ERROR-CORRECTING CODES AND INVARIANT THEORY: NEW APPLICATIONS OF A NINETEENTH-CENTURY TECHNIQUE

N. J. A. SLOANE

Abstract. An unfashionable nineteenth century technique, invariant theory, has recently been used to study error-correcting codes. This technique is potentially of much wider application, is very powerful, often produces startling results, and (not least) is fun to use.

I. Introduction

It will be best to begin with an example, showing how invariant theory is used to solve a typical problem. Most of the undefined terms will be explained in later sections.

A. The problem. Associated with any error-correcting code is a polynomial called its weight enumerator $W(x, y)$ (see Part II). For a certain class of codes this polynomial must satisfy two equations:

$$W\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right) = W(x, y), \tag{1}$$

$$W(x, iy) = W(x, y). \tag{2}$$

The problem we want to solve is to find all polynomials $W(x, y)$ satisfying (1) and (2).

B. Invariants. Equation (1) says that $W(x, y)$ is unchanged, or *invariant*, under the linear transformation

---

For many far-reaching generalizations of the results in this paper, see the book:
G. Nebe, E. M. Rains and N. J. A. Sloane, *Self-Dual Codes and Invariant Theory*, Springer-Verlag, Heidelberg, 2006, ISBN 3-540-30729-x; http://neilsloane.com/doc/cliff2.html.

$$T_1: \begin{array}{l} \text{replace } x \text{ by } (x+y)/\sqrt{2}, \\ \\ \text{replace } y \text{ by } (x-y)/\sqrt{2}, \end{array}$$

or, in matrix notation,

$$T_1: \text{ replace } \begin{pmatrix} x \\ y \end{pmatrix} \text{ by } \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Similarly Eq. (2) says that $W(x, y)$ is also invariant under the transformation

$$T_2: \begin{array}{l} \text{replace } x \text{ by } x \\ \\ \text{replace } y \text{ by } iy \end{array}$$

or

$$T_2: \text{ replace } \begin{pmatrix} x \\ y \end{pmatrix} \text{ by } \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Of course $W(x, y)$ must therefore be invariant under any combination T_1^2, T_1T_2, $T_1T_2T_1, \ldots$ of these transformations. It is not difficult to show (as we shall see in Section A of Part III) that the matrices

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

when multiplied together in all possible ways produce a *group* $\mathfrak{G}_1$ containing 192 matrices.

So our problem now says: find the polynomials $W(x, y)$ which are invariant under all 192 matrices in the group $\mathfrak{G}_1$.

C. How many invariants? The first thing we want to know is how many invariants there are. This isn't too precise, because of course if f and g are invariants, so is any constant multiple cf and also $f+g$, $f-g$ and the product fg. Also it is enough to study the *homogeneous* invariants (in which all terms have the same degree).

So the right question to ask is: how many linearly independent, homogeneous invariants are there of each degree d? Let's call this number a_d.

A convenient way to handle the numbers $a_0, a_1, a_2, \ldots$ is by combining them into a power series or generating function

$$\Phi(\lambda) = a_0 + a_1\lambda + a_2\lambda^2 + \cdots.$$

Conversely, if we know $\Phi(\lambda)$, the numbers a_d can be recovered from the power series expansion of $\Phi(\lambda)$.

At this point we invoke a beautiful theorem of T. Molien, published in 1897 ([**52**], [**14**, p. 301], [**51**, p. 259], [**11**, p. 110]):

THEOREM 1. *For any finite group* $\mathfrak{G}$ *of complex* $m \times m$ *matrices,* $\Phi(\lambda)$ *is given by*

$$\Phi(\lambda) = \frac{1}{|\mathfrak{G}|} \sum_{A \in \mathfrak{G}} \frac{1}{\det(I - \lambda A)}, \tag{3}$$

where $|\mathfrak{G}|$ *is the number of matrices in* $\mathfrak{G}$, det *stands for determinant, and* I *is a unit matrix. In words,* $\Phi(\lambda)$ *is the average, taken over all matrices* A *in the group, of the reciprocal of the polynomial* $\det(I - \lambda A)$.

We call $\Phi(\lambda)$ the *Molien series* of $\mathfrak{G}$. The proof of this theorem is given in Section D of Part III.

For our group $\mathfrak{G}_1$, from the matrices corresponding to I, T_1, $T_2, \ldots$ we get

$$\Phi(\lambda) = \frac{1}{192}\left\{\frac{1}{(1-\lambda)^2} + \frac{1}{1-\lambda^2} + \frac{1}{(1-\lambda)(1-i\lambda)} + \cdots\right\}. \tag{4}$$

There are shortcuts, but it is quite feasible to work out the 192 terms directly (many are the same) and add them. The result is a surprise: everything collapses to give

$$\Phi(\lambda) = \frac{1}{(1-\lambda^8)(1-\lambda^{24})}. \tag{5}$$

D. Interpreting $\Phi(\lambda)$. The very simple form of (5) is trying to tell us something. Expanding in powers of λ, we have

$$\begin{aligned}\Phi(\lambda) &= a_0 + a_1\lambda + a_2\lambda^2 + \cdots \\ &= (1+\lambda^8+\lambda^{16}+\lambda^{24}+\cdots)(1+\lambda^{24}+\lambda^{48}+\cdots).\end{aligned} \tag{6}$$

We can deduce one fact immediately: a_d is zero unless d is a multiple of 8, i.e., the degree of a homogeneous invariant must be a multiple of 8. (This is already a useful theorem in coding theory.) But we can say more. The RHS of (6) is exactly what we would find if there were two "basic" invariants, of degrees 8 and 24, such that all invariants are formed from sums and products of them.

This is because two invariants, θ, of degree 8, and φ, of degree 24, would give rise to the following invariants.

(7)

degree d	invariants	number a_d
0	1	1
8	θ	1
16	θ^2	1
24	θ^3, φ	2
32	θ^4, $\theta\varphi$	2
40	θ^5, $\theta^2\varphi$	2
48	θ^6, $\theta^3\varphi$, φ^2	3
...	...	...

Provided all the products $\theta^i\varphi^j$ are linearly independent — which is the same thing as saying that θ and φ are algebraically independent — the numbers a_d in (7) are exactly the coefficients in

$$\begin{aligned}&1+\lambda^8+\lambda^{16}+2\lambda^{24}+2\lambda^{32}+2\lambda^{40}+3\lambda^{48}+\cdots \\ &= (1+\lambda^8+\lambda^{16}+\lambda^{24}+\cdots)(1+\lambda^{24}+\lambda^{48}+\cdots) \\ &= \frac{1}{(1-\lambda^8)(1-\lambda^{24})},\end{aligned} \tag{8}$$

which agrees with (5). So if we can find two algebraically independent invariants of degrees 8 and 24, we shall have solved our problem. The answer will be that any invariant of this group is a polynomial in θ and φ. We shall find θ and φ in the next section.

Notice how the exponents 8 and 24 in the denominator of (5) led us to guess the degrees of the basic invariants.

This behavior is typical, and is what makes the technique exciting to use. One starts with a group of matrices $\mathfrak{G}$, computes the complicated-looking sum shown in Eq. (3), and simplifies the result. Everything miraculously collapses, leaving a final expression resembling Eq. (5) (although not always quite so simple — the precise form of the final expression is given in Section E of Part III). This expression then tells you the degrees of the basic invariants to look for.

E. Finding the basic invariants. Finding the basic invariants is in general an easier problem than finding $\Phi(\lambda)$. There are two methods.

(a) *Finding invariants by averaging.* This method uses the following simple result (which is proved in Section B of Part II).

THEOREM 2. *If $f(\mathbf{x}) = f(x_1, \ldots, x_m)$ is any polynomial in m variables, and $\mathfrak{G}$ is a finite group of $m \times m$ matrices, then*

$$\bar{f}(\mathbf{x}) = \frac{1}{|\mathfrak{G}|} \sum_{A \in \mathfrak{G}} A \circ f(\mathbf{x})$$

is an invariant, where $A \circ f(\mathbf{x})$ denotes the polynomial obtained by applying the transformation A to the variables in f.

Of course $\bar{f}(\mathbf{x})$ may be zero. We shall give an example of the use of this theorem below. But in our present example the second method is easier to use.

(b) *The indirect method,* which is to use what we know about the problem to find invariants. In the present example we are studying self-dual codes with weights divisible by 4 (defined in Section B of Part II). Their weight enumerators satisfy Eqs. (1) and (2). There are two famous codes in this class, the extended Hamming code of length 8 and the extended Golay code of length 24 (codes C_6 and C_8 of Part II). The weight enumerators of these codes are respectively

$$\theta = x^8 + 14x^4y^4 + y^8 \tag{9}$$

and

$$\varphi' = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}. \tag{10}$$

Since the Hamming and Golay codes are self-dual, and have weights divisible by 4, these two polynomials must be invariant under Eqs. (1) and (2) and hence under the group $\mathfrak{G}_1$. So we have found the two basic invariants we were looking for. (It's not difficult to verify that they are algebraically independent.) Actually it is easier to work with

$$\varphi = \frac{\theta^3 - \varphi'}{42} = x^4y^4(x^4 - y^4)^4 \tag{10a}$$

rather than with φ'. So we have proved the following theorem, discovered by Gleason in 1970.

THEOREM 3a. *Any invariant of the group $\mathfrak{G}_1$ is a polynomial in θ (Eq. (9)) and φ (Eq. (10a)).*

This also gives us the solution to our original problem:

THEOREM 3b. *Any polynomial which satisfies Eqs. (1) and (2) is a polynomial in θ and φ.*

Finally, we have also obtained a very useful theorem about codes.

THEOREM 3c. (Gleason [**26**]) *The weight enumerator of any self-dual code, with weights divisible by 4, is a polynomial in θ and φ.*

Alternative proofs of this theorem are given in [**9**] and [**12**] (see also [**4**]). But the proof given here seems to be the most informative, and the easiest to understand and to generalize.

F. An application. To show how powerful Theorem 3c is, we shall use it to find the weight enumerator of the extended quadratic residue code of length 48 (the code C_9 of Part II).

All we need to know about this code is that it is self-dual, and that the weight of any nonzero codeword is a multiple of 4 and is at least 12 (i.e., this is a 5-error-correcting code). This implies that the weight enumerator of the code, which is a homogeneous polynomial of degree 48, has the form

$$W(x, y) = x^{48} + A_{12}x^{36}y^{12} + \cdots. \tag{11}$$

The coefficients of $x^{47}y, x^{46}y^2, \ldots, x^{37}y^{11}$ are zero. Here A_{12} is the unknown number of codewords of weight 12. It is remarkable that, once we know Eq. (11), the weight enumerator is completely determined by Th. 3c. For Th. 3c says that $W(x, y)$ must be a polynomial in θ and φ. Since $W(x, y)$ is homogeneous of degree 48, θ is homogeneous of degree 8, and φ is homogeneous of degree 24, this polynomial must be a linear combination of θ^6, $\theta^3\varphi$, and φ^2.

Thus Th. 3c says that

$$W(x, y) = a_0\theta^6 + a_1\theta^3\varphi + a_2\varphi^2 \tag{12}$$

for some real numbers a_0, a_1, a_2. Expanding Eq. (12) we have

$$\begin{aligned} W(x, y) = {} & a_0(x^{48} + 84x^{44}y^4 + 2946x^{40}y^8 + \cdots) \\ & + a_1(x^{44}y^4 + 38x^{40}y^8 + \cdots) \\ & + a_2(x^{40}y^8 - \cdots), \end{aligned} \tag{13}$$

and equating coefficients in Eqs. (11), (13) we get

$$a_0 = 1, \qquad a_1 = -84, \qquad a_2 = 246.$$

Therefore $W(x, y)$ is uniquely determined. When the values of a_0, a_1, a_2 are substituted in (12) it is found that

$$\begin{aligned} W(x, y) = {} & x^{48} + 17296x^{36}y^{12} + 535095x^{32}y^{16} \\ & + 3995376x^{28}y^{20} + 7681680x^{24}y^{24} + 3995376x^{20}y^{28} \\ & + 535095x^{16}y^{32} + 17296x^{12}y^{36} + y^{48}. \end{aligned} \tag{14}$$

Direct calculation of this weight enumerator would require finding the weight of each of the $2^{24} \approx 1.7 \times 10^7$ codewords, a respectable job even for a computer.

Of course there is also a fair amount of algebra involved in the invariant theory method, although in the preceding example it can be done by hand. The reader may find it helpful if we give a second example, in which the algebra can be shown in full.

G. A very simple example. The weight enumerator of a self-dual code with symbols from the field of q elements must satisfy the equation

$$W\left(\frac{x + (q-1)y}{\sqrt{q}}, \frac{x - y}{\sqrt{q}}\right) = W(x, y). \tag{15}$$

Problem: Find all polynomials which satisfy Eq. (15).

The solution proceeds as before. Equation (15) says that $W(x, y)$ must be invariant under the transformation

$$T_3\text{: replace } \begin{pmatrix} x \\ y \end{pmatrix} \text{ by } A\begin{pmatrix} x \\ y \end{pmatrix},$$

where

$$A = \frac{1}{\sqrt{q}}\begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix}. \tag{16}$$

Now $A^2 = I$, so $W(x, y)$ must be invariant under the group $\mathfrak{G}_2$ consisting of the two matrices I and A.

To find how many invariants there are, we compute the Molien series $\Phi(\lambda)$ from Eq. (3). We find

$$\det(I-\lambda I)=(1-\lambda)^2,$$

$$\det(I-\lambda A)=\det\begin{pmatrix}1-\frac{\lambda}{\sqrt{q}} & -\frac{q-1}{\sqrt{q}}\lambda\\ -\frac{\lambda}{\sqrt{q}} & 1+\frac{\lambda}{\sqrt{q}}\end{pmatrix}=1-\lambda^2,$$

$$\Phi(\lambda)=\frac{1}{2}\left(\frac{1}{(1-\lambda)^2}+\frac{1}{1-\lambda^2}\right) \tag{17}$$

$$=\frac{1}{(1-\lambda)(1-\lambda^2)},$$

which is even simpler than Eq. (5). Equation (17) suggests that there might be two basic invariants, of degrees 1 and 2 (the exponents in the denominator). If algebraically independent invariants of degrees 1 and 2 can be found, say g and h, then Eq. (17) implies that any invariant of $\mathfrak{G}_2$ is a polynomial in g and h.

This time we shall use the first method (averaging) to find the basic invariants. Let us average x over the group—i.e., apply Theorem 2 with $f(x, y)=x$. The matrix I leaves x unchanged, of course, and the matrix A transforms x into $(1/\sqrt{q})(x+(q-1)y)$. Therefore the average,

$$\bar{f}(x,y)=\frac{1}{2}\left[x+\frac{1}{\sqrt{q}}\{x+(q-1)y\}\right]$$

$$=\frac{(\sqrt{q}+1)\{x+(\sqrt{q}-1)y\}}{2\sqrt{q}},$$

is an invariant. Of course any scalar multiple of $\bar{f}(x, y)$ is also an invariant, so we may divide by $(\sqrt{q}+1)/2\sqrt{q}$ and take

$$g=x+(\sqrt{q}-1)y \tag{18}$$

to be the basic invariant of degree 1. To get an invariant of degree 2 we average x^2 over the group, obtaining

$$\frac{1}{2}\left[x^2+\frac{1}{q}\{x+(q-1)y\}^2\right].$$

This can be cleaned up by subtracting $((q+1)/2q)g^2$ (which of course is an invariant), and dividing by a suitable constant. The result is

$$h=y(x-y),$$

the desired basic invariant of degree 2.

Finally, g and h must be shown to be algebraically independent: it must be shown that no sum of the form

$$\sum_{i,j} c_{ij}g^ih^j, \quad c_{ij} \text{ complex and not all zero,} \tag{19}$$

is identically zero when expanded in powers of x and y. This can be seen by looking at the leading terms. (The leading term of a polynomial is the first one to be written down when using the natural ordering illustrated in Eqs. (9), (14), (18).) Thus the leading term of g is x, the leading term of h is xy,

and the leading term of $g^i h^j$ is $x^{i+j}y^j$. Since distinct summands in Eq. (19) have distinct leading terms, (19) can only add to zero if all the c_{ij} are zero. Therefore g and h are algebraically independent. So we have proved:

THEOREM 4. *Any invariant of the group $\mathfrak{G}_2$, or equivalently any polynomial satisfying* (15), *or equivalently the weight enumerator of any self-dual code with symbols from $GF(q)$, is a polynomial in $g = x + (\sqrt{q}-1)y$ and $h = y(x-y)$.*

At this point the coding theorist will cry "Stop!", and point out that a self-dual code must have even length and so every term in the weight enumerator must have even degree. But in Theorem 4 g has degree 1.

Thus we haven't made use of everything we know about the code. $W(x, y)$ must also be invariant under the transformation

$$\text{replace } \begin{pmatrix} x \\ y \end{pmatrix} \text{ by } B\begin{pmatrix} x \\ y \end{pmatrix},$$

where $B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$. This rules out terms of odd degree. So $W(x, y)$ is invariant under the group $\mathfrak{G}_3$ generated by A and B, which consists of

$$I,\ A,\ -I,\ -A.$$

The reader can easily work out that the new Molien series is

$$\begin{aligned} \Phi_{\mathfrak{G}_3}(\lambda) &= \frac{1}{2}\{\Phi_{\mathfrak{G}_2}(\lambda) + \Phi_{\mathfrak{G}_2}(-\lambda)\} \\ &= \frac{1}{2}\left\{\frac{1}{(1-\lambda)(1-\lambda^2)} + \frac{1}{(1+\lambda)(1-\lambda^2)}\right\} \\ &= \frac{1}{(1-\lambda^2)^2}. \end{aligned} \tag{20}$$

There are now two basic invariants, both of degree 2 (matching the exponents in the denominator of (20)), say g^2 and h, or the equivalent and slightly simpler pair $g^* = x^2 + (q-1)y^2$ and $h = y(x-y)$. Hence:

THEOREM 5. ([**41**]) *The weight enumerator of any self-dual code with symbols from the field of q elements is a polynomial in g^* and h.*

The preceding argument enables us to give a short proof of a recent result of Leontjev.

COROLLARY. (Leontjev [**35**]) *The weight enumerator $W(x, y)$ of a linear code over the field of q elements has the property that*

$$W(x, y)\, W\left(\frac{x + (q-1)y}{\sqrt{q}}, \frac{x-y}{\sqrt{q}}\right)$$

is a polynomial in g^* and h.

Proof. This product is clearly invariant under T_3 and $-I$, and so the result follows from the proof of Th. 5. Q.E.D.

H. The general plan of attack. As these examples have illustrated, there are two stages in using invariant theory to solve a problem.

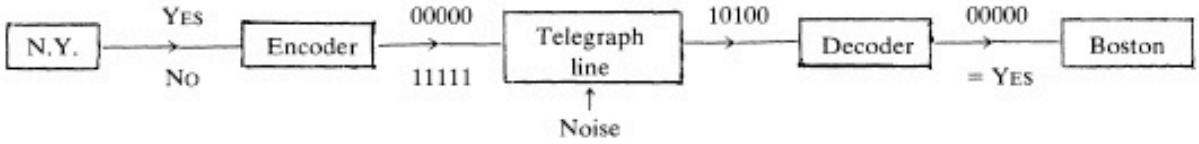
Stage I: Convert the assumptions about the problem (e.g., the code) into algebraic constraints on polynomials (e.g., weight enumerators).

Stage II: Use invariant theory to find all possible polynomials satisfying these constraints.

J. Arrangement of the paper. Part I has been devoted to explication by example. Part II gives the necessary background from coding theory, defines codes and weight enumerators, and explains why they are important. Part III is the main section of the paper and gives a brief account of invariant theory. Then Part IV gives further examples and illustrates more advanced techniques.

II. Background from Coding Theory

A. Definition of a code and examples. Imagine a noisy telegraph line from New York to Boston, which transmits 0's and 1's. Usually when a 0 is sent from New York it is received as a 0 in Boston, but occasionally a 0 is received as a 1. Similarly a 1 is occasionally received as a 0. The problem is to send a lot of important messages down this line, as quickly and as reliably as possible. The coding theorist's solution is to send only certain strings of 0's and 1's, called *codewords*. Here is a simple example: one of two messages will be sent, either YES or NO.



YES will be *encoded* into the codeword 00000, and NO into 11111. Suppose 10100 is received in Boston. The receiver argues that it is more likely that 00000 was sent (and two errors occurred) than that 11111 was sent (and three errors occurred), and therefore *decodes* 10100 as 00000 = YES. For in some sense 10100 is *closer* to 00000 than to 11111. To make this precise, define the *Hamming distance* (or simply the *distance*) between two vectors $\mathbf{u} = (u_1, \ldots, u_n)$ and $\mathbf{v} = (v_1, \ldots, v_n)$ to be the number of places where $u_i \neq v_i$. This is denoted by $\operatorname{dist}(\mathbf{u}, \mathbf{v})$. E.g., $\operatorname{dist}(10100, 00000) = 2$, $\operatorname{dist}(10100, 11111) = 3$, and even $\operatorname{dist}(0122, 2001) = 4$ (the same definition applies to nonbinary vectors). It is easily checked that dist is a metric. Then the receiver should decode the received vector as the closest codeword, measured in Hamming distance.

Notice in this example two errors were corrected. This is possible because the codewords 00000 and 11111 are at distance 5 apart. In general, if d is the minimum Hamming distance between codewords, the code can correct $e = [\frac{1}{2}(d-1)]$ errors, where $[x]$ denotes the greatest integer not exceeding x. For if e or fewer errors occur, by the triangle inequality the received vector is still closer to the transmitted codeword than to any other. This motivates the

DEFINITION. An $[n, k, d]$ binary *code* consists of 2^k vectors $\mathbf{u} = (u_1, \ldots, u_n)$, $u_i \in F_2 = \{0, 1\}$, called *codewords*, such that

(i) the sum, taken componentwise and modulo 2 (without carries!), of any two codewords is again a codeword; and

(ii) any two codewords differ in at least d places.

Then n is called the *length*, k the *dimension*, and d the *minimum distance* of the code. In a good code n is small (for rapid transmission), k is large (for an efficient code), and d is large (to correct many errors). These are incompatible goals! For more about codes see for example [**7**], [**8**], [**10**], [**36**], [**37**], [**42**], [**55**].

Examples:

(1) $C_1 = \{00000, 11111\}$, the code of the example, is a $[5, 1, 5]$ code.

(2) More generally $C_2 = \{00\ldots0, 11\ldots1\}$ is an $[n, 1, n]$ *repetition* code.

(3) $C_3 = \{000, 011, 101, 110\}$ is a $[3, 2, 2]$ code. To verify this, note that each of the 4 codewords has 3 components. Also the sum of the codewords 011 and 101 (for example) is 110. Finally any two codewords differ in at least (in this case exactly) two coordinates.

(4) C_4, a $[7, 3, 4]$ code:

0000000
1110100
0111010
0011101
1001110
0100111
1010011
1101001

(5) C_5, a $[7, 4, 3]$ Hamming code, consists of the codewords of C_4 together with their complements:

0000000	1111111
1110100	0001011
0111010	1000101
0011101	1100010
1001110	0110001
0100111	1011000
1010011	0101100
1101001	0010110

(6) C_6, an $[8, 4, 4]$ extended Hamming code, formed by placing a 1 at the end of the 8 codewords on the left in C_5, and a 0 at the end of the 8 codewords on the right. (This is one of the codes mentioned in Part I, Section E.) The same technique can be applied to any $[n, k, d$ odd$]$ code. Placing a 1 at the end of the codewords containing an odd number of 1's and a 0 at the end of those with an even number of 1's we obtain an $[n+1, k, d+1]$ *extended* code.

For later use we mention a few important larger codes, although without giving any details.

(7) The two binary Golay codes, namely the $[23, 12, 7]$ code C_7 and the $[24, 12, 8]$ extended code C_8 ([**28**], [**29**]).

(8) The codes C_5 and C_7 are both examples of *quadratic residue* codes ([**5**], [**6**]). This is an infinite family of codes. Other quadratic residue codes are the $[31, 16, 7]$ code, the $[47, 24, 11]$ code, and the $[48, 24, 12]$ extended code C_9.

There are many situations in which it is better to use a nonbinary code. Let F_q denote the Galois field with q elements. E.g., $F_3 = \{0, 1, 2\}$ with addition, multiplication, division etc., performed modulo 3.

DEFINITION. An $[n, k, d]$ code over F_q consists of q^k codewords $(u_1, \ldots, u_n)$, which have Hamming distance at least d apart and form a linear space. That is, the sum, performed componentwise in F_q, of any two codewords is again a codeword, and any scalar multiple $(cu_1, \ldots, cu_n)$, $c \in F_q$, of a codeword is again a codeword.

Examples:

(1) C_{10}, a $[4, 2, 2]$ code over F_3:

0000	1120	2102
0111	2210	2021
0222	1201	1012

(10) There is also a $[12, 6, 6]$ Golay code C_{11} over F_3—see [**28**], [**29**].

B. Dual code. Let $\mathscr{C}$ be an $[n, k, d]$ code over F_q. The *dual* (or *orthogonal*) code $\mathscr{C}^\perp$ consists of all vectors having zero dot product (in F_q) with every codeword of $\mathscr{C}$. Thus

$$\mathscr{C}^{\perp} = \Big\{(u_1, \ldots, u_n)\colon u \cdot v = \sum_{i=1}^{n} u_i v_i = 0 \quad \text{for all } v = (v_1, \ldots, v_n) \in \mathscr{C}\Big\}.$$

Then it is easy to see that $\mathscr{C}^{\perp}$ is an $[n, n-k, d']$ code, for some positive integer d'.

Examples: The binary code $\{00, 11\}$ is its own dual! The dual of C_2 is the $[n, n-1, 2]$ code consisting of all codewords with an even number of 1's. The dual of C_3 is $\{000, 111\}$, and C_4 and C_5 are dual to each other. (It is an amusing and informative exercise to verify these facts.)

A *self-dual* code is one for which $\mathscr{C}^{\perp} = \mathscr{C}$. The examples $C_6, C_8, C_9, C_{10}, C_{11}$ are all self-dual.

In a self-dual code k must be equal to $\frac{1}{2}n$, and so n must be even.

Self-dual codes are a particularly interesting class, for several reasons:

(1) It is known that there exist self-dual codes which are about as good as any code can be — more precisely, they meet the Gilbert–Varshamov bound **[44]**, **[60]**.

(2) A number of the best codes known are self-dual. For example, extended quadratic residue codes are self-dual whenever the length is of the form $n = 8m$ where $8m - 1$ is a prime.

(3) Since the codewords of the dual code $\mathscr{C}^{\perp}$ are parity check equations on $\mathscr{C}$, knowing that $\mathscr{C} = \mathscr{C}^{\perp}$ may simplify the decoding procedure (see for example **[27]**).

(4) The codewords in a self-dual code under certain conditions form t-designs, and many 5-designs have been constructed in this way (see **[3]**, **[4]**, **[56]**, **[57]**).

(5) There are connections between self-dual codes and sphere-packings, geometric lattices, large finite groups, and projective planes — see **[3]**, **[4]**, **[12]**, **[15]**–**[17]**, **[34]**, **[42]**, **[45]**, **[67]**.

Binary self-dual codes of length $n \leqq 24$ have been classified in **[58]**, **[61]**, **[62]**. See also **[24]**, **[50]**, **[59]**.

C. Weight enumerators. Examples (5)–(8) should have convinced the reader that codes are large, unwieldly objects. One way of handling a code and extracting some useful information from it is by means of its weight enumerator.

The *Hamming weight* (or simply the *weight*) of a vector $\mathbf{u} = (u_1, \ldots, u_n)$ is the number of nonzero u_i. This is denoted by $\mathrm{wt}(\mathbf{u})$. E.g., $\mathrm{wt}(1101000) = 3$, $\mathrm{wt}(1201) = 3$. Clearly $\mathrm{dist}(\mathbf{u}, \mathbf{v}) = \mathrm{wt}(\mathbf{u} - \mathbf{v})$. Since a code $\mathscr{C}$ is a linear space, for any codewords $\mathbf{u}, \mathbf{v}$, $\mathrm{dist}(\mathbf{u}, \mathbf{v}) = \mathrm{wt}(\mathbf{u} - \mathbf{v}) = \mathrm{wt}(\mathbf{w})$ for some $\mathbf{w} \in \mathscr{C}$. Therefore the minimum distance d between codewords is equal to the smallest weight of any nonzero codeword.

The weight enumerator of an $[n, k, d]$ code $\mathscr{C}$ is simply a polynomial which tells the number of codewords of each weight. If $\mathscr{C}$ contains A_i codewords of weight i, then the *weight enumerator* of $\mathscr{C}$ is defined to be

$$W_{\mathscr{C}}(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i, \tag{21}$$

where x and y are indeterminates. Stated another way,

$$W_{\mathscr{C}}(x, y) = \sum_{\mathbf{u} \in \mathscr{C}} x^{n - \mathrm{wt}(\mathbf{u})} y^{\mathrm{wt}(\mathbf{u})}. \tag{22}$$

Equations (21) and (22) are complicated-looking definitions for a very simple idea, which some examples will make clear.

(23)

Code $\mathscr{C}$	*Weight Enumerator* $W_{\mathscr{C}}(x, y)$
$\{00, 11\}$	$x^2 + y^2$
C_2	$x^n + y^n$
C_3	$x^3 + 3xy^2$

(24)	C_4	$x^7+7x^3y^4$
	C_5	$x^7+7x^4y^3+7x^3y^4+y^7$
(9)	C_6	$\theta=x^8+14x^4y^4+y^8$
(25)	C_7	x^4+8xy^3

For example, the weight enumerator of C_4 is $x^7+7x^3y^4$ because there is one codeword with 7 zeros (giving the term x^7) and 7 codewords with 3 zeros and 4 ones (giving the term $7x^3y^4$). The weight enumerators of C_8 and C_9 were given in Eqs. (10) and (14).

Notice that $W_{\mathscr{C}}(x, y)$ is a homogeneous polynomial of degree n. The weight enumerator immediately gives the minimum distance d of $\mathscr{C}$. For $\mathscr{C}$ always contains the zero codeword, giving the leading term x^n in $W_{\mathscr{C}}(x, y)$, and the next nonzero term is $A_d x^{n-d}y^d$. Thus

$$W_{\mathscr{C}}(x, y)=x^n+0x^{n-1}y+\cdots+0x^{n-d+1}y^{d-1}+A_dx^{n-d}y^d+\cdots.$$

An illustration was given in Eq. (11). $W_{\mathscr{C}}$ is also used to find the error probability of the code, and for other purposes—see [7] or [42].

D. MacWilliams theorem. For a large code it is in general a very tough problem to find the weight enumerator. One of the chief weapons available is the following remarkable theorem of F. J. MacWilliams, which states that the weight enumerator of the dual code $\mathscr{C}^\perp$ is uniquely determined by the weight enumerator of $\mathscr{C}$.

THEOREM 6. (MacWilliams [40]; see also [42], [43]). *If $\mathscr{C}$ is an $[n, k, d]$ code over F_q with dual code $\mathscr{C}^\perp$, then*

$$W_{\mathscr{C}^\perp}(x, y)=\frac{1}{q^k}W_{\mathscr{C}}(x+(q-1)y, x-y). \tag{26}$$

We shall just prove the binary version, when $q=2$. This states that

$$W_{\mathscr{C}^\perp}(x, y)=\frac{1}{2^k}W_{\mathscr{C}}(x+y, x-y), \tag{27}$$

or equivalently

$$\sum_{\mathbf{u}\in\mathscr{C}^\perp}x^{n-\mathrm{wt}(\mathbf{u})}y^{\mathrm{wt}(\mathbf{u})}=\frac{1}{2^k}\sum_{\mathbf{u}\in\mathscr{C}}(x+y)^{n-\mathrm{wt}(\mathbf{u})}(x-y)^{\mathrm{wt}(\mathbf{u})}. \tag{28}$$

The proof depends on the following lemma, which is in fact a version of the Poisson summation formula [23, p. 220]. Let F^n denote the set of all binary vectors of length n.

LEMMA 7. ([37]). *Let f be any mapping defined on F^n. We must be able to add and subtract the values $f(\mathbf{u})$, but otherwise f can be arbitrary. The* ***Hadamard transform*** *of f, $\hat{f}$, is defined by*

$$\hat{f}(\mathbf{u})=\sum_{\mathbf{v}\in F^n}(-1)^{\mathbf{u}\cdot\mathbf{v}}f(\mathbf{v}), \qquad \mathbf{u}\in F^n. \tag{29}$$

Then if $\mathscr{C}$ is an $[n, k, d]$ binary code

$$\sum_{\mathbf{u}\in\mathscr{C}^\perp}f(\mathbf{u})=\frac{1}{2^k}\sum_{\mathbf{u}\in\mathscr{C}}\hat{f}(\mathbf{u}). \tag{30}$$

Proof.

$$\sum_{\mathbf{u}\in\mathscr{C}}\hat{f}(\mathbf{u})=\sum_{\mathbf{u}\in\mathscr{C}}\sum_{\mathbf{v}\in F^n}(-1)^{\mathbf{u}\cdot\mathbf{v}}f(\mathbf{v})=\sum_{\mathbf{v}\in F^n}f(\mathbf{v})\sum_{\mathbf{u}\in\mathscr{C}}(-1)^{\mathbf{u}\cdot\mathbf{v}}.$$

Now if $\mathbf{v}\in\mathscr{C}^\perp$, $\mathbf{u}\cdot\mathbf{v}$ is always zero, and the inner sum is 2^k. But if $\mathbf{v}\notin\mathscr{C}^\perp$ then a moment's thought

shows that $\mathbf{u}\cdot\mathbf{v}$ is 0 and 1 equally often, and the inner sum is 0. Therefore

$$\sum_{\mathbf{u}\in\mathscr{C}} \hat{f}(\mathbf{u}) = 2^k \sum_{\mathbf{v}\in\mathscr{C}^\perp} f(\mathbf{v}). \qquad \text{Q.E.D.}$$

Proof of Theorem 6. We apply the lemma with

$$f(\mathbf{u}) = x^{n-\mathrm{wt}(\mathbf{u})} y^{\mathrm{wt}(\mathbf{u})},$$

$$\hat{f}(\mathbf{u}) = \sum_{\mathbf{v}\in F^n} (-1)^{\mathbf{u}\cdot\mathbf{v}} x^{n-\mathrm{wt}(\mathbf{v})} y^{\mathrm{wt}(\mathbf{v})}. \tag{31}$$

Let $\mathbf{u} = (u_1 \cdots u_n)$, $\mathbf{v} = (v_1 \cdots v_n)$. Then

$$\begin{aligned}\hat{f}(\mathbf{u}) &= \sum_{\mathbf{v}\in F^n} (-1)^{u_1v_1+\cdots+u_nv_n} \prod_{i=1}^{n} x^{1-v_i} y^{v_i} \\ &= \sum_{v_1=0}^{1} \cdots \sum_{v_n=0}^{1} \prod_{i=1}^{n} (-1)^{u_iv_i} x^{1-v_i} y^{v_i}.\end{aligned} \tag{32}$$

Just as

$$a_0b_0c_0 + a_0b_0c_1 + a_0b_1c_0 + a_0b_1c_1 + a_1b_0c_0 + a_1b_0c_1 + a_1b_1c_0 + a_1b_1c_1$$

is equal to $(a_0 + a_1)(b_0 + b_1)(c_0 + c_1)$, so (32) is equal to

$$\prod_{i=1}^{n} \sum_{w=0}^{1} (-1)^{u_iw} x^{1-w} y^{w}.$$

If $u_i = 0$, the inner sum is $x + y$. If $u_i = 1$, it is $x - y$. Thus

$$\hat{f}(\mathbf{u}) = (x+y)^{n-\mathrm{wt}(\mathbf{u})}(x-y)^{\mathrm{wt}(\mathbf{u})}. \tag{33}$$

Then Eq. (30) reads

$$\sum_{\mathbf{u}\in\mathscr{C}^\perp} x^{n-\mathrm{wt}(\mathbf{u})} y^{\mathrm{wt}(\mathbf{u})} = \frac{1}{2^k} \sum_{\mathbf{u}\in\mathscr{C}} (x+y)^{n-\mathrm{wt}(\mathbf{u})}(x-y)^{\mathrm{wt}(\mathbf{u})},$$

which is Eq. (28). Q.E.D.

Examples: Let us illustrate Th. 6 by applying it to the code $\mathscr{C} = C_3$ with weight enumerator $W_{C_3}(x, y) = x^3 + 3xy^2$. Then

$$\tfrac{1}{4} W_{C_3}(x+y, x-y) = \tfrac{1}{4}\{(x+y)^3 + 3(x+y)(x-y)^2\} = x^3 + y^3,$$

which is indeed the weight enumerator of the dual code $C_3^\perp = \{000, 111\}$.

Of course if $\mathscr{C}$ is a self-dual code, both sides of Eqs. (26) and (27) must be the same. For example, if $\mathscr{C} = \{00, 11\}$, $W_{\mathscr{C}}(x, y) = x^2 + y^2$, and

$$\begin{aligned}\tfrac{1}{2} W_{\mathscr{C}}(x+y, x-y) &= \tfrac{1}{2}\{(x+y)^2 + (x-y)^2\} \\ &= x^2 + y^2 = W_{\mathscr{C}}(x, y)\end{aligned}$$

which is correct since $\mathscr{C}$ is self-dual. This is an illustration of

COROLLARY 8. *If $\mathscr{C}$ is an $[n, \frac{1}{2}n, k]$ self-dual code over F_q, then*

$$W_{\mathscr{C}}(x, y) = \frac{1}{q^{n/2}} W_{\mathscr{C}}(x + (q-1)y, x - y).$$

Since $W_{\mathscr{C}}(x, y)$ is a homogeneous polynomial of degree n.we can write this as

$$W_\epsilon(x, y) = W_\epsilon\left(\frac{x+(q-1)y}{\sqrt{q}}, \frac{x-y}{\sqrt{q}}\right). \tag{34}$$

We have already used this fact in Part I, Section G, where we pointed out that (34) implies that $W_\epsilon(x, y)$ is *invariant* under a certain linear transformation. This brings us to the main part of the paper.

III. Invariant Theory

A. Groups of matrices. Throughout this paper the letters $\mathfrak{G}, \mathfrak{H}, \ldots$ denote finite groups of complex $m \times m$ matrices. We remind the reader that the statement "$\mathfrak{G}$ is a group of matrices" means that $\mathfrak{G}$ is set of invertible matrices with the following properties: if A and B are in $\mathfrak{G}$ so is the product AB; the unit matrix I is in $\mathfrak{G}$; and the inverse A^{-1} of every $A \in \mathfrak{G}$ is also in $\mathfrak{G}$. The number of matrices in $\mathfrak{G}$ is called its *order* and will be denoted by g.

Given a collection $A_1, \ldots, A_r$ of $m \times m$ matrices we can form a group $\mathfrak{G}$ from them by multiplying them together in all possible ways. Thus $\mathfrak{G}$ contains the matrices I, A_1, $A_2, \ldots$, $A_1A_2, \ldots$, $A_2A_1^{-1}A_2^{-1}A_3, \ldots$. We say that $\mathfrak{G}$ is *generated* by $A_1, \ldots, A_r$. Of course $\mathfrak{G}$ may be infinite, in which case the theory of invariants described here doesn't directly apply. (But see [20], [63], [74].)

Example: Let us show that the group $\mathfrak{G}_1$ generated by the matrices

$$M = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ and } J = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

that was encountered in Section B of Part I does indeed have order 192. The key is to discover (by randomly multiplying matrices together) that $\mathfrak{G}_1$ contains

$$J^2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad E = (MJ)^3 = \frac{1+i}{\sqrt{2}}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$E^2 = -i\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad R = MJ^2M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Set $\eta = (1+i)/\sqrt{2} = \cos 45° + i \sin 45°$. Then $\mathfrak{G}_1$ contains the 16 matrices

$$\alpha\begin{pmatrix} 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \qquad \alpha\begin{pmatrix} 0 & 1 \\ \pm 1 & 0 \end{pmatrix}, \qquad \alpha \in \{1, i, -1, -i\},$$

which form a subgroup $\mathfrak{H}_1$. From this it is easy to see that $\mathfrak{G}_1$ consists of the union of $\mathfrak{H}_1$ and 11 *cosets* $a_k\mathfrak{H}_1 = \{a_kA : A \in \mathfrak{H}_1\}$. Thus

$$\mathfrak{G}_1 = \bigcup_{k=1}^{12} a_k\mathfrak{H}_1, \tag{35}$$

where $a_1, \ldots, a_6$ are respectively

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \ \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \ \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}, \ \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}, \ \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix},$$

and $a_7 = \eta a_1, \ldots, a_{12} = \eta a_6$. From this it is possible to obtain a list of all 192 matrices in $\mathfrak{G}_1$—they are the matrices

$$\eta^\nu\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}, \quad \eta^\nu\begin{pmatrix} 0 & 1 \\ \alpha & 0 \end{pmatrix}, \quad \eta^\nu\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & \beta \\ \alpha & -\alpha\beta \end{pmatrix}, \tag{36}$$

for $0 \leqq \nu \leqq 7$ and $\alpha, \beta \in \{1, i, -1, -i\}$.

As a check, one verifies that every matrix in (36) can be written as a product of M's and J's; that

the product of two matrices in (36) is again in (36); and that the inverse of every matrix in (36) is in (36). Therefore (36) *is* a group, and is the group generated by M and J. Thus $\mathfrak{G}_1$ is indeed equal to (36).

We have gone into this example in some detail to emphasize that it is important to begin by understanding the group thoroughly. (For an alternative way of studying $\mathfrak{G}_1$ see [**12**; pp. 160–161].)

B. Invariants. To quote Hermann Weyl [**73**], "the theory of invariants came into existence about the middle of the nineteenth century somewhat like Minerva: a grown-up virgin, mailed in the shining armor of algebra, she sprang forth from Cayley's Jovian head." Invariant theory became one of the main branches of nineteenth century mathematics, but dropped out of fashion after Hilbert's work: see [**25**], [**64**]. Recently, however, there has been a resurgence of interest, with applications in algebraic geometry [**20**], [**53**], physics (see for example [**1**] and the references given there), combinatorics [**22**], [**65**], and coding theory [**41**], [**48**], [**49**].

There are several different kinds of invariants, but in this paper an invariant is defined as follows.

Let $\mathfrak{G}$ be a group of g $m \times m$ complex matrices $A_1, \ldots, A_g$, where the (i, k)th entry of A_α is $a_{ik}^{(\alpha)}$. In other words, $\mathfrak{G}$ is a group of linear transformations on the variables $x_1, \ldots, x_m$, consisting of the transformations

$$T^{(\alpha)}\text{: replace } x_i \text{ by } x_i^{(\alpha)} = \sum_{k=1}^{m} a_{ik}^{(\alpha)} x_k, \quad i = 1, \ldots, m \tag{37}$$

for $\alpha = 1, 2, \ldots, g$. It is worthwhile giving a careful description of how a polynomial $f(\mathbf{x}) = f(x_1, \ldots, x_m)$ is transformed by a matrix A_α in $\mathfrak{G}$. The transformed polynomial is

$$A_\alpha \circ f(\mathbf{x}) = f(x_1^{(\alpha)}, \ldots, x_m^{(\alpha)}),$$

where each $x_i^{(\alpha)}$ is replaced by $\sum_{k=1}^{m} a_{ik}^{(\alpha)} x_k$. Another way of describing this is to think of $\mathbf{x} = (x_1, \ldots, x_m)^T$ as a column vector (where the T denotes transpose). Then $f(\mathbf{x})$ is transformed into

$$A_\alpha \circ f(\mathbf{x}) = f(A_\alpha \mathbf{x}), \tag{38}$$

where $A_\alpha \mathbf{x}$ is the usual product of a matrix and a vector. One can check that

$$B \circ (A \circ f(\mathbf{x})) = (AB) \circ f(\mathbf{x}) = f(AB\mathbf{x}). \tag{39}$$

For example, $A = \left(\begin{smallmatrix} 1 & 2 \\ 0 & -1 \end{smallmatrix}\right)$ transforms $x_1^2 + x_2$ into $(x_1 + 2x_2)^2 - x_2$.

DEFINITION. An *invariant* of $\mathfrak{G}$ is a polynomial $f(\mathbf{x})$ which is unchanged by every linear transformation in $\mathfrak{G}$. In other words, $f(\mathbf{x})$ is an invariant of $\mathfrak{G}$ if

$$A_\alpha \circ f(\mathbf{x}) = f(A_\alpha \mathbf{x}) = f(\mathbf{x})$$

for all $\alpha = 1, \ldots, g$.

Example: Let

$$\mathfrak{G}_4 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\},$$

a group of order $g = 2$. Then x^2, xy and y^2 are homogeneous invariants of degree 2.

Even if $f(\mathbf{x})$ isn't an invariant, its average over the group is, as was mentioned in Section E of Part I.

THEOREM 2. *Let $f(\mathbf{x})$ be any polynomial. Then*

$$\bar{f}(\mathbf{x}) = \frac{1}{g} \sum_{\alpha=1}^{g} A_\alpha \circ f(\mathbf{x}) \tag{40}$$

is an invariant of $\mathfrak{G}$.

Proof. Any $A_\beta \in \mathfrak{G}$ transforms the right-hand side of (40) into

$$\frac{1}{g}\sum_{\alpha=1}^{g} (A_\alpha A_\beta)\circ f(\mathbf{x}), \quad \text{by (39).} \tag{41}$$

It is an easy exercise in group theory to see that as A_α runs through $\mathfrak{G}$, so does $A_\alpha A_\beta$, if A_β is fixed. Therefore (41) is equal to

$$\frac{1}{g}\sum_{\gamma=1}^{g} A_\gamma \circ f(\mathbf{x})$$

which is $\bar{f}(\mathbf{x})$. Therefore $\bar{f}(\mathbf{x})$ is an invariant. Q.E.D.

More generally, any symmetric function of the g polynomials $A_1 \circ f(\mathbf{x}), \ldots, A_g \circ f(\mathbf{x})$ is an invariant of $\mathfrak{G}$.

Clearly if $f(\mathbf{x})$ and $h(\mathbf{x})$ are invariants of $\mathfrak{G}$, so are $f(\mathbf{x}) + h(\mathbf{x})$, $f(\mathbf{x})h(\mathbf{x})$, and $cf(\mathbf{x})$ (c complex). This is equivalent to saying that the set of invariants of $\mathfrak{G}$, which we denote by $\mathcal{I}(\mathfrak{G})$, forms a *ring*.

One of the main problems of invariant theory is to describe $\mathcal{I}(\mathfrak{G})$. Since the transformations in $\mathfrak{G}$ don't change the degree of a polynomial, it is enough to describe the homogeneous invariants (for any invariant is a sum of homogeneous invariants).

C. Basic invariants. Our goal is to find a "basis" for the invariants of $\mathfrak{G}$, that is, a set of basic invariants such that any invariant can be expressed in terms of this set. There are three different types of bases one might look for.

DEFINITION. Polynomials $f_1(\mathbf{x}), \ldots, f_r(\mathbf{x})$ are called *algebraically dependent* if there is a polynomial p in r variables with complex coefficients, not all zero, such that $p(f_1(\mathbf{x}), \ldots, f_r(\mathbf{x})) \equiv 0$. Otherwise $f_1(\mathbf{x}), \ldots, f_r(\mathbf{x})$ are called *algebraically independent.* A fundamental result from algebra is:

THEOREM 9 [**32**, p. 154]. *Any $m+1$ polynomials in m variables are algebraically dependent.*

The first type of basis we might look for is a set of m algebraically independent invariants $f_1(\mathbf{x}), \ldots, f_m(\mathbf{x})$. Such a set is indeed a "basis", for by Th. 9 any invariant is algebraically dependent on $f_1, \ldots, f_m$ and so is a root of a polynomial equation in $f_1, \ldots, f_m$. The following theorem guarantees the existence of such a basis.

THEOREM 10 [**14**, p. 357]. *There always exist m algebraically independent invariants of $\mathfrak{G}$.*

Proof. Consider the polynomial $\prod_{\alpha=1}^{g}(t - A_\alpha \circ x_1)$ in the variables $t, x_1, \ldots, x_m$. Since one of the A_α is the identity matrix, $t = x_1$ is a zero of this polynomial. When the polynomial is expanded in powers of t, the coefficients are invariants by the remark immediately following the proof of Th. 2. Therefore x_1 is an algebraic function of invariants. Similarly each of $x_2, \ldots, x_m$ is an algebraic function of invariants. Now if the number of algebraically independent invariants were m' ($< m$), the m independent variables $x_1, \ldots, x_m$ would be algebraic functions of the m' invariants, a contradiction. Therefore the number of algebraically independent invariants is at least m. By Th. 9 this number cannot be greater than m. Q.E.D.

Example: For the preceding group $\mathfrak{G}_4$, we may take $f_1 = (x+y)^2$ and $f_2 = (x-y)^2$ as the algebraically independent invariants. Then any invariant is a root of a polynomial equation in f_1 and f_2. For example,

$$x^2 = \tfrac{1}{4}(\sqrt{f_1} + \sqrt{f_2})^2, \quad xy = \tfrac{1}{4}(f_1 - f_2),$$

and so on.

The second type of basis, whose existence is guaranteed by the next theorem, is easier to work with.

THEOREM 11 [**14**, p. 359]. *There always exist $m+1$ invariants $f_1, \ldots, f_{m+1}$ of $\mathfrak{G}$ such that any invariant of $\mathfrak{G}$ is a rational function in $f_1, \ldots, f_{m+1}$, i.e., is the ratio of two polynomials in $f_1, \ldots, f_{m+1}$.*

Example: For $\mathfrak{G}_4$, x^2, xy and y^2 form such a basis.

However, by far the most convenient description of the invariants is a set $f_1, \ldots, f_l$ of invariants with the property that any invariant is a *polynomial* in $f_1, \ldots, f_l$. Then $f_1, \ldots, f_l$ is called a *polynomial basis* (or an *integrity basis*) for the invariants of $\mathfrak{G}$. Of course if $l > m$, then by Th. 9 there will be polynomial equations, called *syzygies*, relating $f_1, \ldots, f_l$.

For example, $f_1 = x^2$, $f_2 = xy$, $f_3 = y^2$ form a polynomial basis for the invariants of $\mathfrak{G}_4$. The syzygy relating them is $f_1 f_3 - f_2^2 = 0$. The existence of a polynomial basis, and a method of finding it, is given by the next theorem.

THEOREM 12 (Noether [**54**]; see also Weyl [**74**, p. 275]). *The ring of invariants of a finite group $\mathfrak{G}$ of complex $m \times m$ matrices has a polynomial basis consisting of not more than $\binom{m+g}{m}$ invariants, of degree not exceeding g, where g is the order of $\mathfrak{G}$. Furthermore, this basis may be obtained by taking the average over $\mathfrak{G}$ of all monomials*

$$x_1^{b_1} x_2^{b_2} \cdots x_m^{b_m}$$

of total degree Σb_i not exceeding g.

Proof. Let the group $\mathfrak{G}$ consist of the transformations (37). Suppose

$$f(x_1, \ldots, x_m) = \sum_{\mathbf{e}} c_{\mathbf{e}} x_1^{e_1} \cdots x_m^{e_m}, \qquad c_{\mathbf{e}} \text{ complex},$$

is any invariant of $\mathfrak{G}$. (The sum extends over all $\mathbf{e} = e_1, \ldots, e_m$ for which there is a nonzero term $x_1^{e_1} \cdots x_m^{e_m}$ in $f(x_1, \ldots, x_m)$.) Since $f(x_1, \ldots, x_m)$ is an invariant, it is unchanged when we average it over the group, so

$$\begin{aligned} f(x_1, \ldots, x_m) &= \frac{1}{g}\{f(x_1^{(1)}, \ldots, x_m^{(1)}) + \cdots + f(x_1^{(g)}, \ldots, x_m^{(g)})\} \\ &= \frac{1}{g} \sum_{\mathbf{e}} c_{\mathbf{e}}\{(x_1^{(1)})^{e_1} \cdots (x_m^{(1)})^{e_m} + \cdots \\ &\quad \cdots + (x_1^{(g)})^{e_1} \cdots (x_m^{(g)})^{e_m}\} = \frac{1}{g} \sum_{\mathbf{e}} c_{\mathbf{e}} J_{\mathbf{e}} \qquad \text{(say)}. \end{aligned}$$

Every invariant is therefore a linear combination of the (infinitely many) special invariants

$$J_{\mathbf{e}} = \sum_{\alpha=1}^{g} (x_1^{(\alpha)})^{e_1} \cdots (x_m^{(\alpha)})^{e_m}.$$

Now $J_{\mathbf{e}}$ is (apart from a constant factor) the coefficient of $u_1^{e_1} \cdots u_m^{e_m}$ in

$$S_e = \sum_{\alpha=1}^{g} (u_1 x_1^{(\alpha)} + \cdots + u_m x_m^{(\alpha)})^e,$$

where $e = e_1 + \cdots + e_m$. In other words, the S_e are the *power sums* of the g quantities

$$u_1 x_1^{(1)} + \cdots + u_m x_m^{(1)}, \ldots, u_1 x_1^{(g)} + \cdots + u_m x_m^{(g)}.$$

It is well known [**33**] that any power sum S_e, $e = 1, 2, \ldots$, can be written as a polynomial with rational coefficients in the first g power sums

$$S_1, S_2, \ldots, S_g.$$

Therefore any $J_{\mathbf{e}}$ for $e = \Sigma_{i=1}^{m} e_i > g$ (which is a coefficient of S_e) can be written as a polynomial in the

special invariants

$$J_e \text{ with } e_1 + \cdots + e_m \leqq g$$

(which are the coefficients of $S_1, \ldots, S_g$). Thus any invariant can be written as a polynomial in the J_e with $\Sigma_{i=1}^m e_i \leqq g$. The number of such J_e is the number of $e_1 e_2 \cdots e_m$ with $e_i \geqq 0$ and $e_1 + \cdots + e_m \leqq g$, which is $\binom{m+g}{m}$. Finally $\deg J_e \leqq g$, and J_e is obtained by averaging $x_1^{e_1} \cdots x_m^{e_m}$ over the group. Q.E.D.

D. Molien's theorem. Since we know from Th. 12 that a polynomial basis always exists, we can go ahead with confidence and try to find it, using the methods described in Section E of Part I. To discover when a basis has been found, we use Molien's theorem (Theorem 1 above). This states that if a_d is the number of linearly independent homogeneous invariants of $\mathfrak{G}$ with degree d, and

$$\Phi_{\mathfrak{G}}(\lambda) = \sum_{d=0}^{\infty} a_d \lambda^d,$$

then

$$\Phi_{\mathfrak{G}}(\lambda) = \frac{1}{g} \sum_{\alpha=1}^{g} \frac{1}{\det(I - \lambda A_\alpha)}. \tag{42}$$

The proof depends on the following theorem.

THEOREM 13 [**51**, p. 258; **66**, p. 29]. *The number of linearly independent invariants of* $\mathfrak{G}$ *of degree* 1 *is*

$$a_1 = \frac{1}{g} \sum_{\alpha=1}^{g} \text{trace } (A_\alpha).$$

Proof. Let $S = (1/g)\Sigma_{\alpha=1}^{g} A_\alpha$. Changing the variables on which $\mathfrak{G}$ acts from $x_1, \ldots, x_m$ to $y_1, \ldots, y_m$, where $(y_1, \ldots, y_m) = (x_1, \ldots, x_m)T^{tr}$, changes S to $S' = TST^{-1}$. We may choose T so that S' is diagonal (see [**14**, p. 252]). Now $S^2 = S$, $(S')^2 = S'$, hence the diagonal entries of S' are 0 or 1. So with a change of variables we may assume

$$S = \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & \ddots & & & 0 & \\ & & & 1 & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & \ddots \\ 0 & & & & & & 0 \end{bmatrix},$$

with say r 1's on the diagonal. Thus $S \circ y_i = y_i$ if $1 \leqq i \leqq r$, $S \circ y_i = 0$ if $r+1 \leqq i \leqq m$.

Any linear invariant of $\mathfrak{G}$ is certainly fixed by S, so $a_1 \leqq r$. On the other hand, by Th. 2, $S \circ y_i = (1/g)\Sigma_{\alpha=1}^{g} A_\alpha \circ y_i$ is an invariant of $\mathfrak{G}$ for any i, and so $a_1 \geqq r$. Q.E.D.

Before proving Th. 1 let us introduce some more notation. Equation (37) describes how A_α transforms the variables $x_1, \ldots, x_m$. The *d-th induced matrix*, denoted by $A_\alpha^{[d]}$, describes how A_α transforms the products of the x_i taken d at a time, namely $x_1^d, x_2^d, \ldots, x_1^{d-1}x_2, \ldots$ ([**2**], [**39**, p. 122]). E.g., $A_\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ transforms x_1^2, x_1x_2 and x_2^2 into

$$\begin{aligned} &x^2x_1^2 + 2abx_1x_2 + b^2x_2^2, \\ &xcx_1^2 + (ad + bc)x_1x_2 + bdx_2^2, \\ &c^2x_1^2 + 2cdx_1x_2 + d^2x_2^2 \end{aligned}$$

respectively. Thus the 2nd induced matrix is

$$A_\alpha^{[2]} = \begin{bmatrix} a^2 & 2ab & b^2 \\ ac & ad+bc & bd \\ c^2 & 2cd & d^2 \end{bmatrix}.$$

Proof of Theorem 1: To prove Eq. (42), note that a_d is equal to the number of linearly independent invariants of degree 1 of $\mathfrak{G}^{[d]} = \{A_\alpha^{[d]}: \alpha = 1, \ldots, g\}$. By Th. 13,

$$a_d = \frac{1}{g} \sum_{\alpha=1}^{g} \text{trace } A_\alpha^{[d]}.$$

Therefore to prove Th. 1 it is enough to show that the trace of $A_\alpha^{[d]}$ is equal to the coefficient of λ^d in

$$\frac{1}{\det(I - \lambda A_\alpha)} = \frac{1}{(1-\lambda w_1)\cdots(1-\lambda w_m)}, \tag{43}$$

where $w_1, \ldots, w_m$ are the eigenvalues of A_α. By a suitable change of variables we can make

$$A_\alpha = \begin{bmatrix} w_1 & & 0 \\ & \ddots & \\ 0 & & w_m \end{bmatrix}, \qquad A_\alpha^{[d]} = \begin{bmatrix} w_1^d & & & & 0 \\ & w_2^d & & & \\ & & \ddots & & \\ & & & w_1^{d-1} w_2 & \\ & & & & \ddots \\ 0 & & & & \end{bmatrix},$$

and trace $A_\alpha^{[d]}$ = sum of the products of $w_1, \ldots, w_m$ taken d at a time. But this is exactly the coefficient of λ^d in the expansion of (43). Q.E.D.

It is worth remarking that the Molien series does not determine the group. For example there are two groups of 2×2 matrices with order 8 having

$$\Phi(\lambda) = \frac{1}{(1-\lambda^2)(1-\lambda^4)}$$

(namely the dihedral group $\mathfrak{D}_4$ and the abelian group $\mathfrak{Z}_2 \times \mathfrak{Z}_4$). In fact there exist abstract groups $\mathfrak{A}$ and $\mathfrak{B}$ whose matrix representations can be paired in such a way that every representation of $\mathfrak{A}$ has the same Molien series as the corresponding representation of $\mathfrak{B}$ ([**18**]).

E. A standard form for the basic invariants. The following notation is very useful in describing the ring $\mathfrak{I}(\mathfrak{G})$ of invariants of a group $\mathfrak{G}$. The complex numbers are denoted by $\mathbb{C}$, and if $p(\mathbf{x}), q(\mathbf{x}), \ldots$ are polynomials $\mathbb{C}[p(\mathbf{x}), q(\mathbf{x}), \ldots]$ denotes the set of all polynomials in $p(\mathbf{x})$, $q(\mathbf{x})$ with complex coefficients. For example Th. 3a just says that $\mathfrak{I}(\mathfrak{G}_1) = \mathbb{C}[\theta, \varphi]$.

Also $\oplus$ will denote the usual direct sum operation. For example, a statement like $\mathfrak{I}(\mathfrak{G}) = R \oplus S$ means that every invariant of $\mathfrak{G}$ can be written uniquely in the form $r + s$ where $r \in R$, $s \in S$. (Theorem 15 below illustrates this.)

Using this notation we can now specify the most convenient form of polynomial basis for $\mathfrak{I}(\mathfrak{G})$.

DEFINITION. A *good polynomial basis* for $\mathfrak{I}(\mathfrak{G})$ consists of homogeneous invariants $f_1, \ldots, f_l$ $(l \geqq m)$ where $f_1, \ldots, f_m$ are algebraically independent and

$$\mathfrak{I}(\mathfrak{G}) = \mathbb{C}[f_1, \ldots, f_m] \text{ if } l = m, \tag{44a}$$

or, if $l > m$,

(44b) $$\mathcal{I}(\mathfrak{G}) = \mathbb{C}[f_1, \ldots, f_m] \oplus f_{m+1}\mathbb{C}[f_1, \ldots, f_m] \oplus \cdots \oplus f_l\mathbb{C}[f_1, \ldots, f_m].$$

In words, this says that any invariant of $\mathfrak{G}$ can be written as a polynomial in $f_1, \ldots, f_m$ (if $l = m$), or as such a polynomial plus f_{m+1} times another such polynomial plus ... (if $l > m$). Speaking loosely, this says that, to describe an arbitrary invariant, $f_1, \ldots, f_m$ are "free" invariants and can be used as often as needed, while $f_{m+1}, \ldots, f_l$ are "transient" invariants and can each be used at most once.

For a good polynomial basis $f_1, \ldots, f_l$ we can say exactly what the syzygies are. If $l = m$ there are no syzygies. If $l > m$ there are $(l-m)^2$ syzygies expressing the products $f_i f_j$ $(i \geqq m, j \geqq m)$ in terms of $f_1, \ldots, f_l$.

It is important to note that the Molien series can be written down by inspection from the degrees of a good polynomial basis. Let $d_1 = \deg f_1, \ldots, d_l = \deg f_l$. Then

(45a) $$\Phi_{\mathfrak{G}}(\lambda) = \frac{1}{\prod_{i=1}^{m}(1-\lambda^{d_i})}, \text{ if } l = m,$$

or

(45b) $$\Phi_{\mathfrak{G}}(\lambda) = \frac{1 + \sum_{j=l+1}^{m} \lambda^{d_j}}{\prod_{i=1}^{m}(1-\lambda^{d_i})}, \text{ if } l > m.$$

(This is easily verified by expanding (45a) and (45b) in powers of λ and comparing with (44b).)

Some examples will make this clear.

1. For the group $\mathfrak{G}_1$ of Part I, $f_1 = \theta$ and $f_2 = \varphi$ form a good polynomial basis, with degrees $d_1 = 8$, $d_2 = 24$. Indeed, from Th. 3a and Eq. (5),

$$\mathcal{I}(\mathfrak{G}_1) = \mathbb{C}[\theta, \varphi] \text{ and } \Phi_{\mathfrak{G}_1}(\lambda) = \frac{1}{(1-\lambda^8)(1-\lambda^{24})}.$$

2. For the group $\mathfrak{G}_4$ defined in Section B, $f_1 = x^2$, $f_2 = y^2$, $f_3 = xy$ is a good polynomial basis, with $d_1 = d_2 = d_3 = 2$. The invariants can be described as

(46) $$\mathcal{I}(\mathfrak{G}_3) = \mathbb{C}[x^2, y^2] \oplus xy\,\mathbb{C}[x^2, y^2].$$

In words, any invariant can be written uniquely as a polynomial in x^2 and y^2 plus xy times another such polynomial. E.g.,

$$(x+y)^4 = (x^2)^2 + 6x^2y^2 + (y^2)^2 + xy(4x^2 + 4y^2).$$

The Molien series is

$$\Phi_{\mathfrak{G}_3}(\lambda) = \frac{1}{2}\left\{\frac{1}{(1-\lambda)^2} + \frac{1}{(1+\lambda)^2}\right\} = \frac{1+\lambda^2}{(1-\lambda^2)^2}$$

in agreement with (45b) and (46). The single syzygy is $x^2 \cdot y^2 = (xy)^2$. Note that $f_1 = x^2$, $f_2 = xy$, $f_3 = y^2$ is not a good polynomial basis, for the invariant y^4 is not in the set $\mathbb{C}[x^2, xy] \oplus y^2\mathbb{C}[x^2, xy]$.

3. In [41] we gave an example, arising from coding theory, of a group $\mathfrak{G}_5$ (say) of 4×4 matrices with order 128, for which the Molien series is

$$\Phi_{\mathfrak{G}_5}(\lambda) = \frac{1 + \lambda^8 + \lambda^{10} + \lambda^{18}}{(1-\lambda^2)(1-\lambda^4)(1-\lambda^8)^2}.$$

A good polynomial basis for the invariants of this group consists of free invariants f_1, f_2, f_3, f_4, of degrees 2, 4, 8, 8, and transient invariants $f_5 = p$ (deg 8), $f_5 = q$ (deg 10), and $f_6 = pq$ (deg 18). Then if B denotes $\mathbb{C}[f_1, f_2, f_3, f_4]$, we have

$$\mathcal{I}(\mathfrak{G}_5) = B \oplus pB \oplus qB \oplus pqB.$$

There are syzygies expressing p^2 and q^2 in terms of $f_1, \ldots, f_6$.

4. A more complicated example, also arising from coding theory, is described in [**48**]. This is a group of 4×4 matrices, with order 336, having Molien series

$$\frac{1+\lambda^8+\lambda^{10}+\lambda^{12}+\lambda^{16}+\lambda^{18}+\lambda^{20}+\lambda^{28}}{(1-\lambda^4)(1-\lambda^6)(1-\lambda^8)(1-\lambda^{14})}.$$

A good polynomial basis is given in [**48**]. Fortunately the following result holds.

THEOREM 14 (Hochster and Eagon [**31**, Prop. 13]; independently proved by Dade [**19**]). *A good polynomial basis exists for the invariants of any finite group of complex $m \times m$ matrices.* (The proof is too complicated to give here.)

So we know that for any group the Molien series can be put into the standard form of Eqs. (45a), (45b) (with denominator consisting of a product of m factors $(1-\lambda^{d_i})$ and numerator consisting of a sum of powers of λ with positive coefficients); and that a good polynomial basis Eqs. (44a), (44b) can be found whose degrees match the powers of λ occurring in the Molien series.

On the other hand, the converse is not true. It is not always true that when the Molien series has been put into the form (45a), (45b) (by cancelling common factors and multiplying top and bottom by new factors), then a good polynomial basis for $\mathcal{I}(\mathfrak{G})$ can be found whose degrees match the powers of λ in $\Phi(\lambda)$. This is shown by the following example, due to Stanley [**71**].

Let $\mathfrak{G}_6$ be the group of order 8 generated by the matrices

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & i \end{pmatrix}.$$

The Molien series is

$$\Phi_{\mathfrak{G}_6}(\lambda) = \frac{1}{(1-\lambda^2)^3} \tag{47}$$

$$= \frac{1+\lambda^2}{(1-\lambda^2)^2(1-\lambda^4)}. \tag{48}$$

A good polynomial basis exists corresponding to Eq. (48), namely

$$\mathcal{I}(\mathfrak{G}_6) = \mathbb{C}[x^2, y^2, z^4] \oplus xy\,\mathbb{C}[x^2, y^2, z^4],$$

but there is no good polynomial basis corresponding to (47).

The problem of finding which forms of $\Phi(\lambda)$ correspond to a good polynomial basis and which do not remains unsolved in general.

However, one important special case has been solved. Shephard and Todd [**68**] have characterized those groups for which (44a) and (45a) hold, i.e., for which a good polynomial basis exists consisting only of algebraically independent invariants. These are the groups known as unitary groups generated by reflections. A complete list of the 37 irreducible groups of this type is given in [**68**].

IV. APPLICATIONS

We begin with a further example of the use of invariant theory to obtain results about weight enumerators. This illustrates the general plan of attack described in Section H of Part I in a situation where it is rather difficult to find a good polynomial basis. Other examples may be found in [**41**], [**49**] and [**50**]. It is worth mentioning that some of these examples use infinite groups and relative rather than absolute invariants.

A. Complete weight enumerator of a Ternary Self-Dual Code. Let $\mathcal{C}$ be an $[n, \frac{1}{2}n, d]$ self-dual code over F_3 which contains some codeword with no zeros. By suitably multiplying columns by -1

(which doesn't change the error-correcting ability of the code) we can assume that $\mathscr{C}$ contains the codeword $\mathbf{1} = 111\ldots1$.

Let A_{ijk} be the number of codewords in $\mathscr{C}$ containing i 0's, j 1's and k 2's (where $i+j+k=n$). Then the *complete weight enumerator* of $\mathscr{C}$ is defined to be

$$V(x,y,z) = \sum_{i,j,k} A_{ijk} x^i y^j z^k = \sum_{\mathbf{u}\in\mathscr{C}} x^{s_0(\mathbf{u})} y^{s_1(\mathbf{u})} z^{s_2(\mathbf{u})},$$

where $s_i(\mathbf{u})$ is the number of components of u that are equal to i. For example, the complete weight enumerator of the Golay code C_{11} (normalized to contain $\mathbf{1}$) is

$$\begin{aligned} V(x,y,z) = {} & x^{12}+y^{12}+z^{12}+22(x^6y^6+x^6z^6+y^6z^6) \\ & +220(x^6y^3z^3+x^3y^6z^3+x^3y^3z^6). \end{aligned} \tag{49}$$

The complete weight enumerator gives more information about a code than the weight enumerator $W(x,y)$ does. Of course the latter can be obtained from the equation $W(x,y) = V(x,y,y)$.

The goal of this section is to characterize the complete weight enumerator of $\mathscr{C}$ by proving:

THEOREM 15 ([**70**]). *If $V(x,y,z)$ is the complete weight enumerator of a self-dual code over F_3 which contains* $\mathbf{1}$, *then*

$$V(x,y,z) \in \mathbb{C}[a_{12}, \beta_6^2, \delta_{36}] \oplus \beta_6\gamma_{18}\mathbb{C}[\alpha_{12}, \beta_6^2, \delta_{36}]$$

(i.e., *$V(x,y,z)$ can be written uniquely as a polynomial in α_{12}, β_6^2, δ_{36} plus $\beta_6\gamma_{18}$ times another such polynomial*), *where*

$$\begin{aligned} \alpha_{12} &= a(a^3+8p^3), \\ \beta_6 &= a^2-12b, \\ \gamma_{18} &= a^6-20a^3p^3-8p^6, \\ \delta_{36} &= p^3(a^3-p^3)^3, \end{aligned}$$

and

$$\begin{aligned} a &= x^3+y^3+z^3, \\ p &= 3xyz, \\ b &= x^3y^3+x^3z^3+y^3z^3. \end{aligned}$$

Note that $\gamma_{18}^2 = \alpha_{12}^3 - 64\delta_{36}$. (The subscript of a polynomial gives its degree.)

Proof. The proof follows the two stages described in Section H of Part I.

Stage I Let a typical codeword $\mathbf{u} \in \mathscr{C}$ contain a 0's, b 1's, and c 2's. Then since $\mathscr{C}$ is self-dual and contains $\mathbf{1}$

$$\begin{aligned} &\mathbf{u}\cdot\mathbf{u} = 0 \pmod 3 \Rightarrow 3\mid(b+c), \\ &\mathbf{u}\cdot\mathbf{1} = 0 \pmod 3 \Rightarrow 3\mid(b-c) \Rightarrow 3\mid b \text{ and } 3\mid c, \\ &\mathbf{1}\cdot\mathbf{1} = 0 \pmod 3 \Rightarrow 3\mid(a+b+c) \Rightarrow 3\mid a \end{aligned}$$

(where $a\mid b$ means "a divides b"). Therefore $V(x,y,z)$ is invariant under the transformations

$$\begin{pmatrix}\omega&0&0\\0&1&0\\0&0&1\end{pmatrix}, \quad J_3 = \begin{pmatrix}1&0&0\\0&\omega&0\\0&0&1\end{pmatrix}, \begin{pmatrix}1&0&0\\0&1&0\\0&0&\omega\end{pmatrix}, \quad \omega = e^{2\pi i/3}.$$

Also $-\mathbf{u}$ contains a 0's, c 1's, b 2's, and $1+\mathbf{u}$ contains c 0's, a 1's, b 2's. Therefore $V(x,y,z)$ is

invariant under

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

i.e., under any permutation of its arguments.

Finally, from the MacWilliams' theorem for complete weight enumerators ([**42**] or [**43**]), $V(x, y, z)$ is invariant under

$$M_3 = \frac{1}{\sqrt{3}}\begin{pmatrix}1&1&1\\1&\omega&\omega^2\\1&\omega^2&\omega\end{pmatrix}.$$

These 6 matrices generate a group $\mathfrak{G}_7$, of order 2592, consisting of 1944 matrices of the type

$$s^\nu\begin{pmatrix}1&&\\&\omega^a&\\&&\omega^b\end{pmatrix}M_3^e\begin{pmatrix}1&&\\&\omega^c&\\&&\omega^d\end{pmatrix},\qquad s = e^{2\pi i/12},$$

and 648 matrices of the type

$$s^\nu\begin{pmatrix}1&&\\&\omega^a&\\&&\omega^b\end{pmatrix}P,$$

where $0 \leqq \nu \leqq 11$, $0 \leqq a, b, c, d \leqq 2$, $e = 1$ or 3, and P is any 3×3 permutation matrix.

Thus Stage I is completed: the assumptions about the code imply that $V(x, y, z)$ is invariant under the group $\mathfrak{G}_7$.

Stage II consists of showing that the ring of invariants of $\mathfrak{G}_7$ is equal to $\mathbb{C}[\alpha_{12}, \beta_{12}, \delta_{36}] \oplus \gamma_{24}\mathbb{C}[\alpha_{12}, \beta_{12}, \delta_{36}]$. First, since we have a list of the matrices in $\mathfrak{G}_7$, it is a straightforward hand calculation to obtain the Molien series, Eq. (3). As usual everything collapses and the final expression is

$$\Phi_{\mathfrak{G}_7}(\lambda) = \frac{1+\lambda^{24}}{(1-\lambda^{12})^2(1-\lambda^{36})}.$$

This suggests the degrees of a good polynomial basis that we should look for.

Next, $\mathfrak{G}_7$ is generated by J_3, M_3, and all permutation matrices P. Obviously the invariants must be symmetric functions of x, y, z having degree a multiple of 3. So we take the algebraically independent symmetric functions a, p, b, and find functions of them which are invariant under J_3 and M_3. For example, β_6 is invariant under J_3, but is sent into $-\beta_6$ by M_3. We denote this by writing

$$\beta_6 \overset{J_3}{\leftrightarrow} \beta_6, \qquad \beta_6 \overset{M_3}{\leftrightarrow} -\beta_6.$$

Therefore β_6^2 is an invariant. Again

$$a \overset{M_3}{\leftrightarrow} \frac{1}{\sqrt{3}}(a+2p) \overset{J_3}{\rightarrow} \frac{1}{\sqrt{3}}(a+2\omega p) \overset{M_3}{\leftrightarrow} \frac{i}{\sqrt{3}}(a+2\omega^2 p),$$

so another invariant is $\alpha_{12} = a(a+2p)(a+2\omega p)(a+2\omega^2 p) = a(a^3+8p^3)$. Again

$$\gamma_{18} \overset{J_3}{\leftrightarrow} \gamma_{18}, \qquad \gamma_{18} \overset{M_3}{\leftrightarrow} -\gamma_{18},$$

so $\beta_6\gamma_{18}$ is an invariant. Finally

$$p \overset{M_3}{\leftrightarrow} \frac{1}{\sqrt{3}}(a-p) \overset{J_3}{\rightarrow} \frac{1}{\sqrt{3}}(a-\omega p) \overset{M_3}{\leftrightarrow} \frac{s}{\sqrt{3}}(a-\omega^2 p)$$

gives the invariant

$$\delta_{36} = p^3(a-p)^3(a-\omega p)^3(a-\omega^2 p)^3 = p^3(a^3-p^3)^3.$$

The syzygy $\gamma_{18}^2 = \alpha_{12}^3 - 64\delta_{36}$ is easily verified, and one can show that α_{12}, β_6^2, δ_{36} are algebraically independent. Thus $f_1 = \alpha_{12}$, $f_2 = \beta_6^2$, $f_3 = \delta_{36}$, $f_4 = \beta_6\gamma_{18}$ is a good polynomial basis for $\mathcal{I}(\mathfrak{G}_7)$, and the theorem is proved. Q.E.D.

REMARK. Without the assumption that the code contains the all-ones vector, the theorem (due to R. J. McEliece) becomes much more complicated (see [**41**, §4.7], [**50**]).

Applications of Theorem 15. For the ternary Golay code (Eq. (49)) $V = \frac{1}{6}(5\alpha_{12} + \beta_6^2)$. For Pless's [24, 12, 9] symmetry code ([**56**], [**57**]),

$$V = \frac{67}{144}\alpha_{12}^2 + \frac{1}{8}\alpha_{12}\beta_6^2 + \frac{1}{432}\beta_6^4 + \frac{11}{27}\beta_6\gamma_{18}.$$

The complete weight enumerators of the symmetry codes of lengths 36, 48 and 60 have also been obtained with the help of Th. 15 (see [**50**]).

B. The nonexistence of certain very good codes. One application of Th. 3c was given in Section F of Part I, where it was used to determine the weight enumerator of a certain code. Other applications of this type may be found for example in [**47**].

A different type of application of Th. 3c is to show that certain codes with high minimum distance do not exist. The idea is to assume that the code does exist, and then to use Th. 3c to show that one of the coefficients in the weight enumerator is negative. But this is obviously impossible; therefore the code does not exist.

To explain the family of codes to which we shall apply this method, consider first the [7, 4, 3] Hamming code C_5 and the [23, 12, 7] Golay code C_7. These two codes have several properties in common, besides being quadratic residue codes as was mentioned earlier. For example they are both perfect codes. An $[n, k, d]$ code over F_q is called *perfect* if every vector is within Hamming distance $[\frac{1}{2}(d-1)]$ of some codeword. Perfect codes are very rare, and in fact Tietäväinen and van Lint (see [**72**], [**38**]) have given a complete list of all perfect codes. In particular, there is no binary perfect code with $d > 7$, and so the sequence $C_5, C_7, \ldots$ of binary perfect codes stops at C_7.

But there is another way of continuing this sequence. The extended codes, that is, the [8, 4, 4] code C_6 and the [24, 12, 8] code C_8, are both binary self-dual codes with all weights divisible by 4 and having minimum distance $d = 4[n/24] + 4$. This is the highest possible minimum distance for such a code, as the following argument shows.

Let $\mathcal{C}$ be any $[n, \frac{1}{2}n, d]$ binary self-dual code with all weights divisible by 4, and having weight enumerator $W(x, y)$. By Th. 3c, $W(x, y)$ is a polynomial in θ and φ and therefore can be written as

$$W(x, y) = \sum_{i=0}^{\mu} a_i \theta^{j-3i} \varphi^i, \tag{50}$$

where $n = 8j = 24\mu + 8\nu$, $\nu = 0, 1$ or 2.

Suppose the $\mu + 1 = [n/24] + 1$ coefficients a_i in (50) are chosen so that

$$\begin{aligned} W(x, y) &= x^n + A_{4\mu+4}x^{n-4\mu-4}y^{4\mu+4} + \cdots \\ &= W(x, y)^* \qquad \text{(say)}. \end{aligned} \tag{51}$$

I.e., the a_i are chosen so that $W(x, y)$ has as many leading coefficients as possible equal to zero. An example of this was given in Section F of Part I. This determines the a_i and A_j uniquely. The resulting

W^* is the weight enumerator of that self-dual code with the greatest minimum weight we could hope to attain, and is called an *extremal* weight enumerator.

If a code exists with weight enumerator W^*, it has minimum distance $d^* = 4\mu + 4$, unless $A_{4\mu+4}$ is accidentally zero, in which case $d^* \geqq 4\mu + 8$.

But it can be shown [**47**] that $A_{4\mu+4}$, the number of codewords of minimum nonzero weight, is equal to:

$$\begin{cases} \binom{n}{5}\binom{5\mu-2}{\mu-1}\Big/\binom{4\mu+4}{5}, & \text{if } n = 24\mu, \\ \frac{1}{4}n(n-1)(n-2)(n-4)\dfrac{(5\mu)!}{\mu!(4\mu+4)!}, & \text{if } n = 24\mu + 8, \\ \frac{3}{2}n(n-2)\dfrac{(5\mu+2)!}{\mu!(4\mu+4)!}, & \text{if } n = 24\mu + 16, \end{cases}$$

and is never zero. This proves

THEOREM 16 ([**47**]). *The minimum distance of a binary self-dual code of length n with all weights divisible by 4 is at most $4[n/24] + 4$.*

So it is natural to study the sequence of self-dual codes with weights divisible by 4 and minimum distance actually equal to $4[n/24] + 4$. Such codes are known to exist for $n \leqq 48$ and for a few larger values of n (see [**42**]). Length $n = 72$ is the most important open case (see [**69**]). But the next theorem shows that this sequence of codes (like that of perfect codes) is finite.

In fact it turns out that the second coefficient in (51), $A_{4\mu+8}$, is negative if n is large (above about 3712), and so a self-dual code with weight enumerator W^* does not exist for large n. Furthermore, one can show that no self-dual code can even have minimum distance within a constant of $n/6$, if n is sufficiently large:

THEOREM 17 ([**46**]). *Let b be any constant. Suppose the a_i in* (50) *are chosen so that*

$$W(x, y) = x^n + A_{4d}x^{n-4d}y^{4d} + \cdots,$$

where $d \geqq n/6 - b$. Then one of the coefficients A_i is negative, for all sufficiently large n. So a binary self-dual code of length n, weights divisible by 4, and minimum weight d does not exist for all sufficiently large n.

On the other hand it is known that binary self-dual codes with weights divisible by 4 do meet the Gilbert–Varshamov bound [**44**].

Similar results hold for ternary self-dual codes and for certain types of lattice sphere packings (see [**46**]).

V. CONCLUSIONS

We have attempted to show how invariant theory has been used to solve problems in coding theory. There are two stages in a typical application of this technique, which is potentially of much wider application. Stage I: convert assumptions about the problem (e.g., the code) into algebraic constraints on polynomials (e.g., on the weight enumerator of the code). Stage II: use invariant theory to find all possible polynomials satisfying these constraints.

Some unsolved problems are (i) what is the greatest n for which the upper bound of Th. 16 is attained? In particular, does such a code exist with $n = 72$ (see [**69**])? (ii) An unsolved question from [**41**]: characterize the biweight enumerator of a binary self-dual code with all weights divisible by 4. (iii) For a given group of matrices, which forms of the Molien series $\Phi(\lambda)$ correspond to a good polynomial basis? (iv) Given two different groups of matrices, $\mathfrak{G}$ and $\mathfrak{H}$, which are both representations of the same abstract group, what is the relationship between $\mathcal{I}(\mathfrak{G})$ and $\mathcal{I}(\mathfrak{H})$?

Acknowledgments: This article is based on several joint papers [41], [46]–[49] with F. J. MacWilliams, C. L. Mallows and A. M. Odlyzko. I am very grateful for their collaboration. I should also like to thank W. L. Edge, J. McKay, M. K. Sain and R. Stanley for their helpful comments. Some of the calculations were verified with the help of the ALTRAN system for rational function manipulation [13], [30], and the GRAPPA group theory analysis program [21]. There is some overlap with the earlier survey [70], although the present paper is written from a different point of view and for a different audience.

References

1. V. K. Agrawala and J. G. Belinfante, An Algorithm for Computing SU(n) Invariants, BIT II (1971) 1–15.
2. A. C. Aitken, Determinants and Matrices, Oliver and Boyd, 9-th ed., Edinburgh, 1959.
3. E. F. Assmus, Jr., and H. F. Mattson, Jr., New 5-designs, J. Combinatorial Theory, 6 (1969) 122–151.
4. ———, and ———, Coding and combinatorics, SIAM Review, 16 (1974) 349–388.
5. E. F. Assmus, Jr., H. F. Mattson, and R. Turyn, Cyclic codes, Air Force Cambridge Res. Lab., Report AFCRL–65–322, Bedford, Mass., 1965.
6. ———, ———, and ———, Cyclic codes, Air Force Cambridge Res. Lab., Report AF19(604)–8516, Bedford, Mass., 1966.
7. E. R. Berlekamp, Algebraic Coding Theory, McGraw–Hill, New York, N.Y., 1968.
8. ———, Key papers in the development of coding theory, IEEE Press, New York, 1974.
9. E. R. Berlekamp, F. J. MacWilliams, and N. J. A. Sloane, Gleason's theorem on self-dual codes, IEEE Trans. Info. Theory, IT–18 (1972) 409–414.
10. I. F. Blake, Algebraic Coding Theory: History and Development, Dowden, Stroudsburg, Pa., 1973.
11. N. Bourbaki, Groupes et Algèbres de Lie, Ch. 4, 5 & 6, Hermann, Paris, 1968.
12. M. Broué and M. Enguehard, Polynômes des poids de certains codes et fonctions thêta de certains réseaux, Ann. Scient. Ec. Norm. Sup., 5 (1972) 157–181.
13. W. S. Brown, ALTRAN User's Manual, 3rd ed., Bell Laboratories, N. J. 1974.
14. W. Burnside, Theory of Groups of Finite Order, 2nd ed. Dover, New York, 1955.
15. J. H. Conway, A group of order 8, 315, 553, 613, 086, 720, 000, Bull. London Math. Soc., 1 (1969) 79–88.
16. ———, A characterization of Leech's lattice, Invent. Math., 7 (1969) 137–142.
17. ———, Groups, lattices, and quadratic forms, in: Computers in Algebra and Number Theory, SIAM–AMS Proc. IV, Amer. Math. Soc., 1971, 135–139.
18. E. C. Dade, Answer to a question of R. Brauer, J. Algebra, 1 (1964) 1–4.
19. E. C. Dade, letter to the author, 23 April 1972.
20. J. Dieudonné and J. B. Carrell, Invariant Theory, Old and New, Academic Press, New York, 1971.
21. L. A. Dimino, GRAPPA Basic User's Manual, Bell Laboratories, Murray Hill, N.J. 1972.
22. P. Doubilet, G.-C. Rota, and J. Stein, On the foundations of combinatorial theory: IX Combinatorial Methods in Invariant Theory, Studies in Appl. Math., 53 (1974) 185–216.
23. H. Dym and H. P. McKean, Fourier Series and Integrals, Academic Press, New York, 1972.
24. W. Feit, A self-dual even (96, 48, 16) code, IEEE Trans. Info. Theory IT–20 (1974) 136–138.
25. C. S. Fisher, The death of a mathematical theory: A study in the sociology of knowledge, Arch. Hist. Exact Sci., 3 (1967) 136–159.
26. A. M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities, in: Actes Congrès Internl. de Mathématique, 3 (1970) (Gauthier–Villars, Paris 1971) 211–215.
27. J.-M. Goethals, On the Golay perfect binary code, J. Combin. Theory, 11(A) (1971) 178–186.
28. M. J. E. Golay, Notes on digital coding, Proc. IEEE, 37 (1949) 657.
29. ———, Binary Coding, IEEE Trans. Info. Theory, 4 (1954) 23–28.
30. A. D. Hall, Jr., The ALTRAN system for rational function manipulation — A survey, Comm. Assoc. Comput. Mach., 14 (1971) 517–521.
31. M. Hochster and J. A. Eagon, Cohen–Macaulay rings, invariant theory, and the generic perfection of determinantal loci, Amer. J. Math., 93 (1971) 1020–1058.
32. N. Jacobson, Lectures in Abstract Algebra, Vol. 3, Van Nostrand, Princeton, N.J., 1964.
33. M. G. Kendall and A. Stuart, The Advanced Theory of Statistics, Vol. 1, Hafner, New York, 1969.
34. J. Leech and N. J. A. Sloane, Sphere packings and error-correcting codes, Canad. J. Math., 23 (1971) 718–745.
35. V. K. Leontjev, Spectra of Linear Codes, Third International Symposium on Information Theory, Tallinn, Estonia, June 1973, Abstracts of Papers, Part II, pp. 102–106.
36. N. Levinson, Coding Theory: A counterexample to G. H. Hardy's conception of applied mathematics, this MONTHLY, 77 (1970) 249–258.
37. J. H. van Lint, Coding theory, Lecture Notes in Math., 201 (Springer, Berlin, 1971).

38. ———, Recent results on perfect codes and related topics, pp. 163–183 of *Combinatorics*, edited by M. Hall, Jr., and J. H. van Lint, Reidel Publishing Co., Dordrecht, Holland, 1975.

39. D. E. Littlewood, A University Algebra, 2nd ed., Dover, New York, 1970.

40. F. J. MacWilliams, A theorem on the distribution of weights in a systematic code, Bell Syst. Tech. J., 42 (1963) 79–84.

41. F. J. MacWilliams, C. L. Mallows, and N. J. A. Sloane, Generalization of Gleason's theorem on weight enumerators of self-dual codes, IEEE Trans. Info. Theory, IT–18 (1972) 794–805.

42. F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-correcting Codes, North Holland, Amsterdam, 1977, to appear.

43. F. J. MacWilliams, N. J. A. Sloane, and J. M. Goethals, The MacWilliams identities for nonlinear codes, Bell System Tech. J., 51 (1972) 803–819.

44. F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson, Good self-dual codes exist, Discrete Math., 3 (1972) 153–162.

45. ———, ———, and ———, On the existence of a projective plane of order 10, J. Combinatorial Theory, 14A (1973) 66–78.

46. C. L. Mallows, A. M. Odlyzko, and N. J. A. Sloane, Upper bounds for modular forms, lattices, and codes, J. Algebra, 36 (1975) 68–76.

47. C. L. Mallows and N. J. A. Sloane, An upper bound for self-dual codes, Information and Control, 22 (1973) 188–200.

48. ——— and ———, On the invariants of a linear group of order 336, Proc. Camb. Phil. Soc., 74 (1973) 435–440.

49. ——— and ———, Weight enumerators of self-orthogonal codes, Discrete Math., 9 (1974) 391–400.

50. C. L. Mallows, V. Pless, and N. J. A. Sloane, Self-dual codes over GF(3), SIAM J. Applied Math., 31 (December 1976).

51. G. A. Miller, H. F. Blichfeldt and L. E. Dickson, Theory and Applications of Finite Groups, Dover, New York, 1961.

52. T. Molien, Über die Invarianten der linearen Substitutionsgruppe, Sitzungsber. König. Preuss. Akad. Wiss., (1897) 1152–1156.

53. D. Mumford, Geometric Invariant Theory, Springer, New York, 1965.

54. E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen, Math. Ann., 77 (1916) 89–92.

55. W. W. Peterson and E. J. Weldon, Jr., Error-Correcting Codes, 2nd ed., MIT Press, Cambridge, Mass., 1972.

56. V. Pless, On a new family of symmetry codes and related new five-designs, Bull. Amer. Math. Soc., 75 (1969) 1339–1342.

57. ———, Symmetry Codes over GF(3) and New Five-Designs, J. Combinatorial Theory, 12 (1972) 119–142.

58. ———, A classification of self-orthogonal codes over GF(2), Discrete Math., 3 (1972) 209–246.

59. ———, Self-dual codes, Proc. 5th S. -E. Conference on Combinatorics, Graph Theory, and Computing, Utilitas Math., (1974) 111–124.

60. V. Pless and J. N. Pierce, Self-dual codes over GF(q) satisfy a modified Varshamov bound, Information and Control, 23 (1973) 35–40.

61. V. Pless and N. J. A. Sloane, Binary self-dual codes of length 24, Bull. Amer. Math. Soc., 80 (1974) 1173–1178.

62. ——— and ———, On the classification and enumeration of self-dual codes, J. Combinatorial Theory, 18A (1975) 313–335.

63. S. J. Rallis, New and old results in invariant theory with applications to arithmetic groups, pp. 443–458 of *Symmetric Spaces*, edited by W. M. Boothby and G. L. Weiss, Dekker, New York, 1972.

64. C. Reid, Hilbert, Springer–Verlag, New York, 1970.

65. G. ;C. Rota, Combinatorial theory and invariant theory, lecture notes, Bowdoin College, Maine, Summer 1971.

66. J. -P. Serre, Représentations Linéaires des Groupes Finis, 2nd ed., Hermann, Paris, 1971.

67. E. P. Shaughnessy, Codes with simple automorphism groups, Arch. Math., 22 (1971) 459–466.

68. G. C. Shephard and J. A. Todd, Finite unitary reflection groups, Canad. J. Math., 6 (1954) 274–304.

69. N. J. A. Sloane, Is there a (72, 36) $d = 16$ self-dual code? IEEE Trans. Info. Theory, IT–19 (1973) 251.

70. ———, Weight enumerators of codes, pp. 115–142 of *Combinatorics*, M. Hall, Jr., and J. H. van Lint, editors, Reidel Publishing Co., Dordrecht, Holland, 1975.

71. R. P. Stanley, private communication.

72. A. Tietäväinen, On the existence of perfect codes over finite fields, SIAM J. Appl. Math., 24 (1973) 88–96.

73. H. Weyl, Invariants, Duke Math. J., 5 (1939) 489–502.

74. ———, The Classical Groups, Princeton University Press, Princeton, N.J., 1946.

ROOM 2C–363, BELL LABORATORIES, MURRAY HILL, N.J. 07974.