UNIVERSITY OF CALIFORNIA, SAN DIEGO

Magic square subclasses as linear Diophantine systems

A dissertation submitted in partial satisfaction of the
requirements for the degree
Doctor of Philosophy

in

Mathematics

by

Ezra Q. Halleck

Committee in charge:

Professor Adriano M. Garsia, Chair
Professor Mark Haiman
Professor Jeffrey B. Remmel
Professor Walter A. Burkhard
Professor S. Gill Williamson

2000

To my dears,
Kenia and Solmaria

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

Thanks to the UCSD Mathematics Department for all its support during my 12 years in San Diego. My mentor, Adriano Garsia, has an unmatched passion for life in general and for mathematics in particular. He dedicated many computer explorations and summer beach sessions to my project, particularly in 1993 and 1997.

In my first two years, Audrey Terras's and Carl FitzGerald's courses in applied algebra and complex analysis, respectively, were perfect introductions to graduate-level mathematics. By my third year, Adriano's elementary approach to deep mathematics had convinced me to study algebraic combinatorics.

Jeff Remmel showed me the art of proof and the patience needed to grapple with a subject. Mark Haiman situated material in and used tools of a more abstract nature. Among junior faculty, Glenn Tesler spent considerable time with me, both in and out of school. In particular, Chapter 6 and Chapter 12 were joint projects. As for graduate students, the patience of Will Brockman and Joe Alfano were matched only by their eagerness to help me.

In May 1997, I mentioned to Lynn Butler my interest in linear Diophantine equations. She introduced me to Joshua Levenberg, then a graduate student at Berkeley, who had written, under the tutelage of Tom Roby, an undergraduate thesis[Lev94] on magic squares. His thesis stimulated my own investigation of this topic.

In October 1997, I began employment at the San Diego Supercomputer Center and have enjoyed both the company of coworkers and the excellent computer facilities. Thanks to Rachel Chrisman and all the machine room operators, technicians and engineers, who gave much encouragement to my endeavor.

Adriano introduced me to Sicilian and Tunisian cooking and several of the dishes he taught me kept my family's palette satisfied between sumptuous dinner parties given by Diane Favreau and Adriano and Mark. Hans Wenzl and Mark, as well as Peter Teichner and Wendy Greene on occasion, softened my 17 year exile from winter with mad dashes to melting snow in the local mountains.

On the family side, both sets of parents have been supportive in seeing me through this project. To my dears, wife Kenia and daughter Solmaria, thanks for your graceful adaptation to lean times, and your support in all its facets, without which, success would never have come.

VITA

June 17, 1962	Born, New York, New York
1980	High School Diploma, Trinity School, New York
1980–1983	Student, University of Wisconsin at Madison
1985–1988	Teacher, American-Nicaraguan School, Managua
1989	B. A., University of Wisconsin at Madison
1988–1995	Teaching assistant, Depts. of Mathematics and Computer Science, University of California, San Diego
1991	M. A., University of California, San Diego
1995	Lecturer, Department of Mathematics and Computer Science, University of San Diego
1996	Lecturer, Department of Mathematics, San Diego City College
1997	Student Associate, Mathematical Sciences Research Institute, Berkeley
1997–2000	Computer Operator, San Diego Supercomputer Center
1998	Lecturer, Department of Computer Science, University of California, San Diego
2000	Ph. D., University of California, San Diego

ABSTRACT OF THE DISSERTATION

Magic square subclasses as linear Diophantine systems

by

Ezra Q. Halleck
Doctor of Philosophy in Mathematics

University of California San Diego, 2000

Professor Adriano M. Garsia, Chair

The solution space of a system of linear homogeneous equations with integer coefficients over the integers is a $\mathbb{Z}$-module. Geometrically, the solutions form a lattice, the integral points in a subspace of $\mathbb{Q}^n$. Magic squares are $n \times n$ matrices with equal row and column sums; a basis consists of a subset of the permutation matrices. Pandiagonal squares or P-squares are magic squares with equal broken diagonal sums; we show that a basis consists of a subset of "octagons", introduced by [And60].

Requiring the solutions of a system of equations to be nonnegative as well as integral earns the modifier *Diophantine*. Geometrically, such a Diophantine set consists of the integral points of a pointed convex polyhedral cone: the intersection of the non-Diophantine lattice of integer solutions with the n-dimensional generalization of the nonnegative octant.

Take each solution of a Diophantine set $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ and form the monomial $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$. The formal power series in n variables formed by summing all such monomials is a rational function [Sta86, Section 4.6].

The solutions appearing in the denominators of a generating function are *extreme* or *completely fundamental* solutions. There is a one-to-one correspondence between these solutions and the extreme rays emanating from the point of the cone.

For magic squares, the extreme solutions are the $n \times n$ permutation matrices, but the generating function of solutions is unknown in full generality. For P-squares, even the extreme points are unknown. Our computer investigations have yielded the extreme points for pandiagonal systems for all $n \leq 7$.

Our investigation has included other Diophantine sets of matrices, including W-squares. We have the generating function for one subclass of P-squares, the linear span

of cyclic matrices.

To decompose a matrix from a magic square subclass, extract as large a copy as possible of J, the matrix of 1's. The residue is a square on the boundary of the cone. We decompose the boundary by looking at a cross section polytope.

The ability to immediately move to the boundary is related to the fact that the associated Diophantine ring is Gorenstein.

Chapter 1

Linear homogeneous Diophantine systems and polyhedral cones

1.1 Linear homogeneous Diophantine systems

The solutions of an equation or inequality in n variables are sequences of length n or *n-tuples.* The ith element in the sequence is known as the *ith component.* The adjective *Diophantine* is applied to any relation if the solution space is restricted to n-tuples with *nonnegative, integer* components. We are interested in linear homogeneous Diophantine equalities (Diophantine equalities) and nonstrict inequalities (Diophantine inequalities).

Proposition 1.1.1. *Systems of Diophantine equalities and inequalities are enumeratively equivalent.*

Proof. Transform the inequality to an equality by placing a new variable, the *slack* variable, on the side which is smaller. For instance, given $3x + 4y \geq 2z$, introduce the variable w to get $3x + 4y = 2z + w$. Enumerate the solutions to this equality and then ignore the w component of these solutions.

Conversely, given an equality, we can replace it with a pair of inequalities, e.g., $3x + 4y = 2z + 5w$ is equivalent to

$$3x + 4y \geq 2z + 5w$$
$$3x + 4y \leq 2z + 5w.$$

□

Definition 1.1.2. A *linear homogeneous Diophantine system* (Diophantine system) is a Diophantine system of equations and/or nonstrict inequalities whose *coefficients are integers.*

We do not exclude from consideration an equation or inequality with rational coefficients, just multiply by a common denominator.

Remark 1.1.3. Given a Diophantine system $Ax = 0$, the set of solutions, E, forms a (commutative) *monoid* (semigroup with identity) under the operation of component-wise addition. $\underbrace{(0, 0, \ldots .0)}_{n}$ serves as the identity element.

1.2 The Cone of Solutions

The solutions to a Diophantine system form a pointed convex polyhedral cone, the point or *apex* being the origin. We can project a cone onto the linear space that it spans. For example, the solutions for $4x + y = 2z$, lie in 3-space, but span a 2-dimensional subspace (Figure 1.1).

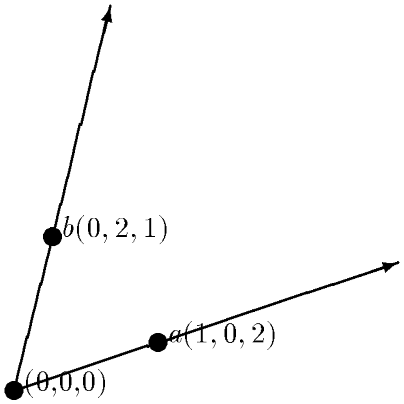


Figure 1.1: cone ab associated with $4x + y = 2z$.

More precisely, the solutions are the integral points inside the cone, as illustrated in Figure 1.2. For nonhomogeneous systems, the solution space is the Minkowski sum of a cone and a polytope [Zie95, p.28].

Given a vector j, the set of nonnegative scalar multiples of j that are integral points is

$$\text{ray}\, J = (\mathbb{Q}^{+} j \cap \mathbb{Z}^{n}).$$

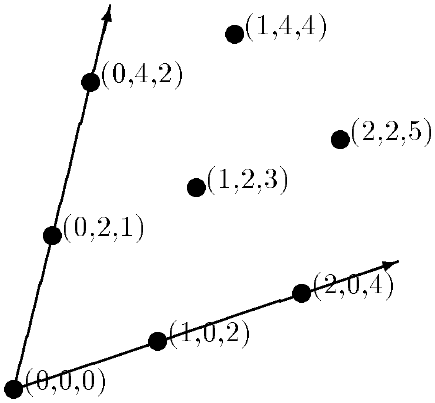


Figure 1.2: Solutions of $4x + y = 2z$ as integral points in a cone.

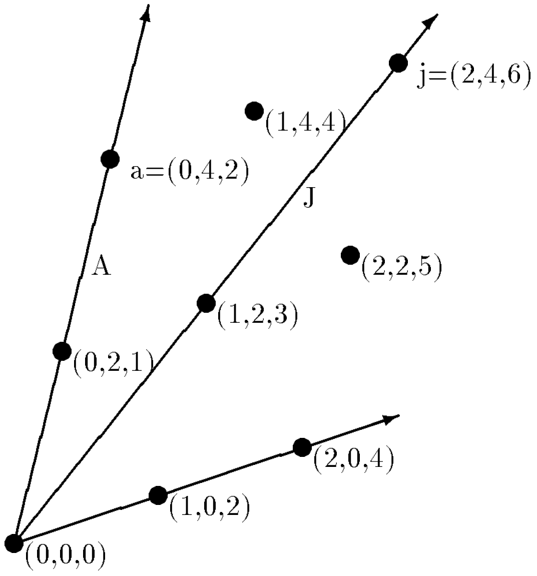


Figure 1.3: Two rays: A and J. Only A is extreme.

In Figure 1.3, ray $J = \{(0,0,0),(1,2,3),(2,4,6),(3,6,9),\dots\}$ is associated with $j = (2,4,6)$ and ray $A = \{(0,0,0),(0,2,1),(0,4,2),(0,6,4),\dots\}$ is with $a = (0,4,2)$. More generally, given a set of points S, the set of finite nonnegative combinations of elements from S that are integral points is the *positive hull*

$$\operatorname{pos} S = \{\sum_{j\in J} \lambda_j a_j \in \mathbb{Z}^n \mid a_j \in S,\ \lambda_j \in \mathbb{Q}^+, |J| < \infty\}.$$

Given a cone E, ray B is *extreme* if none of the nonzero elements in B can be expressed as a nonnegative combination of elements not in B, i.e., if $B \cap \operatorname{pos}(E \backslash B) = \{0\}$. In Figure 1.3, ray A is extreme—any solution not in the ray has a nonzero first coordinate—but ray J is not extreme—$(1,2,3) = (0,2,1) + (1,0,2)$. We will often refer to a cone by naming its extreme rays or points on the rays, e.g., the cone ab of Figure 1.1.

The elements of a minimal generating set for the monoid are *fundamental* solutions. As one travels from the origin along an extreme ray, the first integral point encountered is a *completely fundamental* solution. The set of completely fundamental solutions are not, in general, all the fundamental solutions. A finite number of additional solutions that are nonnegative rational (but not integral) combinations of the completely fundamental solutions may also be needed. For example, the completely fundamental solutions of $x + y = 2z$ are $(2,0,1)$ and $(0,2,1)$, but a generating set must also include $(1,1,1)$ (Figure 1.4). A minimal generating set is finite and unique [Sta86, Section 4.6].

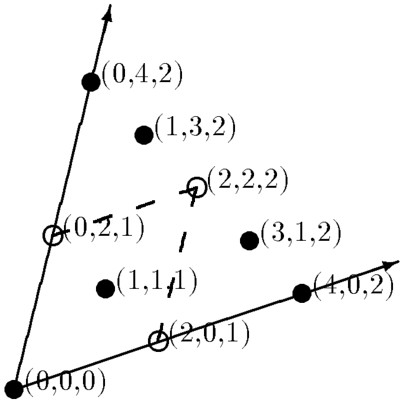


Figure 1.4: Cone of solutions for $x + y = 2z$.

1.3 The triangulation of a cone into simplexes

The solution space of $x + y = z + w$ spans a 3-dimensional subspace of $\mathbf{R}^4$ and a representation of its associated cone is drawn in Figure 1.5. A *simplicial cone*, or *simplex* for short, is a cone spanned by independent vectors $A_1, \ldots, A_n$. In Figure 1.5, cone ABC, and ray D are both simplexes, but cone $ABCD$ is not a simplex ($A + D = B + C$).

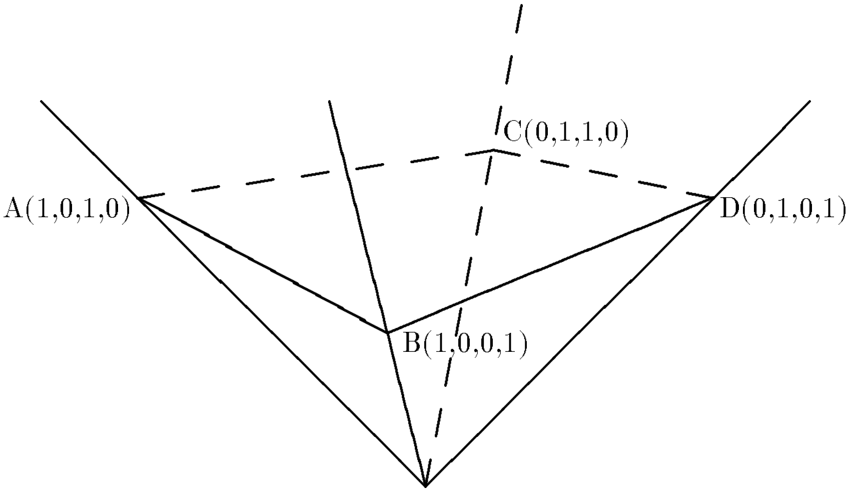


Figure 1.5: Cone associated with $x + y = z + w$.

Definition 1.3.1. A *triangulation* , of a cone C is a set of simplicial cones $\{\sigma_i\}$ such that:

1. $\bigcup_i \sigma_i = C$.

2. If $\sigma \in$, then every face of σ is in , .

3. If σ_i, $\sigma_j \in$, , then $\sigma_i \cap \sigma_j$ is a common face of σ_i and σ_j.

For $x + y = z + w$, we can divide the cone at the plane formed by the rays B and C. The division results in two 3-dimensional cones: ABC and BCD. The triangulation , is the set of these two cones, together with all their faces:

$$, = \{0, A, B, C, D, AB, AC, BC, CD, ABC, BCD\}.$$

1.4 The polytope associated with a cone

In the cone of Figure 1.5, there are 4 extreme rays. Take any plane which cuts through the cone, intersecting each of the extreme rays at a positive distance from the origin. The intersection of the plane and the cone is the *cross section* polytope. In our example, define the cutting plane by requiring the sum of the components to be equal to 2, then the cross section polytope is a polygon with vertices $a(1,0,1,0)$, $b(1,0,0,1)$, $c(0,1,1,0)$ and $d(0,1,0,1)$. Note that $\dim \operatorname{cone} ABCD = 3$ and $\dim \operatorname{quad} abcd = 2$, i.e., the dimension of the cross section polytope is one less than the cone. For another example, the cone of $x+y+z=v+w$ is 4-dimensional, but its polytope is a polyhedron—a prism with triangular base. In Figure 1.6, the commas have been dropped from the points for display purposes. For instance, vertex 01010 refers to the point $(0,1,0,1,0)$.

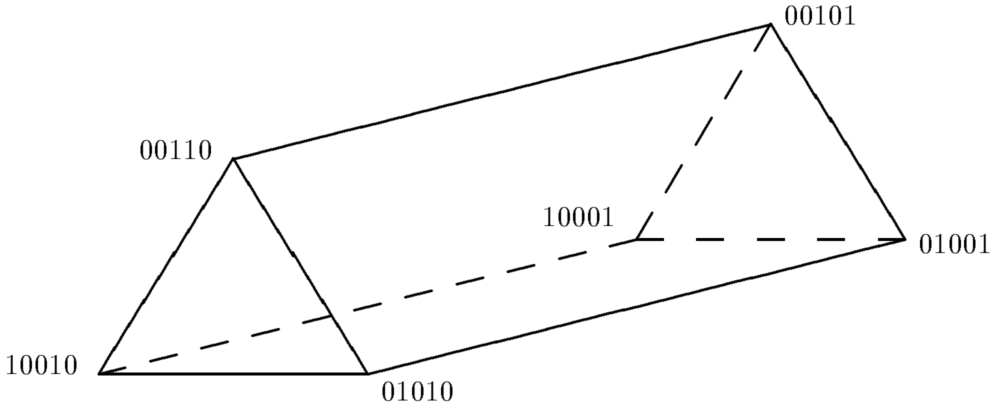


Figure 1.6: Cross section of the cone associated with $x+y+z=v+w$.

The original cone is the positive hull of its cross section polytope, e.g.,

$$\operatorname{cone} ABCD = \operatorname{pos} \operatorname{quad} abcd.$$

1.5 The generating function of solutions

One way to combinatorially decompose a Diophantine system with solution set E is to list or *enumerate* the solutions as a sum of monomials. The *monomial* of a solution $a=(a_1,a_2,\ldots,a_n)$ is $x^a = {x_1}^{a_1}{x_2}^{a_2}\cdots{x_n}^{a_n}$. Replacing each solution in E with its monomial, the *generating function*

$$E(x) = \sum_{a\in E} x^a.$$

For $x+y=z+w$,

$$E=\{(0,0,0,0),(1,0,1,0),(1,0,0,1),(0,1,1,0),(0,1,0,1),(2,0,1,1),\dots\}$$

and hence, $E(x)=1+x_1x_3+x_1x_4+x_2x_3+x_2x_4+{x_1}^2x_3x_4+\cdots$.

$E(x)$ is a rational function [Sta86, Theorem 4.6.11]. Two approaches for finding the rational function will be presented. Formal power series methods are used in the Elliott-MacMahon algorithm, for which a discussion and proof are given in Chapter 3. The *polytopal method* will be illustrated presently with our examples. For a more complete presentation see [Sta86, section 4.6].

For $4x+y=2z$ (Figure 1.1), the cone is a simplex with generating set the completely fundamental elements $a=(0,2,1)$ and $b=(1,0,2)$. Any solution is a unique, nonnegative, integer combination of a and b. Hence,

$$\begin{aligned}E(x)&=\sum_{(m,n)\in\mathbf{N}\times\mathbf{N}}x^{ma+nb}=\sum_{(m,n)\in\mathbf{N}\times\mathbf{N}}(x^a)^m(x^b)^n\\&=\sum_{(m,n)\in\mathbf{N}\times\mathbf{N}}({x_2}^2x_1)^m(x_1{x_3}^2)^n=\sum_{m=0}^{\infty}({x_2}^2x_1)^m\sum_{n=0}^{\infty}(x_1{x_3}^2)^n\\&=\frac{1}{1-{x_2}^2x_1}\,\frac{1}{1-x_1{x_3}^2}=\frac{1}{(1-x^a)(1-x^b)}.\end{aligned}$$

The generating function for a simplex E, with generating set the completely fundamental solutions $a_1,a_2,\dots,a_m$, is

$$E(\mathbf{x})=\frac{1}{(1-x^{a_1})(1-x^{a_2})\cdots(1-x^{a_m})}.$$

If there are fundamental solutions in addition to the completely fundamental ones, there is a nontrivial numerator, e.g., the generating function for $x+y=2z$ (Figure 1.4) is

$$E(x)=\frac{1+x_1x_2x_3}{(1-{x_2}^2x_1)(1-{x_1}^2x_3)}.$$

The monomials which appear are the integral points in the *fundamental domain* defined by the completely fundamental solutions, a half open parallelogram in this case. (A fundamental domain tiles the solution space with no overlap.)

For a non-simplicial example, the cone of $x+y=z+w$ has its cross section triangulated in Figure 1.7. Let the simplex $E_1=\operatorname{cone}abc$, the simplex $E_2=\operatorname{cone}bcd$ and the simplex $E_3=\operatorname{cone}bc$.

If we add the generating functions for E_1 and E_2, the solutions in their intersection are counted twice. Since the intersection is precisely the simplex E_3, an appropriate

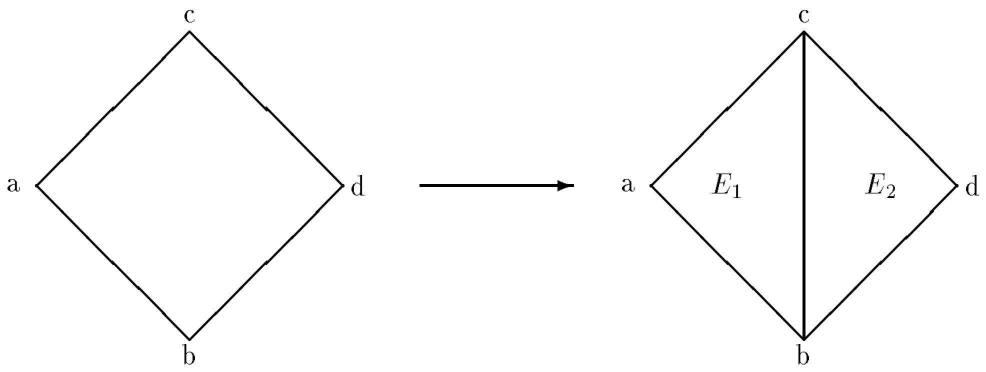


Figure 1.7: Triangulation of a cross section of pos $ABCD$.

subtraction compensates for the duplication.

$$\begin{aligned} E(\mathbf{x}) &= E_1(\mathbf{x}) + E_2(\mathbf{x}) - E_3(\mathbf{x}) \\ &= \frac{1}{(1-x^a)(1-x^b)(1-x^c)} + \frac{1}{(1-x^b)(1-x^c)(1-x^d)} - \frac{1}{(1-x^b)(1-x^c)}. \end{aligned}$$

Substitute $x^a = x_1x_3$, $x^b = x_1x_4$, $x^c = x_2x_3$ and $x^d = x_2x_4$, and simplify, to get

$$E(x) = \frac{1 - x_1x_2x_3x_4}{(1-x_1x_3)(1-x_1x_4)(1-x_2x_3)(1-x_2x_4)}. \tag{1.5.1}$$

In general, form the poset of the various simplexes of a triangulation , ordered by inclusion and adjoin a $\hat{1}$. By Mobius inversion [Sta86, p.225]

$$E(x) = -\sum_{\sigma\in\Gamma} \mu(\sigma, \hat{1}) E_\sigma(\mathbf{x}). \tag{1.5.2}$$

Let d be the dimension of E and let $\partial,$ be the simplexes on the boundary of E, then by [Sta86, p.224],

$$\mu(\sigma, \hat{1}) = \begin{cases} (-1)^{d-\dim(\sigma)+1} & \text{if } \sigma \in \, , \backslash \partial, \\ 0 & \text{if } \sigma \in \partial, \, . \end{cases} \tag{1.5.3}$$

The poset of our example is sketched in Figure 1.8. The only simplexes not on the boundary are $E_1 = \text{cone}\, ABC$, $E_2 = \text{cone}\, BCD$ and $E_3 = \text{cone}\, BC$. The Mobius function for the poset from an adjoined top element $\hat{1}$ is calculated using the formula of (1.5.3). For example,

$$\mu(E_1, \hat{1}) = (-1)^{d-\dim(E_1)+1} = (-1)^{3-3+1} = -1.$$

Similarly, $\mu(E_2, \hat{1}) = -1$, $\mu(E_3, \hat{1}) = 1$ and other values are 0 (Figure 1.9). Substituting

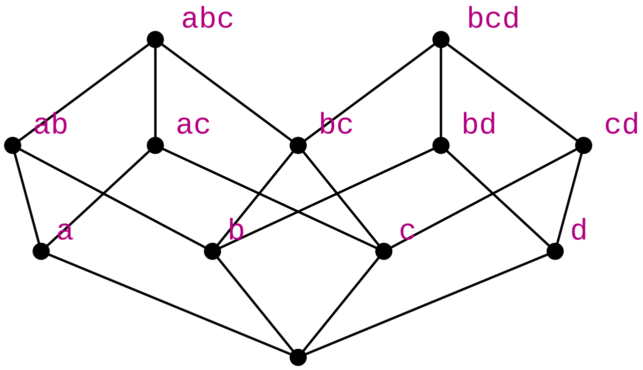


Figure 1.8: Poset of triangulation for $x + y = z + w$.

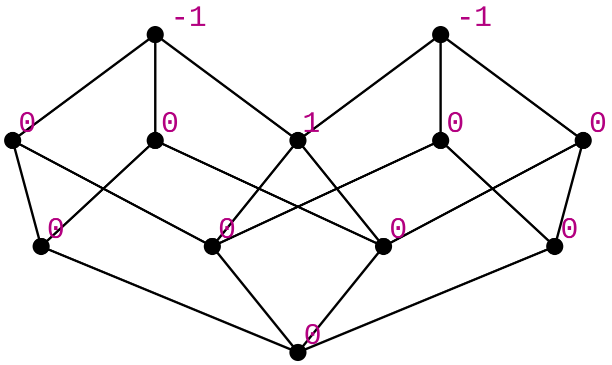


Figure 1.9: The Mobius function $\mu(x, \hat{1})$ for the poset of $x + y = z + w$.

into (1.5.2),

$$\begin{aligned} E(x) &= -\sum_{\sigma\in\Gamma} \mu(\sigma,\hat{1})E_\sigma(\mathbf{x}) \\ &= -\sum_{\sigma\in\Gamma\setminus\partial\Gamma} \mu(\sigma,\hat{1})E_\sigma(\mathbf{x}) \\ &= -\mu(E_1,\hat{1})E_1(\mathbf{x}) - \mu(E_2,\hat{1})E_2(\mathbf{x}) - \mu(E_3,\hat{1})E_3(\mathbf{x}) \\ &= E_1(\mathbf{x}) + E_2(\mathbf{x}) - E_3(\mathbf{x}), \end{aligned}$$

which we had obtained by a more direct reasoning.

Chapter 2

The Diophantine ring

2.1 Introduction

Given k, a field of characteristic 0, and E, the set of solutions to a Diophantine System, let $E_n = \{a \in E : \deg(a) = n\}$, where the degree of a solution is the sum of the components in the solution.

1. The *Diophantine Ring* associated with E is
$$R = k[x^a : a \in E].$$
2. The set of *monomials* of R is $M(R) = \{x^a : a \in E\}$. ($M(R)$ is a vector space basis of R.)
3. The set of monomials of degree n is $M_n(R) = \{x^a : a \in E_n\}$.
4. The *nth homogeneous subspace* of R is $H_n(R)$ = subspace of R spanned by $M_n(R)$.

The number of variables is finite. Hence, $dim(H_n(R)) = |M_n(R)|$ is finite. Thus, the *Hilbert series* of R

$$F_R(t) = \sum_{n \in N} t^n \dim(H_n(R))$$

is an element of the formal power series ring $k[[t]]$. $F_R(t)$ is the specialization of $E(x)$

$$F_R(t) = E(x)|_{x_1 \to t, \ldots, x_m \to t}.$$

Using (1.5.1), the Hilbert series for $x + y = z + w$ is

$$\begin{aligned} F_R(t) &= \left.\frac{1 - x_1x_2x_3x_4}{(1-x_1x_3)(1-x_1x_4)(1-x_2x_3)(1-x_2x_4)}\right|_{x_1 \to t, \ldots, x_4 \to t} \\ &= \frac{1-t^4}{(1-t^2)^4}. \end{aligned} \tag{2.1.1}$$

2.2 Basic systems and Cohen-Macaulay rings

A finitely generated, graded ring R is *Cohen-Macaulay* if there exists a set of homogeneous polynomials $B = \{\eta_1, \ldots, \eta_\ell; \theta_1, \ldots, \theta_m\}$ such that every $P \in R$ can be uniquely expressed as

$$P = \sum_{i=1}^{\ell} \eta_i P_i(\theta_1, \ldots, \theta_m) \quad ; \quad P_i \in k[x_1, \ldots, x_m].$$

B is called a *basic system.* Each η_i is a *separator* and each θ_i is a *generator.*

The ring R associated with a system of linear homogeneous Diophantine equations is known to be Cohen-Macaulay; the proof is non-constructive and uses deep tools of algebraic geometry. An algorithm for constructing a basic system for a particular R would constitute a combinatorial proof that R is Cohen-Macaulay. For the Diophantine ring R, there is a candidate for a natural set of generators. Our task is to construct an accompanying set of separators and show that together, they form a basic system.

We use our running example to introduce the natural candidates for generators and a construction of accompanying separators. Recall that the completely fundamental solutions are

$$\begin{aligned} a &= (1,0,1,0) \quad & b &= (1,0,0,1) \\ c &= (0,1,1,0) \quad & d &= (0,1,0,1). \end{aligned}$$

To simplify notation, we change variables

$$\begin{aligned} y_1 &= x^a = x_1x_3 \qquad & y_2 &= x^b = x_1x_4 \\ y_3 &= x^c = x_2x_3 \qquad & y_4 &= x^d = x_2x_4 \end{aligned}$$

and define a new ring $\hat{R} = k[y_1, \ldots, y_4]$. The sole relation $a + d = b + c = (1,1,1,1)$ becomes $y_1y_4 = y_2y_3$, so

$$\hat{R} = k[y_1, y_2, y_3, y_4]/(y_1y_4 - y_2y_3).$$

Using (2.1.1), the Hilbert series is

$$F_{\hat{R}}(t) = F_R(u)|_{u^2 \to t} = \left.\frac{1-u^4}{(1-u^2)^4}\right|_{u^2 \to t} = \frac{1-t^2}{(1-t)^4}. \tag{2.2.2}$$

Relabel the simplex poset arising from a triangulation , (Figure 1.8) using the variables of $\hat{R}$—replace a with y_1, b with y_2, etc— producing monomials organized by rank (Figure 2.1).

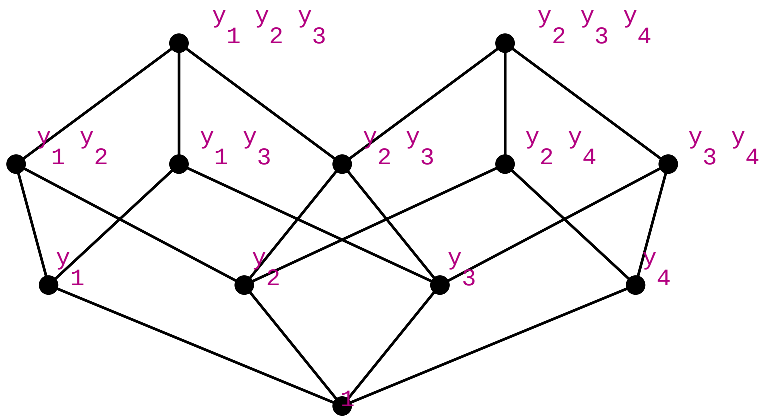


Figure 2.1: Rank row monomials for $x + y = z + w$.

Our natural set of generators are the sums of the monomials for each rank:

$$\psi_1 = y_1 + y_2 + y_3 + y_4$$

$$\psi_2 = y_1y_2 + y_1y_3 + y_2y_3 + y_2y_4 + y_3y_4$$

$$\psi_3 = y_1y_2y_3 + y_2y_3y_4.$$

Definition 2.2.1. A set of homogeneous polynomials $\{\theta_1, \theta_2, \ldots, \theta_m\}$ is a *homogeneous system of parameters* (h.s.o.p.) for R if

1. R has Krull dimension m;

2. $R/(\theta_1, \theta_2, \ldots, \theta_m)$ is a finite dimensional vector space.

For a Diophantine ring, the Krull dimension is the same as the dimension of the cone.

Proposition 2.2.2. *The following are equivalent:*

1. *R is Cohen-Macaulay;*

2. *there exists a system of parameters $\{\theta_1, \ldots, \theta_m\}$ such that*

$$F_R(t) = \frac{F_{R/(\theta_1,\ldots,\theta_m)}(t)}{(1-t^{d_1})\ldots(1-t^{d_m})} \qquad (d_i = \deg(\theta_i));$$

3. *for all system of parameters* $\{\theta_1, \ldots, \theta_m\}$,

$$F_R(t) = \frac{F_{R/(\theta_1,\ldots,\theta_m)}(t)}{(1-t^{d_1})\ldots(1-t^{d_m})} \qquad (d_i = \deg(\theta_i)).$$

See [Gar80, pp.232–233] for a proof.

Corollary 2.2.3. *Given a h.s.o.p.* $\{\theta_1, \ldots, \theta_m\}$ *for a Cohen-Macaulay ring* R*, the set* $\{\eta_1, \ldots, \eta_\ell\}$ *is a* k*-basis for* $R/(\theta_1, \ldots, \theta_m)$ iff $\{\eta_1, \ldots, \eta_\ell; \theta_1, \ldots, \theta_m\}$ *is basic.*

Using a computer algebra system, such as Macaulay, we find that, for our running example, the rank monomial sums $\{\psi_1, \psi_2, \psi_3\}$ are indeed a system of parameters and that $F_{\hat{R}/(\psi_1,\psi_2,\psi_3)}(t) = 1 + 3t + 4t^2 + 3t^3 + t^4$. Hence,

$$\begin{aligned} \frac{F_{\hat{R}/(\psi_1,\psi_2,\psi_3)}(t)}{(1-t)(1-t^2)(1-t^3)} &= \frac{1+3t+4t^2+3t^3+t^4}{(1-t)(1-t^2)(1-t^3)} \\ &= \frac{(1+t)^2(1+t+t^2)}{(1-t)(1-t^2)(1-t^3)} \qquad (2.2.3) \\ &= \frac{1+t}{(1-t)^3} = \frac{1-t^2}{(1-t)^4} = F_{\hat{R}}(t) \end{aligned}$$

(the last equality from (2.2.2)) and by Proposition 2.2.2, the ring R of our running example is Cohen-Macaulay.

In Section 2.4, we will give a proof of the Cohen-Macaulayness for this example, independent of the computer data.

2.3 Accompanying separators for $x + y = z + w$

The first barycentric subdivision on a triangulated solution space proceeds in 2 steps.

1. For each simplex of the triangulation, the barycenter is marked with a point and labeled with the simplex (Figure 2.2).

2. A new simplex in the subdivision corresponds to a chain in the lattice of simplexes for the original triangulation. For instance, point a is contained in edge ac; $\{a, ac\}$ is an edge in the barycentric subdivision. Likewise, point $a \subseteq$ edge $ac \subseteq$ face abc; $\{a, ac, abc\}$ is a face in the subdivision (Figure 2.3).

A *shelling* of a simplicial complex is a linear ordering of the maximal simplexes so that the intersection of a simplex F_i with the previous simplexes is nonempty and is a

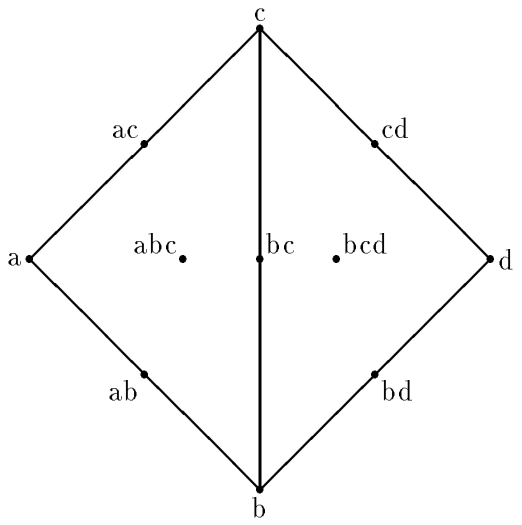


Figure 2.2: Simplex barycenters for a triangulation.

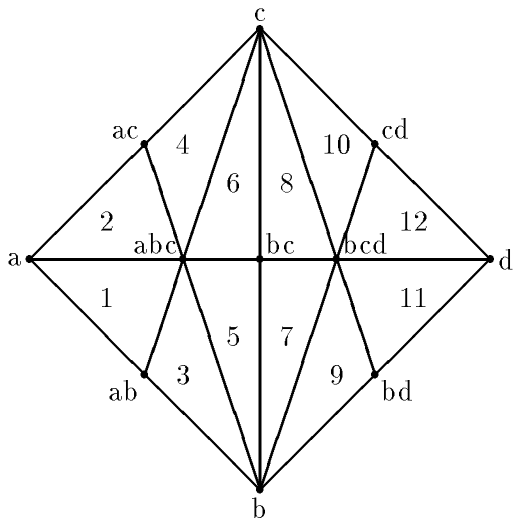


Figure 2.3: New simplexes in the first barycentric subdivision.

stage in a shelling of the boundary complex of F_i [Zie95, Definition 8.1]. In particular, the intersection must be connected and pure $d-1$-dimensional. In Figure 2.3, we have labeled the new faces with the numbers 1 to 12 to indicate a shelling. As the shelling proceeds, adjoin a maximal simplex i and collect the vertices needed to avoid any overlap with the previous simplexes into a set F_i. For instance when simplex 4 is adjoined, the edge $\{ac, abc\}$ is already in the existing union of simplexes; the vertex opposite this edge is c. Hence, $F_4 = \{c\}$. When simplex 6 is adjoined, the edges $\{c, abc\}$ and $\{bc, abc\}$ are already in the existing union of simplexes; the vertices opposite these edges are bc and c. Hence, $F_6 = \{c, bc\}$. The F_i are displayed in Table 2.1.

Simplex	Lists of Vertices F_i	Separator δ_i
1	$\emptyset$	1
2	ac	y_1y_3
3	b	y_2
4	c	y_3
5	bc	y_2y_3
6	c, bc	$y_3(y_2y_3)$
7	bcd	$y_2y_3y_4$
8	c, bcd	$y_3(y_2y_3y_4)$
9	bd	y_2y_4
10	cd	y_3y_4
11	d	y_4
12	d, cd	$y_4(y_3y_4)$

Table 2.1: For each simplex, lists of vertices F_i and associated monomial.

If mon(S) = monomial associated with S, for each simplex i, let

$$\delta_i = \prod_{S \in F_i} (\operatorname{mon} S), \quad \text{e.g.,}$$

$$\delta_6 = (\operatorname{mon} c)(\operatorname{mon} bc) = y_3(y_2y_3) = y_2{y_3}^2 \qquad \text{(see Table 2.1).}$$

In the case of the triangulation of a simplex, the monomials δ_i resulting from a shelling coincide with the descent monomials of its associated poset. We borrow the name from this case and call the δ_i *descent monomials.* The set of descent monomials, DM, is our candidate for the set of separators, which, by Corollary 2.2.3, can be established by showing that DM is a k-basis for $\hat{R}/(\psi_1, \psi_2, \psi_3)$. For the running example, we have grouped the descent monomials by degree in Table 2.2.

Degree	Monomials	# of Monomials
0	1	1
1	y_2, y_3, y_4	3
2	$y_1y_3, y_2y_3, y_2y_4, y_3y_4$	4
3	$y_2{y_3}^2, y_3{y_4}^2, y_2y_3y_4$	3
4	$y_2{y_3}^2y_4$	1

Table 2.2: Descent monomials for the square grouped by degree.

Let CM be the k-basis given by Macaulay. Recall that if C is a set of monomials, then $C_m = \{x \in C : \deg x = m\}$. For each n, we show that the monomials in DM_n are triangularly related to the monomials of CM_n. Note that all calculations are done modulo the ideal (ψ_1, ψ_2, ψ_3). For degrees 0 and 1 the sets are identical:

$$DM_0 = CM_0 = \{1\}$$
$$DM_1 = CM_1 = \{y_2, y_3, y_4\}.$$

For degree 2, the transition matrix between sets is

		CM_2			
		y_3y_4	y_2y_4	${y_4}^2$	${y_3}^2$
DM_2	y_3y_4	1			
	y_2y_4	0	1		
	y_2y_3	-1	-1	-1	
	y_1y_3	0	1	1	-1

,

e.g., line 3 results because

$$y_2y_3 \equiv -y_3y_4 - y_2y_4 - {y_4}^2 \mod (\psi_1, \psi_2, \psi_3).$$

For degree 3, the transition matrix is

		CM_3		
		$y_3{y_4}^2$	$y_2{y_4}^2$	${y_3}^2y_4$
DM_3	$y_3{y_4}^2$	1		
	$y_2y_3y_4$	-1	-1	
	$y_2{y_3}^2$	0	1	-1

.

For degree 4, $DM_4 = \{y_2{y_3}^2y_4\}$, $CM_4 = \{{y_3}^2{y_4}^2\}$ and

$$y_2{y_3}^2y_4 \equiv -{y_3}^2{y_4}^2 \mod (\psi_1, \psi_2, \psi_3).$$

In each case the transition matrices are invertible. Hence, the descent monomials are a k-basis for $\hat{R}/(\psi_1, \psi_2, \psi_3)$ and $\{\delta_1, \ldots, \delta_{12}; \psi_1, \psi_2, \psi_3\}$ is basic.

2.4 The Stanley-Reisner ring of the poset and a transfer of identities

Recall the poset of the triangulation , (Figure 1.8). For the Diophantine ring R or rather the isomorphic ring $\hat{R}$, variables correspond to each vertex of the cross section polytope. Each simplex becomes a product of variables. In contrast, here we create a new variable for each simplex, indexing to facilitate a ring homomorphism to the Diophantine ring, e.g., the simplex abc replaced in Figure 2.1 with $y_1y_2y_3$ is replaced with x_{123} (Figure 2.4). Variables x_a and x_b are *comparable* if the indices a and b are comparable in the face lattice, i.e., if a is contained in b, or vice versa. The *Stanley-Reisner ring* of a poset

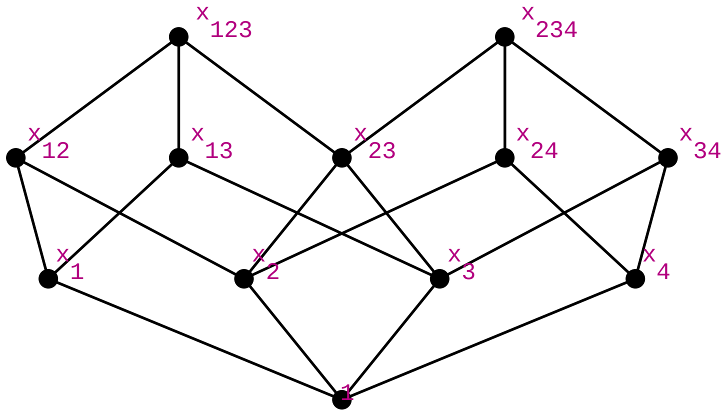


Figure 2.4: Variables of the Stanley-Reisner ring of the poset for $x + y = z + w$.

is

$$SR = k[x_1, x_2, \ldots, x_n]/J$$

where $J = (x_i x_j \mid x_i \text{ incomparable to } x_j)$. For the running example,

$$SR = k[x_1, \ldots, x_4, x_{12}, \ldots, x_{34}, x_{123}, x_{234}]/J \tag{2.4.4}$$

$$J = (x_1x_2, x_1x_3, x_1x_4, x_1x_{23}, x_1x_{24}, x_1x_{34}, x_1x_{234}, x_2x_3, x_2x_4, x_2x_{13}, \ldots, x_{123}x_{234}). \tag{2.4.5}$$

SR is known to be Cohen-Macaulay. The rank row monomial sums

$$\theta_1 = x_1 + x_2 + x_3 + x_4$$
$$\theta_2 = x_{12} + x_{13} + x_{23} + x_{24} + x_{34}$$
$$\theta_3 = x_{123} + x_{234}$$

are a set of generators and the descent monomials (Table 2.3) are an accompanying set of separators [Gar80, p.250]. Included in the cited material is an algorithm for expanding

i	Face Products F_i	SR-Separators ε_i	$\hat{R}$-Separators δ_i
1	1	1	1
2	ac	x_{13}	y_1y_3
3	b	x_2	y_2
4	c	x_3	y_3
5	bc	x_{23}	y_2y_3
6	c, bc	x_3x_{23}	$y_2{y_3}^2$
7	bcd	x_{234}	$y_2y_3y_4$
8	c, bcd	x_3x_{234}	$y_2{y_3}^2y_4$
9	bd	x_{24}	y_2y_4
10	cd	x_{34}	y_3y_4
11	d	x_4	y_4
12	d, cd	x_4x_{34}	$y_3{y_4}^2$

Table 2.3: Face lists and separators from the two rings.

SR monomials in terms of the basic system; some expansions of degree 3 monomials are

$$\begin{aligned} x_{123} &= \theta_3 - x_{234} \\ x_1 x_{13} &= x_{13}\theta_1 - x_3\theta_2 + x_3 x_{23} + x_{34}\theta_1 - x_4 x_{34} \\ {x_1}^3 &= {\theta_1}^2(\theta_1 - x_2 - x_3 - x_4). \end{aligned}$$

Define the map

$$\begin{aligned} \varphi : SR &\to \hat{R} \\ x_S &\mapsto \prod_{i \in S} y_i \end{aligned}$$

and extend so that φ is a ring homomorphism. For example $\varphi(x_2 x_{123}) = \phi(x_2)\varphi(x_{123}) = y_2(y_1 y_2 y_3)$. In particular, the known generators are mapped to the proposed generators and the known separators to the proposed separators:

$$\phi(\theta_i) = \psi_i \qquad \phi(\varepsilon_i) = \delta_i.$$

We transfer the expansions from SR to $\hat{R}$ by means of ϕ. Error terms are introduced, but we order the monomials so that error terms for each monomial are monomials which occur earlier in the ordering. Such an ordering is *transfer permitting.*

For the nth homogeneous subspace, form the error matrix A_n by defining a_{ij} to be the coefficient of the monomial j in the error terms for monomial i. An ordering is transfer permitting if A_n is lower triangular with zeros on the diagonal for every n.

Order the degree 3 monomials as in Figure 2.5. The abscissa of a pair of tableaux is the shape of the part of the monomial in y_1 and y_4. The ordinate is the shape of the part of the monomial in y_2 and y_3. We demonstrate with 2 expansions.

1. At the top shape is $y_1 y_2 y_3$.

   In SR, $x_{123} = \theta_3 - x_{234}$;

   in $\hat{R}$, $y_1 y_2 y_3 = \psi_3 - y_2 y_3 y_4$.

   The transfer of the expansion from SR involves no error.

2. From a shape later in the order is ${y_3}^2 y_4$.

   In SR, $x_3 x_{34} = x_{34}\theta_1 - x_4 x_{34}$;

   in $\hat{R}$, ${y_3}^2 y_4 = \overbrace{y_3 y_4 \psi_1 - y_4(y_3 y_4)}^{\text{from expansion in } SR} - \overbrace{y_2 {y_3}^2 - y_2 y_3 y_4}^{\text{error}}.$

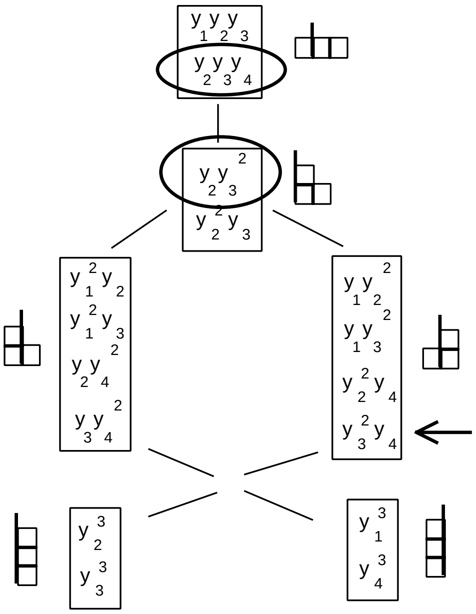


Figure 2.5: Ordering of $deg(3)$ monomials from $x + y = z + w$.

The monomial $y_3{}^2y_4$ is marked with an arrow in Figure 2.5. The error terms are circled and are of shapes which occur earlier in the order.

A similar ordering holds for degrees 0, 1, 2 and 4. Thus, in $\hat{R}$, all monomials of degree 4 or less can be expressed in terms of $\{\delta_1, \ldots, \delta_{12}; \psi_1, \psi_2, \psi_3\}$. Macaulay indicates that only monomials of deg(4) or less are in a k-basis. We can conclude that $\{\delta_1, \ldots, \delta_{12}\}$ is a k-basis for $\hat{R}/(\psi_1, \psi_2, \psi_3)$ independent of a direct comparison with the k-basis given by Macaulay. We are closer to our goal.

Proposition 2.4.1. *A spanning set $B = \{\varepsilon_1, \ldots, \varepsilon_\ell; \theta_1, \ldots, \theta_m\}$ is basic for R if and only if*

$$F_R(t) = \frac{\sum_j t^{\deg(\varepsilon_j)}}{(1 - t^{d_1}) \ldots (1 - t^{d_m})} \qquad (d_i = \deg(\theta_i)). \tag{2.4.6}$$

See [Gar80, p.232] for a proof.

We have shown that (2.4.6) is fulfilled in (2.2.3). Once shown that our proposed basic system spans all monomials, not just those of degree 4 or less, Proposition 2.4.1 gives us our goal.

For the degree 5 monomials, transfer the expansions from SR as before. The monomials of degree 5 can not be ordered so that the matrix of the error terms is lower triangular with zeros on the diagonal (see Figure 2.6). However, if we divide the error

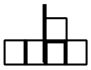
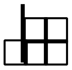
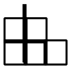
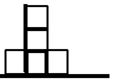
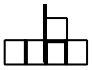
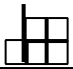
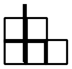
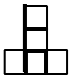
				
	*	*	*	*
	0	0	0	0
	*	0	0	0
	*	*	*	0

Figure 2.6: Matrix of error terms for the deg(5) monomials of $x + y = z + w$.

terms into two parts—the part which is 0 mod (ψ_1, ψ_2, ψ_3) and the part which is not—then the monomials can be ordered so that the matrix of the latter is lower triangular with zeros on the diagonal (see Figure 2.7). Let z be a degree 5 monomial and let $<$ be the ordering on degree 5 monomials. We assume that all monomials preceding z can be expanded in terms of the basic set.

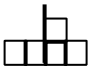
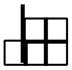
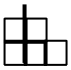
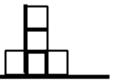
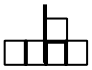
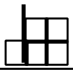
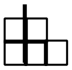
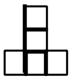
				
	0	0	0	0
	0	0	0	0
	*	0	0	0
	0	*	*	0

Figure 2.7: Matrix of error terms mod (ψ_1, ψ_2, ψ_3) for the deg(5) monomials.

$$\text{error terms of } z = \sum_{z_i < z} a_i z_i + \sum_j v_j \psi_j$$

a_i is an element of k. v_j is a polynomial of degree less than 5 and hence, can be expanded in terms of the basic system. By the induction assumption on the order of the monomials, z_i can be expanded. Thus, z can be expanded in terms of the basic set, which completes the induction step. As a consequence, since no separators have degree more than 4, all degree 5 monomials are 0 mod (ψ_1, ψ_2, ψ_3).

For $n > 5$, we induct on the degree of the polynomial, assuming all polynomials of lower degree can be expanded and all homogeneous polynomials of one degree less are $0 \mod (\psi_1, \psi_2, \psi_3)$. We can start with just a monomial. A degree n monomial z can be written as $y_i v$ where v is a monomial of degree $n - 1$. By assumption, $v = \sum_j p_j \psi_j$, where p_j is a polynomial and $\deg(p_j) < n - 1$. Multiplying the expression for v by y_i, $z = y_i v = \sum_j y_i p_j \psi_j$ where $\deg(y_i p_j) < 1 + (n - 1) = n$. By hypothesis, $y_i p_j$ can be expanded. Thus, z can be expanded in terms of the basic set and is $0 \mod (\psi_1, \psi_2, \psi_3)$, completing the induction step.

We have fulfilled our earlier promise of showing that $\hat{R}$ is Cohen-Macaulay independent of the data about a k-basis given by Macaulay, or even the data that $\{\psi_1, \psi_2, \psi_3\}$ is a system of parameters.

Chapter 3

The Elliott-MacMahon algorithm

3.1 The crude generating function $G(\mathbf{x}, \lambda)$

The *Elliott-MacMahon algorithm* (EMA) is a straightforward but computationally inefficient way to produce the generating function of solutions $E(\mathbf{x})$. Elliott treated the one equation case and informally proved its termination [Ell03]. MacMahon extended the algorithm to Diophantine systems of equations and inequalities [Mac60, Vol.2, Section VIII]. We present the algorithm for equations. The algorithm for inequalities requires only obvious modifications.

Given a system of equations, $Ay = 0$, where A is an l by n matrix, form the formal power series in the variables $\mathbf{x}, \lambda = x_1, \dots, x_n, \lambda_1, \dots, \lambda_m$

$$G(\mathbf{x}, \lambda) = \prod_{j=1}^{n} \frac{1}{1 - {\lambda_1}^{a_{1j}} {\lambda_2}^{a_{2j}} \cdots {\lambda_m}^{a_{mj}} x_j} = \prod_{j=1}^{n} \frac{1}{1 - \lambda^{A_j} x_j}$$

where A_j is the jth column of A. $G(\mathbf{x}, \lambda)$ is known as the *crude generating function* for the system of equations.

Example 3.1.1. For $3x = y + 5z$ which we rewrite as $3x - y - 5z = 0$,

$$G(\mathbf{x}, \lambda) = \frac{1}{(1 - \lambda^3 x)(1 - \lambda^{-1} y)(1 - \lambda^{-5} z)}$$

Example 3.1.2. For the system

$$\begin{aligned} x &= y + w \\ x + y + z &= 2v, \end{aligned}$$

$$G(\mathbf{x}, \lambda) = \frac{1}{(1 - \lambda\gamma x)(1 - \lambda^{-1}\gamma y)(1 - \gamma z)(1 - \gamma^{-2} v)(1 - \lambda^{-1} w)},$$

where $\lambda = (\lambda, \gamma)$.

Proposition 3.1.3.

$$E(\mathbf{x}) = G(\mathbf{x}, \lambda)|_{\lambda=\mathbf{0}}$$

Proof.

$$\begin{aligned} G(\mathbf{x}, \lambda) &= \left(\frac{1}{1-\lambda^{A_1}x_1}\right)\left(\frac{1}{1-\lambda^{A_2}x_2}\right)\cdots\left(\frac{1}{1-\lambda^{A_n}x_n}\right) \\ &= \sum_{b\in\mathbf{N}^n} (\lambda^{A_1}x_1)^{b_1}(\lambda^{A_2}x_2)^{b_2}\cdots(\lambda^{A_n}x_n)^{b_n} \\ &= \sum_{b\in\mathbf{N}^n} \lambda^{b_1A_1+b_2A_2+\cdots+b_nA_n}\mathbf{x}^b = \sum_{b\in\mathbf{N}^n} \lambda^{Ab}\mathbf{x}^b \end{aligned}$$

Restricting to the λ-free part, $\mathbf{x}^b$ will be in the new expression if and only if $Ab = 0$ □

3.2 The key identity and the ternary tree structure

The identity

$$\frac{1}{(1-x)(1-y)} = \frac{1}{(1-xy)}\left(\frac{1}{(1-x)} + \frac{1}{(1-y)} - 1\right) \tag{3.2.1}$$

is the basis of the algorithm.

We first consider the case of one equation which engenders one auxiliary variable λ. The algorithm will extract the part of the crude generating function which is λ-free. Let $\mathbf{E}$ be the multiset of nonzero exponents of λ, $\mathbf{E}^+$ the positive exponents and $\mathbf{E}^-$ the negative exponents. The algorithm has a ternary tree structure. At each node, the multiset $\mathbf{E}$ determines whether the node is an endpoint or whether there is a branching. We display the 4 cases and the actions taken in Table 3.1. Note from the table that a branching occurs iff both $\mathbf{E}^+$ and $\mathbf{E}^-$ are non-empty.

type	$\mathbf{E}^+$	$\mathbf{E}^-$	endpoint	action
1	empty	empty	yes	leave the expression as is
2	empty	non-empty	yes	set the factors with λ to 1
3	non-empty	empty	yes	set the factors with λ to 1
4	non-empty	non-empty	no	apply partial expansion

Table 3.1: Cases and actions to be taken at one node.

Let M and m be the maximum and minimum of $\mathbf{E}$, respectively (or one of them if it has several). Apply (3.2.1) to the expression

$$\frac{1}{(1-*\lambda^{M})(1-*\lambda^{m})}$$

and separate into the three terms:

$$\frac{1}{(1-*\lambda^{M+m})(1-*\lambda^{M})} \qquad \frac{1}{(1-*\lambda^{M+m})(1-*\lambda^{m})} \qquad \frac{-1}{(1-*\lambda^{M+m})}$$

Combining what had remained of the original expression with each of these three expressions, we have three new problems that are 'simpler' in a way that we explain in the proof of the algorithm's termination. Apply the decision Table 3.1 to each of the three new expressions. When the tree has been completed, the expressions from all the endpoints are summed to form the final expression. Some of the endpoints may be just a constant. If the system has l equations, there will be l auxiliary variables: $\{\lambda_1, \ldots, \lambda_l\}$. The algorithm proceeds by first extracting the part which is λ_1-free, then the part which is λ_2-free, etc.

For Example 3.1.1, the crude generating function $G(\mathbf{x}, \lambda) = 1/((1-\lambda^3 x)(1-\lambda^{-1}y)(1-\lambda^{-5}z))$. The multiset $\mathbf{E} = \{-5, -1, 3\}$ and the max/min elements $M = 3$, $m = -5$. Applying (3.2.1),

$$\frac{1}{(1-\lambda^3 x)(1-\lambda^{-5}z)} = \frac{1}{(1-\lambda^{-2}xz)}\left(\frac{1}{(1-\lambda^3 x)} + \frac{1}{(1-\lambda^{-5}z)} - 1\right)$$

The 3 children are

node	$\mathbf{E}_i^+$	$\mathbf{E}_i^-$	endpoint	action
2	$\{3\}$	$\{-2, -1\}$	no	apply (3.2.1)
30	$\{\}$	$\{-5, -2, -1\}$	yes	set the factors with λ to 1
31	$\{\}$	$\{-2, -1\}$	yes	set the factors with λ to 1

The node numbers refer to the node labels of the ternary tree displayed in Figure 3.1. The numbering reflects the order in which the nodes are created by a depth first implementation of the algorithm. In Figure 3.2, the nodes of the tree are labeled by the multiset, allowing for the reader to follow the algorithm directly on the tree. If the multiset is empty, the node is labeled with a zero.

Applying (3.2.1) to the first child ($a_1 = 3$, $b_1 = -2$),

$$\frac{1}{(1-\lambda^3 x)(1-\lambda^{-2}xz)} = \frac{1}{(1-\lambda x^2 z)}\left(\frac{1}{(1-\lambda^3 x)} + \frac{1}{(1-\lambda^{-2}xz)} - 1\right)$$

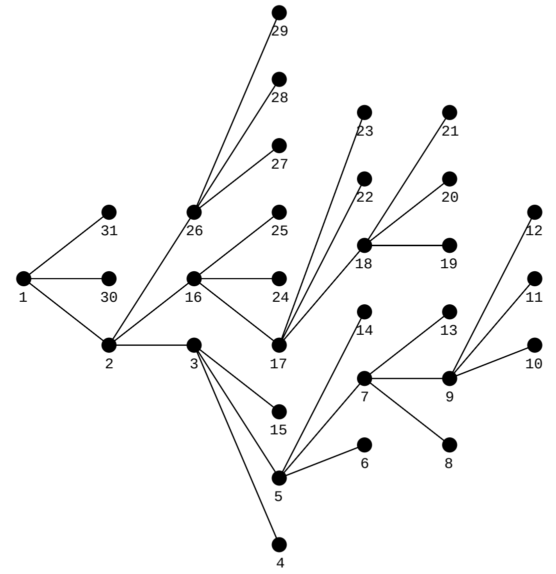


Figure 3.1: Tree with nodes numbered as they are created.

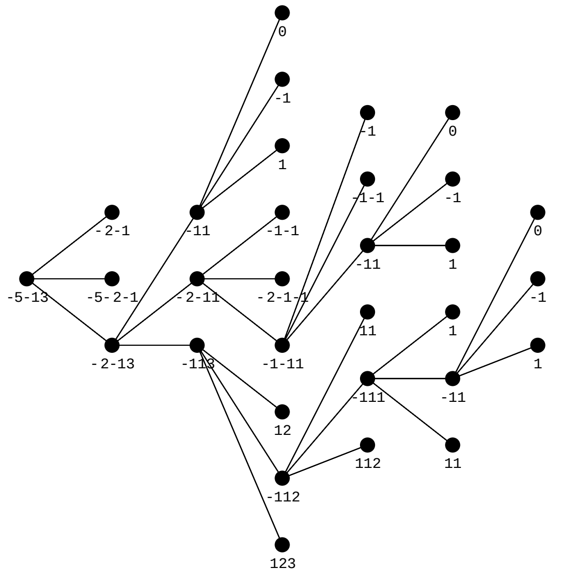


Figure 3.2: Tree with nodes labeled by the exponent multiset.

Its children (grandchildren of the original expression) are

node	$\mathbf{E}_{1i}^{+}$	$\mathbf{E}_{1i}^{-}$	endpoint	action
3	$\{1,3\}$	$\{-1\}$	no	apply (3.2.1)
16	$\{1\}$	$\{-2,-1\}$	no	apply (3.2.1)
26	$\{1\}$	$\{-1\}$	no	apply (3.2.1)

Combining the expressions corresponding to each endpoint and simplifying gives

$$E(\mathbf{x}) = \frac{1}{(1-xy^3)(1-x^2yz)} + \frac{1}{(1-x^5z^3)(1-x^2yz)} - \frac{1}{(1-x^2yz)}$$

3.3 Termination and an upper bound for a single equation

Theorem 3.3.1. *The Elliott-MacMahon algorithm terminates in a finite number of steps.*

Proof. Let $\mathbf{E}$ be multiset of exponents of λ in the formal power series $G(\mathbf{x}, \lambda)$. We show how the multisets $\mathbf{E}_i$ for the children i =1, 2 and 3 are 'simpler' than the one for the parent.

In the third pair, M and m are replaced with $M+m$, i.e., $\mathbf{E}_3 = \mathbf{E} \cup \{M+m\} \backslash \{M, m\}$. The total number of exponents has decreased by 1. Since the algorithm has terminated if there is only 1 exponent, we can induct on the size of $\mathbf{E}$ and ignore this term.

Since the first 2 children are symmetrical cases, it suffices to examine just the first child. Let $\alpha(M), \ldots, \alpha(1)$ be the index of the multiset $\mathbf{E}^+$, i.e.

$$\mathbf{E}^+ = \{\underbrace{M, M, \ldots, M}_{\alpha(M)}, \underbrace{M-1, M-1, \ldots, M-1}_{\alpha(M-1)}, \ldots, \underbrace{1, 1, \ldots, 1}_{\alpha(1)}\}.$$

Similarly, let $\beta(m), \ldots \beta(-1)$ be the index of the multiset $\mathbf{E}^-$. $\mathbf{E}_1$ is identical to $\mathbf{E}$, except that $M+m$ has replaced m. It may lie in either the multiset $\mathbf{E}^+$, the multiset $\mathbf{E}^-$ or it may be 0. In the last case, we can again apply induction on the number of nonzero exponents. Since $M+m$ lies strictly between M and m,

1. $M_1 = M$, $m_1 \geq m$.

2. $\alpha_1(M) = \alpha(M)$ and $\beta_1(m) < \beta(m)$.

In Elliott's words, there is "a diminution ... of absolute value of a numerically greatest negative" exponent, "without any compensating increase at the other end of the scale." [Ell03, p.351]

Pile the exponents on a number line, like bricks, placing them in their namesake spots. Figure 3.3 will help us visualize the process. One bulldozer from the left and one bulldozer from the right are at work. If term 1 of (3.2.1) is called, the bulldozer on the left chips the top brick and pushes it into the interior. If term 2 is called, the bulldozer on the right does a similar job. If term 3 is called, both bulldozers work but the bricks collide in the air, merging into one brick which again lands in the interior. In this case, we can apply induction on the number of bricks. The machines always hit the top brick, making it fly somewhere strictly between the two extreme walls. The origin should be thought of as a bottomless pit. (If a brick is hit onto 0, it falls and is never heard from again). The work is completed when all the bricks are pushed onto one side of the pit or into it.

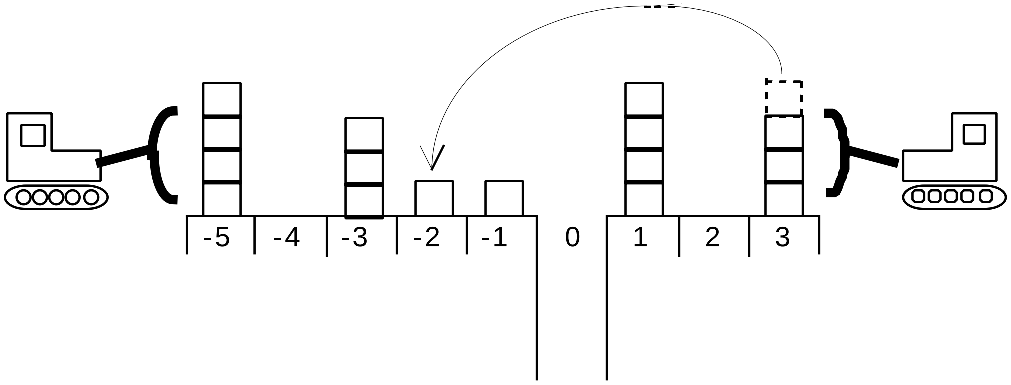


Figure 3.3: Birth of a term 2 child in the EM-algorithm.

Let's get an upper bound on the number of times that a particular brick can be hit. When the brick is hit, the spot where it lands is eliminated from where it can go in the future. If a brick is on one of the extreme walls, there are $a-1$ positive spots, $-b-1$ negative spots and 1 zero spot to which it can land, $a-b-1$ spots altogether. Hence, the brick can be moved a total of $a-b-1$ times. A brick not on an extreme wall has an even smaller upper bound of moves, hence we get

Lemma 3.3.2. *If A and B are the multisets of positive and negative exponents of λ in the crude generating function, then an upper bound on the depth of our tree is $(|A|+|B|)(a-b-1)$, where $a=$max(A) and $b=$min(B).*

For the example $3x = y + 5z$ of the last section, the depth has an upper bound of $(1+2)(3+5-1) = 21$.

If a ternary tree has depth n, then an upper bound on the number of nodes is

$$1 + 3 + 3^2 + \cdots + 3^n = (3^{n+1} - 1)/2.$$

Hence, an upper bound on the number of steps in our algorithm is

$$3^{(|A|+|B|)(a-b-1)+1}/2 \tag{3.3.2}$$

□

(3.3.2) gives an upper bound on the steps of $3^{22}/2$ for Example 3.1.1; in contrast, there are only 29 nodes in Figure 3.1. A great improvement on the upper bound can be made by making a more careful analysis of the depth of the tree.

Chapter 4

Some subclasses of magic squares

4.1 Dürer's magic square

Joseph Leo Koerner argues that Albrecht Dürer articulates in "Melencolia I" (Figure 4.1) a pivotal moment in the history of subjectivity (and I might add, of science, largely alchemy at the time). "The Renaissance abstracted inwardness as an inherent quality of creative genius"[Koe96]. Some objects in the engraving are tools used by Melancholy; others are achievements of her work. Among the latter is the square

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

This square has many properties.

1. The entries are nonnegative integers.

2. Any row—e.g., 16, 3, 2 and 13—or column—e.g., 16, 5, 9 and 4—sums to 34.

3. The *main primary diagonal*—16, 10, 7 and 1— and the *main secondary diagonal* —4, 6, 11 and 13—sum to 34.

4. The entries of the square are $\{1, 2, \ldots, 16\}$.

5. With the center as origin:

   (a) entries that are symmetrically located—e.g., 2 and 15, 4 and 13—sum to 17;

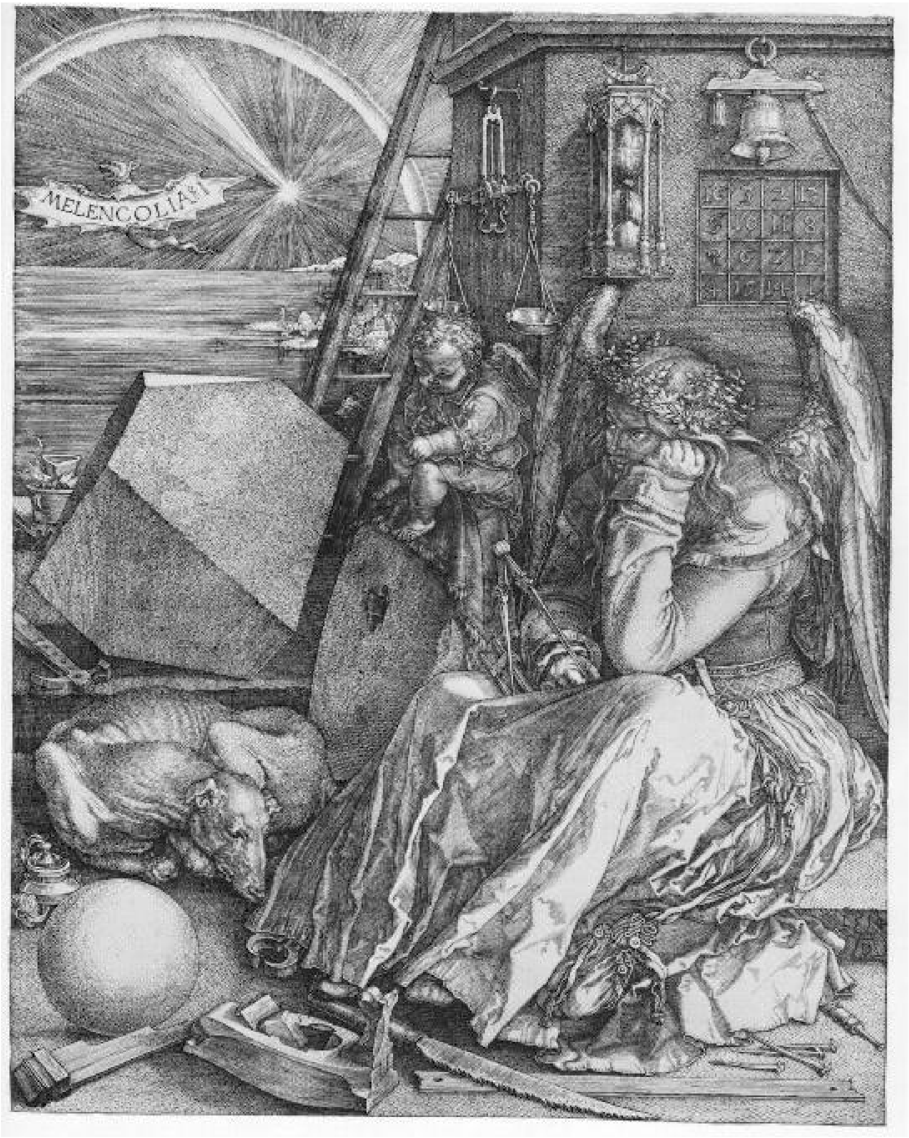


Figure 4.1: Albrecht Durer's Melencolia

.

(b) the entries in each quadrant—e.g., 16, 3, 10 and 5—sum to 34.

6. If we concatenate the middle 2 entries in the bottom row, we get 1514, the date of the engraving.

A square satisfying properties 1 and 2 is *magic*. A magic square which satisfies property 3 is a *recreational magic square* or *R-square*. Property 4 earns the modifier *classic* or “normal”. Matrices having property 5(a) are *anti-symmetric*, or “symmetric”.

Property 5(b) is generalized in Section 4.4.

Property 6 is typical of recreational uses of the subject. For another recreational curiosity,

$$\begin{array}{|ccc|}\hline 67 & 1 & 43 \\ 13 & 37 & 61 \\ 31 & 73 & 7 \\ \hline\end{array}$$

is the 3×3 R-square with smallest index whose entries are prime (allowing 1 to be prime). The 12×12 square found in [BJ76, p. 35] is the smallest R-square with the first consecutive primes as entries.

Much of the recreational literature consists of procedures for constructing examples of squares with specified size and properties. For instance, to construct Dürer's square, begin with

$$\begin{array}{|cccc|}\hline 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \\ \hline\end{array} \tag{4.1.1}$$

(4.1.1) has equal main primary and secondary sums and is anti-symmetric. Reversing the entries in each of the 2 main diagonals preserves these properties and picks up equal row and column sums too, i,e, the resulting square has properties 1–5.

$$\begin{array}{|cccc|}\hline 16 & 2 & 3 & 13 \\ 5 & 11 & 10 & 8 \\ 9 & 7 & 6 & 12 \\ 4 & 14 & 15 & 1 \\ \hline\end{array} \tag{4.1.2}$$

Switching the 2 middle columns of (4.1.2) does not affect the first 5 properties. The result is Dürer's square. See [BJ76, pp. 6–7] for an extension of this procedure to any n a multiple of 4.

In contrast to procedures like the one just illustrated which produce examples of subclasses, we would like to enumerate or combinatorially decompose the set of all squares that have a particular set of properties. In particular, we are interested in the set of squares which satisfy properties which translate directly to a system of linear homogeneous equations like 1–3 and 5. As an aside, we may on occasion address the problem of enumerating squares with a particular set of entries, e.g., the first n^2 natural numbers.

4.2 Magic squares: conventions and dimension

Let A be a $n \times n$ matrix. n is the *order.*

Index the entries using the set $\{0, \ldots, n-1\}$ instead of the usual $\{1, \ldots, n\}$, i.e., $A = \|a_{ij}\|_{i,j=0}^{n-1}$. Indexing in this number theoretic way facilitates the discussion surrounding various properties of and operations on the squares.

Index the rows of A from top to bottom and the columns from left to right. We put a hat on the symbols in the case of sets, reserving the symbol without the hat for the sum of the elements in the respective set.

$$\begin{aligned} \hat{R}_k(A) &= \{\, a_{kj} \mid j = 0, \ldots, n-1 \,\} & \qquad R_k(A) &= \sum_{j=0}^{n-1} a_{kj} \\ \hat{C}_k(A) &= \{\, a_{ik} \mid i = 0, \ldots, n-1 \,\} & \qquad C_k(A) &= \sum_{i=0}^{n-1} a_{ik} \end{aligned}$$

A is *magic* if

$$R_0(A) = R_1(A) = \cdots = R_{n-1}(A) = C_0(A) = C_1(A) = \cdots = C_{n-1}(A).$$

The common sum is the *index.* The entries may come from the set of rationals, $\mathbb{Q}$; the set of integers, $\mathbb{Z}$; or the set of nonnegative integers, $\mathbb{Z}^{\geq 0}$. We use 3 type faces to indicate the sets of such magic squares:

entries	name	entries	name	entries	name
$\mathbb{Q}$	$\mathbf{M}_n$	$\mathbb{Z}$	$\mathfrak{M}_n$	$\mathbb{Z}^{\geq 0}$	$\mathcal{M}_n$.

For example, $\mathbf{M}_n$ is the set of magic squares of order n with entries in $\mathbb{Q}$. We indicate a restriction to matrices with a particular index by putting in a second index. For instance, $\mathfrak{M}_{n,0}$ is the set of magic squares of order n and index 0 with entries in $\mathbb{Z}$.

Let J be the square with all entries 1, then

$$\mathbf{M}_n = \mathbf{M}_{n,0} \oplus \mathbb{Q}J. \tag{4.2.3}$$

Lemma 4.2.1. $\mathbf{M}_{n,0}$ *can be defined directly as the set of* $n \times n$ *matrices with rational entries which satisfy*

$$R_0(A) = R_1(A) = \cdots = R_{n-1}(A) = C_1(A) = \cdots = C_{n-1}(A) = 0. \tag{4.2.4}$$

Proof. The only equation in the definition of magic which is not in (4.2.4) is $C_0(A) = 0$. From the row sum equations, the sum of all the entries in the matrix is 0. From the other column sum equations, the sum of all the entries in the columns 1 through $n-1$ is 0. Subtracting these 2 equations, we get that the sum of the elements in column 0 must also be 0. □

Proposition 4.2.2. *The* $2(n-1)+1$ *column and row sum equations of* (4.2.4) *are independent from each other. As a consequence,*

$$\dim \mathbf{M}_{n,0} = n^2 - (2(n-1)+1) = (n-1)^2 \quad \textit{and} \quad \dim \mathbf{M}_n = (n-1)^2 + 1$$

Proof. Consider the equations in (4.2.4) to be linear functionals on the space of $n \times n$ matrices. Concatenate the rows of each linear functional to get a single vector. Reorder the entries so that the 0th row and then the remainder of the 0th column are first. Form a matrix by laying down as rows the linear functionals so ordered, choosing first the 0th row sum, then the column sums, and finally the rest of the row sums; the resulting matrix is upper triangular with 1's on the diagonal. □

The theory of linear homogeneous Diophantine equations, sketched in Chapter 1, tells us that $\mathcal{M}_n$ is a discrete polyhedral cone. Define the dimension of a cone to be the dimension of the linear span of the vectors found in the cone.

Proposition 4.2.3. $\dim \mathcal{M}_n = \dim \mathbf{M}_n$

Proof. Clearly, $\dim \mathcal{M}_n \leq \dim \mathbf{M}_n$. Let

$$B = \{J, v_1, v_2, \ldots, v_m\},$$

be any basis of $\mathbf{M}_n$ which respects the direct sum of (4.2.3). It suffices to produce a new basis,

$$B' = \{J, v_1', v_2', \ldots, v_m'\},$$

all whose elements are in $\mathcal{M}_n$. The components of each vector v_i are rational numbers. Clear denominators by multiplying by the LCD of all the entries. To each of these now integer vectors, add a large enough multiple of J to get nonnegative entries. The resulting set of vectors together with J is the desired B'. □

As a consequence of Proposition 4.2.2 and Proposition 4.2.3, we get

Corollary 4.2.4.

$$\dim \mathcal{M}_n = (n-1)^2 + 1$$

For any order, the magics are a linear combination of permutation matrices. Hence, the product of any two magic squares is also magic.

Any of the sets of magic squares is invariant under cycling of the rows and/or columns. Any subclass which is closed under such cycling is *torus invariant.* The sets of R-squares are not torus invariant. In what remains of this chapter, we introduce 2 other torus invariant subclasses, P-squares and W-squares. The intersection of these latter 2 subclasses, the *most-perfect pandiagonal magic squares*, is the only magic subclass for which its classic squares have been enumerated [OB98].

4.3 Torus lines and pandiagonal (P-)squares

Fundamental to our discussion is the *torus* line, also known as a "broken" or "wrapping" line. The 2 most important torus lines are

- A *primary* diagonal is the set of entries formed by starting at any entry of the square and moving at a $-45°$ angle with the horizontal, wrapping around the square upon reaching an edge. If the starting entry is any (i, i) entry, the set is the main primary diagonal already encountered. The primary diagonal with start (1,2) whose entries are numbered in the order that they are visited is

$$\begin{pmatrix} 0 & 5 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 3 \\ 4 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

- A *secondary* diagonal is the set of entries formed by starting at any entry of the square and moving at a +45° angle with the horizontal. If the starting point is any $(i, n-1-i)$ entry, the set is the main secondary diagonal. In

  $$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix},$$

  the entries with a 1 form a secondary diagonal.

However, the angle with the horizontal does not have to be ±45°. For example a row is a torus line which makes a 0° angle with the horizontal. The nonzero entries of the square below form the line which starts at (0,0) and proceeds by going down one and over 2. The angle with the horizontal is $-\arctan\frac{1}{2} \approx -26.57°$.

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 3 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 \end{pmatrix} \tag{4.3.5}$$

We can view lines from various perspectives. Glue together the top and bottom edges and the left and right edges of the square to form a torus. A line is just the entries which lie in a "straight" line of the torus. Equivalently, add copies of the original square and lay them down so that edges are adjacent to the original square. Extend this indefinitely. Start at any entry and proceed in a straight line. Require the image of the same entry to eventually be encountered again. A line is just the set of entries picked up until this repetition occurs.

The lines encountered so far pick up a full set of n entries from the square, something that in fact always happens.

Proposition 4.3.1. *A line of an $n \times n$ square has n entries.*

Proof. By an appropriate torus translation, we may assume that the line starts at $(0,0)$. A line terminates when it travels for the first time a multiple of n units in each direction, say (r,s). The line must have traveled through any fraction of (r,s) which is integral. If we divide (r,s) by n, we obtain a second point on the line since not both r/n and s/n are divisible by n. In fact, divide by the entire $\gcd(r,s)$ to get the point (a,b). In our traverse, from $(0,0)$, (a,b) is the first point encountered. All subsequent points are the multiples of this first point. For the line to terminate after m steps, $ma \equiv_n mb \equiv_n 0$. Since a and b have no prime factors in common, n must divide m. □

In Chapter 11, we will study lines like (4.3.5) in more depth. For now, we restrict to the rows, columns and ±45° diagonals.

To reference specific diagonals of a square, we index them from left to right starting with the upper left entry. As with rows and columns, we put a hat on the symbols in the case of sets, reserving the symbol without the hat for the sum of the elements in the respective set.

$$\hat{F}_k(A) = \{\, a_{i,k+i} \mid i = 0, \ldots, n-1 \,\} \qquad F_k(A) = \sum_{j=0}^{n-1} a_{i,k+i}$$

$$\hat{S}_k(A) = \{\, a_{i,k-i} \mid i = 0, \ldots, n-1 \,\} \qquad S_k(A) = \sum_{i=0}^{n-1} a_{i,k-i}$$

For example, if A has order 5, the entries of the kth secondary diagonal $\hat{S}_k(A)$ correspond to the entries labeled k in

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{pmatrix}.$$

A magic square is *pandiagonal* if all its primary and secondary diagonal sums are equal, or directly, a $n \times n$ matrix is a pandiagonal square or *P-square* if

$$R_0 = \cdots = R_{n-1} = C_0 = \cdots = C_{n-1} = F_0 = \cdots = F_{n-1} = S_0 = \cdots = S_{n-1}. \qquad (4.3.6)$$

The sets of P-squares of order n with specified matrix entries are

entries	name	entries	name	entries	name
$\mathbb{Q}$	$\mathbf{P}_n$	$\mathbb{Z}$	$\mathfrak{P}_n$	$\mathbb{Z}^{\geq 0}$	$\mathcal{P}_n$.

Call an element of $\mathbf{P}_{n,0}$ a *zero-square or z-square.*

As with magic squares, we have the direct sum decomposition

$$\mathbf{P}_n = \mathbf{P}_{n,0} \oplus QJ. \tag{4.3.7}$$

For an example of this direct sum decomposition,

$$A = \begin{array}{|cccc|}\hline 16 & 3 & 13 & 2 \\ 5 & 10 & 8 & 11 \\ 4 & 15 & 1 & 14 \\ 9 & 6 & 12 & 7 \\ \hline \end{array} = \frac{1}{2}\begin{array}{|cccc|}\hline 15 & \overline{11} & 9 & \overline{13} \\ \overline{7} & 3 & \overline{1} & 5 \\ \overline{9} & 13 & \overline{15} & 11 \\ 1 & \overline{5} & 7 & \overline{3} \\ \hline \end{array} + \frac{17}{2}\begin{array}{|cccc|}\hline 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ \hline \end{array} = B + mJ,$$

where $m = \frac{17}{2} = (\text{ind}\,A)/n$. $B = \frac{1}{2}B'$, where B' is an integral matrix. Note how entries of B' that are on a diagonal 2 units apart are opposites, a property which holds only for z-squares of order 4.

Lemma 4.3.2. $\mathbf{P}_{n,0}$ *can be defined directly as the set of* $n \times n$ *matrices with rational entries which satisfy*

$$R_0 = \cdots = R_{n-1} = C_1 = \cdots = C_{n-1} = F_1 = \cdots = F_{n-1} = S_1 = \cdots = S_{n-1} = 0. \tag{4.3.8}$$

Proof is identical to that of Lemma 4.2.1.

Theorem 4.3.3. *The* $2(n-1)+1$ *column and row sum equations of* (4.3.8) *are independent from each other and from the diagonal sums. The* $2(n-1)$ *primary and secondary diagonal sum equations are*

1. *independent for* n *odd,*

2. *have exactly one dependence for* n *even.*

As a consequence,

$$\dim \mathbf{P}_n = \begin{cases} (n-2)^2 - 1 & \textit{if } n \textit{ is odd,} \\ (n-2)^2 & \textit{if } n \textit{ is even.} \end{cases}$$

Proof. To find relations among the equations of (4.3.8), thought of as linear functionals, set

$$\sum_{i=0}^{n-1} r_i R_i + \sum_{i=1}^{n-1} c_i C_i + \sum_{i=1}^{n-1} f_i F_i + \sum_{i=1}^{n-1} s_i S_i = 0. \tag{4.3.9}$$

and solve for the coefficients r_i, c_i, f_i and s_i. We prove for general n but use $n = 3$ to illustrate. Writing out (4.3.9) as a system of equations,

$$\begin{bmatrix} r_0 & r_1 & r_2 & c_1 & c_2 & f_1 & f_2 & s_1 & s_2 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} = 0.$$

Multiply on the right by $\langle 1, 0 \ldots, 0\rangle^t$ to get $r_0 = 0$. Every functional corresponding to a diagonal or column picks off exactly one element from each row; multiply on the right by

$$\langle \underbrace{-1, \ldots, -1}_{n}, \underbrace{1, \ldots, 1}_{n}, 0, \ldots, 0\rangle^t$$

to get $n(-r_0 + r_1) = 0$ which implies $r_1 = 0$.

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} -1 \\ -1 \\ -1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} -3 \\ 3 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

What was done for the 0th and 1st rows can be done for the 0th and ith rows. Hence $r_i = 0$ for all i.

Our system is now reduced to columns and diagonals, e.g.,

$$\begin{bmatrix} c_1 & c_2 & f_1 & f_2 & s_1 & s_2 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} = 0.$$

Temporarily augment the system by putting in the 0th column and a new variable c_0, which we can set to 0 at any time, to get

$$\begin{bmatrix} c_0 & c_1 & c_2 & f_1 & f_2 & s_1 & s_2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} = 0.$$

We can perform the same series of operations as we did for the rows to show that $c_i = 0$ for all i, e.g., multiply on right by

$$\langle -1, 1, \underbrace{0, \ldots, 0}_{n-2}, -1, 1, \underbrace{0, \ldots, 0}_{n-2}, \ldots \rangle^t$$

to get $n(-c_0 + c_1) = 0$ which implies $c_1 = 0$.

If n is odd, there is a transformation of the matrices which preserves pandiagonality and switches rows and columns with the diagonals (see Theorem 6.1.1), showing that the $f_i,\ s_i = 0$ for all i. For the rest of the proof, assume n is even. We produce a relation and show that there are no further ones.

Consider the locations of the entries of our matrix to be squares of a checkerboard with upper left hand square black. We account for the white squares in two ways, by summing the odd primary diagonals and the odd secondary diagonals;

$$F_1 + F_3 + \cdots + F_{n-1} = S_1 + S_3 + \cdots + S_{n-1} \quad \text{or} \quad \sum_{i \text{ odd}} F_i - S_i = 0. \qquad (4.3.10)$$

It remains to show that $\{F_2, F_3, \ldots F_{n-1}, S_1, S_2, \ldots S_{n-1}\}$ is independent. To keep the calculations symmetric, we leave in the F_1 and its coefficient f_1, which we can at any time, set to 0. Let us explicitly write out the linear combination of functionals of (4.3.9), only keeping track of the entries that we need.

$$
\begin{aligned}
&f_1 \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix} + f_2 \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \end{pmatrix} + \cdots \\
&\qquad + f_{n-1} \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} = \begin{pmatrix} * & & * \\ f_{n-1} & & * \\ f_{n-2} & & f_{n-3} \\ \vdots & * & \vdots \\ f_3 & & f_2 \\ f_2 & & f_1 \\ * & & 0 \end{pmatrix}
\end{aligned} \tag{4.3.11}
$$

$$
\begin{aligned}
&s_1 \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix} + s_2 \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix} + \cdots \\
&\qquad + s_{n-1} \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ & & \ddots & & \\ 0 & 1 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix} = \begin{pmatrix} * & & * \\ s_1 & & * \\ s_2 & & s_1 \\ \vdots & * & \vdots \\ s_{n-3} & & s_{n-4} \\ s_{n-2} & & s_{n-3} \\ * & & s_{n-2} \end{pmatrix}
\end{aligned} \tag{4.3.12}
$$

Sum (4.3.11) and (4.3.12) to get

$$\begin{pmatrix} * & & * \\ f_{n-1}+s_1 & & * \\ f_{n-2}+s_2 & & f_{n-3}+s_1 \\ \vdots & * & \vdots \\ f_3+s_{n-3} & & f_2+s_{n-4} \\ \boxed{f_2+s_{n-2}} & & f_1+s_{n-3} \\ * & & \boxed{s_{n-2}} \end{pmatrix}. \tag{4.3.13}$$

Remembering that the matrix has been set to zero, use the s's in the nonboxed entries to connect the f's. From the first column, $s_{n-3} = -f_3$. From the last column, $s_{n-3} = -f_1$. Hence, $f_1 = f_3$. After $n-4$ more of these crisscrosses between the first and last columns, we get two strings of equalities involving $\{f_1, \ldots, f_{n-1}\}$.

$$f_1 = f_3 = f_5 = \cdots \qquad f_2 = f_4 = f_6 = \cdots . \tag{4.3.14}$$

From the boxed entries, we get

$$0 = f_2 = f_{\text{even}}. \tag{4.3.15}$$

Recall that we can set $f_1 = 0$, then f_{odd} also is 0. Substituting 0 for all f_i in (4.3.13) and remembering that the matrix is equal to the zero matrix gives $s_i = 0$ for all i. □

Proposition 4.3.4. $\dim \mathcal{P}_n = \dim \mathbf{P}_n$

Proof is again identical to that of the corresponding result for magic squares, Proposition 4.2.3.

As a consequence of Theorem 4.3.3 and Proposition 4.3.4, we get

Corollary 4.3.5.

$$\dim \mathcal{P}_n = \begin{cases} (n-2)^2 & \textit{if } n \textit{ is odd,} \\ (n-2)^2+1 & \textit{if } n \textit{ is even.} \end{cases}$$

In the recreational spirit, could Dürer have replaced the classic magic square in his engraving with a classic *pandiagonal* square keeping the 15 and 14 where they are? We answer this question in Section 8.9.

4.4 W-squares and semidiagonals

The material in this section, in particular Proposition 4.4.5, is largely based on [Mül97a]. A *block* is a 2×2 submatrix of adjacent elements. An $n \times n$ magic square A is a *W-square* if all blocks sum to $\operatorname{ind}_W(A) = 4 \operatorname{ind}(A)/n$. The sets of W-squares of order n with specified matrix entries are

entries	name	entries	name	entries	name
$\mathbb{Q}$	$\mathbf{W}_n$	$\mathbb{Z}$	$\mathfrak{W}_n$	$\mathbb{Z}^{\geq 0}$	$\mathcal{W}_n$.

As usual, we have the direct sum decomposition

$$\mathbf{W}_n = \mathbf{W}_{n,0} \oplus QJ \tag{4.4.16}$$

and a proposition identical to Proposition 4.2.3.

Proposition 4.4.1. $\dim \mathcal{W}_n = \dim \mathbf{W}_n$

Proposition 4.4.2. *Nontrivial W-squares are of even order only.*

Proof. Suppose the order n is odd. Alternately add and subtract the successive blocks of the first two columns to get $2(a_{00} + a_{01}) = \operatorname{ind}_W(A)$. Using torus translations, we get the semi-blocks $a_{0i} + a_{0,i+1} = \operatorname{ind}_W/2$ for $i = 0, \ldots, n$. Taking an alternating sum of these semi-blocks, we get $2a_{00} = \operatorname{ind}_W/2$. □

A W-square is completely determined by row 0 and the middle $n-2$ elements of column 0. Equivalently, a W-square with index 0 is completely determined by the first $n-1$ elements of row 0 and the middle $n-2$ elements of column 0. We claim that, in fact, these entries can be arbitrarily chosen.

Proposition 4.4.3. *For n even,*

$$\dim \mathbf{W}_{n,0} = 2n - 3 \quad \textit{or equivalently,} \quad \dim \mathbf{W}_n = \dim \mathcal{W}_n = 2n - 2.$$

Proof. It suffices to show that a square chosen with arbitrary entries in the determining set above can be filled out to be a W-square. Use the row 0 equation to get the last entry in row 0, and the column 0 equation to get the last entry in column 0. Use the block equations to fill out the rest of the matrix. We are left to check that the defining equations not used in filling out the matrix are satisfied. The blocks used to fill out the matrix are precisely the non-wrapping ones. Taking specific alternating sums of the non-wrapping block equations gives the blocks which involve wrapping. Taking the sum of every other of the top blocks results in the sum of the rows 0 and 1. Since the elements of row 0 sum to 0, then so does row 1, ditto for column 1. The other rows and columns are gotten by repeating the above in rows 1 and 2 and columns 1 and 2, etc. □

Let's investigate 2×2 submatrices of W-squares not taken from adjacent rows and/or columns. Using $\bar{1}$ instead of -1 for display purposes,

$$\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad - \quad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad = \quad \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \bar{1} & \bar{1} \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad = \quad 0.$$

Combining 2 such relations of 4 elements gives us

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & \bar{1} & \bar{1} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad - \quad \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \bar{1} & \bar{1} \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad = \quad \begin{pmatrix} 0 & 1 & 0 & \bar{1} \\ 0 & 0 & 0 & 0 \\ 0 & \bar{1} & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad = \quad 0. \qquad (4.4.17)$$

Taking similar combinations of blocks, we get

Lemma 4.4.4. *The 2×2 submatrix of a W-square formed by taking the intersection of the pair of rows i_1, i_2 with the pair of columns j_1, j_2, has as relation among its entries*

relation	$i_1 - i_2 \mod 2$	$j_1 - j_2 \mod 2$
$a_{i_1,j_1} + a_{i_1,j_2} + a_{i_2,j_2} + a_{i_2,j_1} = \text{ind}_W$	*1*	*1*
$a_{i_1,j_1} + a_{i_1,j_2} - a_{i_2,j_2} - a_{i_2,j_1} = 0$	*0*	*1*
$a_{i_1,j_1} - a_{i_1,j_2} - a_{i_2,j_2} + a_{i_2,j_1} = 0$	*1*	*0*
$a_{i_1,j_1} - a_{i_1,j_2} + a_{i_2,j_2} - a_{i_2,j_1} = 0$	*0*	*0.*

For $k = 0, 1$ and $l = 0, \ldots, n-1$, the primary and secondary *semidiagonals* are

$$p_{k,l} = \sum_{i \equiv_2 k,\ j \equiv_n l+i} a_{i,j} \quad \text{and} \quad s_{k,l} = \sum_{i \equiv_2 k,\ j \equiv_n l-i} a_{i,j},$$

respectively. For an order 6 example,

$$p_{1,3} \quad = \quad \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

The use of the words primary and secondary in the names is justified by

$$P_j = p_{0,j} + p_{1,j} \quad \text{and} \quad S_j = s_{0,j} + s_{1,j}.$$

For example,

$$P_2 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$
$$= p_{0,2} + p_{1,2}.$$

The sum of the entries in row 0 with second index even is

$$E = a_{0,0} + a_{0,2} + \cdots + a_{0,n-2},$$

and with second index odd is

$$O = a_{0,1} + a_{0,3} + \cdots + a_{0,n-1}.$$

Similarly, the sum the entries in column 0 with first index even is

$$E^t = a_{0,0} + a_{2,0} + \cdots + a_{n-2,0},$$

and with first index odd is

$$O^t = a_{1,0} + a_{3,0} + \cdots + a_{n-1,0}.$$

Proposition 4.4.5. *Let A be a W-square with order $n = 2m$ and $\mathrm{ind}_W(A) = t$. If e, e_1, e_2 are even and o, o_1, o_2 are odd, then*

$$\begin{aligned} p_{e_1,e_2} &= s_{e_1,e_2} = E + E^t - ma_{00}; \\ p_{e,o} &= s_{e,o} = E - O^t + ma_{00}; \\ p_{o,e} &= s_{o,e} = O - E^t + ma_{00}; \\ p_{o_1,o_2} &= s_{o_1,o_2} = -O - O^t + m(t - a_{00}). \end{aligned}$$

In particular, the sums of the entries for 2 semidiagonals are equal provided that their indices have the same parity, i.e.,

$$\text{if } i = k \text{ and } j \equiv_2 l, \text{ then } p_{i,j} = p_{k,l} = s_{i,j} = s_{k,l}.$$

Corollary 4.4.6. *Given a W-square A, the primary and secondary diagonal sums with indices of the same parity are equal, i.e.,*

$$P_0 = P_2 = \cdots = P_{n-2} = S_0 = S_2 = \cdots = S_{n-2}$$
$$P_1 = P_3 = \cdots = P_{n-1} = S_1 = S_3 = \cdots = S_{n-1}.$$

In particular, if $P_0 = P_1$, then A is also a P-square.

Proof. Applying Lemma 4.4.4, we get

$$a_{ij} = \begin{cases} -a_{00} + a_{0j} + a_{i0} & i, j \text{ even;} \\ a_{00} - a_{0j} + a_{i0} & i \text{ odd, } j \text{ even;} \\ a_{00} + a_{0j} - a_{i0} & i \text{ even, } j \text{ odd;} \\ t - a_{00} - a_{0j} - a_{i0} & i, j \text{ odd.} \end{cases} \tag{4.4.18}$$

To finish the proposition, replace each of the summands in the semidiagonals with the expressions (4.4.18). □

Chapter 5

P-squares as a vector space

5.1 Operators and z-square identities

Recall that $\mathbf{P}_n$ is the set of P-squares with rational entries and order n. $\mathbf{P}_{n,0}$ restricts further to P-squares with index 0. Call an element of $\mathbf{P}_{n,0}$ a *zero-square or z-square.*

Given a matrix with entry a_{ij}, introduce the commuting operators R, C:

$$Ra_{ij} = a_{i+1,j}, \quad Ca_{ij} = a_{i,j+1}.$$

Andress [And60] used R, C to develop a series of z-square identities. For a fixed order n, the column sum equalities translate as

$$[n]_R a_{ij} = (1 + R + R^2 + R^3 + \cdots + R^{n-1})a_{ij} = 0;$$

$[n]_q$ is known as the q-analog of n. The primary diagonal sum equalities are

$$[n]_{RC} a_{ij} = (1 + RC + R^2C^2 + R^3C^3 + \cdots + R^{n-1}C^{n-1})a_{ij} = 0.$$

Subtracting the former displayed equation from the latter and factoring, we obtain

$$\begin{aligned}(R(C-1) + R^2(C^2-1) + \cdots + R^{n-1}(C^{n-1}-1))a_{ij} \\ = R(C-1)(1 + R(1+C) + R^2(1+C+C^2) + \cdots \\ + R^{n-2}(1 + C + \cdots + C^{n-2}))a_{ij} = 0 \quad (5.1.1)\end{aligned}$$

Multiply both sides by R^{-1} to drop R, the first factor. Call the last factor Q. Applying the factor $C - 1$ to a_{ij} first, we see that Qa_{ij} has no column dependence.

Lemma 5.1.1. *If an operator U is constant along any direction in which a matrix has line sums 0, then it is the 0 operator.*

Proof. We will treat the case of the column direction. Any other case is proved analogously. If Ua_{ij} has no column dependence, sum over the column index:

$$nUa_{ij} = \sum_{k=0}^{n-1} Ua_{ik} = U\sum_{k=0}^{n-1} a_{ik} = 0$$

□

Applying the lemma to Q, we get

Proposition 5.1.2. *As an operator on z-squares,*

$$1 + R(1+C) + R^2(1+C+C^2) + \cdots + R^{n-2}(1+C+\cdots+C^{n-2}) = 0. \tag{5.1.2}$$

Alternatively, we present an identity as a matrix, which, when dotted with a z-square, yields 0. Andress [And60, p.145] called (5.1.2) the *triangle identity*:

$$T_n = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & 1 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix} = 0$$

Subtracting the transpose of (5.1.2) from (5.1.2), we get

$$T_n - (T_n)^t = \sum_{-1<j<i<n-1} R^iC^j - \sum_{-1<i<j<n-1} R^iC^j = 0$$

or pictorially

$$\begin{pmatrix} 0 & \bar{1} & \bar{1} & \cdots & \bar{1} & 0 \\ 1 & 0 & \bar{1} & \cdots & \bar{1} & 0 \\ 1 & 1 & 0 & \cdots & \bar{1} & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}. \tag{5.1.3}$$

Define the *square* $B_k = \sum_{0\leq i,j\leq k} R^iC^j$, e.g.,

$$B_{n-2} = \begin{pmatrix} 1 & 1 & \cdots & 1 & 0 & 0 \\ 1 & 1 & \cdots & 1 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 1 & 1 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}.$$

For illustration purposes, fix $n = 6$, then

$$B_4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad B_2 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Define the *lower hook*

$$L_k = \sum_{j=1}^{k} R^jC^0 + \sum_{j=1}^{k-1} R^kC^j$$

and the *upper hook*

$$U_k = L_k^t,$$

e.g.,

$$L_4 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad U_2 = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Lemma 5.1.3. *$L_i - U_i = (R - C)B_i$, $i = 1, \ldots, n-2$.*

Proof. Instead of a formal proof, a couple of examples will demonstrate the pattern.

$$RB_{n-2} - CB_{n-2} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 1 & \cdots & 1 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 1 & 1 & \cdots & 1 & 0 & 0 \\ 1 & 1 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 & \cdots & 1 & 1 & 0 \\ 0 & 1 & \cdots & 1 & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 1 & \cdots & 1 & 1 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & \overline{1} & \cdots & \overline{1} & \overline{1} & 0 \\ 1 & 0 & \cdots & 0 & \overline{1} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 1 & 0 & \cdots & 0 & \overline{1} & 0 \\ 1 & 1 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix} = L_{n-2} - U_{n-2}.$$

In the case of $n = 6$,

$$RB_3 - CB_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & \overline{1} & \overline{1} & \overline{1} & 0 & 0 \\ 1 & 0 & 0 & \overline{1} & 0 & 0 \\ 1 & 0 & 0 & \overline{1} & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} = L_3 - U_3.$$

□

Returning to (5.1.3),

$$T_n - T_n^t = \sum_{i \geq 0} (RC)^i (L_{n-2-2i} - U_{n-2-2i}) = \sum_{i \geq 0} (RC)^i (R - C) B_{n-2-2i}$$

$$= (R - C)\sum_{i\geq 0}(RC)^i B_{n-2-2i} = 0,$$

the second equality a consequence of Lemma 5.1.3. We see that

$$Q = \sum_{i\geq 0}(RC)^i B_{n-2-2i}$$

has no dependence along a secondary diagonal. By Lemma 5.1.1, $Q = 0$.

Proposition 5.1.4. *As an operator on z-squares,*

$$\sum_{i\geq 0}(RC)^i B_{n-2-2i} = 0. \tag{5.1.4}$$

(5.1.4) is the *square pyramid identity*, a name fully appreciated upon glancing at the $n = 7$ case:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 2 & 2 & 1 & 0 & 0 \\ 1 & 2 & 3 & 2 & 1 & 0 & 0 \\ 1 & 2 & 2 & 2 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} = 0. \tag{5.1.5}$$

The square pyramid identity is actually part of a family of identities, which Andress [And60, p.150] calls complementary squares and which we call *complementary pyramids.*

The kth *square pyramid* of order n is

$$sP_{k,n} = \sum_{i\geq 0}(RC)^i B_{k-2i}.$$

Using this notation, (5.1.4) says $sP_{n-2,n} = 0$. To get the second member of the family, translate and rotate the triangle T_n so that its right angle is in the upper left corner and subtract from $sP_{n-2,n}$. For $n = 7$, we get

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & \bar{1} & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ \bar{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Adding the diagonal S_{n-2} and translating 1 unit up and 1 unit to the left, we get for $n = 7$,

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 2 & 2 & 1 & 0 & 0 & 0 \\ 1 & 2 & 2 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} = 0. \tag{5.1.6}$$

For general n, the result is

Proposition 5.1.5. *As an operator on z-squares,*

$$\sum_{i \geq 0} (RC)^i B_{n-3-2i} + (RC)^{n-2} = 0. \tag{5.1.7}$$

Define the *kth complementary pyramids* of order n to be the block matrix

$$cP_{k,n} = \begin{pmatrix} sP_{k,k} & & & \\ & 0 & & \\ & & sP_{n-2-k,n-2-k} & \\ & & & 0 \end{pmatrix}.$$

Using this notation, (5.1.4) says $cP_{n-2,n} = 0$ and (5.1.7) says $cP_{n-3,n} = 0$.

Proposition 5.1.6. *As an operator on z-squares, the complementary pyramids*

$$cP_{k,n} = 0,$$

for $k = n-2, n-3, \ldots, \left\lceil \frac{n-2}{2} \right\rceil$.

Proof. Define J_{kl} to be the matrix of 1's of size $k \times l$. Induct on k down by 2 from $n-2$ and $n-3$; the base cases being Proposition 5.1.4 and Proposition 5.1.5, respectively. For ease of presentation, we set $l = n-2-k$. Start with

$$cP_{k,n} = \begin{pmatrix} sP_{k,k} & & & \\ & 0 & & \\ & & sP_{l,l} & \\ & & & 0 \end{pmatrix}$$

and subtract the first k rows of 1's

$$\begin{pmatrix} 0 & 0 & 0 & & & \\ 0 & sP_{k-2} & 0 & & -J_{k,l+2} & \\ 0 & 0 & 0 & & & \\ & & & 0 & & \\ & & & & sP_l & \\ & & & & & 0 \end{pmatrix}.$$

Add the last $l+2$ columns of 1's

$$\begin{pmatrix} 0 & & & \\ & sP_{k-2} & & \\ & & 0 & \\ & & & sP_{l+2} \end{pmatrix}$$

and complete the induction step by translating one unit up and one unit to left. □

For n odd, there is one additional identity. Define a *flip* f over the 0th column $fF(R, C) = F(R, C^{-1})$. Start with the triangle T_n and move the $(0, 0)$th entry of the matrix to the center. Using the $n = 7$ case to illustrate,

$$T_7 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Translate T_n $u = \frac{n-3}{2}$ units up and to the right one unit: $R^{-u}CT_n$. Multiply by $(1 - f)$, i.e., subtract the negative of its flip, to get

$$R^{-u}CT_n - fR^{-u}CT_n = (1 - f)R^{-u}CT_n = 0. \tag{5.1.8}$$

Again turning to the $n = 7$ case, $R^{-2}CT_7 - fR^{-2}CT_7 =$

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \bar{1} & 0 & 1 & 0 & 0 \\ 0 & \bar{1} & \bar{1} & 0 & 1 & 1 & 0 \\ \bar{1} & \bar{1} & \bar{1} & 0 & 1 & 1 & 1 \\ 0 & \bar{1} & \bar{1} & 0 & 1 & 1 & 0 \\ 0 & 0 & \bar{1} & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{5.1.9}$$

The result is a filled isosceles right triangle with the hypotenuse taking up the middle $n-2$ entries of column 1, together with the negative of its flip. Define the right *elbow*

$$E_k = E_k(R, C) = C^k + \sum_{i=1}^{k}(R + R^{-1})C^{k-i}$$

and its flip over the 0th column, the left elbow

$$fE_k = E_k(R, C^{-1}).$$

For $n = 5$,

$$E_2 = \begin{pmatrix} 0 & 0 & 1 & & \\ & & & 1 & \\ & & & & 1 \\ & & & 1 & \\ 0 & 0 & 1 & & \end{pmatrix} \quad \text{and} \quad fE_2 = \begin{pmatrix} & & 1 & 0 & 0 \\ & 1 & & & \\ 1 & & & & \\ & 1 & & & \\ & & 1 & 0 & 0 \end{pmatrix}.$$

In terms of elbows, (5.1.9) is

$$(1 - f)(C(E_2 + E_1 + E_0)).$$

The *diamond* with side length k is

$$D_k = \sum_{-k \leq i-j, i+j \leq k} R^i C^j.$$

For $n = 5$,

$$D_2 = \begin{pmatrix} & & 1 & & \\ & 1 & 1 & 1 & \\ 1 & 1 & 1 & 1 & 1 \\ & 1 & 1 & 1 & \\ & & 1 & & \end{pmatrix}.$$

Lemma 5.1.7.

$$(C - C^{-1})D_k = (1 - f)(C(E_k + E_{k-1})) = C(E_k + E_{k-1}) - C^{-1}(fE_k + fE_{k-1}).$$

Proof. A diamond minus an identical diamond shifted 2 units to the left results in two right elbows from the original diamond and two left elbows from the shifted diamond. We illustrate with $n = 9$, $k = 3$, not displaying the first and last rows, since they are identically zero. $CD_3 - C^{-1}D_3 =$

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 & 0 & \bar{1} & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & \bar{1} & \bar{1} & 0 & 1 & 1 & 0 & 0 \\ 0 & \bar{1} & \bar{1} & 0 & 0 & 0 & 1 & 1 & 0 \\ \bar{1} & \bar{1} & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & \bar{1} & \bar{1} & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & \bar{1} & \bar{1} & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & \bar{1} & 0 & 1 & 0 & 0 & 0 \end{pmatrix},$$

which as claimed is $C(E_3 + E_2) - C^{-1}(fE_3 + fE_2)$. □

Continuing with (5.1.8), set $k = \frac{n-3}{2}$ to get

$$(1 - f)R^{-u}CT_n = (1 - f)(C(E_k + E_{k-1} + E_{k-2} + \cdots + E_0))$$

$$= (1 - f)(C(E_k + E_{k-1})) + (1 - f)(C(E_{k-2} + E_{k-3})) + \cdots$$

$$= (C - C^{-1})D_k + (C - C^{-1})D_{k-2} + (C - C^{-1})D_{k-4} + \cdots$$

$$= (C - C^{-1})(D_k + D_{k-2} + D_{k-4} + \cdots); \qquad (5.1.10)$$

the third equality uses Lemma 5.1.7. Define the *diamond step pyramid* to be

$$dsP_{k,n} = D_k + D_{k-2} + D_{k-4} + \cdots .$$

To illustrate, we select $k = 4$ and $n = 9$;

$$dsP_{4,9} = D_4 + D_2 + D_0 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 2 & 2 & 2 & 1 & 1 & 0 \\ 1 & 1 & 2 & 2 & 3 & 2 & 2 & 1 & 1 \\ 0 & 1 & 1 & 2 & 2 & 2 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Since $T_n = 0$, (5.1.10) says

$$(C - C^{-1})dsP_{k,n} = 0, \quad \text{for } k = \frac{n-3}{2}, \tag{5.1.11}$$

or in words, $dsP_{k,n}$, as an operator on z-squares, is constant for alternate entries in the column direction.

Lemma 5.1.8. *Given an operator Q on a matrix M of order n odd. If Q is constant for alternating entries in a direction for which M has line sums 0, then Q is the 0 operator.*

Proof. Since repeatedly collecting every other entry eventually wraps around the matrix to engulf every entry in the line, Q is in fact constant for all entries in the given direction; apply Lemma 5.1.1. □

Applying Lemma 5.1.8 to (5.1.11), we get

Proposition 5.1.9. *For n odd, $k = \frac{n-3}{2}$, the diamond step pyramid*

$$dsP_{k,n} = 0$$

as an operator on z-squares.

For $n = 7$, $k = 2$, Proposition 5.1.9 translates as

$$dsP_{2,7} = \left(\begin{array}{ccccccc} & & & 0 & & & \\ & & & 1 & & & \\ & & 1 & 1 & 1 & & \\ 0 & 1 & 1 & 2 & 1 & 1 & 0 \\ & & 1 & 1 & 1 & & \\ & & & 1 & & & \\ & & & 0 & & & \end{array} \right) = 0.$$

5.2 The rings $\hat{R}$, $\tilde{R}$ and the octagonal matrix

Define the rings

$$\widehat{R} = \mathbb{Z}[R, C]/(R^n - 1, C^n - 1) \quad \text{and} \quad \widetilde{R} = \mathbb{Q}[R, C]/(R^n - 1, C^n - 1).$$

Since $R^n - 1$ is not irreducible, $\widetilde{R}$ $(\widehat{R})$ is not an integral domain. There is a vector space ($\mathbb{Z}$-module) isomorphism between (integral) $n \times n$ matrices and elements of $\widetilde{R}$ $(\widehat{R})$. The map taking a matrix $A = \|a_{ij}\|_{i,j=0}^{n-1}$ into the polynomial is

$$A(R, C) = \sum_{i,j=0}^{n-1} a_{ij} R^i C^j.$$

We recover the matrix A by applying $A(R, C)$ as an operator to the *unit matrix*

$$u = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix},$$

i.e., $A(R, C)u = A$. The image of a (integral) z-square of order n is a (integral) z-*polynomial* of order n (a z-square is integral if and only if the corresponding z-polynomial is integral*)*.

Proposition 5.2.1. *The (integral) z-polynomials of order n form an ideal in $\widetilde{R}$ $(\widehat{R})$.*

Proof. The product of a (integral) polynomial $P(R, C)$ and a (integral) z-polynomial $A(R, C)$ corresponds, in the realm of matrices, to a (integral) linear combination of translates of a z-square A. Since the set of (integral) z-squares is invariant under translation, each of the translates will also be a (integral) z-square. Since the (integral) z-squares form a vector space ($\mathbb{Z}$-module), this (integral) combination is itself a (integral) z-square. □

The *octagonal matrix* or *octagon*

$$o = \begin{pmatrix} & 1 & \bar{1} & & & & \\ \bar{1} & & & 1 & & & \\ 1 & & & \bar{1} & & & \\ & \bar{1} & 1 & & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}$$

has rotational symmetry and "dihedral antisymmetry", meaning that a flip over one of the vertical, horizontal or diagonal axes placed in the center of the nonzero part of the matrix results in the negative of the original. Divide the octagon into pairs of opposite sides. The polynomial of the horizontal pieces of the octagon is

$$\begin{pmatrix} & 1 & \bar{1} & \\ 0 & & & 0 \\ 0 & & & 0 \\ & \bar{1} & 1 & \end{pmatrix}(R, C) = (C - C^2)(1 - R^3) = (1 - C)(1 - R)(C + RC + R^2C).$$

The vertical pieces are the negative of the transpose of the horizontal pieces; the polynomial of the vertical pieces is obtained from that of the horizontal pieces by switching R and C and taking the negative:

$$(1 - C)(1 - R)(-R - RC - RC^2).$$

Adding the polynomials of the horizontal and vertical pieces and taking out the 2 common factors, we get

$$(1 - C)(1 - R)(C - R + R^2C - RC^2),$$

which factors further to give us

$$o(R, C) = (1 - C)(1 - R)(C - R)(1 - RC). \tag{5.2.12}$$

In Table 5.1, we list the 7 non-identity dihedral operations, the corresponding operations on the polynomials and the effect of the operations applied to o, modulo appropriate translations. We demonstrate with the horizontal flip.

Operation	Image of R	Image of C	Result
$\frac{\pi}{2}$ rotation	C	R^{-1}	o
π rotation	R^{-1}	C^{-1}	o
$\frac{3\pi}{2}$ rotation	C^{-1}	R	o
vertical flip	R	C^{-1}	$-o$
horizontal flip	R^{-1}	C	$-o$
primary diagonal flip	C	R	$-o$
secondary diagonal flip	C^{-1}	R^{-1}	$-o$

Table 5.1: Dihedral operations on the octagon.

$$o(R^{-1}, C) = (1 - C)(1 - R^{-1})(C - R^{-1})(1 - R^{-1}C).$$

Multiply by R^3 to get $(1 - C)(R - 1)(CR - 1)(R - C)$. 3 sign changes are required to return to $o(R, C)$.

Proposition 5.2.2. *A integral z-polynomial $A(R, C)$ is*

1. *divisible by $(1 - R)(1 - C)$;*
2. *divisible in $\widehat{R}$ by the product of any 2 of the 4 factors of $o(R, C)$*
   (a) *if n odd,*
   (b) *except $(R - C)(1 - RC)$ if n even.*

Corollary 5.2.3. *A z-polynomial $A(R, C)$ is divisible by any single factor of $o(R, C)$ in the ring $\widehat{R}$.*

We will see in Section 5.4 that $A(R, C)$ is in fact divisible in $\widehat{R}$ by the entire $o(R, C)$.

Proof. Define the column generating function

$$A_j(R) = \sum_{i=0}^{n-1} a_{ij} R^i.$$

Since A has equal column sums,

$$A_j(1) = \sum_{i=0}^{n-1} a_{ij} = 0. \tag{5.2.13}$$

Grouping the terms in the polynomial according to powers of C,

$$A(R, C) = A_0(R)1 + A_1(R)C + \cdots + A_{n-1}(R)C^{n-1}.$$

Setting $R = 1$ and using (5.2.13),

$$A(1, C) = A_0(1)1 + A_1(1)C + \cdots + A_{n-1}(1)C^{n-1}$$

$$= 0(1) + 0(C) + \cdots + 0(C^{n-1}) = 0.$$

Hence, $1 - R$ divides $A(R, C)$. By the symmetry of R and C, $1 - C$ also divides $A(R, C)$.

Working with the polynomial in $\widehat{R}$ corresponds to working with the matrix on the torus; the matrix A can be deformed by translating sections n units in the horizontal direction and/or n units in the vertical direction. If the resulting configuration has lines unbroken in a particular direction, then the variation of $A(R, C)$ corresponding to this configuration is divisible by the factor corresponding to this direction. For example, we claim that the configuration

$$\begin{array}{ccccccc}
a_{00} & a_{01} & \cdots & a_{0,n-1} & & & \\
 & a_{11} & \cdots & a_{1,n-1} & a_{1,0} & & \\
 & & \ddots & \vdots & \vdots & \ddots & \\
 & & & a_{n-1,n-1} & a_{n-1,0} & \cdots & a_{n-1,n-2}
\end{array}$$

is divisible by both $1 - C$ and by $1 - RC$.

$$A(R, C) = \sum_{i,j=0}^{n-1} a_{i,i+j} R^i C^{i+j} = \sum_{i,j=0}^{n-1} a_{i,i+j} (RC)^i C^j, \tag{5.2.14}$$

where the indices of a are calculated modulo n. Setting $R = C^{-1}$, we get

$$A(C^{-1}, C) = \sum_{j=0}^{n-1} (a_{0j} + a_{1,1+j} + \cdots + a_{n-1,n-1+j}) C^j = \sum_{j=0}^{n-1} P_j(A) C^j,$$

where $P_j(A)$ is the sum of the entries in the jth primary diagonal of A. Since A has primary diagonal sums 0, $P_j(A) = 0$, $\forall j$ and hence, $A(C^{-1}, C) = 0$. Thus, $1 - RC$ divides this $A(R, C)$. Setting $C = 1$ in (5.2.14), we get

$$A(R, 1) = \sum_{i=0}^{n-1} \left(\sum_{j=0}^{n-1} a_{i,i+j} \right) R^i = \sum_{i=0}^{n-1} (R_i(A)) R^i,$$

where $R_i(A)$ is the sum of the entries in the ith row of A. Since A has row sums 0, $R_i(A) = 0$, $\forall i$ and hence, $A(R, 1) = 0$. Thus, $1 - C$ divides this same $A(R, C)$.

The only remaining case which is not analogous to the 2 cases already covered is the divisibility by $(R - C)(1 - RC)$ in the case n is odd, which is proved using the configuration

$$\begin{array}{ccccccc}
 & & & a_{0,n-1} & & & \\
 & & \iddots & & \ddots & & \\
 & a_{n-2,1} & & \cdots & & a_{n-1,n-3} & \\
a_{n-1,0} & & \cdots & a_{n-1,n-1} & \cdots & & a_{n-1,n-2} \\
 & a_{0,1} & & \cdots & & a_{0,n-3} & \\
 & & \ddots & & \iddots & & \\
 & & & a_{n-2,n-1} & & &
\end{array} .$$

Note that the indices of adjacent diagonals differ by 2, but since n is odd, all diagonals eventually occur, e.g., the secondary diagonals are, from left to right,

$$\{S_{n-1}, S_1, S_3, \ldots, S_{n-2}, S_0, S_2, \ldots, S_{n-3}\}.$$

□

5.3 Octagonal matrices as a spanning set of $\mathbf{P}_{n,0}$

Denote a translate of the octagon o as

$$o_{ij} = R^i C^{j-1} o.$$

and call any such matrix *an octagonal matrix* or *an octagon.*

In this section we will show that any z-polynomial is divisible by the octagonal polynomial $o(R, C)$. As a byproduct, the octagonal matrices will be shown to span $\mathbf{P}_{n,0}$, the set of z-squares. All results of this section have been taken from the Mathematics Magazine article [And60], written by Andress in 1960. Today, a computer algebra system can be used to easily program his algorithm.

A particular instance of Proposition 5.2.1, we rephrase Theorem 4 of [And60] as

Proposition 5.3.1. *Given any polynomial $P(R, C)$, the product of P and the octagonal polynomial $o(R, C)$ is a z-polynomial.*

Andress provided a converse of Proposition 5.3.1. To get it, Andress divides a z-polynomial $A(R, C)$ by each factor of $o(R, C)$, one at a time, cleverly choosing a particular quotient at each step *which is itself* the polynomial of a z-square. Call any such quotient a *z-square quotient.* More specifically, Andress takes any quotient by one of the factors, which we know to exist by Corollary 5.2.3, and uses it to produce another quotient that is a polynomial multiple of the original polynomial $A(R,C)$. By Proposition 5.2.1, this new quotient is a z-polynomial.

Recall the already introduced q analog of n

$$[n]_q = 1 + q + q^2 + \cdots + q^{n-1}.$$

Let $B(R,C)$ be any quotient of $A(R,C)$ by $1-R$. If

$$B'(R,C) = (1 - n^{-1}[n]_R)B(R,C).$$

then

$$(1-R)B'(R,C) = (1-R)B(R,C) - n^{-1}(1-R)[n]_R B(R,C)$$

$$= A(R,C) - n^{-1}(1-R^n)B(R,C) = A(R,C);$$

the last equality holds since we are working in $\widetilde{R}$. Hence, $B'(R,C)$ is also a quotient of $A(R,C)$ by $1-R$. Since $[n]_1 = n$,

$$(1 - n^{-1}[n]_R) = f(R)(1-R),$$

for some polynomial f. In [And60, (24)], Andress gives an incorrect expression for $f(x)$; it should instead be

$$f(x) = \left((n-1) + (n-2)x + \cdots + x^{n-2}\right)/n. \tag{5.3.15}$$

Putting together some of the previously displayed equations,

$$A(R,C)/(1-R) = B'(R,C) = (1 - n^{-1}[n]_R)B(R,C)$$

$$= f(R)(1-R)B(R,C) = f(R)A(R,C),$$

which is a z-polynomial by Proposition 5.2.1. We have found a z-square quotient. Likewise, $f(C)A(R,C)$ is a z-square quotient of $A(R,C)$ by $1-C$.

Substituting $\alpha = RC$ into (5.2.14), we get

$$A(R,C) = \sum_{i,j=0}^{n-1} a_{i,i+j}(RC)^i C^j = A'(\alpha, C),$$

where $A'(1,C)=0$. As when we divided by $1-R$,

$$A(R,C)/(1-RC)=A'(\alpha,C)/(1-\alpha)=f(\alpha)A'(\alpha,C)=f(RC)A(R,C);$$

we conclude that $f(RC)A(R,C)$ is a z-square quotient of $A(R,C)$ by $1-RC$.

Using another massage on the torus of the z-square A,

$$\begin{array}{ccccccc} & & & a_{0,n-1} & a_{00} & \cdots & a_{0,n-2} \\ & & \cdot^{\cdot^{\cdot}} & \vdots & \vdots & \cdot^{\cdot^{\cdot}} & \\ & a_{n-2,1} & \cdots & a_{n-2,n-1} & a_{n-2,0} & & \\ a_{n-1,0} & a_{n-1,1} & \cdots & a_{n-1,n-1} & & & \end{array},$$

let $\alpha=R/C$ to get

$$A(R,C)=\sum_{i,j=0}^{n-1}a_{i,j-i}(R/C)^iC^j=A'(\alpha,C),$$

where $A'(1,C)=0$. Hence,

$$A(R,C)/(1-R/C)=A'(\alpha,C)/(1-\alpha)=f(\alpha)A'(\alpha,C)=f(R/C)A(R,C),$$

or equivalently,

$$A(R,C)/(C-R)=C^{-1}f(R/C)A(R,C).$$

Since the degree of f is $n-2$, we produce a polynomial by multiplying by C^n (in detail, since we are working in the ring $\widetilde{R}$, we can add to the above polynomial the C^n-1 multiple of itself). We conclude that $C^{n-1}f(R/C)A(R,C)$ is a polynomial z-square quotient of $A(R,C)$ by $C-R$. We have shown

Proposition 5.3.2. *Given a z-square A and $f(x)$ defined by* (5.3.15), *let*

$$A''(R,C)=C^{n-1}f(R)f(C)f(RC)f(R/C)A(R,C)$$

then $A''(R,C)$ is a particular quotient in the ring $\widetilde{R}$ of $A(R,C)$ by $o(R,C)$, which is itself a z-polynomial.

$A(R,C)=A''(R,C)o(R,C)$ means that any z-square can be written as a Q linear combination of octagons.

Corollary 5.3.3. *The octagons of order n span $\mathbf{P}_{n,0}$, the space of z-squares of order n.*

In Proposition 5.4.1, we improve on this corollary by showing that we can work over $\mathbb{Z}$.

5.4 A $\mathbb{Z}$-module basis of octagons for $\mathfrak{P}_{n,0}$

Select the $n-3\times n-1$ upper left block of octagonal matrices

$$O'_n=\{o_{ij}\mid 0\le i\le n-4,\ 0\le j\le n-2\}$$

and define

$$O_n=\begin{cases}O'_n & n\text{ odd;}\\ O'_n\cup\{o_{n-3,n-1}\} & n\text{ even.}\end{cases}$$

Proposition 5.4.1. *O_n is a $\mathbb{Z}$-module basis for $\mathfrak{P}_{n,0}$, the set of integral z-squares.*

Corollary 5.4.2. *Any integral z-polynomial $A(R,C)$ is divisible by o in $\widehat{R}$.*

Proof. By Theorem 4.3.3,

$$\dim Z_n=\dim V_n=\begin{cases}(n-2)^2-1=(n-1)(n-3) & \text{if } n\text{ odd,}\\ (n-2)^2=(n-1)(n-3)+1 & \text{if } n\text{ even.}\end{cases}$$

Hence, O_n has the proper cardinality. To show independence and integrality, the result is almost immediate for n odd. For n even, the result will depend on an intricate induction.

Given any matrix $A=\|a_{ij}\|_{i=0}^{n-1}$ define the subset of entries written as a vector

$$\overline{A}=\{a_{ij}\mid 0\le i\le n-4,\ 0\le j\le n-2\}$$

and

$$A'=\begin{cases}\overline{A} & n\text{ odd;}\\ \overline{A}\cup\{a_{n-3,n-1}\} & n\text{ even.}\end{cases}$$

Assume n odd. Extract the subset O' from each octagon $O\epsilon O_n$ and lay it down as the row of a matrix, then the resulting matrix D_n is upper triangular with 1's down the main diagonal. Suppose that we have decomposed a z-square A in terms of O_n, i.e., $A=O_n.v$, where v is the vector of coefficients of the octagonal matrices in the decomposition. If we focus on the pivot entries, then $v.D_n=A'$. To obtain v, apply D_n^{-1} to A' on the right. The triangularity with 1's on the diagonal for D_n means that D_n^{-1} is integral. Hence, the coefficients of the decomposition are integral, and the proof in the case n odd is complete. We demonstrate the decomposition with

$$A = \begin{pmatrix} \overline{12} & \overline{6} & 0 & 11 & 7 \\ 1 & 12 & 3 & \overline{11} & \overline{5} \\ 4 & \overline{10} & \overline{4} & 2 & 8 \\ \overline{3} & \overline{2} & 9 & 5 & \overline{9} \\ 10 & 6 & \overline{8} & \overline{7} & \overline{1} \end{pmatrix}. \tag{5.4.16}$$

Extract the 2×4 upper right submatrix from each matrix in O_5 and lay it down as a row of

$$D_5 = \begin{pmatrix} 1 & \overline{1} & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & \overline{1} & 0 & \overline{1} & 0 & 0 & 1 \\ 0 & 0 & 1 & \overline{1} & 0 & \overline{1} & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & \overline{1} & 0 \\ 0 & 0 & 0 & 0 & 1 & \overline{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & \overline{1} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \overline{1} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Extract the 2×4 upper right submatrix from (5.4.16) and multiply on the right by D_5^{-1} to get

$$\langle -6, 0, 11, 7, 12, 3, -11, -5 \rangle . \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 & \overline{1} & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & \overline{1} & \overline{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \langle -6, -6, 5, 12, -6, 2, 9, 10 \rangle .$$

Hence, the $\mathbb{Z}$-module decomposition of (5.4.16) is

$$\begin{pmatrix} \overline{12} & \overline{6} & 0 & 11 & 7 \\ 1 & 12 & 3 & \overline{11} & \overline{5} \\ 4 & \overline{10} & \overline{4} & 2 & 8 \\ \overline{3} & \overline{2} & 9 & 5 & \overline{9} \\ 10 & 6 & \overline{8} & \overline{7} & \overline{1} \end{pmatrix} = -12 \begin{pmatrix} 1 & \overline{1} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \overline{1} \\ 0 & 0 & \overline{1} & 0 & 1 \\ \overline{1} & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} - 18 \begin{pmatrix} 0 & 1 & \overline{1} & 0 & 0 \\ \overline{1} & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & \overline{1} & 0 \\ 0 & \overline{1} & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$-18\begin{pmatrix}0&0&1&\bar{1}&0\\0&\bar{1}&0&0&1\\0&1&0&0&\bar{1}\\0&0&\bar{1}&1&0\\0&0&0&0&0\end{pmatrix}-7\begin{pmatrix}0&0&0&1&\bar{1}\\1&0&\bar{1}&0&0\\\bar{1}&0&1&0&0\\0&0&0&\bar{1}&1\\0&0&0&0&0\end{pmatrix}-10\begin{pmatrix}0&0&0&0&0\\1&\bar{1}&0&0&0\\0&0&1&0&\bar{1}\\0&0&\bar{1}&0&1\\\bar{1}&1&0&0&0\end{pmatrix}$$

$$-16\begin{pmatrix}0&0&0&0&0\\0&1&\bar{1}&0&0\\\bar{1}&0&0&1&0\\1&0&0&\bar{1}&0\\0&\bar{1}&1&0&0\end{pmatrix}-8\begin{pmatrix}0&0&0&0&0\\0&0&1&\bar{1}&0\\0&\bar{1}&0&0&1\\0&1&0&0&\bar{1}\\0&0&\bar{1}&1&0\end{pmatrix}-1\begin{pmatrix}0&0&0&0&0\\0&0&0&1&\bar{1}\\1&0&\bar{1}&0&0\\\bar{1}&0&1&0&0\\0&0&0&\bar{1}&1\end{pmatrix}.$$

In terms of polynomials,

$$A(R,C) = C^{n-1}(-12 - 18C - 18C^2 - 7C^3 - 10R - 16RC - 8RC^2 - 1RC^3)o(R,C).$$

Assume n even. To finish the proof, it suffices to show that $|D_n| = 1$. The rest of the proof would then follow exactly as it did for n odd. D_n is almost upper triangular:

$$D_n = \begin{pmatrix} 1 & * & \cdots & * & * \\ 0 & 1 & \cdots & * & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & * \\ 1 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Define D_n^* to be the $(n-1)(n-3) \times (n-1)(n-3)$ upper right submatrix of D_n. To evaluate $|D_n|$, expand along the last row: $|D_n| = 1 - |D_n^*|$. If we can show that $|D_n^*| = 0$, then we will have shown that $|D_n| = 1$ as desired. We proceed by induction on n.

$$D_4 = \begin{pmatrix}1&\bar{1}&0&\bar{1}\\0&1&\bar{1}&1\\0&0&1&0\\1&0&0&1\end{pmatrix}$$

and hence,

$$D_4^* = \begin{pmatrix}\bar{1}&0&\bar{1}\\1&\bar{1}&1\\0&1&0\end{pmatrix}.$$

If $v_4 = \langle 1, 1, 1\rangle$, then $v_4.D_4^* = 0$. Thus, D_4^* has a nontrivial column null-space, completing the base case.

Inductively define a vector v_n, represented as a $n-3 \times n-1$ matrix, in terms of an already defined vector v_{n-2}. To do so, first augment v_{n-2} with 0's around the boundary and denote it with $\widehat{v}_{n-2}$, e.g.,

$$\widehat{v}_4 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Next, define the vector w_n to be the $n-3 \times n-1$ matrix of rows of 1's alternating with rows of 0's, e.g.,

$$w_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Last, define the vector y_n to be the $n-3 \times n-1$ matrix with 0's except for the last row, which is 1's alternating with 0's indented from the right and left 2 units, e.g.,

$$y_8 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Putting the pieces together, recursively define

$$v_n = \widehat{v}_{n-2} + w_n + y_n.$$

For example,

$$v_6 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 2 & 1 & 1 \end{pmatrix}, \qquad v_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 2 & 2 & 2 & 1 & 1 \\ 0 & 1 & 1 & 2 & 1 & 1 & 0 \\ 1 & 1 & 2 & 1 & 2 & 1 & 1 \end{pmatrix}$$

and

$$v_{10} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 2 & 2 & 2 & 2 & 2 & 1 & 1 \\ 0 & 1 & 1 & 2 & 2 & 2 & 1 & 1 & 0 \\ 1 & 1 & 2 & 2 & 3 & 2 & 2 & 1 & 1 \\ 0 & 1 & 1 & 2 & 1 & 2 & 1 & 1 & 0 \\ 1 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 1 \end{pmatrix}.$$

We claim that v_n is a nontrivial vector in the column null-space of D^*_n.

The image of one of the vectors v_n, w_n and $\widehat{v}_n$ dotted with O'_n can be written as a $n \times n$ matrix, the *image matrix.* D^*_n is a matrix which is a selection of columns of O'_n. Hence, the image of one of the vectors v_n, w_n and $\widehat{v}_n$, dotted with D^*_n is a selection of entries from the image matrix. Call these entries *pivot images.* The location of the pivot images are marked with $*$ for $n = 4$ in

$$\begin{pmatrix} - & * & * & - \\ - & - & - & * \\ - & - & - & - \\ - & - & - & - \end{pmatrix}$$

and for $n = 6$ in

$$\begin{pmatrix} - & * & * & * & * & - \\ * & * & * & * & * & - \\ * & * & * & * & * & - \\ - & - & - & - & - & * \\ - & - & - & - & - & - \\ - & - & - & - & - & - \end{pmatrix}.$$

The induction assumption means that $v_n.D^*_n = 0$, i.e., $v_n.O'_n$ is 0 for the $n - 3 \times n - 1$ pivot images.

Due to the antisymmetric nature of the octagons and the vertical symmetry of v_n, $v_n.O'_n$ is antisymmetric. Hence, we can focus on the left side of the image matrices, an observation that simplifies the proof.

The *stamp* of a unit vector is the set of locations of the images of the dot product of this unit vector with O'_n and is contained in the 4×4 square 1 unit to the left, 2 units to the right and 3 units down from the namesake location. The *stamp* of a vector is the union of the stamps of each nonzero component of the vector. We now work in the "$n+2$" environment to complete the induction step. $\widehat{v}_n$ has no stamp in the top row. Using the induction assumption, we claim that $\widehat{v}_n.O'_{n+2}$ is in addition 0 for the block of size $n-3 \times n-2$ horizontally centered and 1 unit down from the top. For example,

$$\hat{v}_4.O'_6 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & \overline{1} & 0 \\ \overline{1} & \overline{1} & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & \overline{1} & \overline{1} \\ \overline{1} & \overline{1} & \overline{1} & 1 & \overline{1} & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & \overline{1} & \overline{1} & \overline{1} \\ 0 & \overline{1} & 0 & \overline{1} & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

In the "n" environment, the images in this block only came from octagons with indices above and to their left. There is no wrap around contribution to these entries. In contrast, the images in the 2nd column, i.e., column 1, were in column 0 in the "n" environment and hence had wrap around contributions from the octagons with column index $n-2$.

$w_{n+2}.O'_{n+2}$ is the sum of the first $\frac{n}{2}$ even-indexed rows of octagons less the $n+1$st octagon in each of these rows. Since the octagons with row index $2i$ sum to 0,

$$w_{n+2}.O'_{n+2} = -\sum_{i=0}^{\frac{n}{2}-1} o_{2i,n+1}.$$

Since the octagons with column index $n+1$ sum to 0,

$$w_{n+2}.O'_{n+2} = o_{n,n+1} + \sum_{i=0}^{\frac{n}{2}-1} o_{2i+1,n+1}.$$

O'_{n+2} does not include these octagons in its row space, but we can temporarily put them in and work with O_{n+2} instead. From the above expansion, the augmented version of w_{n+2}, w^*_{n+2}, could then be written as the matrix with 0's alternating with 1's in the rightmost column and 0's elsewhere plus a 1 in the n, $n+1$ spot.

Lemma 5.4.3. *The dot product of a column (row) of 1's alternating with 0's with O'_n is the vertical (horizontal) checkerboard pattern of 4 adjacent columns (rows) of alternating 1's and -1's. Each "square" in the checkerboard has width 2 and height 1 (width1 and* *height 2). We illustrate in the row case:*

$$\begin{array}{ccccc} \cdots & 1 & \bar{1} & 1 & \cdots \\ \cdots & 1 & \bar{1} & 1 & \cdots \\ \cdots & \bar{1} & 1 & \bar{1} & \cdots \\ \cdots & \bar{1} & 1 & \bar{1} & \cdots \end{array}.$$

In the case of rows, the checkerboard starts in the namesake row and extends down. In the case of columns, the checkerboard starts 1 unit to the left of the namesake column and extends to the right. In both cases, the plus signs are in sync with the locations of the 1's in the preimage.

We demonstrate the checkerboard with w_8. w_8^* is essentially a vector of alternating 0's and 1's in column $n+1$, with the 1's in the odd indexed rows. The location of a 1 in the $n, n+1$ spot destroys the pattern in the first and last 2 rows.

$$w_8.O_8' = w_8^* O_8 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & \bar{1} \\ 0 & \bar{1} & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & \bar{1} & \bar{1} \\ \bar{1} & \bar{1} & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & \bar{1} & \bar{1} \\ \bar{1} & \bar{1} & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & \bar{1} & 0 \\ \bar{1} & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

The stamp of y_{n+2} is in the last 4 rows of which only the fourth to last row, row $n-2$ has pivot images in its stamp.

To complete the induction step and show that

$$v_{n+2}.D_{n+2}^* = 0,$$

it suffices to show, for the pivot images, that

1. in columns 0 and 1, rows 1 to n, $\widehat{v}_n.O_{n+2}'$ is the opposite of $w_{n+2}.O_{n+2}'$;
2. in row $n-1$, columns 2 to $\frac{n}{2}+1$, $\widehat{v}_n.O_{n+2}'$ is the opposite of $y_{n+2}.O_{n+2}'$.

The top and bottom few entries of a column and the leftmost and rightmost few entries of a row are *endpoints*. Only the first 2 nonzero columns of $\widehat{v}_n$ have a stamp in the first 2 columns of $\widehat{v}_n.O_{n+2}'$. The second column of $\widehat{v}_n$ is a column of 1's, which we know to be

0, except near the endpoints. The first column of $\widehat{v}_n$ is an alternating column of 1's and by Lemma 5.4.3, has an image in column's 0 and 1 of alternating horizontal pairs of 1's and -1's, except near the endpoints. The horizontal pairs of 1's are in the odd-indexed rows, precisely the opposite of $w_{n+2}.O'_{n+2}$. At the endpoints, a quick check shows that they match up there too, atleast for the pivot images and the image $(n-1,0)$, which, due to the antisymmetry, gives us the result for the pivot image $(n-1,n+1)$.

The last 3 nonzero rows of of $\widehat{v}_n$ are the only part of $\widehat{v}_n$ which has a stamp in row $n-1$. If we subtract off rows of 1's and almost rows of 1's, the defects of which only impact near the end of the row, we are left with an alternating pattern of 1's and 0's:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & \cdots \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & \cdots \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & \cdots \end{pmatrix}.$$

If we throw in y_{n+2}, it adds a new row to the above pattern:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & \cdots \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & \cdots \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & \cdots \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & \cdots \end{pmatrix}.$$

The progressively indented nature of this pattern going up is a result of the additions of y_{n+2}, y_n, y_{n-2} and y_{n-4} in the recursive definition of v_{n+2}. By Lemma 5.4.3, the contribution to the row $n-2$ of $\widehat{v}_n.O'_{n+2}$ from the first row of alternating 1's will cancel with the contribution from that of the 3rd row. The 2nd and 4th row contributions also will cancel, leaving another easy check near the endpoints. □

Chapter 6

Pandiagonal symmetries

6.1 Definition and theorem

A *pandiagonal symmetry* is a permutation of the entries in a square which preserves the set of columns, rows, primary and secondary diagonals, thought of as one big set. For a particular order, there may be other symmetries which preserve the set of P-squares. In fact, in Section 8.2, we present additional symmetries for order 4.

An *affine transformation on the matrix coordinates* sends

$$\begin{bmatrix} i \\ j \end{bmatrix} \mapsto \begin{bmatrix} ai + bj + i_0 \\ ci + dj + j_0 \end{bmatrix} = Q \begin{bmatrix} i \\ j \end{bmatrix} + \begin{bmatrix} i_0 \\ j_0 \end{bmatrix} \text{ where } Q = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

The transformation is *linear* when the affine part, $\langle i_0, j_0 \rangle$, is 0. When the linear part is the identity, the transformation is a *torus translation* τ^{i_0,j_0}. $\tau^{i_0,0}$ is a *row* translation. τ^{0,j_0} is a *column* translation. The group of torus translations is a direct product of the row and column translations.

An example of a linear transformation is

$$Q \begin{bmatrix} i \\ j \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} = \begin{bmatrix} i \\ -j \end{bmatrix}.$$

Q preserves the rows, reverses the columns $1, \ldots, n-1$ and switches the primary diagonals $0, 1, \ldots, n-1$ with the secondary diagonals $0, n-1, \ldots, 1$ as illustrated below.

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 0 & 1 & 2 \\ 2 & 3 & 0 & 1 \\ 1 & 2 & 3 & 0 \end{pmatrix} \Rightarrow \begin{pmatrix} 0 & 3 & 2 & 1 \\ 3 & 2 & 1 & 0 \\ 2 & 1 & 0 & 3 \\ 1 & 0 & 3 & 2 \end{pmatrix}$$

Theorem 6.1.1. *Any pandiagonal symmetry is an affine transformation with the linear part taken from the following list:*

for any n

$$\left\{ \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}, \begin{bmatrix} \alpha & 0 \\ 0 & -\alpha \end{bmatrix}, \begin{bmatrix} 0 & \alpha \\ \alpha & 0 \end{bmatrix}, \begin{bmatrix} 0 & \alpha \\ -\alpha & 0 \end{bmatrix} : \gcd(\alpha, n) = 1 \right\} \tag{6.1.1}$$

additionally, for n ***odd***

$$\left\{ \begin{bmatrix} \alpha & \alpha \\ \alpha & -\alpha \end{bmatrix}, \begin{bmatrix} \alpha & -\alpha \\ \alpha & \alpha \end{bmatrix}, \begin{bmatrix} \alpha & \alpha \\ -\alpha & \alpha \end{bmatrix}, \begin{bmatrix} -\alpha & \alpha \\ \alpha & \alpha \end{bmatrix} : \gcd(\alpha, n) = 1 \right\} \tag{6.1.2}$$

Recall the Euler phi function,

$$\varphi(n) = \#\{\, i \mid 0 \leq i \leq n-1 \text{ and } \gcd(i, n) = 1 \,\}.$$

Corollary 6.1.2.

$$\#\{\textit{pandiagonal symmetries}\} = \begin{cases} 8\varphi(n)n^2 & \textit{for } n \textit{ odd,} \\ 4\varphi(n)n^2 & \textit{for } n \textit{ even.} \end{cases}$$

The additional operations for the odd P-squares are the ones which switch the rows and columns with the primary and secondary diagonals.

Below, we give a proof that the affine transformations listed in Theorem 6.1.1 are precisely the affine transformations on the indices which are pandiagonal symmetries. The more tedious proof that these are in fact all the pandiagonal symmetries is given in Section 6.2.

Partial proof of Theorem 6.1.1. Call each element in the the set of columns, rows, primary diagonals and secondary diagonals a *line*. Our goal is to determine which affine transformations send each line to some other line. The torus translations τ^{i_0, j_0} clearly preserve the set of lines. Restrict to the linear part. Linear transformations, by their nature, send sets of parallel lines to other sets of parallel line, e.g., a linear transformation can send the rows to columns, but can not send one of the rows to a column and another row to a diagonal. We use the following symbols for the kinds of lines:

columns $\vert$	rows $-$	primary diagonals $\backslash$	secondary diagonals $/$

Let us first examine, for each kind of line, what is required for it to be mapped to another kind of line.

From $\vert$ Slope of $\vert$ is $\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$ and $Q\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right] = \left[\begin{smallmatrix}a\\c\end{smallmatrix}\right]$.

image of $\vert$	slope of image	consequence
$\vert$	$\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$	$c = 0$
$-$	$\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$	$a = 0$
$\backslash$	$\left[\begin{smallmatrix}1\\1\end{smallmatrix}\right]$	$a = c$
/	$\left[\begin{smallmatrix}1\\-1\end{smallmatrix}\right]$	$a = -c$

From $-$ Slope of $-$ is $\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$ and $Q\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right] = \left[\begin{smallmatrix}b\\d\end{smallmatrix}\right]$.

image of $-$	slope of image	consequence
$\vert$	$\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$	$d = 0$
$-$	$\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$	$b = 0$
$\backslash$	$\left[\begin{smallmatrix}1\\1\end{smallmatrix}\right]$	$b = d$
/	$\left[\begin{smallmatrix}1\\-1\end{smallmatrix}\right]$	$b = -d$

From $\backslash$ Slope of $\backslash$ is $\left[\begin{smallmatrix}1\\1\end{smallmatrix}\right]$ and $Q\left[\begin{smallmatrix}1\\1\end{smallmatrix}\right] = \left[\begin{smallmatrix}a+b\\c+d\end{smallmatrix}\right]$.

image of $\backslash$	slope of image	consequence
$\vert$	$\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$	$c = -d$
$-$	$\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$	$a = -b$
$\backslash$	$\left[\begin{smallmatrix}1\\1\end{smallmatrix}\right]$	$a + b = c + d$
/	$\left[\begin{smallmatrix}1\\-1\end{smallmatrix}\right]$	$a + b + c + d = 0$

From / Slope of / is $\left[\begin{smallmatrix}1\\-1\end{smallmatrix}\right]$ and $Q\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right] = \left[\begin{smallmatrix}a-b\\c-d\end{smallmatrix}\right]$.

image of /	slope of image	consequence
$\vert$	$\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$	$c = d$
$-$	$\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$	$a = b$
$\backslash$	$\left[\begin{smallmatrix}1\\1\end{smallmatrix}\right]$	$a + d = b + c$
/	$\left[\begin{smallmatrix}1\\-1\end{smallmatrix}\right]$	$a + c = b + d$

To $\backslash$ From	$\vert$	$-$	$\backslash$	$/$
$\vert$	$c = 0$	$d = 0$	$c = -d$	$c = d$
$-$	$a = 0$	$b = 0$	$a = -b$	$a = b$
$\backslash$	$a = c$	$b = d$	$a + b = c + d$	$a + d = b + c$
$/$	$a = -c$	$b = -d$	$a + b + c + d = 0$	$a + c = b + d$

Table 6.1: Requirements for one type of line to be mapped to another.

We summarize the above investigation as Table 6.1.

From the $4! = 24$ possibilities, corresponding to the permutations of the 4 types of lines, the number can be cut down to 8 with the following lemma.

Lemma 6.1.3. *In a linear transformation of the matrix indices, the rows and columns are either sent to the rows and columns as a set or to the diagonals, i.e., if we place the rows and columns as opposite vertices of a square with the 2 types of diagonals occupying the other vertices, then the possible permutations correspond at most to the dihedral action on this square.*

Proof of Lemma. Let us see what happens when we switch, for example $-$ and $\backslash$, keeping the other 2 types of lines fixed. From Table 6.1, $c = 0$, $b = d$, $a = -b$ and $a + c = b + d$, which implies that $b = d = -a$, and $3a = 0$. In addition Q must be invertible. Hence, $Q = \begin{bmatrix} a & -a \\ 0 & -a \end{bmatrix}$, and $\gcd(-a^2, n) = 1$, which is equivalent to requiring that $\gcd(a, n) = 1$. This is a contradiction unless $n = 3$, but as we will see in Proposition 7.2.1, there are no nontrivial P-squares of degree 3.

While the other cases could be treated similarly, we give a geometric explanation that covers all the cases. If the rows and columns are sent to lets say the rows and primary diagonals, then the primary diagonals, using the parallelogram rule, are sent to the lines which are at a 22.5 degrees below the horizontal. Such lines are not among the 4 types in our set, except in the case $n = 3$, where they are the secondary diagonals. Since nontrivial pandiagonal squares occur only for $n > 3$, we can safely assume that $n > 3$. $\square$

We use 1 line notation to denote permutations, e.g., $-\backslash|/$ refers to the permutation $|-\backslash/ \mapsto -\backslash|/$.

$| - \backslash /$ From Table 6.1, $c = 0$, $b = 0$, $a + b = c + d$ and $a + c = b + d$, which implies that

$b = c = 0$, and $a = d$. Hence,

$$Q = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix},$$

where a^2 is invertible $\mod n$, i.e., $\gcd(a^2, n) = 1$, which is equivalent to requiring that $\gcd(a, n) = 1$.

$|-/\backslash$ $c = 0$, $b = 0$, $a + b + c + d = 0$ and $a + d = b + c$, which implies that $b = c = 0$, and $a = -d$. Hence,

$$Q = \begin{bmatrix} a & 0 \\ 0 & -a \end{bmatrix},$$

where $-a^2$ is invertible $\mod n$, i.e., $\gcd(-a^2, n) = 1$, which again is equivalent to requiring that $\gcd(a, n) = 1$.

$-|\backslash/$ $a = 0$, $d = 0$, $a + b = c + d$ and $a + c = b + d$, which implies that $a = d = 0$, and $b = c$. Hence,

$$Q = \begin{bmatrix} 0 & b \\ b & 0 \end{bmatrix},$$

where $-b^2$ is invertible $\mod n$, i.e., $\gcd(b, n) = 1$.

$-|/\backslash$ $a = 0$, $d = 0$, $a + b + c + d = 0$ and $a + d = b + c$, which implies that $a = d = 0$, and $b = -c$. Hence,

$$Q = \begin{bmatrix} 0 & b \\ -b & 0 \end{bmatrix},$$

where b^2 is invertible $\mod n$, i.e., $\gcd(b, n) = 1$.

$\backslash/|-$ $c = -d$, $a = b$, $a = c$ and $b = -d$, which implies that $a = b = c = -d$. Hence,

$$Q = \begin{bmatrix} a & a \\ a & -a \end{bmatrix},$$

where $-2a^2$ is invertible $\mod n$, i.e., $\gcd(a, n) = 1$ and n is odd.

$\backslash/-\vert$ $a=c$, $b=-d$, $a=-b$ and $c=d$, which implies that $a=-b=c=d$. Hence, $Q=\begin{bmatrix} a & -a \\ a & a \end{bmatrix}$, where $2a^2$ is invertible $\mod n$, i.e., $\gcd(a,n)=1$ and n is odd.

$/\backslash\vert-$ $a=-c$, $b=d$, $c=-d$ and $a=b$, which implies that $a=b=-c=d$. Hence,

$$Q=\begin{bmatrix} a & a \\ -a & a \end{bmatrix},$$

where $2a^2$ is invertible $\mod n$, i.e., $\gcd(a,n)=1$ and n is odd.

$/\backslash-\vert$ $a=-c$, $b=d$, $a=-b$ and $c=d$, which implies that $a=-b=-c=-d$. Hence,

$$Q=\begin{bmatrix} -a & a \\ a & a \end{bmatrix},$$

where $-2a^2$ is invertible $\mod n$, i.e., $\gcd(a,n)=1$ and n is odd.

□

6.2 Completion of proof for Theorem 6.1.1

We first look at transformations that still take types of lines to types of lines. There are 24 permutations of the 4 types of lines. We use the 8 permutations for n odd and 4 permutations for n even of Theorem 6.1.1 to carve the 24 permutations into orbits. The following table lists the orbits for n odd as rows. For n even, each of the orbits is divided in 2. This division is indicated by the double vertical line.

$\vert-\backslash/$	$\vert-/\backslash$	$-\vert\backslash/$	$-\vert/\backslash$	$\backslash/\vert-$	$\backslash/-\vert$	$/\backslash\vert-$	$/\backslash-\vert$
$\vert\backslash-/$	$\vert/-\backslash$	$-\backslash\vert/$	$-/\vert\backslash$	$\backslash\vert/-$	$\backslash-/\vert$	$/\vert\backslash-$	$/-\backslash\vert$
$/-\backslash\vert$	$\backslash-/\vert$	$/\vert\backslash-$	$\backslash\vert/-$	$-/\vert\backslash$	$\vert/-\backslash$	$-\backslash\vert/$	$\vert\backslash-/$

We need only look at one representative from each of the orbits.

$\vert-\backslash/$ The most general permutation of $M=m_{ij}$ to $\pi(M)$ such that $\pi:\vert-\mapsto\vert-$ is $\pi(M)=m_{\sigma(i)\tau(j)}$ for some $\sigma(i),\tau(j)\in S_n$. The condition that $\pi:\backslash\mapsto\backslash$ is

$$\exists\omega\in S_n \text{ such that } \forall i,j,\ \ \sigma(i)-\tau(j)=\omega(i-j). \tag{6.2.3}$$

Specialize (6.2.3), by replacing i and j:

i	j	resulting condition
k	0	$\sigma(k) - \tau(0) = \omega(k)$
$k+1$	1	$\sigma(k+1) - \tau(1) = \omega(k)$
0	k	$\sigma(0) - \tau(k) = \omega(-k)$
1	$k+1$	$\sigma(1) - \tau(k+1) = \omega(-k)$.

(6.2.4)

The first 2 rows of (6.2.4) imply

$$\sigma(k+1) = \sigma(k) + (\tau(1) - \tau(0)).$$

If we begin with $k = 0$ and iterate, we get

$$\sigma(k) = \sigma(0) + k(\tau(1) - \tau(0)) \tag{6.2.5}$$

Similarly, the last 2 rows of (6.2.4) imply

$$\tau(k) = \tau(0) + k(\sigma(1) - \sigma(0)). \tag{6.2.6}$$

(6.2.5) and (6.2.6) together imply that π is in fact an affine transformation on the indices of the square.

all remaining orbits for n even We take care of n even for the rest of the chart with the following lemma.

Lemma 6.2.1. *If π is a permutation of the entries of M, of size n even, which carries lines to lines, then the images of the diagonals must also be diagonals.*

Proof. Recall that we can divide an even length square up into black and white squares like a checkerboard. Diagonals are either completely black or completely white. A primary diagonal and a secondary diagonal have either 0 or 2 entries in common, depending on whether their respective colors are different or are the same. More formally, the system of equations

$$i - j = a$$

$$i + j = b$$

has 2 solutions in common if a and b have the same parity and 0 solutions if they have different parity. π is a bijective map; the images of these 2 diagonals must also have 0 or 2 entries in common, forcing them to also be diagonals. □

Hence, for the remainder of this section, we may assume n is odd. In particular, only 2 orbits remain.

$|\backslash - /$ The most general permutation of $M = m_{ij}$ to $\pi(M)$ such that $\pi : |/ \mapsto |-$ is $\pi(M) = m_{\sigma(i+j)\tau(j)}$ for some $\sigma(i), \tau(j) \in S_n$. The additional condition that $\pi : - \mapsto \backslash$ is

$$\exists \omega \in S_n \text{ such that } \forall i, j,\ \ \sigma(i+j) + \tau(j) = \omega(i). \tag{6.2.7}$$

Specialize (6.2.7), by replacing i and j:

$$\begin{array}{cc|l} i & j & \text{resulting condition} \\ \hline k & 0 & \sigma(k) \quad + \ \ \tau(0) \ \ = \omega(k) \\ k & 1 & \sigma(k+1) + \ \ \tau(1) \ \ = \omega(k) \\ k+1 & -1 & \sigma(k) \quad + \tau(-1) = \omega(k+1). \end{array} \tag{6.2.8}$$

The first 2 rows of (6.2.8) imply

$$\sigma(k+1) - \sigma(k) = \tau(0) - \tau(1),$$

which, as before, implies that σ is affine. Similarly, the first and third rows of (6.2.8) imply

$$\omega(k+1) - \omega(k) = \tau(-1) - \tau(0)$$

and ω is affine.

The affineness of σ and ω together imply the affineness of τ. The affineness of σ and τ in turn imply the affineness of π.

$/ - \backslash|$ The most general permutation of $M = m_{ij}$ to $\pi(M)$ such that $\pi : -/ \mapsto -|$ is $\pi(M) = m_{\sigma(i)\tau(i+j)}$ for some $\sigma(i), \tau(j) \in S_n$. The additional condition that $\pi : | \mapsto /$ is

$$\exists \omega \in S_n \text{ such that } \forall i, j,\ \ \sigma(i) + \tau(i+j) = \omega(j). \tag{6.2.9}$$

Specialize (6.2.9), by replacing i and j:

$$\begin{array}{cc|l} i & j & \text{resulting condition} \\ \hline 0 & k & \sigma(0) \ \ + \quad \tau(k) \quad = \omega(k) \\ 1 & k & \sigma(1) \ \ + \tau(k+1) = \omega(k) \\ -1 & k+1 & \sigma(-1) + \quad \tau(k) \quad = \omega(k+1). \end{array} \tag{6.2.10}$$

The first 2 rows of (6.2.10) imply

$$\tau(k+1) - \tau(k) = \sigma(0) - \sigma(1),$$

i.e., τ is affine. Similarly, the first and third rows of (6.2.10) imply

$$\omega(k+1) - \omega(k) = \sigma(-1) - \sigma(0)$$

and ω is affine.

The affineness of τ and ω together imply the affineness of σ. The affineness of σ and τ in turn imply the affineness of π.

We lastly need to consider the possibility of mapping parallel lines to nonparallel lines or, in the language of the previous section, mapping 2 lines of the same type to 2 lines of different types. If n is odd, two nonparallel lines meet in exactly one entry. Hence, for n odd, such a mapping would mean mapping $2n$ entries to $2n-1$ entries, contradicting the bijective nature of gp. For n even, Lemma 6.2.1 has the corollary that rows and columns are mapped to rows and columns. If 2 rows are mapped to a row and column, we would again have $2n$ entries mapping to $2n-1$ entries. Hence, we have $|- \mapsto |-$ or $-|$. Moreover, if a nonparallel map exists, we can compose, if it is the latter, with one of the known maps which switch rows and columns, resulting in nonparallel map which sends $|- \mapsto |-$. Hence, we assume that rows are mapped to rows and columns are mapped to columns.

A row, which alternates in color, is sent to a row. Hence, the set of primary diagonals are sent to a set of diagonals, half of which are black and half are white. Moreover, in this image, the diagonals of one color must be of the same type, since otherwise there would be an intersection, violating the bijectivity. For obvious reasons, one type of diagonal changes color iff the other does too. Let us list out the possibilities then use the existing symmetry to reduce the number of cases we need to consider. Let $\backslash$, $\boldsymbol{\backslash}$, $/$, $\boldsymbol{/}$ stand for the white and black primary diagonals, and white and black secondary diagonals, respectively. There are 3 independent decisions each with 2 choices to be made. First, the black primaries can be mapped to primaries or secondaries. Second, the white primaries can be mapped to primaries or secondaries. Third, we decide whether there is a color swap or not. The images of the secondaries will be forced. To tabulate, $\backslash\boldsymbol{\backslash}/\boldsymbol{/}$ may be mapped to

\\//	\\//	\//\	\//\
/\\/	/\\/	//\\	//\\

The first 2 entries in the first row and the last 2 entries in the second row do not involve sending parallels to nonparallels so we eliminate them from our consideration. By composing with a torus translation we can reduce to the case where there is no color swap. Finally, a reflection over the line $x = 0$ switches primary and secondary diagonals. Hence we need only consider the case \\// is mapped to \//\. Recall that we are requiring $|-$ to map to $|-$. Hence, π is of the form $\pi(M) = \tilde{M}$, where $\tilde{m}_{i,j} = m_{\sigma(i),\tau(j)}$, for some $\sigma, \tau \in S_n$. Let white have the $0, 0$ location.

The condition \ is mapped to \ implies that

$$\exists \omega \in S_{\{0,2,\ldots,n-2\}} \text{ such that } \forall i, j \ i - j \text{ even}, \ \sigma(i) - \tau(j) = \omega(i - j). \tag{6.2.11}$$

Let k be an even number. Specialize (6.2.11) by replacing i and j:

i	j	resulting condition
k	0	$\sigma(k) - \tau(0) = \omega(k)$
$k+2$	2	$\sigma(k+2) - \tau(2) = \omega(k)$
0	k	$\sigma(0) - \tau(k) = \omega(-k)$
2	$k+2$	$\sigma(2) - \tau(k+2) = \omega(-k)$.

The first 2 rows imply

$$\sigma(k+2) - \sigma(k) = \tau(2) - \tau(0) \overset{\text{def}}{=} a.$$

Similarly, the last 2 rows imply $\tau(k+2) - \tau(k) = \sigma(2) - \sigma(0)$. Set $k = 0$ to get

$$\sigma(2) - \sigma(0) = a. \tag{6.2.12}$$

If we begin with $k = 0$ and iterate, we get

$$\sigma(2m) = \sigma(0) + ma \quad \text{and} \quad \tau(2m) = \tau(0) + ma.$$

Let k be an odd number. Specialize (6.2.11) by replacing i and j:

i	j	resulting condition
k	1	$\sigma(k) - \tau(1) = \omega(k-1)$
$k+2$	3	$\sigma(k+2) - \tau(3) = \omega(k-1)$
1	k	$\sigma(1) - \tau(k) = \omega(1-k)$
3	$k+2$	$\sigma(3) - \tau(k+2) = \omega(1-k)$
.		

The first 2 rows imply $\sigma(k+2) - \sigma(k) = \tau(3) - \tau(1)$. Define $b = \tau(3) - \tau(1)$. The last 2 rows imply $\tau(k+2) - \tau(k) = \sigma(3) - \sigma(1)$. Setting $k = 1$, we get that $\sigma(3) - \sigma(1) = b$ also. Begin with $k = 1$ and iterate to get

$$\sigma(2m+1) = \sigma(1) + mb \quad \text{and} \quad \tau(2m+1) = \tau(1) + mb.$$

The condition $\backslash$ is mapped to $/$ implies that

$$\exists \pi \in S_{\{1,3,\ldots,n-1\}} \text{ such that } \forall i,j \; i+j \text{ odd}, \; \sigma(i) - \tau(j) = \pi(i+j). \tag{6.2.13}$$

Let k be an even number. Specialize (6.2.13) by replacing i and j:

i	j	resulting condition
k	3	$\sigma(k) - \tau(3) = \pi(k+3)$
$k+2$	1	$\sigma(k+2) - \tau(1) = \pi(k+3).$

Subtracting the rows, $\sigma(k+2) - \sigma(k) = \tau(1) - \tau(3) = -b$. Setting $k = 0$ and comparing with (6.2.12), we get that $a = -b$. We summarize our findings as:

$$\begin{aligned} \sigma(2m) &= \sigma(0) + ma & \tau(2m) &= \tau(0) + ma \\ \sigma(2m+1) &= \sigma(1) - ma & \tau(2m+1) &= \tau(1) - ma. \end{aligned} \tag{6.2.14}$$

We plug the expressions of (6.2.14) into the definition for ω found in (6.2.11).

$$\omega(i-j) = \sigma(i) - \tau(j) = \begin{cases} \sigma(0) - \tau(0) + \frac{i-j}{2}a & i,j \text{ even;} \\ \sigma(1) - \tau(1) - \frac{i-j}{2}a & i,j \text{ odd.} \end{cases} \tag{6.2.15}$$

These 2 definitions must be equivalent. Specializing to $i - j = 0$, we get

$$\sigma(0) - \tau(0) = \sigma(1) - \tau(1). \tag{6.2.16}$$

We also plug (6.2.14) into the definitions for π found in (6.2.13).

$$\pi(i-j) = \sigma(i) + \tau(j) = \begin{cases} \sigma(1) + \tau(0) + \frac{j-i-1}{2}a & i \text{ odd, } j \text{ even;} \\ \sigma(0) + \tau(1) + \frac{i-j-1}{2}a & i \text{ even, } j \text{ odd.} \end{cases} \tag{6.2.17}$$

These 2 definitions must be equivalent. Specializing to $i - j = 1$, we get

$$\sigma(1) + \tau(0) - a = \sigma(0) + \tau(1). \tag{6.2.18}$$

Rearranging (6.2.18),

$$a + \sigma(0) - \tau(0) = \sigma(1) - \tau(1)$$

and subtracting (6.2.16), we obtain $a = 0$, which shows that the permutations ω and π defined by (6.2.11) and (6.2.13) can not exist. Hence, for any n, no map exists which sends lines to lines and 2 parallel lines to nonparallel lines. This completes the proof for Theorem 6.1.1.

Chapter 7

Order 3 squares

7.1 Magic squares of order 3 and cyclic squares

Given the coefficient matrix C of a linear system of equations, only certain sets of columns may be used as pivoting columns to row reduce C. If C is of rank r, these sets are precisely those corresponding to nonzero $r \times r$ subdeterminants D. A set of variables S which corresponds to the complement of one of these sets of columns is a *determining set.* If, in addition, $D = \pm 1$, S is a *monic* determining set: any integer solution to the system can be expressed as an integer combination of the variables in S.

Recall that $\mathcal{M}_n$ is the set of magic squares of order n with nonnegative integer entries. The entries not marked x are a monic determining set for $\mathcal{M}_3$:

$$\boxed{\begin{array}{ccc} a & x & b \\ x & c & x \\ d & x & e \end{array}}.$$

Proposition 7.1.1. *Every magic square of order 3 may be written in the form*

$$\begin{pmatrix} a & d+e-c & b \\ b+e-c & c & a+d-c \\ d & a+b-c & e \end{pmatrix}. \tag{7.1.1}$$

Proof. Using the dihedral symmetry, it suffices to find an expression for the 0,1th entry in terms of the claimed determining set. Such an expression follows immediately from the

Y relation

$$\begin{array}{|ccc|}\hline 1&0&1\\ 1&0&1\\ 1&0&1\\ \hline\end{array} - \begin{array}{|ccc|}\hline 1&1&1\\ 1&1&1\\ 0&0&0\\ \hline\end{array} = \begin{array}{|ccc|}\hline 0&\bar{1}&0\\ 0&\bar{1}&0\\ 1&0&1\\ \hline\end{array} = 0.$$

□

A *cyclic* square of order n has a *start* a and a *step* b. In the 0th row, place a 1 in the ath column and 0's elsewhere. In the 1st row, place a 1 in the $a+b$th column. In the 2nd row, place a 1 in the $a+2b$th column. In the ith row, place a 1 in the $a+ib$th column.

$$C_a^b = \|\chi(j \equiv_n a+ib)\|_{i,j=0}^{n-1} \tag{7.1.2}$$

Corollary 7.1.2. *Every magic square of order 3 with vanishing 1,1th entry may be written in the form*

$$\begin{array}{ccc} a & d+e & b\\ b+e & 0 & a+d\\ d & a+b & e \end{array}$$

In other words these matrices are arbitrary nonnegative integral linear combinations of the following 4 cyclic matrices,

$$\begin{gathered} C_1^1 = \begin{array}{|ccc|}\hline 0&1&0\\ 0&0&1\\ 1&0&0\\ \hline\end{array}, \quad C_2^1 = \begin{array}{|ccc|}\hline 0&0&1\\ 1&0&0\\ 0&1&0\\ \hline\end{array},\\ C_0^2 = \begin{array}{|ccc|}\hline 1&0&0\\ 0&0&1\\ 0&1&0\\ \hline\end{array}, \quad C_1^2 = \begin{array}{|ccc|}\hline 0&1&0\\ 1&0&0\\ 0&0&1\\ \hline\end{array}. \end{gathered} \tag{7.1.3}$$

As a result,

$$\sum_{A \in \mathcal{M}_3 \ s.t. \ a_{1,1}=0} X(A) = \frac{1}{(1-X(C_1^1))(1-X(C_2^1))(1-X(C_0^2))(1-X(C_1^2))}. \tag{7.1.4}$$

Let a *cycle* be a full set of cyclics of the same step, e.g. $\{C_0^1, C_1^1, C_2^1\}$. Notice that $\{C_1^1, C_2^1, C_0^2, C_1^2\}$ is a maximal set of cyclics which does not contain a cycle.

Recall that J is the matrix with all entries 1. Any $A \in \mathcal{M}_3$ may be decomposed into two magics

$$A = \min(A)J + (A - \min(A)J) = \min(A)J + A^\circ, \qquad (7.1.5)$$

where A° has a zero entry in say the i, jth location. Let $\tau = \tau^{i-1,j-1}$, then τ^{-1} moves the 0 entry to the 1,1th position. Using Corollary 7.1.2, decompose $\tau^{-1}(A^\circ)$ into a nonnegative integer combination of C_1^1, C_2^1, C_0^2, and C_1^2. Applying τ to both sides gives a decomposition for A°.

Proposition 7.1.3. *The set of cyclic matrices of a given step is invariant under the group of torus translations.*

Proof. Set the order to n. Applying the column translation $\tau^{0,k}$ to C_a^b, is equivalent to adding k to the start a, i.e.,

$$\tau^{0,k}(C_a^b) = C_{a+k}^b.$$

To analyze row translations, we introduce new notation. The *row sequence* of a cyclic is the ordered list recording the columns of the nonzero entries as one descends the matrix by row. For the cyclic C_a^b, the sequence is

$$(a, b + a, b(2) + a, \ldots, b(n-1) + a).$$

If the sequence of A is $(a_0, a_1, \ldots, a_{n-1})$, then

$$\tau^{k,0}(A) = (a_{-k}, a_{-k+1}, \ldots, a_0, a_1, \ldots, a_{-k-1}),$$

where the subscript is as usual calculated modulo n. For our particular sequence,

$$\begin{aligned}\tau^{k,0}(C_a) &= (b(-k) + a, b(-k+1) + a, \ldots, a, b + a, \ldots, b(-k-1) + a)) \\ &= C_{b(-k)+a}^b.\end{aligned}$$

□

To a zero in the i, jth position, there is a unique set of 4 cyclics, 2 of step 1 and 2 of step 2, called an admissible set. There are 9 such sets. Conversely, there are $\binom{3}{2}\binom{3}{2} = 9$ sets of cyclics that do not contain a cycle. Hence, by the pigeonhole principle,

Lemma 7.1.4. *The 9 admissible 4-tuples are precisely the 4-tuples of cyclics that do not contain a cycle.*

This places us in a position to prove our basic result.

Theorem 7.1.5. *Every magic square $A \in \mathcal{M}_3$ may be uniquely written as*

$$A = jJ + a_0C_0^1 + a_1C_1^1 + a_2C_2^1 + b_0C_0^2 + b_1C_1^2 + b_2C_2^2 \tag{7.1.6}$$

where j is an arbitrary integer ≥ 0 and a_0, a_1, a_2, b_0, b_1, and b_2 are integers ≥ 0 subject to the condition that

$$0 = a_0a_1a_2 = b_0b_1b_2 \tag{7.1.7}$$

or equivalently

$$\sum_{A\in\mathcal{M}_3} X(A) = \frac{1}{1-X(J)}\prod_{i=1}^{2}\Bigg(\frac{1}{(1-X(C_0^i))(1-X(C_1^i))} + \frac{X(C_2^i)}{(1-X(C_0^i))(1-X(C_2^i))} + \frac{X(C_1^i)X(C_2^i)}{(1-X(C_1^i))(1-X(C_2^i))}\Bigg). \tag{7.1.8}$$

In particular, the generating function for the index is

$$\begin{aligned}\sum_{A\in\mathcal{D}_3} t^{\operatorname{ind} A} &= \frac{1}{1-t^3}\left(\frac{1+t+t^2}{(1-t)^2}\right)^2\\ &= \frac{(1+t+t^2)}{(1-t)^5}\end{aligned}$$

Proof of Theorem. (7.1.6) and (7.1.7) follow from what has been said. We derive (7.1.8) geometrically. (7.1.6) and (7.1.7) imply that A° is the direct product of 2 cones, each of whose cross sections is a triangle with the interior removed. Let UVW be one of these triangles. To perform a shelling of the boundary of cone UVW, pick any of the integral points on the cone UV arbitrarily. Hence

$$\frac{1}{(1-X(U))(1-X(V))}$$

To avoid an overlap, the integral points chosen from UW must have a positive W component,

$$\frac{X(W)}{(1-X(U))(1-X(W))}.$$

Similarly, the integral points chosen from VW must have positive V and W components,

$$\frac{X(V)X(W)}{(1-X(V))(1-X(W))}.$$

□

Let $\triangle_d$ be the simplex of dimension d. The cross section of $\mathcal{M}_3$ is the dual of the direct product $\triangle_2 \times \triangle_2$. The Schlegel diagram of $\triangle_2 \times \triangle_2$, with 9 vertices and 6 facets, is easy to sketch. Begin with 3 triangles in parallel, the middle one smaller than the outer 2 (Figure 7.1). Finish by connecting the corresponding vertices of the triangles (Figure 7.2).

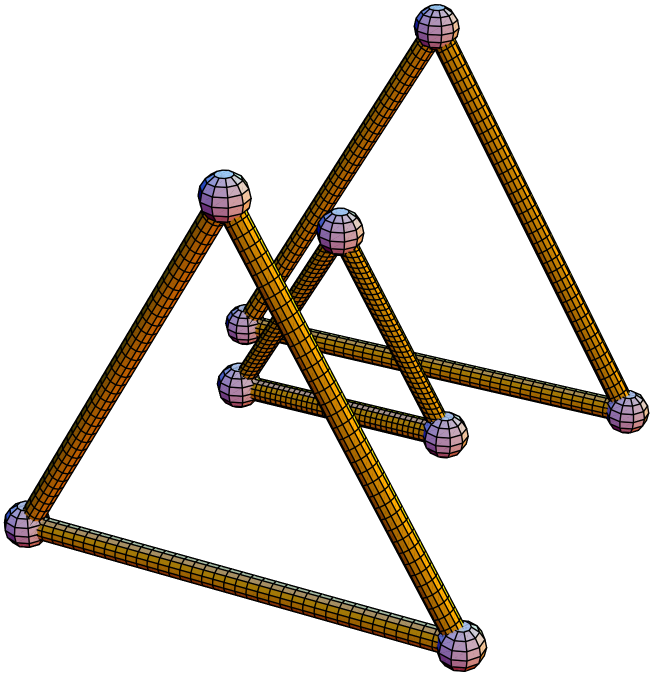


Figure 7.1: 3 triangles in parallel.

For the dual of $\triangle_2 \times \triangle_2$, $(\triangle_2 \times \triangle_2)^*$, begin with 2 linked triangles (Figure 7.3). Complete by constructing edges between each of the vertices of one of the triangles with all the vertices of the other triangle, i.e., form the complete graph on 6 vertices (Figure 7.4).

The 6 vertices correspond to the 6 cyclics, the 9 facets each correspond to an entry of the matrix set equal to 0. Each facet is a tetrahedron with an admissible set as vertices. One remarkable thing about this polytope is that it is neighborly, meaning that all pairs of vertices are connected with an edge, yet it is not a simplex. This phenomenon does not occur in dimension 3.

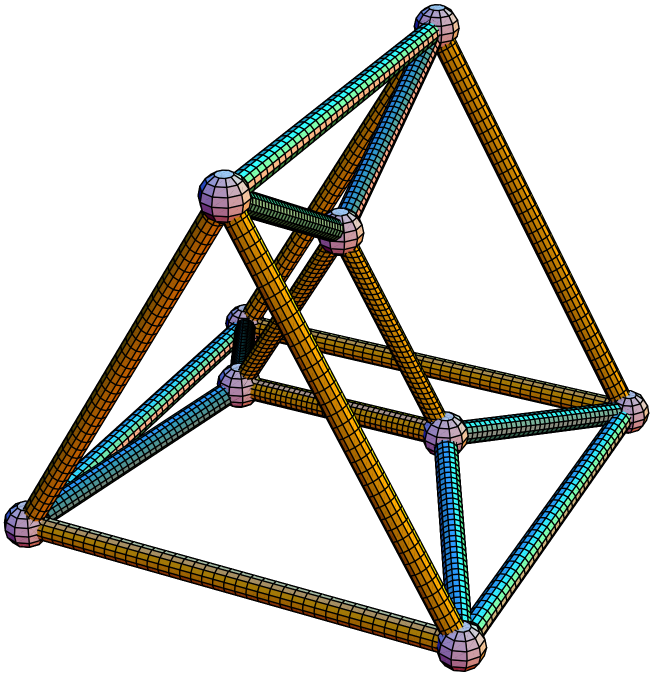


Figure 7.2: Schlegel diagram for $\triangle_2 \times \triangle_2$.

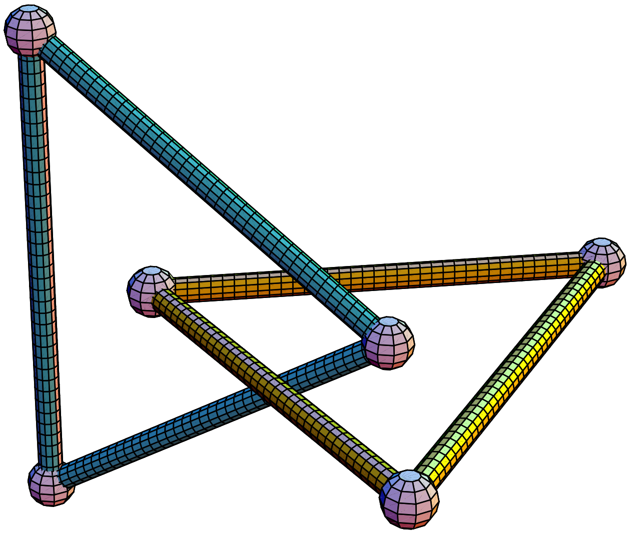


Figure 7.3: 2 linked triangles.

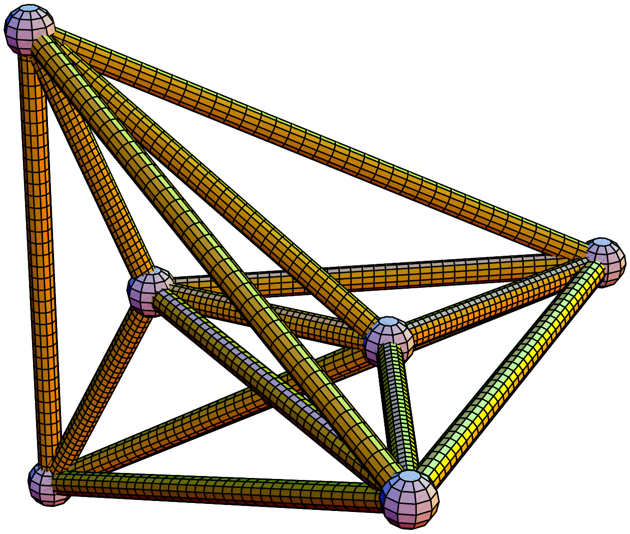


Figure 7.4: Schlegel diagram for $(\triangle_2 \times \triangle_2)^*$.

7.2 P-squares of orders 2 and 3 and reduction of order

Given a permutation $\sigma = (\sigma_0, \sigma_1, \ldots, \sigma_{n-1}) \in S_n = S_{\{0,\ldots,n-1\}}$, its matrix is

$$m(\sigma) = \|\chi(j = \sigma_i)\|_{i,j=0}^{n-1}$$

It is well known that any magic square may be written uniquely as a nonnegative integral linear combination of permutation matrices, i.e.,

$$A = \sum_{\sigma \in S_n} a_\sigma m(\sigma). \tag{7.2.9}$$

For order 3, this fact is a consequence of Theorem 7.1.5.

We can view (7.2.9) as a change of variables. Any $\{a_\sigma\}$ by definition translates into a matrix with equal row and column sums. To solve the Diophantine system, $\{a_\sigma\}$ needs to satisfy equations gotten by substituting (7.2.9) into the equal diagonal sum equations. The number of equations is reduced by a factor of 2, and for orders 2 and 3, the number of variables also is reduced. If we lexicographically order the permutations, then for order 2 matrices, we get

$$A = \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix}.$$

Equal diagonals means $a_1 = a_2$, i.e.,

$$A = a_1 \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

For order 3,

$$A = \begin{pmatrix} a_1 + a_2 & a_3 + a_4 & a_5 + a_6 \\ a_3 + a_5 & a_1 + a_6 & a_2 + a_4 \\ a_4 + a_6 & a_2 + a_5 & a_1 + a_3 \end{pmatrix}. \tag{7.2.10}$$

Equal primary diagonals means

$$3a_1 + a_2 + a_3 + a_6 = 3a_4 + a_2 + a_3 + a_6 = 3a_5 + a_2 + a_3 + a_6,$$

forcing $a_1 = a_4 = a_5$. Similarly, equal secondary diagonal sums forces $a_2 = a_3 = a_6$ and

$$A = \begin{pmatrix} a_1 + a_2 & a_2 + a_1 & a_1 + a_2 \\ a_2 + a_1 & a_1 + a_2 & a_2 + a_1 \\ a_1 + a_2 & a_2 + a_1 & a_1 + a_2 \end{pmatrix} = a_1 \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} + a_2 \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

A *trivial* square is a multiple of J, the matrix with all entries 1.

Proposition 7.2.1. *There are only trivial P-squares of orders 2 and 3.*

Given a matrix A of order $n = mq$, define the *reduction* of A to order m, to be $A \downarrow_m = \|b_{ij}\|_{i,j=0}^{m-1}$ where

$$b_{ij} = \sum_{k,l=0}^{n-1} \chi(k \equiv_m i \text{ and } l \equiv_m j) a_{kl}.$$

Proposition 7.2.2. *If A is a P-square of order $n = mq$, then $A \downarrow_m$ is also pandiagonal.*

Proof. Note that

$$R_t(B) = \sum_{k=0}^{n-1} \chi(u \equiv_m t) R_u(A) = qR_t(A).$$

Since the row sums of A are equal then so are the row sums of B. By the symmetry of the construction, the same is true for column sums.

For the primary diagonal sums, we need to be clever in how we order the indices. Note that $b_{r,s}$ is the sum of $a_{k,l}$ whose indices are listed in the matrix formed as follows.

Multiply m times the Cartesian product of $\{0, \ldots, q-1\}$ with itself, then add (r, s) to each entry. The result is

$$\begin{pmatrix} r, s & r, m+s & \cdots & r, (q-1)m+s \\ m+r, s & m+r, m+s & \cdots & m+r, (q-1)m+s \\ \vdots & \vdots & & \vdots \\ (q-1)m+r, s & (q-1)m+r, m+s & \cdots & (q-1)m+r, (q-1)m+s \end{pmatrix}. \qquad (7.2.11)$$

Reorder by listing as rows the primary diagonals of (7.2.11) to get

$$\begin{pmatrix} r, s & m+r, m+s & \cdots & (q-1)m+r, (q-1)m+s \\ r, m+s & m+r, 2m+s & \cdots & (q-1)m+r, s \\ \vdots & \vdots & & \vdots \\ r, (q-1)m+s & m+r, s & \cdots & (q-1)m+r, (q-2)m+s \end{pmatrix}. \qquad (7.2.12)$$

Returning to the primary diagonal sums, use (7.2.12) with r replaced with i and s with $i+t$ to get

$$\begin{aligned} F_t(B) &= \sum_{i=0}^{m-1} b_{i,i+t} \\ &= \sum_{i=0}^{m-1} a_{i,(i+t)} + a_{m+i,m+(i+t)} + \cdots + a_{(q-1)m+i,(q-1)m+(i+t)} \\ &\quad + a_{i,m+(i+t)} + a_{m+i,2m+(i+t)} + \cdots + a_{(q-1)m+i,(i+t)} \\ &\quad \vdots \\ &\quad + a_{i,(q-1)m+(i+t)} + a_{m+i,(i+t)} + \cdots + a_{(q-1)m+i,(q-2)m+(i+t)} \\ &= \sum_{i=0}^{m-1} a_{i,i+(t)} + a_{m+i,m+i+(t)} + \cdots \qquad + a_{(q-1)m+i,(q-1)m+i+(t)} \\ &\quad + a_{i,i+(m+t)} + a_{m+i,m+i+(m+t)} + \cdots + a_{(q-1)m+i,(q-1)m+i+(m+t)} \\ &\quad \vdots \\ &\quad + a_{i,i+((q-1)m+t)} + a_{m+i,m+i+((q-1)m+t)} + \cdots \\ &\qquad\qquad + a_{(q-1)m+i,(q-1)m+i+((q-1)m+t)} \end{aligned}$$

and summing each row over i,

$$= F_t(A) + F_{m+t}(A) + \cdots + F_{(q-1)m+t}(A) = qF_t(A).$$

Since the primary diagonal sums of A are equal, then so are those of B.

The reduction construction is symmetric and hence does not affect the symmetry between the 2 types of diagonals. So the secondary diagonal sums are also equal. □

Corollary 7.2.3. *1. If $A \in \mathcal{P}_{2q}$ with q odd, then* $\operatorname{ind} A$ *is even.*

2. If $A \in \mathcal{P}_{3q}$ with q not divisible by 3, then $\operatorname{ind} A$ *is divisible by 3.*

Proof. Since m is 2 or 3, Proposition 7.2.1 implies that $B = A \downarrow_m$ must be trivial. $q \operatorname{ind} A = \operatorname{ind} B = tm$, t an integer. q is not divisible by m, m prime, implies $\operatorname{ind} A$ is divisible by m (m is prime). □

7.3 R-magic squares of order 3 and the cross-polytope

Let $\mathcal{R}_n$ be the set of R-magic matrices of order n with nonnegative entries. Since the 6 cyclics (=6 permutation matrices) generate the space of magic squares, we use as starting point (7.2.10) and set the main primary diagonal sum equal to the first row sum to get

$$3a_1 + a_2 + a_3 + a_6 = a_1 + a_2 + a_3 + a_4 + a_5 + a_6, \text{ i.e.,}$$

$$2a_1 = a_4 + a_5. \tag{7.3.13}$$

Setting the main secondary diagonal sum equal to the first row sum,

$$a_1 + a_4 + a_5 + 3a_6 = a_1 + a_2 + a_3 + a_4 + a_5 + a_6, \text{ i.e.,}$$

$$2a_6 = a_2 + a_3. \tag{7.3.14}$$

Multiplying (7.2.10) by 2 and substituting in (7.3.13) and (7.3.14), we get

$$2A = \begin{pmatrix} 2a_2 + a_4 + a_5 & 2a_3 + 2a_4 & 2a_5 + a_2 + a_3 \\ 2a_3 + 2a_5 & a_2 + a_3 + a_4 + a_5 & 2a_2 + 2a_4 \\ 2a_4 + a_2 + a_3 & 2a_2 + 2a_5 & 2a_3 + a_4 + a_5 \end{pmatrix}$$

$$= a_2 \boxed{\begin{matrix} 2 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 0 \end{matrix}} + a_3 \boxed{\begin{matrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{matrix}} + a_4 \boxed{\begin{matrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{matrix}} + a_5 \boxed{\begin{matrix} 1 & 0 & 2 \\ 2 & 1 & 0 \\ 0 & 2 & 1 \end{matrix}}$$

Define these new matrices to be B, C, D and E respectively. Dividing by 2,

$$A = \frac{a_2}{2}B + \frac{a_3}{2}C + \frac{a_4}{2}D + \frac{a_5}{2}E.$$

B, C, D and E are not independent: $B + C = D + E = 2J$. Focusing on the 0,2th entry forces $a_2 + a_3$ to be even, similarly $a_4 + a_5$ must be even. Conversely, if $a_2 + a_3$ and $a_4 + a_5$ are even, then A is integral.

As in the case of the pandiagonals of order 4 and the magics of order 3, extract a multiple of the trivial leaving $A°$. This time we need not examine where is the zero. Neither both a_2 and a_3 are present, nor both a_4 and a_5. Hence, a_2, a_3, a_4 and a_5 are all even. There are no other conditions. We have proven

Theorem 7.3.1. *Let*

$$B = \boxed{\begin{matrix} 2 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 0 \end{matrix}}, \quad C = \boxed{\begin{matrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{matrix}}, \quad D = \boxed{\begin{matrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{matrix}} \quad \textit{and} \quad E = \boxed{\begin{matrix} 1 & 0 & 2 \\ 2 & 1 & 0 \\ 0 & 2 & 1 \end{matrix}}.$$

Then every R-magic square $A \in \Re_3$ may be uniquely written as

$$A = jJ + bB + cC + dD + eE, \tag{7.3.15}$$

where j is an arbitrary integer ≥ 0 and b, c, d, and e are integers ≥ 0 subject to the condition that

$$0 = bc = de \tag{7.3.16}$$

or equivalently

$$\sum_{A \in \Re_3} X(A) = \frac{1}{1 - X(J)} \left(\frac{1}{1 - X(B)} + \frac{X(C)}{1 - X(C)} \right) \left(\frac{1}{1 - X(D)} + \frac{X(E)}{1 - X(E)} \right). \tag{7.3.17}$$

In particular, the generating function for the index is

$$\begin{aligned} \sum_{A \in \Re_3} t^{\operatorname{ind} A} &= \frac{1}{1 - t^3} \left(\frac{1 + t^3}{1 - t^3} \right)^2 \\ &= \frac{(1 + t^3)^2}{(1 - t^3)^3}. \end{aligned}$$

Corollary 7.3.2. *There is a one to one correspondence between*

1. *R-magic squares of order 3, whose minimal entry is in the 0,1th location;*

2. squares of order 3 whose rows and columns are arithmetic progressions.

Proof. Any R-magic square which satisfies condition 1 will be an arbitrary combination of J, B and E. The entries are as follows:

$$\begin{pmatrix} m+2b+e & m & m+b+2e \\ m+2e & m+b+e & m+2b \\ m+b & m+2b+2e & m+e \end{pmatrix}.$$

To get the square of arithmetic progressions, rearrange the terms.

$$\begin{pmatrix} m & m+b & m+2b \\ m+e & m+b+e & m+2b+e \\ m+2e & m+b+2e & m+2b+2e \end{pmatrix}$$

□

The *cross section* of the cone P

$$CS_c(P) = \{\, A \in P \mid \operatorname{ind}(A) = c \,\}.$$

Since B, C, D, E and J all have index 3, they all lie on $CS_3(\mathcal{R}_3)$. Note that J is the midpoint of BC and also of DE. Subtract J from B and D:

$$B - J = \boxed{\begin{array}{ccc} 1 & \bar{1} & 0 \\ \bar{1} & 0 & 1 \\ 0 & 1 & \bar{1} \end{array}}, \quad D - J = \boxed{\begin{array}{ccc} 0 & 1 & \bar{1} \\ \bar{1} & 0 & 1 \\ 1 & \bar{1} & 0 \end{array}}. \qquad (7.3.18)$$

A *regular d-cross-polytope* is the convex hull of the d pairs of points on d orthogonal lines intersecting in a common point O which are a distance D from O. The 2 and 3-cross-polytopes are the square and octahedron, respectively.

Since the inner product $(B - J, D - J) = 0$, the cross section $CS_3(\mathcal{R}_3)$ is a 2-cross-polytope, with center J and with B and C, D and E at opposite corners.

Finding a R-magic square of order 3 with distinct entries which are perfect squares is one of Richard Guy's unsolved problems [Guy94]. In [Rob96], John Robertson uses the equivalence of Corollary 7.3.2 to connect this unsolved problem to the existence of some triples of rational right triangles which is in turn connected to a condition on elliptic curves of the form $y^2 = x^3 - n^2x$, where n is the geometric mean of the legs of a Pythagorean triple.

Unlike the magics, the R-magic squares are not closed under matrix multiplication. However, van den Essen [vdE90], using the Cayley-Hamilton theorem, has shown that the odd powers of order 3 magics are magic.

Chapter 8

P-squares of order 4

8.1 Strongly magic squares

Padmakumar [Pad97] calls a R-square which is also a W-square a *strongly magic* square. We shall show that, in the case $n = 4$, the notions of strongly magic and pandiagonal are equivalent.

Proposition 8.1.1. *Let A be a 4×4 square. A is strongly magic* iff *A is pandiagonal.*

Proof. Suppose that A is strongly magic. To show that A is pandiagonal, by symmetry, it suffices to show that the entries in the diagonals labeled 1 and 2 each sum to the index.

$$\begin{pmatrix} o & 2 & 1 & o \\ o & o & 2 & 1 \\ 1 & o & o & 2 \\ 2 & 1 & o & o \end{pmatrix}$$

We take care of diagonal 1 quickly. The entries marked with 1 in the matrix below correspond to a pair of blocks.

$$\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

Subtract off the principal secondary diagonal to get

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

which is precisely the diagonal 1. Note how the matrix is shorthand for the linear functional which operates by dot product on A, thought of as a vector.

Adding (4.4.17) and the principal secondary diagonal, we get

$$\begin{pmatrix} 0 & 1 & 0 & \bar{1} \\ 0 & 0 & 0 & 0 \\ 0 & \bar{1} & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

which is precisely the 2nd diagonal we needed to show, finishing the forward direction of the proposition.

To show P-squares of order 4 are strongly magic, recall that any of the sets of P-squares is torus invariant. Hence, it suffices to show that just one of the blocks sums to the index. Take the first 2 rows and columns and subtract a matrix which is the sum of the principal secondary diagonal and the 2nd primary diagonal.

$$\begin{pmatrix} 2 & 2 & 1 & 1 \\ 2 & 2 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 0 & 0 \\ 2 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Divide by 2 to get the desired identity. □

8.2 Identities and strongly magic symmetries

Call a 2×2 submatrix of A which is made of nonadjacent entries an *antiblock*. In Section 7.2, we defined the reduction of a P-square $A \downarrow_2$: each entry consists of the sum of the entries of an antiblock of A. If the index of A is I, then $A \downarrow_2$ is the I multiple of the trivial by Proposition 7.2.1. Hence,

Lemma 8.2.1. *Given a P-square of order 4, the entries of an antiblock sum to the index, e.g.,*

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} = I.$$

If we combine this lemma with the last part of Lemma 4.4.4, we get

Lemma 8.2.2. *Any 2 entries of an order 4 P-square, both indices of which differ by 2, sum to $\imath = I/2$, e.g.,*

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \imath.$$

Call any 2 such entries a *diagonal jump.* From Corollary 4.4.6, it follows that Lemma 8.2.2 characterizes when a W-square of order 4 is a P-square:

Proposition 8.2.3. *An order 4 W-square is a P-square* iff *the entries of any diagonal jump sum to $\imath$.*

The W-square definition gives us 16 new sets of 4 elements which sum to the index—the blocks—and Lemma 8.2.1 give us 4 sets with the same property—the antiblocks.

We define a new symmetry which maps the rows to a set of 8 blocks, and the columns to the other 8 blocks. Together with the pandiagonal symmetries, this additional symmetry generates a group of symmetries which has the pandiagonal symmetries as an index 3 subgroup. Send row $\hat{R}_0$ to the block in the upper left corner, row $\hat{R}_1$ to the lower left corner, $\hat{R}_2$ to the lower right corner and $\hat{R}_3$ to the upper right corner:

$$\begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & n & m \\ d & c & o & p \\ h & g & k & l \\ e & f & j & i \end{pmatrix}. \tag{8.2.1}$$

Note that diagonals $\hat{P}_1$, $\hat{P}_3$, $\hat{S}_0$ and $\hat{S}_2$ are mapped to the antiblocks.

The second iteration of this map produces a representative of another nontrivial coset for the factor group of all the symmetries modulo the pandiagonal symmetries.

An alternate representative of this second nontrivial coset is a similar mapping to 8.2.1. Images of rows $\hat{R}_0$ and $\hat{R}_2$ are the same, but the images of rows $\hat{R}_1$ and $\hat{R}_3$ are switched, i.e., $\hat{R}_1$ is mapped to the upper right corner and $\hat{R}_3$ is mapped to the lower left corner:

$$\begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & f & e \\ d & c & g & h \\ p & o & k & l \\ m & n & j & i \end{pmatrix}. \tag{8.2.2}$$

Now the *secondary* diagonals $\hat{S}_1$, $\hat{S}_3$ and the and the *primary* diagonals $\hat{P}_0$ and $\hat{P}_2$ are mapped to the antiblocks. Any symmetry which is not pandiagonal is *strongly magic.*

Let G^s be the group of all symmetries, i.e., the union of the pandiagonal and strongly magic symmetries. We claim that G^s, with cardinality $3 \times 4\varphi(4) \times 16 = 384$, contains all possible symmetries. As proof, we independently show in Section 8.9 that there are exactly 384 classical P-squares of order 4.

Let G_0^s be the subgroup of G^s of index 16 and order 24 which leaves the 0,0 entry fixed.

8.3 Labelings of 4-cubes

Müller [Mül97b] has given a geometric interpretation of the symmetries. Label the 16 vertices of a 4-cube so that each of the 2-faces sums to the same number. Such a labeled 4-cube will be called a *W4-cube.*

Proposition 8.3.1. *W4-cubes are in one-to-one correspondence with W-squares of order 4.*

Proof. The correspondence can be represented as the matrix

$$\begin{array}{cccc} 0000 & 0100 & 0110 & 0010 \\ 0001 & 0101 & 0111 & 0011 \\ 1001 & 1101 & 1111 & 1011 \\ 1000 & 1100 & 1110 & 1010 \end{array}$$

The entry 1011, for example, is shorthand for the coordinate (1,0,1,1). If the coordinates

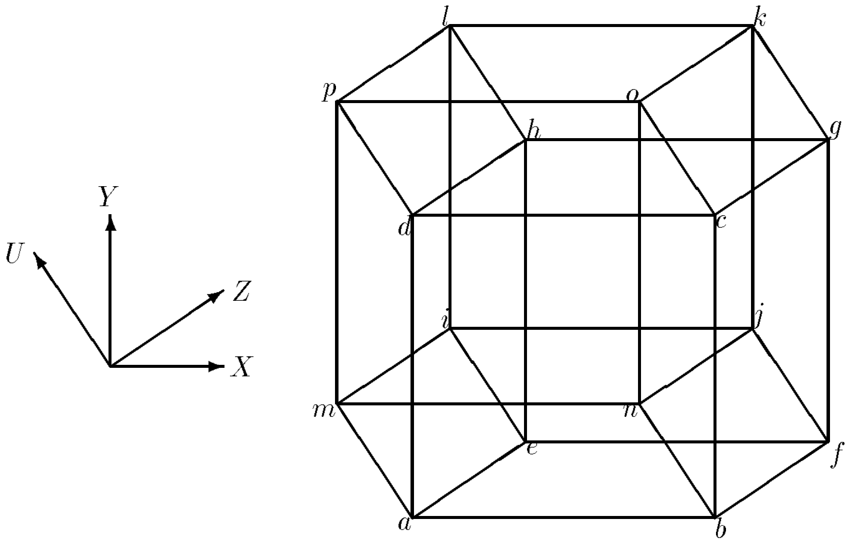


Figure 8.1: Labeled 4-cube (based on Müller [Mül97b])

4-sets in square		plane in 4-cube for corresponding faces
rows		XY
columns		UZ
blocks	a, c, i, k	XZ
with	b, d, j, l	YZ
upper-left	e, g, m, o	UX
corners	f, h, n, p	UY

Table 8.1: 4-sets in square and plane of 4-cube for corresponding faces.

are U, X, Y and Z, the same correspondence is represented by

$$\begin{array}{cccc} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{array}$$

and the 4-cube of Figure 8.3.

In Table 8.1, we show the correspondence between the blocks, rows and columns of the square and the faces parallel to the $\binom{4}{2} = 6$ planes of the 4-cube. □

Figure 8.3 demonstrates how movement around the square corresponds to movement on the 4-cube. The direction of the arrows corresponds to traveling in the positive direction

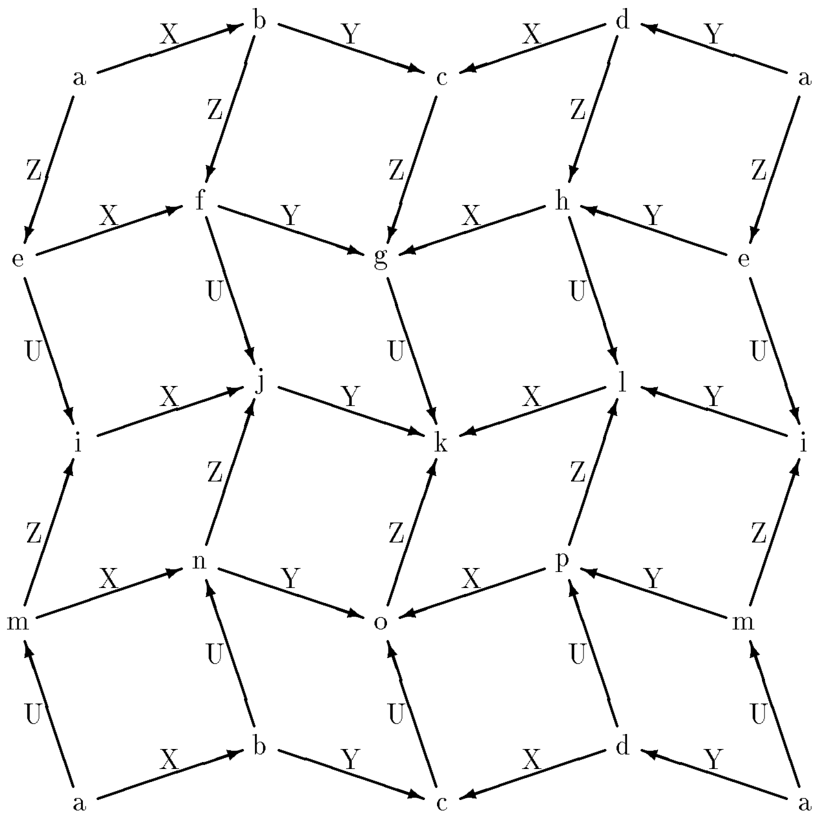


Figure 8.2: Tiling of square to show correspondence with 4-cube.

parallel to the axis indicated by the label. Horizontal travel entails alternately moving parallel to the X-axis and the Y-axis. Vertical travel entails alternately moving parallel to the Z-axis and the U-axis. Moving in the block with upper-left corner the 0,0-entry entails alternately moving parallel to the X-axis and the Z-axis, etc.

The correspondence between 4-cubes and squares of order 4 can also be shown geometrically. In Figure 8.3, we present a Schlegel diagram of the 4-cube, consisting of an inner 3-cube connected vertex to corresponding vertex with an identically positioned outer 3-cube. The X, Y and Z-axes are as the usual ones in both inner and outer cubes.

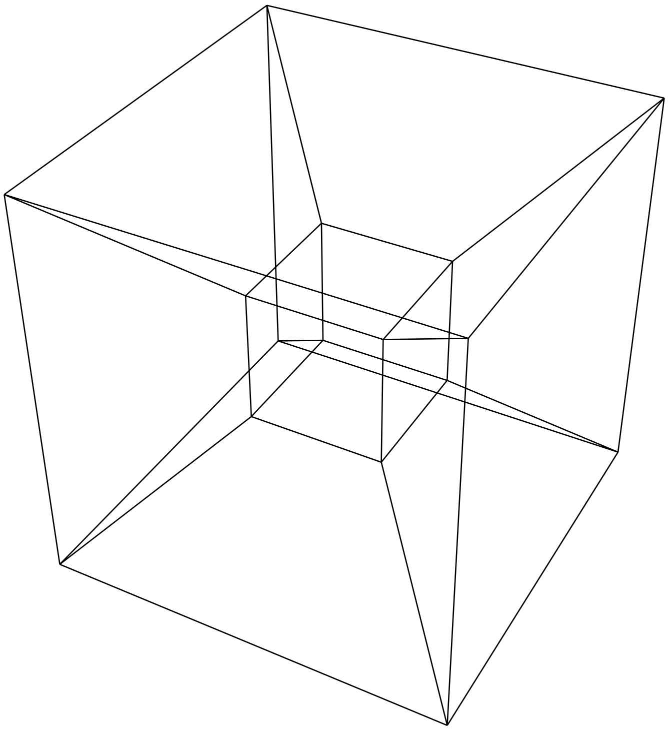


Figure 8.3: A Schlegel diagram of the 4-cube

.

The U-axis corresponds to traveling from the inner cube to the outer cube. In Figure 8.4, we place a torus into the Schlegel diagram. To make the edge map clear, we present in Figure 8.5 a sequence of images showing the transformation of a partitioned torus into the Schlegel diagram of the 4-cube. The faces parallel to the XY-plane correspond to circles which demonstrate that a filled torus is not homotopic to a point, i.e., big circles around the top, the outside, the inside and bottom of the torus. In the square, these are the 4 rows. The faces parallel to the UZ-plane correspond to 4 circles each of which cuts the

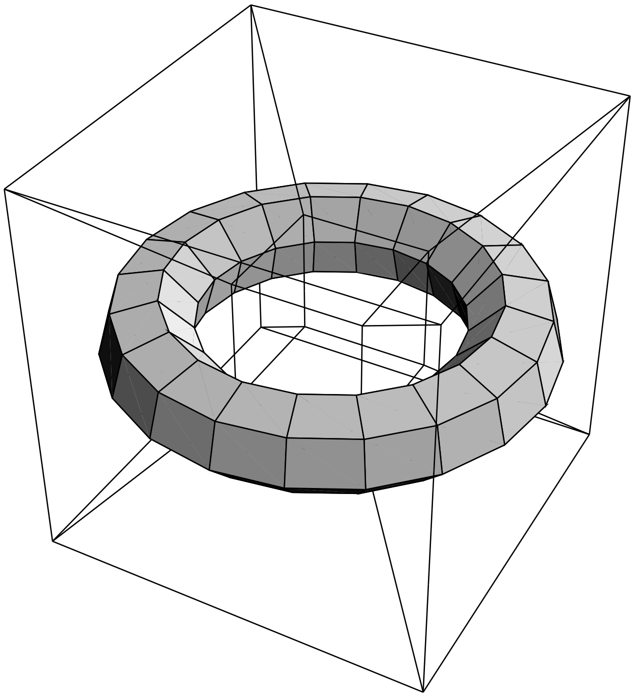


Figure 8.4: Inserting a torus into the 4-cube.

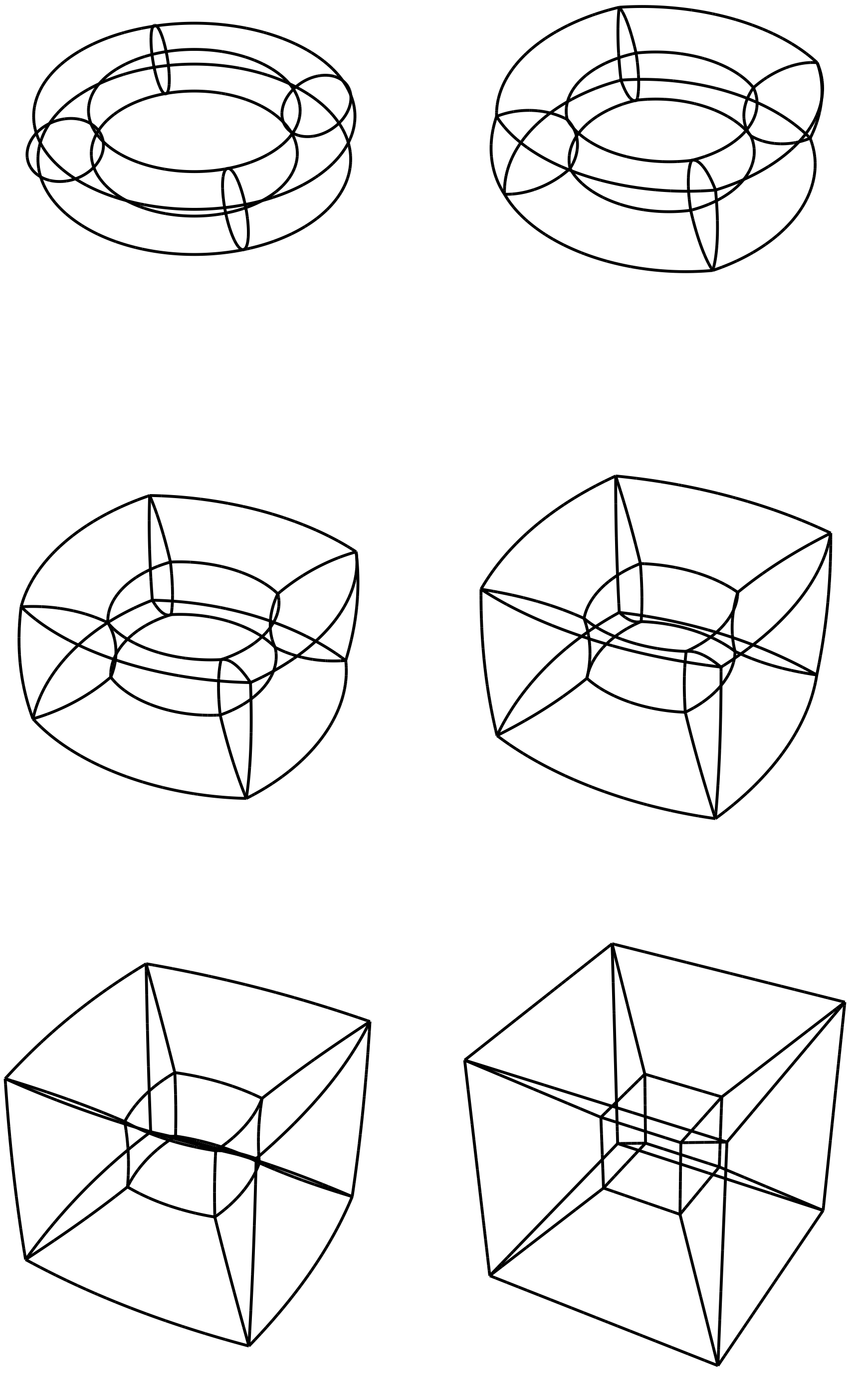


Figure 8.5: Transforming the arcs of a partitioned torus into the edges of a 4-cube.

tube part of the torus. In the square, these are the 4 columns. The other 16 faces of the 4-cube correspond to faces of the partitioned torus. In the square, these are the 16 blocks.

A diagonal jump corresponds to a pair of antipodally located points in the 4-cube. Following Proposition 8.2.3, we define *P4-cubes* to be W4-cubes whose antipodal vertices sum to $\imath = I/2$. If we fix the vertex labeled a, and situate the 4 coordinate axes there, then the 24 permutations of these axes correspond to elements of G_0^s.

8.4 Bicyclics

Recall the definition of a cyclic square (7.1.2). In this chapter, we work primarily with cyclics of step 2; let $C_a = C_a^2$. The 4 cyclics of step 2 are

$$\begin{gathered} C_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad C_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \\ C_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad C_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}. \end{gathered} \tag{8.4.3}$$

Notice that none of these cyclics is pandiagonal. By their construction, cyclic squares of any step have equal row sums. However, more is true for these particular cyclics.

Proposition 8.4.1. *The step 2 cyclics of order 4, listed in* (8.4.3)*, have equal primary and secondary diagonal sums.*

Proof. A primary diagonal may be defined by

$$\hat{F}_k(A) = \{\, a_{ij} \mid j \equiv_4 k + i \,\}.$$

Making the substitutions and eliminating j,

$$\begin{aligned} F_k(C_l) &= \sum_{i,j=0}^{3} \chi(j \equiv_4 k + i)\chi(j \equiv_4 l + 2i) \\ &= \sum_{i,j=0}^{3} \chi(k + i \equiv_4 l + 2i) = \sum_{i,j=0}^{3} \chi(i \equiv_4 k - l). \end{aligned}$$

For a given k and l, the last equivalence is true for exactly one i. Hence, the primary diagonal sums are equal.

A secondary diagonal may be defined by

$$\hat{S}_k(A) = \{\, a_{ij} \mid j \equiv_4 k - i \,\}.$$

Hence

$$\begin{aligned} S_k(C_l) &= \sum_{i,j=0}^{3} \chi(j \equiv_4 k-i)\chi(j \equiv_4 l+2i) \\ &= \sum_{i,j=0}^{3} \chi(k-i \equiv_4 l+2i) = \sum_{i,j=0}^{3} \chi(i \equiv_4 l-k). \end{aligned}$$

Hence, the secondary diagonal sums are equal as well. □

Note that if 2 matrices have the same pandiagonal property, such as equal row sums, then the sum also has that same property. Hence, to find a P-square of order 4, it suffices to sum 2 cyclics so that the sum has equal column sums.

A glance at the cyclics shows that if the start is even, then the sum of the entries in an even column is 2 and the sum of the entries in an odd column is 0. Likewise, if the start is *odd*, then the sum of the entries in an *odd* column is 2 and the sum of the entries in an *even* column is 0. Hence by summing a cyclic with an even start with a cyclic with an odd start, the result is a P-square. We record this discussion as

Proposition 8.4.2. *If e is an even number and o is an odd number, then*

$$B_{e,o} = C_e + C_o$$

is pandiagonal of index 2. $B_{e,o}$ is a bicyclic *of order 4.*

For example,

$$C_2 + C_3 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} = B_{2,3}.$$

The cyclics of a particular step are invariant under the torus translations by Proposition 7.1.3, an easy consequence of which is

Corollary 8.4.3. *The set of bicyclics of a fixed step is invariant under torus translations.*

The transpose of a cyclic C_a is the *tcyclic* ${}^tC_a$. The transpose of a bicyclic B_a is the *tbicyclic* ${}^tB_a$. The tcyclics and tbicyclics of a fixed step are also invariant under torus translations.

8.5 A determining set and decomposition of $\mathcal{P}_4$

Mark each of the entries in the union of the 0th row, column, primary and secondary diagonals with an x and the remaining 4 entries with o.

$$\begin{pmatrix} x & x & x & x \\ x & x & o & x \\ x & o & x & o \\ x & x & o & x \end{pmatrix}$$

The set consisting of a_{00} and the 4 entries marked with o is monic determining.

Proposition 8.5.1. *The five elements a_{00}, a_{23}, a_{21}, a_{32} and a_{12} form a monic determining set. If*

$$a_{00} = \alpha,\ a_{23} = a,\ a_{21} = b,\ a_{32} = c \text{ and } a_{12} = d,$$

then every P-square in $\mathcal{P}_4$ may be written in the form

$$\begin{pmatrix} \alpha & b+c+d-2\alpha & a+b-\alpha & a+c+d-2\alpha \\ a+b+d-2\alpha & a+c-\alpha & d & b+c-\alpha \\ c+d-\alpha & b & a+b+c+d-3\alpha & a \\ a+b+c-2\alpha & a+d-\alpha & c & b+d-\alpha \end{pmatrix}. \tag{8.5.4}$$

Corollary 8.5.2. *Every P-square in $\mathcal{P}_4$ with vanishing 0,0th entry may be written in the form*

$$\begin{pmatrix} 0 & b+c+d & a+b & a+c+d \\ a+b+d & a+c & d & b+c \\ c+d & b & a+b+c+d & a \\ a+b+c & a+d & c & b+d \end{pmatrix}. \tag{8.5.5}$$

In other words these pandiagonals are arbitrary nonnegative integral linear combinations *of the following four matrices, where ${}^tA$ stands for the transpose of A,*

$$B_{2,3} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \quad B_{2,1} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix},$$
$${}^tB_{2,3} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \quad {}^tB_{2,1} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}. \tag{8.5.6}$$

In particular,

$$\sum_{A \in \mathcal{P}_4 \ s.t. \ a_{00}=0} X(A) = \frac{1}{1 - X(B_{2,3})} \frac{1}{1 - X(B_{2,1})} \frac{1}{1 - X({}^tB_{2,3})} \frac{1}{1 - X({}^tB_{2,1})}. \tag{8.5.7}$$

The matrices are the bicyclics and transpose bicyclics defined in Section 8.4.

Lemma 8.5.3. *Let $(,)$ stand for the usual dot product. Given any steps b, c such that $bc - 1$ is invertible (in particular, when $b = c = 2$ and $n = 4$), the cyclics, tcyclics, bicyclics and tbicyclics have the following inner products:*

1. $(C^b_{j_0}, C^b_{i_0}) = \begin{cases} 0 & \textit{for } j_0 \neq i_0 \\ n & \textit{for } j_0 = i_0; \end{cases}$

2. $(C^b_{j_0}, {}^tC^c_{i_0}) = 1$ *for any j_0 and i_0;*

3. $(B^b_{r,s}, B^b_{u,v}) = n\chi(r = u) + n\chi(s = v)$*;*

4. $(B^b_{r,s}, {}^tB^c_{u,v}) = 4$ *for any r, s, u, v.*

Proof. Part 1. is true for any b and n. For Part 2., solve simultaneously

$$\begin{aligned} j &\equiv_n j_0 + bi \\ i &\equiv_n i_0 + cj, \end{aligned}$$

which implies

$$\begin{aligned} bi - j &\equiv_n -j_0 \\ -i + cj &\equiv_n -i_0. \end{aligned}$$

The determinant of the system is $bc - 1$. Hence, for any b, c such that $bc - 1$ is invertible, there is a unique solution for i and j, i.e., a unique location where $C^b_{j_0}$ and ${}^tC^c_{i_0}$ are both

1. To get Parts 3. and 4., expand the bicyclics into cyclics, use the linearity of the dot product, and apply Parts 1. and 2. of the lemma. □

Proof of Corollary. Set $\alpha = 0$ in (8.5.4) to get (8.5.5). Decompose (8.5.5) by extracting the coefficients of a, b, c and d. Then this subset of $\mathcal{P}_4$ is the nonnegative integral linear span of $\mathcal{L}\{B_{2,3}, B_{2,1}, {}^tB_{2,3}, {}^tB_{2,1}\}$. Let

$$\begin{aligned} B &= \{B_{2,3}, B_{2,1}, {}^tB_{2,3}, {}^tB_{2,1}\} \\ D &= \{B_{2,3} - B_{0,1}, B_{2,1} - B_{0,3}, {}^tB_{2,3} - {}^tB_{0,1}, {}^tB_{2,1} - {}^tB_{0,3}\}. \end{aligned}$$

Using Lemma 8.5.3,

$$(B_{2,3} - B_{0,1}, {}^tB_{2,3}) = (B_{2,3}, {}^tB_{2,3}) - (B_{0,1}, {}^tB_{2,3}) = 4 - 4 = 0$$

and

$$(B_{2,3} - B_{0,1}, B_{2,1}) = (B_{2,3}, B_{2,1}) - (B_{0,1}, B_{2,1}) = (4 + 0) - (0 + 4) = 0.$$

The other dot products are similar. We can conclude that an appropriate scalar multiple of D is a dual basis to B. In particular, we get the independence of the 4 matrices of B, which implies (8.5.7). □

Recall the 8 symmetry operations defined in Section 6.1. Note that

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -1 \\ 0 \end{bmatrix}.$$

Hence, a_{30} is in the same orbit as a_{01}. Via similar hand calculations or a computer program, label the orbits of the entries under the linear symmetries sequentially as they appear from top to bottom, left to right, to get

$$\begin{pmatrix} 1 & 2 & 3 & 2 \\ 2 & 4 & 5 & 4 \\ 3 & 5 & 6 & 5 \\ 2 & 4 & 5 & 4 \end{pmatrix}.$$

Note that the claimed determining set is the union of the orbits marked 1 and 5. If we add the strongly magic symmetries, then the orbits 3 and 4 are combined into one larger orbit.

8.6 Proof of Proposition 8.5.1

Our strategy for proving Proposition 8.5.1 is to use as tools the lemmas from Section 8.2 and express the pivot elements in terms of the determining set.

Proof. For the moment, let's add $\imath = \frac{1}{2}\operatorname{ind} A$ to our set of determining entries. The entries divided up into orbits under all symmetries which fix the 0,0th entry are

$$\begin{pmatrix} 1 & 2 & 3 & 2 \\ 2 & 3 & 4 & 3 \\ 3 & 4 & 5 & 4 \\ 2 & 3 & 4 & 3 \end{pmatrix}$$

Use Lemma 8.2.2 to get the entries for the 2nd and 5th orbits:

$$\begin{pmatrix} \alpha & \imath - a & 3 & \imath - b \\ \imath - c & 3 & d & 3 \\ 3 & b & \imath - \alpha & a \\ \imath - d & 3 & c & 3 \end{pmatrix}$$

To get the entries for the 3rd orbit use either a block or a generalized diagonal. For instance, for $a_{0,2}$ use R_0 and for $a_{1,1}$ use the block in the upper left corner.

$$\begin{pmatrix} \alpha & \imath - a & a + b - \alpha & \imath - b \\ \imath - c & a + c - \alpha & d & b + c - \alpha \\ c + d - \alpha & b & \imath - \alpha & a \\ \imath - d & a + d - \alpha & c & b + d - \alpha \end{pmatrix}$$

To get an expression for $\imath$, use any row or column with $\imath$ appearing only once. For instance, the 3rd column gives $a + b + c + d - 2\alpha + \imath = I = 2\imath$. Subtracting $\imath$ from both sides gives

$$\imath = a + b + c + d - 2\alpha.$$

Substituting this expression for $\imath$ back into the previous matrix gives (8.5.4). Alternatively, we could have gotten expressions for just one representative from orbits 2 and 3 and applied the symmetries to get the other entries of the orbits. For example,

$$\begin{aligned} a_{0,2} &= a + b - \alpha \\ &= a_{2,3} + a_{2,1} - a_{0,0}. \end{aligned}$$

Apply the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ to the indices to get

$$\begin{aligned} a_{2,0} &= a_{3,2} + a_{1,2} - a_{0,0} \\ &= c + d - \alpha. \end{aligned}$$

□

8.7 Admissible sets and the generating function

Designate the 4-tuple of 2 bicyclics and 2 tbicyclics which is the image of (8.5.6) under $\tau^{i,j}$ as the i,jth *admissible* 4-tuple.

The proof of Proposition 7.1.3 contains the seeds for a calculation of the admissibles. A column translation of j adds j to the start of a cyclic. A row translation of i adds $2i$ to the start. Hence the start increases by $2i + j$.

To get the 2 bicyclics associated with i, j, appropriately combine the cyclics with starts taken from adding $2i + j$ to the set $\{1, 2, 3\}$. To get a compact display, we show the complement, i.e., the start which is not allowed.

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix}$$

For example, the 2 bicyclics associated with the 0,1th entry are those that do not have the cyclic with start 1, namely $B_{0,3}$ and $B_{2,3}$.

The 0,0th entry of the matrix of (8.5.5) is the only entry which is identically 0. The 2 bicyclics associated with i, j are precisely those which have a 0 in the i, jth entry. Each i, jth admissible has only the i, jth entry where all its constituents are 0. Hence, the 16 admissibles are distinct.

Recall that

$$J = \begin{pmatrix} 1\,1\,1\,1 \\ 1\,1\,1\,1 \\ 1\,1\,1\,1 \\ 1\,1\,1\,1 \end{pmatrix}.$$

Define the *opposite* of a bicyclic $B_{a,b}$ to be $B^{\mathrm{op}}_{a,b} = J - B_{a,b}$. Note that $B^{\mathrm{op}}_{a,b} = B_{a-2,b-2}$.

Lemma 8.7.1. *The 16 admissible 4-tuples are precisely the 4-tuples which do not have any opposites.*

Proof. The admissibles have a common zero. The opposites do not. Hence, the admissibles are contained in the set of 4-tuples with no opposites. There are $\binom{2}{1}^4 = 16$ 4-tuples with no opposites. By the pigeonhole principle, the two sets are the same. □

To deal with the most general P-squares in $\mathcal{P}_4$, we need some notation. Let $\min(A)$ denote the minimum entry in a matrix A. This given, any pandiagonal $A \in \mathcal{P}_4$ may be decomposed as:

$$A = \min(A)J + (A - \min(A)J) = \min(A)J + A^\circ. \tag{8.7.8}$$

A° will have a zero entry in some location, say the i,jth location. Applying $\tau^{-i,-j}$ moves that entry to the 00th position. Using Proposition 8.5.1, decompose $\tau^{-i,-j}(A^\circ)$ into a nonnegative integer combination of $B_{2,3}$, $B_{2,1}$, ${}^tB_{2,3}$ and ${}^tB_{2,1}$. To express A° as a nonnegative integer combination of the matrices of the i,jth admissible 4- tuple, apply $\tau^{i,j}$ to this decomposition.

This places us in a position to prove our basic result for P-squares in $\mathcal{P}_4$.

Theorem 8.7.2. *Every pandiagonal $A \in \mathcal{P}_4$ may be uniquely written as*

$$A = jJ + A^\circ,$$

$$\begin{aligned} A^\circ = b_{01}B_{0,1} + b_{03}B_{0,3} + b_{12}B_{2,1} + b_{23}B_{2,3} \\ + c_{01}{}^tB_{0,1} + c_{03}{}^tB_{0,3} + c_{12}{}^tB_{2,1} + c_{23}{}^tB_{2,3}; \end{aligned} \tag{8.7.9}$$

where j is an arbitrary integer ≥ 0 and b_{ij}, c_{kl} are integers ≥ 0 subject to the condition that

$$\begin{aligned} 0 &= b_{01}b_{23} = b_{03}b_{12} \\ &= c_{01}c_{23} = c_{03}c_{12}. \end{aligned} \tag{8.7.10}$$

We deduce that

$$\begin{aligned} \sum_{A \in \mathcal{P}_4} X(A) = \frac{1}{1-X(J)} & \left(\frac{1}{1-X(B_{2,3})} + \frac{X(B_{0,1})}{1-X(B_{0,1})} \right) \\ & \left(\frac{1}{1-X(B_{2,1})} + \frac{X(B_{0,3})}{1-X(B_{0,3})} \right) \\ & \left(\frac{1}{1-X({}^tB_{2,3})} + \frac{X({}^tB_{0,1})}{1-X({}^tB_{0,1})} \right) \\ & \left(\frac{1}{1-X({}^tB_{2,1})} + \frac{X({}^tB_{0,3})}{1-X({}^tB_{0,3})} \right). \end{aligned} \tag{8.7.11}$$

In particular, the generating function for the index is

$$\sum_{A\in\mathcal{P}_4} t^{\operatorname{ind} A} = \frac{1}{1-t^4}\left(\frac{1+t^2}{1-t^2}\right)^4$$
$$= \frac{(1+t^2)^3}{(1-t^2)^5}.$$

Proof. The decomposition of A° described after (8.7.8) implies that A° is an arbitrary nonnegative linear combination of the matrices of an admissible set, which by Lemma 8.7.1 is equivalent to a 4-tuple with no opposite bicyclics. Hence, we get the basic decomposition of (8.7.9) including the conditions of (8.7.10). Moreover, since A° has a zero say at i, j, there are exactly 2 bicyclics and 2 tbicyclics which are 0 at i, j. Since no cancellation is possible, any expansion of type (8.7.9) must have support a subset of the admissible set. By Corollary 8.5.2, the expansion will be unique.

The generating function for one pair of bicyclics $\{B, B^{\mathrm{op}}\}$ is

$$\frac{X(B)}{1-X(B)} + \frac{X(B^{\mathrm{op}})}{1-X(B^{\mathrm{op}})} + 1.$$

(8.7.11) follows by noting that the configuration of one pair of opposite bicyclics is independent from the configuration of another. □

8.8 The cross section of the cone as a cross-polytope

Proposition 8.8.1. *Let $\jmath = J/2$, then $CS_2(\mathcal{P}_4)$, the cross section polytope, is a 4-crosspolytope with center $\jmath$. Each of the 16 facets is a tetrahedron with an admissible set as vertices.*

Proof. Subtracting $\jmath$ from each of the 4 bicyclics and 4 tbicyclics gives 4 pairs of opposite vectors of equal length. We need to show that a vector $B_1 - \jmath$ from one pair is orthogonal to a vector $B_2 - \jmath$ from another pair. Note that

$$(\jmath, \jmath) = (\frac{J}{2}, \frac{J}{2}) = \frac{1}{4}(J, J) = 4$$
$$(\jmath, B_1) = \frac{1}{2}(J, B_1) = 4.$$

Hence

$$(B_1 - \jmath, B_2 - \jmath) = (B_1, B_2) - (B_1, \jmath) - (B_2, \jmath) + (\jmath, \jmath)$$
$$= (B_1, B_2) - 4 - 4 + 4 = (B_1, B_2) - 4.$$

Thus, we have reduced the problem to showing that $(B_1, B_2) = 4$.

By *type*, we mean either bicyclic or transpose bicyclic.

B_1 and B_2 are of the same type Then B_1 and B_2 share exactly one subscript. Part 3 of Lemma 8.5.3 implies that $(B_1, B_2) = 4$.

B_1 and B_2 are of different types Part 4 of Lemma 8.5.3 applies.

□

A Schlegel diagram consists of a tetrahedron fitted dually inside another tetrahedron. (See Figure 8.6). There are $2\binom{4}{2}$ edges of the outer and inner tetrahedrons, plus 4×3 edges which connect vertices on the outer tetrahedron to vertices of the adjacent triangle of the dual inner tetrahedron (see Figure 8.7). The group of symmetries for the 4-crosspolytope is the hyperoctahedral group of order $2^4(4!) = 16(24) = 384$. The pairs of opposite vertices can be permuted. Sign changes correspond to switching one pair of opposite vertices. Let

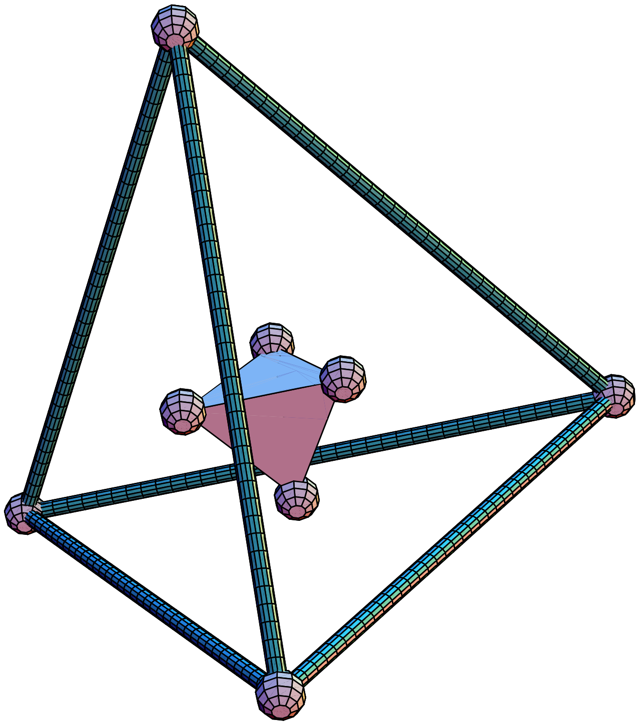


Figure 8.6: Tetrahedron dually fitted inside larger tetrahedron.

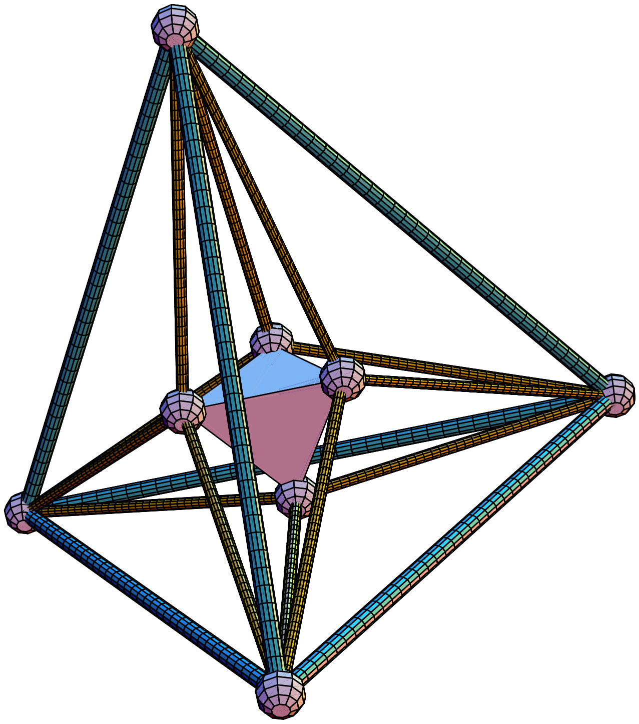


Figure 8.7: 30 of the 36 facets of the hexagon×hexagon.

us call vertices of (8.5.6) 1, 2, 3 and 4.

$$\begin{array}{cccc} \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \\ 1 & 2 & 3 & 4 \end{array} \tag{8.8.12}$$

The opposites are $\overline{1}$, $\overline{2}$, $\overline{3}$, and $\overline{4}$. The hyperoctahedral group is generated by the adjacent transpositions 2134, 1324 and 1243, together with a sign change $\overline{1}234$.

The linear pandiagonal symmetry acting on the indices with

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

switches the columns 1 and 3 of each matrix. It corresponds to the transposition 2134.

The linear pandiagonal symmetry acting on the indices with

$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

switches the rows 1 and 3 of each matrix. It corresponds to the transposition 1243.

Note that if we apply the transposition 1243 and then the 3 cycle 1342, we get the transposition 1324. Hence, it suffices to show what corresponds to the 3 cycle 1342. The strongly magic symmetry (8.2.1) acts on vertices 1, 2, 3 and 4 precisely in this fashion.

As you can see, the subgroup of order 24 which involves no sign changes corresponds precisely to the group generated by the linear pandiagonal symmetries and the strongly magic symmetry (8.2.1).

The sign changes require the torus translations. $\tau_{0,2}$ and then a flip over the y-axis, corresponds to $\overline{1}234$. Although that finishes a description of a generating set, the other sign changes are very similar. For instance, $\tau_{0,2}$ and then a flip over the line one unit above the y-axis corresponds to $1\overline{2}34$.

8.9 Classical pandiagonals

A classical matrix A has entries $\{0, \ldots, n^2 - 1\}$. Apply a torus translation to place the 0 in the upper left hand corner. If $n = 4$, the resulting matrix is a nonnegative linear combination of the matrices of (8.5.6). Encode the entries of the matrix (8.5.5) with the 01 words of length 4:

$$\begin{pmatrix} 0000 & 1110 & 0110 & 1101 \\ 1011 & 0101 & 1000 & 0110 \\ 1100 & 0010 & 1111 & 0001 \\ 0111 & 1001 & 0100 & 1010 \end{pmatrix}. \tag{8.9.13}$$

The (i, j)th entry of (8.5.5) is the dot product of the (i, j)th entry of (8.9.13) with (d, c, b, a). For instance, the 0,1th entry of (8.5.5) is $1110.(d, c, b, a) = b + c + d$. Notice that all the binary numbers from 0 to 15 appear in (8.9.13). Hence, assigning a, b, c and d to a permutation of the numbers 1, 2, 4 and 8, and substituting into (8.5.5) gives a matrix with entries the numbers from 0 to 15.

Conversely, let's construct a P-square from (8.5.5) with the entries from 0 to 15. Since a, b, c or d are each positive, we must assign the 1 to a, b, c or d, say a. (8.5.5) becomes

$$\begin{pmatrix} 0 & b+c+d & 1+b & 1+c+d \\ 1+b+d & 1+c & d & b+c \\ c+d & b & 1+b+c+d & 1 \\ 1+b+c & 1+d & c & b+d \end{pmatrix}.$$

To get the 2 in the matrix we must assign it to one of the other letters, say b:

$$\begin{pmatrix} 0 & 2+c+d & 3 & 1+c+d \\ 3+d & 1+c & d & 2+c \\ c+d & 2 & 3+c+d & 1 \\ 3+c & 1+d & c & 2+d \end{pmatrix}.$$

Similarly, we are forced to assign the 4 to one of c or d, say c,

$$\begin{pmatrix} 0 & 6+d & 3 & 5+d \\ 3+d & 5 & d & 6 \\ 4+d & 2 & 7+d & 1 \\ 7 & 1+d & 4 & 2+d \end{pmatrix}$$

and the 8 to the last letter, d,

$$\begin{pmatrix} 0 & 14 & 3 & 13 \\ 11 & 5 & 8 & 6 \\ 12 & 2 & 15 & 1 \\ 7 & 9 & 4 & 10 \end{pmatrix}. \tag{8.9.14}$$

Since the set of entries of (8.5.5) is symmetric in a, b, c and d, a P-square with vanishing 0,0th entry and with entries 0 to 15 must assign a, b, c and d with a permutation of the numbers 1, 2, 4 and 8.

To get a set of representatives for the orbits under the pandiagonal symmetries, we study the subgroup of pandiagonal symmetries which fix the 0,0th entry. In general they are the set of matrices given by (6.1.1) which act linearly on the indices. α can be 1 or -1. The group of 8 matrices obtained by making this substitution is isomorphic to the dihedral group d_4. How does this group act on the entries which fall in the locations a, b, c and d of (8.5.5)?

The action is the necklace group as is illustrated with the action of the symmetries on the order 4 classical P-square

$$\begin{array}{cccc} \boxed{0} & 14 & 3 & 13 \\ 11 & 5 & \boxed{8} & 6 \\ 12 & \boxed{2} & 15 & \boxed{1} \\ 7 & 9 & \boxed{4} & 10 \end{array}$$

from (8.9.14). The elements of the determining set are boxed. For the action of the non-identity pandiagonal symmetries which fix the 0,0th entry, see Table 8.2. To get distinct

index operator	effect on matrix	new matrix	effect on entries 1, 2, 4 & 8
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	transposes matrix	$\begin{matrix} \boxed{0} & 11 & 12 & 7 \\ 14 & 5 & \boxed{2} & 9 \\ 3 & \boxed{8} & 15 & \boxed{4} \\ 13 & 6 & \boxed{1} & 10 \end{matrix}$	$y = -x$ reflection
$\begin{pmatrix} 1 & 0 \\ 0 & \bar{1} \end{pmatrix}$	reverses last 3 cols	$\begin{matrix} \boxed{0} & 13 & 3 & 14 \\ 11 & 6 & \boxed{8} & 5 \\ 12 & \boxed{1} & 15 & \boxed{2} \\ 7 & 10 & \boxed{4} & 9 \end{matrix}$	y-axis reflection
$\begin{pmatrix} \bar{1} & 0 \\ 0 & 1 \end{pmatrix}$	reverses last 3 rows	$\begin{matrix} \boxed{0} & 14 & 3 & 13 \\ 7 & 9 & \boxed{4} & 10 \\ 12 & \boxed{2} & 15 & \boxed{1} \\ 11 & 5 & \boxed{8} & 6 \end{matrix}$	x-axis reflection
$\begin{pmatrix} \bar{1} & 0 \\ 0 & \bar{1} \end{pmatrix}$	reverses last 3 rows & last 3 cols	$\begin{matrix} \boxed{0} & 13 & 3 & 14 \\ 7 & 10 & \boxed{4} & 9 \\ 12 & \boxed{1} & 15 & \boxed{2} \\ 11 & 6 & \boxed{8} & 5 \end{matrix}$	180° rotation
$\begin{pmatrix} 0 & \bar{1} \\ \bar{1} & 0 \end{pmatrix}$	reverses last 3 rows & cols, then transposes	$\begin{matrix} \boxed{0} & 7 & 12 & 11 \\ 13 & 10 & \boxed{1} & 6 \\ 3 & \boxed{4} & 15 & \boxed{8} \\ 14 & 9 & \boxed{2} & 5 \end{matrix}$	$y = x$ reflection
$\begin{pmatrix} 0 & 1 \\ \bar{1} & 0 \end{pmatrix}$	reverses last 3 cols of transpose	$\begin{matrix} \boxed{0} & 7 & 12 & 11 \\ 14 & 9 & \boxed{2} & 5 \\ 3 & \boxed{4} & 15 & \boxed{8} \\ 13 & 10 & \boxed{1} & 6 \end{matrix}$	90° rotation
$\begin{pmatrix} 0 & \bar{1} \\ 1 & 0 \end{pmatrix}$	reverses last 3 rows of transpose	$\begin{matrix} \boxed{0} & 11 & 12 & 7 \\ 13 & 6 & \boxed{1} & 10 \\ 3 & \boxed{8} & 15 & \boxed{4} \\ 14 & 5 & \boxed{2} & 9 \end{matrix}$	270° rotation

Table 8.2: Action of the non-identity pandiagonal symmetries which fix the 0,0th entry on the order 4 classical P-square (8.9.14).

representatives, we enumerate necklaces with 4 distinct beads, labeled 1, 2, 4 and 8. Using one of the rotations, move the 1 bead to the a location.

$b = 2$ 2 could be assigned to b. If the bead labeled 4 has been assigned to the d location, an x-axis reflection moves the 4 bead to the c location while keeping the 1 and 2 beads assigned to the a and b locations fixed. Hence this case gives one necklace.

$b \neq 2$ If the 2 is assigned to the d location, again use the x-axis reflection to move it to the c location while keeping the 1 assigned to the a. The 4 bead could be assigned to either of the remaining locations, giving rise to 2 new distinct necklaces.

Making the appropriate substitutions, the following 3 matrices are orbit representatives:

$$\begin{pmatrix} 0 & 14 & 3 & 13 \\ 11 & 5 & 8 & 6 \\ 12 & 2 & 15 & 1 \\ 7 & 9 & 4 & 10 \end{pmatrix}, \quad \begin{pmatrix} 0 & 14 & 5 & 11 \\ 13 & 3 & 8 & 6 \\ 10 & 4 & 15 & 1 \\ 7 & 9 & 2 & 12 \end{pmatrix}, \quad \begin{pmatrix} 0 & 14 & 9 & 7 \\ 13 & 3 & 4 & 10 \\ 6 & 8 & 15 & 1 \\ 11 & 5 & 2 & 12 \end{pmatrix}.$$

To get the usual classical pandiagonals, we add a copy of the trivial.

Proposition 8.9.1. *Up to the pandiagonal symmetries, there are 3 classical pandiagonals:*

$$\begin{pmatrix} 1 & 15 & 4 & 14 \\ 12 & 6 & 9 & 7 \\ 13 & 3 & 16 & 2 \\ 8 & 10 & 5 & 11 \end{pmatrix}, \quad \begin{pmatrix} 1 & 15 & 6 & 12 \\ 14 & 4 & 9 & 7 \\ 11 & 5 & 16 & 2 \\ 8 & 10 & 3 & 13 \end{pmatrix}, \quad \begin{pmatrix} 1 & 15 & 10 & 8 \\ 14 & 4 & 5 & 11 \\ 7 & 9 & 16 & 2 \\ 12 & 6 & 3 & 13 \end{pmatrix}.$$

Note that the second two matrices are precisely the images of the strongly magic symmetries (8.2.1) and (8.2.2) applied to the first matrix.

Returning to the question asked at the end of Section 4.3, we would like to get 15 and 14 to be adjacent in the same row. The torus translations can not change the adjacency, thought of in a torus sense.

Lemma 8.9.2. *A set of coset representatives for the pandiagonal symmetries modulo the torus translations is the 8 square symmetries.*

Proof. We have the correct number. Since the set is a group and since only the identity is a torus translation, the 8 symmetries must be a set of representatives. □

Hence, it suffices to look at the effect of the 8 square symmetries. By inspection, none of these 8 symmetries applied to the 3 representatives can place 15 and 14 adjacent in the same row.

Note however, that there are adjacencies via diagonals in the 2nd and 3rd cases. Tipping these squares 45° and using pandiagonal symmetries to move the 15 and 14 down to the 2nd to last row, we get

$$\begin{array}{ccccccc} & & & 16 & & & \\ & & 2 & & 3 & & \\ & 11 & & 13 & & 6 & \\ 5 & & 8 & & 12 & & 9 \\ & 10 & & 1 & & 7 & \\ & & 15 & & 14 & & \\ & & & 4 & & & \end{array} \qquad \begin{array}{ccccccc} & & & 16 & & & \\ & & 2 & & 3 & & \\ & 7 & & 13 & & 10 & \\ 9 & & 12 & & 8 & & 5. \\ & 6 & & 1 & & 11 & \\ & & 15 & & 14 & & \\ & & & 4 & & & \end{array}$$

Chapter 9

W-squares of order 4

9.1 Identities and symmetries

We need one more identity:

Lemma 9.1.1. *In a W-square of order 4, the sum of the entries of any 2 horizontally or vertically adjacent diagonal jumps is equal to the index.*

Proof. From Lemma 4.4.4,

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & \bar{1} & \bar{1} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{9.1.1}$$

□

Let $\overline{i,j}$ denote a horizontally adjacent pair; (i,j) is the pair of coordinates for the left element of the adjacent pair in the top 2 rows, e.g., (9.1.1) is $\overline{0,1}$. Similarly, let $|i,j$ denote a vertically adjacent pair; (i,j) is the pair of coordinates for the top element of the adjacent pair in the left 2 columns, e.g.,

$$|3,0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

There are 8 identities of each type.

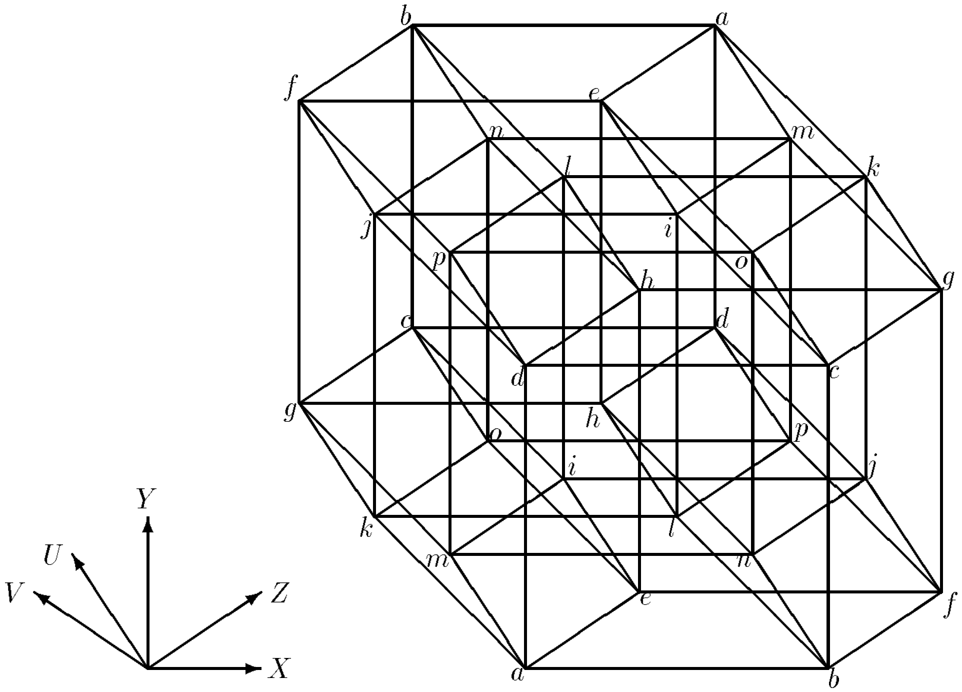


Figure 9.1: Antipodally identified 5-cube (based on Müller [Mül97b]).

The symmetry group for W-squares of order 4 is larger than that for P-squares. Wolfgang Müller [Mül97b] showed how the notion of a labeled 5-cube is helpful in identifying all the symmetries. Take the 4-cube of Proposition 8.3.1 and extend to another dimension. A 5-cube has 32 vertices, but we need only 16 labels since we identify antipodal vertices. Again we take the generic matrix

$$\begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{pmatrix} \tag{9.1.2}$$

and map letter-to-letter to the antipodally identified 5-cube in Figure 9.1. A 5-cube is a *W5-cube* if the labels of each of the 80 2-faces have the same sum.

Proposition 9.1.2. *Antipodally identified W5-cubes are in one-to-one correspondence with W-squares.*

Proof. Since the 5-cube is antipodally identified, there are in fact only 40 distinct faces.

adjacent diagonal jumps	plane to which faces in 5-cube are parallel
$\vert e$, $\vert f$, $\vert m$, $\vert n$	UV-plane
$\overline{a}$, $\overline{e}$, $\overline{c}$, $\overline{g}$	VX-plane
$\overline{b}$, $\overline{f}$, $\overline{d}$, $\overline{h}$	VY-plane
$\vert a$, $\vert b$, $\vert i$, $\vert j$	VZ-plane

Table 9.1: Correspondence between adjacent diagonal jumps and faces of the 5-cube.

The 4 rows, 4 columns and 16 blocks correspond to the same faces as before. The 16 adjacent diagonal jumps of Lemma 9.1.1 account for the remaining faces as listed in Table 9.1. Instead of coordinates, we refer to entries using the letters in the generic matrix (9.1.2). $\overline{e}$ refers to the set of 4 elements e, f, o, p:

$$\begin{pmatrix} a & b & c & d \\ \boxed{e} & \boxed{f} & g & h \\ i & j & k & l \\ m & n & \boxed{o} & \boxed{p} \end{pmatrix}.$$

$|m$ refers to the set of 4 elements a, m, g, k:

$$\begin{pmatrix} \boxed{a} & b & c & d \\ e & f & \boxed{g} & h \\ i & j & \boxed{k} & l \\ \boxed{m} & n & o & p \end{pmatrix}.$$

□

The symmetry group of our antipodally identified 5-cube is the factor group of the full symmetry group of the 5-cube modulo the order 2 group which switches antipodes. This symmetry group modulo the 384 symmetries of the 4-cube has as coset representatives the cyclic group which cycles the 5 coordinate axes with say a as the origin.

One of the entries of the matrix is the origin. 5 of the entries correspond to the axes. The remaining entries correspond to the $\binom{5}{2} = 10$ joins of axes. Making these substitutions, we get

$$\begin{pmatrix} O & X & X,Y & Y \\ Z & X,Z & U,V & Y,Z \\ U,Z & V,Y & V & V,X \\ U & U,X & V,Z & U,Y \end{pmatrix}.$$

With the axes alphabetically ordered, cyclically permute the axes, substituting into the above matrix. Replace the axes and joins of axes with their corresponding lowercase letters to get a representative of a generator for the factor group of new symmetries modulo the 384 previous symmetries:

$$\begin{pmatrix} a & d & h & e \\ m & p & l & i \\ g & f & b & c \\ k & j & n & o \end{pmatrix}.$$

The rows correspond to the XY-plane which has been replaced by the YZ-plane, i.e., by the blocks with upper-left corners d, l, b and j, respectively, which in turn has been replaced with the UZ-plane, i.e., the columns. The columns have in turn been replaced by the UV-plane, i.e., the vertical pairs of diagonal jumps with uppermost upper entries, m, f, n and e, respectively. These 4-tuples have been replaced by the VX-plane, i.e., the horizontal pairs of diagonal jumps with leftmost left entries a, e, c and g, respectively, which in turn have been replaced by the rows. We summarize our findings.

Proposition 9.1.3. *There are atleast* $2^4 \times 5! = 1920$ *W-symmetries for order 4, of which 120 leave fixed the 0,0th entry.*

If we independently show that there are precisely this number of classical W-squares of order 4, then we could conclude that these are indeed all possible symmetries.

9.2 Completely fundamental elements

In addition to the 8 bicyclics anchoring the P-squares, there are 2 additional bicyclics and 16 new objects, which I shall call tricyclics, although they are not the sum of 3 cyclics.

The new bicyclics are $B^1_{0,2}$ and $B^1_{1,3}$. If we checkerboard the square, these are the black squares as one of the objects and the white squares as the other object. By definition, the row sums of cyclics are equal. Since 1 is prime to anything, the column sums are also equal. Since every block contains exactly 2 black squares and 2 white squares, all the block sums are also equal.

A *tricyclic* $T_{c,t}$ is a combination of the step 2 cyclic of start c, C_c, the step 2 transpose cyclic of start t, ${}^tC_t$ plus the antiblock needed so that the sum has equal row and column sums. A cyclic has equal row sums, but for step 2, only odd columns have entries if the start is odd and only even columns have entries if the start is even. Likewise, a transpose cyclic has equal column sums, but for step 2, only odd rows have entries if the start is odd and only even rows have entries if the start is even.

Let's name the antiblock with upper-leftmost entry i, j as $AB_{i,j}$ The following table shows how the various ingredients are put together. As usual, e, e_1, e_2 are even numbers and o, o_1, o_2 are odd numbers.

tricyclic	cyclic	transpose cyclic	antiblock
T_{e_1,e_2}	C_{e_1}	${}^tC_{e_2}$	$AB_{1,1}$
$T_{o,e}$	C_o	${}^tC_e$	$AB_{0,1}$
$T_{e,o}$	C_e	${}^tC_o$	$AB_{0,1}$
T_{o_1,o_2}	C_{o_1}	${}^tC_{o_2}$	$AB_{0,0}$

For example,

$$T_{0,0} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

and

$$T_{0,3} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 2 & 0 \end{pmatrix}.$$

Note how tricyclics have by construction equal row and column sums. In addition, since each of the ingredients has equal block sums, so do the tricyclics. Thus,

Proposition 9.2.1. *Tricyclics are W-squares.*

9.3 Determining sets and an equivalent problem

There is one more dimension of freedom for W-squares of order 4 than there is for the P-squares. Hence, determining sets will have 6 elements. The obvious determining set is the hook shape, the 6 entries marked $a, \ldots, f$:

$$\begin{pmatrix} a & b & c & d \\ e & * & * & * \\ f & * & * & * \\ * & * & * & * \end{pmatrix}.$$

Note that the shape is not symmetric. Use the block and column sums to fill in the rest of the matrix:

$$\begin{pmatrix} a & b & c & d \\ e & c+d-e & a-c+e & b+c-e \\ f & a+b-f & -a+c+f & a+d-f \\ b+c+d-e-f & -b+e+f & a+b+d-e-f & -d+e+f \end{pmatrix}$$

$$= a \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & \bar{1} & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} + b \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & \bar{1} & 1 & 0 \end{pmatrix} + c \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & \bar{1} & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$+ d \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & \bar{1} \end{pmatrix} + e \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & \bar{1} & 1 & \bar{1} \\ 0 & 0 & 0 & 0 \\ \bar{1} & 1 & \bar{1} & 1 \end{pmatrix} + f \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & \bar{1} & 1 & \bar{1} \\ \bar{1} & 1 & \bar{1} & 1 \end{pmatrix}$$

Two symmetrical shapes that give similar decompositions are

$$\begin{pmatrix} a & b & c & * \\ d & e & * & * \\ f & * & * & * \\ * & * & * & * \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} a & b & * & * \\ c & d & e & * \\ * & f & * & * \\ * & * & * & * \end{pmatrix}.$$

This time the decomposition is similar to but more complicated than the hook shape.

If we take the diagonally symmetric shape used in the pandiagonal decomposition and add the entry in the middle of the cross, we get

$$\begin{pmatrix} a & * & * & * \\ * & * & b & * \\ * & c & d & e \\ * & * & f & * \end{pmatrix}.$$

Multiplying by 2 to avoid fractions and using the various identities available:

$2a$	$-a+b+c$ $+d-e+f$	$a-b+c$ $+d+e-f$	$-a+b-c$ $+d+e+f$
$-a+b+c$ $+d+e-f$	$a-b-c$ $+d+e+f$	$2b$	$a-b+c$ $+d-e+f$
$a+b-c$ $+d-e+f$	$2c$	$2d$	$2e$
$-a-b+c$ $+d+e+f$	$a+b-c$ $+d+e-f$	$2f$	$a+b+c$ $+d-e-f$

$$= a \begin{pmatrix} 2 & \bar{1} & 1 & \bar{1} \\ \bar{1} & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ \bar{1} & 1 & 0 & 1 \end{pmatrix} + b \begin{pmatrix} 0 & 1 & \bar{1} & 1 \\ 1 & \bar{1} & 2 & \bar{1} \\ 1 & 0 & 0 & 0 \\ \bar{1} & 1 & 0 & 1 \end{pmatrix} + c \begin{pmatrix} 0 & 1 & 1 & \bar{1} \\ 1 & \bar{1} & 0 & 1 \\ \bar{1} & 2 & 0 & 0 \\ 1 & \bar{1} & 0 & 1 \end{pmatrix}$$

$$+ d \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 2 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} + e \begin{pmatrix} 0 & \bar{1} & 1 & 1 \\ 1 & 1 & 0 & \bar{1} \\ \bar{1} & 0 & 0 & 2 \\ 1 & 1 & 0 & \bar{1} \end{pmatrix} + f \begin{pmatrix} 0 & 1 & \bar{1} & 1 \\ \bar{1} & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & \bar{1} & 2 & \bar{1} \end{pmatrix}.$$

Note that in the decomposition, all the matrices are translates of one another except for the matrix accompanying d. Beginning with a W-square $A \in \mathcal{W}_4$, decompose by identifying the minimum of all the entries, say j. Let $A^0 = A - jJ$; note that A^0 is another W-square with atleast one entry 0. We can use a torus translation to move that 0 to the d spot. Hence, we assume that the d location is 0. Setting $d = 0$, the resulting matrix is:

$$\begin{pmatrix} 2a & -a+b+c-e+f & a-b+c+e-f & -a+b-c+e+f \\ -a+b+c+e-f & a-b-c+e+f & 2b & a-b+c-e+f \\ a+b-c-e+f & 2c & 0 & 2e \\ -a-b+c+e+f & a+b-c+e-f & 2f & a+b+c-e-f \end{pmatrix}.$$

If we divide by 2, the resulting matrix will have entries the 5 remaining variables plus 10 entries which consist of all 10 ways to sum 3 elements from a 5 element set and subtract the remaining 2 elements, dividing the final result by 2. Remembering to take account of the fact that we have multiplied the matrix by 2, we can restate the problem as follows:

Proposition 9.3.1. *The decomposition of the space of W-squares with 1 entry set to 0 is equivalent to finding 5 nonnegative integers such that each sum of 3 of the numbers minus the other 2 is even and nonnegative.*

9.4 A geometric decomposition of the solutions space

From the data given by cdd([FP96]), an implementation of the Double Description Method of Motzkin et al.([MRTT53]), there are 16 facets, each corresponding to one of the entries set to 0. Once a multiple of the trivial has been extracted, one can assume that the solution is in one of the facets.

For ease of presentation, we assume that all vertices have been scaled appropriately so that they all lie on the same cross section of the cone. Each facet consists of 5 linearly independent bicyclics and 5 linearly independent tricyclics. The facets of a facet consist of 10 bipyramids formed by 3 bicyclics as base plus two tricyclics as the opposite points of the bipyramid.

Each facet has as center the average of the 5 bicyclics or the 5 tricyclics. In addition, each bicyclic has a complement among the tricyclics, i.e., the bicyclics can be paired up with the tricyclics so that the average of each pair is the center.

Let's look at the facet corresponding to the 0,0th entry set to 0. The center of this facet is

$$\begin{pmatrix} 0 & 2 & 1 & 2 \\ 2 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 2 & 1 & 1 & 1 \end{pmatrix}.$$

From the standpoint of the 0,0 entry, the 2's are precisely in the 5 entries which correspond to adjacent vertices on the 5-cube. The bicyclics and transpose bicyclics in this facet are

$$\underset{B^2_{2,1}}{\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}} \quad \underset{B^2_{2,3}}{\begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}} \quad \underset{{}^tB^2_{2,1}}{\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}} \quad \underset{{}^tB^2_{2,3}}{\begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}} \quad \underset{B^1_{1,3}}{\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}} .$$

The tricyclics, written in the order to complement the above bicyclics, are

$$\underset{T_{3,2}}{\begin{pmatrix} 0 & 1 & 0 & 2 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}} \quad \underset{T_{1,2}}{\begin{pmatrix} 0 & 2 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}} \quad \underset{T_{2,3}}{\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 2 & 0 & 1 & 0 \end{pmatrix}} \quad \underset{T_{2,1}}{\begin{pmatrix} 0 & 1 & 1 & 1 \\ 2 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}} \quad \underset{T_{2,2}}{\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 2 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}} .$$

The 2's again appear, from the standpoint of the 0,0 entry, in precisely the entries corresponding to the adjacent vertices on the 5-cube. Also notice that the tricyclic with a 2 in the i, j spot is matched precisely with the bicyclic in this facet that has a 0 at the i, j spot.

Proposition 9.4.1. *Removing the maximal multiple of the center of a facet results in an element on the boundary of the facet, i.e., on one of the bipyramids.*

Proof. We use the facet corresponding to a 0 in the 0,0 entry for ease of presentation. We claim that removing a maximal multiple of the facet's center results in a matrix with an additional entry that is 0. Removing such a maximal multiple could conceivably leave a 1 in one or several of the 5 adjacent vertices (to the 0,0 entry on the cube). Suppose, for example that there is a 1 in the 0,3 entry, then the matrix must be precisely one of the 4 bicyclics or 4 tricyclics that has a 1 in this entry. This matrix has a 0 in some entry other than the 0,0 spot. Hence our claim.

Having another 0 entry means that we are on the boundary with another facet. What are the possibilities for the intersection of 2 facets? If the 0 entries defining each of the facets are not adjacent vertices on the 5 cube, then the intersection is one of the bipyramids. If the 0 entries are adjacent on the 5-cube, then the intersection corresponds to a single bicyclic. An example of the former case is the facets corresponding to the 0,0 entry and the 0,2 entry being 0. The intersection of these 2 facets corresponds to the bipyramid consisting of the 3 bicyclics ${}^tB^2_{2,1}$, ${}^tB^2_{2,3}$ and $B^1_{1,3}$ and the 2 tricyclics $T_{3,2}$ and

$T_{1,2}$. An example of the latter is the facets corresponding to the 0,0 entry and the 2,2 entry being 0. The single element in the intersection is the bicyclic $B^1_{1,3}$. □

For a triangulation, take the bipyramids of each facet. Break each bipyramid into 2 tetrahedrons and join each of the resulting tetrahedrons with the center of the facet in question. Already we can get a count of the maximal faces of this triangulation. There are $\binom{5}{3} = 10$ bipyramids for each facet, or 20 tetrahedrons. Hence, there are $20 \times 16 = 320$ maximal faces in this triangulation.

Once a polytope has been triangulated into simplexes, a decomposition can be performed using inclusion-exclusion. We get quite a mess, but we can specialize to the index by replacing bicyclics with t^2, tricyclics with t^3, etc. The index generating function for one of the facets is

$$\frac{1+2\,t^2+4\,t^3+3\,t^4+3\,t^5+4\,t^6+2\,t^7+t^9}{(1-t^2)^3(1-t^3)(1-t^5)} = \frac{1-2\,t+4\,t^2-2\,t^3+t^4}{(1-t)^2\,(1-t^2)^2\,(1-t^3)}.$$

The index generating function for the entire solution space is

$$\frac{1+7\,t^2+15\,t^3+23\,t^4+40\,t^5+49\,t^6+50\,t^7+49\,t^8+\cdots+t^{14}}{(1-t^2)^3(1-t^3)(1-t^4)(1-t^5)}$$
$$= \frac{1-3\,t+11\,t^2-10\,t^3+11\,t^4-3\,t^5+t^6}{(1-t)^3\,(1-t^2)^2\,(1-t^3)}.$$

Since the associated ring is Gorenstein, the degree of the polynomial in the numerator is less than or equal to the degree of the denominator minus the degree of the center and the numerator is a symmetric polynomial.

Chapter 10

P-squares of order 5

10.1 The key identity and matrix decomposition

To unlock the structure of order 5, the following single relation suffices:

Proposition 10.1.1. *For all* $A = \|a_{ij}\| \in \mathcal{P}_5$,

$$a_{00} + a_{11} = a_{24} + a_{42} \quad \textit{or pictorially} \quad \begin{pmatrix} \bar{1} & 0 & 0 & 0 & 0 \\ 0 & \bar{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} = 0. \tag{10.1.1}$$

Proof. Using Proposition 5.1.5, begin with $-cP_{2,5}$ and add S_1:

$$\begin{pmatrix} \bar{1} & \bar{1} & 0 & 0 & 0 \\ \bar{1} & \bar{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \bar{1} & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

□

Going from order 4 to order 5, the number of pandiagonals for a given index has increased, but the symmetries have increased even faster, greatly enhancing the scope of any identity. Applying the symmetries to identity (10.1.1) gives a family of identities with which to decompose the whole matrix. We show a few members of the family to give a feeling for the scope of the identity. There are $8\varphi(5) = 32$ linear transformations of the indices.

However, because of the $y = -x$ symmetry of the identity, there are only 16 distinct images. We list 4 of them. The new identities are named for the location of the second -1. Using this naming scheme, (10.1.1) is R_{11}.

name	linear transformation on indices	identity
R_{01}	$\begin{bmatrix} 3 & 2 \\ 3 & 3 \end{bmatrix}$	$\begin{pmatrix} \bar{1} & \bar{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} = 0$
R_{02}	$\begin{bmatrix} 1 & 4 \\ 1 & 1 \end{bmatrix}$	$\begin{pmatrix} \bar{1} & 0 & \bar{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} = 0$
R_{03}	$\begin{bmatrix} 4 & 1 \\ 4 & 4 \end{bmatrix}$	$\begin{pmatrix} \bar{1} & 0 & 0 & \bar{1} & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} = 0$
R_{04}	$\begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix}$	$\begin{pmatrix} \bar{1} & 0 & 0 & 0 & \bar{1} \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} = 0$

Applying the linear transformations on the indices, the entries break up into 3 orbits

$$\begin{pmatrix} 1 & 2 & 2 & 2 & 2 \\ 2 & 2 & 3 & 3 & 2 \\ 2 & 3 & 2 & 2 & 3 \\ 2 & 3 & 2 & 2 & 3 \\ 2 & 2 & 3 & 3 & 2 \end{pmatrix}.$$

Notice that there are 16 locations in the orbit labeled 2, confirming our statement earlier about the number of identities in the family of (10.1.1). We claim that the orbits marked

1 and 3 are a determining set, whose elements we label as follows:

$$\begin{pmatrix} \alpha & 2 & 2 & 2 & 2 \\ 2 & 2 & a & b & 2 \\ 2 & h & 2 & 2 & c \\ 2 & g & 2 & 2 & d \\ 2 & 2 & f & e & 2 \end{pmatrix}.$$

(10.1.1) can be rewritten as $a_{11} = c + f - \alpha$. To get the expressions for the other elements in the second orbit, apply the linear transformations to the indices of (10.1.1) and solve for the image of the a_{11}. The result is

Proposition 10.1.2. *Every P-square in $\mathcal{P}$ can be written in the form*

$$\begin{pmatrix} \alpha & b+e-\alpha & g+h-\alpha & c+d-\alpha & a+f-\alpha \\ d+g-\alpha & c+f-\alpha & a & b & e+h-\alpha \\ a+b-\alpha & h & d+e-\alpha & f+g-\alpha & c \\ e+f-\alpha & g & b+c-\alpha & a+h-\alpha & d \\ c+h-\alpha & a+d-\alpha & f & e & b+g-\alpha \end{pmatrix}.$$

Setting α to 0, we get as a corollary

Corollary 10.1.3. *Every P-square in $\mathcal{P}$ with vanishing a_{00} entry may be uniquely written as*

$$\begin{pmatrix} 0 & b+e & g+h & c+d & a+f \\ d+g & c+f & a & b & e+h \\ a+b & h & d+e & f+g & c \\ e+f & g & b+c & a+h & d \\ c+h & a+d & f & e & b+g \end{pmatrix} \tag{10.1.2}$$

where $\{a, b, \ldots, h\}$ are arbitrary nonnegative integers. In other words, any such matrix is a nonnegative integral combination of the 8 linearly independent cyclic matrices

$$\{\, C_i^j \mid i = 1, \ldots, 4;\ j = 2, 3 \,\}, \tag{10.1.3}$$

where i is the start and j is the step (see (7.1.2) *for the definition). In particular,*

$$\sum_{A \in \mathcal{P}_5 \ s.t.\ a_{00}=0} X(A) = \prod_{i=1}^{4} \prod_{j=2}^{3} \frac{1}{1 - X(C_i^j)}. \tag{10.1.4}$$

Proof of Corollary. For each C_i^j, there is one entry where it is the only matrix among (10.1.3) which contributes to the sum found in (10.1.2), showing the independence of the 8 cyclic matrices C_i^j, which implies the generating function (10.1.4). □

10.2 The generating function and geometry for $\mathcal{P}_5$

Recall that

$$J = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Given $A \in \mathcal{P}_5$, let $m = \min(A)$ and $A^\circ = A - mJ$. A° will have a zero entry somewhere and is in $\mathcal{P}_5$. Using a torus translation τ, we can move that entry to the a_{00} position. Use Corollary 10.1.3 to decompose τA°. We deduce that A° may be decomposed into a sum of torus translates of the matrices $\{\, C_i^j \mid i = 1, \ldots, 4;\ j = 2, 3\,\}$. These translates are easily identified; by Proposition 7.1.3, the set of cyclic matrices of step l is invariant under torus translations. Call a set of 8 cyclics which is the image of (10.1.3) under a torus translation *admissible.* Each of the 25 admissible sets corresponds to precisely those 8 cyclics which are 0 in a fixed entry of the matrix. We are ready for the basic result of order 5 pandiagonals.

Theorem 10.2.1. *Every P-square $A \in \mathcal{P}_5$ may be uniquely written as*

$$A = mJ + \sum_{i=0}^{4} c_i C_i^2 + d_i C_i^3, \tag{10.2.5}$$

where m is an arbitrary integer ≥ 0 and c_i, d_i are integers ≥ 0 subject to the condition that

$$0 = c_0 c_1 c_2 c_3 c_4 = d_0 d_1 d_2 d_3 d_4. \tag{10.2.6}$$

We deduce that

$$\begin{aligned} \sum_{A \in \mathcal{P}_5} X(A) = \frac{1}{1 - X(J)} & \\ \frac{1 - X(C_0^2)X(C_1^2)X(C_2^2)X(C_3^2)X(C_4^2)}{(1 - X(C_0^2))(1 - X(C_1^2))(1 - X(C_2^2))(1 - X(C_3^2))(1 - X(C_4^2))} & \\ \frac{1 - X(C_0^3)X(C_1^3)X(C_2^3)X(C_3^3)X(C_4^3)}{(1 - X(C_0^3))(1 - X(C_1^3))(1 - X(C_2^3))(1 - X(C_3^3))(1 - X(C_4^3))} & . \end{aligned} \tag{10.2.7}$$

In particular, the generating function for the index is

$$\sum_{A\in\mathcal{P}_5} t^{\operatorname{ind} A} = \frac{1}{1-t^5}\left(\frac{1-t^5}{(1-t)^5}\right)^2$$
$$= \frac{1+t+t^2+t^3+t^4}{(1-t)^9}.$$

Proof. The decomposition of A° described before the statement of the theorem implies that A° is an arbitrary nonnegative linear combination of the matrices of an admissible set which is equivalent to a 8-tuple with no cycles. Hence, we get the basic decomposition of (10.2.5) including the conditions of (10.2.6). Moreover, since A° has a zero say at i, j, there are exactly 4 cyclics of step 2 and 4 cyclics of step 3 which are 0 at i, j. Since no cycles are present, any expansion of type (10.2.5) must have support a subset of the admissible set. By Corollary 10.1.3, the expansion will be unique.

Extracting the multiple of J corresponds to $\frac{1}{1-X(J)}$ in the generating function. What remains, A°, has 2 independent parts, a non-cycle combination of step 2 cyclics and a non-cycle combination of step 3 cyclics. Fix a step j and let $C_i = C_i^j$. Without any restriction, the generating function is

$$GF_I = \frac{1}{(1-X(C_0))(1-X(C_1))(1-X(C_2))(1-X(C_3))(1-X(C_4))}.$$

Forcing a cycle, the generating function is

$$GF_{II} = \frac{X(C_0)X(C_1)X(C_2)X(C_3)X(C_4)}{(1-X(C_0))(1-X(C_1))(1-X(C_2))(1-X(C_3))(1-X(C_4))}.$$

Hence, the generating function which prevents any cycle is the difference

$$GF_I - GF_{II} = \frac{1-X(C_0)X(C_1)X(C_2)X(C_3)X(C_4)}{(1-X(C_0))(1-X(C_1))(1-X(C_2))(1-X(C_3))(1-X(C_4))}.$$

(10.2.7) follows by combining the parts coinciding with the multiple of J, the step 2 non-cycle and the step 3 non-cycle. □

The structure revealed by the generating function is also present in the geometry of the cone. Let $\hat{J} = J/\text{order}$. Recall that the cyclics of a fixed step are mutually orthogonal. Hence,

Lemma 10.2.2. *The cyclics for a fixed step b and order n, $\{\, C_i \mid i = 0, \ldots, n-1 \,\}$ are the vertices of a $n-1$-simplex with center $\hat{J}$, denoted by $\triangle_n^b$.*

2 cyclics of different steps, C^b and C^c, share exactly one nonzero entry provided the system

$$\begin{array}{c} j \equiv_n i_1 + bi \\ j \equiv_n i_2 + ci \end{array} \text{ or } \begin{array}{c} j - bi \equiv_n i_1 \\ j - ci \equiv_n i_2 \end{array}$$

has a unique solution. This is true iff the determinant of the system, $b - c$, is invertible.

Lemma 10.2.3. *Given 2 cyclics of order n of different steps, C^b and C^c, where $b - c$ is invertible modulo n (for n prime, $b \neq c$, that is always the case), then $C^j - \hat{J}$ and $C^k - \hat{J}$ are orthogonal.*

Proof.

$$(C^j - \hat{J}, C^k - \hat{J}) = (C^j, C^k) - (\hat{J}, C^k) - (C^j, \hat{J}) - (\hat{J}, \hat{J}) = 1 - 1 - 1 + 1 = 0$$

□

Lemma 10.2.2 and Lemma 10.2.3 imply

Proposition 10.2.4. *The cross section of $\mathcal{P}_5$*

$$CS_1(\mathcal{P}_5) = (\triangle_5^2 - \hat{J}) \times (\triangle_5^3 - \hat{J}) + \hat{J}.$$

In other words, the $CS_1(\mathcal{P}_5)$ is the internal direct product of the two simplexes $\triangle_5^2$ and $\triangle_5^3$, but where the product operation is performed with center $\hat{J}$.

10.3 Classical pandiagonals

Let A be a classical pandiagonal with entries $0, 1, \ldots, 24$. Apply a torus translation to place the 0 in the upper left hand corner. The resulting matrix is a nonnegative linear combination of the matrices of (10.1.3). Due to how cyclics of the same and different steps interact, the set of entries of the matrix (10.1.2) is the cross product of the set $\{0, a, c, e, g\}$ with the set $\{0, b, d, f, h\}$, with the entries of each resulting ordered pair added, a process which can be expressed with polynomials:

$$(1 + x^a + x^c + x^e + x^g)(1 + x^b + x^d + x^f + x^h) = 1 + x + x^2 + \cdots + x^{24}.$$

Note that

$$(1 + x + x^2 + x^3 + x^4)(1 + x^5 + x^{10} + x^{15} + x^{20}) = 1 + x + x^2 + \cdots + x^{24}.$$

Hence, if we set $\{a, c, e, g\}$ equal to a permutation of $\{1, 2, 3, 4\}$ and $\{b, d, f, h\}$ to a permutation of $\{5, 10, 15, 20\}$ (or vice versa), we will get a classical order 5 pandiagonal. For the converse, we use

Lemma 10.3.1. *For any prime p,*

1. $1 + x + x^2 + \cdots + x^{p-1}$ *is irreducible;*
2. $1 + x^p + x^{2p} + \cdots + x^{(p-1)p}$ *is irreducible.*

Proof.

$$\begin{aligned}(x-1)(1 + x + \cdots + x^{p-1}) = x^p - 1 &= (y+1)^p - 1 \\ &= y^p + \binom{p}{1} y^{p-1} + \binom{p}{2} y^{p-2} + \cdots + py \\ &= y(y^{p-1} + \binom{p}{1} y^{p-2} + \binom{p}{2} y^{p-3} + \cdots + p)\end{aligned}$$

Zeroing in on the second factor of the last expansion, p divides all the non-leading terms and p^2 does not divide the constant term. By the Eisenstein criterion, this polynomial is irreducible. Irreducibility is not affected by linear substitution; replace y with $x - 1$ to get that $1 + x + x^2 + \cdots + x^{p-1}$ also is irreducible.

For the second polynomial, I was unable to find a way to use the Eisenstein criterion. Instead, we cite an elementary result from algebraic number theory [Mar77, p.17]: let ω be a primitive mth root of unity, then $\mathbb{Q}[w]$ has degree $\varphi(m)$. $\varphi(p^2) = p^2 - p$. Hence the second polynomial is irreducible. □

Summarizing the above discussion, we get

Proposition 10.3.2. *A classical pandiagonal square of order 5 with vanishing 0,0 entry is formed precisely by using* (10.1.2)*, setting* $\{a, c, e, g\}$ *equal to a permutation of* $\{1, 2, 3, 4\}$ *and* $\{b, d, f, h\}$ *to a permutation of* $\{5, 10, 15, 20\}$ *(or vice versa).*

To get a set of representatives up to symmetry, we study the subgroup of pandiagonal symmetries which fix the 0,0th entry. They are the set of matrices given by (6.1.1) which act linearly on the indices. α can be 1, 2, 3 or 4. The group of 32 matrices obtained acts in a complicated fashion on the entries marked $a, b, \ldots, h$. A big simplification arises by using information we already have, namely that either $\{a, c, e, g\}$ or $\{b, d, f, h\}$ is $\{1, 2, 3, 4\}$. Hence, we can look at the subgroup of index 2 which fixes $\{a, c, e, g\}$. We list in Table 10.3 the 16 elements of this subgroup and their action on the determining

index operator	action on a, c, e, g	action on b, d, f, h
$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$	identity	identity
$\begin{bmatrix}2 & 0\\ 0 & 2\end{bmatrix}$	rotates to right 90°	rotates to left 90°
$\begin{bmatrix}3 & 0\\ 0 & 3\end{bmatrix}$	rotates to left 90°	rotates to right 90°
$\begin{bmatrix}4 & 0\\ 0 & 4\end{bmatrix}$	rotates 180°	rotates 180°
$\begin{bmatrix}0 & 1\\ 4 & 0\end{bmatrix}$	rotates to right 90°	rotates to right 90°
$\begin{bmatrix}0 & 4\\ 1 & 0\end{bmatrix}$	rotates to left 90°	rotates to left 90°
$\begin{bmatrix}0 & 2\\ 3 & 0\end{bmatrix}$	rotates 180°	identity
$\begin{bmatrix}0 & 3\\ 2 & 0\end{bmatrix}$	identity	rotates 180°
$\begin{bmatrix}1 & 1\\ 4 & 1\end{bmatrix}$	rotates to left 90°	rotates 180°
$\begin{bmatrix}2 & 2\\ 3 & 2\end{bmatrix}$	identity	rotates to right 90°
$\begin{bmatrix}3 & 3\\ 2 & 3\end{bmatrix}$	rotates 180°	rotates to left 90°
$\begin{bmatrix}4 & 4\\ 1 & 4\end{bmatrix}$	rotates to right 90°	identity
$\begin{bmatrix}1 & 4\\ 1 & 1\end{bmatrix}$	rotates 180°	rotates to right 90°
$\begin{bmatrix}2 & 3\\ 2 & 2\end{bmatrix}$	rotates to left 90°	identity
$\begin{bmatrix}3 & 2\\ 3 & 3\end{bmatrix}$	rotates to right 90°	rotates 180°
$\begin{bmatrix}4 & 1\\ 4 & 4\end{bmatrix}$	identity	rotates to left 90°

Table 10.1: Action of pandiagonal symmetries on a classic order 5 matrix

set, showing that the action of the subgroup is the cross product of the rotation group on a, c, e, g with the rotation group on b, d, f, h. To get a set of 36 representatives up to symmetry, set a to 1 and b to 5, then c, e, g is an arbitrary permutation of $2, 3, 4$ and d, f, h is an arbitrary permutation of $10, 15, 20$.

Chapter 11

Generalized diagonals and very magic squares

11.1 The number of generalized diagonals for a fixed order

The results of the first 3 sections of this chapter have been taken largely from [Knu68]. A *generalized diagonal* is the set of entries of a square matrix of size n which satisfies an equation of the form $ax + by \equiv_n c$, where $\gcd(a, b, n) = 1$. A slope (a, b) is *legitimate* if $\gcd(a, b, n) = 1$. Unless stated otherwise, a slope is assumed to be legitimate. The GCD condition is necessary to ensure a full n elements in the set. As is customary, an equation will often denote the solutions to the equation.

The n diagonals in the set

$$\{ax + by \equiv_n c \mid 0 \leq c \leq n-1\}$$

constitute the *family* of diagonals corresponding to and denoted by the slope (a, b). Actually a family is not identified by a unique slope. 2 slopes determine the same family of diagonals iff they differ by a factor which is prime to n. Call 2 such slopes *equivalent*. Let

$$\begin{aligned}\psi(n) &= \#\{\text{families of diagonals of order } n\} \\ &= \#\{\text{inequivalent slopes}\} = \#\{\text{legitimate slopes}\}/\varphi(n).\end{aligned} \tag{11.1.1}$$

Proposition 11.1.1. *If* $n = p_1^{i_1} p_2^{i_2} \ldots p_m^{i_m}$, *then*

$$\psi(n) = n\left(\frac{p_1+1}{p_1}\right)\left(\frac{p_2+1}{p_2}\right)\ldots\left(\frac{p_m+1}{p_m}\right).$$

Proof. Let $\psi'(n) = \#\{\text{legitimate slopes for order } n\}$. By (11.1.1), $\psi'(n) = \psi(n)\varphi(n)$. Recall that

$$\varphi(n) = n\left(\frac{p_1-1}{p_1}\right)\left(\frac{p_2-1}{p_2}\right)\dots\left(\frac{p_m-1}{p_m}\right).$$

Hence, we can alternatively show that

$$\begin{aligned}\psi'(n) &= \left(n\left(\frac{p_1+1}{p_1}\right)\left(\frac{p_2+1}{p_2}\right)\dots\left(\frac{p_m+1}{p_m}\right)\right)\varphi(n)\\ &= n^2\left(\frac{p_1^2-1}{p_1^2}\right)\left(\frac{p_2^2-1}{p_2^2}\right)\dots\left(\frac{p_m^2-1}{p_m^2}\right).\end{aligned} \tag{11.1.2}$$

Any illegitimate slope is divisible by a prime p_i. There are $(n/p_i)^2$ such slopes for each prime factor p_i. If $\sum_{i=1}^{m}(n/p_i)^2$ is subtracted from n^2, the total number of slopes, the slopes that are divisible by atleast 2 primes are subtracted multiple times. Hence, we have to add them back. Continuing with this analysis, called inclusion-exclusion, we get

$$\begin{aligned}\psi'(n) &= n^2 - \sum_{i=1}^{m}(\frac{n}{p_i})^2 + \sum_{1\le i<j\le m}(\frac{n}{p_ip_j})^2 - \dots \pm (\frac{n}{p_1p_2\dots p_m})^2\\ &= n^2\left(1-\frac{1}{p_1^2}\right)\left(1-\frac{1}{p_2^2}\right)\dots\left(1-\frac{1}{p_m^2}\right).\end{aligned}$$

□

11.2 The Fourier transform and very magic squares

Given a matrix $A = \|A_{ij}\|$ of order n and a primitive nth root of unity ω, define the Fourier transform to be $a = \|a_{kl}\|$, where

$$a_{kl} = \sum_{0\le i,j\le n-1} \omega^{-(ik+jl)}A_{ij}.$$

Proposition 11.2.1.

$$A_{ij} = \frac{1}{n^2}\sum_{0\le k,l\le n-1}\omega^{ik+jl}a_{kl}. \tag{11.2.3}$$

Proof.

$$\begin{aligned}
\sum_{0\leq k,l\leq n-1} \omega^{ik+jl} a_{kl} &= \sum_{0\leq k,l\leq n-1} \omega^{ik+jl} \sum_{0\leq r,s\leq n-1} \omega^{-(rk+sl)} A_{rs} \\
&= \sum_{0\leq r,s\leq n-1} A_{rs} \sum_{0\leq k,l\leq n-1} \omega^{k(i-r)+l(j-s)} \\
&= \sum_{0\leq r,s\leq n-1} A_{rs} \sum_{k=0}^{n-1} \omega^{k(i-r)} \sum_{l=0}^{n-1} \omega^{l(j-s)} \\
&= \sum_{0\leq r,s\leq n-1} A_{rs} \left(n\chi(r=i)\right)\left(n\chi(s=j)\right) = n^2 A_{ij}.
\end{aligned}$$

□

Given a matrix in the linear span of the generalized diagonals, the transform indicates the contribution from the various families of diagonals as follows. Let $A_{ij} = \chi(k'i + l'j = c)$ for some fixed constant c and slope (k', l').

$$\begin{aligned}
a_{kl} &= \sum_{0\leq i,j\leq n-1} \omega^{-(ik+jl)} \chi(k'i + l'j = c) \\
&= \sum_{i,j|k'i+l'j=c} \omega^{-(ik+jl)} = \begin{cases} 0 & \text{if } (k,l) \neq d(k',l') \text{ for all } d; \\ n\omega^{-dc} & \text{if } (k,l) = d(k',l'), \end{cases}
\end{aligned}$$

from which we gleam

1. The transform of a diagonal has nonzero entries precisely on the n multiples of the slope.

2. All diagonals of a family are mapped to the same diagonal.

3. Since $A \mapsto a$ is reversible by Proposition 11.2.1, the information needed to sort out the individual diagonals of a family must be encoded into this diagonal; in fact, the entries are the one dimensional discrete Fourier transform.

A *very magic square* is a matrix all of whose generalized diagonals sum to the same quantity, called the index. We quickly dispense with these squares.

Proposition 11.2.2. *Very magic squares are trivial.*

Proof. Given a very magic matrix A with order n and index s, let $(k,l) = d(k',l')$, where (k',l') is a legitimate slope.

$$\begin{aligned} a_{kl} &= \sum_{0\le i,j\le n-1} \omega^{-(ik+jl)} A_{ij} \\ &= \sum_{c=0}^{n-1} \omega^{-dc} \sum_{\{i,j|k'i+l'j=c\}} A_{ij} \\ &= s\sum_{c=0}^{n-1} \omega^{-dc} = \begin{cases} ns & \text{if } d=0; \\ 0 & \text{if } d\neq 0. \end{cases} \end{aligned}$$

Hence, a reduces to the matrix with one nonzero entry, namely the 0,0th entry with value ns. Applying the inverse transform (11.2.3), the sum reduces to a single term and $A_{i,j} = s/n$. □

11.3 Semi-very magic squares

A *semi-very magic square* (k,l) or semi-very for short is a matrix, whose generalized diagonals not in the family (k,l) sum to the same quantity, called the index.

Proposition 11.3.1. *For any primitive nth root of unity ω, the matrix A of order n defined by*

$$A_{ij} = \omega^{ik+jl}$$

is semi-very (k,l).

To prove the proposition, we need a variant of the Chinese Remainder Theorem:

Lemma 11.3.2. *Given $n = q_1q_2\dots q_m$, where q_1, q_2, ..., q_m are pairwise relatively prime, set $b_t = \hat{q}_t^{\varphi(q_t)}$ for each t then $b_t \equiv_{q_t} 1$ (by Euler's theorem) and $b_u \equiv_{q_t} 0$ for all $u \neq t$. Having chosen such a set, given any x, $x \equiv_{q_u} x_u$, $1 \le u \le m$,* iff

$$x \equiv_n b_1x_1 + b_2x_2 + \cdots + b_mx_m.$$

We call finding such a sum decomposing into coordinates.

Proof.

Case 1$(n = p^e)$ Let $ri + sj = c$ be a diagonal. Either $p \not| r$ or $p \not| s$. WLOG assume $p \not| r$, then $\exists t$ such that $rt \equiv_n 1$. Multiplying the equation by t, we get an equivalent equation $i + s'j = c'$. Hence we can assume $r = 1$. The sum of the entries in the diagonal is

$$\sum_{i+js\equiv_n c} A_{ij} = \sum_{i+js\equiv_n c} \omega^{ik+jl} = \sum_{i+js\equiv_n c} \omega^{(c-js)k+jl}$$
$$= \omega^{ck} \sum_{i+js\equiv_n c} \omega^{j(l-sk)}$$

which is 0 unless $l = sk$. If so, $(k, l) = (k, sk) = k(r, s)$, which implies that $p \not| k$ since $\gcd(k, l, n) = 1$. Thus $(r, s) = k^{-1}(k, l)$, which implies that (r, s) is equivalent to (k, l).

Case 2$(n = p_1^{e_1} p_2^{e_2} \ldots p_m^{e_m})$ Let $q_t = p_t^{e_t}$ and $\hat{q}_t = \prod_{u\neq t} q_u$. Using Lemma 11.3.2 to decompose i and j into coordinates,

$$\sum_{ir+js\equiv_n c} A_{ij} = \sum_{i+js\equiv_n c} \omega^{ik+jl}$$
$$= \sum_{ir+js\equiv_n c} \omega^{k(b_1 i_1+b_2 i_2+\cdots b_m i_m)+l(b_1 j_1+b_2 j_2+\cdots b_m j_m)}$$
$$= \sum_{ir+js\equiv_n c} \omega^{b_1(ki_1+lj_1)+\cdots b_m(ki_m+lj_m)}$$
$$= \sum_{ir+js\equiv_n c} \omega_1^{ki_1+lj_1} \cdots \omega_m^{ki_m+lj_m}.$$

In the last equality, we have set $\omega_u = \omega^{b_u}$. To determine the conditions on the coordinates of i and j, take the condition $ir + js \equiv_n c$ and modulo q_u to get $ri_u + sj_u \equiv_{q_u} c$. The converse is also true. Hence, we can divide the sum as follows:

$$\sum_{ir+js\equiv_n c} A_{ij} = \sum_{ri_1+sj_1\equiv_{q_1} c} \omega_1^{ki_1+lj_1} \cdots \sum_{ri_m+sj_m\equiv_{q_m} c} \omega_m^{ki_m+lj_m}. \qquad (11.3.4)$$

To be nonzero, each of the sums must be nonzero. Since $\omega_t = \omega^{b_t} = \omega^{\hat{q}_t^{\varphi(q_t)}}$,

$$\omega_t^{q_t} = \omega^{\hat{q}_t^{\varphi(q_t)} q_t} = \omega_t^{n\hat{q}_t^{\varphi(q_t)-1}} = (\omega_t^n)^{\hat{q}_t^{\varphi(q_t)-1}} = 1.$$

Also, since there are no factors of p_t in $\hat{q}_t$, there is no smaller power of ω_t which equals one. Hence, ω_t is a primitive q_tth root of unity. Applying the result from case 1 for each of the sums of (11.3.4), $\exists y_u$, such that $(r,s) \equiv_{q_u} y_u(k,l)$. Setting $y = b_1y_1 + b_2y_2 + \cdots + b_my_m$ and applying Lemma 11.3.2 one last time, we get $(r,s) \equiv_n y(k,l)$.

□

Corollary 11.3.3. *There are non-trivial, integral, semi-very magic squares for each order and slope.*

Proof. Each matrix of Proposition 11.3.1 is complex, whose real part is not constant. Adding an appropriate multiple of the trivial matrix to this real part, we obtain a positive, real, nontrivial solution. Thus the cone of nonnegative solutions must have a nontrivial extreme ray. Since our system of equations has integral coefficients, this extreme ray must contain an integral solution. □

Chapter 12

Pandiagonal permutations and cyclic squares

12.1 P-perms and a recursive algorithm

Define a *sequence* σ to be an ordered list of n elements taken from $\{0,\ldots,n-1\}$; the ith element specifies the column placement of the single 1 in the ith row of its representation as a square

$$m(\sigma)=\|\chi(j=\sigma_i)\|_{i,j=0}^{n-1}.$$

We will often identify the squares that originate from sequences with the sequences themselves or vice versa. Hence, C_a^b, the cyclic squares introduced in Section 7.1, are sequences. Permutations are other examples of sequences.

Remark 12.1.1. A sequence is a permutation iff it has no duplication iff its range is the *full set.*

Magic squares from $\mathcal{M}_n$ of index 1 are precisely the permutation matrices of order n. For the permutations which are in a particular subset, e.g., W-squares, we use an appropriate prefix, e.g., W-permutations. Actually, the W-squares are a bad example. Since none of the extreme rays for W-squares of order 4 are permutation matrices, there are no W-permutations of order 4. Since the $\text{ind}_W(A)$ would have to have a non-integral fraction of the index which is 1, neither are there W-permutations of order more than 4.

We confine our investigation to permutations which are also P-squares, i.e., *P-permutations* or P-perms for short. Let $\delta=(0,1,\ldots,n-1)$.

Proposition 12.1.2. *A permutation σ is pandiagonal* iff *both $\sigma + \delta \mod n$ and $\sigma - \delta \mod n$ are permutations.*

Proof. σ is primary diagonal iff

$$P_k(\sigma) = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} \chi(j = \sigma_i)\chi(j = i + k) = 1 \ \forall k$$

$$\iff \quad \sum_{i=0}^{n-1} \chi(i + k = \sigma_i) = 1 \ \forall k \qquad \iff \sum_{i=0}^{n-1} \chi(k = \sigma_i - i) = 1 \ \forall k$$

iff $\sigma - \delta$ is a permutation. Similarly, σ is secondary diagonal iff $\sigma + \delta$ is a permutation. □

We combine Remark 12.1.1 with Proposition 12.1.2 to compute recursively the P-perms of a fixed order. Having constructed

$$\sigma_0, \sigma_1, \dots, \sigma_{i-1}$$

choose σ_i (if possible) as one of the values in $\{0, 1, \dots, n-1\}$ that are different mod n than any of the numbers

$$\begin{array}{llll} \sigma_0 & \sigma_1 & \dots & \sigma_{i-1} \\ \sigma_0 - i & \sigma_1 + 1 - i & \dots & \sigma_{i-1} + (i-1) - i \\ \sigma_0 + i & \sigma_1 - 1 + i & \dots & \sigma_{i-1} - (i-1) + i. \end{array}$$

Checking against the first row assures that a permutation is being created, against the second row assures secondary diagonality, and against the last row assures primary diagonality.

In performing a computer search, there are several additional measures that can be taken. By cycling the columns, we can assume that the first element of the sequence is 0. By performing a combination of dihedral operations and torus translations, we can assume that the 2nd element is between 2 and $\lfloor \frac{n-2}{2} \rfloor$. We are really interested in a representative for each orbit under the pandiagonal symmetries, hence more sophisticated measures are possible which take into account these symmetries. See for example work done on 8 non-attacking queens on a chess-board [Wil85, p.36]. By Corollary 7.2.3, there are no P-perms for orders that are singly even and for orders that are multiples of 3 but not 9. Hence, the orders up to 30 that a computer search should examine are $\{7, 8, 9, 11, 13, 16, 17, 19, 20, 23, 25, 27, 28, 29\}$. A preliminary search has shown that there are no P-perms for orders 8 and 9. For orders 7 and 11, the only P-perms are cyclic squares. For order 13 with $\sigma(0) = 0$, there are 10 cyclic and 338 noncyclic P-perms.

12.2 Cyclic squares and a generalized Euler φ function

The principal examples of P-perms are a subset of the cyclic squares.

Proposition 12.2.1. *A cyclic square C_a^b is*

1. *a permutation* iff $(b, n) = 1$*;*
2. *secondary diagonal* iff $(b+1, n) = 1$*;*
3. *primary diagonal* iff $(b-1, n) = 1$*;*
4. *a P-perm* iff $(b, n) = (b+1, n) = (b-1, n) = 1$.

If condition 4 holds, the square is *P-cyclic* and b is *superprime* to n, denoted $((b, n) = 1$.

Corollary 12.2.2. *For prime $p > 3$, C_a^b of order p is P-cyclic, i.e.,* $((b, p) = 1$ iff

$$b \in \{2, 3, \ldots, p-2\}.$$

Proof. Treat the cyclic square as a sequence. If $(b, n) = d \neq 1$, $b\frac{n}{d}$ is divisible by n and the sequence will be periodic with period $\frac{n}{d}$.

Conversely, if $(b, n) = 1$ and $a + bi = a + bj$ for some i, j. Then $b(i - j) \equiv_n 0$. Divide by b to get $i \equiv_n j$. This completes part 1.

By Proposition 12.1.2, a sequence is secondary diagonal iff its progressive cyclic shift to the right, i.e., its sum with δ is a permutation. Now use part 1.

Similarly, a sequence is primary diagonal iff its progressive cyclic shift to the left, i.e., its difference with δ is a permutation. Again use part 1. □

To facilitate additional discussion of the cyclics, let

$$C_n(b) = \{C_a^b \text{ of order } n \mid a = 0, \ldots, n-1\} \quad \textit{and} \quad C_n = \{C_n(b) \mid ((b, n) = 1\}.$$

Corollary 12.2.2 implies that $|C_p| = p(p-3)$ for p prime. What is the corresponding statement for composite n? To answer the question, we present an extension of the Euler phi function. Given $S \subseteq \mathbb{Z}_n$, let

$$\mathcal{B}_S(n) = \{b \mid 0 \leq b < n, (b + x, n) = 1 \ \forall x \in S\},$$

and $\varphi_S(n) = |\mathcal{B}_S(n)|$. To recover the Euler phi function, set $S = \{0\}$. We are interested in φ_S when $S = \{-1, 0, 1\}$.

Proposition 12.2.3. *For p prime,*

1. $\varphi_S(p) = p - |S|$ *if* $p > \max S - \min S$;
2. $\varphi_S(p^k) = \varphi_S(p)p^{k-1}$;
3. φ_S *is multiplicative, i.e.,* $(m,n) = 1 \Rightarrow \varphi_S(mn) = \varphi_S(m)\varphi_S(n)$.

Corollary 12.2.4. *Given the distinct prime powers factorization* $n = p_1^{k_1} p_2^{k_2} \dots p_\ell^{k_\ell}$,

$$\begin{aligned}\varphi_S(n) &= \varphi_S(p_1)p_1^{k_1-1}\varphi_S(p_2)p_2^{k_2-1}\dots\varphi_S(p_\ell)p_\ell^{k_\ell-1}\\ &= n\frac{\varphi_S(p_1)}{p_1}\frac{\varphi_S(p_2)}{p_2}\dots\frac{\varphi_S(p_\ell)}{p_\ell}.\end{aligned}$$

Proof.

For Part 1, $\mathcal{B}_S(p)$ is the complement of $-S$ in $\{0,\dots,p-1\}$.

For Part 2, $\mathcal{B}_S(p^k) = \{b + cp \mid b \in \mathcal{B}_S(p), 0 \le c < p^{k-1}\}$.

For Part 3, by the Fundamental Theorem of Arithmetic, $\exists \alpha, \beta \in \mathbb{Z}$ such that $m\alpha + n\beta = 1$. Let

$$\mathcal{B} = \{bm\alpha + b'n\beta \mod mn \mid b \in \mathcal{B}_S(n), b' \in \mathcal{B}_S(m)\}.$$

We claim that $\mathcal{B} = \mathcal{B}_S(mn)$.

($\subseteq$) For $bm\alpha + b'n\beta \in \mathcal{B}$, and $x \in S$,

$$(bm\alpha + b'n\beta + x, m) = (b'n\beta + x, m) = (b'(1 - m\alpha) + x, m) = (b' + x, m) = 1;$$

the last equality holds since $b' \in \mathcal{B}_S(m)$. Similarly, $(bm\alpha + b'n\beta + x, n) = 1$.

Since $(m,n) = 1$, $(bm\alpha + b'n\beta + x, mn) = 1$.

($\supseteq$) Given $a \in \mathcal{B}_S(mn)$. Let

$$\begin{aligned} b &\equiv_n a, \quad 0 \le b < n\\ b' &\equiv_m a, \quad 0 \le b' < m.\end{aligned}$$

We claim $a \equiv_{mn} bm\alpha + b'n\beta$.

$$a - bm\alpha - b'n\beta = a - bm\alpha - b'(1 - m\alpha) = a - b' - m(b + b')\alpha.$$

Since $m|a - b'$, we get

$$m|(a - bm\alpha - b'n\beta).$$

Similarly, $n|(a - bm\alpha - b'n\beta)$, and hence, $mn|(a - bm\alpha - b'n\beta)$, which completes the claim.

Given $x \in S$, $(b + x, n) = (a + x, n)|(a + x, mn) = 1$. Hence, $(b + x, n) = 1$ and $b \in \mathcal{B}_S(n)$. Similarly, $b' \in \mathcal{B}_S(m)$. □

Let $\varphi' = \varphi_{\{-1,0,1\}}$. By direct calculation, $\varphi'(2) = \varphi'(3) = 0$. For $p > 3$ prime, by Proposition 12.2.3, Part 1, $\varphi'(p) = p - 3$. Substituting into Corollary 12.2.4, we get

Proposition 12.2.5. *Let $n = p_1^{k_1} p_2^{k_2} \dots p_\ell^{k_\ell}$ be the usual prime factorization of n, then*

$$\varphi'(n) = \begin{cases} 0 & \textit{if } n \textit{ is divisible by 2 or 3;} \\ n\frac{p_1-3}{p_1}\frac{p_2-3}{p_2}\dots\frac{p_\ell-3}{p_\ell} & \textit{otherwise.} \end{cases}$$

Corollary 12.2.6. *P-cyclics exist for a given order n* iff *n is not divisible by 2 or 3.*

12.3 The orbits of P-cyclics under pandiagonal symmetries

To determine the orbits of P-cyclics under pandiagonal symmetries, apply the matrices (6.1.1) and (6.1.2) to the displacement vector $\left[\begin{smallmatrix}1\\ b\end{smallmatrix}\right]$ and normalize so that the top component is 1.

$$\begin{bmatrix} \alpha & \\ & \pm\alpha \end{bmatrix} \begin{bmatrix} 1 \\ b \end{bmatrix} = \alpha \begin{bmatrix} 1 \\ \pm b \end{bmatrix}$$

$$\begin{bmatrix} & \alpha \\ \pm\alpha & \end{bmatrix} \begin{bmatrix} 1 \\ b \end{bmatrix} = \alpha \begin{bmatrix} \pm b \\ 1 \end{bmatrix} = \pm\alpha b \begin{bmatrix} 1 \\ \pm b^{-1} \end{bmatrix}$$

$$\begin{bmatrix} \mp\alpha & \pm\alpha \\ \alpha & \alpha \end{bmatrix} \begin{bmatrix} 1 \\ b \end{bmatrix} = \alpha \begin{bmatrix} \pm(b-1) \\ b+1 \end{bmatrix} = \pm\alpha(b-1) \begin{bmatrix} 1 \\ \frac{b+1}{\pm(b-1)} \end{bmatrix}$$

$$\begin{bmatrix} \alpha & \alpha \\ \mp\alpha & \pm\alpha \end{bmatrix} \begin{bmatrix} 1 \\ b \end{bmatrix} = \alpha \begin{bmatrix} b+1 \\ \pm(b-1) \end{bmatrix} = \alpha(b+1) \begin{bmatrix} 1 \\ \frac{\pm(b-1)}{b+1} \end{bmatrix}$$

Hence, the orbit for the P-cyclics of step b is

$$\{\pm b, \pm b^{-1}, \pm\frac{b+1}{b-1}, \pm\frac{b-1}{b+1}\}.$$

We next investigate when these set of steps contain duplication.

- Setting $b = -b$, we get $2b = 0$ which implies $b = 0$ since n is odd. However, we have excluded $b = 0$ from consideration.

- Setting $b = b^{-1}$, we get $b^2 = 1$ which implies $b = \pm 1$. Again, we have excluded these values of b from consideration.

- Setting b equal to $-b^{-1}$, $-\frac{b+1}{b-1}$, or $\frac{b-1}{b+1}$, we get $b^2 = -1$. Such b's exist iff $\sqrt{-1} \in \mathbb{Z}_n$.

- Setting $b = \frac{b+1}{b-1}$, we get $b^2 - 2b - 1 = 0$ which implies $b = 1 \pm \sqrt{2}$. Such b's exist iff $\sqrt{2} \in \mathbb{Z}_n$.

- Setting $b = -\frac{b-1}{b+1}$ we get $b^2 + 2b - 1 = 0$ which implies $b = -1 \pm \sqrt{2}$. Such b's exist iff $\sqrt{2} \in \mathbb{Z}_n$.

We gather from our investigation that if $\sqrt{-1} \in \mathbb{Z}_n$ and if b is either of these roots, then

$$b = -b^{-1} = -\frac{b+1}{b-1} = \frac{b-1}{b+1} \quad \text{and} \quad -b = b^{-1} = \frac{b+1}{b-1} = -\frac{b-1}{b+1}.$$

If $\sqrt{2} \in \mathbb{Z}_n$ and if b is either of these roots $+1$, then

$$b = \frac{b+1}{b-1}, \quad -b = -\frac{b+1}{b-1}, \quad b^{-1} = \frac{b-1}{b+1} \quad \text{and} \quad -b^{-1} = -\frac{b-1}{b+1}.$$

When is $\sqrt{-1}$ or $\sqrt{2} \in \mathbb{Z}_n$? We restrict our investigation further to n prime, which by previous exclusion means $n > 3$ prime. Using quadratic reciprocity,

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = \begin{cases} 1 & n \equiv_4 1 \\ -1 & n \equiv_4 3 \end{cases}$$

and

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} 1 & n \equiv_8 1, 7 \\ -1 & n \equiv_8 3, 5 \end{cases}$$

where $\left(\frac{x}{n}\right)$ is the Legendre symbol. To summarize,

n mod 8	existence	n mod 8	existence
1	$\sqrt{-1}$,$\sqrt{2}$	5	$\sqrt{-1}$
3	neither	7	$\sqrt{2}$

.

We next check possible duplication among our 6 candidate b's, $\{\pm\sqrt{-1}\}, \pm 1 \pm \sqrt{2}$. For odd n, $\pm\sqrt{-1}$ can not coincide, likewise $1 \pm \sqrt{2}$ and $-1 \pm \sqrt{2}$. We next pair off $\sqrt{-1}$ with $1 + \sqrt{2}$:

$$-1 = 3 + 2\sqrt{2} \Rightarrow \sqrt{2} = -2 \Rightarrow 2 = 4 \Rightarrow 0 = 2.$$

Similarly for all other pairs which include $\sqrt{-1}$. Finally, we pair $1 \pm \sqrt{2}$ with $-1 - \pm\sqrt{2}$. All such cases require $n = 2$. We can conclude

Proposition 12.3.1. *Under pandiagonal symmetries, the orbits of P-cyclics of order $n > 3$ prime are of cardinality 8, except for at most 1 orbit of cardinality 4 and/or 1 orbit of cardinality 2 (Table 12.1).*

mod n	# orbits of size 8	# orbits of size 4	# orbits of size 2
1	$\frac{n-9}{8}$	1	1
3	$\frac{n-3}{8}$	0	0
5	$\frac{n-5}{8}$	0	1
7	$\frac{n-7}{8}$	1	0

Table 12.1: The P-cyclic orbit configuration under pandiagonal symmetries for $n > 3$ prime.

Chapter 13

Linear span of cyclic P-squares for prime order

13.1 Generating series for order 7

Denote by $\mathcal{C}_n$ the nonnegative integer span of the pandiagonal cyclic matrices of order n. From Proposition 12.2.5, we know that $\mathcal{C}_n$ is empty iff n is divisible by 2 or 3. For the moment, we will restrict to the case when n is prime. One of the consequences of Theorem 10.2.1 is that $\mathcal{P}_5 = \mathcal{C}_5$. This single fact is responsible for the beauty and simplicity of our solution of the 5 case. In this section, we consider $\mathcal{C}_7$. The generalization to arbitrary order will follow easily.

The pandiagonal cyclics of order 7 have steps 2, 3, 4 and 5. For $k = 0, \ldots, 6$, let

$$\begin{aligned} A_k &= \|\chi(j \equiv_7 k + 2i)\|_{i,j=0}^{6}, & B_k &= \|\chi(j \equiv_7 k + 3i)\|_{i,j=0}^{6}, \\ C_k &= \|\chi(j \equiv_7 k + 4i)\|_{i,j=0}^{6}, & D_k &= \|\chi(j \equiv_7 k + 5i)\|_{i,j=0}^{6}. \end{aligned}$$

$\mathcal{C}_7$ consists of all nonnegative integral linear combinations of these 28 matrices. Letting a_k, b_k, c_k and d_k denote generic nonnegative integer coefficients, we get for any matrix

$E \in \mathcal{C}_7$, $E = A + B + C + D$, where

$$A = \sum_{k=0}^{6} a_k A_k = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_5 & a_6 & a_0 & a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_5 & a_6 & a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_0 \\ a_6 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_5 & a_6 & a_0 & a_1 & a_2 & a_3 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_0 & a_1 \end{pmatrix}, \quad B = \sum_{k=0}^{6} b_k B_k = \begin{pmatrix} b_0 & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 \\ b_4 & b_5 & b_6 & b_0 & b_1 & b_2 & b_3 \\ b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_0 \\ b_5 & b_6 & b_0 & b_1 & b_2 & b_3 & b_4 \\ b_2 & b_3 & b_4 & b_5 & b_6 & b_0 & b_1 \\ b_6 & b_0 & b_1 & b_2 & b_3 & b_4 & b_5 \\ b_3 & b_4 & b_5 & b_6 & b_0 & b_1 & b_2 \end{pmatrix},$$

$$C = \sum_{k=0}^{6} c_k C_k = \begin{pmatrix} c_0 & c_1 & c_2 & c_3 & c_4 & c_5 & c_6 \\ c_3 & c_4 & c_5 & c_6 & c_0 & c_1 & c_2 \\ c_6 & c_0 & c_1 & c_2 & c_3 & c_4 & c_5 \\ c_2 & c_3 & c_4 & c_5 & c_6 & c_0 & c_1 \\ c_5 & c_6 & c_0 & c_1 & c_2 & c_3 & c_4 \\ c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_0 \\ c_4 & c_5 & c_6 & c_0 & c_1 & c_2 & c_3 \end{pmatrix}, \quad D = \sum_{k=0}^{6} d_k D_k = \begin{pmatrix} d_0 & d_1 & d_2 & d_3 & d_4 & d_5 & d_6 \\ d_2 & d_3 & d_4 & d_5 & d_6 & d_0 & d_1 \\ d_4 & d_5 & d_6 & d_0 & d_1 & d_2 & d_3 \\ d_6 & d_0 & d_1 & d_2 & d_3 & d_4 & d_5 \\ d_1 & d_2 & d_3 & d_4 & d_5 & d_6 & d_0 \\ d_3 & d_4 & d_5 & d_6 & d_0 & d_1 & d_2 \\ d_5 & d_6 & d_0 & d_1 & d_2 & d_3 & d_4 \end{pmatrix}.$$

Of course the expansion just described is not unique; we have the relations

$$\sum_{k=0}^{6} A_k = \sum_{k=0}^{6} B_k = \sum_{k=0}^{6} C_k = \sum_{k=0}^{6} D_k = J = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}. \qquad (13.1.1)$$

To state the main result of the section we need some auxiliary facts and definitions. To begin, let us call "admissible" any 24^{tuple} of matrices obtained by removing one element from each of the cyclic classes. The admissible 24^{tuple} obtained by removing A_h, B_k, C_l and A_m, will be denoted by $\{A_h, B_k, C_l, A_m\}^c$. Let us treat the matrices as vectors with 49 components. Cyclics of the same step are orthogonal with respect to the usual dot product. The discussion preceding Lemma 10.2.3 shows that cyclics of steps b and c have dot product 1 provided that $b - c$ is invertible modulo n. For n prime, all nonzero elements are invertible. We record these facts as

Lemma 13.1.1. *Let $\{A_r\}$ be the set of cyclics of step a and $\{B_r\}$ be the set of cyclics of step b.*

$$(A_r, A_s) = \begin{cases} n & \textit{if } r = s \\ 0 & \textit{if } r \neq s \end{cases},$$

and provided $b - c$ is invertible modulo n,

$$(A_r, B_s) = 1 \quad \textit{for all } r, s.$$

Proposition 13.1.2. *The matrices of an admissible set $\{A_h, B_k, C_l, A_m\}^c$ are linearly independent, or equivalently, an expansion*

$$E = \sum_{i=0, i\neq h}^{6} a_i A_i + \sum_{i=0, i\neq k}^{6} b_i B_i + \sum_{i=0, i\neq l}^{6} c_i C_i + \sum_{i=0, i\neq m}^{6} d_i D_i$$

is unique. In fact,

$$\{(A_i - A_h)/7, i \neq h; (B_i - B_k)/7, i \neq k; (C_i - C_l)/7, i \neq l; (D_i - D_k)/7, i \neq m\} \quad (13.1.2)$$

is a dual basis to $\{A_h, B_k, C_l, A_m\}^c$, i.e.,

$$a_i = (A_i - A_h, E)/7 \qquad b_i = (B_i - B_k, E)/7$$
$$c_i = (C_i - C_l, E)/7 \qquad d_i = (D_i - D_m, E)/7.$$

Proof. If $\{A_i\}$ and $\{B_j\}$ are as in Lemma 13.1.1,

$$(A_j, A_i - A_h)/7 = \begin{cases} 1 & \text{if } j = i; \\ -1 & \text{if } j = h; \\ 0 & \text{otherwise;} \end{cases}$$

and for any i and j,

$$(B_j, A_i - A_h) = (B_j, A_i) - (B_j, A_h) = 1 - 1 = 0.$$

If there is a relation among $\{A_h, B_k, C_l, A_m\}^c$, then taking the dot product with each element of (13.1.2), shows that each coefficient is 0, a contradiction. □

By definition, a matrix $E \in \mathcal{C}_7$ can be expressed in the form

$$E = \sum_{i=0}^{6} a_i A_i + \sum_{j=0}^{6} b_j B_j + \sum_{k=0}^{6} c_k C_k + \sum_{l=0}^{6} d_l D_l \quad (13.1.3)$$

with the coefficients a_i, b_j, c_k, d_l nonnegative integers. Because of (13.1.1), these coefficients are not uniquely determined by E. However, something almost as strong is true.

Lemma 13.1.3. *Within a particular step, the coefficients in the expansion* (13.1.3) *are determined up to an additive constant.*

Proof. Apply the dot product with A_i to the expansion in (13.1.3):

$$(A_i, E) = 7a_i + \sum_{j=0}^{6} b_j + \sum_{k=0}^{6} c_k + \sum_{l=0}^{6} d_l. \tag{13.1.4}$$

In particular, when $i = 0$,

$$(A_0, E) = 7a_0 + \sum_{j=0}^{6} b_j + \sum_{k=0}^{6} c_k + \sum_{l=0}^{6} d_l. \tag{13.1.5}$$

Subtracting (13.1.5) from (13.1.4) and dividing by 7, we derive that

$$a_i - a_0 = (E, A_i - A_0)/7.$$

Note the use of $A_i - A_0$ introduced with (13.1.2). The same relations hold for the other steps. □

We are now in a position to establish the main result of the section.

Theorem 13.1.4. *Every matrix $E \in \mathcal{C}_7$ has a unique expansion of the form*

$$E = mJ + \sum_{i=0}^{6} a_i A_i + \sum_{j=0}^{6} b_j B_j + \sum_{k=0}^{6} c_k C_k + \sum_{l=0}^{6} d_l D_l \tag{13.1.6}$$

with a_i, b_j, c_k, d_l nonnegative integers, subject to the condition that atleast one a_i, one b_j, one c_k and one d_l is zero. As a consequence,

$$\sum_{E \in \mathcal{C}_7} X(E) = \frac{1}{1 - X(J)} \left(\frac{1 - \prod_{i=0}^{6} X(A_i)}{\prod_{i=0}^{6} (1 - X(A_i))} \right) \left(\frac{1 - \prod_{i=0}^{6} X(B_i)}{\prod_{i=0}^{6} (1 - X(B_i))} \right)$$
$$\left(\frac{1 - \prod_{i=0}^{6} X(C_i)}{\prod_{i=0}^{6} (1 - X(C_i))} \right) \left(\frac{1 - \prod_{i=0}^{6} X(D_i)}{\prod_{i=0}^{6} (1 - X(D_i))} \right).$$

Proof. Given an expansion (13.1.3), set

$$a = \min\{\, a_i \mid i = 0, \ldots, 6 \,\}, \qquad b = \min\{\, b_i \mid i = 0, \ldots, 6 \,\},$$
$$c = \min\{\, c_i \mid i = 0, \ldots, 6 \,\}, \qquad d = \min\{\, d_i \mid i = 0, \ldots, 6 \,\}.$$

Extract copies of the trivial to get

$$\begin{aligned} E = {} & (a + b + c + d)J \\ & + \sum_{i=0}^{6} (a_i - a) A_i + \sum_{j=0}^{6} (b_j - b) B_j + \sum_{k=0}^{6} (c_k - c) C_k + \sum_{l=0}^{6} (d_l - d) D_l. \end{aligned} \tag{13.1.7}$$

The new coefficients are nonnegative yet atleast one new coefficient from each step is 0. Hence, (13.1.7) demonstrates the existence of the expansion in (13.1.6).

Setting the minimal coefficients for each step to 0 fixes the constant referred to in Lemma 13.1.3. Hence, the resulting expansion is unique.

The generating function follows by a similar argument to that found in the proof of Theorem 10.2.1. □

Using Lemma 10.2.2 and Lemma 10.2.3 together with the notation defined there, we get

Proposition 13.1.5. *The cross section of* $\mathcal{C}_7$ *defined by setting the index to 1 is*

$$CS_1(\mathcal{C}_7) = (\triangle_7^2 - \hat{J}) \times (\triangle_7^3 - \hat{J}) \times (\triangle_7^4 - \hat{J}) \times (\triangle_7^5 - \hat{J}) + \hat{J}.$$

In other words, the $CS_1(\mathcal{C}_7)$ *is the product of the four simplexes* $\triangle_7^2$, $\triangle_7^3$, $\triangle_7^4$, $\triangle_7^5$, *but where the product operation is performed with center* $\hat{J}$.

For classical order 7 pandiagonals, further restrict to those in the linear span of 2 types of steps, then the material in the beginning of Section 10.3 has an exact analogue. To get a count of such pandiagonals which have the 0 in the upper left corner, we select an ordered pair of steps and then a permutation of the numbers 1, 2, 3, 4, 5 and 6 for the first step and a permutation of 7, 14, 21, 28, 35 and 42 for the second step. There are $4(3)(6!)^2$ such matrices. There are $8\phi(7) = 48$ symmetries. Hence, there are $9(5!)^2$ such pandiagonals up to symmetry. How many classical pandiagonals in $\mathcal{C}_7$ there are in general is an open question.

13.2 Generating series for general prime order

The pandiagonal cyclics of order p have steps $2, 3, \ldots, p-2$. For $k = 0, \ldots, p-1$, $m = 2, \ldots, p-2$ let

$$A_k^m = \|\chi(j \equiv_p k + mi)\|_{i,j=0}^{p-1}.$$

$\mathcal{C}_p$ consists of all nonnegative integral linear combinations of these $(p-3)p$ matrices. Letting $a_{k,m}$ denote generic nonnegative integer coefficients, we get for any matrix $A \in \mathcal{C}_p$,

$$A = \sum a_{k,m} A_k^m. \tag{13.2.8}$$

Of course the expansion just described is not unique; we have the relations, for all n, m,

$$\sum_{k=0}^{p-1} A_k^m = \sum_{k=0}^{p-1} A_k^n = J \tag{13.2.9}$$

where J is the trivial matrix of all 1's.

Call "admissible" any $(p-1)(p-3)^{tuple}$ of matrices obtained by removing one element from each of the cyclic classes. The admissible $(p-1)(p-3)^{tuple}$ obtained by removing $A_{k_2}^2, A_{k_3}^3, \ldots, A_{k_{p-2}}^{p-2}$, will be denoted by $\{A_{k_2}^2, A_{k_3}^3, \ldots, A_{k_{p-2}}^{p-2}\}^c$. Let us treat the matrices as vectors with p^2 components.

Proposition 13.2.1. *The matrices of an admissible set* $\{A_{k_2}^2, A_{k_3}^3, \ldots, A_{k_{p-2}}^{p-2}\}^c$ *are linearly independent, or equivalently, an expansion*

$$A = \sum_{m=2}^{p-2} \sum_{k=0,\ k \neq k_m}^{p-1} a_{k,m} A_k^m$$

is unique. In fact,

$$\{(A_k^m - A_{k_m}^m)/p;\ k \neq k_m\} \tag{13.2.10}$$

is a dual basis to $\{A_{k_2}^2, A_{k_3}^3, \ldots, A_{k_{p-2}}^{p-2}\}^c$, *i.e.,*

$$a_{k,m} = (A_k^m - A_{k_m}^m, A)/p.$$

We are now in a position to establish the main result of the section.

Theorem 13.2.2. *Every matrix* $A \in \mathcal{C}_p$ *has a unique expansion of the form*

$$A = mJ + \sum a_{k,m} A_k^m \tag{13.2.11}$$

with $a_{k,m}$ *nonnegative integers, subject to the condition that atleast one* $a_{k,m}$ *for each* m *is zero. As a consequence,*

$$\sum_{A \in \mathcal{C}_p} X(A) = \frac{1}{1 - X(J)} \prod_{m=2}^{p-2} \left(\frac{1 - \prod_{k=0}^{p-1} X(A_k^m)}{\prod_{k=0}^{p-1} (1 - X(A_k^m))} \right).$$

Proof. Given an expansion (13.2.8), set

$$a_m = \min\{\, a_{k,m} \mid k = 0, \ldots, p-1\,\}.$$

Extract copies of the trivial to get

$$A = (a_2 + a_3 + \cdots + a_{p-2})J + \sum_{m=2}^{p-2} \sum_{k=0}^{p-1} (a_{k,m} - a_m) A_k^m.$$

□

As for the geometry, using Lemma 10.2.2 and Lemma 10.2.3 together with the notation defined there, we get

Proposition 13.2.3. *The cross section of $\mathcal{C}_p$ defined by requiring the index to be 1 is*

$$CS_1(\mathcal{C}_p) = \prod_{m=2}^{p-2} (\triangle_p^m - \hat{J}) + \hat{J}.$$

In other words, the $CS_1(\mathcal{C}_p)$ is the product of the $p-3$ simplexes $\triangle_p^2, \ldots, \triangle_p^{p-2}$, but where the product operation is performed with center $\hat{J}$.

For classical order p pandiagonals, further restrict to those in the linear span of 2 types of steps, then the material in the beginning of Section 10.3 has an exact analogue. To enumerate such pandiagonals which have the 0 in the upper left corner, select an ordered pair of steps and then a permutation of the numbers $1, 2, \ldots, p-1$ for the first step and a permutation of $p, 2p, \ldots, (p-1)p$ for the second step. There are $(p-2)(p-3)((p-1)!)^2$ such matrices. There are $8\phi(p) = 8(p-1)$ symmetries. Hence, there are $(p-1)(p-2)(p-3)((p-2)!)^2/8$ such pandiagonals up to symmetry. Enumeration of all classical pandiagonals in $\mathcal{C}_p$ is an open question.

Chapter 14

Linear span of cyclic P-squares for prime power order

Prime powers can be decomposed with a similar approach to that of primes. For demonstration purposes, we will present and sketch a proof for the solution spaces of orders 25 and 125. Finally, we will present the results for the general case.

14.1 Generating series for order 25

The pandiagonal cyclics of order 25 have steps 2, 3, 7, 8, 12, 13, 17, 18, 22 and 23. The sum of each of the cyclics for a particular step still equals the trivial, but there is a finer relation.

Definition 14.1.1. The *compound* cyclic of step a and start r is

$$M_r^a = \|\chi(j \equiv_5 ai + r)\|.$$

For $r = 0, \ldots, 4$, we get the additional relations

$$M_r^2 = \sum_{i=0}^{4} C_{r+5i}^2 = \sum_{i=0}^{4} C_{r+5i}^7 = \cdots = \sum_{i=0}^{4} C_{r+5i}^{22}$$

and

$$M_r^3 = \sum_{i=0}^{4} C_{r+5i}^3 = \sum_{i=0}^{4} C_{r+5i}^8 = \cdots = \sum_{i=0}^{4} C_{r+5i}^{23}.$$

The subset of cyclics which appears in a sum is a *mod 5 subclass* of cyclic matrices, e.g., residue $r = 3$ gives a subclass of step 7 cyclics, $\{C_3^7, C_8^7, \ldots, C_{23}^7\}$. Call "admissible" any

$10 \times 5 \times 4^{tuple}$ of matrices obtained by removing one element from each of the cyclic mod 5 subclasses. The admissible 200^{tuple}, obtained by removing $C^2_{i_{2,0}}, C^2_{i_{2,1}}, \ldots, C^{23}_{i_{23,4}}$ from a list of all 250 cyclics, will be denoted by

$$\{C^2_{i_{2,0}}, C^2_{i_{2,1}}, \ldots, C^{23}_{i_{23,4}}\}^c.$$

Treating the matrices as vectors with 625 components, different cyclics of the same step are orthogonal with respect to the usual dot product. The discussion preceding Lemma 10.2.3 shows that cyclics of steps a and b have dot product 1 provided that $a-b$ is invertible modulo n. For n a p prime power, all elements prime to p are invertible. If $a-b$ is not prime to p, then the dot product depends on the difference of the starts $r-s$. When n is the square of a prime p, we record the needed dot products as:

Lemma 14.1.2.

$$(C^a_r, C^a_s) = \begin{cases} n & \textit{if } r = s; \\ 0 & \textit{if } r \neq s. \end{cases}$$

For $a \neq b$,

$$(C^a_r, C^b_s) = \begin{cases} 1 & \textit{if } p \nmid a-b; \\ 0 & \textit{if } p|a-b \textit{ but } \nmid r-s; \\ p & \textit{if } p|a-b \textit{ and } |r-s. \end{cases}$$

Proposition 14.1.3. *The matrices of an admissible set*

$$\{C^2_{i_{2,0}}, C^2_{i_{2,1}}, \ldots, C^{23}_{i_{23,4}}\}^c$$

are linearly independent, or equivalently, an expansion

$$E = \sum_{a \in \{2,3,7,\ldots,23\}} \sum_{i=0, i \neq i_{a,0}, i_{a,1}, \ldots, i_{a,4}}^{24} c_{i,a} C^a_i$$

is unique. In fact,

$$\{(C^a_i - C^a_{i_{a,r}})/25, i \neq i_{a,r}, i \equiv_5 r;\ r = 0, \ldots, 4;\ a \in \{2,3,7,\ldots,23\}\} \tag{14.1.1}$$

is a dual basis to $\{C^2_{i_{2,0}}, C^2_{i_{2,1}}, \ldots, C^{23}_{i_{23,4}}\}^c$, i.e.,

$$c_{i,a} = (C^a_i - C^a_{i_{a,r}}, E)/25,\ i \equiv_5 r.$$

Proof. The proof follows by breaking the situation into cases and using Lemma 14.1.2. For example, let's look at the case $a \equiv_5 b$ and $i \equiv_5 s$. By the way we chose our candidates for a dual basis, $i \equiv_5 i_{a,r}$ and using the transitivity of congruence, $s \equiv_5 i_{a,r}$. Hence,

$$(C_s^b, C_i^a - C_{i_{a,r}}^a)/25 = ((C_s^b, C_i^a) - (C_s^b, C_{i_{a,r}}^a))/25 = (5-5)/25 = 0.$$

□

We are now in a position to establish the main result of the section.

Theorem 14.1.4. *Every matrix $E \in \mathcal{C}_{25}$ has a unique expansion of the form*

$$E = mJ + \sum_{r=0}^{4} \left(m_{r,2} M_r^2 + m_{r,3} M_r^3 \right) + \sum_{i=0}^{24} \sum_{a \in \{2,3,7,\ldots,23\}} c_{i,a} C_i^a, \tag{14.1.2}$$

where m is an arbitrary integer ≥ 0, and $m_{r,2}$, $m_{r,3}$ and $c_{i,a}$ are integers ≥ 0, such that

$$\prod_{r=0}^{4} m_{r,2} = \prod_{r=0}^{4} m_{r,3} = 0,$$

$$\prod_{i \equiv_5 r} c_{i,a} = 0 \ \forall a \in \{2,3,7,\ldots,23\} \text{ and } r = 0, \ldots, 4.$$

We deduce that

$$\begin{aligned}
\sum_{E \in \mathcal{C}_{25}} X(E) = {} & \frac{1}{1 - X(J)} \\
& \frac{1 - X(M_0^2)X(M_1^2)X(M_2^2)X(M_3^2)X(M_4^2)}{(1 - X(M_0^2))(1 - X(M_1^2))(1 - X(M_2^2))(1 - X(M_3^2))(1 - X(M_4^2))} \\
& \frac{1 - X(M_0^3)X(M_1^3)X(M_2^3)X(M_3^3)X(M_4^3)}{(1 - X(M_0^3))(1 - X(M_1^3))(1 - X(M_2^3))(1 - X(M_3^3))(1 - X(M_4^3))} \\
& \prod_{a \in \{2,3,7,\ldots,23\}} \left(\frac{1 - X(C_0^a)X(C_5^a)X(C_{10}^a)X(C_{15}^a)X(C_{20}^a)}{(1 - X(C_0^a))(1 - X(C_5^a))(1 - X(C_{10}^a))(1 - X(C_{15}^a))(1 - X(C_{20}^a))} \right. \\
& \frac{1 - X(C_1^a)X(C_6^a)X(C_{11}^a)X(C_{16}^a)X(C_{21}^a)}{(1 - X(C_1^a))(1 - X(C_6^a))(1 - X(C_{11}^a))(1 - X(C_{16}^a))(1 - X(C_{21}^a))} \\
& \vdots \\
& \left. \frac{1 - X(C_4^a)X(C_9^a)X(C_{14}^a)X(C_{19}^a)X(C_{24}^a)}{(1 - X(C_4^a))(1 - X(C_9^a))(1 - X(C_{14}^a))(1 - X(C_{19}^a))(1 - X(C_{24}^a))} \right).
\end{aligned} \tag{14.1.3}$$

In particular, the generating function for the index is

$$\begin{aligned}
\sum_{A \in \mathcal{C}_{125}} t^{\operatorname{ind} A} &= \frac{1}{1 - t^{25}} \left(\frac{1 - t^{25}}{(1 - t^5)^5} \right)^2 \left(\frac{1 - t^5}{(1 - t)^5} \right)^{50} \\
&= \frac{(1 - t^{25})(1 - t^5)^{40}}{(1 - t)^{250}}.
\end{aligned}$$

Proof. Extract the maximum possible copy of the trivial as possible. Take what's left and divide the entries based on locations congruent modulo 5. Take the minimum for each of these sets. Compound cyclics interact like cyclics for order 5. Hence, use Theorem 10.2.1 to decompose this compound cyclic part.

What remains is compound cyclic-free. Use Proposition 14.1.3 to decompose this part. The generating function follows from the same reasoning as used in the proof of Theorem 10.2.1. □

14.2 Generating series for order 125

We iterate the procedure performed with order 25. In addition to the relations gotten from the trivial and from M_r^2 and M_r^3, we get even finer relations from N_r^2, N_r^3, N_r^7, N_r^8, ... , N_r^{23}, for $r = 0, 1, \ldots, 24$, where

Definition 14.2.1. The compound cyclic of step a and start r

$$N_r^a = \|\chi(j \equiv_{25} ai + r)\|.$$

For $r = 0, \ldots, 24$, we get the additional relations

$$N_r^2 = \sum_{i=0}^{4} C_{r+25i}^{2} = \sum_{i=0}^{4} C_{r+25i}^{27} = \cdots = \sum_{i=0}^{4} C_{r+25i}^{102}$$
$$N_r^3 = \sum_{i=0}^{4} C_{r+25i}^{3} = \sum_{i=0}^{4} C_{r+25i}^{28} = \cdots = \sum_{i=0}^{4} C_{r+25i}^{103}$$
$$\vdots$$
$$N_r^2 = \sum_{i=0}^{4} C_{r+25i}^{23} = \sum_{i=0}^{4} C_{r+25i}^{48} = \cdots = \sum_{i=0}^{4} C_{r+25i}^{123}.$$

The subset of cyclics which appears in a sum is a *mod 25 subclass* of cyclic matrices, e.g., residue $r = 14$ gives a subclass of step 32 cyclics, $\{C_{14}^{32}, C_{39}^{32}, \ldots, C_{114}^{32}\}$. Call "admissible" any $50 \times 25 \times 4^{tuple}$ of matrices obtained by removing one element from each of the cyclic mod 25 subclasses. The admissible 5000^{tuple}, obtained by removing $C_{i_{2,0}}^2, C_{i_{2,1}}^2, \ldots, C_{i_{123,24}}^{123}$ from a list of all 6250 cyclics, will be denoted by

$$\{C_{i_{2,0}}^2, C_{i_{2,1}}^2, \ldots, C_{i_{123,24}}^{123}\}^c.$$

Treating the matrices as vectors with 15,625 components, different cyclics of the same step are orthogonal with respect to the usual dot product. The discussion preceding

Lemma 10.2.3 shows that cyclics of steps a and b have dot product 1 provided that $a-b$ is invertible modulo n. For n a p prime power, all elements prime to p are invertible. If $a-b$ is not prime to p, then the dot product depends on the difference of the starts $r-s$. When n is the cube of a prime p, we record the needed dot products as:

Lemma 14.2.2.

$$(C_r^a, C_s^a) = \begin{cases} n & \textit{if } r = s; \\ 0 & \textit{if } r \neq s. \end{cases}$$

For $a \neq b$,

$$(C_r^a, C_s^b) = \begin{cases} 1 & \textit{if } p \not| a-b; \\ 0 & \textit{if } p|a-b \textit{ but } \not| r-s \textit{ or } p^2|a-b \textit{ but } \not| r-s; \\ p & \textit{if } p|a-b \textit{ and } |r-s \textit{ but } p^2 \not| a-b; \\ p^2 & \textit{if } p^2|a-b \textit{ and } |r-s. \end{cases}$$

Proposition 14.2.3. *The matrices of an admissible set*

$$\{C_{i_{2,0}}^2, C_{i_{2,1}}^2, \ldots, C_{i_{123,24}}^{123}\}^c$$

are linearly independent, or equivalently, an expansion

$$E = \sum_{a\in\{2,3,7,\ldots,123\}} \sum_{i=0, i\neq i_{a,0}, i_{a,1}, \ldots, i_{a,24}}^{124} c_{i,a} C_i^a$$

is unique. In fact,

$$\{(C_i^a - C_{i_{a,r}}^a)/125, i \neq i_{a,r}, i \equiv_{25} r;\ \ r = 0, \ldots, 24;\ a \in \{2,3,7,\ldots,123\}\} \qquad (14.2.4)$$

is a dual basis to $\{C_{i_{2,0}}^2, C_{i_{2,1}}^2, \ldots, C_{i_{123,24}}^{123}\}^c$, i.e.,

$$c_{i,a} = (C_i^a - C_{i_{a,r}}^a, E)/125,\ i \equiv_{25} r.$$

Proof. The proof follows by breaking the situation into cases and using Lemma 14.2.2. For example, let's look at the case $a \equiv_{25} b$ and $i \equiv_{25} s$. By the way we chose our candidates for a dual basis, $i \equiv_{25} i_{a,r}$ and using the transitivity of congruence, $s \equiv_{25} i_{a,r}$. Hence,

$$(C_s^b, C_i^a - C_{i_{a,r}}^a)/125 = ((C_s^b, C_i^a) - (C_s^b, C_{i_{a,r}}^a))/125 = (25-25)/125 = 0.$$

□

We are now in a position to establish the main result of the section.

Theorem 14.2.4. *Every matrix $E \in \mathcal{C}_{125}$ has a unique expansion of the form*

$$\begin{aligned} E = mJ &+ \sum_{r=0}^{4} \left(m_{r,2} M_r^2 + m_{r,3} M_r^3 \right) \\ &+ \sum_{r=0}^{24} \left(n_{r,2} N_r^2 + n_{r,3} N_r^3 + \cdots + n_{r,23} N_r^{23} \right) + \sum_{i=0}^{124} \sum_{a \in \{2,3,7,\ldots,123\}} c_{i,a} C_i^a, \end{aligned} \tag{14.2.5}$$

where m is an arbitrary integer ≥ 0, $m_{r,2}$, $m_{r,3}$, $n_{r,2}$, $n_{r,3}$, $\ldots$, $n_{r,23}$ and $c_{i,a}$ are integers ≥ 0, subject to the condition that

$$\prod_{r=0}^{4} m_{r,2} = \prod_{r=0}^{4} m_{r,3} = 0,$$

$$\prod_{i=0}^{4} n_{5i+r,2} = \prod_{i=0}^{4} n_{5i+r,3} = \cdots = \prod_{i=0}^{4} n_{5i+r,23} = 0, \;\; r = 0, \ldots, 4$$

$$\prod_{i \equiv_{25} r} c_{i,a} = 0 \;\forall a \in \{2, 3, 7, \ldots, 123\} \text{ and } r = 0, \ldots, 24.$$

We deduce that

$$\begin{aligned}
\sum_{E\in\mathcal{C}_{125}} X(E) = {} & \frac{1}{1-X(J)} \\
& \frac{1-X(M_0^2)X(M_1^2)X(M_2^2)X(M_3^2)X(M_4^2)}{(1-X(M_0^2))(1-X(M_1^2))(1-X(M_2^2))(1-X(M_3^2))(1-X(M_4^2))} \\
& \frac{1-X(M_0^3)X(M_1^3)X(M_2^3)X(M_3^3)X(M_4^3)}{(1-X(M_0^3))(1-X(M_1^3))(1-X(M_2^3))(1-X(M_3^3))(1-X(M_4^3))} \\
& \frac{1-X(N_0^2)X(N_5^2)\dots X(N_{20}^2)}{(1-X(N_0^2))(1-X(N_5^2))\dots(1-X(N_{20}^2))} \\
& \frac{1-X(N_1^2)X(N_6^2)\dots X(N_{21}^2)}{(1-X(N_1^2))(1-X(N_6^2))\dots(1-X(N_{21}^2))} \\
& \vdots \\
& \frac{1-X(N_4^2)X(N_9^2)\dots X(N_{24}^2)}{(1-X(N_4^2))(1-X(N_9^2))\dots(1-X(N_{24}^2))} \\
& \frac{1-X(N_0^3)X(N_5^3)\dots X(N_{20}^3)}{(1-X(N_0^3))(1-X(N_5^3))\dots(1-X(N_{20}^3))} \\
& \vdots \\
& \frac{1-X(N_4^{23})X(N_9^{23})\dots X(N_{24}^{23})}{(1-X(N_4^{23}))(1-X(N_9^{23}))\dots(1-X(N_{24}^{23}))} \\
& \prod_{a\in\{2,3,7,\dots,123\}} \Bigg(\frac{1-X(C_0^a)X(C_{25}^a)X(C_{50}^a)X(C_{75}^a)X(C_{100}^a)}{(1-X(C_0^a))(1-X(C_{25}^a))(1-X(C_{50}^a))(1-X(C_{75}^a))(1-X(C_{100}^a))} \\
& \frac{1-X(C_1^a)X(C_{26}^a)X(C_{51}^a)X(C_{76}^a)X(C_{101}^a)}{(1-X(C_1^a))(1-X(C_{26}^a))(1-X(C_{51}^a))(1-X(C_{76}^a))(1-X(C_{101}^a))} \\
& \vdots \\
& \frac{1-X(C_{24}^a)X(C_{49}^a)X(C_{74}^a)X(C_{99}^a)X(C_{124}^a)}{(1-X(C_{24}^a))(1-X(C_{49}^a))(1-X(C_{74}^a))(1-X(C_{99}^a))(1-X(C_{124}^a))} \Bigg). \qquad (14.2.6)
\end{aligned}$$

In particular, the generating function for the index is

$$\begin{aligned}
\sum_{A\in\mathcal{C}_{125}} t^{\operatorname{ind} A} &= \frac{1}{1-t^{125}} \left(\frac{1-t^{125}}{(1-t^{25})^5}\right)^2 \left(\frac{1-t^{25}}{(1-t^5)^5}\right)^{50} \left(\frac{1-t^5}{(1-t)^5}\right)^{1250} \\
&= \frac{(1-t^{125})(1-t^{25})^{40}(1-t^5)^{1000}}{(1-t)^{6250}}.
\end{aligned}$$

Proof. Extract the maximum possible copy of the trivial as possible. Take what's left and divide the entries based on locations congruent modulo 5. Take the minimum for each of these sets. M-Compound cyclics interact like cyclics for order 5. Hence, use Theorem 10.2.1 to decompose this M-compound cyclic part.

Take what's left and divide the entries based on locations congruent modulo 25. Take the minimum for each of these sets. N-Compound cyclics interact like cyclics for order 25. Hence, use Theorem 14.1.4 to decompose this N-compound cyclic part.

What remains is compound cyclic-free. Use Proposition 14.2.3 to decompose this part. The generating function follows from the same reasoning as used in the proof of Theorem 10.2.1. □

14.3 Result for general prime power

We present notation which allow us to formalize the iterations introduced in the previous 2 sections.

Let $C(q)$ stand for the set of starts of cyclics of order q, e.g.,

$$C(25) = \{2, 3, 7, 8, 12, 13, 17, 18, 22, 23\}.$$

Let's define the compound cyclic of step a, start r and modulus p^k to be

$$M_r^a(p^k) = \left\|\chi(j \equiv_{p^k} ai + r)\right\|.$$

Compound cyclics are defined for $a \in C(p^k)$, $r = 0, \ldots, p^k$, and $k = 1, \ldots, n-1$.

Theorem 14.3.1. *Every matrix $E \in \mathcal{C}_{p^n}$ has a unique expansion of the form*

$$\begin{aligned} E = mJ + \sum_{a \in C(p)} \sum_{r=0}^{p-1} m_{r,a,1} M_r^a(p) + \sum_{a \in C(p^2)} \sum_{r=0}^{p^2-1} m_{r,a,2} M_r^a(p^2) \\ + \cdots + \sum_{a \in C(p^{n-1})} \sum_{r=0}^{p^{n-1}-1} m_{r,a,n-1} M_r^a(p^{n-1}) + \sum_{i=0}^{p^n-1} \sum_{a \in C(n-1)} c_{i,a} C_i^a, \end{aligned} \tag{14.3.7}$$

where m is an arbitrary integer ≥ 0, $m_{r,a,k}$, $c_{i,a}$ are integers ≥ 0, subject to the condition that

$$\prod_{r=0}^{p^k-1} m_{r,a,k} = 0, \ \forall a \in C(p^k), \ k = 1, \ldots, n-1$$

$$\prod_{i \equiv_{p^{n-1}} r} c_{i,a} = 0 \ \forall a \in C(p^n) \textit{ and } r = 0, \ldots, p^{n-1} - 1.$$

We deduce that

$$\sum_{E\in\mathcal{C}_{p^n}} X(E) = \frac{1}{1-X(J)}\prod_{k=1}^{n-1}\prod_{a\in C(p^k)}\prod_{r=0}^{4}\frac{1-\prod_{i\equiv_{p^{k-1}} r} X(M_i^a)}{\prod_{i\equiv_{p^{k-1}} r}(1-X(M_i^a))}$$
$$\prod_{a\in C(p^n)}\prod_{r=0}^{4}\frac{1-\prod_{i\equiv_{p^{n-1}} r} X(C_i^a)}{\prod_{i\equiv_{p^{n-1}} r}(1-X(C_i^a))}.$$

In particular, the generating function specialized to the index is

$$\sum_{A\in\mathcal{C}_{p^n}} t^{\operatorname{ind} A}$$
$$= \frac{1}{1-t^{p^n}}\left(\frac{1-t^{p^n}}{(1-t^{p^{n-1}})^p}\right)^{c(p)}\left(\frac{1-t^{p^{n-1}}}{(1-t^{p^{n-2}})^p}\right)^{c(p^2)p}\cdots\left(\frac{1-t^p}{(1-t)^p}\right)^{c(p^n)p^{n-1}}$$
$$= \frac{(1-t^{p^n})(1-t^{p^{n-1}})^{(c(p^2)-c(p))p}\ldots(1-t^p)^{(c(p^n)-c(p^{n-1}))p^{n-1}}}{(1-t)^{c(p^n)p^n}}$$

where $c(q) = |C(q)|$.

Chapter 15

Linear span of cyclic P-squares for composite order

Composite orders require more sophisticated techniques than primes and prime powers. We present the solution space of order 35 cyclics, a model for the general case.

15.1 Generating series for order 35

The pandiagonal cyclics of order 35 have steps 2, 3, 12, 17, 18, 23, 32 and 33. The sum of each of the cyclics for a particular step still equals the trivial, but there are finer relations.

The *compound* cyclic of step a, start r and modulus 5 is

$$M_r^a = \|\chi(j \equiv_5 ai + r)\|.$$

For the residues $r = 0, \ldots, 4$, we get some relations associated with the modulus 5 compound cyclics,

$$M_r^2 = \sum_{i=0}^{4} C_{r+5i}^{2} = \sum_{i=0}^{4} C_{r+5i}^{12} = \sum_{i=0}^{4} C_{r+5i}^{17} = \sum_{i=0}^{4} C_{r+5i}^{32}$$

and

$$M_r^3 = \sum_{i=0}^{4} C_{r+5i}^{3} = \sum_{i=0}^{4} C_{r+5i}^{18} = \sum_{i=0}^{4} C_{r+5i}^{23} = \sum_{i=0}^{4} C_{r+5i}^{33}.$$

The subset of cyclics which appears in a sum is a *mod 5 subclass* of cyclic matrices, e.g., residue $r = 3$ gives a subclass of step 12 cyclics, $\{C_3^{12}, C_8^{12}, \ldots, C_{33}^{12}\}$.

The *compound* cyclic of step a, start r and modulus 7 is

$$N_r^a = \|\chi(j \equiv_7 ai + r)\|.$$

For the residues $r = 0, \ldots, 6$, the associated relations are

$$N_r^2 = \sum_{i=0}^{6} C_{r+7i}^{2} = \sum_{i=0}^{6} C_{r+7i}^{23} \qquad N_r^3 = \sum_{i=0}^{6} C_{r+7i}^{3} = \sum_{i=0}^{6} C_{r+7i}^{17}$$

and

$$N_r^4 = \sum_{i=0}^{6} C_{r+7i}^{18} = \sum_{i=0}^{6} C_{r+7i}^{32} \qquad N_r^5 = \sum_{i=0}^{6} C_{r+7i}^{12} = \sum_{i=0}^{6} C_{r+7i}^{33}.$$

The subset of cyclics which appears in a sum is a *mod 7 subclass* of cyclic matrices, e.g., residue $r = 3$ gives a subclass of step 17 cyclics, $\{C_3^{17}, C_{10}^{17}, \ldots, C_{31}^{17}\}$.

For composite order n, there is no unique way to decompose an element of $E \in \mathcal{C}_n$. Instead, we give a canonical such decomposition. Extract a multiple of the trivial by as usual looking for the minimum of entries. Next, extract multiples of the modulus 5 compound cyclics, then the modulus 7 compound cyclics. The extracted compound-cyclics are an *admissible compound-cyclic set*, a $2 \times 4 + 4 \times 6$-tuple of compound-cyclics formed by taking the complement of a $2 + 4$-tuple of compound-cyclics

$$\{M_{i_2}^2, M_{i_3}^3, N_{j_2}^2, N_{j_3}^3, N_{j_4}^4, N_{j_5}^5\}.$$

Proposition 15.1.1. *An admissible compound-cyclic set is independent. In fact,* $(M_r^a - M_{i_a}^a)/245$*,* $r = 0, \ldots, 4$*,* $r \neq i_a$*,* $a = 2, 3$*,* $(N_r^a - N_{j_a}^a)/175$*,* $r = 0, \ldots, 6$*,* $r \neq j_a$*,* $a = 2, \ldots, 5$*, is a dual basis to*

$$\{M_{i_2}^2, M_{i_3}^3, N_{j_2}^2, N_{j_3}^3, N_{j_4}^4, N_{j_5}^5\}^c.$$

Proof. The nonzero elements which appear in a particular row of M_r^c are at the locations $\{a, a + 5, \ldots, a + 30\}$. The nonzero elements which appear in a particular row of N_s^d are at the locations $\{b, b + 7, \ldots, b + 28\}$. Finding the intersection of these 2 sets is equivalent to solving the simultaneous set of equations modulo 35

$$x \equiv_5 a$$

$$x \equiv_7 b.$$

By the Chinese remainder theorem, there is a unique solution for each such system. Hence,

$$(M_r^a, N_s^b) = 35 \qquad \forall r, s, a, b$$

A modulus 5 compound-cyclic is 7×7 copies of an order 5 cyclic. A modulus 7 compound-cyclic is 5×5 copies of an order 7 cyclic. Hence, we can use the results from Chapter 13 for relations within each of the modulus 5 and modulus 7 compound-cyclic parts. □

Corollary 15.1.2. *The generating function for the compound-cyclic part is*

$$\begin{gathered}\frac{1}{1-X(J)} \\ \frac{1-X(M_0^2)X(M_1^2)X(M_2^2)X(M_3^2)X(M_4^2)}{(1-X(M_0^2))(1-X(M_1^2))(1-X(M_2^2))(1-X(M_3^2))(1-X(M_4^2))} \\ \frac{1-X(M_0^3)X(M_1^3)X(M_2^3)X(M_3^3)X(M_4^3)}{(1-X(M_0^3))(1-X(M_1^3))(1-X(M_2^3))(1-X(M_3^3))(1-X(M_4^3))} \\ \frac{1-X(N_0^2)X(N_1^2)\cdots X(N_6^2)}{(1-X(N_0^2))(1-X(N_1^2))\cdots(1-X(N_6^2))} \\ \vdots \\ \frac{1-X(N_0^5)X(N_1^5)\cdots X(N_6^5)}{(1-X(N_0^5))(1-X(N_1^5))\cdots(1-X(N_6^5))}.\end{gathered} \tag{15.1.1}$$

What's left is compound-cyclic-free. The generating function requires an operation "$*$". Define $\prod_{i \in A} X(C_i) * \prod_{i \in B} X(C_i) = \prod_{i \in A \cup B} X(C_i)$. In words, the "$*$" eliminates any duplication.

Proposition 15.1.3. *The generating function for the compound-cyclic-free part has as numerator*

$$\begin{aligned}\prod_{a \in \{2,3,12,17,18,23,32,33\}} & (((1-X(C_0^a)X(C_5^a)\ldots X(C_{30}^a)) \\ & (1-X(C_1^a)X(C_6^a)\ldots X(C_{31}^a))\ldots(1-X(C_4^a)X(C_9^a)\ldots X(C_{34}^a))) * \\ & ((1-X(C_0^a)X(C_7^a)\ldots X(C_{28}^a))(1-X(C_1^a)X(C_8^a)\ldots X(C_{29}^a))\ldots \\ & (1-X(C_6^a)X(C_{13}^a)\ldots X(C_{34}^a))))\end{aligned}$$

and denominator

$$\prod_{a \in \{2,3,12,17,18,23,32,33\}} \prod_{r=0}^{34} (1-X(C_r^a)).$$

After programming the star operation, Mathematica outputs:

Corollary 15.1.4. *The generating function for the compound-cyclic-free part restricted to cyclics of one particular step, specialized to the index has as numerator*

$$\begin{gathered}
1-7\,t^{5}-5\,t^{7}+21\,t^{10}+35\,t^{11}+10\,t^{14}-140\,t^{15}-70\,t^{17}\\
+175\,t^{19}+245\,t^{20}-10\,t^{21}-455\,t^{23}-231\,t^{25}+350\,t^{26}+455\,t^{27}\\
+5\,t^{28}-595\,t^{29}+112\,t^{30}+245\,t^{32}-175\,t^{33}+35\,t^{34}-t^{35}=\\
(1-t)^{7}(1+7\,t+28\,t^{2}+84\,t^{3}+210\,t^{4}+455\,t^{5}+875\,t^{6}+1515\,t^{7}\\
+2380\,t^{8}+3395\,t^{9}+4375\,t^{10}+5040\,t^{11}+5075\,t^{12}+4235\,t^{13}+2505\,t^{14}\\
+175\,t^{15}-2170\,t^{16}-3815\,t^{17}-4235\,t^{18}-3395\,t^{19}-1785\,t^{20}\\
-200\,t^{21}+735\,t^{22}+840\,t^{23}+455\,t^{24}+84\,t^{25}-42\,t^{26}-28\,t^{27}+t^{28})
\end{gathered}$$

and as denominator $(1-t)^{35}$.

The generating function for the entire compound-cyclic-free part specialized to the index is the 8th power of the above. Putting the pieces together,

Proposition 15.1.5. *The generating function for $\mathcal{C}_{35}$, specialized to the index, is*

$$\frac{(1-t^{35})^{6}(1-7\,t^{5}-5\,t^{7}+21\,t^{10}+35\,t^{11}+10\,t^{14}-140\,t^{15}-\cdots-t^{35})^{8}}{(1-t^{35})(1-t^{7})^{10}(1-t^{5})^{28}(1-t)^{280}}.$$

Proof of Proposition 15.1.3. The conditions that an expression be compound-cyclic-free in one step are independent from those of another step. Hence, we need only consider a fixed step.

Within a fixed step, the generating function follows from inclusion-exclusion. Since inclusion-exclusion involves union, the "$*$" operation takes care of overlap. Note that the "$*$" operation is not needed within compound-cyclics of the same type since those sets are disjoint. □

15.2 Generating series for general composite orders

Factor the order n into a product of maximal prime powers. Take each of these prime powers and extract the composite-cyclics modulo that prime power. The Chinese remainder theorem shows as in the proof of Proposition 15.1.1 that the composite-cyclics modulo one prime power are independent of the composite-cyclics modulo another. Hence, the generating function for the composite-cyclic part is the product of the generating functions for each of the composite-cyclics modulo one of the prime powers.

Since the composite-cyclics modulo a prime power are just multiple copies of cyclics with prime power order, such a generating function follows from the material of Chapter 14. For the composite-cyclic-free part, use the "*" operation between the products of the cyclics in the numerator which arise from compound-cyclics of different moduli.

Chapter 16

Order 6, 7 and 8 examples

16.1 Bicyclic squares of order 2^m: general facts

Since the order n is a power of 2, all odd numbers are prime to n.

Definition 16.1.1. Given an even start e, an odd start o, and a singly even step a, $B^a_{e,o} = C^a_e + C^a_o$ is a *bicyclic.*

Denote by $\mathcal{B}_n$ the nonnegative integer span of the order n pandiagonal bicyclic and transpose bicyclic matrices. In the next section, we present the generating function for the bicyclic space of order 8.

Proposition 16.1.2. *Bicyclics are pandiagonal.*

Proof. By definition, cyclics have equal row sums. Since $a - 1$ and $a + 1$ are prime to n, C^a_e and C^a_o are primary and secondary diagonal by Proposition 12.2.1 Parts 2 and 3.

$j \equiv_n ai + e$ clearly has no solution for j odd. For j even, divide j, a, e and n by two. Since a is singly even, $a/2$ is invertible. For a fixed even j, there is a unique i modulo $n/2$ or exactly 2 i's modulo n. Hence, C^a_e hits every even column twice. Similarly, C^a_o hits every odd column twice. (If j is odd, subtract o from both sides of $j \equiv_n ai + o$. $j - o$ is even and we can again divide the whole equation by 2.) □

Proposition 16.1.3. *$\mathcal{B}_n$ is invariant under pandiagonal symmetries.*

Proof. Under toric translations, the cyclics of a particular step are invariant and the parities of the starts of a bicyclic remain the same or switch. Hence, the bicyclics are invariant under toric translations.

The linear symmetries are

$$\begin{bmatrix}\alpha & 0\\ 0 & \alpha\end{bmatrix}\quad\begin{bmatrix}\alpha & 0\\ 0 & -\alpha\end{bmatrix}\quad\begin{bmatrix}\alpha & 0\\ 0 & \alpha\end{bmatrix}\quad\begin{bmatrix}0 & \alpha\\ \alpha & 0\end{bmatrix}\quad\begin{bmatrix}0 & \alpha\\ -\alpha & 0\end{bmatrix}$$

for all α odd.

Given the cyclic C_r^a, $\chi(j \equiv_n ai + r)$, the first matrix gives us $\chi(\alpha^{-1}j \equiv_n a\alpha^{-1}i + r)$ or $\chi(j \equiv_n ai + \alpha r)$, i.e., the start is multiplied by α. Since α is odd, the parity is unaffected.

The second matrix gives us $\chi(-\alpha^{-1}j \equiv_n a\alpha^{-1}i + r)$ or $\chi(j \equiv_n -ai - \alpha r)$. The step is multiplied by -1 and the start is multiplied by $-\alpha$. Since a is singly even, then so is the new step $-a$. α is odd which implies that $-\alpha$ is too; hence the parity of the start is unaffected.

The other matrices are just the composition of a previously considered case and the matrix

$$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

which transposes the matrix. Since transpose cyclics are included in our space, we get closure under these matrices too. □

16.2 The bicyclic squares of order 8

The step of an order 8 bicyclic can be either 2 or 6. Once the step is chosen, there are 4 choices for e and 4 choices for o. We need to find the relations among the bicyclics and transpose bicyclics.

Solving simultaneously

$$j \equiv_n 2i + r$$
$$j \equiv_n 6i + s,$$

we get

$$(C_r^2, C_s^6) = \begin{cases} 0 & 4 \not| r - s; \\ 4 & 4 | r - s. \end{cases} \tag{16.2.1}$$

As a consequence, we get

$$(B^2_{e_1,o_1}, B^6_{e_2,o_2}) = \begin{cases} 0 & 4 \nmid e_1 - e_2, 4 \nmid o_1 - o_2; \\ 4 & 4 \nmid e_1 - e_2, 4 | o_1 - o_2 \text{ or } 4 | e_1 - e_2, 4 \nmid o_1 - o_2; \\ 8 & 4 | e_1 - e_2, 4 | o_1 - o_2. \end{cases} \tag{16.2.2}$$

As was done for the linear span of the cyclics, we define compound objects which we extract first, leaving a compound-free part. Each of the compound objects, which we shall call a *compound bicyclic*, can be thought of either as the sum of 2 compound cyclics of different parity or as the sum of 2 bicyclics. We shall call such a pair of bicyclics *compound complements.*

Definition 16.2.1. The *compound cyclic* modulo 4 with start r and step 2 is

$$CC_r = \chi(j \equiv_4 ai + r).$$

The *compound bicyclic* modulo 4 with starts e and o and step 2 is

$$CB_{e,o} = CC_e + CC_o.$$

Recall that

$$CC_r = C^a_r + C^a_{r+4},$$

for $r = 0, 1, 2, 3$, $a = 2, 6$. In a similar vein, we get

$$CB_{e,o} = B^a_{e,o} + B^a_{e+4,o+4}$$
$$CB_{e,o} = B^a_{e,o+4} + B^a_{e+4,o},$$

for $e = 0, 2$, $o = 1, 3$, $a = 2, 6$.

An order 8 compound bicyclic is 4 copies of an order 4 bicyclic juxtaposed to get an order 8 matrix. Hence, we can use Theorem 8.7.2 for the generating function of the space of compound bicyclics and compound tbicyclics. What's left is compound-free.

Proposition 16.2.2. *The bicyclics of order 8 in a compound-free set are independent.*

Proof. For a fixed bicyclic, the conditions of divisibility by 4 in (16.2.2) will be the same for a bicyclic of a different step and its complement, allowing us to apply the collection of each bicyclic minus its complement as linear functionals to separate the bicyclics of step 2 from those of step 6. Lemma 8.5.3 allows us to separate the bicyclics from the transpose bicyclics using the same linear functionals. Hence, it suffices to show the independence of the compound-free within one step. The entire set of bicyclics for a particular step is none other than the direct product of the space of odd cyclics and the space of the even cyclics for that step. A basis for this space is the tensor product of bases for each of the spaces. The cyclics of a fixed step are orthogonal. Since the compound-free are a subset of this set, they are certainly independent. □

Corollary 16.2.3. *The generating function for the compound-free subset of $\mathcal{B}_8$ is*

$$\frac{\prod_{a\in\{2,6\},\ e\in\{0,2\},\ o\in\{1,3,5,7\}}\left(1-X(CB^a_{e,o})X(CB^a_{e+4,o+4})\right)\left(1-X({}^tCB^a_{e,o})X({}^tCB^a_{e+4,o+4})\right)}{\prod_{a\in\{2,6\},\ e\in\{0,2,4,6\},\ o\in\{1,3,5,7\}}\left(1-X(CB^a_{e,o})\right)\left(1-X({}^tCB^a_{e,o})\right)}$$

Specializing to the index, we get

$$\frac{(1-t^4)^{32}}{(1-t^2)^{64}}=\left(\frac{1+t^2}{1-t^2}\right)^{32}.$$

Combining with the compound-cyclics, we get

Corollary 16.2.4. *The generating function specialized to the index for $\mathcal{B}_8$ is*

$$\sum_{A\in\mathcal{B}_8} t^{\operatorname{ind} A}=\frac{1}{1-t^8}\left(\frac{1+t^4}{1-t^4}\right)^4\left(\frac{1+t^2}{1-t^2}\right)^{32}.$$

16.3 P-squares and most-perfect squares

Our methods have not yet yielded decompositions for $\mathcal{P}_6$ and $\mathcal{P}_7$. Computer experimentation reveals that each space has several 100's of thousands of extreme rays. Up to symmetry, the number reduces down in both cases to around 1000 with a wide spectrum of orders. For order 6, there are 265,536 extreme rays. Up to pandiagonal symmetries, there are 960 completely fundamental elements. Enumerating the completely fundamental element representatives with regards to the size of the stabilizer, we get

order of stabilizer	1	2	4
#	889	61	72.

As a check, $265536 = 889 * 288 + 61 * 144 + 10 * 72$. Enumerating with regards to the indices,

index	6	12	18	24	30	36
#	384	385	145	36	8	2.

Most perfect squares are magic squares that are both W-squares and P-squares. By Corollary 4.4.6, only an additional equation which links two diagonals with index of different parity is needed to obtain the space of most-perfect squares from W-squares. Hence, the dimension of the space of most-perfect squares of order n is $2n-3$. Computer experimentation has shown that there are 918 extreme rays for $n=6$ and 10568 extreme rays for $n=8$, with 250 and 2496 extreme rays in a facet, respectively. For order 6, there is an additional symmetry which is not pandiagonal.

Proposition 16.3.1. *An order 6 most perfect square which has 3 consecutive columns (rows) reversed remains a most perfect square.*

Proof. Using the torus transformations, we can assume that the first 3 columns have been reversed. Use ”′” to indicate the objects in the transformed square. The transformation leaves the sets of rows and columns invariant. The blocks of 4 squares will still have equal sums, e.g., the 3rd upper block is an alternating sum of the first 3 original blocks. By Corollary 4.4.6, it suffices to show that 1 diagonal has a sum equal to a previous diagonal. In terms of the entries of the original square, P_0' is

$$\begin{pmatrix} & & a' & & & \\ & b & & & & \\ c' & & & & & \\ & & & d & & \\ & & & & e & \\ & & & & & f \end{pmatrix}$$

By Lemma 4.4.4, $a'+c'$ is equal to the $a+c$ of the diagonal P_0

$$\begin{pmatrix} a & & & & & \\ & b & & & & \\ & & c & & & \\ & & & d & & \\ & & & & e & \\ & & & & & f \end{pmatrix}$$

of the original square. □

Up to symmetry, including this new most perfect symmetry, there are 5 extreme rays for order 6, with indices, 6,6,12,12 and 24:

$$\begin{pmatrix}0&0&1&1&2&2\\2&2&1&1&0&0\\0&0&1&1&2&2\\2&2&1&1&0&0\\0&0&1&1&2&2\\2&2&1&1&0&0\end{pmatrix}\qquad\begin{pmatrix}0&1&0&2&1&2\\1&2&1&1&0&1\\1&0&1&1&2&1\\1&2&1&1&0&1\\1&0&1&1&2&1\\2&1&2&0&1&0\end{pmatrix}$$

$$0^{12}1^{12}2^{12}\qquad 0^{8}1^{20}2^{8}$$

$$\begin{pmatrix}0&0&3&3&3&3\\3&5&0&2&0&2\\0&0&3&3&3&3\\4&4&1&1&1&1\\0&0&3&3&3&3\\5&3&2&0&2&0\end{pmatrix}\qquad\begin{pmatrix}0&2&3&2&3&2\\3&3&0&3&0&3\\0&2&3&2&3&2\\3&3&0&3&0&3\\0&2&3&2&3&2\\6&0&3&0&3&0\end{pmatrix}$$

$$0^{10}1^{4}2^{4}3^{14}4^{2}5^{2}\qquad 0^{10}2^{9}3^{16}6$$

$$\begin{pmatrix}0&0&5&6&7&6\\7&9&2&3&0&3\\0&0&5&6&7&6\\7&9&2&3&0&3\\0&0&5&6&7&6\\10&6&5&0&3&0\end{pmatrix}$$

$$0^{10}2^{2}3^{5}5^{4}6^{7}7^{5}9^{2}(10).$$

16.4 Jump W-squares of order 6

Recall that in P-squares of order 4, nonadjacent elements in a diagonal sum to half the index. We say that a square of order n, even, is *diagonally jump* or jump for short if elements that are located a distance $n/2$ along any diagonal sum to $\frac{2}{n}$ times the index. Let $\mathfrak{JW}_n$ denote the set of jump W-squares of order n with nonnegative integer entries. For order 6, there is only one completely fundamental square up to torus translation and dihedral operations:

$$\begin{pmatrix}2&1&0&2&1&0\\0&1&2&0&1&2\\2&1&0&2&1&0\\0&1&2&0&1&2\\2&1&0&2&1&0\\0&1&2&0&1&2\end{pmatrix}.$$

We classify the completely fundamental squares by whether the rows of 1's are horizontal, as above, or vertical. There are 6 of each type.

To decompose a jump W-square A, proceed as usual by finding the minimal value of the entries, m, and subtracting mJ from A to get A^O. With at least one entry 0, A^O will be on at least one of the facets. The cross section polytope is a hexagon×hexagon centered at J; each hexagon is a composed of one type of completely fundamental square. Each facet of the cross section polytope is a tetrahedron with 2 horizontal and 2 vertical completely fundamental squares. Instead of a Schlegel diagram, we depict the figure by cutting one of the hexagons and straightening it out on the y-axis. The other hexagon is left undistorted but projected onto the xz-plane. (See Figure 16.1). If we now connect each vertex in one of the hexagons with the vertices of the other hexagon, we get 30 of the facets (see Figure 16.2). The other 6 facets are formed by rejoining the hexagon which has been cut. Denote the 6 horizontal completely fundamental squares by $\{H_{0,1}, \ldots, H_{3,2}\}$, where indices indicate respectively the locations of the first 0 and and the first 2 in row 0. The example is $H_{2,0}$. Similarly list the 6 vertical extremes as $\{V_{0,1}, \ldots, H_{2,0}\}$, where the indices correspond respectively to the locations of the first 0 and the first 2 in column 0. Two extremes of the same type are adjacent iff one of their indices is the same. Two extremes of the same type are opposite iff their indices are the reverse of one another.

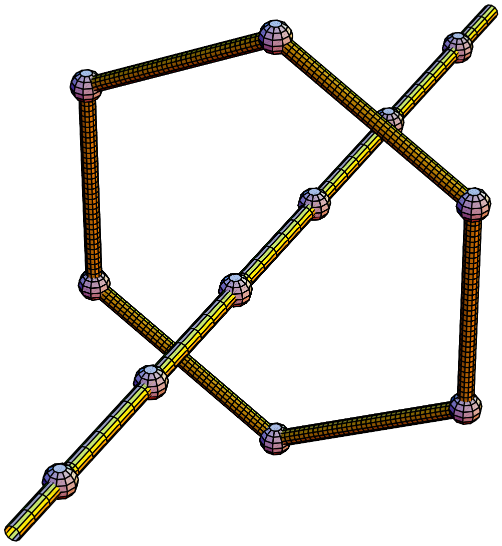


Figure 16.1: 2 perpendicular hexagons, one "straightened" onto the y axis.

Proposition 16.4.1. *The generating function for diagonally jump W-squares of order 6*

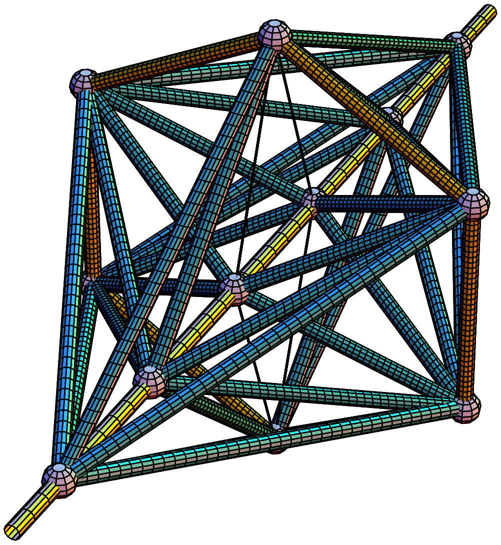


Figure 16.2: 30 of the 36 facets of the hexagon×hexagon.

is

$$\begin{aligned}\sum_{A\in\mathcal{J}\mathcal{P}_6} X(A) = \frac{1}{1-X(J)} \\ &\left(\frac{1}{(1-X(H_{0,1}))(1-X(H_{0,2}))}+\frac{X(H_{1,2})}{(1-X(H_{0,2}))(1-X(H_{1,2}))}+\dots\right. \\ &\left.+\frac{X(H_{2,1})}{(1-X(H_{2,0}))(1-X(H_{2,1}))}+\frac{X(H_{0,1})X(H_{2,1})}{(1-X(H_{0,1}))(1-X(H_{2,1}))}\right) \\ &\left(\frac{1}{(1-X(V_{0,1}))(1-X(V_{0,2}))}+\frac{X(V_{1,2})}{(1-X(V_{0,2}))(1-X(V_{1,2}))}+\dots\right. \\ &\left.+\frac{X(V_{2,1})}{(1-X(v_{2,0}))(1-X(V_{2,1}))}+\frac{X(V_{0,1})X(V_{2,1})}{(1-X(V_{0,1}))(1-X(V_{2,1}))}\right)\end{aligned} \qquad (16.4.3)$$

In particular, the generating function specialized to the index is

$$\begin{aligned}\sum_{A\in\mathcal{J}\mathcal{P}_6} t^{\operatorname{ind} A} &= \frac{1}{1-t^6}\left(\frac{1+4t^6+t^{12}}{(1-t^6)^2}\right)^2 \\ &= \frac{(1+4t^6+t^{12})^2}{(1-t^6)^5}.\end{aligned}$$

Proof. It remains to check whether there are any other fundamental squares within a facet besides the completely fundamental. Restricting to a facet, the index of the subgroup generated by the completely fundamental jump squares in the group of all jump squares is the GCD of all the 4×4 subdeterminants of the 4 completely fundamental which define a facet written as row vectors. A quick look at a group of 4 completely fundamental squares which define a facet

$$\begin{array}{cccccccccccccc}
2 & 1 & 0 & 2 & 1 & 0 & 0 & 1 & 2 & 0 & 1 & 2 & 2 & \cdots \\
2 & 0 & 1 & 2 & 0 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 2 & \cdots \\
2 & 0 & 2 & 0 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 2 & 1 & \cdots \\
2 & 0 & 2 & 0 & 2 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & \cdots
\end{array}$$

reveals that the GCD is 1, e.g., choose columns 2,6,7 and 13. □

16.5 Jump W-squares of order 8

For jump W-squares of order 8, the completely fundamental squares up to dihedral operations and torus translation are

$$\begin{pmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1
\end{pmatrix} \quad \text{and} \quad \begin{pmatrix}
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1
\end{pmatrix},$$

but the pandiagonal symmetry defined by the index operator $\begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}$ is an involution which transforms each matrix above into the other. Hence, up to pandiagonal symmetries, there is again only one completely fundamental square.

Denote the 8 completely fundamental squares with horizontal blocks of 1's of size 2, such as the first one above, with $\{H2_0, \ldots, H2_7\}$ and the 8 completely fundamental squares with horizontal blocks of 1's of size 4, such as the second one above, with $\{H4_0, \ldots, H4_7\}$, the index in each case identifying the start of the block of consecutive 1's in row 0. The remaining 16 fundamental elements have vertical blocks of 1's of size 2 and 4 and are denoted with $\{V2_0, \ldots, V2_7\}$ and $\{V4_0, \ldots, V4_7\}$, respectively, the index in each case identifying the start of the block of consecutive 1's in row 0. . To decompose a square A, extract a multiple of the trivial J to get A^0, a square which is located on the boundary. Each facet of the cross section polytope is the direct product of a cube with 8 horizontal extreme rays and a cube of 8 vertical extreme rays. For an example of the extreme rays of such a cube, we have

$$H4_1 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \qquad H2_3 = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$$H4_2 = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \qquad H4_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$H2_4 \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \qquad H4_4 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$H2_1 = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} \qquad H2_6 = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

The squares have been presented above so that adjacencies are preserved, see Figure 16.3. Notice that any 2 opposite vertices of the cube sum to

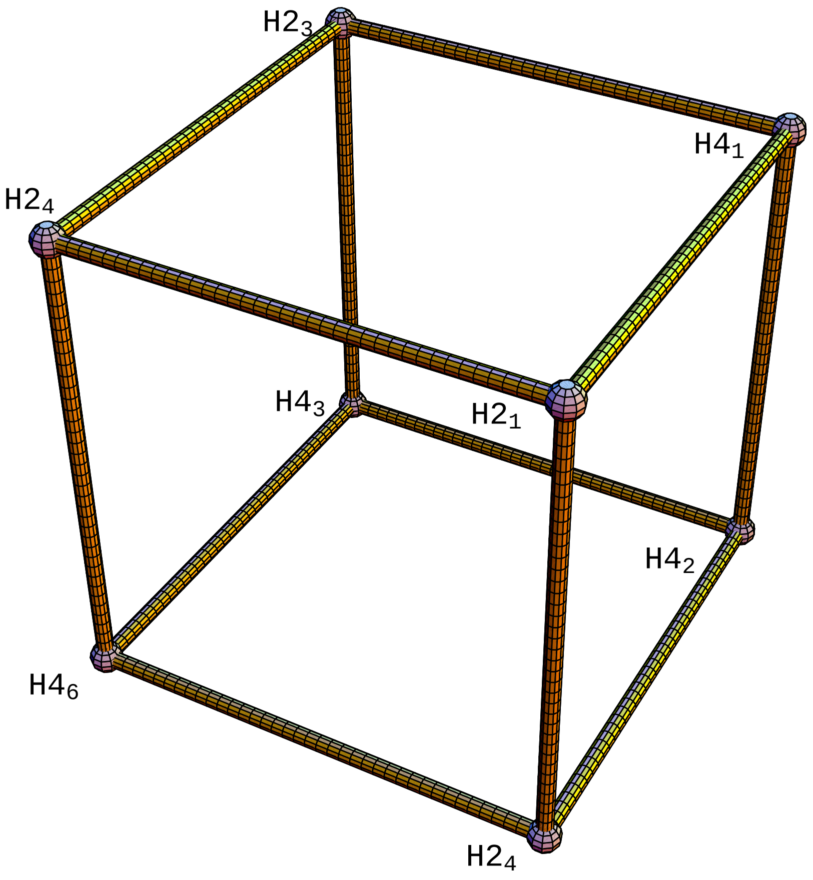


Figure 16.3: A horizontal cube in a facet for jump W-squares of order 8.

$$C = \begin{pmatrix} 0 & 1 & 1 & 1 & 2 & 1 & 1 & 1 \\ 2 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 2 & 1 & 1 & 1 \\ 2 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 2 & 1 & 1 & 1 \\ 2 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 2 & 1 & 1 & 1 \\ 2 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

By removing any multiples of C, we are assured of being on the boundary of the cube. The GCD of the 4×4 subdeterminants formed from 3 adjacent vertices of the cube and C is 1. To get the generating function for the facet, it remains to shell the cube. Instead of getting an explicit form for the generating function, I will instead sketch the process and derive the generating function specialized to the index. Since the index is always a multiple of 4, let $u = t^4$, where the power of t is keeping track of the index. We begin the shelling with the top of a cube, which is a square: $\frac{1+u}{(1-u)^3}$. Triangulating the sides of the cube so that the triangles adjacent to the top have no common edges, we add $\frac{4u}{(1-u)^3}$. The remaining 4 triangles of the sides and first triangle of the bottom contribute $\frac{5u^2}{(1-u)^3}$. The last triangle in the bottom contributes $\frac{u^3}{(1-u)^3}$. Adding C back into the picture and remembering that we are looking at only half of a direct product, we conclude that the generating function specialized to the index for a facet of jump W-squares of order 8 is

$$\frac{1}{(1-u^2)^2}\frac{(1+5u+5u^2+u^3)^2}{(1-u)^6},$$

with u replaced by t^4.

Bibliography

[And60] W. R. Andress. Basic properties of pandiagonal magic squares. *Amer. Math. Monthly*, 67:143–152; correction, 658, 1960.

[BJ76] William H. Benson and Oswald Jacoby. *New recreations with magic squares.* Dover, 1976.

[Ell03] E. B. Elliott. On linear homogeneous diophantine equations. *Quart. J. of Pure and Applied Math.*, 34(2):348–377, 1903.

[FP96] Komei Fukuda and Alain Prodon. Double description method revisited. In *Combinatorics and computer science (Brest, 1995)*, pages 91–111. Springer, Berlin, 1996.

[Gar80] Adriano M. Garsia. Combinatorial methods in the theory of Cohen-Macaulay rings. *Adv. in Math.*, 38(3):229–266, 1980.

[Guy94] Richard K. Guy. *Unsolved problems in number theory.* Springer-Verlag, New York, second edition, 1994. Unsolved Problems in Intuitive Mathematics, I.

[Knu68] D. E. Knuth. Very magic squares. *Amer. Math. Monthly*, 75:260–264, 1968.

[Koe96] Joseph L. Koerner. *The Moment of Self-Portraiture in German Renaissance Art.* University of Chicago Press, Chicago, 1993; paperback edition, 1996.

[Lev94] Joshua L. Levenberg. *Counting pandiagonal magic squares.* Undergraduate Thesis, Reed College, Portland, OR, 1994.

[Mac60] Percy A. MacMahon. *Combinatory analysis.* Chelsea Publishing Co., New York, 1960. Two volumes (bound as one).

[Mar77] Daniel A. Marcus. *Number fields.* Springer-Verlag, New York, 1977. Universitext.

[MRTT53] T. S. Motzkin, H. Raiffa, G. L. Thompson, and R. M. Thrall. The double description method. In *Contributions to the theory of games, vol. 2*, pages 51–73. Princeton University Press, Princeton, N. J., 1953. Annals of Mathematics Studies, no. 28.

[Mül97a] Wolfgang Müller. Group actions on magic squares. *Sém. Lothar. Combin.*, 39:Art. B39b, 14 pp. (electronic), 1997.

[Mül97b] Wolfgang Müller. Magische 4×4-quadrate. *Math. Semesterber.*, 44(2):131–137, 1997.

[OB98] Kathleen Ollerenshaw and David S. Brée. *Most-perfect pandiagonal magic squares.* Institute of Mathematics and its Applications, Southend, 1998. Their construction and enumeration, With a foreword by Hermann Bondi.

[Pad97] T. V. Padmakumar. Strongly magic squares. *Fibonacci Quart.*, 35(3):198–205, 1997.

[Rob96] John P. Robertson. Magic squares of squares. *Math. Mag.*, 69(4):289–293, 1996.

[Sta86] Richard P. Stanley. *Enumerative combinatorics. Vol. I.* Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, Calif., 1986. With a foreword by Gian-Carlo Rota.

[vdE90] Arno van den Essen. Magic squares and linear algebra. *Amer. Math. Monthly*, 97(1):60–62, 1990.

[Wil85] S. Gill Williamson. *Combinatorics for computer science.* Computer Science Press, Rockville, Md., 1985.

[Zie95] Günter M. Ziegler. *Lectures on polytopes.* Springer-Verlag, New York, 1995.