the d-sphere B (defined in Section 4.2). We have shown that for each enlarged vertex component $S'(V_i)$, if δ is sufficiently small then $S'(V_i)$ lies in a hyperplane and so $S^\star(V_i)$ lies in the same hyperplane.

The dimension of the integer point set $S^\star(V_i)$ is defined to be the least e for which $S^\star(V_i)$ lies in an e-dimensional hyperplane and $|S^\star(V_i)|$ to be the number of elements of $S^\star(V_i)$ in S.

When $e = 0$ we merely have to count the vertices of H. When $e = d$, the points of the boundary component lie on two or more hyperfaces of H, and we use a volume argument (Lemma 5.1.2 below). When $e = d - 1$ and $d = 3$, we have a straightforward estimation (Lemma 5.2.1 below), but when $e = d-1$ and $d \geq 4$ the argument becomes more complicated (Lemma 5.2.2). For intermediate dimensions $1 \leq e \leq d - 2$ we consider "girdles" of parallel planes and use a solid angle spacing argument. This takes its simplest form when $e = 1$ (Lemma 5.1.1 below). The cases $2 \leq e \leq d - 2$ require more combinatorial geometry and will be considered in chapter 7.

Chapter 5

Integer Points Close to Convex Surfaces

This chapter gives a proof of the non-trivial upper bound on the number of integer points lying on or near to a convex closed surface.

In Lemma 3.4.9 we counted all the vertices of the convex hull H and in Lemma 3.5.2, we counted all of the integer points in the enlarged vertex components that lie strictly inside H. Therefore, when $d = 3$, we need only consider the set $S(H)$ of integer points in our enlarged vertex components that lie strictly on the plane faces and edges of H in S. That is, the integer points in the boundary components of dimensions 1, 2 and 3.

5.1 Integer Points on One and d-Dimensional Boundary Components

We define a one-dimensional girdle to be the set of all the boundary components $S^*(V)$ of H which are one-dimensional and which lie parallel to some primitive integer vector $\mathbf{e}$. When considering the j-dimensional boundary components with $j \leq d-2$, we must also take into account the possibility that many of these components may be parallel. The completely parallel condition in higher dimensions was clarified in Chapter 3, where we introduced the idea of degrees of parallelism, as described in [38]. Henceforth, when referring to a girdle of parallel planes, we will always mean that the planes in the girdle are completely parallel.

LEMMA 5.1.1. *The number of integer points on 1-dimensional boundary components is estimated by*

$$\sum_{\dim S^*(V_i)=1} |S^*(V_i)| \leq \frac{2^{6d-1}3^3 c_1^{(d-1)/2}\pi^{d-1}}{\alpha_{d-1}c_0^{(d+1)/2}}\delta(c_1M)^{d-1}, \tag{5.1}$$

and when $d = 3$, this can be refined to

$$\sum_{\dim S^*(V_i)=1} |S^*(V_i)| \leq \left(\frac{2^{16}3^3\pi c_1}{c_0^2}\right)\delta(c_1M)^2. \tag{5.2}$$

Proof. We consider all the boundary components $S^*(V_i)$ which are 1-dimensional lying parallel to some primitive integer vector $\mathbf{e}$. Suppose that the component contains l points of $S(H)$, where

$$L+1 \leq l \leq 2L, \tag{5.3}$$

for some L equal to a power of two. We can take $\mathbf{g} = (l-1)\mathbf{e}$ in Lemma 4.2.3, with

$$|\mathbf{g}| \geq (l-1)|\mathbf{e}| \geq L|\mathbf{e}|.$$

In Lemma 4.2.3 the angle α between the vector $\mathbf{e}$ and the normal to C_1 at T, the point of C_1 nearest to V, satisfies

$$|\cos\alpha| \leq \frac{52\delta c_1}{c_0 L|\mathbf{e}|}.$$

Hence

$$\left|\frac{\pi}{2} - \alpha\right| \leq \frac{26c_1\pi\delta}{c_0 L|\mathbf{e}|}. \tag{5.4}$$

We consider distances along the surface of the d-sphere B, radius c_1M, as defined at the beginning of section 4.2. For each vector $\mathbf{e}$, there is an equatorial hyperplane through the centre of B at right angles to $\mathbf{e}$, which intersects with the surface of B in a set B'. By (5.4), the point W_i on the surface of B, where the normal is parallel to the normal $\mathbf{n}$ to C_1 at V lies

$$\leq \frac{26\pi\delta c_1 M}{c_0 L|\mathbf{e}|}$$

from the set B' measured along the surface of B. As stated the set A_i, lying on the surface of B, is the intersection of the surface of B with a d-ball radius

$\frac{1}{2}\sqrt{c_0\delta M}$, so it forms a $(d-1)$-ball in the spherical geometry of the surface of B, whose radius in spherical geometry is

$$\leq \frac{\pi}{2}\cdot\sqrt{\frac{c_0\delta M}{4}} \leq \pi\sqrt{\frac{c_0\delta M}{16}}\cdot\frac{4\sqrt{\delta c_1 M}}{L|\mathbf{e}|}$$

$$= \frac{\pi\delta c_1 M}{L|\mathbf{e}|}\left(\frac{c_0}{c_1}\right)^{\frac{1}{2}} \leq \frac{\pi\delta c_1 M}{c_0 L|\mathbf{e}|},$$

by (3.6) and (3.33).
Hence, each point of A lies within a distance

$$\leq \frac{26\pi\delta c_1 M}{c_0 L|\mathbf{e}|} + \frac{\pi\delta c_1 M}{c_0 L|\mathbf{e}|} = \frac{27\pi\delta c_1 M}{c_0 L|\mathbf{e}|}$$

from the equatorial hyperplane, measured along the surface of the d-sphere B.

We consider the "girdle" of one-dimensional boundary components $S^*(V_i)$ which are parallel to the fixed vector $\mathbf{e}$. The components in the girdle satisfying (5.3) correspond to points W_i and sets A_i on the surface of B, such that every point of A_i lies close to the equatorial hyperplane perpendicular to $\mathbf{e}$. The sets A_i lie in a $(d-1)$-annulus whose volume in spherical geometry is at most

$$(2\pi c_1 M)^{d-2}\left(\frac{54\pi\delta c_1 M}{c_0 L|\mathbf{e}|}\right) = \frac{27(2\pi)^{d-1}\delta(c_1 M)^{d-1}}{c_0 L|\mathbf{e}|}.$$

By (4.3) the number of disjoint sets A_i in the girdle is at most

$$\frac{2^{d-1}}{\alpha_{d-1}(c_0\delta M)^{(d-1)/2}}\cdot\frac{27(2\pi)^{d-1}\delta(c_1 M)^{d-1}}{c_0 L|\mathbf{e}|}$$

$$= \frac{27(4\pi c_1)^{d-1}M^{d-1/2}}{\alpha_{d-1}c_0^{(d+1)/2}\delta^{(d-3)/2}L|\mathbf{e}|}. \tag{5.5}$$

Each boundary component with l in the range (5.3) contains at most $2L$ integer points. Hence the boundary components $S^*(V_i)$ in the girdle for which the number l of points is in the range (5.3) contribute at most

$$\frac{54(4\pi c_1)^{d-1}M^{(d-1)/2}}{\alpha_{d-1}c_0^{(d+1)/2}\delta^{(d-3)/2}|\mathbf{e}|} \tag{5.6}$$

integer points. The estimate (5.6) refers only to components in the girdle for which l lies in the range (5.3). We keep the condition (5.3), and sum over primitive integer vectors $\mathbf{e}$. Since the component is a straight line segment lying within the strip E, by (3.33) we have

$$L|\mathbf{e}| \leq (l-1)|\mathbf{e}| \leq 4\sqrt{\delta c_1 M}.$$

We note that if two boundary components lie on the same line, then the vertices V_i which label the boundary components $S^*(V_i)$ must be different, so they are counted separately in this argument. We use the bounds of Lemma 4.2.4 to sum over $\mathbf{e}$, so that in the specific case, when $d = 3$, the number of points on one-dimensional boundary components with l in the range (5.3) is at most

$$\frac{54(4\pi c_1)^2 M}{\pi c_0}.2^6\left(\frac{4\sqrt{\delta c_1 M}}{L}\right)^2$$
$$= \frac{2^{15}3^3 c_1 \pi \delta (c_1 M)^2}{c_0^2 L^2},$$

and in the general case, with $j = 1$ in Lemma 4.2.4, we have at most

$$\frac{54(4\pi c_1)^{d-1} M^{(d-1)/2}}{\alpha_{d-1} c_0^{(d+1)/2} \delta^{(d-3)/2}}.2^{2d+1}\left(\frac{4\sqrt{\delta c_1 M}}{L}\right)^{d-1}$$
$$= \frac{2^{6d-2}3^3 c_1^{(d-1)/2}\pi^{d-1}\delta (c_1 M)^{d-1}}{\alpha_{d-1} c_0^{(d+1)/2} L^{d-1}}. \tag{5.7}$$

Finally we remove the condition (5.3) by summing L through powers of 2, noting that

$$\left(1 + \frac{1}{2^k} + \frac{1}{4^k} + \frac{1}{8^k} + \ldots\right) \leq \frac{2^k}{2^k - 1} \leq 2.$$

Hence the total number of integer points of $S(H)$ which lie on one-dimensional boundary components is at most

$$\left(\frac{2^{16}3^3\pi c_1}{c_0^2}\right)\delta (c_1 M)^2,$$

when $d = 3$, and

$$\leq \left(\frac{2^{6d-1}3^3 c_1^{(d-1)/2}\pi^{d-1}}{\alpha_{d-1} c_0^{(d+1)/2}}\right)\delta (c_1 M)^{d-1}. \qquad \square$$

when $d \geq 4$.

LEMMA 5.1.2. *The number of integer points on d-dimensional boundary components, when $\delta \leq \delta_0$, is estimated by*

$$\sum_{\dim S^*(V_i)=d} |S^*(V_i)| \leq 2(d+1)\,(3\alpha_d d!)^{\frac{d}{d+1}}\,(2c_1M)^{\frac{d(d-1)}{d+1}}$$

$$\leq 36(d+1)!\,(2c_1M)^{\frac{d(d-1)}{d+1}}, \tag{5.8}$$

and when $d = 3$, this can be refined to

$$\sum_{\dim S^*(V_i)=3} |S^*(V_i)| \leq 2^9\delta(c_1M)^{3/2}. \tag{5.9}$$

Proof. From (4.9) of Lemma 4.2.2, the d-dimensional boundary component $S^*(V_i)$ will have a d-dimensional volume $\mathrm{Vol}(H_i)$, with

$$\mathrm{Vol}(H_i) \leq \frac{52\delta c_1}{c_0}\left(20\sqrt{\delta c_1 M}\right)^{d-1}.$$

Since $\delta = \delta_0$ this gives a d-volume of at most $1/d!$. Applying the minor arc case of Lemma 3.5.4 then gives

$$K_i \leq d!\mathrm{Vol}(H_i) + d \leq (d+1)!\mathrm{Vol}(H_i)$$

$$\leq (d+1), \tag{5.10}$$

where K_i is the number of integer points contained in $S^*(V_i)$. However, the existence of d-dimensional $S^*(V_i)$ in $S'(V_i)$ requires that $K_i \geq d+1$, and so if we consider $\delta = \delta_0$, then K_i, the number of integer points in the d-dimensional boundary component is exactly $d+1$. The number of vertices of the convex hull is

$$\leq 2\,(3\alpha_d d!)^{\frac{d}{d+1}}\,(2c_1M)^{\frac{d(d-1)}{d+1}},$$

by Theorem 3.4.9. Hence, when $\delta = \delta_0$, the total number of integer points in the d-dimensional components is estimated by

$$\leq 2(d+1)\,(3\alpha_d d!)^{\frac{d}{d+1}}\,(2c_1M)^{\frac{d(d-1)}{d+1}}. \tag{5.11}$$

□

5.2 Integer Points on Boundary Components of Dimension $d-1$

LEMMA 5.2.1. *When $d = 3$, the number of integer points lying on the plane (2-dimensional) boundary components is estimated by*

$$\leq 2^{19}\delta(c_1 M)^2. \tag{5.12}$$

Proof. For each plane boundary component, by (4.8) of Lemma 4.2.2, the integer points will all lie in a square of area

$$400\delta c_1 M.$$

Either these planes will all have different outward normal vectors $\mathbf{n}_i$, or some will share vectors and so form convex sets that all lie on the same plane. In the latter instance, these plane boundary components will all lie in an annulus as described in Lemma 3.5.1. As each component is convex in this annulus we can apply the Lemma 3.5.4 and summing over all possible normal vectors gives the total number of integer points to be

$$\leq 3!2^6 3\delta c_1 M \sum \frac{1}{|\mathbf{n}_i|}. \tag{5.13}$$

Applying similar logic to the former case yields

$$\leq 3!400\delta c_1 M \sum \frac{1}{|\mathbf{n}_i|} \tag{5.14}$$

integer points. The constant in (5.14) is greater than that in (5.13) and for each $\mathbf{n}_i$ only one of the cases can occur. Hence we need only calculate the sum in (5.14). We note that the sum over all possible short normal vectors will be greater than that over all possible long normal vectors and so we consider

$$\leq 2.3!400\delta c_1 M \sum_{1\leq|\mathbf{n}_i|\leq N} \frac{1}{|\mathbf{n}_i|},$$

where, by Theorem 3.4.7,

$$N = 2^K = \left(\frac{8\pi}{27}\right)^{\frac{1}{4}} (c_1 M)^{\frac{1}{2}}.$$

Applying Lemma 4.2.4 yields

$$2.3!400\delta c_1 M \sum_{1\le|\mathbf{n}_i|\le N} \frac{1}{|\mathbf{n}_i|} \le 2^{12}3.5^2\delta c_1 M N^2$$

$$\le 2^{12}3.5^2\delta(c_1M)^2 \le 2^{19}\delta(c_1M)^2,$$

as required. □

LEMMA 5.2.2. *The number of integer points on $(d-1)$-dimensional boundary components, when $\delta \le \delta_0$ and $d \ge 4$, is estimated by*

$$\sum_{\dim S^*(V_i)=d-1} |S^*(V_i)| \tag{5.15}$$

$$\le d!(d+1)!2^{\frac{9d+17}{2}} \left(\frac{c_1}{c_0}\right)^{(d-1)/2} \left((c_1M)^{\frac{d(d-1)}{d+1}} + 2\left(\frac{c_1}{c_0}\right)^{(d-1)/2} \delta_0(c_1M)^{d-1}\right).$$

Proof. Each $(d-1)$-dimensional boundary component $S^*(V_i)$ is part of a hyperplane. The intersection of all such hyperplanes forms a convex polytope, H^*, that is contained within the convex hull H and the vertices of H^* are points of $S(H)$. Let Ψ be a hyperplane face of H^*, with outward normal vector $\mathbf{n}$ with respect to H^* (a primitive integer vector). Let Z be the point of C at which the normal $\mathbf{m}$ to C is parallel to $\mathbf{n}$, with $\mathbf{n}$ as outward normal vector. Let $\mathbf{m}$ cut Ψ in Y and the boundary surfaces C_0 and C_1 in W and X respectively (Figure 5.1). Then $\mathbf{m}$ is also the outward normal to C_0 at W, to C_1 at X, and the boundary hyperplane Ψ of the convex hull H^* at Y. Let $h = XY$, $h' = WY$ be the heights of X above Ψ and of W above or below Ψ as depicted in Figure 5.1. Each component in the annulus $E \cap \Pi$ is convex. We apply Lemma 3.5.4 with $j = d-1$. The set of points is strictly $(d-1)$-dimensional so we use the minor arc case of Lemma 3.5.4 with $j = d-1$, and lattice determinant $n = |\mathbf{n}|$ by Lemma 3.5.3. The volume V is estimated in Lemma 3.5.1, so we have an estimate for the number of integer points $N(\Psi)$ that lie in $E \cap \Psi$ such that

$$N(\Psi) \le \frac{(d-1)!V}{|\mathbf{n}|} + d - 1 \le \frac{d!V}{|\mathbf{n}|}$$

$$\le \frac{d!2^{\frac{d+9}{2}} d\delta(c_1M)^{\frac{d-1}{2}} h^{\frac{d-3}{2}}}{|\mathbf{n}|}. \tag{5.16}$$

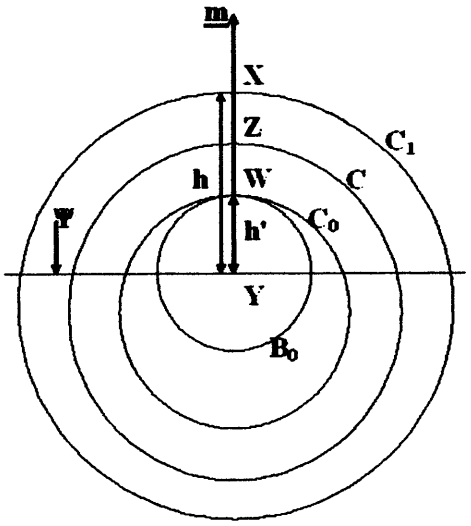

Figure 5.1: Heights along the common normal ℓ.

We sum over all the outward normal vectors of the hyperplanes Ψ. We get the total number of integer points on the $(d-1)$-boundary components, N, to be

$$N \leq \sum N(\Psi) \leq d! 2^{\frac{d+9}{2}} d\delta (c_1 M)^{\frac{d-1}{2}} h^{\frac{d-3}{2}} \sum \frac{1}{|\mathbf{n}|}. \tag{5.17}$$

We distinguish various cases according to the order of the points W, X, Y and Z on the normal l. If $h > 2\delta$ then the point W lies between X and Y and $h' > 0$, as shown in Figure 5.1. By the Curvature Condition, a d-ball B_0 of radius $c_0 M$, touching C_0 at W, fits completely inside C_0. Since $h' > 0$, the hyperplane Ψ cuts both C_0 and B_0. A "cap" of the hypersurface C_0 lies above the hyperplane Ψ. The $(d-1)$-dimensional surface content A of the cap cut from C_0 is greater than the content A' of its projection onto the plane Ψ. If $h \leq c_0 M + 2\delta$, then the equator of the d-ball B_0 lies below Ψ, and $A' \geq A''$, the $(d-1)$-dimensional content of $B_0 \cap \Psi$. This was calculated in the proof of Lemma 3.5.1, so we have

$$A \geq A' \geq A'' = \alpha_{d-1} \left((2c_0 M - h')h'\right)^{\frac{d-1}{2}}. \tag{5.18}$$

For given $h_0 \geq 4\delta$, let $Q(h_0)$ be the number of hyperplane faces of H with height in the range $h \geq h_0$. Let $h_0' = h_0 - 2\delta$ $(\geq 2\delta)$.

First we consider the extreme case

$$h \geq c_0 M + 2\delta. \tag{5.19}$$

The equatorial plane $\Psi^\star$ parallel to Ψ through the centre of B_0, cuts off a cap from C_0 of smaller $(d-1)$-dimensional content $A^\star$. Then $A^\star$ is greater than or equal to half the surface content of the ball B_0, which is greater than $B_0 \cap \Psi^\star$, so that

$$A \geq A^\star \geq \frac{1}{2} d\alpha_d (c_0 M)^{d-1} \geq B_0 \cap \Psi^\star = \alpha_{d-1}(c_0 M)^{d-1}. \tag{5.20}$$

The boundary content of C_0 is less than or equal to that of a d-sphere radius $c_1 M$,

$$\leq d\alpha_d (c_1 M)^{d-1}. \tag{5.21}$$

Let Q_E be the number of 'extreme faces' satisfying (5.19). Dividing the upper bound (5.21) by the lower bound (5.20) gives

$$Q_E \leq \frac{d\alpha_d (c_1 M)^{d-1}}{\alpha_{d-1}(c_0 M)^{d-1}} = \frac{d\alpha_d}{\alpha_{d-1}} \left(\frac{c_1}{c_0}\right)^{d-1} = \lambda_E, \tag{5.22}$$

say.

Secondly we consider the usual case

$$h \leq c_0 M + 2\delta, \tag{5.23}$$

so that $h_0' = h_0 - 2\delta \leq h - 2\delta \leq c_0 M$. Then from (5.18)

$$A \geq \alpha_{d-1} \left((2c_0 M - h')h'\right)^{\frac{d-1}{2}} \geq \alpha_{d-1} \left((2c_0 M - h_0')h_0'\right)^{\frac{d-1}{2}}. \tag{5.24}$$

Let $Q_U(h_0)$ be the number of 'usual' faces with height $h \geq h_0$ satisfying (5.23). Dividing the upper bound, (5.21), by the lower bound, (5.24) for this case gives

$$Q_U(h_0) \leq \frac{d\alpha_d (c_1 M)^{d-1}}{\alpha_{d-1} \left((2c_0 M - h_0')h_0'\right)^{\frac{d-1}{2}}}. \tag{5.25}$$

We simplify the upper bound (5.25). When $4\delta \leq h_0 \leq c_0 M + 2\delta$, then $2\delta \leq h_0' \leq c_0 M$. This implies that

$$\frac{1}{2c_0 M - h_0'} = \frac{1}{2c_0 M - h_0 + 2\delta} \leq \frac{1}{c_0 M}$$

and

$$\frac{1}{h_0'} \leq \frac{2}{h_0}.$$

Hence we can write

$$Q_U(h_0) \leq \frac{2^{\frac{d-1}{2}} d\alpha_d (c_1 M)^{d-1}}{\alpha_{d-1} (c_0 M h_0)^{\frac{d-1}{2}}} \tag{5.26}$$

$$\leq \frac{d\alpha_d}{\alpha_{d-1}} \left(\frac{c_1}{c_0}\right)^{\frac{d-1}{2}} \left(\frac{2c_1 M}{h_0}\right)^{\frac{d-1}{2}} = \lambda_U \left(\frac{2c_1 M}{h_0}\right)^{\frac{d-1}{2}}$$

say.

Each face Ψ is contained within the outer shell boundary C_1, which itself is contained within a d-hypersphere of radius $c_1 M$. Therefore all heights are at most $2c_1 M$, and we have

$$Q(h_0) \leq Q_U(h_0) + Q_E$$

$$\leq (\lambda_E + \lambda_U) \left(\frac{2c_1 M}{h_0}\right)^{\frac{d-1}{2}} \leq \left(\frac{2d\alpha_d}{\alpha_{d-1}}\right) \left(\frac{\sqrt{2}c_1}{c_0}\right)^{d-1} \left(\frac{c_1 M}{h_0}\right)^{\frac{d-1}{2}}$$

$$\leq 2^{\frac{d+5}{2}} d \left(\frac{c_1}{c_0}\right)^{d-1} \left(\frac{c_1 M}{h_0}\right)^{\frac{d-1}{2}} = \lambda_1 \left(\frac{c_1 M}{h_0}\right)^{\frac{d-1}{2}}, \tag{5.27}$$

say, where we have used (3.12). This result is valid for all faces with height $h \geq h_0 \geq 4\delta$.

For a fixed height h_0, the sum in (5.17) is maximal when as many short vectors as possible are counted, up to the upper bound in (5.27). In the proof of Lemma 4.2.4 we saw that there are at most $2^{2d-1}F^d$ vectors in each of the partitions and the inequality (4.11) is calculated assuming this maximum.

The total number of faces counted is

$$2^{2d-1}\left((2^0)^d + (2^1)^d + (2^2)^d + \ldots + (2^k)^d\right) = 2^{2d-1}\frac{((2^d)^{k+1} - 1)}{2^d - 1}$$

$$\geq 2^{d(k+1)+d-1} \geq 2^{d(k+1)}.$$

Therefore, to ensure that all possible faces are counted, we require

$$2^{d(k+1)} \geq \lambda_1 \left(\frac{c_1 M}{h_0}\right)^{\frac{d-1}{2}},$$

which implies that

$$2^{dk} \geq \frac{\lambda_1}{2^d}\left(\frac{c_1 M}{h_0}\right)^{\frac{d-1}{2}}.$$

Hence if

$$E = \lambda_1^{\frac{1}{d}}\left(\frac{c_1 M}{h_0}\right)^{\frac{d-1}{2d}} \geq 2^k \geq \left(\frac{\lambda_1}{2^d}\right)^{\frac{1}{d}}\left(\frac{c_1 M}{h_0}\right)^{\frac{d-1}{2d}} \tag{5.28}$$

in Lemma 4.2.4 with $j = 1$, then (5.17) is maximal. We have

$$\sum_{1\leq|\mathbf{e}|\leq 2^k}\frac{1}{|\mathbf{e}|} \leq 2^{2d+1}\left(\lambda_1^{\frac{1}{d}}\left(\frac{c_1 M}{h_0}\right)^{\frac{d-1}{2d}}\right)^{d-1}. \tag{5.29}$$

We now consider three cases.

Case 1.

$$h \geq \frac{1}{(c_1 M)^{\frac{d-1}{d+1}}} \geq 4\delta. \tag{5.30}$$

Let L be the total number of $(d-1)$-faces satisfying (5.30). We partition these $(d-1)$-faces into sets $G_1, G_2, \ldots, G_n$, according to their respective heights $h_i, 1 \leq i \leq n$, where $h_n > h_{n-1} > \ldots > h_2 > h_1 \geq 4\delta$. Let $L_i = |G_i|$, the number of hyperplane faces whose height is h_i; let $\mathbf{n}_{i,1}, \mathbf{n}_{i,2}, \ldots, \mathbf{n}_{i,L_i}$ be the normal vectors of the faces in G_i and let

$$\sigma_i = \sum_{j=1}^{L_i}\frac{1}{|\mathbf{n}_{i,j}|}. \tag{5.31}$$

By (5.28) we have

$$\sum_{i=1}^{n}\sigma_i \leq \sum_{1\leq|\mathbf{e}|\leq 2^k}\frac{1}{|\mathbf{e}|} \leq 2^{2d+1}\left(\lambda_1^{\frac{1}{d}}\left(\frac{c_1 M}{h_i}\right)^{\frac{d-1}{2d}}\right)^{d-1}.$$

Hence for each h_i, there exists a real number τ_i, $0 < \tau \leq 1$ with

$$\sigma_i = \tau_i 2^{2d+1}\left(\lambda_1^{\frac{1}{d}}\left(\frac{c_1 M}{h_i}\right)^{\frac{d-1}{2d}}\right)^{d-1}, \tag{5.32}$$

and

$$0 < \sum_{i=1}^{n} \tau_i \leq 1. \tag{5.33}$$

Let $N(h_i)$ be the number of integer points lying in $G_i \cap E$. Then by (5.16) and (5.32), we have

$$N(h_i) \leq d! 2^{\frac{d+9}{2}} d\delta (c_1 M)^{\frac{d-1}{2}} h_i^{\frac{d-3}{2}} \sum_{j=1}^{L_i} \frac{1}{|\mathbf{n}_{i,j}|}$$

$$\leq d! 2^{\frac{d+9}{2}} d\delta (c_1 M)^{\frac{d-1}{2}} h_i^{\frac{d-3}{2}} \tau_i 2^{2d+1} \left(\lambda_1^{\frac{1}{d}} \left(\frac{c_1 M}{h_i} \right)^{\frac{d-1}{2d}} \right)^{d-1}$$

$$= \lambda_2 \tau_i \delta (c_1 M)^{\frac{d-1}{2} + \frac{(d-1)^2}{2d}} h_i^{\frac{d-3}{2} - \frac{(d-1)^2}{2d}}$$

say. Summing over all heights h_i gives N_1, the total number of integer points contributed in this case to be

$$\leq \lambda_2 \delta (c_1 M)^{\frac{(d-1)(2d-1)}{2d}} \sum_{i=1}^{n} \tau_i h_i^{\frac{-(d+1)}{2d}}. \tag{5.34}$$

The exponent of h_i in (5.34) is negative, and as the h_i are positive, the sum is maximal when the h_i are as small as possible and the τ_i are as large as possible for the smallest h_i. Hence we take

$$\sum_{i=1}^{n} \tau_i = 1$$

in (5.34), and

$$h_i = \frac{1}{(c_1 M)^{\frac{d-1}{d+1}}},$$

for all i. Substituting for h_i in (5.34) gives the total number of integer points N_1 contributed to be

$$N_1 \leq \lambda_2 \delta (c_1 M)^{\frac{(d-1)(2d-1)}{2d} + \frac{d-1}{2d}} \sum_{i=1}^{n} \tau_i = \lambda_2 \delta (c_1 M)^{d-1}. \tag{5.35}$$

Case 2.

$$4\delta \leq h \leq \frac{1}{(c_1 M)^{\frac{d-1}{d+1}}}. \tag{5.36}$$

By Theorem 3.4.7, the maximum possible number of faces is

$$\leq 2(3\alpha_d d!)^{\frac{d}{d+1}}(c_1 M)^{\frac{d(d-1)}{d+1}}.$$

Hence if

$$E = 4(3\alpha_d d!)^{\frac{1}{d+1}}(c_1 M)^{\frac{d-1}{d+1}} \geq 2^k \geq 2(3\alpha_d d!)^{\frac{1}{d+1}}(c_1 M)^{\frac{d-1}{d+1}}$$

in Lemma 4.2.4 with $j = 1$,then (5.17) is maximal. We have

$$\sum_{1 \leq |\mathbf{e}| \leq 2^k} \frac{1}{|\mathbf{e}|} \leq 2^{2d+1}\left(4(3\alpha_d d!)^{\frac{1}{d+1}}(c_1 M)^{\frac{d-1}{d+1}}\right)^{d-1}. \tag{5.37}$$

Let N_2 be the total number of integer points in this case. Then substituting (5.37) into (5.17) yields

$$N_2 \leq d! 2^{\frac{d+9}{2}} d\delta (c_1 M)^{\frac{d-1}{2}} h^{\frac{d-3}{2}} . 2^{2d+1} 4^{d-1} (3\alpha_d d!)^{\frac{d-1}{d+1}} (c_1 M)^{\frac{(d-1)^2}{d+1}}. \tag{5.38}$$

Taking

$$h = \frac{1}{(c_1 M)^{\frac{d-1}{d+1}}}$$

to maximise (5.38) we have

$$N_2 \leq \lambda_3 \delta (c_1 M)^{\frac{(d-1)^2}{d+1} - \frac{(d-3)(d-1)}{2(d+1)} + \frac{d-1}{2}} = \lambda_3 \delta (c_1 M)^{d-1}. \tag{5.39}$$

Case 3. $0 \leq h \leq 4\delta$. As in the previous case, we assume the maximum number of short vector faces and we take $h = 4\delta$ to maximise (5.38). Let N_3 be the total number of integer points in this case. Then

$$N_3 \leq \lambda_3 \delta (4\delta)^{\frac{d-3}{2}} (c_1 M)^{\frac{(d-1)^2}{d+1} + \frac{d-1}{2}}$$

$$= \lambda_3 4^{\frac{d-3}{2}} (\delta c_1 M)^{\frac{d-1}{2}} (c_1 M)^{\frac{(d-1)^2}{d+1}}.$$

When

$$\delta \leq \delta_0 = \left(\frac{c_0}{2^{2d} 5^{d-1} 13 d! c_1} \right)^{\frac{2}{d+1}} (c_1 M)^{\frac{-(d-1)}{d+1}} = \mu (c_1 M)^{\frac{-(d-1)}{d+1}}$$

then we have the bound

$$N_3 \leq \lambda_3 \mu^{\frac{(d-1)}{2}} 2^{d-3} \left((c_1 M)^{\frac{2}{d+1}} \right)^{\frac{d-1}{2}} (c_1 M)^{\frac{(d-1)^2}{d+1}} = \lambda_3 \mu^{\frac{(d-1)}{2}} 2^{d-3} (c_1 M)^{\frac{d(d-1)}{d+1}}. \tag{5.40}$$

Finally we add together the upper bounds for N_1, N_2 and N_3 in (5.35), (5.39) and (5.40) respectively. When $\delta = \delta_0$ this gives the total number of integer points lying on the $(d-1)$-dimensional boundary components, N, to be

$$N \leq (\lambda_2 + \lambda_3) \delta_0 (c_1 M)^{d-1} + \lambda_3 \mu^{\frac{d-1}{2}} 2^{d-3} (c_1 M)^{\frac{d(d-1)}{d+1}}.$$

After simplification we find that

$$\lambda_2 \leq d(d+1)! 2^{3d+8} \left(\frac{c_1}{c_0} \right)^{\frac{d-1}{2}},$$

$$\lambda_3 \leq d!(d+1)! 2^{\frac{9d+17}{2}},$$

and

$$\mu^{\frac{d-1}{2}} 2^{d-3} \leq 1,$$

where we have used (3.11). Hence, if $\delta \leq \delta_0$ then N

$$\leq d!(d+1)! 2^{\frac{9d+17}{2}} \left(\frac{c_1}{c_0} \right)^{(d-1)/2} \left((c_1 M)^{\frac{d(d-1)}{d+1}} + 2 \left(\frac{c_1}{c_0} \right)^{(d-1)/2} \delta_0 (c_1 M)^{d-1} \right).$$

□

5.3 The Shelling Argument in 3-Dimensions

We now collect together the terms (3.31), (5.2), (5.12), (5.9) and (3.45) to obtain an upper bound for the total number of integer points contributed

from the j-dimensional boundary components, $0 \leq j \leq 3$, along with the internal integer points, when $\delta \leq \delta_0$. This gives

$$\leq \left(\frac{c_1}{c_0}\right)\left((2^7+2^9)(c_1M)^{\frac{3}{2}} + (2^{19}+2^{16}3^3\pi+2^8)\delta_0(c_1M)^2\right)$$

$$\leq \left(\frac{c_1}{c_0}\right)\left(2^{10}(c_1M)^{\frac{3}{2}} + 2^{23}\delta_0(c_1M)^2\right). \tag{5.41}$$

This result is valid for a shell of thickness $\delta = \delta_0$ and consists of terms independent of δ (degree zero) , and those with a factor of δ (degree one).

We cover the shell E of all extended vertex components, bounded internally by C_0 and externally by C_1, by R thinner concentric shells $E_1, \ldots, E_R$ of thickness δ_0. The distance between C_1 and C_0 along any inward normal vector to these two surfaces is 2δ. Hence we choose R to be the smallest such integer with

$$R\delta_0 \geq 2\delta, \qquad (R-1)\delta_0 < 2\delta,$$

so that

$$R < \frac{2\delta}{\delta_0} + 1. \tag{5.42}$$

The shell E_r consists of the points on some inward normal whose distance l from the surface C_1 lies in the range

$$(r-1)\delta_0 \leq l \leq r\delta_0.$$

When we replace δ with $r\delta_0$ in Lemma 3.3.2, we see that each shell E_r will satisfy the Curvature Condition, so that any plane sectional curve of E_r will lie in the range

$$c_0M \leq \rho \leq c_1M.$$

Therefore, expression (5.41) gives a uniform upper bound for the number of integer points contributed by any shell E_r. We note that

$$\delta_0\sqrt{c_1M} \leq \left(\frac{c_1}{c_0}\right)\left(\frac{1}{2^8}\right), \tag{5.43}$$

and

$$\left(\delta_0\sqrt{c_1M}\right)^{-1} \leq \left(\frac{c_1}{c_0}\right)2^9. \tag{5.44}$$

THEOREM 1. *Suppose that C is a convex surface in 3-dimensional Euclidean space $\mathbb{E}^3$, satisfying the Curvature Condition at size M (so that C is contained in a sphere radius $c_1 M$). Then the total number, N, of integer points lying either on C, or within a distance δ of C, is bounded by*

$$\leq \left(\frac{c_1}{c_0}\right)^2 2^{16} \left((c_1 M)^{\frac{3}{2}} + 2^9 \delta (c_1 M)^2\right).$$

Proof. We multiply the upper bound (5.41) by the maximum number of shells given by (5.42). This yields

$$\left(\frac{2\delta}{\delta_0} + 1\right)\left(\frac{c_1}{c_0}\right)\left(2^{10}(c_1 M)^{\frac{3}{2}} + 2^{23}\delta_0 (c_1 M)^2\right).$$

Simplifying using (5.43) and (5.44) and combining terms we have at most

$$\left(\frac{c_1}{c_0}\right)^2 2^{16} \left((c_1 M)^{\frac{3}{2}} + 2^9 \delta (c_1 M)^2\right)$$

integer points. □

Chapter 6

Boundary Content, Relative Volumes and Ehrhart Theory

This chapter gives an overview of Ehrhart theory and convex polytopes, concluding with results that appear to be new.

6.1 Andrews' Theorem and Ehrhart Theory

Let C be the boundary surface of a strictly convex bounded d-dimensional body. Strictly convex means that if P and Q are points on C, then points on the line segment PQ between P and Q lie in the convex body, but not on its boundary C. Let MC denote the dilation of C by a factor M. Andrews [1], [2] proved that the number of points of the integer lattice on MC is

$$O\left(M^{\frac{d(d-1)}{d+1}}\right),$$

as M tends to infinity. Strict convexity is necessary because a part of a $(d-1)$-dimensional hyperplane in the boundary C can give as many as a constant times M^{d-1} integer points for infinitely many values of M.

Andrews defines the closed strictly convex body by the homogeneous function $f(x_1, \ldots, f_d)$, such that

$$f(x_1, \ldots, f_d) \leq R,$$

and the boundary of the strictly convex body by the equality

$$f(x_1, \ldots, f_d) = R. \tag{6.1}$$

The number of solutions to (6.1) then corresponds to the number of solutions of a general class of diophantine equations.

Definition.

(1) Let $\mathcal{K}$ be a convex closed body. We define the boundary content of $\mathcal{K}$ to be the surface content of the boundary of $\mathcal{K}$

(2) Let $\mathcal{P}$ be a convex d-polytope and F a j-dimensional face of $\mathcal{P}$. By the relative j-dimensional volume of F we mean the volume of F normalised with respect to the sublattice of the j-dimensional plane containing F.

LEMMA 6.1.1. *Let $\mathcal{P}$ be a convex d-polytope contained in a d-hypersphere of radius length R and let $B(\mathcal{P})$ denoted the boundary content of $\mathcal{P}$. Let the number of vertices of $\mathcal{P}$ which are integer points be R^k. Then*

$$k \leq \frac{d(d-1)}{(d+1)}.$$

If equality holds, then

$$B(\mathcal{P}) \asymp R^{d-1}$$

Proof. By convexity, $B(\mathcal{P})$ is less than or equal to the boundary content of a d-hypersphere containing the polytope and if $\mathcal{P}$ has $O(R^k)$ integer point vertices, then using Andrew's Theorem [1] on boundary content we have

$$O(R^{d-1}) \gg B(\mathcal{P}) \gg O(R^{\frac{k(d+1)}{d}}),$$

or

$$O(R^{d-1}) = B(\mathcal{P}) = O(R^{\frac{k(d+1)}{d}}). \qquad \square$$

We now introduce the concept of Ehrhart polynomials [6] and some derived results [5] in order to further our analysis of the convex hull H in d-dimensional Euclidean space.

THEOREM 6.1.2 (Ehrhart's Theorem). *Let $N_{\mathcal{P}}(t)$ be the lattice point enumerator function of a convex integral d-polytope $\mathcal{P}$, the number of lattice*

points in the closed set $t\mathcal{P}$. Then there is a polynomial $L_{\mathcal{P}}(t)$ of degree d with rational coefficients ($L_{\mathcal{P}}(t) \in \mathbb{Q}[t]$) such that for positive integer values of t,

$$N_{\mathcal{P}}(t) = L_{\mathcal{P}}(t)$$

satisfying the combinatorial identities

$$(1-z)^{d+1}\left(1+\sum_{t=1}^{\infty} L_{\mathcal{P}}(t)z^t\right) = a_d z^d + a_{d-1}z^{d-1} + \cdots + a_1 z + 1,$$

$$L_{\mathcal{P}}(t) = \sum_{j=0}^{d} a_j \binom{d+t-j}{d}. \tag{6.2}$$

where $a_1, a_2, \ldots, a_d$ take integral values greater than or equal to zero depending only on the polytope $\mathcal{P}$.

COROLLARY. *Let $N^{\circ}_{\mathcal{P}}(t)$ be the number of lattice points in the interior of the polytope $t\mathcal{P}$. The values of $N^{\circ}_{\mathcal{P}}(t)$ at positive integers t are again given by the values of some polynomial $L^{\circ}_{\mathcal{P}}(t)$,*

$$N^{\circ}_{\mathcal{P}}(t) = L^{\circ}_{\mathcal{P}}(t).$$

Proof of Corollary. The faces and facets of $\mathcal{P}$ are lattice polytopes of lower dimension, so $N^{\circ}_{\mathcal{P}}(t)$ can be calculated by an inclusion-exclusion sieve. That is, count all of the integer points in $\mathcal{P}$ and then subtract the ones on the facets, add back the points that you have overcounted and so forth. □

PROPOSITION 6.1.3 (Basic Properties of Ehrhart Polynomials). *If $\mathcal{P}$ is a convex d-polytope with integer point vertices and Ehrhart polynomial*

$$L_{\mathcal{P}}(t) = c_d t^d + c_{d-1}t^{d-1} + \cdots + c_0 t + c_0,$$

then the following properties hold.

$$d!c_i \in \mathbb{Z}, \quad 0 \le i \le d. \tag{6.3}$$

$$c_0 = 1. \tag{6.4}$$

$$c_d = V_{\mathcal{P}} = \frac{1}{d!}\sum_{j=0}^{d} a_j > 0, \tag{6.5}$$

where $V_{\mathcal{P}}$ is the d-dimensional volume of $\mathcal{P}$ in $\mathbb{Z}^d$. For a "general d-lattice" Λ with determinant n, we have c_d equal to the relative volume of $\mathcal{P}$, so that

$$c_d = \frac{V_{\mathcal{P}}}{n}. \tag{6.6}$$

If $S_{\mathcal{P}}$ is the sum of the relative volumes of the facets of $\mathcal{P}$, then

$$c_{d-1} = \frac{1}{2}S_{\mathcal{P}} = \frac{1}{2(d-1)!}\sum_{j=0}^{d} a_j(d-2j+1) > 0. \tag{6.7}$$

The inclusion-exclusion sieve for $N^{\circ}_{\mathcal{P}}(t)$ yields

$$L^{\circ}_{\mathcal{P}}(t) = c_d t^d - c_{d-1}t^{d-1} + c_{d-2}t^{d-2} - \cdots \tag{6.8}$$

An immediate consequence of (6.8) is that the discrete boundary content of $t\mathcal{P}$ is given by

$$L_{\mathcal{P}}(t) - L^{\circ}_{\mathcal{P}}(t) = 2c_{d-1}t^{d-1} + 2c_{d-3}t^{d-3} + \cdots. \tag{6.9}$$

For example, if $\mathcal{P}$ is the unit d-cube with sides parallel to the coordinate axes, then

$$L_{\mathcal{P}}(t) - L^{\circ}_{\mathcal{P}}(t) = (t+1)^d - (t-1)^t = 2\binom{d}{d-1}t^{d-1} + 2\binom{d}{d-3}t^{d-3} + \cdots$$

and the discrete volume of the boundary is equal to the continuous volume of the boundary. If $d = 4$ and $t = R$ then the boundary content of the 4-cube is given by the expression

$$8R^3 + 8R.$$

Definition. If $\mathcal{P}$ is a convex d-polytope with integer point vertices and F_j a j-dimensional face of $\mathcal{P}$, then F_j lies in a vector space V for which $\mathbb{Z}^d \cap V$ is a full j-dimensional lattice.

More generally we can have a d-space V and a d-dimensional lattice Λ in V, and a d-polytope $\mathcal{P}$ in V with lattice vertices, and count $N_{\mathcal{P},\Lambda}(t)$. There is a linear map which transforms V to $\mathbb{R}^d$, Λ to the integer lattice $\mathbb{Z}^d$, and $\mathcal{P}$ to a d-polytope $\mathcal{Q}$ with integer point vertices, so there is an Ehrhart polynomial $L_{\mathcal{P},\Lambda}(t)$.

One useful interpretation of this is that for every j-face of $\mathcal{P}$ there exists an Ehrhart polynomial of degree j.

Definition. Let $\mathcal{F}_{j,\mathcal{P}}(t)$ be the face lattice point enumerator of our convex d-polytope with integer point vertices such that

$$\mathcal{F}_{j,\mathcal{P}}(t) = \sum_{\mathcal{Q}} L_{j,\mathcal{Q}}(t) = c_{j,j}t^j + c_{j,j-1}t^{j-1} + \ldots + c_{j,1}t + c_{j,0}, \tag{6.10}$$

where $\mathcal{Q}$ runs through all of the j-dimensional faces of $\mathcal{P}$. Hence $\mathcal{F}_{j,\mathcal{P}}(t)$ counts all of the integer points lying on the individual j-faces of $\mathcal{P}$ and for $j = d$ we have the special identity

$$L_{\mathcal{P}}(t) = L_{d,\mathcal{P}}(t) = \mathcal{F}_{d,\mathcal{P}}(t) \tag{6.11}$$

We note that as $\mathcal{F}_{j,\mathcal{P}}(t)$ is the sum of all of the individual Ehrhart polynomials of the j-faces of $\mathcal{P}$, the leading coefficient of its polynomial must be equal to the relative volume of the union of these j-faces. This union is sometimes referred to as the "j-skeleton" of $\mathcal{P}$.

The next proposition was originally conjectured by Ehrhart and later proved by Macdonald.

PROPOSITION 6.1.4 (Ehrhart-Macdonald Reciprocity). *If $\mathcal{P}$ is a convex d-polytope with integer point vertices then*

$$L^{\circ}_{\mathcal{P}}(t) = (-1)^d L_{\mathcal{P}}(-t), \tag{6.12}$$

and similarly for the face lattice point enumerator

$$\mathcal{F}^{\circ}_{j,\mathcal{P}}(t) = (-1)^j \mathcal{F}_{j,\mathcal{P}}(-t), \tag{6.13}$$

where $\mathcal{F}^{\circ}_{j,\mathcal{P}}(t)$ counts the integer points lying strictly inside the boundary $(j-1)$-polytopes of the j-faces.

Given that $\mathcal{F}^{\circ}_{j,\mathcal{P}}(t)$ counts the integer points by faces, we can re-write (6.11) as

$$L_{\mathcal{P}}(t) = L_{d,\mathcal{P}}(t) = \mathcal{F}_{d,\mathcal{P}}(t) = \sum_{j=0}^{d} \mathcal{F}^{\circ}_{j,\mathcal{P}}(t) = \sum_{j=0}^{d} (-1)^j \mathcal{F}_{j,\mathcal{P}}(-t), \tag{6.14}$$

where

$$(-1)^d \mathcal{F}_{d,\mathcal{P}}(-t) = (-1)^d L_{\mathcal{P}}(-t) = L^{\circ}_{\mathcal{P}}(t),$$

so that

$$L_{\mathcal{P}}(t) - L^{\circ}_{\mathcal{P}}(t) = \sum_{j=0}^{d-1} (-1)^j \mathcal{F}_{j,\mathcal{P}}(-t), \tag{6.15}$$

and comparing the coefficients of powers of t in (6.15) with those of (6.9) yields

$$c_r = \frac{1}{2} \sum_{j=0}^{d-1} (-1)^{j+r} c_{j,r}, \tag{6.16}$$

where $c_{j,r} = 0$ for $r > j$.

6.2 Stirling Numbers of the First Kind

Definition. The signed Stirling numbers of the first kind, denoted $s(n,m)$, are defined such that the number of permutations of n objects which contain exactly m permutation cycles is the non-negative number

$$|s(n,m)| = (-1)^{n-m} s(n,m).$$

If the number of objects in a permutation cycle is greater than or equal to three, then the reverse cycle is counted as distinct. For example $(123) \neq (321)$ but $(12) = (21)$ under this definition.

For $m > n$ we must have $s(n,m) = 0$ and $s(n,n) = 1$ as the only possible option is $(1)(2)(3)\ldots(n)$. The generating function for the Stirling numbers of the first kind is

$$\sum_{j=0}^{k} s(k,j) x^j = x(x-1)(x-2)\cdots(x-k+1) = n! \binom{x}{n},$$

from which it can be shown that

$$s(n,1) = (-1)^{n-1}(n-1)! \tag{6.17}$$

and

$$s(n,n-1) = -\binom{n}{2}. \tag{6.18}$$

The Stirling numbers of the first kind also satisfy

$$s(n+1,m) = s(n,m-1) - n s(n,m), \tag{6.19}$$

for $1 \leq m \leq n$ and

$$s(n,m) = \sum_{k=m}^{n} n^{k-m} s(n+1, k+1), \tag{6.20}$$

for $m \geq 1$ and

$$\binom{m}{r} s(n,m) = \sum_{k=m-r}^{n-r} \binom{n}{k} s(n-k, r) s(k, m-r), \tag{6.21}$$

for $0 \leq r \leq m$.

The triangle of signed Stirling numbers of the first kind for $1 \leq m \leq n \leq 5$ is given below.

$$\begin{array}{ccccc} 1 & & & & \\ -1 & 1 & & & \\ 2 & -3 & 1 & & \\ -6 & 11 & -6 & 1 & \\ 24 & -50 & 35 & -10 & 1 \end{array}$$

The following important theorem, obtained by Betke and McMullen in 1984, involves the Stirling numbers of the first kind.

THEOREM 6.2.1. *Let $\mathcal{P}$ be a convex d-polytope with integer point vertices and with Ehrhart polynomial*

$$L_{\mathcal{P}}(t) = c_d t^d + c_{d-1} t^{d-1} + \cdots + c_0 t + c_0,$$

then

$$c_r \leq (-1)^{d-r} s(d,r) c_d + (-1)^{d-r-1} \frac{s(d, r+1)}{(d-1)!} \tag{6.22}$$

for $r = 1, 2, \cdots, d-1$.

The following three results follow from Theorem 6.2.1 and to the best of the our knowledge, have not been published anywhere else prior to this thesis.

LEMMA 6.2.2. *Let $\mathcal{P}$ be a convex d-polytope with integer point vertices and let $\mathcal{Q}$ be a j-dimensional face of $\mathcal{P}$ with Ehrhart polynomial*

$$L_{j,\mathcal{Q}}(t) = c_{j,j} t^j + c_{j,j-1} t^{j-1} + \ldots + c_{j,1} t + c_{j,0}.$$

Then for $j \geq 2$

$$\nu_{j-1} \leq j^2 \nu_j, \tag{6.23}$$

and for $j \geq 1$

$$\nu_j \leq \frac{((d-1)!)^2}{(j!)^2} \nu_{d-1} \leq \frac{(d!)^2}{(j!)^2} \nu_d \tag{6.24}$$

where ν_j *is the sum of the* j*-dimensional relative volumes of the* j*-faces of* $\mathcal{P}$.

COROLLARY. *Let* K_j *be the number of integer points lying strictly in the interior of the* j*-faces of* $\mathcal{P}$*, so that none of these integer points lie on a face of lower dimension, then*

$$K_j \leq \frac{d((d-1)!)^2}{j!} \nu_{d-1} \leq \frac{d(d!)^2}{j!} \nu_d. \tag{6.25}$$

Proof. Let V_Q be the relative j-dimensional volume of Q and V_i be the relative $(j-1)$-dimensional volume of facet F_i of Q, so that

$$c_{j,j} = V_Q, \quad c_{j,j-1} = \frac{1}{2} \sum_i V_i.$$

By Theorem 6.2.1, for $j \geq 2$ we have

$$c_{j,j-1} \leq (-1)^1 s(j, j-1) c_{j,j} + (-1)^0 \frac{s(j,j)}{(j-1)!},$$

and by (6.18) this simplifies to

$$c_{j,j-1} \leq \binom{j}{2} c_{j,j} + \frac{1}{(j-1)!},$$

so that

$$c_{j,j-1} \leq \frac{j(j-1)}{2} c_{j,j} + \frac{1}{(j-1)!}.$$

Now, in any lattice, a j-dimensional polytope with lattice point vertices has volume at least $1/j!$ times the volume of the lattice cell (relative volume at least $1/j!$). This idea has already been used in Lemma 3.5.4. Hence

$$c_{j,j-1} \leq \frac{j(j-1)}{2} c_{j,j} + j c_j = \left(\frac{j(j-1)}{2} + j \right) c_{j,j},$$

and

$$c_{j,j-1} \leq j^2 c_{j,j},$$

so that

$$\sum_i V_i \leq 2j^2 V_Q.$$

Each $(j-1)$-face is the intersection of at least two j-faces, so that summing over all of the j-faces in $\mathcal{P}$ counts each of the $(j-1)$-faces at least twice. Therefore

$$\nu_{j-1} \leq \frac{1}{2} \sum_Q \sum_i V_i \leq j^2 \sum_Q V_Q = j^2 \nu_j,$$

and recursive use of this inequality yields the required result

$$\nu_j \leq (j+1)^2 \nu_{j+1} \leq (j+1)^2 (j+2)^2 \nu_{j+2} \cdots \leq \frac{((d-1)!)^2}{(j!)^2} \nu_{d-1} \leq \frac{(d!)^2}{(j!)^2} \nu_d.$$

That is, in terms of order of magnitude notation, we have

$$\nu_j = O(\nu_{d-1}) = O(\nu_d), \quad 1 \leq j \leq (d-1).$$

By the minor case of Lemma 3.5.4 (stated in chapter 3), if K_j is the number of integer points lying on the j-dimensional faces of $\mathcal{P}$, then

$$K_j \leq j! \nu_j + j \leq (j+1)! \nu_j,$$

so that

$$K_j \leq \frac{((d-1)!)^2 (j+1)!}{(j!)^2} \nu_{d-1} \leq \frac{d((d-1)!)^2 j!}{(j!)^2} \nu_{d-1}.$$

Hence

$$K_j \leq \frac{d((d-1)!)^2}{j!} \nu_{d-1} \leq \frac{d(d!)^2}{j!} \nu_d. \qquad \square$$

THEOREM 6.2.3. *Let $\mathcal{P}$ be a convex d-polytope with integer point vertices, with volume ν_d. Let ν_{d-1} be the sum of the relative volumes of the hyperplane faces (with respect to the sublattice on the appropriate hyperplane). Let M be the number of integer points on the surface of $\mathcal{P}$ which are not vertices of $\mathcal{P}$. Then*

$$M \leq (e-1)d((d-1)!)^2 \nu_{d-1} \leq (e-1)d(d!)^2 \nu_d. \tag{6.26}$$

Proof. In the notation of the Corollary to Lemma 6.2.2, for each $j = 1$ to $d-1$ we have

$$K_j \leq \frac{d((d-1)!)^2}{j!}\nu_{d-1}, \quad 1 \leq j \leq d-1.$$

To count all boundary points which are not vertices, we sum from $j = 1$ to $d-1$.

$$\sum_{j=1}^{d-1} K_j \leq d((d-1)!)^2\nu_{d-1}\sum_{j=1}^{d-1}\frac{1}{j!},$$

$$\leq d((d-1)!)^2\nu_{d-1}\sum_{j=1}^{\infty}\frac{1}{j!} = d((d-1)!)^2(e-1)\nu_{d-1}.$$

By (6.23)

$$\nu_{d-1} \leq d^2\nu_d,$$

which gives the second inequality in (6.26). □

Thus the relative volume of the boundary content of the facets of a convex d-polytope with integer point vertices controls the total number of integer points (excluding the vertices) that can lie on the convex hull.

Hence, letting $\mathcal{P}$ have Ehrhart polynomial

$$L_{\mathcal{P}}(t) = c_d t^d + c_{d-1}t^{d-1} + \cdots + c_0 t + c_0,$$

then N, the total number of integer points lying on its convex hull, satisfies

$$N \leq d((d-1)!)^2(e-1)2c_{d-1} + f_0, \tag{6.27}$$

where f_0 is the number of vertices of $\mathcal{P}$.

We conclude this chapter with a short glance at the well documented subject of Ehrhart Polynomials and simplices.

Equation (6.2) implies that the set of binomial coefficients

$$\left\{\binom{d+n-j}{d} : 0 \leq j \leq d\right\}$$

forms an alternative basis for the vector space of Ehrhart polynomials of degree d, compared to the standard polynomial basis

$$\left\{n^j : 0 \leq j \leq d\right\}.$$

This is emphasized further by the link between simplices and binomial coefficients, which we state without proof in the following Lemma.

LEMMA 6.2.4. *Let $L_\Delta(t)$ be the Ehrhart polynomial of the standard simplex Δ in $\mathbb{R}^d$, with vertices at the origin and at unit distance along the coordinate axes. Then*

$$L_\Delta(t) = \binom{d+t}{d} = \frac{1}{d!}\sum_{j=0}^{d}(-1)^{d-j}s(d+1,j+1)t^j, \tag{6.28}$$

and

$$L^\circ_\Delta(t) = \binom{t-1}{d} = (-1)^d\binom{d-t}{d} = (-1)^d L_\Delta(-t) \tag{6.29}$$

COROLLARY. *Let $L_\mathcal{P}(t)$ be the Ehrhart polynomial of a convex d-polytope $\mathcal{P}$ with integer point vertices. Then*

$$L_\mathcal{P}(t) = \sum_{j=0}^{d} a_j L_\Delta(t-j). \tag{6.30}$$

Proof of Corollary. Direct substitution of equation (6.28) into (6.2) gives the required result. □

Hence the lattice point enumerator of a convex d-polytope $\mathcal{P}$ can be expressed as a linear combination of the lattice point enumerators of the standard d-simplex with different integer multiples.

This result agrees with a very important theorem in polytope theory, which states that "every convex polytope can be triangulated using no new vertices".

Chapter 7

Integer Points Close to Convex Hypersurfaces

This chapter gives a proof of a natural generalisation on a Theorem by George E. Andrews.

7.1 Girdles and Lattice Determinants

Definition.

(1) By *lattice* we will understand a discrete submodule Λ of a finite-dimensional Euclidean space.

(2) A compact convex set with non-empty interior is called a *convex body.*

We now recall Minkowski's Second Theorem [17].

LEMMA 7.1.1 (Minkowski's Second Theorem). *Let K be a convex body symmetrical in the origin. Let Λ be a lattice. Let the successive minima of K with respect to Λ be $\lambda_1, \lambda_2, \ldots, \lambda_d$, defined by*

$$\lambda_i = \inf \{\lambda > 0 : \lambda K \textit{ contains at least } i \textit{ linearly independent vectors of } \Lambda\},$$

where

$$0 < \lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_d < +\infty.$$

Then they obey the inequality

$$\frac{2^d D(\Lambda)}{d!} \leq \lambda_1\lambda_2\lambda_3\ldots\lambda_d V(K) \leq 2^d D(\Lambda), \tag{7.1}$$

where $V(K)$ is the volume of K and $D(\Lambda)$ is the determinant of the lattice.

COROLLARY. *Let Λ and $D(\Lambda)$ be defined as above, with $\lambda_1, \ldots, \lambda_d$ the ordinary Euclidean lengths of the lattice vectors. Let K be the open unit d-ball, then the determinant or fundamental volume of the lattice satisfies*

$$\frac{\lambda_1\lambda_2\lambda_3\ldots\lambda_d\alpha_d}{2^d} \leq D(\Lambda) \leq \lambda_1\lambda_2\lambda_3\ldots\lambda_d. \tag{7.2}$$

Proof of Corollary. By construction, if $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_d$ are linearly independent vectors of Λ with respective Euclidean lengths $\lambda_1, \lambda_2, \ldots \lambda_d$, then the $\mathbf{e}_i$ are ordered by length. Let θ_i be the angle between $\mathbf{e}_{i+1}$ and the i-dimensional plane lattice defined by $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_i$ with determinant $D(\Lambda_i)$. Then

$$D(\Lambda) = \lambda_d \sin\theta_{d-1} D(\Lambda_{d-1}) = \lambda_d\lambda_{d-1} \sin\theta_{d-1} \sin\theta_{d-2} D(\Lambda_{d-2}) = \ldots$$

$$\ldots = \lambda_1\lambda_2\lambda_3\ldots\lambda_d \prod_{i=1}^{d} \sin\theta_i \leq \lambda_1\lambda_2\lambda_3\ldots\lambda_d.$$

The upper bound of (7.1) gives

$$\frac{\lambda_1\lambda_2\lambda_3\ldots\lambda_d V(K)}{2^d} \leq D(\Lambda),$$

and taking $V(K) = \alpha_d$ gives the required result. □

Here we introduce the idea of a j-dimensional girdle, $2 \leq j \leq d-2$, with fixed basis vectors $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \ldots, \mathbf{e}_j$. The vectors $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \ldots, \mathbf{e}_j$ through the origin generate a j-dimensional lattice Λ in a j-plane Π_0. Each j-girdle is therefore defined to be a set of j-dimensional boundary components whose j-planes Π are all completely parallel to Π_0. The sets of integer points on each j-plane Π are cosets of Λ, congruent to Λ by translation, and the number of integer points lying on each j-girdle is related to the fundamental j-volume or determinant of the lattice Λ. Conversely the lattice Λ determines the linearly independent vectors $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \ldots, \mathbf{e}_j$ in the Corollary to Lemma 7.1.1. We write $l(\Lambda)$ for the length λ_j of the longest basis vector $\mathbf{e}_j$ and introduce the following lemma to assist with our counting argument.

LEMMA 7.1.2 (sums of reciprocal lattice determinants). *For* $k = 1, 2, \ldots$ $\ldots, d-1$ *we have*

$$\sum_{l(\Lambda)\le E} \frac{1}{(D(\Lambda))^k} \le \frac{\left(2^{2d+2k} E^{d-k}\right)^j}{\alpha_j^k}, \tag{7.3}$$

where the sum ranges over all possible j*-dimensional lattice determinants,* $j \le d-1$*, whose basis vectors have length* $\le E$*. When we take* E *to be the maximum possible length of a boundary component basis vector, then by* (4.6), $E = 10\sqrt{\delta c_1 M}$ *and*

$$\sum_{l(\Lambda)\le E} \frac{1}{(D(\Lambda))^k} \le \frac{\left(2^{3d+k}\left(5\sqrt{\delta c_1 M}\right)^{d-k}\right)^j}{\alpha_j^k}. \tag{7.4}$$

Proof. By the Corollary to Lemma 7.1.1, there are linearly independent vectors $\mathbf{e}_i, 1 \le i \le j$, of the lattice Λ with

$$\frac{|\mathbf{e}_1||\mathbf{e}_2|\ldots|\mathbf{e}_j|\alpha_j}{2^j} \le D(\Lambda) \le |\mathbf{e}_1||\mathbf{e}_2|\ldots|\mathbf{e}_j|.$$

Hence by Lemma 7.1.1 and Lemma 4.2.4

$$\sum_{l(\Lambda)\le E} \frac{1}{(D(\Lambda))^k} \le \left(\frac{2^j}{\alpha_j}\right)^k \sum_{|\mathbf{e}_1|\le E} \sum_{|\mathbf{e}_2|\le E} \cdots \sum_{|\mathbf{e}_j|\le E} \frac{1}{|\mathbf{e}_1|^k |\mathbf{e}_2|^k \ldots |\mathbf{e}_j|^k}$$

$$\le \left(\frac{2^j}{\alpha_j}\right)^k \left(2^{2d+k} E^{d-k}\right)^j = \frac{\left(2^{2d+2k} E^{d-k}\right)^j}{\alpha_j^k}.$$

By (4.6) the vectors $|\mathbf{e}_i|$ are non-zero integer vectors with

$$|\mathbf{e}_i| \le l(\Lambda) \le E = 10\sqrt{\delta c_1 M}, \tag{7.5}$$

so that

$$\sum_{l(\Lambda)\le E} \frac{1}{(D(\Lambda))^k} \le \frac{\left(2^{2d+2k}\left(10\sqrt{\delta c_1 M}\right)^{d-k}\right)^j}{\alpha_j^k} = \frac{\left(2^{3d+k}\left(5\sqrt{\delta c_1 M}\right)^{d-k}\right)^j}{\alpha_j^k},$$

which establishes the result. □

7.2 Summing the Boundary Components

When we consider a j-dimensional boundary component $S^\star(V)$, $2 \leq j \leq d-2$, there are geometrical considerations. The points of $S^\star(V)$ lie on some j-dimensional plane Π containing the vertex V. The lattice of integer points meets Π is some j-dimensional lattice Λ with a basis consisting of j integer vectors $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \ldots, \mathbf{e}_j$. The points of $S^\star(V)$ lie in the set E, the shell bounded by the surfaces C_1 and C_0. By the calculations of Lemma 4.2.1 the points of $S^\star(V)$ lie in a d-dimensional cylindrical slab G whose axis is the normal $\mathbf{n}$ to C_1 at R, the point of C_1 closest to the vertex V. The upper and lower faces of the d-cylinder G lie in the tangent hyperplane F at R and in a completely parallel hyperplane F', separated by a small distance

$$\eta = \frac{52\delta c_1}{c_0}.$$

The upper and lower faces of the d-cylinder are $(d-1)$-spheres of radius $10\sqrt{\delta c_1 M}$ by inequality (4.6) of Lemma 4.2.1.

As defined in section 3.2, in d-dimensional space, through a given point V on a j-plane Π, there exists a unique $(d-j)$-plane Ψ that is completely orthogonal to Π.

Let W_1 be a point of F' not in Π or Ψ and lying at a distance $10\sqrt{\delta c_1 M}$ from the axis of the d-cylinder. As $2 \leq j, d-j \leq d-2$, we can choose W_1 such that Y, the (two-dimensional) affine plane defined by $\mathbf{n}$ and W_1, contains at least one other point P of the j-plane Π in addition to the vertex V. Then $Y \cap G$ is a rectangle containing P, R and V, and W_1 is a corner of the rectangle. Hence the line segment VP is also contained in $Y \cap \Pi$. Let $\mathbf{k}$ be the line VP produced in $Y \cap \Pi$, cutting the hyperplanes of the upper and lower faces of the cylinder in W_3 and W_4. Let W_2 be the corner of the rectangle on F that is diametrically opposite W_1 as depicted in Figure 7.1.

We can construct in Y a line $\mathbf{m}$, through V, that is orthogonal to the line $\mathbf{k}$. By the defintion of completely orthogonal planes, all lines perpendicular to $\mathbf{k}$ and not in Π must lie in Ψ. Therefore the line $\mathbf{m}$ lies in $Y \cap \Psi$ making an angle θ with $\mathbf{n}$, the normal to the tangent hyperplane to C_1 at R.

By construction, any vector lying wholly within the d-cylinder G has length $\leq W_1W_2$, so that

$$W_3W_4 = \eta \operatorname{cosec} \theta \leq W_1W_2 = \eta \operatorname{cosec} \alpha.$$

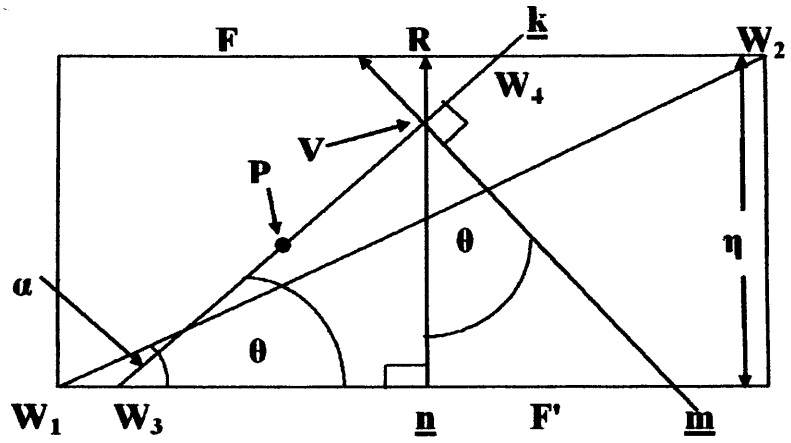

Figure 7.1:

By inequality (4.6), the distance of points of $S^*(V)$ from V is at most

$$r = 10\sqrt{\delta c_1 M},$$

so that $S^*(V)$ lies within a distance r of the line **k** in a j-dimensional plane Π. Hence $S^*(V)$ must be contained in a j-cylinder, G', with axis k, whose upper and lower faces are $(j-1)$-spheres of radius r. The j-dimensional volume of G' is therefore

$$\alpha_{j-1} r^{j-1} W_3 W_4 = \alpha_{j-1} r^{j-1} \eta \text{ cosec } \theta. \tag{7.6}$$

Suppose that the j-dimensional boundary component $S^*(V_i)$ contains l points of S, where

$$L + 1 \leq l \leq 2L \tag{7.7}$$

for some L equal to a power of two. By Lemma 3.5.4 in dimension j, the convex hull of $S^*(V)$ has j-dimensional volume

$$\text{Vol}(S^*(V)) \geq \frac{(l-j)}{j!} D(\Lambda) \geq \frac{(L-j+1)}{j!} D(\Lambda) \geq \frac{L}{(j+1)!} D(\Lambda), \tag{7.8}$$

where $|S^*(V)|$ lies in the range of (7.7).

Comparing (7.6) and (7.8), we see that

$$\sin\theta \leq \frac{(j+1)!\eta\alpha_{j-1}r^{j-1}}{D(\Lambda)L}, \tag{7.9}$$

and for acute angles we can write

$$\theta \leq \frac{\pi}{2}\sin\theta \leq \frac{\pi(j+1)!\eta\alpha_{j-1}r^{j-1}}{2D(\Lambda)L}, \tag{7.10}$$

As stated before, a j-girdle is a set of j-dimensional boundary components whose j-planes Π are all completely parallel. We want to count the number of components in the girdle for which (7.7) holds for each L equal to a power of two. Each boundary component $S^{\star}(V)$ gives rise to a set A along the surface of the sphere B. The set A has a centre, the point W where the outward normal is parallel to the line VR normal to C_1. Corresponding to the unique pair of completely orthogonal j and $(d-j)$-planes Π and Ψ through V, there are diametric planes of the sphere B, Π' parallel to Π, Ψ' parallel to Ψ, that form a unique completely orthogonal pair of planes through the origin. The distance of W from Ψ', measured along the surface of B, is $\theta c_1 M$. The distance of each point of A from W is

$$\leq \sqrt{\frac{c_0\delta M}{4}},$$

so that the distance of each point of A from the $(d-j)$-plane Ψ' is

$$\leq \theta c_1 M + \sqrt{\frac{c_0\delta M}{4}} \leq 2\max(\theta c_1 M, \theta_0 c_1 M), \tag{7.11}$$

where

$$\theta_0 = \frac{1}{c_1}\sqrt{\frac{c_0\delta}{4M}}.$$

There are two cases according to which term gives the maximum in (7.11). In both cases we consider the maximum $(d-1)$-dimensional surface region available on the surface of the d-sphere B and relate this to the minimum surface requirement for each set A on the surface of B. We note that if more than one j-dimensional boundary component in a j-girdle of the convex hull H lies on the same j-plane, then the vertices V_i, which label the boundary

components $S^*(V_i)$ must be different, so they are counted separately in this argument.

First we consider L so small that

$$\frac{\pi(j+1)!\eta\alpha_{j-1}r^{j-1}}{2D(\Lambda)L} \geq \frac{\pi}{2}\sin\theta \geq \theta \geq \theta_0 = \frac{1}{c_1}\sqrt{\frac{c_0\delta}{4M}}. \tag{7.12}$$

Then

$$\frac{\pi(j+1)!\eta\alpha_{j-1}r^{j-1}c_1M}{D(\Lambda)L} \geq 2\max(\theta c_1M, \theta_o c_1M).$$

The intersection of Ψ' with B is a $(d-j)$-dimensional sphere, B_1, with diameter $2c_1M$. The $(d-j-1)$-dimensional surface of B_1 is contained within the $(d-1)$-dimensional surface of B, and by (3.11) this is given by

$$(d-j)\alpha_{d-j}(c_1M)^{d-j-1}. \tag{7.13}$$

The set A has distance at most $2\theta c_1M$ from the $(d-j)$-plane Ψ' on the surface of B in j further perpendicular directions, and so has cross-section at most $4\theta c_1M$ in these j dimensions. Hence the search region on the surface of B has $(d-1)$-dimensional volume at most

$$(d-j)\alpha_{d-j}(c_1M)^{d-j-1}(4\theta c_1M)^j \leq (2\pi c_1M)^{d-j-1}(4\theta c_1M)^j$$

$$\leq (2\pi c_1M)^{d-j-1}\left(\frac{2\pi(j+1)!\eta\alpha_{j-1}r^{j-1}c_1M}{D(\Lambda)L}\right)^j,$$

where we have used (3.13). By (4.3), the number of such sets A is at most

$$\frac{1}{\alpha_{d-1}}\left(\sqrt{\frac{4}{c_0\delta M}}\right)^{d-1}(2\pi c_1M)^{d-j-1}\left(\frac{2\pi(j+1)!\eta\alpha_{j-1}r^{j-1}c_1M}{D(\Lambda)L}\right)^j =$$

$$\left(\frac{2^{2(d-1)+j^2}5^{j(j-1)}13^j\alpha_{j-1}^j\pi^{d-1}((j+1)!)^jc_1^{\frac{2d+j^2+j-2}{2}}}{\alpha_{d-1}c_0^{\frac{d+2j-1}{2}}(D(\Lambda)L)^j}\right)\delta^{\frac{j^2+j-d+1}{2}}M^{\frac{d+j^2-j-1}{2}}.$$

The corresponding boundary components $S^*(V)$ have at most $2L$ points. We then sum over $L = 2, 4, 8, \ldots$ to get a contribution

$$\leq \left(\frac{2^{2d+j^2}5^{j(j-1)}13^j\alpha_{j-1}^j\pi^{d-1}((j+1)!)^jc_1^{\frac{2d+j^2+j-2}{2}}}{\alpha_{d-1}c_0^{\frac{d+2j-1}{2}}(D(\Lambda))^j}\right)\delta^{\frac{j^2+j-d+1}{2}}M^{\frac{d+j^2-j-1}{2}} \tag{7.14}$$

of points to S from all the boundary components in the girdle in the cases (7.12).

For ranges of L for which (7.12) is false we have

$$\sin\theta \leq \frac{(j+1)!\eta\alpha_{j-1}r^{j-1}}{D(\Lambda)L} < \frac{2\theta_0}{\pi} = \frac{1}{\pi c_1}\sqrt{\frac{c_0\delta}{M}},$$

$$\theta \leq \frac{\pi}{2}\sin\theta < \theta_0 = \frac{1}{2c_1}\sqrt{\frac{c_0\delta}{M}},$$

$$2\max(\theta c_1 M, \theta_o c_1 M) < 2\theta_0 c_1 M = \sqrt{c_0\delta M}.$$

The sets A corresponding to the boundary components with all L for which (7.12) is false are disjoint, and they lie within a region of $(d-1)$-volume at most

$$(2\pi c_1 M)^{d-j-1}(4\theta_0 c_1 M)^j \leq (2\pi c_1 M)^{d-j-1}\left(2\sqrt{c_0\delta M}\right)^j,$$

$$= 2^{d-1}(\pi c_1)^{d-j-1}(c_0\delta)^{\frac{j}{2}}M^{\frac{2d-j-2}{2}}$$

using the same reasoning as that of the previous case.

By (4.3), the number of such sets A is at most

$$\frac{1}{\alpha_{d-1}}\left(\sqrt{\frac{4}{c_0\delta M}}\right)^{d-1} 2^{d-1}(\pi c_1)^{d-j-1}c_0^{\frac{j}{2}}\delta^{\frac{j}{2}}M^{\frac{2d-j-2}{2}},$$

$$= \left(\frac{2^{2d-2}(\pi c_1)^{d-j-1}c_0^{\frac{j+1-d}{2}}}{\alpha_{d-1}}\right)\delta^{\frac{j+1-d}{2}}M^{\frac{d-j-1}{2}}.$$

However small θ is, the integer points of $S^*(V)$ lie in a j-dimensional cube of j-volume

$$\left(20\sqrt{\delta c_1 M}\right)^j,$$

so if there are $l \geq (j+1)$ integer points in $S^*(V)$, by the minor arc case $d = j$ in Lemma 3.5.4

$$\frac{l}{(j+1)!}D(\Lambda) \leq \frac{l-j+1}{j!}D(\Lambda) \leq \left(20\sqrt{\delta c_1 M}\right)^j,$$

so that,

$$l \leq \frac{(j+1)!}{D(\Lambda)}\left(20\sqrt{\delta c_1 M}\right)^j,$$

and the boundary components $S^*(V)$ in the girdle for which (7.12) is false contribute

$$\leq \frac{(j+1)!}{D(\Lambda)}\left(20\sqrt{\delta c_1 M}\right)^j \cdot \left(\frac{2^{2d-2}(\pi c_1)^{d-j-1}c_0^{\frac{j+1-d}{2}}}{\alpha_{d-1}}\right)\delta^{\frac{j+1-d}{2}}M^{\frac{d-j-1}{2}}$$

$$= \left(\frac{(j+1)!2^{2d+2j-2}5^j\pi^{d-j-1}c_0^{\frac{j+1-d}{2}}c_1^{\frac{2d-j-2}{2}}}{\alpha_{d-1}D(\Lambda)}\right)\delta^{\frac{2j+1-d}{2}}M^{\frac{d-1}{2}} \tag{7.15}$$

integer points to $S(H)$.

We use Lemma 7.1.2 with $j = k$ to estimate the contribution of all boundary components with L small in all j-girdles given by (7.14) as

$$\left(\frac{2^{3jd+2d+2j^2}5^{j(d-1)}13^j\alpha_{j-1}^j\pi^{d-1}((j+1)!)^j c_1^{\frac{2d+jd+j-2}{2}}}{\alpha_{d-1}\alpha_j^j c_0^{\frac{d+2j-1}{2}}}\right)$$

$$\times\delta^{\frac{(d+1)(j-1)}{2}+1}M^{\frac{(d-1)(j+1)}{2}} \tag{7.16}$$

integer points, and the contribution of all boundary components with L large from all j-girdles given by (7.15) as

$$\left(\frac{(j+1)!2^{3jd+3j+2d-2}5^{jd}\pi^{d-j-1}c_0^{\frac{j+1-d}{2}}c_1^{\frac{jd+2d-2j-2}{2}}}{\alpha_{d-1}\alpha_j}\right)\delta^{\frac{(d+1)(j-1)}{2}+1}M^{\frac{(d-1)(j+1)}{2}}. \tag{7.17}$$

After some calculation we find that

$$\frac{c_1^{\frac{2d+jd+j-2}{2}}}{c_0^{\frac{d+2j-1}{2}}} \geq c_0^{\frac{j+1-d}{2}}c_1^{\frac{jd+2d-2j-2}{2}},$$

$$\frac{\alpha_{j-1}}{\alpha_j} \leq j,$$

and

$$(j(j+1)!)^j \geq \frac{(j+1)!}{\alpha_j},$$

for all $j \geq 0$, $d \geq 1$, where we have used (3.6) (3.11) and (3.12) to obtain the above inequalities. Hence we can write the sum of these two terms from (7.16) and (7.17) as

$$\leq \left(\frac{2^{3jd+2d+2j^2+j} 5^{j(d-1)} \pi^{d-1} (j(j+1)!)^j}{\alpha_{d-1}} \right) \left(\frac{c_1}{c_0} \right)^{\frac{d+2j-1}{2}} (5^j + 13^j)$$

$$\times \delta^{\frac{(d+1)(j-1)}{2}+1} (c_1 M)^{\frac{(d-1)(j+1)}{2}}$$

$$\leq \lambda_j \left(\frac{c_1}{c_0} \right)^{\frac{d+2j-1}{2}} \delta^{\frac{(d+1)(j-1)}{2}+1} (c_1 M)^{\frac{(d-1)(j+1)}{2}}$$

$$= \lambda_j \left(\frac{c_1^2}{c_0^2} \delta^{d+1} (c_1 M)^{d-1} \right)^{\frac{j-1}{2}} \left(\left(\frac{c_1}{c_0} \right)^{\frac{d+1}{2}} \delta (c_1 M)^{d-1} \right), \qquad (7.18)$$

where we have written

$$\lambda_j = \left(\frac{2^{3jd+2d+2j^2+2j} (5^j \pi)^{d-1} (9j(j+1)!)^j}{\alpha_{d-1}} \right),$$

using

$$5^j + 13^j \leq 18^j.$$

We now consider the total number of integer points contributed by the j-girdles in all boundary components with $\delta \leq \delta_0$, defined in (4.7) by

$$\delta_0 = \left(\frac{100 c_0}{13 d!} \right)^{\frac{2}{d+1}} \left(400 c_1 M^{\frac{d-1}{d+1}} \right)^{-1},$$

$$= \left(\frac{100 c_0}{20^{d+1} 13 d! c_1} \right)^{\frac{2}{d+1}} (c_1 M)^{\frac{-(d-1)}{d+1}},$$

$$= \left(\frac{c_0}{2^{2d} 5^{d-1} 13 d! c_1} \right)^{\frac{2}{d+1}} (c_1 M)^{\frac{-(d-1)}{d+1}}.$$

Hence

$$\delta^{d+1} \leq \delta_0^{d+1} = \left(\frac{c_0}{2^{2d} 5^{d-1} 13 d! c_1} \right)^2 (c_1 M)^{-(d-1)},$$

and

$$\left(\frac{c_1^2}{c_0^2}\delta^{d+1}(c_1M)^{d-1}\right)^{\frac{j-1}{2}} \leq \left(\frac{1}{2^{2d}5^{d-1}13d!}\right)^{j-1} = \mu_j,$$

say, where μ_j is a constant depending only on d and j.

In this notation, the upper bound in (7.18) for the components with $\delta \leq \delta_0$ is

$$\begin{aligned}
&\lambda_j\mu_j\left(\left(\frac{c_1}{c_0}\right)^{\frac{d+1}{2}}\delta(c_1M)^{d-1}\right) \\
&\leq \left(\frac{2^{jd+4d+2j^2+2j}(5\pi)^{d-1}(9j(j+1)!)^j}{(13d!)^{j-1}\alpha_{d-1}}\right) \\
&\quad \times \left(\left(\frac{c_1}{c_0}\right)^{\frac{d+1}{2}}\delta_0(c_1M)^{d-1}\right). \qquad (7.19)
\end{aligned}$$

Using the inequalities

$$\frac{9^j}{13^{j-1}} \leq 9, \quad j \geq 1,$$

$$\frac{j^j(j+1)!^j}{d!^{j-1}} \leq d!, \quad j \leq d-2,$$

we can write

$$\begin{aligned}
\lambda_j\mu_j &\leq \left(\frac{2^{jd+4d+2j^2+2j}(2^4)^{d-1}2^4d!}{\alpha_{d-1}}\right) \\
&\leq \frac{2^{8d+3jd+2j}d!}{\alpha_{d-1}}.
\end{aligned}$$

Now

$$\sum_{j=2}^{d-2} 2^{2j} = \frac{(2^d-8)(2^d+8)}{12} \leq 2^{2d-3},$$

and

$$\sum_{j=2}^{d-2} 2^{jd+2j^2} \leq \sum_{j=2}^{d-2} 2^{3jd} = \frac{2^{3d^2}-2^{6d}}{2^{6d}-2^{3d}} \leq 2^{3d^2-5d}.$$

Hence we estimate the contribution of integer points from all j-dimensional girdles, with $2 \leq j \leq (d-2)$, and $\delta \leq \delta_0$ as

$$N_g \leq \left(\frac{2^{3d^2-5d+8d+2d-3} d!}{\alpha_{d-1}} \right) \left(\left(\frac{c_1}{c_0} \right)^{\frac{d+1}{2}} \delta_0 (c_1 M)^{d-1} \right),$$

$$\leq \left(\frac{2^{3d^2+5d-3} d!}{\alpha_{d-1}} \right) \left(\left(\frac{c_1}{c_0} \right)^{\frac{d+1}{2}} \delta_0 (c_1 M)^{d-1} \right). \tag{7.20}$$

Next, for $\delta \leq \delta_0$, we consider the integer points contributed by the boundary components of dimension $0, 1, d-1$ and d, along with the points lying strictly inside the convex hull H. These individual upper bounds correspond to (3.31), (5.1), (5.15), (5.8) and (3.45) respectively. We have

$$N_0 \leq 36 d! (2 c_1 M)^{\frac{d(d-1)}{d+1}}$$

$$\leq 2^{d+6} d! (c_1 M)^{\frac{d(d-1)}{d+1}} \tag{7.21}$$

integer points which are vertices of the convex hull (case $j = 0$),

$$N_1 \leq \frac{2^{6d-1} 3^3 \pi^{d-1}}{\alpha_{d-1}} \left(\frac{c_1}{c_0} \right)^{\frac{d+1}{2}} \delta_0 (c_1 M)^{d-1},$$

$$\leq \frac{2^{8d+2}}{\alpha_{d-1}} \left(\frac{c_1}{c_0} \right)^{\frac{d+1}{2}} \delta_0 (c_1 M)^{d-1} \tag{7.22}$$

integer points on one-dimensional boundary component girdles (case $j = 1$).

Using the inequality

$$d \leq 2^{d-1}, \qquad d \geq 1,$$

we have

$$d! \leq 2^{\frac{d^2-d}{2}}, \tag{7.23}$$

and so there are N_{d-1}

$$\leq d!(d+1)! 2^{\frac{9d+17}{2}} \left(\frac{c_1}{c_0} \right)^{(d-1)/2} \left((c_1 M)^{\frac{d(d-1)}{d+1}} + 2 \left(\frac{c_1}{c_0} \right)^{(d-1)/2} \delta_0 (c_1 M)^{d-1} \right),$$

$$\leq d!2^{\frac{d^2+10d+17}{2}}\left(\frac{c_1}{c_0}\right)^{(d-1)/2}\left((c_1M)^{\frac{d(d-1)}{d+1}}+2\left(\frac{c_1}{c_0}\right)^{(d-1)/2}\delta_0(c_1M)^{d-1}\right),$$

$$\leq d!2^{\frac{d^2+10d+17}{2}}\left(\frac{c_1}{c_0}\right)^{(d-1)/2}\left((c_1M)^{\frac{d(d-1)}{d+1}}+\frac{2^4}{\alpha_{d-1}}\left(\frac{c_1}{c_0}\right)^{(d-1)/2}\delta_0(c_1M)^{d-1}\right), \tag{7.24}$$

integer points on $(d-1)$-dimensional boundary components (case $j=d-1$),

$$N_d \leq 2(d+1)(3\alpha_d d!)^{\frac{d}{d+1}}(2c_1M)^{\frac{d(d-1)}{d+1}}$$

$$\leq 36(d+1)!(2c_1M)^{\frac{d(d-1)}{d+1}}$$

$$\leq 2^{2d+6}d!(c_1M)^{\frac{d(d-1)}{d+1}} \tag{7.25}$$

integer points lying on d-dimensional boundary components, and

$$N' \leq 12(d+1)!\delta_0(c_1M)^{d-1}$$

$$\leq \frac{2^{d+7}d!\delta_0}{\alpha_{d-1}}(c_1M)^{d-1} \tag{7.26}$$

integer points lying strictly inside the convex hull H.

Collecting together the terms in (7.21), (7.22), (7.24), (7.25) and (7.26) we have

$$\leq d!\left(\frac{c_1}{c_0}\right)^{\frac{d-1}{2}}(c_1M)^{\frac{d(d-1)}{d+1}}\left(2^{d+6}+2^{\frac{d^2+10d+17}{2}}+2^{2d+6}\right)$$

$$+\frac{d!}{\alpha_{d-1}}\left(\frac{c_1}{c_0}\right)^{d-1}\delta_0(c_1M)^{d-1}\left(\frac{2^{8d+2}}{d!}+2^{\frac{d^2+10d+25}{2}}+2^{d+7}\right)$$

$$\leq 2^{\frac{d^2+10d+18}{2}}d!\left(\frac{c_1}{c_0}\right)^{\frac{d-1}{2}}\left((c_1M)^{\frac{d(d-1)}{d+1}}+\frac{2^4}{\alpha_{d-1}}\left(\frac{c_1}{c_0}\right)^{\frac{d-1}{2}}\delta_0(c_1M)^{d-1}\right) \tag{7.27}$$

integer points counted in N_0, N_1, N_{d-1}, N_d and N'. Combining (7.20) with the bound (7.27) for N_g, the number of points on girdles of intermediate

dimensions, we estimate the total number of integer points lying on within a distance δ_0 from the convex hull H as

$$\leq 2^{\frac{d^2+10d+18}{2}} d! \left(\frac{c_1}{c_0}\right)^{\frac{d-1}{2}} \left((c_1 M)^{\frac{d(d-1)}{d+1}} + \frac{2^{\frac{5d^2-22}{2}}}{\alpha_{d-1}} \left(\frac{c_1}{c_0}\right)^{\frac{d-1}{2}} \delta_0 (c_1 M)^{d-1} \right), \tag{7.28}$$

where we have used the result that for $d \geq 3$

$$2^{\frac{d^2+10d+26}{2}} \leq 2^{3d^2+5d-3}.$$

The bound in (7.28) is valid for a shell of thickness $\delta = \delta_0$ and consists of terms independent of δ (degree zero), and those with a factor of δ (degree one).

We cover the shell E of all extended vertex components, bounded internally by C_0 and externally by C_1, by R thinner concentric shells $E_1, \ldots, E_R$ of thickness δ_0. The distance between C_1 and C_0 along any inward normal vector to these two surfaces is 2δ. Hence we choose R to be the smallest integer with

$$R\delta_0 \geq 2\delta, \quad (R-1)\delta_0 < 2\delta,$$

so that

$$R < \frac{2\delta}{\delta_0} + 1. \tag{7.29}$$

The shell E_r consists of the points on some inward normal whose distance l, measured along the inward normal, from the hypersurface C_1 lies in the range

$$(r-1)\delta_0 \leq l \leq r\delta_0.$$

Lemma 3.3.2, with δ replaced by $r\delta_0$, ensures that each shell E_r will satisfy the Curvature Condition, so that any two-dimensional plane section curve of E_r will have radius of curvature ρ in the range

$$c_0 M \leq \rho \leq c_1 M.$$

Therefore equation (7.28) gives the uniform upper bound for the number of integer points contributed by any shell E_r

$$2^{\frac{d^2+10d+18}{2}} d! \left(\frac{c_1}{c_0}\right)^{\frac{d-1}{2}} (c_1 M)^{\frac{d(d-1)}{d+1}} + \frac{2^{3d^2+5d-2}}{\alpha_{d-1}} \left(\frac{c_1}{c_0}\right)^{d-1} \delta_0 (c_1 M)^{d-1}.$$

Now let

$$\eta = \delta_0 (c_1 M)^{\frac{d-1}{d+1}} = \left(\frac{c_0}{2^{2d} 5^{d-1} 13 d! c_1} \right)^{\frac{2}{d+1}} \leq \frac{1}{2^6}, \tag{7.30}$$

by the definition (4.7) of δ_0; we see that η is a constant and by (7.23)

$$\begin{aligned} \frac{1}{\eta} &= \left(\frac{2^{2d} 5^{d-1} 13 d! c_1}{c_0} \right)^{\frac{2}{d+1}} \\ &\leq \left(\frac{2^{2d} 2^{3d-3} 2^4 2^{\frac{d^2-d}{2}} c_1}{c_0} \right)^{\frac{2}{d+1}} \leq \left(\frac{2^{\frac{d^2+9d+2}{2}} c_1}{c_0} \right)^{\frac{2}{d+1}} \\ &\leq \left(\frac{2^{\frac{d^2+9d+8}{2}} c_1}{c_0} \right)^{\frac{2}{d+1}} \leq 2^{d+8} \left(\frac{c_1}{c_0} \right)^{\frac{2}{d+1}} \\ &\leq 2^{d+8} \frac{c_1}{c_0}. \end{aligned} \tag{7.31}$$

We note that by (7.30)

$$\delta_0 = \frac{\eta}{(c_1 M)^{\frac{d-1}{d+1}}} \leq \frac{1}{2^6 (c_1 M)^{\frac{d-1}{d+1}}}. \tag{7.32}$$

THEOREM 2. *Suppose that C is a convex hypersurface in d-dimensional Euclidean space $\mathbf{E}^d$ $(d \geq 3)$, satisfying the Curvature Condition at size M (so that C is contained in a hypersphere radius $c_1 M$). Then the total number, N, of integer points lying either on C or within a distance δ of C, is bounded by*

$$N \leq \frac{2^{3d^2+5d-7} d!}{\alpha_{d-1}} \left(\frac{c_1}{c_0} \right)^{d-1} \left((c_1 M)^{\frac{d(d-1)}{d+1}} + 2^9 \delta (c_1 M)^{d-1} \right). \tag{7.33}$$

Proof. We multiply the upper bound (7.28) by the maximum number of shells allowed by (7.29). For the degree zero terms this yields

$$\leq \left(\frac{2\delta}{\delta_0} + 1 \right) 2^{\frac{d^2+10d+18}{2}} d! \left(\frac{c_1}{c_0} \right)^{\frac{d-1}{2}} (c_1 M)^{\frac{d(d-1)}{d+1}}$$

$$\leq \frac{2^{\frac{d^2+10d+18}{2}} d!}{\eta} \left(\frac{c_1}{c_0}\right)^{\frac{d-1}{2}} \delta (c_1 M)^{d-1} + 2^{\frac{d^2+10d+18}{2}} d! \left(\frac{c_1}{c_0}\right)^{\frac{d-1}{2}} (c_1 M)^{\frac{d(d-1)}{d+1}}$$

$$\leq 2^{\frac{d^2+12d+34}{2}} d! \left(\frac{c_1}{c_0}\right)^{\frac{d+1}{2}} \delta (c_1 M)^{d-1} + 2^{\frac{d^2+10d+18}{2}} d! \left(\frac{c_1}{c_0}\right)^{\frac{d-1}{2}} (c_1 M)^{\frac{d(d-1)}{d+1}}, \tag{7.34}$$

where we have used (7.30) and (7.31).

For the degree one terms we have

$$\leq \left(\frac{2\delta}{\delta_0} + 1\right) \frac{2^{3d^2+5d-2} d!}{\alpha_{d-1}} \left(\frac{c_1}{c_0}\right)^{d-1} \delta_0 (c_1 M)^{d-1}$$

$$\leq \frac{2^{3d^2+5d-1} d!}{\alpha_{d-1}} \left(\frac{c_1}{c_0}\right)^{d-1} \delta (c_1 M)^{d-1} + \frac{2^{3d^2+5d-2} d!}{\alpha_{d-1}} \left(\frac{c_1}{c_0}\right)^{d-1} \eta (c_1 M)^{\frac{d(d-1)}{d+1}}$$

by (7.32), and as $\eta \leq 2^{-6}$, this simplifies to

$$\leq \frac{2^{3d^2+5d-1} d!}{\alpha_{d-1}} \left(\frac{c_1}{c_0}\right)^{d-1} \delta (c_1 M)^{d-1} + \frac{2^{3d^2+5d-8} d!}{\alpha_{d-1}} \left(\frac{c_1}{c_0}\right)^{d-1} (c_1 M)^{\frac{d(d-1)}{d+1}}. \tag{7.35}$$

Finally we combine the terms from (7.34) and (7.35) to estimate the total number of integer points by

$$\leq \frac{2^{3d^2+5d-7} d!}{\alpha_{d-1}} \left(\frac{c_1}{c_0}\right)^{d-1} \left((c_1 M)^{\frac{d(d-1)}{d+1}} + 2^9 \delta (c_1 M)^{d-1} \right),$$

as required. □

THEOREM 3. *Suppose that C is a convex hypersurface in d-dimensional Euclidean space $\mathbf{E}^d$ ($d \geq 3$), satisfying the Local Curvature Condition at size M (so that C is contained in a hypersphere radius $c_1 M$), with*

$$M \geq \frac{100 \delta c_1}{\kappa^2}. \tag{7.36}$$

Then N, the total number of integer points lying either on C, or within a distance δ of C, satisfies the same bound (7.33) *as in Theorem* 2.

Proof. In the proof of Theorem 2, we consider an enlarged component $S'(V)$, where all the calculations for distances between points on the outer surface C_1 take place within the reach $\mathcal{R}(V)$ of $S'(V)$, with respect to V.

By Lemma 4.2.5, the Local Curvature Condition holds at all points in $\mathcal{R}(V)$, so the calculations which establish Theorem 2 are valid under the weaker hypothesis of the Local Curvature Condition. □

It is interesting to compare the constants in Theorems 1 and 2 when $d = 3$. Theorem 1 gives

$$\leq \left(\frac{c_1}{c_0}\right)^2 2^{16} \left((c_1 M)^{\frac{3}{2}} + 2^9 \delta (c_1 M)^2\right),$$

whereas in Theorem 2 (the general case) we have

$$\leq \left(\frac{c_1}{c_0}\right)^2 2^{36} \left((c_1 M)^{\frac{3}{2}} + 2^9 \delta (c_1 M)^2\right).$$

The structure of the bounds in Theorems 1 and 2 is the same. The constants are numerically larger in Theorem 2 because Theorem 2 allows for girdles of intermediate dimension which do not occur when $d = 3$, and also because we have used sharper estimates for the volume constants α_2 and α_3.

PART II

Associated Magic Squares and a Zeta Identity

Chapter 8

Overview

This chapter introduces and defines the most common types of magic square, explaining the symmetries that motivate our results.

8.1 Brief History

The magic square [3] of order 3 or "Loh Shu square" [32] was known in China as early as the Warring States period, which lasted from 481 BC until 221 BC. An impression of the square is depicted in Figure 8.1 with the more modern matrix representation given below this in Table 8.1. It was used

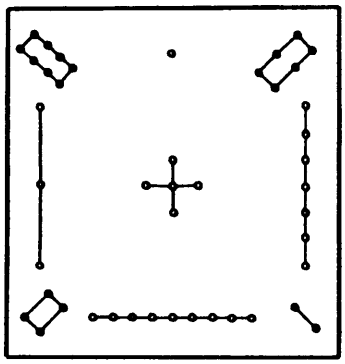

Figure 8.1: The Loh Shu square.

in China as a hopscotch to symbolise harmony and the balance of natural

forces, has the property that the rows, columns and main diagonals add up to 15, and any pair of associated elements adds up to 10; two such positions within the matrix are called *associated* if the centre of the line adjoining them is also the centre of the square. More formally, an associated magic square satisfies $(s1)$, $(s2)$ and $(s3)$ of the five symmetry conditions, defined below.

Symmetry Conditions. Let $A = (a_{i,j})$ be an $n \times n$ square matrix and c a constant. We define five symmetry conditions on A as follows:

(s1) Row and column symmetry

$$\sum_{\substack{j=1 \\ 1 \le i \le n}}^{n} a_{i,j} = c, \qquad \sum_{\substack{i=1 \\ 1 \le j \le n}}^{n} a_{i,j} = c.$$

(s2) Principal diagonals symmetry

$$\sum_{i=1}^{n} a_{i,i} = c, \qquad \sum_{i=1}^{n} a_{i,(n+1-i)} = c.$$

(s3) Associated symmetry

$$a_{i,j} + a_{(n+1-i),(n+1-j)} = \frac{2c}{n},$$

for all (i, j).

(s4) Pandiagonal symmetry

$$\sum_{\substack{i=1 \\ i+j \equiv s \pmod n}}^{n} a_{i,j} = c, \qquad \sum_{\substack{i=1 \\ i-j \equiv s \pmod n}}^{n} a_{i,j} = c.$$

for each residue class $s (\mathrm{mod} n)$.

(s5) Most-perfect symmetry

$$a_{i,j} + a_{i,j+1} + a_{i+1,j} + a_{i+1,j+1} = \frac{4c}{n}, \qquad a_{i,j} + a_{i+\frac{1}{2}n,j+\frac{1}{2}n} = \frac{2c}{n},$$

for all (i, j), where the subscripts of a are taken (mod n) using the residue classes $1, 2, \ldots, n$.

8	1	6
3	5	7
4	9	2

Table 8.1: The unique 3×3 square.

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Table 8.2: The "Melancholia" 4×4 associated magic square engraved 1514.

We note that either of conditions $(s3)$ or $(s4)$ imply condition $(s2)$.

A square in which only the rows and columns sum to c (condition $(s1)$) is called *semi-magic*. The extra condition that the two main or principal diagonals also sum to c (conditions $(s1)$ and $(s2)$) defines the standard *magic square* and if the square also has the associated property (condition $(s3)$) then we have an *associated magic square* with associated sum $2c/n$.

The smallest possible magic square is the 3×3 square and it is well known that (ignoring rotations and reflections) this square is unique. In this case, the associated property $(s3)$ is simply a result of the row, column and diagonal conditions ($(s1)$ and $(s2)$). For larger squares this is not always the case and so one has to impose the associated property $(s3)$ as an extra condition. It is also possible to impose further conditions on the sums or partial sums of elements of a square and we give a brief description of the more popular refinements.

Traditionally a magic square of size n contains the integers $0, 1, \ldots n^2 - 1$ or $1, 2, \ldots n^2$. The respective constant sums are $n(n^2-1)/2$ and $n(n^2+1)/2$. In practice the square can contain many different progressions and still satisfy the magic conditions with constant sum c.

A *pandiagonal magic square* has the usual row, column and main diagonal requirements along with the additional property that any *broken diagonal* also sums to c as defined in condition $(s4)$. That is, if we imagine that the top and bottom of the square are joined together and also that the left and right sides are joined then the square will look like a doughnut. The extra requirement $(s4)$ means that any n integers read in sequence along

1	15	24	8	17
23	7	16	5	14
20	4	13	22	6
12	21	10	19	3
9	18	2	11	25

Table 8.3: A 5 × 5 pandiagonal associated magic square.

0	14	3	13	= 4 ×	0	3	0	3	+	0	2	3	1
7	9	4	10		1	2	1	2		3	1	0	2
14	2	15	1		3	0	3	0		0	2	3	1
11	5	8	6		2	1	2	1		3	1	0	2

Table 8.4: A 4 × 4 most-perfect square and its auxiliary squares.

a diagonal line of the original array that crosses a "join" of the doughnut forms a "broken diagonal" of the original square. A magic square in which the broken and principal diagonals sum to c is called "pandiagonal". It was proved by C. Planck in 1919 that there are no traditional pandiagonal magic squares of singly-even order ($n \equiv 2 \pmod 4$).

A *most-perfect square* is defined to be a pandiagonal magic square in which any "sub-square of 4 integers" on the surface of our doughnut sum to $4c/n$; each integer is associated to the one distant from it $\frac{1}{2}n$ places in the same diagonal (i.e. their sum $= 2c/n$). It follows that there are no most-perfect squares of odd order, (apart from the trivial case when $n = 1$) and, due to the pandiagonal condition, that there are no traditional most-perfect squares of singly even order. In 1998, Ollerenshaw and Brée [35] managed to enumerate all traditional most-perfect squares of doubly-even order ($n \equiv 0 \pmod 4$). They also showed when $n \equiv 0 \pmod 4$ that condition ($s5$) implies conditions ($s1$), ($s2$) and ($s4$). In Table 8.4 the most-perfect square, A say, is split into two auxiliary squares, B and C say, so that $A = 4B + C$.

A *Latin square* of order n is an $n \times n$ array of n different symbols, each used n times, arranged in such a way, that each row or column of the array contains each symbol exactly once. In our language, a Latin square is semi-magic under formal addition of the symbols. We call a Latin square magic when both the principal diagonals also contain each symbol exactly once. Traditionally the n symbols are identified with the numbers $0, 1, \ldots, n-1$.

23	1	2	20	19
22	16	9	14	4
5	11	13	15	21
8	12	17	10	18
7	25	24	6	3

Table 8.5: A 5×5 (non-associated) magic square.

We follow this tradition.

Two Latin squares $B = (b_{i,j})$ and $C = (c_{i,j})$ are said to be orthogonal when the n^2 ordered pairs $(b_{i,j}, c_{i,j})$ are all different, so that every possible pair of symbols actually occurs as a pair $(b_{i,j}, c_{i,j})$. Euler observed [35] in 1779 that if B and C are an orthogonal pair of traditional magic Latin squares of order n, then $A = nB + C$ is a magic square with entries $0, 1, 2, \ldots, n^2 - 1$, as in Table 8.4. In this construction the auxiliary magic Latin squares B and C are called the *radix* and the *unit* respectively. The use of symmetry to construct the auxiliary squares motivates our results.

If we consider magic squares as square matrices, then the set of magic squares is closed under matrix addition, and addition preserves these symmetries. Are any symmetries preserved under matrix multiplication or inversion? It is known [13] that the set of semi-magic squares with real entries forms a ring under matrix multiplication. Thompson [40] proved in 1988 that the odd powers of a 3×3 magic square A, are themselves magic, and so satisfy conditions $(s1)$ and $(s2)$. Furthermore, if A is invertible as a matrix, then the odd negative powers of A are also magic. The corresponding result holds for a 5×5 pandiagonal magic square A, that A^k is pandiagonal magic for every odd positive integer k, if A is invertible, also for odd negative k. The 4×4 pandiagonal magic squares are not invertible, but again, the positive odd powers of the square are also pandiagonal magic. It appears to be the case that extra symmetry conditions in a square can lead to the preservation of symmetry in its odd powers. Table 8.5 is an example of a 5×5 magic square where the third power and inverse are not magic, although recently, a method has been devised by Guyker [18], [19] that generates magic squares with magic inverses for all orders n.

Table 8.6 summarises current progress with the exact enumeration of different types of traditional magic square. For most-perfect squares enumeration is known [35] and there are again 48 of order 4. For order 8 there

Order	*Semi magic*	*Magic*	*Associated*	*Pandiag.*	*Most perf.*
3	9	1	1	0	0
4	68688	880	48	48	48
5	579043051200	275305224	48544	3600	0

Table 8.6: Known enumeration results for different types of traditional magic squares.

are 368640 squares, for order 12 there are 530841600 and for order 36 there are more than 2×10^{44} squares.

8.2 Structure and Symmetry

The Pythagoreans declared that *number is the essence of all things.* Magic squares are instances of the intrinsic harmony of number.

The main body of research into magic squares has been in the areas of construction and enumeration but not in the study of their multiplicative properties. We show in the Corollary to Lemma 9.2.1 that associated magic squares of real numbers hold their symmetry to all positive odd powers and that this symmetry is also passed onto their inverses (if they exist) and subsequent negative odd powers. These results appear to be new.

I thank Professor Jim Wiegold for the advice "always let the symmetry work for you". Construction techniques for singly-even associated magic squares are less symmetric than those for odd and doubly-even squares. No non-singular associated magic square of doubly-even order is known. Henceforth we consider odd squares, which are non-singular in general.

Thompson [40] observed that a magic square A of order n with row-sum c can be written as

$$A = A' + \frac{c}{n}E, \tag{8.1}$$

where E is the $n \times n$ matrix with all entries equal to 1 and A' (the *kernel square*) is a magic square with constant sum 0. From a multiplicative perspective this means that $A'E = EA' = 0_n$. Hence

$$A^k = (A')^k + E^k = (A')^k + n^{k-1}E. \tag{8.2}$$

−12	2	11	−5	4
10	−6	3	−8	1
7	−9	0	9	−7
−1	8	−3	6	−10
−4	5	−11	−2	12

$= 5 \times$

−2	0	2	−1	1
2	−1	1	−2	0
1	−2	0	2	−1
0	2	−1	1	−2
−1	1	−2	0	2

$+$

−2	2	1	0	−1
0	−1	−2	2	1
2	1	0	−1	−2
−1	−2	2	1	0
1	0	−1	−2	2

Table 8.7: The auxiliary kernel squares of a 5×5 associated pandiagonal magic square.

For $n = 2m + 1$, the traditional kernel square A' will contain the integers $-(2m^2 + 2m), \ldots, 0, \ldots, 2m^2 + 2m - 1, 2m^2 + 2m$. Using the idea of Euler's auxiliary Latin squares, the traditional kernel square A' can then be expressed as a sum of two auxiliary orthogonal traditional squares B and C such that

$$A' = nB + C, \tag{8.3}$$

with B and C each constructed using the integers

$$-m, -(m-1), \ldots, 0, 1, \ldots, (m-1), m.$$

If the original square A is associated, then so is the kernel square A', and also the auxiliary squares B and C.

We look for symmetry between the two auxiliary squares (to try and simplify future calculations). For example, consider the associated pandiagonal 5×5 magic square depicted in Table 8.3. The square has strong symmetry and the two auxiliary kernel squares, B and C, (depicted in Table 8.7) are closely related with $C = B^T$. The square B has a "knight's move" structure, repeating at "one across and two down". The effects of multiplication on this symmetry are not so simple. One possible basis matrix for the vector space of all such squares is given in Table 8.8. As the powers of this basis matrix increase through $1, 2, 3, 4, 5$, the matrix structure changes from "knight's move" to "right-left diagonal", to "reversed knight's move", to "left-right diagonal" and finally back to the original "knight's move" on the fifth power. Although

0	0	0	−1	1
0	−1	1	0	0
1	0	0	0	−1
0	0	−1	1	0
−1	1	0	0	0

Table 8.8: A 5 × 5 kernel basis matrix (knight's move).

$$\frac{1}{5.65.19.29}\begin{array}{|c|c|c|c|c|}\hline -5689 & 8351 & -1334 & 2176 & -749 \\ \hline -1009 & 2501 & -8874 & 9911 & 226 \\ \hline 6726 & 1786 & 551 & -684 & -5624 \\ \hline 876 & -8809 & 9976 & -1399 & 2111 \\ \hline 1851 & -1074 & 2436 & -7249 & 6791 \\ \hline \end{array}$$

Table 8.9: The inverse pandiagonal associated magic square of Table 8.3.

this process is easily understood by looking at permutations of the rows of I, the different structures will add complexity to any model describing powers of this matrix. The determinant of the matrix is $5^3.65.19.29$ and the inverse is shown below in Table 8.9. As with the original square, the inverse kernel square can be expressed as the sum of two auxiliary kernel squares.

Analysis of permutations of the basis vectors $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ showed that any basis matrix of order n with a knight's move structure, be it elongated or otherwise, follows a succession of structural changes as it passes through increasing powers of $1, \ldots, n$.

The simplest type of basis matrix for considering matrix powers has a diagonal structure which means that the magic squares created with such a basis cannot be pandiagonal. They can however be associated, and as the unique 3×3 square is also an associated square, the conclusion was to create a general $n \times n$ (with n odd) associated magic square from these diagonal basis matrices. A 5×5 example is given in Table 8.10 (determinant $2^6.3^2.5^3.60$) and the simplicity of the inverse square (depicted in Table 8.11) is quite striking.

10	23	6	19	2
3	11	24	7	15
16	4	12	20	8
9	17	0	13	21
22	5	18	1	14

$$= 5 \times \begin{array}{|c|c|c|c|c|}\hline 0 & 2 & -1 & 1 & -2 \\ \hline -2 & 0 & 2 & -1 & 1 \\ \hline 1 & -2 & 0 & 2 & -1 \\ \hline -1 & 1 & -2 & 0 & 2 \\ \hline 2 & -1 & 1 & -2 & 0 \\ \hline \end{array} + \begin{array}{|c|c|c|c|c|}\hline -2 & 1 & -1 & 2 & 0 \\ \hline 1 & -1 & 2 & 0 & -2 \\ \hline -1 & 2 & 0 & -2 & 1 \\ \hline 2 & 0 & -2 & 1 & -1 \\ \hline 0 & -2 & 1 & -1 & 2 \\ \hline \end{array} + 12E_5$$

Table 8.10: A 5×5 associated magic square constructed from diagonal basis matrices.

$$\frac{1}{2.5.60} \begin{array}{|c|c|c|c|c|}\hline 7 & -23 & 2 & -3 & 27 \\ \hline 27 & 2 & -28 & 2 & 7 \\ \hline 2 & 22 & 2 & -18 & 2 \\ \hline -3 & 2 & 32 & 2 & -23 \\ \hline -23 & 7 & 2 & 27 & -3 \\ \hline \end{array} =$$

$$\frac{1}{2.60}\left(5 \times \begin{array}{|c|c|c|c|c|}\hline 0 & -1 & 0 & 0 & 1 \\ \hline 1 & 0 & -1 & 0 & 0 \\ \hline 0 & 1 & 0 & -1 & 0 \\ \hline 0 & 0 & 1 & 0 & -1 \\ \hline -1 & 0 & 0 & 1 & 0 \\ \hline \end{array} + \begin{array}{|c|c|c|c|c|}\hline 1 & 0 & 0 & -1 & 0 \\ \hline 0 & 0 & -1 & 0 & 1 \\ \hline 0 & -1 & 0 & 1 & 0 \\ \hline -1 & 0 & 1 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 & -1 \\ \hline \end{array} \right)$$

$$+ \frac{1}{5.60} E_5$$

Table 8.11: The inverse associated magic square of Table 8.10.

Chapter 9

Matrix Algebra

In this chapter we translate the properties of general and diagonally constructed associated magic squares into matrix algebra. We will revert to standard matrix notation and will refer to an associated magic square as an AM square for short.

9.1 Vector Space Fundamentals.

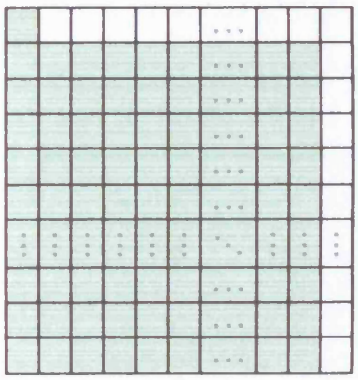

Table 9.1: Semi-magic square vector space dimension $= n^2 - 2n + 2$.

We begin with a brief re-cap of known vector spaces dimensions of magic squares [36] of real numbers. It is easily shown that the dimension of the

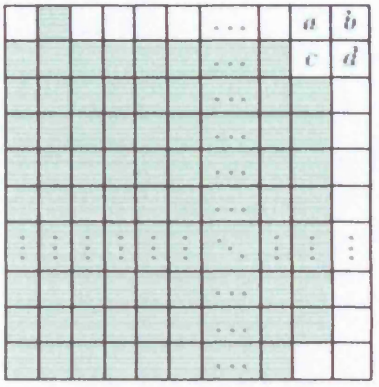

Table 9.2: Magic square vector space dimension $= n^2 - 2n$.

vector space of real semi-magic squares of order n is $n^2 - 2n + 2$ and one possible basis is depicted in Table 9.1. In the table, once the $n^2 - 2n + 2$ grey cells are chosen, then the remaining white cells are determined.

For the vector space of real magic squares of order n, it was proved by Chernick [9] in 1938 that this has dimension $n^2 - 2n$. Again we give an example of one possible basis in Table 9.2. Here the grey cells determine the white cells at which point the equations pertaining to the four remaining cells a, b, c, d can be solved.

As expected, the increased symmetry of the AM squares of order n reduces the size of the vector space and in Tables 9.3 and 9.4 we demonstrate that an upper bound for the dimension of this space is given by

$$\frac{n^2 - 2n + 3}{2}, \tag{9.1}$$

when n is odd, and

$$\frac{n^2 - 2n + 2}{2}, \tag{9.2}$$

when n is even. It is interesting to note that for $n = 3$, the unique magic square has to be associated, and that the dimension of the basis is three [40] which agrees with the upper bound in (9.1). When $n = 5$, the vector space of real pandiagonal magic squares is known to be of dimension 9 [40], which is the same as the upper bound for AM squares in (9.1).

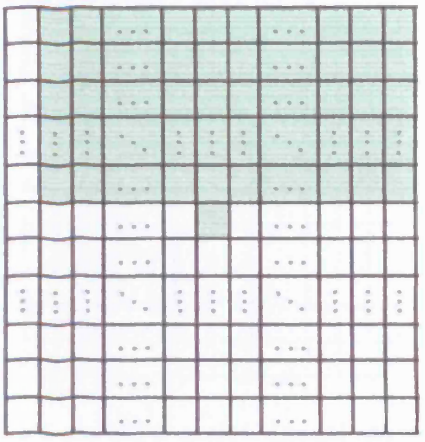

Table 9.3: Upper bound for AM square (odd) vector space dimension = $(n^2 - 2n + 3)/2$.

We now translate the properties of AM squares into matrix algebra in a more rigorous fashion.

Definition. First we define the $n \times n$ permutation matrices. Let $\underline{e}_1, \cdots, \underline{e}_n$ be the unit vectors $(1, 0, \cdots), (0, 1, 0, \cdots), \cdots, (0, \cdots, 0, 1)$ written as rows. A permutation of the n rows $\underline{m}_1, \cdots, \underline{m}_n$ of an $n \times n$ matrix M can be accomplished by the product $P_\sigma M$, where P_σ is the matrix with rows $\underline{e}_{\sigma 1}, \cdots, \underline{e}_{\sigma n}$. Similarly MP_σ has columns $\underline{k}_{\tau 1}, \cdots, \underline{k}_{\tau n}$ where $\underline{k}_1, \cdots, \underline{k}_n$ are the columns of M, and τ is the permutation inverse to σ. In particular let J be the matrix with rows $\underline{e}_n, \underline{e}_{n-1}, \cdots, \underline{e}_1$, and let K be the matrix with rows $\underline{e}_2, \cdots, \underline{e}_n, \underline{e}_1$. In the 3×3 case they are

$$J = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, K = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

The matrices J and K under multiplication generate the dihedral group D_{2n}. The product JMJ^{-1} has the original entry in row $n+1-i$, column $n+1-j$, where $J^{-1} = J$. Let E be defined as in the previous chapter, so that E is the $n \times n$ matrix with every entry 1. We define any matrix that can be expressed as a linear combination of products of powers of J, K and E to be *diagonally expressible.*

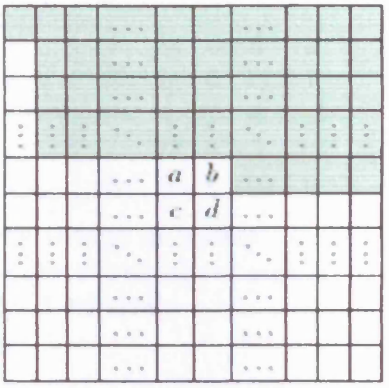

Table 9.4: Upper bound for AM square (even) vector space dimension = $(n^2 - 2n + 2)/2$.

We call an $n \times n$ matrix M semi-magic of *weight* z if M and its transpose M^T satisfy

$$ME = nzE = M^T E. \tag{9.3}$$

If M is traditional then the weight z is equal to either $(n^2-1)/2$ or $(n^2+1)/2$.

The condition (9.3) says that the rows and columns sum to nz. The permutation matrices P_σ are semi-magic of weight $1/n$. The AM squares of the title (type A for short) are the matrices M which satisfy (9.3) and also

$$M + JMJ = 2zE, \tag{9.4}$$

which says that the sum of the two associated elements is always $2z$, so the main diagonals also sum to nz. If M satisfies (9.3) and

$$JMJ = M, \tag{9.5}$$

then we say that M is a balanced semi-magic square (type B for short). These conditions are linear, so the type A squares form a vector space $\mathcal{V}$, which contains the transpose M^T for every M in $\mathcal{V}$. The matrix E is a basis matrix of $\mathcal{V}$, and $M - zE$ is a matrix in $\mathcal{V}$ with weight zero. Similarly the type B squares form a vector space $\mathcal{W}$, and for $n = 3$ and $n = 5$ we give the non-trivial examples

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 2 & 2 \\ 3 & 2 & 1 \end{bmatrix},$$

and

$$\begin{bmatrix} 9 & 13 & 8 & 2 & 3 \\ 12 & 5 & 6 & 11 & 1 \\ 10 & 4 & 7 & 4 & 10 \\ 1 & 11 & 6 & 5 & 12 \\ 3 & 2 & 8 & 13 & 9 \end{bmatrix}.$$

We note that although a type B square can never be a traditional magic square, the 5×5 example shown above satisfies the principal diagonals criterion as well the type B criteria.

9.2 Multiplication and Constructions

LEMMA 9.2.1.

(1) If M and N are semi-magic with weights z and w, then MN is semi-magic with weight nzw.

(2) If M and N are both type A, then MN is type B.

(3) If M is type A and N is type B, then MN and NM are type A.

(4) If M is type B and N is type B, then MN and NM are type B.

(5) If M is semi-magic and invertible, then M^{-1} is semi-magic with weight $1/n^2z$.

(6) If M is type B and invertible, then M^{-1} is also type B.

(7) If M is type A and invertible, then M^{-1} is type A with weight $1/n^2z$.

COROLLARY.

(i) If M is type A then M^t is type A for all positive odd t and type B for all positive even t . If M is also non-singular then the positive condition can be removed from the above statement.

(ii) If M is type B then M^t is type B for all positive t. If M is also non-singular then the result holds for all t.

Proof. If M and N are both semi-magic with weights z and w, then

$$MNE = MnwE = n^2zwE = N^TM^TE = (MN)^TE,$$

so MN is semi-magic with weight nzw.

If M and N are both type A, then

$$JMNJ = (JMJ)(JNJ) = (2zE - M)(2wE - N)$$

$$= 4zwE^2 - 2zEN - 2wME + MN$$

$$= 4nzwE - 2znwE - 2wnzE + MN = MN,$$

so MN is type B.

If M is type A and N is type B, then

$$JMNJ = (JMJ)(JNJ) = (2zE - M)N$$

$$= 2zEN - MN = 2nzwE - MN,$$

so MN is type A.

If M is type B and N is type B, then

$$JMNJ = (JM(JJ)NJ) = (JMJ)(JNJ) = MN,$$

so MN is type B.

If M is semi-magic and invertible, then from (9.3)

$$E = nzM^{-1}E,$$

and

$$E = nz(M^T)^{-1}E = nz(M^{-1})^TE,$$

so M^{-1} is semi-magic with weight $1/n^2z$.

If M is type B, then by (9.5)

$$M^{-1} = J^{-1}M^{-1}J^{-1} = JM^{-1}J,$$

and so M^{-1} is also type B.

If M is type A, then we calculate

$$(2zE - JMJ)\left(\frac{2E}{n^2z} - JM^{-1}J\right)$$

$$= \frac{4E^2}{n^2} - 2zEJM^{-1}J - \frac{2}{n^2z}JMJE + (JMJ)(JM^{-1}J)$$

$$= \frac{4E}{n} - 2zEM^{-1}J - \frac{2}{n^2z}JME + JMM^{-1}J$$

$$= \frac{4E}{n} - 2z\frac{n}{n^2z}EJ - \frac{2}{n^2z}JnzE + J^2,$$

so

$$\frac{4E}{n} - \frac{2E}{n} - \frac{2E}{n} + I = I.$$

The first factor $2zE - JMJ$ is just M by (9.4), so

$$M^{-1} = \frac{2E}{n^2z} - JM^{-1}J,$$

and hence

$$M^{-1} \in \mathcal{V}.$$

If M is type A then by statements (2) and (3) of the Lemma, M^2 is type B, M^3 is type A. We inductively assume that M^t is type A for $t = 2k + 1$, multiply by M^2, and apply statement (3) of the Lemma to complete the proof for positive odd powers t.

If M is type A then by statement (3) of the Lemma, M^2 is type B and by statement (4) of the Lemma $M^2M^2 = M^4$ is also type B. We inductively assume that M^t is type B for $t = 2k$, multiply by M^2, and again apply statement (4) of the Lemma to complete the proof for positive even powers t.

The proofs in the non-singular cases are similar and the second statement in the Corollary also follows from statement (4) of the Lemma. □

Remark. The identity matrix I_n is of type B and the $n \times n$ matrix with zero entries 0_n is simultaneously of types A and B. Hence the Corollary implies that the set of all $n \times n$ type A and type B squares is closed under multiplication and addition and so forms a ring, $\mathcal{R}(A, B)$, containing the subring $\mathcal{R}(B)$, of all $n \times n$ type B squares. This raises interesting questions such as "if M is type B then does the solution to the matrix equation

$$M = N^2$$

exist, and if so must N be of type A?" If this is the case then we can think of the ring $\mathcal{R}(A, B)$ as being a "quadratic extension" to the ring $\mathcal{R}(B)$.

From a group theory perspective, the Corollary implies that the set of all non-singular type A and B squares over a field $\mathbf{F}$ forms a group, $G(A,B)$, under multiplication, containing the subgroup, $G(B)$, of all $n \times n$ non-singular type B squares. Both groups are subgroups of $GL(n,\mathbf{F})$.

How do we construct squares of types A and B? If M is semi-magic, then so is $N = M - JMJ$ and

$$N + JNJ = M - JMJ + JMJ - M,$$

so N satisfies (9.4) with $z = 0$. The permutation matrices are semi-magic, and

$$JK^rJ = K^{-r}. \tag{9.6}$$

so

$$K^r - JK^rJ = K^r - K^{-r} \tag{9.7}$$

is a matrix in $\mathcal{V}$ of weight zero, and

$$K^r + JK^rJ = K^r + K^{-r} \tag{9.8}$$

is a matrix in $\mathcal{W}$ of weight $2/n$.

We now define the basis matrices, that along with J and E, span the vector spaces of diagonally expressible type A and B squares.

Definition. For $n = 2m+1$ and $r \in \mathbf{Z}$ let K^r be the permutation matrices of order n and let

$$A_r = K^{2r-1} - K^{-(2r-1)}, \tag{9.9}$$

and

$$B_r = K^{2r} + K^{-2r}. \tag{9.10}$$

Then

$$JA_rJ = -A_r \in \mathcal{V} \tag{9.11}$$

with weight zero and

$$JB_rJ = B_r \in \mathcal{W} \tag{9.12}$$

with weight $2/n$.

We note that $A_rE = EA_r = 0_n$ and $EB_r = B_rE = 2E$.

Under the above definition, the following identities hold.

$$A_{-r} = -A_{r+1} \tag{9.13}$$

$$A_{m+r} = -A_{m+2-r} \tag{9.14}$$

$$A_{m+1} = 0_n \tag{9.15}$$

$$A_r A_s = B_{r+s-1} - B_{r-s} \tag{9.16}$$

$$A_r B_s = A_{r+s} + A_{r-s} \tag{9.17}$$

$$B_{-r} = B_r \tag{9.18}$$

$$B_{m+r} = B_{m+1-r} \tag{9.19}$$

$$B_0 = 2I \tag{9.20}$$

$$B_r B_s = B_{r+s} + B_{r-s} \tag{9.21}$$

LEMMA 9.2.2. *For natural number m let $n = 2m + 1$ be odd. Then:*

(1) The n matrices $E, A_1, \ldots, A_m, JA_1, \ldots, JA_m$ span the vector subspace $\mathcal{V}' \subseteqq \mathcal{V}$ of diagonally expressible type A squares.

(2) The n matrices $E, B_1, \ldots, B_m, JB_1, \ldots, JB_m$ span the vector subspace $\mathcal{W}' \subseteqq \mathcal{W}$ of diagonally expressible type B squares.

Proof. Let M and N be diagonally expressible squares of type A and B with weights z and w respectively. Let

$$M' = M - zE, \qquad N' = N - wE,$$

so that M' and N' are diagonally expressible squares of type A and B respectively, both with weight 0. That is, M' and N' are the respective kernel squares of M and N.

Using Euler's method we write

$$M' = nM_1 + M_2, \qquad N' = nN_1 + N_2,$$

where M_1, M_2 are the diagonally expressible auxiliary type A Latin squares of M' and N_1, N_2 are the diagonally expressible auxiliary type B Latin squares of N'.

One of the squares M_1, M_2 will be expressible as a linear combination of the A_r matrices and the other as a linear combination of the JA_r matrices. For n odd, the auxiliary squares M_1 and M_2 are orthogonal (in the Latin sense) and so their individual weights must be zero. The type A matrices A_r and JA_r all have weight zero but as the principal diagonal matrices I and J are "self-associated", they do not feature in either linear combination as they are only of type A if all entries are also zero. Hence $\{E, A_1, \ldots, A_m, JA_1, \ldots, JA_m\}$ span the vector subspace $\mathcal{V}' \subseteqq \mathcal{V}$ of diagonally expressible type A magic squares.

For N_1, N_2 we use a similar argument with respect to orthogonality and so N_1 and N_2 both have weight zero even though the matrices B_r and JB_r all have weight $2/n$. The only difference here is that the matrices I and J are both of type B and so can occur in the linear combination expressions for N_1 and N_2. However,

$$E - \sum_{r=1}^{m} B_r = I,$$

and

$$E - \sum_{r=1}^{m} JB_r = J,$$

and so this eventuality is covered . Therefore $\{E, B_1, \ldots, B_m, JB_1, \ldots, JB_m\}$ span the vector subspace $\mathcal{W}' \subseteqq \mathcal{W}$ of diagonally expressible type B squares. □

9.3 Two and Three Parameter Families

LEMMA 9.3.1. *For natural number m let $n = 2m + 1$ and let the three parameter family of type A squares be defined such that*

$$M(z, y, x) = (zI - yJ) \sum_{r=1}^{m} (m + 1 - r)A_r + (m(z + y) + x)E. \qquad (9.22)$$

Then

$$M^{-1}(z, y, x) = \frac{(zI - yJ)}{n(z^2 - y^2)} A_0 + \frac{E}{n^2(m(z + y) + x)}.$$

COROLLARY. *For some positive integer $t \geq 0$ we have*

$$M^{-t}(z,y,x) =$$

$$\frac{(zI-yJ)^{t(mod 2)}(z^2-y^2)^{[\frac{t}{2}]}}{n^t(z^2-y^2)^t}A_0^t + \frac{E}{n^{t+1}(m(z+y)+x)^t}, \tag{9.23}$$

and

$$M^t(z,y,x) =$$

$$(zI-yJ)^{t(mod 2)}(z^2-y^2)^{[\frac{t}{2}]}\left(\sum_{r=1}^{m}(m+1-r)A_r\right)^t + n^{t-1}(m(z+y)+x)^tE. \tag{9.24}$$

We note that

$$A_0^{2t} = (-1)^t\binom{2t}{t}I + \sum_{r=1}^{t}(-1)^{t+r}\binom{2t}{t+r}B_r, \tag{9.25}$$

and

$$A_0^{2t+1} = \sum_{r=1}^{t+1}(-1)^{t+r}\binom{2t+1}{t+r}A_r. \tag{9.26}$$

Proof. A_rE vanishes so that

$$MM^{-1} = \frac{1}{n}\sum_{r=1}^{m}(m+1-r)A_rA_0 + \frac{E}{n}$$

$$= \frac{1}{n}\left(\sum_{r=1}^{m}(m+1-r)(B_{r-1}-B_r) + E\right)$$

by (9.16)

$$= \frac{1}{n}\left(mB_0 - \sum_{r=1}^{m}B_r + E\right) = \frac{1}{n}(2mI - (E-I) + E)$$

$$= \frac{(2m+1)}{n}I = I.$$

To see the Corollary, we have

$$(zI-yJ)A_r(zI-yJ) = (z^2-y^2)A_r,$$

from which equation (9.23) follows. Multiplying (9.23) by (9.24) then gives

$$M^t M^{-t} = \frac{1}{n^t}\left(\left(\sum_{r=1}^{m}(m+1-r)A_rA_0\right)^t + n^{t-1}E\right)$$

$$= \frac{1}{n^t}\left((nI-E)^t + n^{t-1}E\right)$$

$$= \frac{1}{n^t}\left(n^{t-1}(nI-E) + n^{t-1}E\right) = I,$$

as required.

This highlights the natural representation of $M^0(z,y,x)$ as

$$M^0(z,y,x) = \left(I - \frac{1}{n}E\right) + \frac{1}{n}E. \tag{9.27}$$

Hence, like its non-zero powers, $M^0(z,y,x)$ can be thought of as the sum of two auxiliary Latin type B squares, one of which has weight zero and the other 1/n.

To obtain the identities (9.25) and (9.26) we make repeated use of (9.16), (9.17) and (9.21). □

For $x,y,z \in \mathbb{N}$, the matrix $M(z,y,x)$ contains an arrangement of the integers

$$\begin{array}{ccccc} x & x+y & x+2y & \dots & x+2my \\ x+z & x+y+z & x+2y+z & \dots & x+2my+z \\ x+2z & x+y+2z & x+2y+2z & \dots & x+2my+2z \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x+2mz & x+y+2mz & x+2y+2mz & \dots & x+2my+2mz \end{array}$$

Hence to create the traditional type A square we set $x=1, y=1$ and $z=n$ in (9.22), and this ensures that the associated magic square contains the integers $1,2,\dots,n^2$. If we set x to zero then our model reduces to the two parameter family of type A matrices.

$$M(z,y) = (zI - yJ)\sum_{r=1}^{m}(m+1-r)A_r + m(z+y)E. \tag{9.28}$$

As a worked example, if $n = 5$, $z = 5$ and $y = 1$ then we have

$$M(5,1) = 10A_1 - 2JA_1 + 5A_2 - JA_2 + 12E$$

$$= \begin{bmatrix} 0 & 10 & 0 & 0 & -10 \\ -10 & 0 & 10 & 0 & 0 \\ 0 & -10 & 0 & 10 & 0 \\ 0 & 0 & -10 & 0 & 10 \\ 10 & 0 & 0 & -10 & 0 \end{bmatrix} - \begin{bmatrix} 2 & 0 & 0 & -2 & 0 \\ 0 & 0 & -2 & 0 & 2 \\ 0 & -2 & 0 & 2 & 0 \\ -1 & 0 & 2 & 0 & 0 \\ 0 & 2 & 0 & 0 & -2 \end{bmatrix}$$

$$+ \begin{bmatrix} 0 & 0 & -5 & 5 & 0 \\ 0 & 0 & 0 & -5 & 5 \\ 5 & 0 & 0 & 0 & -5 \\ -5 & 5 & 0 & 0 & 0 \\ 0 & -5 & 5 & 0 & 0 \end{bmatrix}$$

$$- \begin{bmatrix} 0 & -1 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & -1 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 12 & 12 & 12 & 12 & 12 \\ 12 & 12 & 12 & 12 & 12 \\ 12 & 12 & 12 & 12 & 12 \\ 12 & 12 & 12 & 12 & 12 \\ 12 & 12 & 12 & 12 & 12 \end{bmatrix}$$

$$= \begin{bmatrix} 10 & 23 & 6 & 19 & 2 \\ 3 & 11 & 24 & 7 & 15 \\ 16 & 4 & 12 & 20 & 8 \\ 9 & 17 & 0 & 13 & 21 \\ 12 & 5 & 18 & 1 & 14 \end{bmatrix},$$

and this is the 5×5 associated magic square originally depicted in Table 8.10 of chapter 1.

Due to the construction of the square $M(z, y)$, the auxiliary type A Latin squares are just reflections of each other and there is also symmetry between the index of the matrices A_r, JA_r and their respective coefficients $z(m+1-r)$ and $-y(m+1-r)$. It is this symmetry which leads to such a simple inverse matrix structure. The traditional 5×5 example is given in Table 8.11. Ignoring reflections and rotations the square, $M(n, 1)$, is unique for any given odd order $n = 2m + 1$. However, for any given order, it is interesting to enumerate the class of diagonally expressible traditional type A squares.

LEMMA 9.3.2. *For $m \in \mathbb{N}$, let D_n be the total number of diagonally expressible traditional type A squares of odd order $n = 2m + 1$. Then*

$$D_n = (2^{m-1}m!)^2. \tag{9.29}$$

Proof. Removing the weight zE from each type A squares does not affect this number and so we need only consider the number of pairs of orthogonal auxiliary Latin kernel squares M_1 and M_2. Let

$$M_1 = \sum_{r=1}^{m} \lambda_r A_r,$$

and

$$M_2 = \sum_{s=1}^{m} \mu_s J A_s,$$

Ignoring signs, the set of coefficients $\{\lambda_1, \ldots, \lambda_m\}$ must be a permutation of the integers $1, 2, \ldots, m$ and so this gives $m!$ possible matrices. For each choice of coefficient there is also the option of sign and so this brings the total number of possibilities for M_1 up to $2^m m!$. Similar counting applies for the Latin square M_2 and so the total number of ways of choosing the diagonal coefficients for M_1 and M_2 is $(2^m m!)^2$. Finally we must choose which of M_1, M_2 is the unitary matrix and which is the radix matrix (That is which one to multiply by n). This multiplies the total number of choices by 2 and so the total number of diagonally expressible traditional type A kernel squares is

$$2(2^m m!)^2. \tag{9.30}$$

This figure includes all rotations and reflections of any given construction. There are two reflections across the principal diagonals, two further reflections across either the central row or column and three rotations (90°, 180° and 270°). Therefore, in total, for any given matrix there exist seven other rotational and reflectional matrices. Hence if we choose to ignore rotations and reflections in our enumeration of such type A squares then we must divide the total in (9.30) by 8. This reduces the total number of diagonally expressible traditional type A squares of odd order $n = 2m + 1$ to

$$(2^{m-1} m!)^2.$$

□

When $n = 3, 5, 7, 9, 11$ and 13 we get at most $1, 4^2, 24^2, 192^2, 1920^2$, and 23040^2 diagonally expressible traditional type A squares respectively. For $n = 5$, the diagonally expressible type A squares account for only $\frac{1}{3034}$ of the

total number of traditional 5×5 type A squares, and this fraction decreases rapidly with increasing n.

The result (9.29) in Lemma 9.3.2, however, also occurs in Ollerenshaw and Brée's enumeration of most-perfect pandiagonal magic squares of order $q = 2r$, say, where r is an even natural number.

The method employed by Ollerenshaw and Brée relies on a one-to-one correspondence between the most-perfect squares and the "reversible squares" (not defined here). They showed that the reversible squares of even order can be grouped into N_q sets in which all squares are mutually accessible from each other by legitimate transformations. The number of elements in each set, D_q, is given by

$$D_q = 2^{q-2}\left(\left(\frac{q}{2}\right)!\right)^2 = (2^{r-1}r!)^2,$$

and when $r = m$ we have $D_q = D_n$. Hence when $r = m$ the total number of most perfect squares is given by the product $D_q N_q = D_n N_{n-1}$.

Returning now to the type A squares of odd order we see that there exist similarities in potential enumeration methods. We know that every traditional type A square of odd order $n = 2m + 1$ can be written as the sum of two orthogonal associated auxiliary squares, and that each auxiliary square can be written as a linear combination of m basis squares, say. For each unique pair of orthogonal associated auxiliary squares there exist D_n possibilities for assigning the coefficients to the basis squares. This in turn gives rise to D_n distinct type A squares. Let T_n be the total number of distinct pairs of $n \times n$ orthogonal associated auxiliary squares. Then the total number of $n \times n$ traditional type A squares is given simply by $D_n T_n$.

The difficult part of this argument, as with N_q in [35], is to calculate T_n. In the basic magic square case (no associated condition as in Table 8.5) the auxiliary squares are not always magic or Latin themselves. Whether this lack of symmetry can also occur in the auxiliary squares of a traditional type A square is one question whose answer might simplify future calculations for T_n.

A final word on most-perfect (pandiagonal) magic squares concerns preservation of symmetry under matrix multiplication. Of the most-perfect squares studied so far it appears to be the case, that as with the type A squares, the symmetry is preserved to odd powers. It also appears to be the case that most-perfect squares are singular.

Chapter 10

Explicit Calculations

This chapter develops the mathematical theory required to clearly understand how the entries of $M^t(z,y)$ vary with respect to t.

10.1 Diagonal Coefficients

The expressions (9.22) for $M(z,y,x)$ and (9.28) for $M(z,y)$ are identical apart from the inclusion of an x term in the coefficient of E. For simplicity we now restrict our calculations to the two parameter family $M(z,y)$ and introduce some notation to simplify the expression $M^t(z,y)$. Let

$$f_s = \frac{1}{2s+1}\binom{m+s}{2s}, \quad s \geq 0, \tag{10.1}$$

$$V_r = \sum_{q=1}^{m-r} \binom{m+r+1-q}{2r+1} A_q, \tag{10.2}$$

and

$$W_r = \sum_{q=1}^{m-r} \binom{m+r-q}{2r} B_q, \tag{10.3}$$

where $r \geq 0$. Then $M^t(z,y)$ can be written in the form:

$$(zI - yJ)^{t(mod 2)}(z^2 - y^2)^{\left[\frac{t}{2}\right]} V_0^t + n^{t-1}(m(z+y)+x)^t E, \tag{10.4}$$

and we call

$$V_0^t = \left(\sum_{q=1}^{m} (m+1-q) A_q \right)^t ,$$

the *fundamental matrix* of $M^t(z,y)$. When $t = 2k+1$ in (9.28), then using (9.16) and (9.17) we have

$$\left(\sum_{r=1}^{m} (m+1-q) A_q \right)^{2k+1} = V_0^{2k+1} = \sum_{q=1}^{m} a_q^{(2k+1)} A_q, \tag{10.5}$$

and when $t = 2k$ is even we use (9.16) and (9.21) to obtain

$$\left(\sum_{q=1}^{m} (m+1-q) A_q \right)^{2k} = V_0^{2k} = \sum_{q=0}^{m} a_q^{(2k)} B_q. \tag{10.6}$$

Hence, when t is odd, the fundamental matrix of $M^t(z,y)$ can be written as a linear combination of the diagonal type A matrices, $A_1, A_2, \ldots, A_m$, each of weight zero, and when t is even, the fundamental matrix of $M^t(z,y)$ can be written as a linear combination of the diagonal type B matrices, $B_0, B_1, B_2, \ldots, B_m$, each of weight $2/n$.

We define $a_q^{(2k+1)}$ to be the coefficient of the diagonal type A matrix A_q in the expression (10.5) for $M^{2k}(z,y)$ and $a_q^{(2k)}$ to be the coefficient of the diagonal type B matrix B_q in the expression (10.6) for $M^{2k}(z,y)$. We now state a result from [15].

PROPOSITION 10.1.1. *Let $\lambda, \mu, \nu, \epsilon$ be integers such that $\lambda, \mu \geq 0$ and $\nu \geq \epsilon \geq 0$. Then the following binomial identities hold.*

$$\sum_{k=0}^{\lambda} \binom{\lambda - k}{\mu} \binom{\epsilon + k}{\nu} = \binom{\lambda + \epsilon + 1}{\mu + \nu + 1}, \tag{10.7}$$

"diagonals $\times$ reversed diagonals".

$$\sum_{k=0}^{\lambda} \binom{k}{\mu} = \binom{\lambda + 1}{\mu + 1}, \tag{10.8}$$

"summation on the upper index".

LEMMA 10.1.2. *The following two binomial relations hold.*

$$\sum_{k=1}^{m-r}(2k-1)\binom{m+r+1-k}{2r+1} = \frac{2m+1}{2r+3}\binom{m+r+1}{2r+2}. \tag{10.9}$$

and

$$\sum_{k=2r+1}^{m+r-q}\binom{m+r+1-k-q}{1}\binom{k}{2r+1} = \binom{m+r+2-q}{2r+3}. \tag{10.10}$$

Proof. Using (10.7) with $\lambda = m+r+1, \mu = 2r+1, \nu = 1$ and $\epsilon = 0$ gives

$$\sum_{k=1}^{m-r}\binom{k}{1}\binom{m+r+1-k}{2r+1} = \binom{m+r+2}{2r+3}, \tag{10.11}$$

and by (10.8)

$$\sum_{k=1}^{m-r}\binom{m+r+1-k}{2r+1} = \binom{m+r+1}{2r+2}. \tag{10.12}$$

Combining the two terms (10.11) and (10.12) we deduce the result (10.9)

To establish (10.10) we again use (10.7), but this time with $\lambda = m+r+1-q, \mu = 1, \nu = 2r+1$ and $\epsilon = 0$.

□

LEMMA 10.1.3. *With V_r and W_r defined as in* (10.2) *and* (10.3) *we have*

$$A_r V_0^2 = n^2\sum_{q=1}^{r-1}(r-q)A_q - n\sum_{q=1}^{m}(2r-1)(m+1-q)A_q, \tag{10.13}$$

$$V_0^2 = n\left(-3f_1 I + f_1 E - W_1\right), \tag{10.14}$$

$$V_0 V_r = n\left(-(r+1)f_{r+1}B_0 + f_{r+1}W_0 - W_{r+1}\right), \tag{10.15}$$

$$V_0 W_r = \left(n-(2r+1)\right)f_r V_0 - nV_r, \tag{10.16}$$

and

$$V_0^2 V_r = n^2\left(V_{r+1} - f_{r+1}V_0\right). \tag{10.17}$$

Proof. Equation (10.13) follows with some straightforward manipulation using (9.13), (9.14), (9.15) and (9.17). We give the proofs for (10.14) and (10.17). The proofs for (10.15) and (10.16) are similar although it is easy to show that together they satisfy (10.17). By (9.21)

$$V_0^2 = \sum_{r=1}^{m}\sum_{s=1}^{m} A_r B_s = \sum_{r=1}^{m}\sum_{s=1}^{m}(B_{r+s-1} - B_{r-s}).$$

Now

$$\sum_{s=1}^{m}(m+1-s)B_{r+s-1}$$

$$= \sum_{s=r}^{m}(m+r-s)B_s + \sum_{s=m+2-r}^{m}(r+s-m-1)B_s, \tag{10.18}$$

and

$$-\sum_{s=1}^{m}(m+1-s)B_{s-r}$$

$$= -2(m+1-r)I - \sum_{s=1}^{r-1}(m+1+s-r)B_s - \sum_{s=1}^{m-r+1}(m+1-s-r)B_s, \tag{10.19}$$

where we have used equations (9.18), (9.19) and (9.20). The s multiples of B_s in (10.18) and (10.19) cancel out completely, and collecting together the remaining terms we have

$$V_0^2 = \sum_{r=1}^{m}(m+1-r)\left(-2(m+1-r)I + (2r-1)(E-I) - (2m+1)\sum_{s=1}^{r-1}B_s\right)$$

$$= \sum_{r=1}^{m}(m+1-r)\left(-nI + (2r-1)E - n\sum_{s=1}^{r-1}B_s\right).$$

The coefficient of B_k in

$$\sum_{r=2}^{m}\sum_{s=1}^{r-1}(m+1-r)B_s$$

is

$$\sum_{j=1}^{m-k} j = \binom{m+1-k}{2}, \qquad 1 \le k \le m-1,$$

so that

$$\sum_{r=2}^{m}\sum_{s=1}^{r-1}(m+1-r)B_s = \sum_{k=1}^{m-1}\binom{m+1-k}{2} = W_1.$$

Hence we have

$$V_0^2 = n\left(-3f_1 I + f_1 E - W_1\right),$$

which is (10.14).

To obtain (10.13) we use

$$V_r V_0^2 = \sum_{k=1}^{m-r}\binom{m+r+1-k}{2r+1}A_k V_0^2$$

$$= \sum_{k=1}^{m-r}\binom{m+r+1-k}{2r+1}\left(n^2\sum_{q=1}^{k-1}(k-q)A_q - n\sum_{q=1}^{m}(2k-1)(m+1-q)A_q\right)$$

$$= n^2\sum_{k=2}^{m-r}\binom{m+r+1-k}{2r+1}\sum_{q=1}^{k-1}(k-q)A_q - n\sum_{k=1}^{m-r}\binom{m+r+1-k}{2r+1}(2k-1)V_0.$$

For fixed s, the coefficient of A_s in

$$\sum_{k=2}^{m-r}\binom{m+r+1-k}{2r+1}\sum_{q=1}^{k-1}(k-q)A_q$$

is given by (10.10). Therefore using both parts of Lemma 10.1.2 we have

$$V_r V_0^2 = n^2\left(V_{r+1} - f_{r+1}V_0\right),$$

and hence the result. □

An immediate consequence of (10.17) is that

$$V_0^3 + n^2 f_1 V_0 = n^2 V_1, \tag{10.20}$$

and repeated use of this identity yields the result

$$\sum_{k=0}^{r} n^{2(r-k)} f_{r-k} V_0^{2k+1} = n^{2r} V_r. \tag{10.21}$$

Applying (10.15), multiplying through by n and rearranging gives

$$\sum_{k=0}^{r} n^{2(r-k)+1} f_{r-k} V_0^{2k} = n^{2r} \left(2\binom{m+r}{2r+1} I - W_r \right), \tag{10.22}$$

where, by (9.27), we have taken

$$V_0^0 = I - \frac{1}{n} E. \tag{10.23}$$

Together (10.21) and (10.22) imply that the diagonal coefficients $a_q^{(t)}$ of V_0^t can be written in the form $n^{t-1} b_q^{(t)}$, where we call $b_q^{(t)}$ the *reduced coefficients* of V_0^t. Hence the equations in (10.5) and (10.6) for the fundamental matrix of $M^t(z, y)$ become

$$\left(\sum_{q=1}^{m} (m+1-q) A_q \right)^{2k+1} = V_0^{2k+1} = \sum_{q=1}^{m} n^{2k} b_q^{(2k+1)} A_q, \tag{10.24}$$

and when $t = 2k$ is even we use (9.16) and (9.21) to obtain

$$\left(\sum_{q=1}^{m} (m+1-q) A_q \right)^{2k} = V_0^{2k} = \sum_{q=0}^{m} n^{2k-1} b_q^{(2k)} B_q, \tag{10.25}$$

where by (10.22), $b_0^{(0)} = m$. We re-write (10.21) and (10.22) in terms of the reduced coefficients $b_q^{(2k)}$ and $b_q^{(2k+1)}$ to obtain the following Lemma.

LEMMA 10.1.4. *For $q \geq 1$, $r \geq 0$, the reduced coefficients $b_q^{(t)}$ of $M^t(z, y)$ satisfy*

$$\sum_{k=0}^{r} \binom{m+r-k}{2(r-k)} \frac{b_q^{(2k+1)}}{2(r-k)+1} = \binom{m+r-q+1}{2r+1}, \tag{10.26}$$

and

$$\sum_{k=0}^{r} \binom{m+r-k}{2(r-k)} \frac{b_q^{(2k)}}{2(r-k)+1} = -\binom{m+r-q}{2r}, \tag{10.27}$$

which can be rearranged as

$$b_q^{(2r+1)} = \binom{m+r-q+1}{2r+1} - \sum_{k=0}^{r-1} f_{r-k} b_q^{(2k+1)}, \tag{10.28}$$

and

$$b_q^{(2r)} = -\binom{m+r-q}{2r} - \sum_{k=0}^{r-1} f_{r-k} b_q^{(2k)}, \tag{10.29}$$

respectively.

Proof. By (10.21), (10.1) and (10.2) we have

$$f_0 V_0^{2r+1} = V_0^{2r+1} = n^{2r} V_r - \sum_{k=0}^{r-1} n^{2(r-k)} f_{r-k} V_0^{2k+1}$$

$$= n^{2r} \left(\sum_{q=1}^{m-r} \binom{m+r+1-q}{2r+1} A_q - \sum_{k=0}^{r-1} n^{-2k} f_{r-k} \sum_{q=0}^{m} n^{2k} b_q^{(2k+1)} A_q \right),$$

by (10.25). Hence

$$\sum_{q=0}^{m} n^{2r} b_q^{(2r+1)} A_q =$$

$$n^{2r} \left(\sum_{q=1}^{m-r} \binom{m+r+1-q}{2r+1} A_q - \sum_{k=0}^{r-1} n^{-2k} f_{r-k} \sum_{q=0}^{m} n^{2k} b_q^{(2k+1)} A_q \right),$$

and comparing coefficients of A_q we have

$$b_q^{(2r+1)} = \binom{m+r+1-q}{2r+1} - \sum_{k=0}^{r-1} f_{r-k} b_q^{(2k+1)}.$$

The proof for $b_q^{(2r)}$ is similar.

□

We note that for even powers, the coefficient of $B_0 = 2I$ is given by $b_0^{(2r)}$, where by (10.22)

$$\sum_{k=0}^{r} f_{r-k} b_0^{(2k)} = \binom{m+r}{2r+1}. \tag{10.30}$$

Comparing (10.30) with (10.26) when $q = 1$ and taking into account that $b_0^{(0)} = b_1^{(1)} = m$, it follows that $b_0^{(2r)} = b_1^{(2r+1)}$, for $r \geq 0$. By (10.29) it also follows that for $q \geq 1$, $b_q^{(0)} = -1$. Hence

$$V_0^0 = \frac{1}{n} \sum_{k=0}^{m} b_0^{(2k)} = \frac{1}{n}(2mI - (E - I)),$$

which also satisfies (10.23).

In the case $q = m$ we have

$$\binom{m+r-q+1}{2r+1} = 0, \qquad \binom{m+r-q}{2r} = 0,$$

for $r \geq 1$ and $r \geq 0$ respectively. Hence

$$b_m^{(2r+1)} = -\sum_{k=0}^{r-1} f_{r-k} b_m^{(2k+1)}, \qquad b_m^{(2r)} = -\sum_{k=0}^{r-1} f_{r-k} b_m^{(2k)}, \tag{10.31}$$

and as $b_m^{(1)} = -b_m^{(0)} = 1$, it follows that $b_m^{(2k+1)} = -b_m^{(2k)}$.

10.2 Characteristic Polynomials of $M(z, y)$

Given that $V_m = W_m = 0_n$, we can use (10.21) and (10.22) to write the characteristic polynomial of V_0 as

$$\sum_{k=0}^{m} n^{2(m-k)} f_{m-k} V_0^{2k+1} = 0_n = \sum_{k=0}^{m} n^{2(m-k)+1} f_{m-k} V_0^{2k}. \tag{10.32}$$

Adjusting for factors of $(z^2 - y^2)$, we find that the characteristic coefficients of $M(z, y)$ are given by

$$\lambda_{2k+1} = n^{2(m-k)} f_{m-k} (z^2 - y^2)^{m-k},$$

and

$$\lambda_{2k} = -nm(z + y)\lambda_{2k+1}, \tag{10.33}$$

from which we deduce that

$$\mathrm{Det}\,(M(z, y)) = n^{n-1}(m(z + y))(z^2 - y^2)^m. \tag{10.34}$$

By (10.32), the sum of the kernel matrices vanish. The characteristic polynomial of $M(z, y)$ reduces to

$$\sum_{k=0}^{m} \lambda_{2k+1} M^{2k+1}(z, y) = -\sum_{k=0}^{m} \lambda_{2k} M^{2k}(z, y) = \kappa E,$$

for some constant κ, where

$$\kappa = n^{n-1} \sum_{k=0}^{m} (z^2 - y^2)^{m-k} (m(z+y))^{2k+1} f_{m-k}. \tag{10.35}$$

If we take

(1) $y = mc^2 - m + c$,

(2) $z = mc^2 + m + c$,

then when $c = 1$, $M(z, y)$ contains the integers $0, 1, \cdots, n^2 - 1$ and so is a traditional associated magic square of order n. Applying the above values of (z, y) to (10.35) we have

$$\kappa = n^{n-1} \sum_{k=0}^{m} (z-y)^{m-k} (z+y)^{m+k+1} m^{2k+1} f_{m-k}$$

$$= n^{n-2} 2^n (mc)^{m+1} (mc+1)^{m+1} \sum_{k=0}^{m} (mc)^k (mc+1)^k f_{m-k} n. \tag{10.36}$$

We now use the identity

$$\sum_{k=0}^{m} w^k (w+1)^k f_{m-k} = \frac{(w+1)^n - w^n}{n}, \tag{10.37}$$

to obtain

$$\kappa = n^{n-2} 2^n (mc)^{m+1} (mc+1)^{m+1} \left((mc+1)^n - (mc)^n \right). \tag{10.38}$$

For example, if $m = 2$ (so $n = 5$) and $c = 1$, then

$$\kappa = 5^4 2^5 2^3 3^3 \sum_{k=0}^{2} \binom{4-k}{k} \frac{2^k 3^k}{5-2k}$$

$$= 5^4 2^8 3^3 \left(\frac{6^0 \times 1}{5} + \frac{6 \times 3}{3} + \frac{6^2 \times 1}{1} \right)$$

$$= 5^4 2^8 3^3 \left(\frac{211}{5} \right) = 5^3 2^8 3^3 \left(3^5 - 2^5 \right).$$

10.3 Sums and Differences of Two n-th Powers

Repeated use of (10.37) leads to

$$w^n = 1 + n\sum_{t=0}^{m} f_{m-t} \sum_{k=1}^{w-1} (k^2+k)^t, \tag{10.39}$$

which can be written in the form

$$w^n - w = n\sum_{t=1}^{m} f_{m-t} \sum_{k=1}^{w-1} (k^2+k)^t. \tag{10.40}$$

Noting that

$$nf_k \in \mathbf{N}, \forall\ 0 \leq k \leq m,$$

and using (10.40) we have the explicit form of Fermat's Little Theorem

$$\frac{w^{n-1}-1}{n} = \frac{1}{w}\sum_{t=1}^{m} f_{m-t} \sum_{k=1}^{w-1} (k^2+k)^t \in \mathbf{N}, \tag{10.41}$$

where n is prime and highest common factor $(w, n) = 1$.

Further consequences of (10.39) are

$$w^n + v^n = 2 + n\sum_{t=0}^{m} f_{m-t} \left(\sum_{k=1}^{w-1} (k^2+k)^t + \sum_{k=1}^{v-1} (k^2+k)^t \right), \tag{10.42}$$

for all $w, v, n \geq 1$ and without loss of generality, assuming that $w \geq v$, we have

$$w^n - v^n = n\sum_{t=0}^{m} f_{m-t} \sum_{k=v}^{w-1} (k^2+k)^t. \tag{10.43}$$

Chapter 11

Identities and Determinants

In this chapter we show that a Corollary to this examination of $M(z,y)$ is a particularly simple recurrence for the Bernoulli numbers (and so for the Riemann zeta function at even integers) which does not appear to have been written down before.

11.1 Coefficients of the $b_q^{(2r+1)}$ Polynomials

LEMMA 11.1.1. *Let $b_q^{(2r+1)}$ be the reduced coefficient of A_q in the expansion of $M^{2r+1}(z,y)$. Then for $r \geq 1$, we can write*

$$b_q^{(2r+1)} = \sum_{j=0}^{2r} c_{q,j}^{(2r+1)} m^j, \tag{11.1}$$

where

$$c_{q,2r}^{(2r+1)} = \frac{-r(2q-1)}{(2r+1)!} - \sum_{k=1}^{r-1} \frac{c_{q,2k}^{(2k+1)}}{(2r-2k+1)!}, \tag{11.2}$$

and

$$c_{m,2r}^{(2r+1)} = -\sum_{k=0}^{r-1} \frac{c_{m,2k}^{(2k+1)}}{(2r-2k+1)!}, \tag{11.3}$$

Proof. The coefficient of m^{2r+1} in

$$\binom{m+r+1-q}{2r+1},$$

is $1/(2r+1)!$ and this always cancels with the coefficient of

$$\frac{1}{2r+1}\binom{m+r}{2r}b_q^{(1)} = \frac{1}{2r+1}\binom{m+r}{2r}(m+1-q).$$

in (10.28). Therefore $b_q^{(3)}$ is a polynomial in m of degree at most 2 and by the recursive definition it follows that for $r \geq 1$ $b_q^{(2r+1)}$ is a polynomial in m of degree at most $2r$.

As defined in chapter 6, let $s(n,k)$ denote the Stirling numbers of the first kind and let $m^{\underline{n}}$ denote the falling factorial

$$m(m-1)(m-2)\dots(m-n+1).$$

The $s(n,k)$ count the number of permutations of n elements with k disjoint cycles and are related to $m^{\underline{n}}$ by the identity

$$m^{\underline{n}} = \sum_{k=1}^{n} s(n,k)m^k.$$

Replacing m with $m+i$ yields

$$(m+i)^{\underline{n}} = (m+i)(m+i-1)(m+i-2)\dots(m+i-n+1) \tag{11.4}$$

$$= \sum_{k=1}^{n} s(n,k)(m+i)^k = \sum_{k=1}^{n} s(n,k)\sum_{j=0}^{k}\binom{k}{j}m^j i^{k-j}, \tag{11.5}$$

and collecting terms we have

$$(m+i)^{\underline{n}} = \sum_{j=0}^{n} m^j \sum_{t=0}^{n-j}\binom{j+t}{j}s(n,j+t)i^t.$$

By (11.4) we can write (10.28) as

$$\sum_{j=0}^{2r} c_{q,j}^{(2r+1)}m^j = \frac{(m+r+1-q)^{\underline{2r+1}}}{(2r+1)!} - \sum_{k=0}^{r-1}\frac{(m+r-k)^{\underline{2r-2k}}}{(2r-2k+1)!}\sum_{j=0}^{2k} c_{q,j}^{(2k+1)}m^j, \tag{11.6}$$

and we use (11.5) to consider coefficients of m^{2r} in (11.6). We have

$$c_{q,2r}^{(2r+1)} = \frac{1}{(2r+1)!}\sum_{t=0}^{1}\binom{2r+t}{2r}s(2r+1,2r+t)(r+1-q)^t$$

$$-\frac{1}{(2r+1)!}\sum_{t=0}^{1}\binom{2r-1+t}{2r-1}s(2r,2r-1+t)r^t-\frac{1-q}{(2r+1)!},$$

$$-\sum_{k=1}^{r-1}\frac{c_{q,2k}^{(2k+1)}}{(2r-2k+1)!},$$

so that

$$c_{q,2r}^{(2r+1)}=\frac{-r(2q-1)}{(2r+1)!}-\sum_{k=1}^{r-1}\frac{c_{q,2k}^{(2k+1)}}{(2r-2k+1)!}.$$

The proof for (11.3) is simpler as we start with (10.31). Corresponding recurrence relations for the even power coefficients $c_{q,2r}^{(2r)}$ in the polynomial $b_q^{(2r)}$ can also be derived. □

In order that we may prove that the coefficients in $M^{2r+1}(z,y)$ are related to the even integer zeta numbers, we first prove the identity itself.

LEMMA 11.1.2.

$$\zeta(2j)=(-1)^j\left(\frac{-j\pi^{2j}}{(2j+1)!}-\sum_{k=1}^{j-1}\frac{(-1)^k\pi^{2j-2k}}{(2j-2k+1)!}\zeta(2k)\right).$$

Proof. We begin with the well known Bernoulli identity [43]

$$B(r)=-\frac{1}{r+1}\sum_{k=0}^{r-1}\binom{r+1}{k}B(k), \tag{11.7}$$

the Bernoulli-zeta even integer relation

$$\zeta(2j)=\frac{(-1)^{j+1}2^{2j-1}\pi^{2j}B(2j)}{(2j)!} \tag{11.8}$$

and the even integer zeta identity [7]

$$\sum_{k=0}^{j}\frac{(-1)^k\pi^{2k}}{(2k+1)!}(1-2^{2k-2j+1})\zeta(2j-2k)=0, \tag{11.9}$$

where $B(k)$ is the *kth* Bernoulli number and $\zeta(k)$ is the usual zeta number. From (11.9)

$$\zeta(2j)=\sum_{k=0}^{j-1}\frac{(-1)^{k+1-j}\pi^{2j-2k}(1-2^{1-2k})}{(2j-2k+1)!(1-2^{1-2j})}\zeta(2k),$$

and substituting from (11.8) gives

$$(2^{2j-1}-1)(-1)^{2j+1}B(2j)=\sum_{k=0}^{j-1}\frac{(2j)!(2^{2k-1}-1)}{(2k)!(2j-2k+1)!}B(2k).$$

Using the property that $B(2k+1)=0$ for $k\geq 1$ we can write

$$(2^{2j-1}-1)B(2j)=-\frac{1}{2j+1}\sum_{k=0}^{2j-1}\binom{2j+1}{k}(2^{k-1}-1)B(k),$$

where $(2^{k-1}-1)=0$ when $k=1$. Setting $r=2j$ yields

$$(2^{r-1}-1)B(r)=-\frac{1}{r+1}\sum_{k=0}^{r-1}\binom{r+1}{k}(2^{k-1}-1)B(k),$$

which by (11.7) simplifies to the relation

$$2^{r-1}B(r)=-\frac{1}{r+1}\sum_{k=0}^{r-1}\binom{r+1}{k}2^{k-1}B(k). \tag{11.10}$$

We now separate the $k=0$ term from the sum in (11.10) to get

$$2^{r-1}B(r)=-\frac{1}{2(r+1)}-\frac{1}{r+1}\sum_{k=1}^{r-1}\binom{r+1}{k}2^{k-1}B(k),$$

and re-substituting for r with $2j$ we have

$$\begin{aligned}2^{2j-1}B(2j)&=-\frac{1}{2(2j+1)}-\frac{1}{2j+1}\sum_{k=1}^{2j-1}\binom{2j+1}{k}2^{k-1}B(k)\\&=\frac{2j-(2j+1)}{2(2j+1)}-\frac{1}{2j+1}\sum_{k=1}^{2j-1}\binom{2j+1}{k}2^{k-1}B(k)\\&=\frac{j}{2j+1}-\frac{1}{2}-\frac{1}{2j+1}\sum_{k=1}^{2j-1}\binom{2j+1}{k}2^{k-1}B(k)\\&=\frac{j}{2j+1}-\frac{1}{2j+1}\sum_{k=1}^{j-1}\binom{2j+1}{2k}2^{2k-1}B(2k).\end{aligned}$$

Hence we can write

$$\frac{2^{2j-1}(-1)^{j+1}\pi^{2j}}{(2j)!}B(2j)$$

$$= (-1)^j \left(\frac{-j\pi^{2j}}{(2j+1)!} - \sum_{k=1}^{j-1} \frac{(-1)^k \pi^{2j-2k} 2^{2k-1} (-1)^{k+1} \pi^{2k} B(2k)}{(2j-2k+1)!(2k)!} \right),$$

so that

$$\zeta(2j) = (-1)^j \left(\frac{-j\pi^{2j}}{(2j+1)!} - \sum_{k=1}^{j-1} \frac{(-1)^k \pi^{2j-2k}}{(2j-2k+1)!} \zeta(2k) \right),$$

by (11.8) as required. □

LEMMA 11.1.3 (coefficient lemma). *We have*

$$c_{1,1}^{(2r+1)} = r c_{m,1}^{(2r+1)}. \tag{11.11}$$

$$c_{m,1}^{(2r+1)} = \frac{(-1)^r (r!)^2}{r(2r+1)!} \tag{11.12}$$

$$c_{m,2r}^{(2r+1)} = \frac{(-1)^r (2^{2r-1}-1)}{2^{2r-2}\pi^{2r}} \zeta(2r) \tag{11.13}$$

$$c_{q,2r}^{(2r+1)} = \frac{(-1)^r (2q-1)}{\pi^{2r}} \zeta(2r) \tag{11.14}$$

$$c_{q,2r-1}^{(2r+1)} = r c_{q,2r}^{(2r+1)}. \tag{11.15}$$

Proof. Equations (11.11) and (11.12) follow directly from the recurrence relations (10.28) and (10.31). Equation (11.13) follows from the relations (11.3) and (11.9).

When $r = 1$ and 2 in (11.2) we have

$$c_{q,2}^{(3)} = \frac{-(2q-1)}{6}, \qquad c_{q,4}^{(5)} = \frac{(2q-1)}{90},$$

which agrees with (11.14). Inductively assuming true in (11.2) gives

$$c_{q,2r}^{(2r+1)} = \frac{-r(2q-1)}{(2r+1)!} - \sum_{k=1}^{r-1} \frac{(-1)^k (2q-1)}{\pi^{2r}(2r-2k+1)!} \zeta(2r),$$

and by Lemma 11.1.2 this implies that

$$c_{q,2r}^{(2r+1)} = \frac{(-1)^r(2q-1)}{\pi^{2r}}\zeta(2r).$$

Equation (11.15) then follows directly from the recurrence relation (10.28). □

We note that similar relations exist for the even power coefficients $c_{q,s}^{(2r)}$ in the polynomial $b_q^{(2r)}$. One of the most notable being that

$$c_{q,2r}^{(2r)} = \frac{2(-1)^r}{\pi^{2r}}\zeta(2r).$$

11.2 Recurrence Determinants

In this section we prove that the reduced coefficients $b_q^{(2r)}$, $b_q^{(2r+1)}$, in the expressions for $M^t(z,y)$, given in Lemma 11.1.1, can each be expressed as a determinant, and we show that these determinants are related to known determinant generators for the Bernoulli numbers.

Definition. We define any $r \times r$ determinant of the form

$$(-1)^r \begin{vmatrix} h_1 & 1 & 0 & 0 & \dots & 0 \\ h_2 & h_1 & 1 & 0 & \dots & 0 \\ h_3 & h_2 & h_1 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ h_{r-1} & h_{r-2} & h_{r-3} & h_{r-4} & \dots & 1 \\ h_r & h_{r-1} & h_{r-2} & h_{r-3} & \dots & h_1 \end{vmatrix} \tag{11.16}$$

to be a *minor corner layered determinant* or MCL determinant for short. The name comes from the minor of $a_{1,r+1}$ in the $(r+1) \times (r+1)$ lower triangular determinant shown below.

$$\begin{vmatrix} 1 & 0 & 0 & 0 & \dots & 0 & 0 \\ h_1 & 1 & 0 & 0 & \dots & 0 & 0 \\ h_2 & h_1 & 1 & 0 & \dots & 0 & 0 \\ h_3 & h_2 & h_1 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ h_{r-1} & h_{r-2} & h_{r-3} & h_{r-4} & \dots & 1 & 0 \\ h_r & h_{r-1} & h_{r-2} & h_{r-3} & \dots & h_1 & 1 \end{vmatrix}.$$

LEMMA 11.2.1. *Let $h_1, \ldots, h_r$ be given. For $k = 1, \ldots, r$, let Δ_k be the $k \times k$ MCL determinant* (11.16). *Let $\Delta_0 = 1$. Then*

$$\Delta_r = -\sum_{k=0}^{r-1} h_{r-k}\Delta_k. \tag{11.17}$$

Conversely, if $\Delta_0 = 1$ and $\Delta_1, \Delta_2, \ldots, \Delta_r, h_1, \ldots, h_r$ are real numbers satisfying (11.17) *then Δ_r is given in terms of $h_1, \ldots, h_r$ by* (11.16).

COROLLARY. *For $r \geq 1$, let g_r be defined by the recurrence relation*

$$g_r = -\sum_{k=0}^{r-1} h_{r-k}g_k, \tag{11.18}$$

where $g_0 = 1$. Then g_r is given by the MCL determinant in the statement of the lemma with $\Delta_r = g_r$.

Proof. We expand the determinant along its first column starting at the r-th row so that

$$(-1)^r\Delta_r = (-1)^{r-1}1^{r-1}h_r + (-1)^{r-2}1^{r-2}h_{r-1}\,|h_1| +$$

$$(-1)^{r-3}1^{r-3}h_{r-2}\begin{vmatrix} h_1 & 1 \\ h_2 & h_1 \end{vmatrix} + \ldots + h_1\begin{vmatrix} h_1 & 1 & \ldots & 0 \\ h_2 & h_1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ h_{r-2} & h_{r-1} & \ldots & 1 \\ h_{r-1} & h_{r-2} & \ldots & h_1 \end{vmatrix}$$

and hence the result. The converse follows from re-packing the original determinant.

To see the Corollary, we only need to show that each g_r can be expressed as a determinant of the required form. By (11.18) we have

$$g_1 = -h_1g_0 = -\,|h_1|\,g_0$$

$$g_2 = -\left(h_2g_0 + h_1g_1\right) = -\left(h_2 - h_1^2\right) = \begin{vmatrix} h_1 & 1 \\ h_2 & h_1 \end{vmatrix}.$$

We inductively assume true for g_r, $1 \leq r \leq n$, and we consider the case g_{n+1} in the relation (11.18), replacing the g_r with the corresponding $r \times r$ determinants. The Corollary follows by the second assertion of the Lemma. □

An immediate consequence of this result, is that for $r \geq 1$, the expressions for $b_m^{(2r+1)}$ and $b_m^{(2r)}$ in (10.28) and (10.29) can be expressed as MCL determinants. That is

$$b_m^{(2r+1)} = -b_m^{(2r)} = -\sum_{k=0}^{r-1} f_{r-k} b_m^{(2k+1)} \tag{11.19}$$

$$= (-1)^r \begin{vmatrix} f_1 & 1 & 0 & 0 & \dots & 0 \\ f_2 & f_1 & 1 & 0 & \dots & 0 \\ f_3 & f_2 & f_1 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ f_{r-1} & f_{r-2} & f_{r-3} & f_{r-4} & \dots & 1 \\ f_r & f_{r-1} & f_{r-2} & f_{r-3} & \dots & f_1 \end{vmatrix}. \tag{11.20}$$

Having expressed $b_m^{(2r+1)}$ and $b_m^{(2r)}$ as $r \times r$ MCL determinants, we now show that there is a family of determinants that relate to the reduced coefficients $b_q^{(2r+1)}$ and $b_q^{(2r)}$, $1 \leq q \leq m$.

LEMMA 11.2.2. *Let the matrices V_r and W_r be defined as at the beginning of Section* 10.1. *Then the fundamental matrix V_0^t of $M^t(z, y)$ satisfies*

$$V_0^{2r+1} = n^{2r} \sum_{k=0}^{r} b_m^{(2k+1)} V_{r-k}, \tag{11.21}$$

and

$$V_0^{2r} = n^{2r-1} \left(2I \sum_{k=0}^{r-1} (r-k) f_{r-k} b_m^{(2k)} + \sum_{k=0}^{r} b_m^{(2k)} W_{r-k} \right). \tag{11.22}$$

We deduce that the reduced coefficients in the fundamental matrix satisfy

$$b_q^{(2r+1)} = \sum_{k=0}^{\min(r,\, m-q)} \binom{m-q+k+1}{2k+1} b_m^{(2r-2k+1)}, \tag{11.23}$$

and

$$b_q^{(2r)} = \sum_{k=0}^{\min(r,\, m-q)} \binom{m-q+k}{2k} b_m^{(2r-2k)}. \tag{11.24}$$

Proof. Putting $r = 0$ and 1 in (11.21) gives

$$V_0 = V_0, \qquad V_0^3 = n^2(V_1 - f_1 V_0),$$

which agrees with (10.20).

We inductively assume true so that

$$V_0^{2r+1} V_0^2 = n^{2r} \sum_{k=0}^{r} b_m^{(2k+1)} V_{r-k} V_0^2,$$

and by (10.17) we have

$$V_0^{2r+3} = n^{2r} \sum_{k=0}^{r} b_m^{(2k+1)} n^2 (V_{r-k+1} - f_{r-k+1} V_0)$$

$$= n^{2r+2} \left(\sum_{k=0}^{r} b_m^{(2k+1)} V_{r-k+1} - V_0 \sum_{k=0}^{r} b_m^{(2k+1)} f_{r-k+1} \right).$$

Using (10.31) this reduces to

$$V_0^{2r+3} = n^{2r+2} \sum_{k=0}^{r+1} b_m^{(2k+1)} V_{r+1-k},$$

and the induction is complete.

To obtain (11.22), we simply take the above equation for V_0^{2r-1}, multiply by V_0 and apply (10.15). We then rearrange using (10.31) and replace $b_m^{(2k+1)}$ with $-b_m^{(2k)}$. The results (11.23) and (11.24) then follow by considering coefficients of A_q and B_q in V_r and W_r respectively. □

Hence, for the odd powers of the fundamental matrix we have

$$b_{m-1}^{(2r+1)} = 2b_m^{(2r+1)} + b_m^{(2r-1)},$$

$$b_{m-2}^{(2r+1)} = 3b_m^{(2r+1)} + 4b_m^{(2r+1)} + b_m^{(2r-1)} + b_m^{(2r-3)},$$

$$\vdots \quad \vdots \quad \vdots \quad \vdots$$

$$b_2^{(2r+1)} = \sum_{k=0}^{\min(r,\, m-2)} \binom{m-1+k}{2k+1} b_m^{(2r-2k+1)},$$

$$b_1^{(2r+1)} = \sum_{k=0}^{\min(r,\, m-1)} \binom{m+k}{2k+1} b_m^{(2r-2k+1)}.$$

Translating these equations into determinant format yields

$$b_m^{(2r+1)} = (-1)^r \begin{vmatrix} 1 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & f_1 & 1 & 0 & 0 & \dots & 0 \\ 0 & f_2 & f_1 & 1 & 0 & \dots & 0 \\ 0 & f_3 & f_2 & f_1 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & f_{r-1} & f_{r-2} & f_{r-3} & f_{r-4} & \dots & 1 \\ 0 & f_r & f_{r-1} & f_{r-2} & f_{r-3} & \dots & f_1 \end{vmatrix},$$

$$b_{m-1}^{(2r+1)} = (-1)^{r+1} \begin{vmatrix} 2 & 1 & 0 & 0 & 0 & \dots & 0 \\ 1 & f_1 & 1 & 0 & 0 & \dots & 0 \\ 0 & f_2 & f_1 & 1 & 0 & \dots & 0 \\ 0 & f_3 & f_2 & f_1 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & f_{r-1} & f_{r-2} & f_{r-3} & f_{r-4} & \dots & 1 \\ 0 & f_r & f_{r-1} & f_{r-2} & f_{r-3} & \dots & f_1 \end{vmatrix},$$

$$b_{m-2}^{(2r+1)} = (-1)^{r+2} \begin{vmatrix} 3 & 1 & 0 & 0 & 0 & \dots & 0 \\ 4 & f_1 & 1 & 0 & 0 & \dots & 0 \\ 1 & f_2 & f_1 & 1 & 0 & \dots & 0 \\ 0 & f_3 & f_2 & f_1 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & f_{r-1} & f_{r-2} & f_{r-3} & f_{r-4} & \dots & 1 \\ 0 & f_r & f_{r-1} & f_{r-2} & f_{r-3} & \dots & f_1 \end{vmatrix},$$

$$\vdots \quad \vdots \quad \vdots$$

$$b_2^{(2r+1)} = (-1)^{r+m-2} \begin{vmatrix} \binom{m-1}{1} & 1 & 0 & 0 & 0 & \dots & 0 \\ \binom{m}{3} & f_1 & 1 & 0 & 0 & \dots & 0 \\ \binom{m+1}{5} & f_2 & f_1 & 1 & 0 & \dots & 0 \\ \binom{m+2}{7} & f_3 & f_2 & f_1 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \binom{m+r-2}{2r-1} & f_{r-1} & f_{r-2} & f_{r-3} & f_{r-4} & \dots & 1 \\ \binom{m+r-1}{2r+1} & f_r & f_{r-1} & f_{r-2} & f_{r-3} & \dots & f_1 \end{vmatrix},$$

$$b_1^{(2r+1)} = (-1)^{r+m-1} \begin{vmatrix} \binom{m}{1} & 1 & 0 & 0 & 0 & \dots & 0 \\ \binom{m+1}{3} & f_1 & 1 & 0 & 0 & \dots & 0 \\ \binom{m+2}{5} & f_2 & f_1 & 1 & 0 & \dots & 0 \\ \binom{m+3}{7} & f_3 & f_2 & f_1 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \binom{m+r-1}{2r-1} & f_{r-1} & f_{r-2} & f_{r-3} & f_{r-4} & \dots & 1 \\ \binom{m+r}{2r+1} & f_r & f_{r-1} & f_{r-2} & f_{r-3} & \dots & f_1 \end{vmatrix}.$$

Corresponding families of determinants exist for the even power reduced coefficients $b_q^{(2r)}$. We give the first few polynomials in m for $b_1^{(2r+1)}$ and $b_m^{(2r+1)}$ below. We have

$$b_1^{(1)} = m, \qquad b_m^{(1)} = 1,$$

$$b_1^{(3)} = b_m^{(3)} = -\frac{m^2}{6} - \frac{m}{6},$$

$$b_1^{(5)} = \frac{m^4}{90} + \frac{m^3}{45} + \frac{2m^2}{45} + \frac{m}{30},$$

$$b_m^{(5)} = \frac{7m^4}{360} + \frac{7m^3}{180} + \frac{13m^2}{360} + \frac{m}{60},$$

$$b_1^{(7)} = -\frac{m^6}{945} - \frac{m^5}{315} - \frac{17m^4}{2520} - \frac{31m^3}{3780} - \frac{3m^2}{280} - \frac{m}{140},$$

$$b_m^{(7)} = -\frac{31m^6}{15120} - \frac{31m^5}{5040} - \frac{17m^4}{1680} - \frac{151m^3}{15120} - \frac{2m^2}{315} - \frac{m}{420}.$$

Remark. Geometric interpretations are often of interest and referring to Lemma 3.4.2 we see that their exists a natural relationship between determinants of order $r+1$ and $\pm r!$ times the volume of an r-dimensional simplex. Hence one interpretation of the reduced coefficients $b_q^{(t)}$ is as a multiple of the volume of a simplex. For example, the determinant for the coefficient $b_m^{(2r+1)}$ can be written as the $(r+1) \times (r+1)$ determinant

$$(-1)^r \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & \dots & 0 \\ 1 & f_1 & 1 & 0 & 0 & \dots & 0 \\ 1 & f_2 & f_1 & 1 & 0 & \dots & 0 \\ 1 & f_3 & f_2 & f_1 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & f_{r-1} & f_{r-2} & f_{r-3} & f_{r-4} & \dots & 1 \\ 1 & f_r & f_{r-1} & f_{r-2} & f_{r-3} & \dots & f_1 \end{vmatrix}.$$

Here, $|b_m^{(2r+1)}/r!|$ is equal to the r-dimensional volume of a simplex with corners

$$\begin{gathered}(0,0,0\ldots,0),\\(f_1,1,0,\ldots,0),\\(f_2,f_1,1,\ldots,0),\\\vdots\quad\vdots\quad\vdots\\(f_r,f_{r-1},f_{r-2},\ldots,f_1).\end{gathered}$$

Adding the extra row and column means that for $q \leq m-1$, the simplex determinants are of order $(r+2)$. For example

$$b_1^{(7)} = (-1)^3 \begin{vmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & m & 1 & 0 & 0 \\ 1 & (m-1)f_1 & f_1 & 1 & 0 \\ 1 & (m-2)f_2 & f_2 & f_1 & 1 \\ 1 & (m-3)f_3 & f_3 & f_2 & f_1 \end{vmatrix}.$$

A parallel interpretation can be made for the reduced coefficients of the fundamental inverse matrix of $M^{-t}(z,y)$ as they are just binomial coefficients, and by Chapter 6, these can represent the lattice point enumerators of a simplex. The difference here being that the volume is discrete rather than continuous.

The denominator of f_r is $(2r+1)!$ and we now highlight further the link between the coefficients $b_q^{(2r+1)}$ and the Bernoulli numbers (and so the even zeta values) with some known results concerning MCL determinants of these denominators.

LEMMA 11.2.3. *The Bernoulli numbers, $B(r)$, are generated by the $r \times r$ MCL determinant of factorial denominators*

$$B(r) = (-1)^r r! \begin{vmatrix} \frac{1}{2!} & 1 & 0 & \ldots & 0 \\ \frac{1}{3!} & \frac{1}{2!} & 1 & \ldots & 0 \\ \frac{1}{4!} & \frac{1}{3!} & \frac{1}{2!} & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{1}{r!} & \frac{1}{(r-1)!} & \frac{1}{(r-2)!} & \ldots & 1 \\ \frac{1}{(r+1)!} & \frac{1}{r!} & \frac{1}{(r-1)!} & \ldots & \frac{1}{2!} \end{vmatrix}, \qquad (11.25)$$

and the even Bernoulli numbers $B(2r)$ are generated by the $r \times r$ MCL determinant of odd factorial denominators

$$B(2r) = (-1)^{r-1}\frac{2r!}{2(2^{2r-1}-1)}\begin{vmatrix} \frac{1}{3!} & 1 & 0 & 0 & \dots & 0 \\ \frac{1}{5!} & \frac{1}{3!} & 1 & 0 & \dots & 0 \\ \frac{1}{7!} & \frac{1}{5!} & \frac{1}{3!} & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{1}{(2r-1)!} & \frac{1}{(2r-3)!} & \frac{1}{(2r-5)!} & \frac{1}{(2r-7)!} & \dots & 1 \\ \frac{1}{(2r+1)!} & \frac{1}{(2r-1)!} & \frac{1}{(2r-3)!} & \frac{1}{(2r-5)!} & \dots & \frac{1}{3!} \end{vmatrix}. \tag{11.26}$$

Proof. We refer the reader to [43] and [28]. A related identity is given in [41]. □

Let the $r \times r$ determinants (11.25) and (11.26) be denoted by Δ'_r and $\Delta^\star_r$ respectively. Then by (11.8) we have

$$\frac{\zeta(2r)}{\pi^{2r}} = (-1)^{r+1}2^{2r-1}\Delta'_{2r} = \frac{2^{2r-2}}{2^{2r-1}-1}\Delta^\star_r,$$

and Lemma 11.1.2 can be written in Bernoulli determinant form as

$$\frac{\zeta(2r)}{\pi^{2r}} = \frac{(-1)^{r+1}r}{(2r+1)!} + \sum_{k=1}^{r-1}\frac{(-1)^k 2^{2k-1}}{(2r-2k+1)!}\Delta'_{2r}$$

$$= (-1)^r\left(\frac{-r}{(2r+1)!} - \sum_{k=1}^{r-1}\frac{(-1)^k 2^{2k-2}}{(2r-2k+1)!(2^{2k-1}-1)}\Delta^\star_r\right). \tag{11.27}$$

11.3 Residues and Inverses modulo n

We draw to a close our investigations into the world of type A magic squares of odd order with a return to the basic concepts involved.

Fundamentally a traditional type A square contains all of the residues (mod n^2), and this square can be decomposed into two orthogonal auxiliary squares which each contain the integers $0, 1, \dots, n-1$. That is, all of the residues (mod n). So far in this study, we have shown that preservation of symmetry to all odd powers, binomial coefficients and divisions thereof, binomial sums, even zeta numbers, MCL determinants and geometric interpretations all naturally occur when matrix powers of the type A square

$M(z,y)$ are considered. However, we have not considered the possibility that any of the fundamental squares $k(nI - yJ)V_0^t$ of $kM^t(z,y)$ can be traditional (mod n^2) for some constant k and with $t \neq 1$. When t is even, the squares $M^t(z,y)$ are of type B and therefore cannot be traditional. Hence we consider odd powers of $M(z,y)$.

LEMMA 11.3.1. *Let m and k be positive integers. Then $(2m+1)f_k$ takes integer values.*

Proof. We put $t = m + k$, $r = 2k + 1$ in the binomial identity

$$\binom{t}{r} + \binom{t+1}{r} = \frac{2t+2-r}{r}\binom{t}{r-1} = \frac{2m+1}{2k+1}\binom{m+k}{2k}. \tag{11.28}$$

The identity is easily verified by cancelation of factorial terms on both sides. □

Remark. If f_k is an integer for all k in $1 \leq k \leq m-1$, then $2m+1$ must be prime. It can be shown that the converse statement also holds.

LEMMA 11.3.2 (denominator lemma). *Let m and k be positive integers, with*

$$2m + 1 = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_r^{a_r}$$

as a product of primes. Let $p_1, \dots, p_s$ be the prime factors of $2m+1$ with $p \leq 2k+1$; only these primes can occur in the denominator of $b_m^{(2k+1)}$. For $i \leq s$, let $p_i = 2t_i + 1$, and let $k = q_i t_i + w_i$, where q_i and w_i are positive integers with $q_i \geq 1$, $0 \leq w_i \leq t_i - 1$. Let

$$Q = p_1^{q_1} p_2^{q_2} \dots p_s^{q_s}.$$

Then $Qb_q^{(2k+1)}$ is an integer.

COROLLARY 1. *The rational number*

$$(2m+1)^k b_q^{(2k+1)} \tag{11.29}$$

is an integer, $1 \leq q \leq m$.

COROLLARY 2. *Let $\ell = \ell(k,m)$ of $b_q^{(2k+1)}$ be the smallest ℓ for which*

$$(2m+1)^\ell b_q^{(2k+1)}$$

is an integer. Then for $(2m+1)$ a prime we have

$$\ell = \left\lceil \frac{k}{m} \right\rceil.$$

Proof. From the definition of $b_m^{(2k+1)}$ as a determinant, $b_m^{(2k+1)}$ is a sum of monomials of the form

$$\pm f_{c_1}^{d_1} f_{c_2}^{d_2} \dots f_{c_j}^{d_j},$$

with

$$c_1 d_1 + c_2 d_2 + \dots + c_j d_j = k.$$

Let D_k be the minimal denominator of f_k. Then $D_k \leq 2k+1$. We want to establish the power of p in

$$D_{c_1}^{d_1} D_{c_2}^{d_2} \dots D_{c_j}^{d_j}.$$

This is at most

$$d_1 \left[\frac{2c_1+1}{2t+1}\right] + d_2 \left[\frac{2c_2+1}{2t+1}\right] + \dots + d_j \left[\frac{2c_j+1}{2t+1}\right].$$

We note that

$$\frac{2c_i+1}{2t+1} \leq \frac{c_i}{t}$$

when $2ct + t \leq 2ct + c$, $t \leq c$, and that

$$\left[\frac{2c_1+1}{2t+1}\right] = 0 \leq \frac{c}{t},$$

when $t > c$. So the power of p in $D_{c_1}^{d_1} D_{c_2}^{d_2} \dots D_{c_j}^{d_j}$ is at most

$$\frac{c_1 d_1 + \dots + c_j d_j}{t} \leq \frac{k}{t} = q + \frac{w}{t}.$$

The power is an integer, so it is at most q. We deduce the result of the Lemma.

To see the first Corollary we have

$$Qb_m^{(1)}, Qb_m^{(3)}, \dots, Qb_m^{(2k+1)} \in \mathbf{N},$$

with

$$Q | (2m+1)^k.$$

The $b_q^{(2k+1)}$ are just linear integer combinations of the $b_m^{(2j+1)}$, with $0 \leq j \leq k$, and the results follows. In the second Corollary, $2m+1$ is the only prime that can occur in the denominator, and so in the proof of the Lemma we have

$$\ell = q = \left[\frac{k}{m}\right].$$

□

LEMMA 11.3.3. *For $p = 2m + 1$, a prime, the fundamental matrix V_0^p of order p, defined in* (10.24) *and* (10.25), *satisfies the congruence*

$$\frac{1}{p^{p-2}} V_0^p \equiv -V_0 \pmod{p},$$

so that

$$\frac{1}{p^{p-2}} (pI - J) V_0^p$$

contains all of the residues $\pmod{p^2}$.

Proof. From Lemma 11.2.2 we have

$$V_0^{2m+1} = p^{2m} \sum_{k=0}^{m} b_m^{(2k+1)} V_{m-k},$$

so that

$$\frac{1}{p^{p-2}} V_0^{2m+1} = \sum_{k=0}^{m} p b_m^{(2k+1)} V_{m-k}.$$

Now by the second Corollary to Lemma 11.3.2 we have $b_m^{(2k+1)} \in \mathbb{N}$ for $0 \leq k \leq m - 1$, but

$$b_m^{(p)} = -\sum_{k=0}^{m-1} f_{m-k} b_m^{(2k+1)} = -\frac{1}{p} - \sum_{k=1}^{m-1} f_{m-k} b_m^{(2k+1)}.$$

Hence, by Lemma 11.3.1,

$$p b_m^{(p)} \equiv -1 \pmod{p},$$

and

$$\frac{1}{p^{p-2}} V_0^p = \sum_{k=0}^{m} p b_m^{(2k+1)} V_{m-k} \equiv -V_0 \pmod{p},$$

as required. □

For the fundamental matrix of $M^{-t}(z, y)$, we again need to add the restriction that $n = p$ a prime. Although the fundamental matrix V_0^t has weight

zero and hence is not invertible, we define the pseudo-inverse matrix or fundamental matrix of $M^{-t}(z,y)$ from the Corollary to Lemma 9.3.1. That is, we write

$$V_0^{-(2k+1)} = \frac{1}{n^{2k+1}} A_0^{2k+1} = \frac{1}{n^{2k+1}} \sum_{r=1}^{k+1} (-1)^{k+r} \binom{2k+1}{k+r} A_r, \tag{11.30}$$

and $(m+1-r)^{(-1)}$ for the inverse residue of $(m+1-r)$ under multiplication (mod p), where $p = 2m+1$ is a prime.

LEMMA 11.3.4. *Let $p = 2m+1$ be a prime and let $V_0^{-(2k+1)}$ be defined as in* (11.30). *Then*

$$\frac{1}{p} \sum_{r=1}^{m} (-1)^{m+r} \binom{p}{m+r} A_r \equiv \sum_{r=1}^{m} (m+1-r)^{(-1)} A_r \pmod{p},$$

so that

$$p^{p-1}(pI - J)V_0^{-p}$$

contains all of the residues (mod p^2).

Proof. We give a sketch proof.

By Fermat, when p is prime, 1 and $p-1$ are their own inverses under multiplication (mod p), and for all numbers $a \not\equiv 0$, there exists r such that

$$ar \equiv 1 \pmod{p}.$$

The inverses are unique (mod p), so that every non-zero residue has a unique inverse and the $2m$ non-zero residues consist of $m-1$ disjoint pairs and then 1 and $p-1$.

The proof then uses the identity

$$\frac{1}{m+1-r} \binom{p-1}{m+r} \equiv (-1)^{m-r} (m+1-r)^{(-1)} \pmod{p},$$

from which we deduce that the $2m$ values,

$$\frac{\pm 1}{p} \binom{p}{m+r} \pmod{p},$$

with $1 \le r \le m$, are the $2m$ non-zero residues (mod p). Hence

$$p^{p-1}(pI - J)V_0^{-p}$$

contains all of the residues (mod p^2). □

LEMMA 11.3.5. *Let $n = 2m+1$ and $1 \leq t \leq n$. Let $N^{(-t)}$ and $N^{(t)}$ be the respective matrices*

$$-n^t V_0^{-t} = -A_0^t, \qquad \frac{1}{n^{t-1}} V_0^t,$$

so that $N^{(-t)}$ contains binomial entries and $N^{(t)}$ the reduced coefficients $b_q^{(t)}$, as defined in (10.24) *and* (10.25). *Then under matrix multiplication, $N^{(-t)}$ is the inverse matrix of $N^{(t)}$* (mod$n$).

Proof. By (9.27) we have

$$N^{-t} N^t = -(nI - E) \equiv E \pmod{n}.$$

□

It is interesting to note that when $n = 2m+1$ is not prime there are not always unique inverses (mod n). However, when V_0 is of order n, and so contains all the n residues $-m, \ldots, -1, 0, 1, \ldots, m$, there does exist an inverse matrix modulo n for the reduced coefficients of V_0^t that is constructed from binomial coefficients.

There are other recurrent arrays which connect the reduced coefficients $b_q^{(t)}$ to the binomial coefficients and hint at further structure. The following example, Table 11.1, is the case $m = 5$ of polynomials in m of even degrees.

Table 11.1: Table of $b_q^{(t)}$ values when $m = 5$ and $-12 \leq t \leq 11$.

t	$b_0^{(t)}$	$b_1^{(t)}$	$b_2^{(t)}$	$b_3^{(t)}$	$b_4^{(t)}$	$b_5^{(t)}$	$b_6^{(t)}$	$b_7^{(t)}$	$b_8^{(t)}$	$b_9^{(t)}$	$b_{10}^{(t)}$	$b_{11}^{(t)}$
11		$-310\frac{5}{11}$	$-832\frac{4}{11}$	$-1089\frac{3}{11}$	$-1000\frac{2}{11}$	$-594\frac{1}{11}$	0	$594\frac{1}{11}$	$1000\frac{2}{11}$	$1089\frac{3}{11}$	$832\frac{4}{11}$	$310\frac{5}{11}$
10	$-620\frac{10}{11}$	$-521\frac{10}{11}$	$-256\frac{10}{11}$	$89\frac{1}{11}$	$406\frac{1}{11}$	$594\frac{1}{11}$	$594\frac{1}{11}$	$406\frac{1}{11}$	$89\frac{2}{11}$	$-256\frac{10}{11}$	$-521\frac{10}{11}$	
9		99	265	346	317	188	0	-188	-317	-346	-265	-99
8	198	166	81	-29	-129	-188	-188	-129	-29	81	166	
7		-32	-85	-110	-100	-59	0	59	100	110	85	32
6	-64	-53	-25	10	41	59	59	41	10	-25	-53	
5		11	28	35	31	18	0	-18	-31	-35	-28	-11
4	22	17	7	-4	-13	-18	-18	-13	-4	7	17	
3		-5	-10	-11	-9	-5	0	5	9	11	10	5
2	-10	-5	-1	2	4	5	5	4	2	-1	-5	
1		5	4	3	2	1	0	-1	-2	-3	-4	-5
0	10	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	
-1		-1	0	0	0	0	0	0	0	0	0	-1
-2	-2	1	0	0	0	0	0	0	0	0	1	
-3		3	-1	0	0	0	0	0	0	0	1	-3
-4	6	-4	1	0	0	0	0	0	0	1	-4	
-5		-10	5	-1	0	0	0	0	0	1	-5	10
-6	-20	15	-6	1	0	0	0	0	1	-6	15	
-7		35	-21	7	-1	0	0	0	1	-7	21	-35
-8	70	-56	28	-8	1	0	0	1	-8	28	-56	
-9		-126	84	-36	9	-1	0	1	-9	36	-84	126
-10	-252	210	-120	45	-10	1	1	-10	45	-120	210	
-11		462	-330	165	-55	11	0	-11	55	-165	330	-462
-12	924	-792	495	-220	66	-11	-11	66	-220	495	-792	

Chapter 12

Addendum

Many thanks to the PhD examiners Dr I. Aliev and Dr K. Nair for allowing the inclusion of this addendum to part II of the thesis.

12.1 Multinomial Identities

From (11.23) and (11.24) the reduced coefficients $b_m^{(2k+1)}$ and $-b_m^{(2k)}$ can be used to express the reduced coefficients $b_q^{(t)}$ of V_0^t. By (11.19) we have

$$b_m^{(2r+1)} = -b_m^{(2r)} = -\sum_{k=0}^{r-1} f_{r-k} b_m^{(2k+1)}, \tag{12.1}$$

and repeated use of (12.1) gives

$$b_m^{(2r+1)} = (-1)^r \sum_{k_1=0}^{r-1} \sum_{k_2=0}^{k_1-1} \cdots \sum_{k_w=0}^{k_{w-1}-1} f_{r-k_1} f_{k_1-k_2} \cdots f_{k_{w-1}-k_w} b_m^{(2k_w+1)},$$

with $k_w = k_{w-1} - 1 = 0$, so that $b_m^{(2k_w+1)} = b_m^{(1)} = 1$. Hence we can write

$$b_m^{(2r+1)} = (-1)^r \sum_{k_1=0}^{r-1} \sum_{k_2=0}^{k_1-1} \cdots \sum_{k_w=0}^{k_{w-1}-1} f_{r-k_1} f_{k_1-k_2} \cdots f_{k_{w-1}-k_w}, \tag{12.2}$$

which is just a sum of products of f_k, where the subscripts in each product sum to r. By considering the determinant expansion (11.20) of $b_m^{(2r+1)}$ we see that number of products is 2^{r-1}. That is, when the expressions for the sum

of the products is simplified, then ignoring sign, the sum of the coefficients of the products is 2^{r-1}. For example, when $r = 5$, we have

$$b_m^{(11)} = -f_1^5 + 4f_1^3 f_2 - 3f_1 f_2^2 - 3f_1^2 f_3 f_2^2 + 2f_2 f_3 + 2f_1 f_4 - f_5.$$

Therefore we have established that $b_m^{(2r+1)}$ is a sum of monomials of the form

$$\pm f_1^{d_1} f_2^{d_2} \dots f_r^{d_r}, \tag{12.3}$$

with

$$d_i \geq 0, \qquad d_1 + 2d_2 + \dots + rd_r = r.$$

We note that for a given $d_1 + 2d_2 + \dots + rd_r = r$, with $d_1 + d_2 + \dots + d_j = s$, the coefficient of the product in (12.3) is the same (ignoring sign) as that in the multinomial expansion of

$$(f_1 + f_2 + \dots + f_r)^s.$$

Hence we can write

$$b_m^{(2r+1)} = \sum_{s=1}^{r} \sum_{\substack{d_i \geq 0 \\ d_1+d_2+\dots+d_r=s \\ d_1+2d_2+\dots+rd_r=r}} (-1)^s \binom{s}{d_1, d_2, \dots, d_r} f_1^{d_1} f_2^{d_2} \dots f_r^{d_r}. \tag{12.4}$$

From (11.13) of Lemma 11.1.3 the leading coefficient $c_{m,2r}^{(2r+1)}$ of the polynomial expansion of $b_m^{(2r+1)}$ satisfies

$$c_{m,2r}^{(2r+1)} = \frac{(-1)^r (2^{2r-1} - 1)}{2^{2r-2} \pi^{2r}} \zeta(2r), \tag{12.5}$$

from which we deduce the identity

$$\frac{\zeta(2r)}{\pi^{2r}} = \frac{2^{2r-2}}{(2^{2r-1} - 1)} \sum_{s=1}^{r} \sum_{\substack{d_i \geq 0 \\ d_1+d_2+\dots+d_r=s \\ d_1+2d_2+\dots+rd_r=r}} \binom{s}{d_1, d_2, \dots, d_r} \frac{(-1)^{s+r}}{3!^{d_1} 5!^{d_2} \dots (2r+1)!^{d_r}}. \tag{12.6}$$

Similar identities can be obtained by comparing (12.4) with (11.23) and (11.14).

12.2 p-adic Relations

Structure of a p-adic nature [26] in the diagonal coefficients, $a_q^{(t)}$ of V_0^t, becomes apparent when one considers the matrix powers t with $t \geq |n|$. For $t > 0$, we define $b_q^{(-t)}$ to be the diagonal coefficients of A_0^t, so that

$$V_0^{-(2t+1)} = \frac{1}{n^{2t+1}} A_0^{2t+1} = \sum_{q=1}^{m} a_q^{(-(2t+1))} A_q = \frac{1}{n^{2t+1}} \sum_{q=1}^{m} b_q^{(-(2t+1))} A_q \qquad (12.7)$$

$$V_0^{-2t} = \frac{1}{n^{2t}} A_0^{2t} = \sum_{q=0}^{m} a_q^{(-2t)} B_q = \frac{1}{n^{2t}} \sum_{q=0}^{m} b_q^{(-2t)} B_q. \qquad (12.8)$$

We now recall Fleck's congruence [12]. Let p be a prime and r be an integer. In 1913 A. Fleck discovered that

$$\sum_{k \equiv q \pmod{p}} (-1)^k \binom{h}{k} \equiv 0 \left(\mod p^{\left\lfloor \frac{h-1}{p-1} \right\rfloor} \right) \qquad (12.9)$$

for all positive integers $h > 0$. In 1977 C. S. Weisman [42] extended Fleck's congruence to obtain

$$\sum_{k \equiv q \pmod{p^\alpha}} (-1)^k \binom{h}{k} \equiv 0 \left(\mod p^{\left\lfloor \frac{h-p^{\alpha-1}}{\phi(p^\alpha)} \right\rfloor} \right), \qquad (12.10)$$

where α, h are positive integers ≥ 0, $h \geq p^{\alpha-1}$ and ϕ denotes the Euler totient function. When $\alpha = 1$ it is clear that (12.10) reduces to (12.9). Much research is current in this area [11], [10], [39].

Using the theory developed so far, it can be shown that

$$b_q^{(-(2t+1))} = (-1)^{t+q} \, {}^{2t+1}C_{t+q} + \sum_{a=1}^{\infty} (-1)^{t+q+a} \left({}^{2t+1}C_{t+q-an} + {}^{2t+1}C_{t+q+an} \right), \qquad (12.11)$$

and

$$b_q^{(-2t)} = (-1)^{t+q} \, {}^{2t}C_{t+q} + \sum_{a=1}^{\infty} (-1)^{t+q+a} \left({}^{2t}C_{t+q-an} + {}^{2t}C_{t+q+an} \right). \qquad (12.12)$$

The right hand sides of (12.11) and (12.12) are just rearrangements of the left hand sides of Fleck's and Weisman's congruences. Hence, $b_q^{(-(2t+1))}$ and

$b_q^{(-(2t))}$ are just alternating lower index summations of the binomial coefficients over the residue class $t+q \pmod{n}$. It follows that when A_0 is of side length $n = 2m+1 = p^\alpha$, with p a prime, then for positive integer h we have

$$b_q^{(-h)} \equiv 0 \left(\bmod p^{\left\lfloor \frac{h-p^{\alpha-1}}{\phi(p^\alpha)} \right\rfloor} \right), \tag{12.13}$$

which, in ordinal notation, can be written as

$$\mathrm{Ord}_p\, b_q^{(-h)} \geq \left\lfloor \frac{h-p^{\alpha-1}}{\phi(p^\alpha)} \right\rfloor = F(p^\alpha, h). \tag{12.14}$$

When $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ is composite, these congruences do not in general seem to hold and it often appears to be the case that $\mathrm{Ord}_{p_i}\, b_q^{(-h)} = 0$. For simplicity we define $F(n,h) = 0$ when n is not a prime power.

Composite side length does not however seem to destroy the p-adic relations for the reduced coefficients of V_0^h. From (10.24) and (10.25) we can write the diagonal coefficients of V_0^h as $n^{h-1} b_q^{(h)}$, where by Lemma 11.3.2, we have

$$\mathrm{Ord}_{p_i}\, b_q^{(h)} \geq -\left\lfloor \frac{h}{p_i - 1} \right\rfloor = -G(p_i, h), \qquad 1 \leq i \leq r. \tag{12.15}$$

Combining (12.14) and (12.15) when $n = p^\alpha$ we have

$$\mathrm{Ord}_p\, b_q^{(-h)} b_q^{(h)} \geq \left\lfloor \frac{h-p^{\alpha-1}}{\phi(p^\alpha)} \right\rfloor - \left\lfloor \frac{h}{p-1} \right\rfloor, \tag{12.16}$$

and when $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ is composite then

$$\mathrm{Ord}_{p_i}\, b_q^{(-h)} b_q^{(h)} \geq -\left\lfloor \frac{h}{p_i - 1} \right\rfloor, \qquad 1 \leq i \leq r. \tag{12.17}$$

Experimentally it often seems to be the case that the inequality signs in (12.16) and (12.17) can be replaced with equality signs.

Determinants can also be used to display the symmetry that exists between the $b_q^{(h)}$. For example, ignoring sign, the $r \times r$ determinant

$$\begin{vmatrix} b_1^{(1)} & b_1^{(2)} & b_1^{(3)} & \ldots & b_1^{(r)} \\ b_2^{(1)} & b_2^{(2)} & b_2^{(3)} & \ldots & b_2^{(r)} \\ b_3^{(1)} & b_3^{(2)} & b_3^{(3)} & \ldots & b_3^{(r)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{r-1}^{(1)} & b_{r-1}^{(2)} & b_{r-1}^{(3)} & \ldots & b_{r-1}^{(r)} \\ b_r^{(1)} & b_r^{(2)} & b_r^{(3)} & \ldots & b_r^{(r)} \end{vmatrix}, \tag{12.18}$$

appears to give the symmetric result

$$\frac{m(m-1)(m-2)\dots(m-k+1)}{k!}\cdot\frac{(2m-1)(2m-3)\dots(2m-(2k-1))}{(2k+1)!!},$$

when $r=2k$ is even, and

$$\frac{m(m-1)(m-2)\dots(m-k)}{(k+1)!}\cdot\frac{(2m-1)(2m-3)\dots(2m-(2k-1))}{(2k+1)!!}$$

when $r=2k+1$ is odd.

Considering determinants constructed from either odd or even power diagonal coefficients is also quite illuminating. We give the odd power example. Let $d(r,0)$ be the $r\times r$ determinant defined such that

$$d(r,0)=\begin{vmatrix} b_1^{(1)} & b_1^{(3)} & b_1^{(5)} & \dots & b_1^{(2r-1)} \\ b_2^{(1)} & b_2^{(3)} & b_2^{(5)} & \dots & b_2^{(2r-1)} \\ b_3^{(1)} & b_3^{(3)} & b_3^{(5)} & \dots & b_3^{(2r-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{r-1}^{(1)} & b_{r-1}^{(3)} & b_{r-1}^{(5)} & \dots & b_{r-1}^{(2r-1)} \\ b_r^{(1)} & b_r^{(3)} & b_r^{(5)} & \dots & b_r^{(2r-1)} \end{vmatrix}. \tag{12.19}$$

Then, ignoring sign, we seem to have

$$\begin{aligned} d(r,0)=&\frac{m}{1}\frac{(m-1)^2}{2^2}\frac{(m-2)^3}{3^3}\cdots\frac{(m-k+1)^k}{k^k}\frac{(m-k)^k}{(k+1)^k}\frac{(m-k-1)^{k-1}}{(k+2)^{k-1}}\cdots \\ &\cdots\frac{(m-(r-2))^2}{(r-1)^2}\frac{(m-(r-1))}{r}\times\frac{(2m-1)}{3}\frac{(2m-3)^2}{5^2}\frac{(2m-5)^3}{7^3}\cdots \\ &\cdots\frac{(2m-(2k-3))^{k-1}}{(2k-1)^{k-1}}\frac{(2m-(2k-1))^k}{(2k+1)^k}\frac{(2m-(2k+1))^{k-1}}{(2k+3)^{k-1}} \\ &\cdots\frac{(2m-(2r-5))^2}{(2r-3)^2}\frac{(2m-(2r-3))}{(2r-1)}, \end{aligned} \tag{12.20}$$

when $r=2k$ is even, and

$$d(r,0)=\frac{m}{1}\frac{(m-1)^2}{2^2}\frac{(m-2)^3}{3^3}\cdots\frac{(m-k+1)^k}{k^k}\frac{(m-k)^{k+1}}{(k+1)^{k+1}}\frac{(m-k-1)^k}{(k+2)^k}\cdots$$

$$\cdots \frac{(m-(r-2))^2}{(r-1)^2}\frac{(m-(r-1))}{r} \times \frac{(2m-1)}{3}\frac{(2m-3)^2}{5^2}\frac{(2m-5)^3}{7^3}\cdots$$
$$\cdots \frac{(2m-(2k-3))^{k-1}}{(2k-1)^{k-1}}\frac{(2m-(2k-1))^k}{(2k+1)^k}\frac{(2m-(2k+1))^{k-1}}{(2k+3)^{k-1}}$$
$$\cdots \frac{(2m-(2r-5))^2}{(2r-3)^2}\frac{(2m-(2r-3))}{(2r-1)}, \tag{12.21}$$

when $r = 2k+1$ is odd.

Let s be and integer and define $d(r,s)$ such that

$$d(r,s) = \begin{vmatrix} b_1^{(1+2s)} & b_1^{(3+2s)} & b_1^{(5+2s)} & \cdots & b_1^{(2r-1+2s)} \\ b_2^{(1+2s)} & b_2^{(3+2s)} & b_2^{(5+2s)} & \cdots & b_2^{(2r-1+2s)} \\ b_3^{(1+s)} & b_3^{(3+s)} & b_3^{(5+s)} & \cdots & b_3^{(2r-1+s)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{r-1}^{(1+2s)} & b_{r-1}^{(3+2s)} & b_{r-1}^{(5+2s)} & \cdots & b_{r-1}^{(2r-1+2s)} \\ b_r^{(1+2s)} & b_r^{(3+2s)} & b_r^{(5+2s)} & \cdots & b_r^{(2r-1+2s)} \end{vmatrix}. \tag{12.22}$$

Then for $r > |s|$ with s negative (ignoring determinant sign) we seem to have

$$d(r,s) = \underset{m\to m-s}{d(r-s,0)},$$

and for $r \geq s$ with s positive (ignoring determinant sign) we seem to have

$$d(r,s) = \frac{1}{(2m+1)^s}\underset{m\to m+s}{d(r+s,0)},$$

where $d(r-s,0)_{m\to m-s}$ means that we consider the $(r-s)\times(r-s)$ determinant defined in (12.19), with m replaced with $m-s$ in either of (12.20) or (12.21), depending on the parity of r.

The idea for the above determinants stemmed from M. N. Huxley's Determinant Mean Value Theorem that appears in an appendix to the paper *Integer points in a plane curve* [23].

Observations on Residues of $b_q^{(-h)}$ and $b_q^{(h)}$ modulo n

For any integer n, the diagonal coefficients $b_q^{(-h)}$ of our $n \times n$ square A_0^t,

correspond to the numbers in the left hand side summation of Fleck's and Weisman's congruences. That is, when $h = 2t + 1$, then

$$b_q^{(-(2t+1))} = \sum_{k \equiv t+q \pmod{n}} (-1)^k \binom{2t+1}{k},$$

and similarly for $h = 2t$.

It appears to be the case that the $n = 2m + 1$ numbers

$$n^{-F(n,h)} \left(b_1^{(-h)}, b_2^{(-h)}, \ldots, b_{m-1}^{(-h)}, b_m^{(-h)}, 0, -b_m^{(-h)}, -b_{m-1}^{(-h)}, \ldots, -b_2^{(-h)}, -b_1^{(-h)} \right)$$

are only congruent to all n residues modulo n when n is a prime $p \geq 3$ and either the power $h = p$, or $h = k \times \phi(p) - 1$, for some integer $k \geq 1$. Moreover, it also seems to be true that when $h = k \times \phi(p) - 1$, then

$$p^{-F(p,h)} \left(b_1^{(-h)}, b_2^{(-h)}, \ldots, b_{m-1}^{(-h)}, b_m^{(-h)}, 0, -b_m^{(-h)}, -b_{m-1}^{(-h)}, \ldots, -b_2^{(-h)}, -b_1^{(-h)} \right)$$

$$\equiv (-1)^k (m, m-1, \ldots, 2, 1, 0, -1, -2, \ldots, -(m-1), -m) \pmod{p}, \tag{12.23}$$

and when $h = k \times \phi(p)$, then

$$p^{-F(p,h)} \left(b_1^{(-h)}, b_2^{(-h)}, \ldots, b_m^{(-h)}, b_0^{(-h)}, -b_m^{(-h)}, \ldots, -b_2^{(-h)}, -b_1^{(-h)} \right)$$

$$\equiv (-1)^{k-1} (1, 1, \ldots, 1, 1, 1, \ldots, 1, 1) \pmod{p}. \tag{12.24}$$

For $n = p^\alpha$ a prime power, with $\alpha \geq 2$, there do seem to exist symmetries modulo p but not modulo n.

Turning our attention now to the diagonal coefficients $b_q^{(h)}$, in the $n \times n$ square V_0^h, we again look for symmetries modulo n that are either all different or all equal. For n a prime p, and $h = k \times \phi(p)$, we also seem to have the congruence (12.24) but with the $b_q^{(-h)}$ replaced with $b_q^{(h)}$ and with $F(p,h)$ replaced with $-G(p,h)$. The congruence in (12.23) also appears to hold with these replacements, but this time for values of $h = k \times \phi(p) + 1$.

For $n = p^\alpha$ a prime power, with $\alpha \geq 2$, there again seem to exist symmetries modulo p but not modulo n.

The final observation on such congruences concerns square free $n = 2m + 1$. Let $n = p_1 p_2 \ldots p_r$ be square free, where the p_i are the odd prime factors of n, and let

$$w(n) = \phi(p_1)\phi(p_2)\ldots\phi(p_r).$$

Then for $h = k \times w(n) + 1$ we appear to have

$$p_1^{G(p_1,h)} p_2^{G(p_2,h)} \dots p_r^{G(p_r,h)}$$

$$\times \left(b_1^{(h)}, b_2^{(h)}, \dots, b_{m-1}^{(h)}, b_m^{(h)}, 0, -b_m^{(h)}, -b_{m-1}^{(h)}, \dots, -b_2^{(h)}, -b_1^{(h)} \right)$$

$$\equiv (m, m-1, \dots, 2, 1, 0, -1, -2, \dots, -(m-1), -m) \pmod{n}, \quad (12.25)$$

and when $h = k \times w(n)$, then

$$p_1^{G(p_1,h)} p_2^{G(p_2,h)} \dots p_r^{G(p_r,h)}$$

$$\times \left(b_1^{(h)}, b_2^{(h)}, \dots, b_{m-1}^{(h)}, b_m^{(h)}, b_0^{(h)}, -b_m^{(h)}, -b_{m-1}^{(h)}, \dots, -b_2^{(h)}, -b_1^{(h)} \right).$$

$$\equiv -(1, 1, \dots, 1, 1, 1, 1, 1, \dots, 1, 1) \pmod{n}. \quad (12.26)$$

For

$$v(n) = \text{LCM}\,(\phi(p_1), \phi(p_2), \dots \phi(p_r)) < w(n),$$

further symmetries appear to exist when $h = k \times v(n)$ and $h = k \times v(n) + 1$.

A final note considers some vector properties of the coefficients $b_q^{(h)}$. Taking into account that

$$V_0^h V_0^{-h} = I_n - \frac{1}{n} E, \quad (12.27)$$

we deduce that for $n = 2m + 1$ and $h = 2t + 1$ odd

$$\sum_{r=1}^{m} b_q^{(-h)} b_q^{(h)} = -m, \quad (12.28)$$

which is just the dot product of the two m dimensional vectors

$$(b_1^{(-h)}, \dots, b_m^{(-h)}), \qquad (b_1^{(h)}, \dots, b_m^{(h)}).$$

Let $\mathbf{x} = (b_1^{(-h)}, b_2^{(-h)}, \dots, b_m^{(-h)})$ and $\mathbf{y} = (b_1^{(h)}, b_2^{(h)}, \dots, b_m^{(h)})$. When equality holds in (12.16) and (12.17), and taking into account the prime powers already present in the vector entries, it is interesting to note that the dot product $\mathbf{x}.\mathbf{y}$ generates the prime powers

$$p^{\left\lfloor \frac{h}{p-1} \right\rfloor - \left\lfloor \frac{h - p^{\alpha-1}}{\phi(p^\alpha)} \right\rfloor} \qquad \text{or} \qquad p_i^{\left\lfloor \frac{h}{p_i - 1} \right\rfloor}, \qquad 1 \le i \le r,$$

depending on whether n is a prime power or composite. It is also interesting to note that for large values of h and n the rational vectors $\mathbf{x}$ and $\mathbf{y}$ are almost perpendicular.

If Weisman's congruence is one end of a fundamental relationship between binomial coefficients and prime numbers, then it may be the case that the $b_q^{(h)}$, formed from linear combinations of MCL determinants, are in fact the other end. Under this assumption they may well be worthy of further study.

August 2009.

Bibliography

[1] G. E. Andrews, *An asymptotic expression for the number of solutions of a general class of diophantine equation*, Trans. Amer. Math. Soc. 99, 1961, 272-277.

[2] G. E. Andrews, *A lower bound for the volume of strictly convex bodies with many boundary lattice points*, Trans. Amer. Math. Soc. 106, 1963, 270-279.

[3] W. S. Andrews, *Magic Squares and Cubes*, Dover, 1960.

[4] G. Averkov and M. Henk, *Respresenting simple d-dimensional polytopes by d polynomials*, arXiv:0709.2099v1, 2007.

[5] M. Beck et al, *Coefficients and Roots of Ehrhart Polynomials*, Contemporary Mathematics 374, Amer. Math. Soc. 2005, 15-35.

[6] M. Beck, and S. Robins, *Computing the Continuous Discretely*, Springer, Heidelberg, 2006.

[7] J. M. Borwein et al, *Computational strategies for the Riemann zeta function*, Journal of Computational and Applied Mathematics, 121, 2000, 247-296.

[8] M. Branton and P. Sargos, *Points entiers au voisinage d'une courbe plane á trés faible courbure*, Bull. Sci. Math. 118, 1994, 15-28.

[9] J. Chernick, *Solution of the general magic square*, Amer. Math. Monthly, 45, 1938, 172-175.

[10] H. Q. Cao and H. Pan, *Congruences on Stirling numbers and Eulerian numbers*, arXiv:math/0608564v2, 2006.

[11] D. M. Davis and Z. W. Sun, *Combinatorial congruences modulo prime powers*, Trans. Amer. Math. Soc. (11) 359, 2007, 5525-5553.

[12] L. E. Dickson, *History of the Theory of Numbers*, Vol I, AMS, Chelsea Publ., 1999.

[13] A. V. Den Essen, *Magic squares and linear algebra*, Amer. Math. Monthly, (1) 97, 1990, 60-62.

[14] M. Filaseta and O. Trifonov, *The distribution of fractional parts with applications to gap results in number theory*, Proc. London. Math. Soc. (3) 73, 1996, 241-278.

[15] R. L. Graham, D. E. Knuth and O. Patshnik, *Concrete Mathematics*, Addison Wesley, 1989.

[16] E. Grosswald, *Representations of Integer as Sums of Squares*, Springer-Verlag, 1985.

[17] P. M. Gruber, and C. G. Lekkerkerker, *Geometry of Numbers*, North-Holland Mathematical Library, 1987.

[18] J. Guyker, *A magic decomposition*, International Journal of Mathematical Education in Science and Technology, 33, 2002, 272-276.

[19] J. Guyker, *Magic squares with magic inverses*, International Journal of Mathematical Education in Science and Technology, (5) 38, 2007, 683-688.

[20] E. Hlawka, *Integrale auf konvexen Körpern*, Monatshefte Math. 54, 1950, 1-36, 81-99.

[21] M. N. Huxley, *Area, Lattice Points and Exponential Sums*, Oxford University Press, 1996.

[22] M. N. Huxley, *The integer points close to a curve III*, in: Number Theory in Progress, K. Győry et al (ed.), de Gruyter, Berlin, 1999, Vol II, 911-940.

[23] M. N. Huxley, *The integer points in a plane curve*, Funct. Approx. Comment. Math, (1) 37, 2007, 213-231.

[24] M. N. Huxley and P. Sargos, *Points entiers au voisinage d'une courbe plane de classe C^n II*, Functiones et Approximatio XXXV, 2006, 91-115.

[25] V. Jarník, *Über die Gitterpunkte auf konvexen Kurven*, Math. Zeitschrift 24, 1925, 500-518.

[26] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer 1984.

[27] E. Krätzel, *Analytische Funktionen in der Zahlentheorie*, Teubner, 2000, 200-243.

[28] R. V. Malderens, *Non-recursive expressions for even index Bernoulli numbers: A remarkable sequence of determinants*, arXiv:math/0505437v1, 2005.

[29] G. Martin, *The limiting curve of Jarník's polygons*, arXiv:math/0206168v1, 2002.

[30] P. McMullen and G. C. Shephard, *Convex Polytopes and the Upper Bound Conjecture*, London. Math. Soc. Lecture Note Series 3, Cambridge University Press, 1971.

[31] P. McMullen, *The maximum number of faces of a convex polytope*, Mathematika 17, 1970, 179-184.

[32] S. Moore, *The Trigrams of Han*, The Aquarian Press, 1989.

[33] W. Müller, *Lattice points in large convex bodies*, Monatsh. Math. 128, 1999, 315-330.

[34] A. W. Nutbourne and R. R. Martin, *Differential Geometry applied to Curve and Surface Design*, Ellis Horwood, 1988.

[35] K. Ollerenshaw and D. Brée, *Most-Perfect Pandiagonal Magic Squares*, The Institute of Mathematics and its Applications, 1998.

[36] L. J. Ratcliff Jr, *The dimension of the magic square vector space*, Amer. Math. Monthly, (9) 66, 1959, 793-795.

[37] W. Schwarz and J. Spilker, *Arithmetic Functions*, London. Math. Soc. Lecture Note Series 184, Cambridge University Press, 1994.

[38] D. M. Y. Sommerville, *An Introduction to the Geometry of N Dimensions*, Methuen, London, 1929.

[39] Z. W. Sun, *Polynomial extensions of Fleck's congruence*, Acta Arith. (1) 122, 2006, 91-100.

[40] A. C. Thompson, *Odd magic powers*, Amer. Math. Monthly, (4) 101, 1994, 339-342.

[41] R. S. Underwood, *An expression for the summation* $\sum_{m=1}^{n} m^p$, Amer. Math Monthly (8) 35, 1928, 424-428.

[42] C. S. Weisman, *Some congruences for binomial coefficients*, Michigan Math. J. 24, 1977, 141-151.

[43] S. C. Woon, *Analytic continuation of Bernoulli numbers, a new formula for the Riemann Zeta Function, and the phenomenon of scattering of zeros*, arXiv:physics/9705021v2, 1997.