Lattices, Linear Codes, and Invariants, Part II

Noam D. Elkies

In Part I of this article we introduced "lattices" $L \subset \mathbb{R}^n$ and described some of their relations with other branches of mathematics, focusing on "theta functions". Those ideas have a natural combinatorial analogue in the theory of "linear codes". This theory, though much more recent than the study of lattices, is more accessible, and its numerous applications include the construction and analysis of many important lattices.

A lattice L is a special kind of subgroup of the additive group $\mathbb{R}^n$; in Part I we associated to L a theta function, which is a generating function for the lengths of the vectors of L. A linear code C, to be defined below, is a subgroup of a finite additive group F^n. Analogous to the theta functions of lattices are "weight enumerators" of codes, which are generating functions for the coordinates of elements of C. We shall see how most of the uses and properties of theta functions that we described in Part I have counterparts in the setting of weight enumerators. In particular, just as the theta function $\theta_L(\tau)$ associated to a "self-dual lattice" L is invariant under certain fractional linear transformations of the variable τ, we shall encounter "self-dual codes" C with weight enumerators invariant under certain linear transformations of the variables. This invariance yields much information about C, and about an associated self-dual lattice L_C and its theta function.

Noam D. Elkies is professor of mathematics at Harvard University. His e-mail address is elkies@math.harvard.edu.

Part I of this article—concerning lattices, lattice packings of spheres, theta functions, and modular forms—appeared in the November 2000 issue of the Notices, *pages 1238–1245.*

As was true of Part I, there is little if any of the mathematics described herein for whose discovery I can claim credit. The one possible exception is the use of theta functions near the end to relate the occurrences of the groups $SL_2(\mathbb{Z}/p\mathbb{Z})$ and $SL_2(\mathbb{Z})$ in the functional equations for weight enumerators and lattices respectively; I know of no published statement of this observation, though it may well be common knowledge in some circles. All other results and ideas I have attributed when their source is known to me, and I apologize in advance for any mis- or missing attribution.

Sphere Packing in Hamming Space: Error-correcting Codes

Most of the problems and ideas concerning sphere packing have natural, and often more tractable, discrete analogues in the theory of error-correcting codes (ECCs). Though easier in many ways than the sphere-packing problem, the theory of ECCs is much more recent: its systematic development began only with R. W. Hamming's 1947 paper.[1] In our digital age, ECCs are ubiquitous wherever there is information to reliably store or transmit; applications range from the familiar compact disc in one's computer or stereo to close-up photographs of Jovian moons sent back to Earth with a transmitter too weak to power a lightbulb. The theoretical study of ECCs has also led to surprisingly varied and deep mathematics, including for instance orthogonal polynomials and arithmetic algebraic geometry. In the present exposition we concentrate on the connections with sphere packings, particularly as regards theta functions and their discrete analogues.

[1] *Hamming's work is discussed in the memorial article about him in the September 1998* Notices.

To see ECCs as discrete sphere packings, we must specify the metric space containing our spheres. The space will be F^n, i.e., the set of ordered n-tuples of elements of a finite set F, for some choice of F and n. In the ECC context, such n-tuples are often called *words* of *length* n, with *letters* drawn from an *alphabet* F. To assure that $|F^n| > 1$ (so that a word contains some information), we assume $|F| > 1$ and $n > 0$. The set F^n itself is called *Hamming space* and is given a metric structure by the *Hamming distance* $d(\cdot, \cdot)$ defined thus: The distance between words $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ is

$$d(a, b) := \#\{i \mid 1 \le i \le n,\ a_i \ne b_i\}.$$

That is, $d(a, b)$ is the number of single-letter changes ("errors") one must make to get from a to b. A *code* is then just a nonempty subset $C \subseteq F^n$. The *minimal (nonzero) distance* of a code is

$$\delta(C) := \min_{\substack{a,b \in C \\ a \ne b}} d(a, b).$$

In the degenerate case $|C| = 1$, we set $\delta(C) = n + 1$.

In the standard application to error-resistant data storage or transmission, the words that can be stored or transmitted are those in C, rather than arbitrary words in F^n. A code C with minimal distance δ is then said to *detect* $\delta - 1$ errors, and to *correct* $\lfloor (\delta - 1)/2 \rfloor$ errors. This is because if some information is stored or sent as a word of C, and this word is changed in at most $\delta - 1$ coordinates, the resulting word cannot be in C, and thus cannot be the word originally intended; moreover, if at most $\lfloor (\delta - 1)/2 \rfloor$ letters were changed, then the original word is still uniquely determined, else by the triangle inequality C would contain two words at distance at most $\delta - 1$. Equivalently, an e-error-correcting code is a code C such that the (closed) *Hamming spheres* $\overline{B}_e(a) := \{x \in F^n \mid d(a, x) \le e\}$ of common radius e about the codewords $a \in C$ are pairwise disjoint. Such a code detects $2e$ errors and has minimal distance at least $2e + 1$.

The basic problem of error-correcting codes is: *what is the maximum size of a code* if its length, the size of the alphabet, and a lower bound on the minimal distance are given? That is, how efficiently can we encode information while detecting or correcting a given number of errors? This is also a natural mathematical problem, asking how many points can be packed into F^n without any two coming closer than δ to each other. Naturally, the smaller δ is, the larger C can get, and conversely. At the extreme ends are $C = F^n$ itself (maximal efficiency but no error correction), and $|C| = 1$ (maximal δ but no information). Other simple examples are the *repetition code*, consisting of the $|F|$ words all of whose letters are the same (with $\delta = n$), and the *parity check code*, for which F is $\{0, 1\}$ and C consists of the 2^{n-1} words a with an even number of 1's (equivalently, such that $\sum_{i=1}^{n} a_i$ is even; here $\delta = 2$). A more interesting example is the *extended Hamming code* H_8, in which $F = \{0, 1\}$ again, $n = 8$, and H_8 consists of the words

00000000, 00001111, 00110011, 00111100,
01010101, 01011010, 01100110, 01101001,

and their ones' complements

11111111, 11110000, 11001100, 11000011,
10101010, 10100101, 10011001, 10010110.

Thus $|H_8| = 16$, and one may check that $\delta = 4$. All these codes are known to have maximal size for their respective F, n, and δ. We shall again encounter each of these important codes, and especially H_8, several times.

Linear Codes

The discrete analogue of a lattice is a *linear code*. A linear code is a vector subspace of Hamming space F^n. For F^n to have the structure of a vector space, F must be a (finite) *field*, such as $\mathbb{Z}/p\mathbb{Z}$ for some prime p.[2] For instance, if in the previous paragraph F is always chosen to be a field (so that in particular $\{0, 1\}$ is identified with $\mathbb{Z}/2\mathbb{Z}$), and $\{\mathbf{0}\}$ is chosen for the single-word code, then each of the codes in that paragraph is linear. Henceforth F will denote a finite field.

The powerful framework of linear algebra makes it possible to work with codes much larger than would be accessible otherwise, since a linear code of size $|F|^k$ can be specified by only k basis words. The minimal distance δ also simplifies somewhat: for any $a, b \in F^n$, we have $d(a, b) = d(a - b, 0)$; if a, b are in a linear code, then so is $a - b$, whence δ is the minimum of $d(c, 0)$ over all nonzero $c \in C$. For any $c \in F^n$, the distance $d(c, 0)$ is the number of nonzero coordinates of c, a number known as the *Hamming weight* of c and denoted by $\mathrm{wt}(c)$. Thus for a linear code δ is the *minimum* (nonzero Hamming) *weight*. The basic problem for linear ECCs thus becomes: *what is the maximum dimension of a linear code* if its length, the size of the alphabet, and a lower bound on the minimum weight are given?

As is the case for sphere packings, for most values of $(|F|, n, \delta)$ one cannot at present hope to solve the problem exactly or even asymptotically, only to give upper and lower bounds. Many of the bounds for codes are analogous to sphere-packing

[2] *It is a fundamental theorem of E. H. Moore that a set of $q > 1$ elements can be given the structure of a field if and only if q is a power of a prime; in the vast majority of "real-world" applications of ECCs, q is a power of 2, often either 2 itself or $256 = 2^8$, but other choices of q are also important in the mathematical theory. A finite field of q elements is often called "GF(q)"; the "GF" stands for "Galois field" , in tribute to Galois who first studied finite fields in this generality.*

bounds. For instance, the Minkowski bound becomes the *Gilbert-Varshamov bound*, and can be proved in the same simple way: increase C by one word at a time subject to the condition that no two words come closer than δ. Once no room is left, the open balls of radius δ centered at C must cover F^n. Each of these balls contains the same number of points, say V_δ. Thus $|C| \geq |F|^n / V_\delta$.

Warning: the formula

$$V_\delta = \sum_{r=0}^{\delta-1} \binom{n}{r} (|F| - 1)^r$$

for the size of an open ball of radius r in Hamming is more complicated than the formula for the volume of a ball in Euclidean space. Thus the resulting lower bound V_e / V_{2e} for the packing density of radius-e Hamming spheres does not simplify to 2^{-n}. One can, however, use Stirling's formula to obtain asymptotic formulas for V_e / V_{2e} for large n.

In the setting of sphere packings, we reported in Part I that the Minkowski bound also holds for lattice packings, and indeed for average lattice packings. Likewise here the Gilbert-Varshamov bound holds for linear codes, and indeed for a positive proportion of linear codes. (Here there are only finitely many C for each choice of $(F, n, \dim C)$, so there is no difficulty in defining this average.) It is even rather easy to prove that a randomly chosen code satisfies the Gilbert-Varshamov bound with positive probability. But, again as with lattice packings, it is easy to choose a "random" code that almost certainly comes within a small factor of satisfying the Gilbert-Varshamov bound, but hard to prove such an estimate because no computationally feasible way is known to find the minimal weight of a general linear code. For linear codes over a fixed field F, unlike sphere packings, one can do much better than random for arbitrarily large n, as long as $|F| = q_1^2$ for an integer $q_1 \geq 7$ and $\delta / n \in (a(q_1), b(q_1))$ for certain $a(q_1), b(q_1) \in (0, 1)$. These are the famed "Goppa codes" , obtained by applying V. D. Goppa's construction to "modular curves" over F; again considerable machinery from number theory and algebraic geometry is needed to prove that these codes improve on the Gilbert-Varshamov bound. These matters are discussed in [TV], esp. pages 350ff. But when $(|F|, \delta/n)$ is outside the range where Goppa codes are known to improve on the Gilbert-Varshamov bound, we face the same embarrassment that afflicted us in the sphere-packing context. For instance, if $F = \mathbb{Z}/2\mathbb{Z}$ and $\delta = n/4$ for some large n, it is known that there exist linear codes whose dimension is at least $(\frac{3}{4}\log_2 3 - o(1))n = (.1887\ldots - o(1))n$, but we cannot exhibit one and prove that it works, even though a randomly chosen code of that dimension has minimum weight $\geq n/4$ with probability almost 1.

Weight Enumerators

Once more in analogy with the sphere-packing situation, we can gain some understanding of the difficult problem of the minimal weight of a linear code by introducing generating functions for the much harder problem of the distribution of the weights or coordinates of all the codewords. These generating functions are called *weight enumerators*, and are homogeneous polynomials of degree n in several variables. The *complete weight enumerator* is a polynomial cwe_C with integer coefficients in $|F|$ variables X_a, with $a \in F$ and $X_a \in \mathbb{C}$. It is defined as follows:

$$\mathrm{cwe}_C(\mathbf{X}) := \sum_{c \in C} \left(\prod_{i=1}^{n} X_{c_i} \right).$$

That is, cwe_C is the polynomial whose $\prod_{a \in F} X_a^{n_a}$ coefficient is the number of codewords with n_0 zero coordinates, n_1 coordinates of 1, etc. Other weight enumerators can be obtained as specializations of cwe_C. For instance, for the weight distribution of C we are concerned only with the number of zero and nonzero coordinates in each codeword. We thus introduce the *Hamming weight enumerator* $\mathrm{hwe}_C(X, Y)$. This is the homogeneous polynomial of degree n in two variables obtained from cwe_C by setting $X_a = Y$ for each nonzero $a \in F$ and by setting $X_0 = X$. Equivalently,

$$\begin{aligned} \mathrm{hwe}_C(X, Y) &:= \sum_{c \in C} X^{n - \mathrm{wt}(c)} Y^{\mathrm{wt}(c)} \\ &= \sum_{m=0}^{n} N_m(C) X^{n-m} Y^m, \end{aligned}$$

where $N_m(C)$ is the number of codewords of weight m.

We illustrate these definitions with the weight enumerators of the codes introduced earlier:

- if $C = \{\mathbf{0}\}$ then $\mathrm{cwe}_C(\mathbf{X}) = X_0^n$ and $\mathrm{hwe}_C(X, Y) = X^n$;
- if $C = F^n$ then $\mathrm{cwe}_C(\mathbf{X}) = (\sum_{a \in F} X_a)^n$ and $\mathrm{hwe}_C(X, Y) = (X + (|F| - 1)Y)^n$;
- if C is the repetition code in F^n then $\mathrm{cwe}_C(\mathbf{X}) = \sum_{a \in F} X_a^n$ and $\mathrm{hwe}_C(X, Y) = X^n + (|F| - 1)Y^n$.

If $F = \mathbb{Z}/2\mathbb{Z}$ then the complete and Hamming weight enumerators are the same polynomial with the variables differently named; we call this polynomial simply W_C. We then have:

- The weight enumerator of the parity-check code of length n is $((X + Y)^n + (X - Y)^n)/2$;
- the extended Hamming code H_8 has weight enumerator $W_{H_8}(X, Y) = X^8 + 14X^4Y^4 + Y^8$.

In Part I of this article, we associated to any lattice $L \subset \mathbb{R}^n$ a similar generating function Θ_L encoding the squared lengths of lattice vectors. This generating function, called the theta function of L, is defined by

$$\Theta_C(z) := \sum_{x\in C} z^{(x,x)} = 1 + \sum_{m>0} N_m(C) z^m.$$

We noted various identities satisfied by theta functions. Weight enumerators of codes satisfy analogous identities. Like theta functions, they are multiplicative: the direct sum of any two linear codes $C_1 \subseteq F^{n_1}$ and $C_2 \subseteq F^{n_2}$ is a linear code $C_1 \oplus C_2 \subseteq \mathbb{R}^{n_1+n_2}$, with complete weight enumerator given by

$$\mathrm{cwe}_{C_1\oplus C_2}(\mathbf{X}) = \mathrm{cwe}_{C_1}(\mathbf{X})\ \mathrm{cwe}_{C_2}(\mathbf{X}).$$

The same relation thus holds for the Hamming weight enumerators of C_1, C_2, and $C_1 \oplus C_2$. The identity relating the theta functions of a lattice with its dual also has an analogue here, obtained by F. J. MacWilliams; it relates the weight enumerators of a code C with its *dual code*

$$C^\perp := \{a \in F^n \mid (a,c) = 0 \text{ for all } c \in C\}.$$

Here $(\cdot\,,\cdot)$ is the nondegenerate symmetric bilinear pairing on F^n taking values in F, defined by

$$(a,c) := \sum_{i=1}^{n} a_i c_i.$$

Thus $C^\perp$ is a linear code of dimension $n - \dim C$, with $(C^\perp)^\perp = C$. For example, the codes $\{\mathbf{0}\}$ and F^n are each other's dual; over $\mathbb{Z}/2\mathbb{Z}$, so are the repetition and parity-check codes of the same length, while H_8 is its own dual. There is a discrete analogue of the Poisson summation formula that relates the sum over C of a function $f : F^n \to \mathbb{C}$ with the sum over $C^\perp$ of the "discrete Fourier transform" $\hat{f}$ of f. For instance, if $F = \mathbb{Z}/p\mathbb{Z}$ with p prime, then we may define $\hat{f}$ by

$$\hat{f}(a) := \sum_{c\in F^n} f(c) e^{2\pi i(a,c)/p},$$

and discrete Poisson summation is the identity

$$\sum_{c\in C} f(c) = \frac{1}{|C^\perp|} \sum_{a\in C^\perp} \hat{f}(a).$$

Now $\mathrm{cwe}_C(\mathbf{X})$ is just $\sum_{c\in C} f(c)$ for the choice $f(c) := \prod_{i=1}^n X_{c_i}$. Then $\hat{f}(a) = \prod_{i=1}^n \hat{X}_{a_i}$ where

$$\hat{X}_a := \sum_{c \bmod p} e^{2\pi i ac/p} X_c.$$

From discrete Poisson summation, we deduce the *MacWilliams identity* for complete weight enumerators:

$$\mathrm{cwe}_C(\mathbf{X}) = \frac{1}{|C^\perp|}\, \mathrm{cwe}_{C^\perp}(\hat{\mathbf{X}}),$$

from which follows the MacWilliams identity for Hamming weight enumerators:

$$\mathrm{hwe}_C(X,Y) = \frac{1}{|C^\perp|}\, \mathrm{hwe}_{C^\perp}(X + (|F|-1)Y,\ X - Y).$$

(This identity can be proved even when F is a finite field other than $\mathbb{Z}/p\mathbb{Z}$; the cwe_C identity also has a generalization to arbitrary finite fields.) Note that the weight enumerators we obtained for $\{\mathbf{0}\}$ and F^n, and for the repetition and parity-check codes over $\mathbb{Z}/2\mathbb{Z}$, do in fact satisfy these identities; so does $W_{H_8}(X,Y) = X^8 + 14X^4Y^4 + Y^8$, which is multiplied by 2^4 under the linear transformation $(X,Y) \mapsto (X+Y, X-Y)$.

Applications of the MacWilliams identity include upper bounds on $|C|$ for given n and δ. The coefficients $N_m(C)$ of hwe_C are constrained on the one hand by $N_m(C) \geq 0$, $N_0(C) = 1$, and $N_m(C) = 0$ for positive $m < \delta$, and on the other hand by $N_m(C^\perp) \geq 0$. For C of given size $|C|$, the MacWilliams identity expresses each $N_m(C^\perp)$ as a linear combination of the $N_m(C)$. If δ is large enough the resulting linear constraints cannot all be simultaneously satisfied. For instance, if $(|F|, n, |C|) = (2, 8, 16)$, one can calculate that $\delta \leq 4$, with equality only if $N_m(C) = N_m(H_8)$ for each m. These inequalities, generalized by J. Delsarte to nonlinear codes, are the source of most of the best upper bounds known on $|C|$ for large n and δ.

Self-dual Binary Codes and Their Weight Enumerators

As with lattices, it is for self-dual codes such as H_8 that the MacWilliams identity gives the most detailed information on $N_m(C)$. Consider for instance the case $F = \mathbb{Z}/2\mathbb{Z}$. We saw in this case that cwe_C and hwe_C are the same polynomial, and called this polynomial W_C. If $C^\perp = C$ then $|C| = 2^{n/2}$. Thus the identity between W_C and $W_{C^\perp}$ becomes the statement that W_C is invariant under the linear transformation $(X,Y) \mapsto 2^{-1/2}(X+Y, X-Y)$, which reflects (X,Y) about the line $Y = (\tan \pi/8)X$ (since it rotates (X,Y) counterclockwise by $\pi/4$ and then reflects about the line $X = Y$). Since C is self-dual, $(c,c) = 0$ for each word $c \in C$, and thus the weight of each word c is even.[3] Therefore W_C is invariant also under the reflection $(X,Y) \mapsto (X,-Y)$ in the Y-axis. These two reflections generate the 16-element dihedral group D_{16}. A. M. Gleason determined the ring of polynomials in (X,Y) invariant under this group: it is generated by two homogeneous polynomials, the quadratic X^2+Y^2 and the degree-8 polynomial $(XY(X^2-Y^2))^2$ vanishing to order 2 on each of the four lines $Y/X = \tan k\pi/4$, $k \in \mathbb{Z}/4\mathbb{Z}$. See Figure 1. Thus we have *Gleason's theorem* for self-dual codes C over the two-element field: W_C must be a weighted-homogeneous polynomial in X^2+Y^2 and $(XY(X^2-Y^2))^2$. For example, X^2+Y^2 is the enumerator of the repetition code of length 2 (which is also the parity check code of the same length,

[3] *We remark parenthetically that c has even weight if and only if it is orthogonal to the all-1's word 1^n, whence $1^n \in C^\perp = C$.*

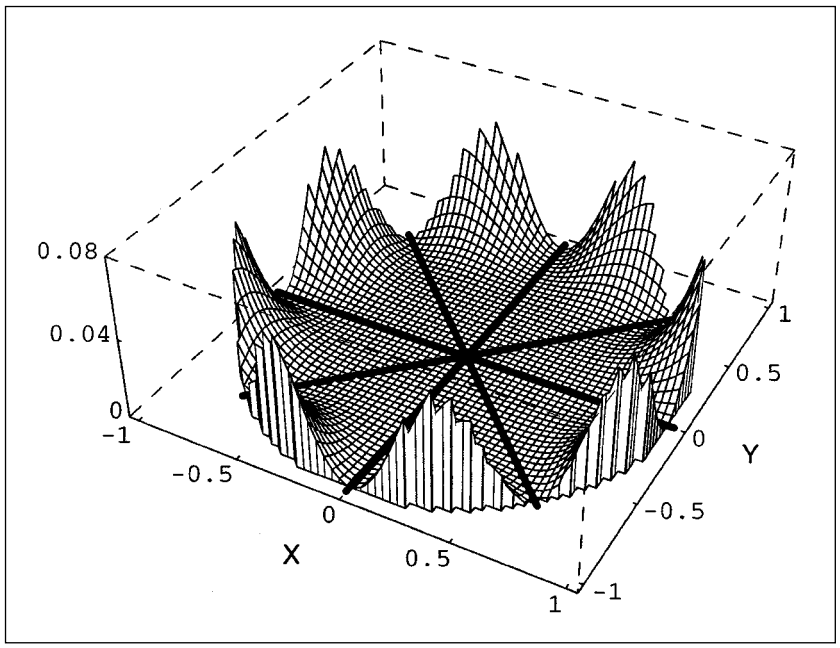

Figure 1. The graph of the function $(XY(X^2 - Y^2))^2$ with domain the unit disk. The lines of the zero locus are shown in bold. The graph is invariant under the 16-element symmetry group of a regular octagon.

and is thus self-dual), while W_{H_8} can be written as $(X^2 + Y^2)^4 - 4(XY(X^2 - Y^2))^2$.

The code H_8 satisfies a further constraint: all its codewords have weight divisible by 4. Such a code over $\mathbb{Z}/2\mathbb{Z}$ is said to be *doubly even*. For any self-dual code C (or a code contained in its dual) over $\mathbb{Z}/2\mathbb{Z}$, the map $\nu : c \mapsto \frac{1}{2}\mathrm{wt}(c) \bmod 2$ is a homomorphism from C to $\mathbb{Z}/2\mathbb{Z}$, and the code is doubly even if and only if ν is the zero homomorphism, a condition that can be checked on generators of the code.[4] In terms of W_C, the condition that C be doubly even is $W_C(X, Y) = W_C(X, iY)$. Thus if C is also self-dual then W_C must be invariant under the group G_1 generated by $(X, Y) \mapsto (X, iY)$ together with D_{16}.

This group can no longer be visualized in the real plane $\mathbb{R}^2$, so instead we consider its action on the ratio $z = Y/X$ in the complex plane $\mathbb{C}^1$. The linear transformation $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G_1$ acts on z by the fractional linear transformation $z \mapsto (az + b)/(cz + d)$. Since the denominator may vanish, we must consider z as an element of the *Riemann sphere* $S = \mathbb{C} \cup \{\infty\}$.[5] Each generator of G_1 is a *unitary* linear transformation, preserving the Hermitian form $|X|^2 + |Y|^2$; thus G_1 is contained in the unitary group $U_2(\mathbb{C})$, and the corresponding transformations $z \mapsto (az + b)/(cz + d)$ act on S by orientation-preserving isometries. The generators $z \mapsto (1 + z)/(1 - z)$ and $z \mapsto i^k z$ of G_1 each permute the real axis, the imaginary axis, and the unit circle $|z| = 1$; thus the same is true of G_1. On the Riemann sphere S, the two axes and the unit circle become three pairwise orthogonal great circles. Thus G_1 acts on S as a subgroup of the group of orientation-preserving symmetries of the regular octahedron whose vertices are the pairwise intersections of these great circles. See Figure 2. It is known that these symmetries constitute a group isomorphic with the symmetric group Sym_4 on 4 letters.[6] One readily checks that the resulting homomorphism from G_1 to Sym_4 is surjective. The kernel of the map $G_1 \to \mathrm{Sym}_4$ is the group of scalar matrices in G_1. Since the determinant of each element of g is a power of i (again this can be checked on the generators), these scalars must be 8-th roots of unity, and again one can check that each 8-th root occurs. Thus G_1 is a group of order $8 \cdot 4! = 192$.

Since G_1 contains the 8-th roots of unity, any polynomial invariant under G_1 must have degree divisible by 8. Thus *the length n of any doubly even self-dual code is a multiple of* 8. The ring of all G_1-invariant polynomials was again determined by Gleason. It too is generated by two homogeneous polynomials, this time W_{H_8} and $(XY(X^4 - Y^4))^4$. Geometrically, the points $z = Y/X$ where W_{H_8} vanishes are the centers of the 8 faces of our octahedron, which are vertices of a cube inscribed in S, while $(XY(X^4 - Y^4))^4$ has quadruple zeros at the six vertices of the octahedron. So, for instance, a doubly even self-dual code C with minimal distance at least 8 must have length $n \geq 24$, and if $n = 24$ then

$$\begin{aligned} W_C &= W_{H_8}^3 - 42(XY(X^4 - Y^4))^4 \\ &= X^{24} + 759X^{16}Y^8 + 2576X^{12}Y^{12} \\ &\quad + 759X^8Y^{16} + Y^{24}. \end{aligned}$$

In particular, C must contain exactly 759 words of its minimal weight 8.

It turns out that such a code exists, and is unique up to coordinate permutations: the remarkable *extended Golay code* $\mathcal{G}_{24}$,[7] found by

[4] *In Part I an* integral lattice *was defined to be a lattice L such that (x, y) is an integer for all x and y in L. Such a lattice was defined to be* even *if the length of every vector is the square root of an even integer. The role of "even" in this situation mirrors that of "doubly even" for linear codes. In particular, an integral lattice is even if and only if it is generated by vectors the square of whose length is even.*

[5] *The Riemann sphere arises naturally as the complex projective line $\mathbf{P}^1(\mathbb{C}) = (\mathbb{C}^2 - \{\mathbf{0}\})/\mathbb{C}^*$, since linear transformations act linearly on $\mathbb{C}^2$ and commute with the multiplicative group $\mathbb{C}^*$.*

[6] *The four objects permuted are the opposite pairs of faces of the octahedron; the homomorphism $\mathrm{Sym}_4 \to \mathrm{Sym}_3$ is then obtained from the permutation action on the three great circles, or equivalently on the three opposite pairs of vertices of the octahedron.*

[7] *More properly, the "extended binary Golay code", since there is also an "extended ternary Golay code" $\mathcal{G}_{12} \subset (\mathbb{Z}/3\mathbb{Z})^{12}$, which we shall encounter later.*

M. J. E. Golay in 1954. This code can be defined in various ways; for example, $\mathcal{G}$ is generated by its 759 minimal words, whose supports constitute the *Steiner system* of 8-element subsets (*octads*) of a 24-element set, such that each 5-element subset is contained in a unique octad. It is known that this $(5, 8, 24)$ Steiner system is unique, and its automorphism group is the quintuply transitive group M_{24}, the largest of Mathieu's sporadic simple groups; M_{24} is thus also the group of permutations preserving $\mathcal{G}_{24}$. By ignoring any one of the 24 coordinates we obtain Golay's code $\mathcal{G}_{23}$, which has length 23, dimension 12, and minimal distance 7. Thus $\mathcal{G}_{23}$ is a 3-error-correcting code. In $(\mathbb{Z}/2\mathbb{Z})^{23}$, a Hamming sphere of radius 3 contains $\sum_{r=0}^{3}\binom{23}{r} = 2048$ words, i.e., exactly $2^{11} = |(\mathbb{Z}/2\mathbb{Z})^{23}| \Big/ |\mathcal{G}_{23}|$. Therefore $|\mathcal{G}_{23}|$ comprises the centers of a *perfect* packing of $(\mathbb{Z}/2\mathbb{Z})^{23}$ by radius-3 Hamming spheres! One explicit recipe for $\mathcal{G}_{23}$ is the span of the cyclic shifts of the word

$$11111010110011001010000,$$

in which the i-th coordinate is 1 if and only if i is a nonzero square mod 23. The code $\mathcal{G}_{24}$ can be recovered from $\mathcal{G}_{23}$ by appending a "check digit" to each word of $\mathcal{G}_{23}$ to make its weight even.

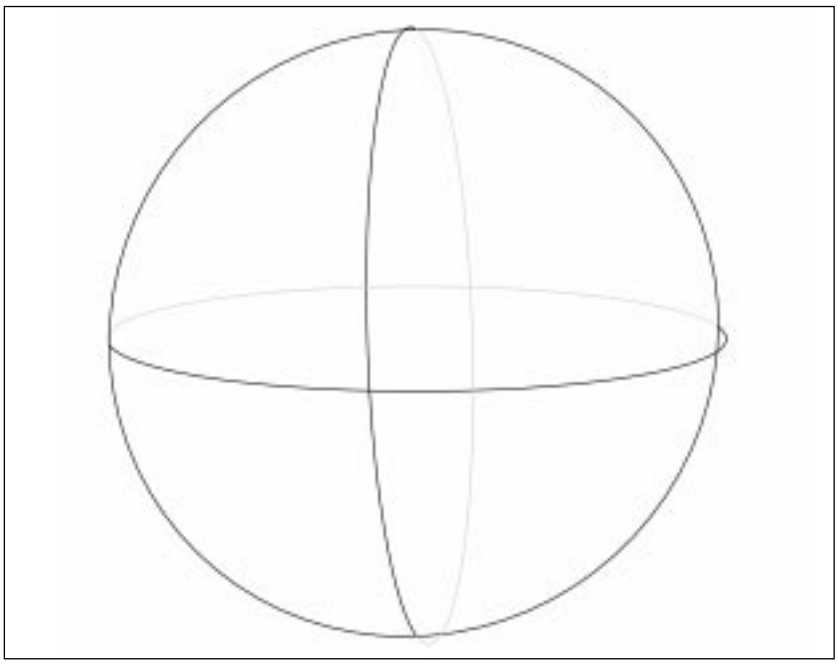

Figure 2. Under stereographic projection the images of the real axis, the imaginary axis, and the unit circle are three orthogonal great circles on the Riemann sphere. The six intersection points are the vertices of a regular octahedron.

Each of D_{16} and G_1 is a finite subgroup of $\mathrm{GL}_n(\mathbb{C})$ whose ring of invariant polynomials is generated by n polynomials. Such a group $G \subset \mathrm{GL}_n(\mathbb{C})$ is said to have *free invariant ring* (because a set of generators for the G-invariant polynomials is algebraically independent if and only if it has size n.) Other familiar examples are:

- $\{\pm 1\} \subset \mathrm{GL}_1(\mathbb{C})$, with invariant ring generated by X^2;
- more generally, the m-th roots of unity in $\mathrm{GL}_1(\mathbb{C})$, with invariants generated by X^m; and
- the group of permutation matrices in $\mathrm{GL}_n(\mathbb{C})$, whose invariants are generated by the elementary symmetric functions in the coordinates of $\mathbb{C}^n$.

Once $n > 1$, most finite subgroups of $\mathrm{GL}_n(\mathbb{C})$ do not have free invariant rings; already for $n = 2$, the invariant ring of the 2-element group $\{\pm 1\} \subset \mathrm{GL}_2(\mathbb{C})$ requires 3 generators to account for X^2, XY, and Y^2. The classification of finite $G \subset \mathrm{GL}_n(\mathbb{C})$ with free invariant rings was completed in 1954 by J. C. Shephard and J. A. Todd, who combined theoretical insights with explicit computation. As a consequence of their theorem, it followed that a finite group $G \subset \mathrm{GL}_n(\mathbb{C})$ has free invariant ring if and only if it is generated by *complex reflections*, i.e., $r \in \mathrm{GL}_n(\mathbb{C})$ such that $\ker(1 - r)$ has dimension $n - 1$. For instance, the automorphism group of the root lattice E_8 has free invariant ring, because it is generated by reflections in the hyperplanes orthogonal to the roots of E_8. The complex reflection groups in the Shephard-Todd list, and their invariant rings, arise with some frequency in some branches of mathematics. We have already encountered two of the groups in identities satisfied by weight enumerators of certain self-dual codes. Several others also occur in this way, as we shall see in the next section.

Some Direct Connections between Weight Enumerators and Theta Functions

The analogy we have drawn between lattices and linear codes seems particularly tight between self-dual lattices and self-dual codes over $\mathbb{Z}/2\mathbb{Z}$, and between even self-dual lattices and doubly even self-dual codes over $\mathbb{Z}/2\mathbb{Z}$. The analogy extends even to the theta series and weight enumerators. For instance, in the (doubly) even case, the theta series is in the ring of modular forms for $\mathrm{SL}_2(\mathbb{Z})$, whose generators have weights corresponding to lattices of dimensions 8 and 24; and the weight enumerator is in the ring of G_1-invariant polynomials, whose generators again have degrees 8 and 24. This apparent coincidence is explained by N. J. A. Sloane's "Construction A", which associates to any linear code $C \subseteq (\mathbb{Z}/2\mathbb{Z})^n$ a lattice $L_C \subset \mathbb{R}^n$, whose density, dual lattice, minimal (Euclidean) length,[8] and theta function are predictable from the corresponding invariants of C. We devote this

[8] *Inevitably the word "length" is used for both the length $|v|$ of $v \in \mathbb{R}^n$ and the dimension of the finite vector space F^n containing C. It will always be clear from context which kind of length is meant at each use of the word.*

section to that construction and some of its consequences and variations.

The lattice L_C comes from integer vectors that reduce mod 2 to codewords. To make this consistent with duality, we scale the lattice to multiply all the inner products by $1/2$:

$$L_C := \{2^{-1/2}v \mid v \in \mathbb{Z}^n,\ v \bmod 2 \in C\}.$$

We then have:

- the density of L_C is $2^{-n/2}|C|$;
- the dual lattice of L_C is the lattice $L_{C^\perp}$ associated with the dual code.

In particular, L_C is self-dual if and only if C is, and L_C is even if and only if C is doubly even. For example, if C is the repetition code of length 2, then L_C is a self-dual lattice in $\mathbb{R}^2$, and thus[9] isometric with $\mathbb{Z}^2$, as can also be seen directly. Likewise L_{H_8} is an even self-dual lattice in $\mathbb{R}^8$, and thus isometric with E_8. This gives a different construction of the E_8 lattice. (In this case it is not entirely trivial to see that the two constructions yield isometric lattices!)

The theta series of L_C can be obtained from the weight enumerator W_C as follows: define $\Theta_0(z)$ and $\Theta_1(z)$ by

$$\begin{aligned}\Theta_0(z) &:= \sum_{k=-\infty}^{\infty} z^{2k^2}\\ &= 1 + 2(z^2 + z^8 + z^{18} + \cdots),\\ \Theta_1(z) &:= \sum_{k=-\infty}^{\infty} z^{2(k+\frac{1}{2})^2}\\ &= z^{1/2}(1 + z^4 + z^{12} + z^{24} + \cdots);\end{aligned}$$

then

$$\Theta_{L_C} = W_C(\Theta_0, \Theta_1).$$

This is not hard to see from the fact that Θ_0 is the theta series of $2^{1/2}\mathbb{Z}$ while Θ_1 can be viewed as the theta series of $2^{1/2}(\mathbb{Z} + \frac{1}{2})$. Special cases of this identity are

$$\Theta_0^2 + \Theta_1^2 = \Theta_{\mathbb{Z}^2} = \Theta_{\mathbb{Z}}^2,$$
$$\Theta_0^8 + 14\Theta_0^4\Theta_1^4 + \Theta_1^8 = \Theta_{E_8}.$$

A consequence either of the formula for Θ_{L_C} or of the definition of L_C is that

- the minimal length of L_C is the square root of $\min\left(2, \frac{1}{2}\delta(C)\right)$.

What then of the Poisson and MacWilliams identities? Let $z = e^{\pi i\tau}$ as in Part I, with $\tau \in \mathcal{H}$ and

$$\theta_L(\tau) := \Theta_L(e^{\pi i\tau}), \quad \theta_i(\tau) := \Theta_i(e^{\pi i\tau}).$$

The Poisson identity relates $\theta_L(\tau)$ with $\theta_{L^*}(-1/\tau)$. Applying this identity to the sums defining $\theta_i(\tau)$, we find

$$(\tau/i)^{-1/2}\theta_0(-1/\tau) = 2^{-1/2}\Big(\theta_0(\tau) + \theta_1(\tau)\Big),$$
$$(\tau/i)^{-1/2}\theta_1(-1/\tau) = 2^{-1/2}\Big(\theta_0(\tau) - \theta_1(\tau)\Big).$$

That is, the involution $\phi(\tau) \leftrightarrow (\tau/i)^{-1/2}\phi(-1/\tau)$ acts on (θ_0, θ_1) exactly as the MacWilliams involution $(X, Y) \leftrightarrow 2^{-1/2}(X + Y, X - Y)$ does! Moreover, the translation $\tau \mapsto \tau + 1$ takes (θ_0, θ_1) to $(\theta_0, i\theta_1)$. Thus if $W(X, Y)$ is any homogeneous polynomial then $W(\theta_0, \theta_1)$ is a modular form for $\mathrm{SL}_2(\mathbb{Z})$ if and only if W is invariant under those two linear transformations, and thus under the group G_1 generated by them. Moreover, $W(\theta_0, \theta_1)$ is a modular form for the congruence subgroup Γ generated by $\tau \leftrightarrow -1/\tau$ and $\tau \mapsto \tau + 2$ if and only if W is invariant under the dihedral group D_{16} generated by $(X, Y) \leftrightarrow 2^{-1/2}(X + Y, X - Y)$ and $(X, Y) \leftrightarrow (X, -Y)$. This explains the "coincidence" involving dimensions 8 and 24: the basic modular forms are obtained from the basic D_{16} or G_1 invariants by substituting for X, Y the forms θ_0, θ_1 of weight $1/2$. We have already seen this for the theta series of $\mathbb{Z}^2$ and E_8; we also have $\delta_{24} = \theta_0^4\theta_1^4(\theta_0^4 - \theta_1^4)^4/16$.

Construction of the Leech Lattice

Construction A also figures in Leech's original construction of L_{24}, a lattice described but not defined in Part I. There we asserted the existence of a unique even self-dual lattice $L_{24} \subset \mathbb{R}^{24}$ with all nonzero vectors of length strictly greater than $\sqrt{2}$, and reported that this important lattice is, among other things, central to the classification of simple finite groups. The lattice L_{24} cannot be L_C for any code C, because L_C has minimal length at most $\sqrt{2}$. But $L_{\mathcal{G}_{24}}$ comes close: it is a self-dual even lattice in $\mathbb{R}^{24}$, and since $\mathcal{G}_{24}$ has minimal weight 8, the only vectors of length < 2 in $L_{\mathcal{G}_{24}}$ are the scaled unit vectors $\pm 2^{1/2}e_i$. Let L', then, be the index-2 sublattice of $L_{\mathcal{G}_{24}}$ consisting of those $2^{-1/2}v \in L_{\mathcal{G}_{24}}$ for which $\sum_{i=1}^{24} v_i$ is a multiple of 4. (This sum $\sum_{i=1}^{24} v_i$ is already even for all $v \in 2^{1/2}L_{\mathcal{G}_{24}}$ because every word in $\mathcal{G}_{24}$ has even weight.) Then L' is a lattice of minimal length at least 2, and in fact exactly 2 because it contains vectors of the form $\sqrt{2}$ times the sum of two unit vectors. The density of L' is $1/2$. Now let $v_1 \in \mathbb{R}^{24}$ be the vector $(-3, 1, 1, 1, \ldots, 1)/\sqrt{8}$ of length 2. We can check that $(v, v_1) \in \mathbb{Z}$ for all $v \in L'$, and that $2v_1 \in L'$ while $v_1 \notin L'$. We can now define

$$L_{24} := L' \cup (L' + v_1).$$

Let us see that L_{24} is unimodular of minimal length 2. It is unimodular because it has density 1. Since L_{24} is an even lattice, it is enough to show that it has vectors of length 2 but has no vectors of length $\sqrt{2}$. We know already that L' has vectors of length 2 but not of length $\sqrt{2}$. Thus we need only check that if $v \in L' + v_1$ then $|v| > \sqrt{2}$. But each coordinate of v is an odd integer divided by $\sqrt{8}$,

[9] *As reported in Part I, for every $n < 8$ every self-dual lattice in $\mathbb{R}^n$ is isometric with $\mathbb{Z}^n$.*

so $(v,v) \geq 24/8 > 2$. Therefore L_{24} has minimal nonzero length 2, as claimed. This construction of L_{24} shows that the Mathieu group M_{24} is involved in the group $Co_0 = \mathrm{Aut}(L_{24})$ of isometries of the Leech lattice; Conway used further properties of $\mathcal{G}_{24}$ to construct the full group of isometries and prove that $Co_0/\{\pm 1\}$ is a sporadic simple group.

Construction A_p, for $p = |F|$, an Odd Prime

Construction A can be generalized and varied in many ways; the dozen that appear in the index of [CS] under "Construction" are a large but not exhaustive sample. The simplest variation is "Construction A_p", which replaces $\mathbb{Z}/2\mathbb{Z}$ by $\mathbb{Z}/p\mathbb{Z}$ for some odd prime p. To a linear code $C \subseteq (\mathbb{Z}/p\mathbb{Z})^n$, this construction associates the lattice

$$L_C := \{p^{-1/2}v \mid v \in \mathbb{Z}^n,\ v \bmod p \in C\}$$

in $\mathbb{R}^n$, with density $p^{-n/2}|C|$ and dual lattice $L_{C^\perp}$. The theta series of L_C can be obtained from the complete weight enumerator of C:

$$\Theta_{L_C} = \mathrm{cwe}_C(\Theta_0^{(p)}, \Theta_1^{(p)}, \ldots, \Theta_{p-1}^{(p)}),$$

where for $m \bmod p$ we have

$$\Theta_m^{(p)}(z) := \sum_{\substack{k\in\mathbb{Z} \\ k\equiv m \bmod p}} z^{k^2/p}.$$

Under our usual substitution $z = e^{\pi i\tau}$, each of these $\Theta_m^{(p)}$ becomes a modular form $\theta_m^{(p)}$ of weight $1/2$ for the congruence subgroup $\Gamma_p \subset \mathrm{SL}_2(\mathbb{Z})$ consisting of matrices in Γ congruent to $\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) \bmod p$. By summing over $-k$ instead of k we may see that $\Theta_m^{(p)} = \Theta_{-m}^{(p)}$. Thus if $p = 3$ the theta series of L_C still depends only on the Hamming weight enumerator of C:

$$\Theta_{L_C} = \mathrm{hwe}_C(\Theta_0^{(3)}, \Theta_1^{(3)}).$$

For any p, the generators of Γ behave nicely on the modular forms $\theta_m^{(p)}$: since each exponent k^2/p is congruent to $m^2/p \bmod 1$, we have

$$\theta_m^{(p)}(\tau+2) = e^{\frac{2\pi i}{p}m^2}\theta_m^{(p)}(\tau);$$

and Poisson summation yields

$$(\tau/i)^{-1/2}\theta_m^{(p)}(-1/\tau) = p^{-1/2}\sum_{j \bmod p} e^{2\pi i jm/p}\,\theta_j^{(p)}(\tau).$$

So, as with $p = 2$, we see that $\phi(\tau) \mapsto (\tau/i)^{-1/2}\phi(-1/\tau)$ acts on the $\theta_m^{(p)}$ as $p^{-1/2}$ times the discrete Fourier transform, i.e., by the linear transformation that leaves cwe_C invariant if C is self-dual (MacWilliams again). Also, $\tau \mapsto \tau + 2$ acts on the $\theta_m^{(p)}$ by the diagonal linear transformation $X_m \mapsto e^{2\pi i m^2/p}X_m$, which again fixes cwe_C because $\sum_{i=1}^n c_i^2 = (c,c) = 0$ for each $c \in C$.

When $p = 3$, this condition still depends only on $\mathrm{wt}(c)$ because $a^2 = 1$ for both nonzero choices of $a \in \mathbb{Z}/3\mathbb{Z}$, and we find that the Hamming weight enumerator $\mathrm{hwe}_C(X,Y)$ is invariant under the group G_3 generated by

$$(X,Y) \mapsto 3^{-1/2}(X+2Y, X-Y) \quad \text{and} \quad (X,Y) \mapsto (X, e^{2\pi i/3}Y).$$

Both these linear maps preserve $|X|^2 + 2|Y|^2$, and are thus contained in $U_2(\mathbb{C})$ and act by orientation-preserving isometries on the Riemann sphere parametrized by $z = 2^{1/2}Y/X$. We find that G_3 acts on the sphere by the group of orientation-preserving symmetries of the regular tetrahedron with vertices $z = \infty$ and $z = -e^{2\pi ik/3}/\sqrt{2}$ for $k = 0,1,2$. This group is isomorphic with the alternating group Alt_4 (each even permutation of the vertices arises uniquely), and the kernel of $G_3 \to \mathrm{Alt}_4$, which is the group of scalar matrices in G_3, is the group of 4-th roots of unity. Thus if $C \subset (\mathbb{Z}/3\mathbb{Z})^n$ is a self-dual code then n is a multiple of 4. It turns out that G_3, like G_1, is a complex reflection group, this time with invariant ring generated by polynomials of degrees 4 and 12. Once more, Gleason gave explicit generators: $X^4 + 8XY^3$, with simple zeros at the vertices of our tetrahedron, and $Y^3(X^3 - Y^3)^3$, with triple zeros at the vertices $z = 0$ and $z = e^{2\pi ik/3}\sqrt{2}$ of the dual tetrahedron. Recall that in the case of self-dual doubly even codes in $(\mathbb{Z}/2\mathbb{Z})^n$ the Gleason generators were nicely explained by the Hamming and Golay codes H_8 and $\mathcal{G}_{24}$. There are analogous self-dual codes in $(\mathbb{Z}/3\mathbb{Z})^n$. The "tetracode", generated by 1110 and 0121, has weight enumerator $X^4 + 8XY^3$. If a self-dual code $C \subset (\mathbb{Z}/3\mathbb{Z})^n$ has minimal distance 6 then n must be at least 12, and if $n = 12$ then hwe_C must be

$$(X^4 + 8XY^3)^3 - 24Y^3(X^3 - Y^3)^3 = X^{12} + 264X^6Y^6 + 440X^3Y^9 + 24Y^{12}.$$

Once more Golay found a code $\mathcal{G}_{12}$ with this weight enumerator; like the tetracode, it is unique up to signed coordinate permutations. There is a strong analogy between the codes $\mathcal{G}_{12}$ and $\mathcal{G}_{24}$: the supports of the minimal nonzero words in $\mathcal{G}_{12}$ constitute a Steiner $(5,6,12)$ system, whose automorphism group is Mathieu's quintuply transitive sporadic Mathieu group M_{12}. Ignoring any one coordinate yields a code $\mathcal{G}_{11}$ of length 11, dimension 6, and minimal distance 5. Thus $\mathcal{G}_{11}$ is a 2-error-correcting code. As with $\mathcal{G}_{23}$, the resulting packing of Hamming spheres is perfect, since each radius-2 sphere contains exactly $\sum_{r=0}^{2} 2^r\binom{11}{r} = 243 = 3^5 = |(\mathbb{Z}/3\mathbb{Z})^{11}|\,/\,|\mathcal{G}_{11}|$ words. A. Tietäväinen and J. H. van Lint showed that $\mathcal{G}_{11}$ and $\mathcal{G}_{23}$ are the *only* perfect linear e-error correcting codes for $e > 1$ except for trivial codes of size 1 and the only slightly less trivial repetition code in $(\mathbb{Z}/2\mathbb{Z})^n$ for

$n = 2e + 1$.[10] The $\mathcal{G}_{12}$ is generated by the rows of a *Hadamard matrix* of order 12, i.e., a 12×12 matrix H each of whose entries is ± 1, and whose rows are pairwise orthogonal (equivalently, a ± 1 matrix such that $HH^{\mathrm{T}} = 12I_{12}$). It is known that such a matrix of order 12 exists and is unique up to signed permutations of the rows and columns. One choice is

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

with the diagonals of +1's determined by the nonzero squares mod 11. The span of the rows of H mod 3 generates $\mathcal{G}_{12}$.

We return now to self-dual codes $C \subset (\mathbb{Z}/p\mathbb{Z})$ for a general odd prime p. Once $p > 3$, the condition $(c, c) = 0$ no longer constrains $\mathrm{wt}(c)$, so we consider the complete weight enumerator cwe_C. We have seen already that C must be invariant under $X_m \mapsto e^{2\pi i m^2/p} X_m$ as well as the normalized discrete Fourier transform $X_m \mapsto p^{-1/2}\hat{X}_m$. If moreover C contains the all-1's word $\mathbf{1}$ then $(c, \mathbf{1}) = 0$ for each $c \in C$, whence cwe_C is invariant also under $X_m \mapsto e^{2\pi i m/p} X_m$. Thus cwe_C is invariant under the group generated by these three unitary linear transformations of $\mathbb{C}^p$; call this group $W_p \subset U_p(\mathbb{C})$. It turns out that Weil had already extensively investigated this group in another context [W]. Perhaps surprisingly, this group is finite. Weil shows this finiteness by proving that conjugation by elements of W_p permutes the *Heisenberg group* $H_p \subset U_p(\mathbb{C})$. This H_p is the non-commutative group of order p^3 and exponent p generated by $X_m \mapsto e^{2\pi i m/p} X_m$ and the cyclic permutation $X_m \mapsto X_{m+1}$ (with subscripts mod p and hence $X_p = X_0$). The commutator of these two linear transformations is the scalar $e^{2\pi i/p}$. Thus the quotient $\overline{H}_p$ of H_p by its scalar subgroup is isomorphic with $(\mathbb{Z}/p\mathbb{Z})^2$, and is normal in the quotient $\overline{W}_p$ of W_p by *its* scalar subgroup. Moreover $\overline{W}_p/\overline{H}_p$ acts on $\overline{H}_p \cong (\mathbb{Z}/p\mathbb{Z})^2$, and it turns out that $\overline{W}_p/\overline{H}_p \cong \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

[10] *The same is believed, but not yet proved, to be the case for arbitrary codes, not only linear ones; Van Lint and Tietäväinen prove this only when the alphabet size is a prime power.*

What should $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ have to do with weight enumerators of self-dual codes? We return to the theta function of L_C. Since θ_{L_C} is obtained from cwe_C by substituting $\theta_m^{(p)}$ for X_m, and since $\theta_m^{(p)} = \theta_{-m}^{(p)}$, we consider the "symmetrized weight enumerator" swe_C, obtained from hwe_C by setting $X_m = X_{-m}$. This is a homogeneous polynomial of degree n in $(p+1)/2$ variables. It is invariant under the subgroup of W_p commuting with the involution $X_m \leftrightarrow X_{-m}$; this subgroup turns out to be the same as the group generated by the linear transformations $X_m \mapsto e^{2\pi i m^2/p} X_m$ and $X_m \mapsto p^{1/2}\hat{X}_m$ that we encountered earlier. Up to scalars, this group is isomorphic with the projective linear group $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})/\{\pm 1\}$. Our explanation for the appearance of this group is the relationship between the congruence groups for which θ_{L_C} and the $\theta_m^{(p)}$ are modular. For θ_{L_C}, that group is Γ; for $\theta_m^{(p)}$, it is the normal subgroup of Γ consisting of matrices congruent to $\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ mod p. The quotient of Γ by this subgroup is generated by $\tau \mapsto \tau + 2$ and $\tau \leftrightarrow -1/\tau$, which acts on the $\theta_m^{(p)}$ linearly by transformations proportional to $\theta_m^{(p)} \mapsto e^{\frac{2\pi i}{p} m^2} \theta_m^{(p)}$ and the discrete Fourier transform; on the other hand, the quotient is obtained by reducing the matrices in Γ mod p, and is thus identified with $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$!

We illustrate this for the first two cases $p = 3, 5$, which are the only ones for which a complex reflection group arises.[11] For $p = 3$, the symmetrized and Hamming weight enumerators coincide. We already found that hwe_C is invariant under G_3, and we recognized the quotient of G_3 by its scalar subgroup as Alt_4. We can now observe that Alt_4 is in fact isomorphic with $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$. For $p = 5$, we write the symmetrized weight enumerator as

$$\mathrm{swe}_C(X, Y, Z) = \mathrm{hwe}_C(X, Y, Z, Z, Y).$$

If $C \subset (\mathbb{Z}/5\mathbb{Z})^n$ is self-dual then $\mathrm{swe}_C(X, Y, Z)$ is invariant under the reflection group G_5 generated by $(X, Y, Z) \mapsto (X, e^{2\pi i/5}Y, e^{-2\pi i/5}Z)$ and (by MacWilliams) the transformation

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} \mapsto \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 2 & 2 \\ 1 & (\sqrt{5}-1)/2 & (-\sqrt{5}-1)/2 \\ 1 & (-\sqrt{5}-1)/2 & (\sqrt{5}-1)/2 \end{pmatrix} \begin{bmatrix} X \\ Y \\ Z \end{bmatrix}.$$

[11] *What of $p = 2$? Even the anomalous case of doubly even codes can be explained in a similar way; here instead of Γ we have all of $\mathrm{SL}_2(\mathbb{Z})$, and the normal subgroup for which θ_0 and θ_1 are modular consists of matrices congruent to $\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ mod 4. Thus we expect the group $\mathrm{PSL}_2(\mathbb{Z}/4\mathbb{Z})$, and indeed $\mathrm{PSL}_2(\mathbb{Z}/4\mathbb{Z})$ is isomorphic with Sym_4, the quotient of G_1 by its scalar subgroup.*

The simplest example is $n = 2$, for which C consists of the multiples of $(1,2)$, and $\mathrm{swe}_C(X,Y,Z) = X^2 + 4YZ$. For this code, $L_C \cong \mathbb{Z}^2$, whence $(\theta_0^{(5)})^2 + 4\theta_1^{(5)}\theta_2^{(5)} = \theta_{\mathbb{Z}}^2$. Since G_5 is a finite group that fixes the quadratic form $X^2 + 4YZ$, we can regard it after a linear change of variables as a subgroup of the orthogonal group $O_3(\mathbb{R})$. Thus once more we have a finite group of isometries of the sphere, though here not all these isometries are orientation preserving. For instance, the above 3×3 matrix yields a reflection. It turns out that G_5 is the group of isometries of a regular icosahedron, and is thus isomorphic with $\{\pm 1\} \times \mathrm{Alt}_5$. This is a reflection group whose invariants are generated by polynomials of degrees 2, 6, and 10. We have already seen a degree-2 invariant; for the invariants of degrees 6 and 10, we may take the products of linear forms vanishing respectively on the planes perpendicular to the six opposite pairs of vertices of the icosahedron and the planes parallel to its ten opposite pairs of faces. For instance, we have the degree-6 invariant

$$X \prod_{k=0}^{4} (X + e^{2\pi ik/5}Y + e^{-\pi ik/5}Z) = X^6 - 20X^4YZ + 80(XYZ)^2 + 32X(Y^5 + Z^5).$$

Once $p \geq 5$, the $\theta_m^{(p)}$ for $0 \leq m \leq (p+1)/2$, while linearly independent, are not algebraically independent. For $p = 5$, there is a single dependence, necessarily invariant under G_5; we calculate that the above degree-6 invariant, evaluated at $(X,Y,Z) = (\theta_0^{(5)}, \theta_1^{(5)}, \theta_2^{(5)})$, equals $\theta_{\mathbb{Z}}^6$, the cube of our degree-2 invariant. That is, $(\theta_0^{(5)}, \theta_1^{(5)}, \theta_2^{(5)})$ satisfy the homogeneous sextic

$$X^4YZ - (XYZ)^2 - X(Y^5 + Z^5) + 2(YZ)^3 = 0.$$

This sextic, considered as a subset of the projective plane, is an example of a "modular curve"—but that is a topic for a different expository article.

References

[CS] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer, New York, 1993.

[McWS] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 3rd ed., North-Holland, Amsterdam-New York-Oxford, 1981.

[S] J.-P. Serre, *A Course in Arithmetic*, Springer, New York, 1973.

[TV] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-Geometric Codes*, Kluwer, Dordrecht, 1991.

[W] A. Weil, Sur certaines groupes d'opérateurs unitaires, *Acta Math.* **111** (1964), 143–211.