STANLEY'S THEORY OF MAGIC SQUARES

Qimh Richey Xantcha*

EAUMP Summer School on Combinatorial Commutative Algebra
Arusha, 13th August – 21st August 2012

> Mombi was not exactly a Witch, because the Good Witch who ruled that part of the Land of Oz had forbidden any other Witch to exist in her dominions. So Tip's guardian, however much she might aspire to working magic, realized it was unlawful to be more than a Sorceress, or at most a Wizardess.
>
> — L. Frank Baum: *The Marvelous Land of Oz*

This is an introduction to Magic Squares using the tools of Commutative Algebra, following Stanley: [4], [5], [6]. We lay no claims to originality, nor do we vouch for the correctness of these notes.

The prerequisites are rather modest: basic knowledge of graded rings and modules, exact sequences, projective resolutions, and Hilbert's Syzygy Theorem.

§1. — Magic Squares

Magic squares have spelt fascination to mankind throughout history and all across the globe. The qualifying epithet "magic" is not simply an expression of awe. Supernatural properties were indeed once ascribed to these objects. The Chinese legend of *Lo Shu* features a turtle wearing the pattern of a magic 3×3 square on its shell. Floor mosaics in India may sport a certain 3×3 square, known as the *Kubera-Kolam*.

A famous specimen of measure 4×4 has been immortalised in Albrecht Dürer's engraving *Melencolia I*; see Figure 1. Not only do the rows, columns, and main diagonals sum to 34; but also the little 2×2 squares located in the corners and at the centre. (The reader can, no doubt, exhibit still more quadruples in this square adding to 34.) The art-work is unusually ripe with the exuberant symbolism of the Renaissance. For example, the middle two numbers of the bottom row of the magic square read *1514*, marking the exact year of creation. The flanking entries, 1 and 4, encode the initials of the

*Qimh Richey Xantcha, Uppsala University: qimh@math.uu.se

Figure 1: Albrecht Dürer: *Melencolia I*, 1514.

artist: *A.D.* The mathematician may be pleased to learn that the truncated rhombohedron in the background has come to be known as *Dürer's solid*, and its graph of vertices and edges as the *Dürer graph*.

There is an ever-ascending hierarchy of squares "more and more magical". For example, Euler found a magic 8×8 square, consisting of the numbers from 1 through 64 arranged in such a pattern, that the sequence of numbers, taken in order, would form a knight's tour on a chess board. One wonders how he went about finding such a miraculous construction.

We shall be concerned with squares of admittedly very low magical potential.

DEFINITION 1. — A **magic square** is a *natural* matrix whose row and column sums all equal a fixed number, called the square's **magical number** or **magical sum**.

We shall denote by $H_n(s)$ the number of $n \times n$ magic squares of sum s.

It will be the principal aim of these notes to study the properties of the functions H_n and derive explicit formulæ for low values of n.

EXAMPLE 1. — The number $H_1(s) = 1$, for clearly (s) is the only 1×1 magic square of sum s. △

EXAMPLE 2. — The number $H_n(0) = 1$, for the zero matrix is the only magic square of sum 0. △

EXAMPLE 3. — The number $H_2(1) = 2$, corresponding to

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

△

EXAMPLE 4. — Magic squares can be added, for example as in

$$\begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 4 & 1 & 2 \\ 2 & 3 & 2 \\ 1 & 3 & 3 \end{pmatrix} = \begin{pmatrix} 5 & 3 & 2 \\ 2 & 4 & 4 \\ 3 & 3 & 4 \end{pmatrix},$$

where two magic squares of sums 3 and 7, respectively, produce a magic square of sum 10. This extra structure will be exploited presently.

Compare with the definition of *classical* magic square in Problem 1.5. The much stronger property required for those squares will be destroyed under addition. △

Problems.

1. Determine the function H_2.
2. Shew that the magic squares of sum 1 are precisely the *permutation matrices*, having exactly one 1 in each row and column, and 0 for the remaining entries. Use this to compute $H_n(1)$.

3. Calculate the number $H_3(2)$.

4. Dropping the requirement that all entries be natural, allowing complex entries, the set of magic squares will then constitute a linear subspace of the space $\mathbf{C}^{n\times n}$. Verify this and calculate its dimension.

5. A **classical magic square** of order n is an $n\times n$ matrix meeting some harder prescriptions. It must contain specifically the numbers from 1 through n^2, and its rows, columns, and also *main diagonals* should sum to the same magic number.

   (a) What is the magic sum of a classical magic square of order n?

   (b) Find the number of distinct classical magic squares of orders 1, 2, and 3, up to rotation and reflexion.

   (We remark that there are 880 squares of order 4, and exactly 275, 305, 224 of order 5. There is no known formula generating these numbers. In particular, the number of classical magic 6×6 squares is currently unknown, though estimated to be at around $1.7745\cdot 10^{19}$.)

§2. — Hilbert Series

Let $A = \bigoplus_{n=0}^{\infty} A_n$ be a complex algebra, commutative, associative, unital, and graded over $\mathbf{N}$. We assume it is finitely dimensional in each degree, and also that $A_0 = \mathbf{C}$.

Modules over a graded ring are always assumed to be graded as well. That is, if $M = \bigoplus_{n=0}^{\infty} M_n$ is a module over this A, then

$$A_m M_n \subseteq M_{m+n}.$$

Definition 2. — Let $M = \bigoplus_{n=0}^{\infty} M_n$ be a module over the algebra A, finitely dimensional in each degree. Its **Hilbert series** is the formal power series

$$F_M(\lambda) = \sum_{n=0}^{\infty} (\dim M_n)\lambda^n.$$

Example 5. — Consider the module $M = \mathbf{C}[x,y]/(x^2, xy)$, which is a module over the polynomial algebra $A = \mathbf{C}[x,y]$. Its components are given by:

$$\begin{aligned} M_0 &= \langle 1 \rangle \\ M_1 &= \langle x, y \rangle \\ M_2 &= \langle y^2 \rangle \\ M_3 &= \langle y^3 \rangle \\ &\vdots \end{aligned}$$

The Hilbert series is

$$F_M(\lambda) = 1 + 2\lambda + \lambda^2 + \lambda^3 + \cdots = \lambda + \frac{1}{1-\lambda} = \frac{1+\lambda-\lambda^2}{1-\lambda}.$$

△

Let $a \in A$ be a ring element and let M be a module over A. Define the submodule

$$_aM = \{\, p \in M \mid ap = 0 \,\}.$$

LEMMA 1. — *Suppose $a \in A_m$, for some $m > 0$. Then*

$$F_M(\lambda) = \frac{F_{M/aM}(\lambda) - \lambda^m F_{aM}(\lambda)}{1-\lambda^m}.$$

Proof. For a given $n \in \mathbf{N}$, consider the homomorphism $a\colon M_{n-m} \to M_n$. By the Rank–Nullity Theorem,

$$\dim M_{n-m} = \dim \operatorname{Ker} a + \dim \operatorname{Im} a = \dim {}_aM_{n-m} + \dim(aM)_n.$$

It follows that, for any n,

$$\begin{aligned}\dim(M/aM)_n - \dim {}_aM_{n-m} &= \dim M_n/(aM)_n - (\dim M_{n-m} - \dim(aM)_n)\\ &= \dim M_n - \dim(aM)_n - \dim M_{n-m} + \dim(aM)_n\\ &= \dim M_n - \dim M_{n-m}.\end{aligned}$$

Consequently,

$$\begin{aligned}F_{M/aM}(\lambda) - \lambda^m F_{aM}(\lambda) &= \sum_{n=0}^{\infty} \dim(M/aM)_n \lambda^n - \lambda^m \sum_{n=0}^{\infty} (\dim {}_aM_n)\lambda^n\\ &= \sum_{n=0}^{\infty} (\dim(M/aM)_n - \dim {}_aM_{n-m})\lambda^n\\ &= \sum_{n=0}^{\infty} (\dim M_n - \dim M_{n-m})\lambda^n\\ &= \sum_{n=0}^{\infty} (\dim M_n)\lambda^n - \sum_{n=0}^{\infty} (\dim M_{n-m})\lambda^n = (1-\lambda^m)F_M(\lambda).\end{aligned}$$

□

EXAMPLE 6. — Let us apply the lemma to the module $\mathbf{C}[x,y]/(x^2,xy)$ with $a = y \in \mathbf{C}[x,y]$. We have

$$\begin{aligned}M/yM &= \langle 1\rangle \oplus \langle x\rangle \oplus 0 \oplus \cdots\\ {}_yM &= 0 \oplus \langle x\rangle \oplus 0 \oplus \cdots,\end{aligned}$$

and so, once more, we arrive at the formula

$$F_M(\lambda) = \frac{F_{M/yM}(\lambda) - \lambda F_{yM}(\lambda)}{1-\lambda} = \frac{(1+\lambda) - \lambda\cdot\lambda}{1-\lambda} = \frac{1+\lambda-\lambda^2}{1-\lambda}.$$

△

Theorem 1 (Hilbert). — *Let A be generated by d elements of degree 1, and let M be a module. Then*

$$F_M(\lambda) = \frac{g(\lambda)}{(1-\lambda)^d}$$

for some integral polynomial $g(\lambda)$.

Proof. If $d = 0$, then $A = \mathbf{C}$, and the assertion is true, for $F_{\mathbf{C}}(\lambda) = 1$.

Suppose now that A is generated by d elements of degree 1, among which is a. The modules ${}_aM$ and M/aM are both annihilated by a, so they are in fact modules over A/aA, which is generated by $d-1$ elements of degree 1. Hence, by induction,

$$F_{{}_aM}(\lambda) = \frac{g(\lambda)}{(1-\lambda)^{d-1}} \qquad \text{and} \qquad F_{M/aM}(\lambda) = \frac{h(\lambda)}{(1-\lambda)^{d-1}},$$

and so, by the lemma,

$$F_M(\lambda) = \frac{F_{M/aM}(\lambda) - \lambda F_{{}_aM}(\lambda)}{1-\lambda} = \frac{h(\lambda) - \lambda g(\lambda)}{(1-\lambda)^d}.$$

□

Theorem 2. — *Let A be generated by $d \geqslant 1$ elements of degree 1. For all sufficiently large n, the function*

$$n \mapsto \dim M_n$$

is a rational polynomial of degree at most $d-1$. It is called the ***Hilbert polynomial*** *of M.*

Proof. $\dim M_n$ is the co-efficient of λ^n in $\frac{g(\lambda)}{(1-\lambda)^d}$. Let $g(\lambda) = \sum_{j=0}^{m} a_j \lambda^j$. Since

$$\frac{1}{(1-\lambda)^d} = \sum_{j=0}^{\infty} \binom{d+j-1}{d-1} \lambda^j,$$

we have

$$\dim M_n = \sum_{j=0}^{m} a_j \binom{d+n-j-1}{d-1}$$

for all $n \geqslant m$, which is a polynomial in n of degree at most $d-1$. □

Example 7. — The Hilbert polynomial of the module $M = \mathbf{C}[x,y]/(x^2, xy)$ is the constant function 1. △

Problems.

1. Calculate the Hilbert series and Hilbert polynomial of the polynomial ring $\mathbf{C}[x]$.
2. Calculate the Hilbert series and Hilbert polynomial of the polynomial ring $\mathbf{C}[x, y]$.
3. Suppose a module has Hilbert series equal to the polynomial $h(\lambda)$. What is its Hilbert polynomial?
4. If N is a submodule of M, shew that
$$F_M = F_N + F_{M/N}.$$
5. Develop formulæ for the Hilbert series of the direct sum $M \oplus N$ and tensor product $M \otimes N$ of two modules M and N.

§3. — Linear Diophantine Systems of Equations

Consider an $n \times n$ matrix $X = (x_{pq})$ of natural numbers. The condition for X to be a magic square amounts to the following system of equations:

$$\sum_i x_{i1} = \sum_i x_{iq} = \sum_j x_{pj}, \quad 1 \leqslant p, q \leqslant n.$$

The proper context is therefore as follows. Let D be an integral matrix with k rows. We are seeking *natural solutions* to the linear system of equations

$$DX = 0. \tag{1}$$

Theorem 3. — *The solutions $X \in \mathbf{N}^k$ to the linear system (1) form a commutative monoid.*

Proof. 0 is a solution, and if X and Y are solutions, then so is $X + Y$. □

Definition 3. — A non-zero solution is said to be **fundamental** if it cannot be written as the sum of two non-zero solutions.

It is said to be **completely fundamental** if no natural multiple of it can be written as the sum of two non-zero, non-parallel solutions.

Example 8. — Consider the system

$$\begin{pmatrix} 1 & 1 & -2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0$$

and the three solutions $(2, 0, 1)$, $(0, 2, 1)$, and $(1, 1, 1)$. All three are fundamental, but only the first two are completely fundamental, for

$$2(1, 1, 1) = (2, 0, 1) + (0, 2, 1).$$

△

THEOREM 4 (HILBERT). — *There are only finitely many fundamental solutions, and every non-trivial solution is a positive integral combination of such.*

Proof. It is clear that any solution can be written as a positive integer combination of fundamental solutions — just reduce a given solution until no longer possible.

We now shew the number of fundamental solutions is finite. Consider first the case of a *single* equation, which we opt to write as

$$a_1x_1 + \cdots + a_mx_m = b_1y_1 + \cdots + b_ny_n,$$

where all the numbers a_i and b_i are positive, and, as always, we seek *natural* solutions.

Suppose $y_i > a_1 + \cdots + a_m$. Then

$$a_1x_1 + \cdots + a_mx_m = b_1y_1 + \cdots + b_ny_n > b_i(a_1 + \cdots + a_m),$$

so that

$$a_1(x_1 - b_i) + \cdots + a_m(x_m - b_i) > 0.$$

It follows that some $x_j > b_i$. But if $x_j > b_i$ and $y_i \geqslant a_j$, then the solution cannot be fundamental, for the solution $(x_j, y_i) = (b_i, a_j)$ (all other letters equal to 0) may be deducted from it.

Consequently, in a fundamental solution, all variables $y_i \leqslant a_1 + \cdots + a_m$, and similarly all $x_j \leqslant b_1 + \cdots + b_n$, and there can only be finitely many.

Suppose now that there are *two* equations. Write the solutions to the first one as a natural combination of its fundamental solutions (which we know are finitely many), with variable co-efficients. Substituting this expression into the second equation will yield a new integral equation in these co-efficients, of which, by the argument just produced, has a finite number of fundamental solutions.

This procedure may be repeated for any given number of equations. □

THEOREM 5. — *There are only finitely many completely fundamental solutions, and every non-trivial solution is a positive rational combination of such.*

Proof. Since every completely fundamental solution is fundamental, their number must also be finite.

Let the fundamental solutions be $Q_1, \ldots, Q_k$. Then every solution can be written as a positive rational (in fact, positive integral) combination of these.

Suppose that Q_k is not completely fundamental. We shall shew that some positive multiple of Q_k can be expressed as a positive rational combination of $Q_1, \ldots, Q_{k-1}$. Since Q_k is not completely fundamental, there exists an $m \in \mathbf{Z}^+$ such that

$$mQ_k = (a_1Q_1 + \cdots + a_{k-1}Q_{k-1} + a_kQ_k) + (b_1Q_1 + \cdots + b_{k-1}Q_{k-1} + b_kQ_k),$$

where some a_i or some b_j is non-zero, for $1 \leqslant i,j \leqslant k-1$. All co-efficients are rational and non-negative. Collecting the terms containing Q_k on one side of the equality yields:

$$m'Q_k = (a_1Q_1 + \cdots + a_{k-1}Q_{k-1}) + (b_1Q_1 + \cdots + b_{k-1}Q_{k-1}).$$

If $m' \leqslant 0$, there is a contradiction, for the right-hand side is certainly positive. Hence $m' > 0$, and we are done. A positive multiple of Q_k, and therefore of any solution, can be written as a positive combination of $Q_1, \ldots, Q_{k-1}$ only.

Suppose now that Q_{k-1} is not completely fundamental either. Then there exists a positive integer n such that

$$nQ_{k-1} = (a_1Q_1 + \cdots + a_{k-2}Q_{k-2} + a_{k-1}Q_{k-1}) + (b_1Q_1 + \cdots + b_{k-2}Q_{k-2} + b_{k-1}Q_{k-1}),$$

where some a_i or some b_j are non-zero, for $1 \leqslant i,j \leqslant k-2$. This yields

$$n'Q_{k-1} = (a_1Q_1 + \cdots + a_{k-2}Q_{k-2}) + (b_1Q_1 + \cdots + b_{k-2}Q_{k-2}),$$

and again $n' > 0$.

Repeat this procedure until only completely fundamental solutions remain. □

EXAMPLE 9. — As an illustration of the technique, let us solve the system

$$\begin{cases} x - 2z + w &= 0 \\ y - 2z - w &= 0 \end{cases}$$

in accordance with the proof of Theorem 4.

The first equation is easily seen to have the four fundamental solutions

$$(x,y,z,w) = (2,0,1,0),\ (0,0,1,2),\ (1,0,1,1),\ (0,1,0,0)$$

and the general solution to this equation may be accordingly written

$$(x,y,z,w) = (2p + r, s, p + q + r, 2q + r), \quad p,q,r,s \in \mathbf{N}. \tag{2}$$

Substitution of this into the second equation yields

$$0 = y - 2z - w = s - 2(p + q + r) - (2q + r) = -2p - 4q - 3r + s,$$

so that $s = 2p + 4q + 3r$. Substituting back into (2) then yields the solution to the system:

$$(x,y,z,w) = (2p + r, 2p + 4q + 3r, p + q + r, 2q + r).$$

The three generating solutions are

$$P = (2,2,1,0), \quad Q = (0,4,1,2), \quad R = (1,3,1,1).$$

It will be observed that they are all fundamental, but, since $P + Q = 2R$, only P and Q are completely fundamental. △

Problems.

1. Solve, in natural numbers, the diophantine system of equations

$$\begin{cases} 2x + 3y - z - w &= 0 \\ x - y - z + w &= 0. \end{cases}$$

   What are the fundamental solutions?

2. What is the number of fundamental solutions of the equation

$$a_1x_1 + \cdots + a_nx_n - 2y = 0,$$

   where each $a_j \in \mathbf{Z}^+$?

§4. — The Generating Function of a System of Equations

The objective is, as before, to study the natural solutions $X \in \mathbf{N}^k$ of the system of equations $DX = 0$. These solutions form a commutative monoid, which we denote by S.

Suppose that $R_1, \ldots, R_q$ are solutions, and form the polynomial ring

$$A = \mathbf{C}[x_1, \ldots, x_q]$$

in q indeterminates. The polynomial ring A is **graded by the monoid** S, whereby we define $\deg x_j = R_j$. This amounts to the following. The ring

$$A = \bigoplus_{P \in S} A_P$$

splits up into graded components

$$A_P = \left\langle x_1^{m_1} \cdots x_q^{m_q} \,\middle|\, m_1R_1 + \cdots + m_qR_q = P \right\rangle, \quad P \in S;$$

and $A_PA_Q \subseteq A_{P+Q}$.

Example 10. — Continuing the previous example, consider the three (fundamental) solutions

$$P = (2, 2, 1, 0), \qquad Q = (0, 4, 1, 2), \qquad \text{and} \qquad R = (1, 3, 1, 1),$$

and form the polynomial ring $A = \mathbf{C}[x, y, z]$. We have, for example,

$$\begin{aligned} \deg 1 &= 0 = (0, 0, 0, 0) \\ \deg x &= P = (2, 2, 1, 0) \\ \deg y &= Q = (0, 4, 1, 2) \\ \deg z &= R = (1, 3, 1, 1) \\ \deg x^2y &= 2P + Q = (4, 8, 3, 2). \end{aligned}$$

The graded components of A may be 0-, 1-, or 2-dimensional:

$$\begin{aligned} A_{(0,0,0,0)} &= \langle 1 \rangle \\ A_{(1,0,0,0)} &= 0 \\ A_{(2,2,1,0)} &= \langle x \rangle \\ A_{(2,6,2,2)} &= \langle xy, z^2 \rangle . \end{aligned}$$

△

Next, define a module M over A as follows. As a vector space, M has a complex basis consisting of all the elements of the monoid S (that is to say: all the natural solutions to the system $DX = 0$):

$$M = \mathbf{C}S = \langle [P] \mid P \in S \rangle .$$

The action of A on M is given by

$$x_j \cdot [P] = [R_j + P].$$

Defining the graded components of M to be 1-dimensional,

$$M_P = \langle [P] \rangle , \quad P \in S;$$

it is easily verified that $A_P M_Q \subseteq M_{P+Q}$; i. e. M is a graded module over A.

Theorem 6. — *If $R_1, \ldots, R_q$ include the completely fundamental solutions, the module M is finitely generated.*

Proof. Suppose $R_1, \ldots, R_q$ are completely fundamental, and consider the finitely many fundamental solutions $Q_1, \ldots, Q_k$. To each Q_j there is an m_j such that $m_j Q_j$ is a natural combination of the completely fundamental solutions. Then M is generated by the $m_1 \cdots m_q$ elements

$$[a_1 Q_1 + \cdots + a_k Q_k] , \quad 0 \leqslant a_j < m_j.$$

For suppose $w \in M$. Then $w = c_1 Q_1 + \cdots + c_k Q_k$. Writing

$$c_j = g_j m_j + a_j, \quad g_j \in \mathbf{N},\ 0 \leqslant a_j < m_j$$

gives

$$w = \sum_j g_j m_j Q_j + \sum_j a_j Q_j.$$

Since $m_j Q_j$ is a natural combination of the completely fundamental solutions, we have

$$w = \sum_i h_i R_i + \sum_j a_j Q_j$$

for some natural numbers h_i. Consequently,

$$[w] = \prod_i x_i^{h_i} \left[\sum_j a_j Q_j \right] .$$

□

Definition 4. — The **generating function** of the system $DX = 0$, is the formal power series

$$f(\lambda_1, \dots, \lambda_k) = \sum_P (\dim M_P)\lambda^P = \sum_{P \in S} \lambda^P = \sum_{(p_1, \dots, p_k) \in S} \lambda_1^{p_1} \cdots \lambda_k^{p_k}.$$

Example 11. — Continuing the previous example, the generating function is

$$\begin{aligned} f(\lambda_1, \lambda_2, \lambda_3, \lambda_4) &= 1 + \lambda_1^2\lambda_2^2\lambda_3 + \lambda_2^4\lambda_3\lambda_4^2 + \lambda_1\lambda_2^3\lambda_3\lambda_4 + \cdots \\ &= 1 + \lambda^P + \lambda^Q + \lambda^R + \cdots \\ &= (1 + \lambda^P + \lambda^{2P} + \cdots)(1 + \lambda^Q + \lambda^{2Q} + \cdots)(1 + \lambda^R) \\ &= \frac{1 + \lambda^R}{(1 - \lambda^P)(1 - \lambda^Q)}. \end{aligned}$$

This is no accident, as shewn by the subsequent theorem. △

Theorem 7 (Stanley). — *The generating function f is a rational function, which, when reduced to lowest terms, is of the form*

$$f(\lambda) = \frac{g(\lambda)}{(1 - \lambda^{R_1}) \cdots (1 - \lambda^{R_q})},$$

where g is an integral polynomial and $R_1, \dots, R_q$ are the completely fundamental solutions.

Proof. When $R_1, \dots, R_q$ are the completely fundamental solutions, the module M is finitely generated, and so we may use Hilbert's Syzygy Theorem to produce a free resolution:

$$0 \longrightarrow F^q \longrightarrow F^{q-1} \longrightarrow \cdots \longrightarrow F^1 \longrightarrow F^0 \longrightarrow M \longrightarrow 0.$$

This sequence splits over the graded components into free resolutions:

$$0 \longrightarrow F_P^q \longrightarrow F_P^{q-1} \longrightarrow \cdots \longrightarrow F_P^1 \longrightarrow F_P^0 \longrightarrow M_P \longrightarrow 0$$

for each $P \in S$. By a well-known property of such sequences,

$$\dim M_P = \dim F_P^0 - \dim F_P^1 + \cdots.$$

Multiplying by λ^P and summing yields

$$f(\lambda) = f^0(\lambda) - f^1(\lambda) + \cdots.$$

Suppose now F^p has free, homogeneous generators $y_1, \dots, y_j$. Then F_P^p has a complex basis consisting of all elements

$$x_1^{a_1} \cdots x_q^{a_q} y_i, \qquad \text{where} \qquad a_1R_1 + \cdots + a_qR_q + \deg y_i = P.$$

Consequently,

$$f^p(\lambda) = \sum_{a_1,\ldots,a_q=0}^{\infty} \sum_{i=1}^{k} \lambda^{a_1R_1+\cdots+a_qR_q+\deg y_i} = \frac{\sum_{i=1}^{k} \lambda^{\deg y_i}}{(1-\lambda^{R_1})\cdots(1-\lambda^{R_q})},$$

and so f itself must be of the desired form.

It remains to prove that the true denominator of f cannot be a proper factor of the one given. By Problem 3 below, each polynomial $1-\lambda^{R_j}$ is irreducible. Hence it will suffice to shew f cannot be written in the form

$$f(\lambda) = \frac{g(\lambda)}{\prod_{j\neq l}(1-\lambda^{R_j})}.$$

Suppose it can. For any $r \in \mathbf{N}$, the term λ^{rR_l} must appear in the numerator $p(\lambda)$, because $rR_l \in S$ and so must appear in the generating function. Hence, there is some term λ^U in the numerator $g(\lambda)$ and natural numbers b_j such that

$$U + \sum_{j\neq l} b_j R_j = rR_l.$$

Since U is a vector of natural numbers and all $R_j \in S$, also $U \in S$. From the fact that all R_j are completely fundamental solutions, it follows that $\sum_{j\neq l} b_j R_j = 0$, so $U = rR_l$. Having thus established that $\lambda^{rR_l} = \lambda^U$ occurs in the numerator $g(\lambda)$ for all $r \in \mathbf{N}$, we conclude that g cannot be a polynomial, but a proper series. This contradiction finishes the proof. □

Problems.

1. Return to Example 10.
   (a) Find more examples of graded components of A having dimensions 0, 1, and 2, respectively.
   (b) Do there exist components of A having dimensions greater than 2?
2. Shew that the generating function f of M may be viewed as a more finely graded version of the Hilbert series, in the sense that putting $\lambda_1 = \cdots = \lambda_k$ yields the Hilbert series.
3. In the notation of the proof of Theorem 7, shew that each factor $1-\lambda^R$ is irreducible as long as R is a (completely) fundamental solution.
4. Find a criterion for M to be *cyclic*, that is, generated by a single element (which one?).
5. Prove the following converse to Theorem 6: If M is finitely generated, one can, among the R_j, find multiples of all the completely fundamental solutions.

§5. — The Fundamental Magic Squares

Let G be a graph with vertices $V(G)$ and edges $E(G)$. When A is a set of vertices, denote by $N(A)$ the set of neighbours of A, that is,

$$N(A) = \{\, v \in V(G) \mid \exists u \in A : uv \in E(G) \,\}.$$

Suppose now that G is *bipartite*, so that the vertices of G split up into two vertex sets U and V, with all edges running between these two sets.

Definition 5. — Assuming $|U| = |V|$, a **perfect matching** for G is a bijection $\mu\colon U \to V$ such that $u\mu(u) \in E(G)$ for all $u \in U$.

Theorem 8: Hall's Marriage Theorem. — *G possesses a perfect matching if and only if, for all $X \subseteq U$,*

$$|N(X)| \geqslant |X|. \tag{3}$$

Proof. The condition is clearly necessary. To shew sufficiency, we proceed by induction on $n = |U| = |V|$. The case $n = 1$ is trivial.

Case 1: For all $A \subset U$, one has $|N(A)| \geqslant |A| + 1$. Choose any $u \in U$. Since $|N(u)| \geqslant |\{u\}| = 1$, the set $N(u)$ is non-empty, and we choose a neighbour $v \in N(u)$. The rest of the graph, $G\backslash\{u, v\}$, is a smaller bipartite graph that will still satisfy condition (3). Induction yields the result.

Case 2: There is some $A \subset U$ such that $|N(A)| = |A|$. Consider the following two induced, non-empty, bipartite subgraphs of G:

$$H = A \cup N(A) \qquad \text{and} \qquad K = (U\backslash A) \cup (V\backslash N(A)).$$

For any set $X \subseteq A$, we have $N_H(X) = N_G(X)$, so the graph H will satisfy condition (3). As for K, assume $X \subseteq U\backslash A$. The equation

$$N_G(X \cup A) = N_K(X) \cup N_G(A)$$

shews that

$$|X| + |A| = |X \cup A| \leqslant |N_G(X \cup A)| = |N_K(X)| + |N_G(A)| = |N_K(X)| + |A|.$$

Consequently, the graph K also satisfies the condition (3). Since the graphs H and K are both smaller than G, we may conclude by induction. □

Theorem 9: The Birkhoff–von Neumann Theorem. — *A magic square of magic sum s is the sum of s permutation matrices.*

Proof. Consider an $n \times n$ magic square Q. If $Q = 0$, it is an empty sum of permutation matrices, so suppose $Q \neq 0$. In keeping with the above notation, construct a bipartite graph G by letting $U = V = [n]$, and including the edge uv in G if and only if $Q_{uv} > 0$. We leave it to the reader to verify that G fulfils condition (3), and so we can apply Hall's Marriage Theorem to find a perfect matching $\mu\colon U \to V$. This permutation μ satisfies $Q_{u\mu(u)} > 0$ for all $u \in [n]$, and so the matrix $Q - \mu$ still has natural entries and will still be magic, of magic sum decreased by 1. We may then repeat the procedure until the zero matrix is attained. □

Theorem 10. — *The following conditions on a magic square Q are equivalent:*

A. Q is fundamental.

B. Q is completely fundamental.

C. Q is a permutation matrix.

Proof. C implies B is clear, for a multiple of a permutation matrix, of minimal magic sum 1, cannot be written as the sum of other magic squares. Also, B implies A is clear, for a completely fundamental solution is of course fundamental. That A implies C follows from the Birkhoff–von Neumann Theorem. □

Problems.

1. Write the matrix
$$\begin{pmatrix} 4 & 1 & 2 \\ 2 & 3 & 2 \\ 1 & 3 & 3 \end{pmatrix}$$
as the sum of permutation matrices. Can this be done in more than one way?

2. Give an application to real life that would motivate the name Marriage Theorem!

3. Subdivide a standard deck of cards into thirteen piles, containing four cards each. Shew that it is possible to choose one card from each pile, so that, among the thirteen cards chosen, all the ranks from ace to king be represented.

4. Complete the proof of the Birkhoff–von Neumann Theorem, by verifying that the graph G indeed satisfies the condition of Hall's Marriage Theorem.

5. Shew that magic squares can be multiplied, and the result will again be magical. What is the magic sum of the product?

§6. — Counting Magic Squares

Once more, we turn our attention towards

$$\mathbf{C}S = \langle [P] \mid P \in S \rangle,$$

though this time considered, not as a module, but rather as a ring in its own right. Multiplication is given by the formula

$$[P] \cdot [Q] = [P + Q]$$

and the ring is **N**-graded by magic sum.

It is almost uncanny what a simple inspection of this ring will yield. We implore the reader to examine carefully the first three lines of the subsequent proof. Four lines only — in order to reach such a strong and triumphant conclusion! Surely this will convince the reader (if he were not already a holder of this conviction) of the power and glory of Abstract Algebra?

THEOREM 11. — *The function H_n is a rational polynomial.*

Proof. The ring $\mathbf{C}S$ is generated by elements of degree (magic sum) 1, viz. the permutation matrices. The dimension $\dim(\mathbf{C}S)_s$ counts the number of magic squares of sum s, and so an immediate application of Theorem 2 yields that $H_n(s)$ agrees with a polynomial for sufficiently large values of s.

To prove that H_n co-incides with this polynomial function *everywhere*, some detailed analysis of the generating function will be required. Stanley's original proof is given in [4]. □

THEOREM 12. — *The degree of H_n is exactly $(n-1)^2$.*

Proof. Consider a magic square $Q = (q_{ij})$ of sum s. Each entry $0 \leqslant q_{ij} \leqslant s$, and if q_{ij} is specified for all $1 \leqslant i,j \leqslant n-1$, then the remaining entries are uniquely determined. This shews that

$$H_n(s) \leqslant (s+1)^{(n-1)^2},$$

and so the degree of H_n cannot exceed $(n-1)^2$.

On the other hand, after arbitrarily choosing natural numbers

$$\frac{(n-2)s}{(n-1)^2} \leqslant q_{ij} \leqslant \frac{s}{n-1}, \quad 1 \leqslant i,j \leqslant n-1;$$

the remaining entries (found by enforcing the magical property) are forced to be natural. Hence

$$H_n(s) \geqslant \left(\frac{s}{n-1} - \frac{(n-2)s}{(n-1)^2} - 1\right)^{(n-1)^2} = \left(\frac{s}{(n-1)^2} - 1\right)^{(n-1)^2},$$

so that the degree of H_n must be exactly $(n-1)^2$. □

We record one auxiliary result before we put the finishing touch.

THEOREM 13: POPOVICIU'S THEOREM ([3]). — *Let $h(s)$ be a complex polynomial. Define*

$$F(\lambda) = \sum_{s=0}^{\infty} h(s)\lambda^s \qquad \text{and} \qquad \tilde{F}(\lambda) = \sum_{s=1}^{\infty} h(-s)\lambda^s.$$

There is an equality of rational functions:

$$F(\lambda) = -\tilde{F}(\lambda^{-1}).$$

Proof.

$$\begin{aligned} F(\lambda) + \tilde{F}(\lambda^{-1}) &= \sum_{s=0}^{\infty} h(s)\lambda^s + \sum_{s=1}^{\infty} h(-s)\lambda^{-s} \\ &= \sum_{s=0}^{\infty} h(s)\lambda^s + \sum_{s=-\infty}^{-1} h(s)\lambda^s = \sum_{s=-\infty}^{\infty} h(s)\lambda^s. \end{aligned}$$

The equality of the theorem will be established once we have shewn that

$$\sum_{s=-\infty}^{\infty} s^m \lambda^s = 0$$

for all $m \in \mathbf{N}$. We proceed inductively. The equality is true for $m = 0$, for

$$\sum_{s=-\infty}^{\infty} \lambda^s = \sum_{s=0}^{\infty} \lambda^s + \sum_{s=1}^{\infty} \lambda^{-s} = \frac{1}{1-\lambda} + \frac{\lambda^{-1}}{1-\lambda^{-1}} = 0.$$

Differentiating this equation with respect to λ yields

$$\sum_{s=-\infty}^{\infty} s\lambda^s = \sum_{s=-\infty}^{\infty} (s+1)\lambda^s = \sum_{s=-\infty}^{\infty} s\lambda^{s-1} = 0,$$

and so forth. □

The *Gorenstein* property is a pleasant property for rings to possess, and the notion is ubiquitous in Commutative Algebra. A precise definition is unfortunately beyond the scope of these notes, and we shall content ourselves with recording the following facts:

1. The ring $\mathbf{C}S$ has the Gorenstein property and is of Krull dimension n. This was essentially proven by Hochster in [2].
2. When R is a Gorenstein ring of Krull dimension n, there is an integer g such that
   $$F_R(\lambda^{-1}) = (-1)^n \lambda^g F_R(\lambda).$$
   This was proven by Stanley in [5].
3. For the ring $\mathbf{C}S$, the number $g = n$. There is a vague attempt at an explanation in [6], which, unfortunately, makes no effort to trace the origins of this illation.

Theorem 14. — *The polynomial H_n has the following properties, for all $s \in \mathbf{C}$:*

$$H_n(-1) = H_n(-2) = \cdots = H_n(-(n-1)) = 0$$

and

$$H_n(-(n+s)) = (-1)^{n-1} H_n(s).$$

Proof. By the enumerated list above and Popoviciu's Theorem, the Hilbert series $F(\lambda) = \sum_{s=0}^{\infty} H_n(s)\lambda^s$ of the ring $\mathbf{C}S$ fulfils

$$\sum_{s=1}^{\infty} H_n(-s)\lambda^s = \tilde{F}(\lambda) = -F(\lambda^{-1}) = (-1)^{n-1}\lambda^n F(\lambda) = (-1)^{n-1}\lambda^n \sum_{s=0}^{\infty} H_n(s)\lambda^s,$$

from which the theorem follows. □

EXAMPLE 12. — The function H_2 has degree 1 and satisfies $H_2(-1) = 0$ (from the theorem) and $H_2(0) = 1$ (easy). Hence it must be given by the formula

$$H_2(s) = 1 + s,$$

which was established by elementary means in an exercise. △

Problems.

1. Determine H_3.
2. Considering the information jointly provided by the above theorems, what is the minimum value of p, for which knowledge of the quantities $H_n(0), \ldots, H_n(p)$ will suffice in order to deduce the polynomial H_n?
3. Give an algebraical proof that $\deg H_n = (n-1)^2$ along the following lines.
   (a) Shew that, if the space of all complex solutions to $DX = 0$ has dimension d, then the denominator of the Hilbert series $\sum(\dim M_m)\lambda^m$, when reduced to lowest terms, is $(1-\lambda)^d$.
   (b) Shew that this implies that the function $m \mapsto \dim M_m$ is polynomial of degree $d-1$.
   (c) Now use Problem 1.4 to conclude the proof.

REFERENCES

[1] David Hilbert: *Ueber die Theorie der algebraischen Formen*, MATHEMATISCHE ANNALEN Vol. 36, 1890.

[2] M. Hochster: *Rings of invariants of tori, Cohen–Macaulay rings generated by monomials, and polytopes*, ANNALS OF MATHEMATICS 96, 1972.

[3] T. Popoviciu: *Studie şi cercetari ştiintifice*, ACAD. R.P.R. FILIALA CLUJ 4, 1953.

[4] Richard P. Stanley: *Linear Homogeneous Diophantine Equations and Magic Labelings of Graphs*, DUKE MATHEMATICAL JOURNAL 40, 1973.

[5] Richard P. Stanley: *Hilbert Functions of Graded Algebras*, ADVANCES IN MATHEMATICS 28, 1978.

[6] Richard P. Stanley: *An Introduction to Combinatorial Commutative Algebra*, in *Enumeration and Design* (D. Jackson and S. Vanstone, eds.), Academic Press 1984.

Hints and Answers to Problems

1.1. $H_2(s) = 1 + s$.

1.2. $H_n(1) = n!$.

1.3. $H_3(2) = 21$.

1.4. The dimension is $n^2 - 2n + 2$.

1.5. (a) The magic sum is $\frac{n(n^2+1)}{2}$.
(b) The number of classical magic squares of order 1, 2, 3 is 1, 0, 1, respectively. For the case 3×3, begin by shewing the central entry has to be 5.

2.1. $\frac{1}{1-\lambda}$ and 1, respectively.

2.2. $\frac{1}{(1-\lambda)^2}$ and $1 + n$, respectively.

2.3. 0. The module contains only a finite number of non-zero graded components.

2.4. —

2.5. $F_{M\oplus N} = F_M + F_N$ and $F_{M\otimes N} = F_M \cdot F_N$.

3.1. The fundamental solutions are $(2, 0, 3, 1)$ and $(0, 1, 1, 2)$. The system is most easily solved by starting with the second equation.

3.2. There are exactly $n + \frac{k(k-1)}{2}$ fundamental solutions to the equation, where k is the number of odd a's.

4.1. (a) —
(b) Yes, for instance: $A_{(4,12,4,4)} = \langle x^2y^2, xyz^2, z^4\rangle$.

4.2. —

4.3. Consider the special case of a single variable. A polynomial $1 - x^r$ can only reduce as

$$1 - x^{pq} = (1 + x^q + x^{2q} + \cdots + x^{(p-1)q})(1 - x^q),$$

where $r = pq$.

4.4. M is generated by [0] if and only if $R_1, \ldots, R_q$ include all the fundamental solutions.

4.5. The generators of M may be taken to be of the pure form $[Q]$. Given an element $[P] \in M$, express $[nP]$, for any $n \in \mathbf{N}$, in the generators $[Q]$, and use the fact that there are only finitely many $[Q]$ to shew that some nP can be written as a linear combination of these generators. Then consider what happens when P is completely fundamental.

5.1. Yes, it can.

5.2. —

5.3. Let U be the set of piles and V be the set of values.

5.4. —

5.5. Deploy the Birkhoff–von Neumann Theorem. The magic sum of a product is the product of magic sums.

6.1. $H_3(s) = \frac{(s+1)(s+2)(s^2+3s+4)}{8}$.

6.2. $p = \frac{(n-1)(n-2)}{2}$.

6.3. —