ACKNOWLEDGMENT

The authors wish to thank Dr. E. R. Berlekamp for his helpful comments and the referees for their suggestions.

APPENDIX

GENERALIZED NEWTON'S IDENTITIES

Let

$$S_j = \sum_{i=1}^{t} Y_i X_i^j$$

and

$$\sigma(x) = \prod_{i=1}^{t} (x - X_i^{\delta}) = x^t + \sigma_1 x^{t-1} + \cdots + \sigma_{t-1} x + \sigma_t,$$

where δ is any integer.

Since $\sigma(X_i^{\delta}) = 0$, we have the following generalized Newton's identities:

$$S_j + \sigma_1 S_{j-\delta} + \sigma_2 S_{j-2\delta} + \cdots + \sigma_t S_{j-t\delta} = \sum_{i=1}^{t} Y_i X_i^{j-\delta t} \sigma(X_i^{\delta}) = 0.$$

REFERENCES

[1] R. T. Chien and C. R. P. Hartmann, "On the minimum distance structure of cyclic codes," presented at the IEEE Int. Symp. Information Theory, Noordwijk, Holland, June 1970.
[2] R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error-correcting binary group codes," *Inform. Contr.*, vol. 3, pp. 68–79, Mar. 1960.
[3] R. C. Bose and D. K. Ray-Chaudhuri, "Further results on error-correcting binary group codes," *Inform. Contr.*, vol. 3, pp. 279–290, Sept. 1960.
[4] A. Hocquenghem, "Codes correcteurs d'erreurs," *Chiffres*, vol. 2, pp. 147–156, 1959.
[5] H. F. Mattson and G. Solomon, "A new treatment of Bose–Chaudhuri codes," *SIAM*, vol. 9, pp. 654–699, Dec. 1961.
[6] J. MacWilliams, "A theorem on the distribution of weights in a systematic code," *Bell Syst. Tech. J.*, vol. 42, pp. 79–94, Jan. 1963.
[7] J.-M. Goethals, "Analysis of weight distribution in binary cyclic codes," *IEEE Trans. Inform. Theory* (Corresp.), vol. IT-12, pp. 401–402, July 1966.
[8] ——, "Factorization of cyclic codes," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 242–246, Apr. 1967.
[9] T. Kasami, "Some lower bounds on the minimum weight of cyclic codes of composite length," *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 814–818, Nov. 1968.
[10] V. Lum and R. T. Chien, "On the minimum distance of Bose–Chaudhuri–Hocquenghem codes," *SIAM*, vol. 16, pp. 1325–1337, Nov. 1968.
[11] T. Kasami and N. Tokura, "Some remarks on BCH bounds and minimum weights of binary primitive BCH codes," *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 408–413, May 1969.
[12] P. Delsarte, "BCH bounds for a class of cyclic codes," MBLE Res. Lab., Brussels, Belgium, Rep. R108, May 1969.
[13] W. W. Peterson, *Error Correcting Codes*. Cambridge, Mass: M.I.T. Press and New York: Wiley, 1961.
[14] V. Lum, "Comments on 'The weight structure of some Bose–Chaudhuri codes'," *IEEE Trans. Inform. Theory* (Corresp.), vol. IT-15, pp. 618–619, Sept. 1969.
[15] D. Gorenstein and N. Zierler, "A class of cyclic linear error-correcting codes in p^M symbols," *SIAM J. Appl. Math.*, vol. 9, pp. 207–214, June 1961.
[16] W. W. Peterson, "On the weight structure and symmetry of BCH codes," Univ. Hawaii, Honolulu, Sci. Rep. 1, July 1965.
[17] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.
[18] K. K. Tzeng and C. R. P. Hartmann, "On the minimum distance of certain reversible cyclic codes," *IEEE Trans. Inform. Theory* (Corresp.), vol. IT-16, pp. 644–645, Sept. 1970.
[19] C. R. P. Hartmann, "On the minimum distance structure of cyclic codes and decoding beyond the BCH bound," Coordinated Sci. Lab., Univ. Illinois, Urbana, Tech. Rep. R-458, Feb. 1970.
[20] H. D. Goldman, M. Klimen, and H. Smola, "The weight structure of some Bose–Chaudhuri codes," *IEEE Trans. Inform. Theory* (Corresp.), vol. IT-14, pp. 167–169, Jan. 1968.
[21] C. L. Chen, "Computer results on the minimum distance of some binary cyclic codes," *IEEE Trans. Inform. Theory* (Corresp.), vol. IT-16, pp. 359–360, May 1970.

Gleason's Theorem on Self-Dual Codes

ELWYN R. BERLEKAMP, FELLOW, IEEE, F. JESSIE MACWILLIAMS, AND NEIL J. A. SLOANE, MEMBER, IEEE

***Abstract*—The weight enumerator of a code is the polynomial**

$$W(x,y) = \sum_{r=0}^{n} A_r x^{n-r} y^r,$$

where n denotes the block length and A_r denotes the number of codewords of weight r. Let C be a self-dual code over $GF(q)$ in which every weight is divisible by c. Then Gleason's theorem states that 1) if $q = 2$ and $c = 2$, the weight enumerator of C is a sum of products of the polynomials $x^2 + y^2$ and $x^2y^2(x^2 - y^2)^2$; 2) if $q = 2$ and $c = 4$, the weight enumerator is a sum of products of $x^8 + 14x^4y^4 + y^8$ and $x^4y^4(x^4 - y^4)^4$; and 3) if $q = 3$ and $c = 3$, the weight enumerator is a sum of products of $x^4 + 8xy^3$ and $y^3(x^3 - y^3)^3$. In this paper we give several proofs of Gleason's theorem.

Manuscript received June 6, 1971.

E. R. Berlekamp is with the Departments of Electrical Engineering—Computer Sciences and Mathematics, University of California, Berkeley, Calif.

F. J. MacWilliams and N. J. A. Sloane are with the Bell Telephone Laboratories, Inc., Murray Hill, N.J.

INTRODUCTION

LET C be a code of block length n over $GF(q)$ and let $C^{\perp}$ denote the *dual code* consisting of all vectors $\mathbf{x}$ such that

$$\mathbf{x} \cdot \mathbf{y} = \sum_{r=0}^{n} x_r y_r = 0$$

for all $\mathbf{y} \in C$. Let A_r be the number of codewords of weight r in C and let

$$W(x,y) = \sum_{r=0}^{n} A_r x^{n-r} y^r$$

be the *weight enumerator* of C. Similarly let

$$W^{\perp}(x,y) = \sum_{r=0}^{n} A_r^{\perp} x^{n-r} y^r$$

be the weight enumerator of $C^{\perp}$. Then W and $W^{\perp}$ are related by the MacWilliams identity [8]:

$$\sum_{r=0}^{n} A_r x^{n-r} y^r = \frac{1}{|C^{\perp}|} \sum_{r=0}^{n} A_r^{\perp} (x + (q-1)y)^{n-r} (x-y)^r.$$

A code C is said to be *self-dual* if $C^{\perp} = C$, in which case its weights A_r satisfy

$$\sum_{r=0}^{n} A_r x^{n-r} y^r = \sum_{r=0}^{n} A_r \left(\frac{x + (q-1)y}{\sqrt{q}}\right)^{n-r} \left(\frac{x-y}{\sqrt{q}}\right)^r \quad (1)$$

or equivalently its weight enumerator satisfies

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

Any homogeneous polynomial

$$W(x,y) = \sum_{r=0}^{n} A_r x^{n-r} y^r$$

with complex coefficients will be called a *formally self-dual* weight enumerator over $GF(q)$ if it satisfies (2), and the subscripts r for which $A_r \neq 0$ will be called the weights occurring in $W(x,y)$.

Clearly the weight enumerator of a self-dual code is formally self-dual, but the converse is not true. [There is no code having the weight enumerator $x^2y^2(x^2 - y^2)^2$.]

The Theorems

Gleason's theorem is a series of statements about the possible forms that formally self-dual weight enumerators can take. By the previous remarks, these statements also apply to the weight enumerators of self-dual codes. We are concerned here only with codes over $GF(2)$ and $GF(3)$, but a similar statement applies to codes over $GF(5)$ [5]. Another proof of Theorem 1 was given by Feit [3], [4].

Theorem 1—Gleason [5]: Let

$$W(x,y) = \sum_{r=0}^{n} A_r x^{n-r} y^r$$

be a formally self-dual weight enumerator of length n over $GF(q)$, in which every weight is divisible by c.

Part 1: If $q = 2$ and $c = 2$, then n is even, $A_{n-r} = A_r$ for all r, and

$$W(x,y) = \sum_{r,s} K_{rs} f_1(x,y)^r f_2(x,y)^s, \quad (3)$$

where r, s are nonnegative integers, K_{rs} are complex numbers,

$$f_1(x,y) = x^2 + y^2$$
$$f_2(x,y) = x^2y^2(x^2 - y^2)^2$$

and $n = 2r + 8s$.

Part 2: If $q = 2$ and $c = 4$, then n is divisible by 8, and

$$W(x,y) = \sum_{r,s} K_{rs} f_3(x,y)^r f_4(x,y)^s, \quad (4)$$

where r, s are nonnegative integers, K_{rs} are complex numbers,

$$f_3(x,y) = x^8 + 14x^4y^4 + y^8$$
$$f_4(x,y) = x^4y^4(x^4 - y^4)^4$$

and $n = 8r + 24s$.

Part 3: If $q = 3$ and $c = 3$, then n is divisible by 4, and

$$W(x,y) = \sum_{r,s} K_{rs} f_5(x,y)^r f_6(x,y)^s, \quad (5)$$

where r, s are nonnegative integers, K_{rs} are complex numbers,

$$f_5(x,y) = x^4 + 8xy^3$$
$$f_6(x,y) = y^3(x^3 - y^3)^3$$

and $n = 4r + 12s$.

Examples of Self-Dual Codes

By an (n,M,d) code we mean a code of block length n, with M codewords, and minimum distance d. If C_i is an (n_i,M_i,d_i) code with weight enumerator $W_i(x,y)$, for $i = 1,2$, the *direct sum* code $C_1 + C_2$ consisting of all codewords (x,y), $x \in C_1$, $y \in C_2$, is easily seen to be an $(n_1 + n_2, M_1M_2, d = \min(d_1,d_2))$ code with weight enumerator $W_1(x,y)W_2(x,y)$.

We list some self-dual codes that illustrate Theorem 1.

i) $C_1 = \{00,11\}$ is a (2,2,2) code with weight enumerator $x^2 + y^2 = f_1$.

ii) $C_1 + C_1 + C_1 + C_1$, an (8,16,2) code generated by {11000000, 00110000, 00001100, 00000011}, has $W(x,y) = f_1^4$.

iii) The (8,16,4) extended Hamming code has $W(x,y) = x^8 + 14x^4y^4 + y^8 = f_1^4 - 4f_2 = f_3$. (This is an example of Parts 1 and 2 of Theorem 1.)

Examples ii) and iii) are the only self-dual binary codes of length 8 [11].

iv) The $(24,2^{12},8)$ extended Golay binary perfect code [1, p. 359] has $W(x,y) = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24} = f_3^3 - 672f_4 = (f_1^4 - 4f_2)^3 - 672 f_1^4 f_2^2$. (See the second proof of Part 2.) This code is the unique self-dual code of length 24 with minimum weight 8 [10]. Further examples of binary self-dual codes have been given by Pless [11].

v) The (4,9,3) ternary code generated by {1 0 − 1 1, 0111} has $W(x,y) = x^4 + 8xy^3 = f_5$.

vi) The $(12,3^6,6)$ extended Golay ternary perfect code [1, p. 307] has $W(x,y) = x^{12} + 264x^6y^6 + 440x^3y^9 + 24y^{12} = f_5^4 + 24f_6$.

In the course of proving Theorem 1 the following theorem will be established.

Theorem 2: With the same hypotheses as Theorem 1, the formally self-dual weight enumerator $W(x,y)$ has the following forms.

Part 1:

$$W(x,y) = af_1(x,y)^b f_2(x,y)^c \prod_{r=1}^{d} \{f_1(x,y)^4 + \beta_r f_2(x,y)\} \quad (6)$$

Part 2:

$$W(x,y) = af_3(x,y)^b f_4(x,y)^c \prod_{r=1}^{d} \{f_3(x,y)^3 + \beta_r f_4(x,y)\} \tag{7}$$

Part 3:

$$W(x,y) = af_5(x,y)^b f_6(x,y)^c \prod_{r=1}^{d} \{\beta_r f_5(x,y)^3 - f_6(x,y)\}, \tag{8}$$

where b,c,d denote integers, a, β_r denote complex numbers, and $2b + 8(c + d) = n$ in (6), $8b + 24(c + d) = n$ in (7), and $4b + 12(c + d) = n$ in (8).

Remark: If $W(x,y)$ is the weight enumerator of a self-dual code (and not just a formal solution of the MacWilliams identity), then the coefficients K_{rs} in (3), (4), and (5) must be integers [since so are the coefficients of $W(x,y)$], and in (6)–(8) we must have $a = 1$ and $c = 0$ (since $W(1,0) = A_0 = 1$).

Proofs of The Theorems

First Proof of Theorem 1 and Proof of Theorem 2: Let $z = y/x$, and write the MacWilliams identity (1) as

$$\sum_{r=0}^{n} A_r z^r = \sum_{r=0}^{n} A_r \left(\frac{1 + (q-1)z}{\sqrt{q}}\right)^{n-r} \left(\frac{1-z}{\sqrt{q}}\right)^r, \tag{9}$$

where q is now either 2 or 3.

Consider the complex zeros of the polynomial

$$F(z) = \sum_{r=0}^{n} A_r z^r.$$

If α is a zero, so is $(1 - \alpha)/[1 + (q - 1)\alpha]$, provided $1 + (q - 1)\alpha \neq 0$. To show this, let ϕ be the transformation $\phi: \alpha \to (1 - \alpha)/[1 + (q - 1)\alpha]$.

Substituting $z = \phi(\alpha)$ in (9) we obtain

$$F(\phi(\alpha)) = \left(\frac{\sqrt{q}}{1 + (q-1)\alpha}\right)^n F(\alpha) = 0.$$

Lemma: Let

$$W(x,y) = \sum_{r=0}^{n} A_r x^{n-r} y^r$$

be a formally self-dual weight enumerator over $GF(2)$ in which all weights are divisible by 2. Then $W(x,y) = W(y,x)$, and $A_r = A_{n-r}$ for $r = 0,1,\cdots,n$.

Proof: By hypothesis $W(x,y)$ is invariant under the transformation

$$\pi: x \to x, \qquad y \to -y$$

and since $W(x,y)$ satisfies (2) it is also invariant under

$$\rho: x \to (x + y)/\sqrt{2}, \qquad y \to (x - y)/\sqrt{2}.$$

Since $\rho\pi\rho$ interchanges x and y, $W(x,y) = W(y,x)$.

Proof of Part 1 of Theorems 1 and 2: By hypothesis $A_r = 0$ unless r is divisible by 2. Thus $F(\alpha) = 0$ implies $F(-\alpha) = 0$. Let ψ_1 be the transformation $\alpha \to -\alpha$. Let ϕ_1 be the transformation ϕ with $q = 2$. The transformations ϕ_1 and ψ_1 generate a group of order 8, so that if $\alpha \neq 0, \pm 1$ is a zero of $F(z)$, so are $\pm\alpha$, $\pm 1/\alpha$, $\pm(1 - \alpha)/(1 + \alpha)$, $\pm(1 + \alpha)/(1 - \alpha)$, although these are not necessarily all distinct. If they are all distinct, $F(z)$ contains the factor

$$(z^2 - \alpha^2)\left(z^2 - \frac{1}{\alpha^2}\right)\left(z^2 - \left(\frac{1-\alpha}{1+\alpha}\right)^2\right)\left(z^2 - \left(\frac{1+\alpha}{1-\alpha}\right)^2\right)$$

$$= 1 - (z^2 + z^6)(1 + 14\alpha^4 + \alpha^8)\alpha^{-2}(1 - \alpha^2)^{-2} + 2z^4\{1 + (1 + \alpha^4)(1 + 6\alpha^2 + \alpha^4) \cdot \alpha^{-2}(1 - \alpha^2)^{-2}\} + z^8 \tag{10}$$

$$= (1 + z^2)^4 + \beta z^2(1 - z^2)^2, \tag{11}$$

where $\beta = -(1 + \alpha^2)^4\alpha^{-2}(1 - \alpha^2)^{-2}$. If the zeros are not all distinct, there are the following possibilities.

i) $\alpha = \pm i$, so that $F(z)$ contains the factor $1 + z^2$;

ii) $\alpha = \pm 1 \pm \sqrt{2}$, so that $F(z)$ contains the factor $(1 - 6z^2 + z^4)^2 = (1 + z^2)^4 - 16z^2(1 - z^2)^2$, which is of the same form as (11).

Finally we must consider the cases when one or more of $0, \pm 1$ is a zero of $F(z)$. Suppose $F(-1) = 0$. From (9), $A_n = 0$ and $A_0 = 0$ by the lemma. From the left-hand side of (9), $F(z)$ is divisible by z^2; and from the right-hand side, by $(1 + z)^2(1 - z)^2 = (1 - z^2)^2$. Thus $F(z)$ contains the factor $z^2(1 - z^2)^2$. The remaining cases also lead to this factor. We have shown that

$$F(z) = a(1 + z^2)^b[(1 - z^2)^2 z^2]^c \cdot \prod [(1 + z^2)^4 + \beta z^2(1 - z^2)^2]$$

or, returning to the homogeneous case,

$$W(x,y) = a(x^2 + y^2)^b[(x^2 - y^2)^2 x^2 y^2]^c \cdot \prod [(x^2 + y^2)^4 + \beta x^2 y^2 (x^2 - y^2)^2]. \tag{16}$$

Expanding the product we obtain

$$W(x,y) = \sum_{r,s} K_{rs}(x^2 + y^2)^r((x^2 - y^2)^2 x^2 y^2)^s,$$

which completes the proof of Part 1 of Theorems 1 and 2.

Proof of Part 2 of Theorems 1 and 2: Since all weights are divisible by 4, $F(z)$ is invariant under the transformation $\theta: z \to iz$. The transformations ϕ_1, ψ, and θ generate a group of order 24, so that if $\alpha \neq 0, \pm 1$, $\pm i$ is a zero of $F(z)$, so are $\varepsilon\alpha$, ε/α, $\varepsilon(1 - \alpha)/(1 + \alpha)$, $\varepsilon(1 + \alpha)/(1 - \alpha)$, $\varepsilon(1 - i\alpha)/(1 + i\alpha)$, $\varepsilon(1 + i\alpha)/(1 - i\alpha)$, for $\varepsilon = \pm 1, \pm i$. Suppose first that all 24 zeros are distinct. We have already combined one set of 8 and we can simplify the algebra by using this. We rewrite (10) as

$$(1 + 14z^4 + z^8) - \frac{1 + 14\alpha^4 + \alpha^8}{\alpha^2(1 - \alpha^2)^2} z^2(1 - z^2)^2 = H - \frac{\gamma}{\alpha^2(1 - \alpha^2)^2} G \text{ (say).}$$

Applying $\alpha \to i\alpha$ we obtain the factor $H + [\gamma/\alpha^2(1 + \alpha^2)^2]G$. Applying instead $\alpha \to i(1 - \alpha)/(1 + \alpha)$ we obtain the factor $H + [4\gamma/(1 - \alpha^2)^2(1 + \alpha^2)^2]G$.

Thus $F(z)$ contains the factor

$$\left(H - \frac{\gamma}{\alpha^2(1-\alpha^2)^2}G\right)\left(H + \frac{\gamma}{\alpha^2(1+\alpha^2)^2}G\right) \cdot \left(H + \frac{4\gamma}{(1-\alpha^2)^2(1+\alpha^2)^2}G\right)$$
$$= H^3 - \frac{\gamma^3}{\alpha^4(1-\alpha^4)^4}(H+4G)G^2$$
$$= (1 + 14z^4 + z^8)^3 + \beta z^4(1-z^4)^4,$$

where $\beta = -(1 + 14\alpha^4 + \alpha^8)^3\alpha^{-4}(1-\alpha^4)^{-4}$. The analysis of multiple zeros shows that $1 + 14z^4 + z^8$ can occur separately. Finally, if any one of $0, \pm 1, \pm i$ is a zero of $F(z)$, we can use the group of transformations to show that $F(-1) = 0$, and then the argument used in the first proof shows that $F(z)$ contains $z^4(1-z^4)^4$ as a factor. This proves Part 2 of Theorem 2, and Part 2 of Theorem 1 follows immediately.

Proof of Part 3 of Theorems 1 and 2: By hypothesis, $A_r = 0$ unless r is divisible by 3. Thus $F(\alpha) = 0$ implies $F(\omega\alpha) = 0$, where $\omega = e^{2\pi i/3}$. Let ψ_2 be the transformation $\alpha \to \omega\alpha$ and ϕ_2 the transformation ϕ with $q = 3$. These transformations generate a group of order 12. If α is a zero of $F(z)$ so are

$$\begin{array}{ccc} & \omega\alpha, \quad \omega^2\alpha & \\ \dfrac{1-\alpha}{1+2\alpha}, & \omega\dfrac{1-\alpha}{1+2\alpha}, & \omega^2\dfrac{1-\alpha}{1+2\alpha}, \\ \dfrac{\omega-\alpha}{\omega+2\alpha}, & \omega\dfrac{\omega-\alpha}{\omega+2\alpha}, & \omega^2\dfrac{\omega-\alpha}{\omega+2\alpha}, \\ \dfrac{\omega^2-\alpha}{\omega^2+2\alpha}, & \omega\dfrac{\omega^2-\alpha}{\omega^2+2\alpha}, & \omega^2\dfrac{\omega^2-\alpha}{\omega^2+2\alpha}, \end{array} \quad (12)$$

provided none of the denominators is zero. If these 12 zeros of $F(z)$ are distinct, we obtain, combining them in the obvious way, a factor

$$(z^3 - \alpha^3)\left(z^3 - \left(\frac{1-\alpha}{1+2\alpha}\right)^3\right) \cdot \left(z^3 - \left(\frac{\omega-\alpha}{\omega+2\alpha}\right)^3\right)\left(z^3 - \left(\frac{\omega^2-\alpha}{\omega^2+2\alpha}\right)^3\right). \quad (13)$$

This may be simplified to

$$\frac{\alpha^3(1-\alpha^3)^3}{(1+8\alpha^3)^3}(1 + 8z^3)^3 - (1-z^3)^3z^3. \quad (14)$$

The equality of (13) and (14) may be checked either by expanding both in powers of z and comparing coefficients, or more simply by verifying that they have the same set of roots. The analysis of multiple zeros shows that $z^3(1-z^3)^3$ can occur separately.

Finally we consider the case in which $F(z)$ has a zero that is also a zero of one of the denominators of (12). Without loss of generality we may take this to be $\alpha = -\frac{1}{2}$. Setting $x = -2y$ in (1) shows that $A_n = 0$, and so $W(x,y)$ is divisible by x. Clearly it is also divisible by $(x + 2y)$ $(x + 2\omega y)(x + 2\omega^3 y) = x^3 + 8y^3$, hence by $x^4 + 8xy^3$. Thus we have $W(x,y) = a(x^4 + 8xy^3)^b[y^3(x^3 - y^3)^3]^c \times \prod[\beta(x^4 + 8xy^3)^3 - y^3(x^3 - y^3)^3]$. As before, this proves Part 3 of Theorems 1 and 2.

Second Proof of Theorem 1, Part 2: Although less elementary than the first proof, this proof seems to us to be of considerable interest since it relates self-dual codes to even unimodular lattices, for which a substantial body of theory exists; and also it shows how in some cases such lattices may be constructed from self-dual codes, and vice versa. The main ideas of this proof are due to Thompson [13]. Some recent references on even unimodular lattices are [2], [6], and [12].

Let $n \geq 1$ be a fixed integer. Let $\mathscr{C}$ be the family of all self-dual binary codes of block length n in which every weight is divisible by 4. Any code $C \in \mathscr{C}$ contains $2^{\frac{1}{2}n}$ codewords and has minimum weight at least 4.

i) Construction of Lattices: For each $C \in \mathscr{C}$ we construct a lattice Λ in n-dimensional Euclidean space E^n as follows. (This is Construction A of [7]).

The points of Λ are all $\boldsymbol{x} = (x_1, \cdots, x_n)$ that are congruent to a codeword of C (modulo 2).

If two distinct points of Λ are congruent to the same codeword of C, then they differ by at least 2 in at least one coordinate. If they are congruent to different codewords, they differ by at least 1 in at least four coordinates. Hence any two distinct points of Λ are at a distance of at least two apart.

So if spheres of unit radius are constructed with the points of Λ as centers, they do not overlap, and form a sphere packing in E^n.

The volume of a sphere of radius ρ in E^n is $V_n\rho^n$, where $V_n = \pi^{\frac{1}{2}n}/\Gamma(\frac{1}{2}n + 1)$. Since $2^{\frac{1}{2}n}$ out of every 2^n points of E^n are accepted as lattice points, the density of the sphere packing (i.e., the fraction of E^n covered by the spheres) is

$$\Delta = V_n\rho^n 2^{-\frac{1}{2}n} = V_n 2^{-\frac{1}{2}n}$$

and the number of centers per unit volume is

$$D = \frac{\Delta}{V_n\rho^n} = 2^{-\frac{1}{2}n}.$$

It follows from the assumptions about C that if $\boldsymbol{x}, \boldsymbol{y} \in \Lambda$, $\boldsymbol{x} \cdot \boldsymbol{x}$ is divisible by 4 and $\boldsymbol{x} \cdot \boldsymbol{y}$ is divisible by 2.

Let us change the scale and define a new lattice Λ' with points $(1/\sqrt{2})\boldsymbol{x}$, for $\boldsymbol{x} \in \Lambda$. Then Λ' contains $D' = 2^{\frac{1}{2}n}D = 1$ point per unit volume (and so Λ' is unimodular), and if $\boldsymbol{x}, \boldsymbol{y} \in \Lambda'$, $\boldsymbol{x} \cdot \boldsymbol{x}$ is divisible by 2 (and so Λ' is even) and $\boldsymbol{x} \cdot \boldsymbol{y}$ is an integer.

ii) Theta Functions: Let t_r be the number of points in Λ' whose distance from the origin is $\sqrt{r}$. Then

$$T(z) = \sum_{r=0}^{\infty} t_{2r}e^{2\pi irz} = \sum_{r=0}^{\infty} t_{2r}q^r, \qquad q = e^{2\pi iz}$$

is called the *theta function* of Λ'. Since Λ' is an even unimodular lattice it follows from [12, p. 174, theorem 8] that i) n is a multiple of 8 and ii) $T(z)$ is a modular form of weight $\frac{1}{2}n$. [A modular form of weight $\frac{1}{2}n$ is a series

$$f(z) = \sum_{r=0}^{\infty} a_r e^{2\pi i r z}$$

that converges for $\mathrm{Im}(z) > 0$ and that satisfies the identity

$$f\left(-\frac{1}{z}\right) = z^{\frac{1}{2}n} f(z).]$$

Let $\mathcal{M}$ denote the set of all modular forms of weight $\frac{1}{2}n$. It is known [12, p. 144, corollary 1], [6, p. 26, example 1] that $\mathcal{M}$ is a vector space of dimension $[(1/24)n] + 1$, and that if $n = 24u + 8v$, $0 \le v \le 2$, a basis for $\mathcal{M}$ may be taken to be the functions $E(z)^{v+3a}\Delta(z)^{u-a}$ for $0 \le a \le u$, where

$$E(z) = 1 + 240 \sum_{r=1}^{\infty} \sigma_3(r) q^r$$

$$= 1 + 240q + 2160q^2 + 6720q^3 + \cdots$$

and

$$\Delta(z) = q \prod_{r=1}^{\infty} (1 - q^r)^{24} = \prod_{r=1}^{\infty} \tau(r) q^r$$

$$= q - 24q^2 + 252q^3 - \cdots$$

Here $\sigma_3(n)$ denotes the sum of the cubes of the divisors of n_1 and $\tau(n)$ is Ramanujan's function. It follows that

$$T(z) = \sum_{8i+24j=n} K_{ij} E(z)^i \Delta(z)^j. \tag{15}$$

We shall express $T(z)$ in terms of the weight enumerator

$$W(x,y) = \sum_{r=0}^{\infty} A_r x^{n-r} y^r$$

of C. Now t_r is the number of vectors $(x_1, \cdots, x_n)$ that are congruent (modulo 2) to some codeword of C and satisfy

$$\sum_{j=1}^{n} x_j^2 = 2r.$$

The numbers congruent to 0 (modulo 2) are $0, \pm 2, \pm 4, \pm 6, \cdots$ and the number of such numbers at a squared distance of r from 0 is the coefficient of x^r in

$$\theta(x) = 1 + 2x^{2^2} + 2x^{4^2} + 2x^{6^2} + \cdots.$$

Similarly the number of numbers congruent to 1 (modulo 2) at a squared distance of r from 0 is the coefficient of x^r in

$$\phi(x) = 2x^{1^2} + 2x^{3^2} + 2x^{5^2} + \cdots.$$

Let $\boldsymbol{c} \in C$ have weight w. Then the number of points $\boldsymbol{x} \in E^n$ that are congruent to $\boldsymbol{c}$ (modulo 2) and that are at a squared distance of r from $\boldsymbol{0}$ is the coefficient of x^r in $\theta(x)^{n-w}\phi(x)^w$. Summing over all codewords in C, we obtain

$$\sum_{r=0}^{\infty} t_{2r} x^{4r} = \sum_{r=0}^{n} A_r \theta(x)^{n-r} \phi(x)^r.$$

Set $x = q^{\frac{1}{4}}$. Then

$$T(z) = \sum_{r=0}^{\infty} t_{2r} q^r = \sum_{r=0}^{n} A_r \theta(q^{\frac{1}{4}})^{n-r} \phi(q^{\frac{1}{4}})^r$$

$$= W(\theta_1(z), \phi_1(z)), \tag{16}$$

where

$$\theta_1(z) = \theta(q^{\frac{1}{4}}) = 1 + 2 \sum_{r=1}^{\infty} q^{r^2}$$

$$\phi_1(z) = \phi(q^{\frac{1}{4}}) = 2q^{\frac{1}{4}} \sum_{r=0}^{\infty} q^{r(r+1)}.$$

Example—$n = 8$: The (8,16,4) extended Hamming code has weight enumerator $W(x,y) = x^8 + 14x^4y^4 + y^8$. Therefore $T(z) = \theta_1{}^8 + 14\theta_1{}^4\phi_1{}^4 + \phi_1{}^8 = 1 + 240q + 2160q^2 + \cdots$.

Here $\mathcal{M}$ has dimension 1 and so from (15),

$$T(z) = E(z) = \theta_1{}^8 + 14\theta_1{}^4\phi_1{}^4 + \phi_1{}^8. \tag{17}$$

Example—$n = 24$: The $(24,2^{12},8)$ extended Golay code has weight enumerator $W(x,y) = x^{24} + 759x^{16}y^8 + 2576x^8y^8 + 759x^8y^{16} + y^{24}$. Therefore

$$T(z) = \theta_1{}^{24} + 759\theta_1{}^{16}\phi_1{}^8 + 2576\theta_1{}^8\phi_1{}^8 + 759\theta_1{}^8\phi_1{}^{16} + \phi_1{}^{24}$$

$$= 1 + 48q + 195408q^2 + \cdots.$$

Here $\mathcal{M}$ has dimension 2, and so from (15) $T(z) = aE(z)^3 + b\Delta(z)$. By equating coefficients of 1 and q we find $a = 1$ and $b = -672$. Then using (17) to eliminate $E(z)$, we have

$$\Delta(z) = \tfrac{1}{16}\theta_1{}^4\phi_1{}^4(\theta_1{}^4 - \phi_1{}^4)^4. \tag{18}$$

Combining (15), (17), and (18) completes the proof of Theorem 1, Part 2.

Third Partial Proof of Theorem 1: If we assume in Part 1 of the theorem that n is even and $A_{n-i} = A_i$ for all i, in Part 2 that n is divisible by 8, and in Part 3 that n is divisible by 4, then we can give an elementary proof that the corresponding weight enumerators have the forms (3), (4), and (5).

First, it is easily verified that if W_1 and W_2 are both solutions to the functional equation (2), then so are W_1W_2 and $\alpha W_1 + \beta W_2$, where α and β may be arbitrary complex numbers. In other words, products and linear combinations of solutions of (2) are also solutions of (2).

It is also easy to verify, using the examples of self-dual codes given after the statement of Theorem 1, that $f_1, f_2, \cdots, f_6$ solve (2) for the appropriate choices of n and q. Therefore, every expression of the form of (3), (4), or (5) is also a solution to (2). It remains to show that there are no other solutions. This can be done by the following dimension argument.

One well-known form of the MacWilliams identity between $W(x,y)$ and $W^{\perp}(x,y)$, first introduced by Pless [9], expresses the first r moments of $A_0, A_1, \cdots, A_n$ in terms of $A_0{}^{\perp}, A_1{}^{\perp}, \cdots, A_{r-1}^{\perp}$. The coefficient matrix is invertible, so that if one knows $A_0{}^{\perp}, A_1{}^{\perp}, \cdots, A_{r-1}^{\perp}$ and all but r of the A_i, then the equations have a unique solution for the unknown A_i and the remaining $A_i{}^{\perp}$.

If $q = 2$, $A_i{}^{\perp} = A_i$, and $A_i = A_{n-i}$, and if we know $A_0, A_c, A_{2c}, \cdots, A_{(j-1)c}$, then we also know $A_n, A_{n-c}, \cdots, A_{n-(j-1)c}$. Assuming all weights are divisible by c, the only

$(n/c) - 2j + 1$ unknown weights are $A_{jc}, A_{(j+1)c}, \cdots, A_{n-jc}$. However, from $A_i^{\perp} = A_i$, we know $A_0^{\perp}, A_1^{\perp}, A_2^{\perp}, \cdots, A_{jc-1}^{\perp}$. The Pless identities give us jc equations in the $(n/c) - 2j + 1$ unknowns, and this system of linear equations has at most one solution whenever

$$jc \geq \frac{n}{c} - 2j + 1$$

or

$$j \geq \frac{n + c}{c^2 + 2c}.$$

It follows that if $A_{n-i} = A_i$, then the dimension of the space of all solutions of (2) is no greater than $\lceil (n + c)/(c^2 + 2c) \rceil$ (where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x). If $c = 2$, this bound is $\lceil (n + 2)/8 \rceil$. Since this is equal to the dimensionality of solutions of the form (3), all solutions have this form. If $c = 4$, the bound is $\lceil (n + 4)/24 \rceil$, which agrees with the dimensionality of solutions of (2) of the form (4).

Finally, when $q = 3$, we do not have that $A_{n-i} = A_i$, so the Pless identities give us jc equations, which express the unknown $A_{jc}, A_{(j+1)c}, \cdots, A_{n-a}$ (where $0 \leq a < c$) in terms of the known $A_0^{\perp}, A_{\perp}^{\perp}, \cdots, A_{jc-1}^{\perp}$. There will be no more than one solution if

$$jc \geq \frac{n - a}{c} - j + 1$$

or

$$j \geq \left\lceil \frac{n + c - a}{c^2 + c} \right\rceil.$$

With $c = 3$, this bound agrees with the dimensionality of solutions of the form (5), and again all solutions must have this form.

References

[1] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.

[2] J. H. Conway, "A characterization of Leech's lattice," *Invent. Math.*, vol. 7, pp. 137–142, 1969.

[3] W. Feit, "Some remarks on weight functions of spaces over GF(2)," to be published.

[4] ——, "On weight functions of self-orthogonal spaces over GF(3)," to be published.

[5] A. M. Gleason, "Weight polynomials of self-dual codes and the MacWilliams identities," in *1970 Act. Congr. Int. Math.*, vol. 3. Paris: Gauthier-Villars, 1971, pp. 211–215.

[6] R. C. Gunning, *Lectures on Modular Forms*. Princeton, N.J.: Princeton Univ. Press, 1962.

[7] J. Leech and N. J. A. Sloane, "Sphere packings and error-correcting codes," *Can. J. Math.*, vol. 23, pp. 718–745, July 1971.

[8] F. J. MacWilliams, "A theorem on the distribution of weights in a systematic code," *Bell Syst. Tech. J.*, vol. 42, pp. 79–94, Jan. 1963.

[9] V. S. Pless, "Power moment identities on weight distributions in error-correcting codes," *Inform. Contr.*, vol. 6, pp. 147–152, June 1963.

[10] ——, "On the uniqueness of the Golay codes," *J. Combinat. Theory*, vol. 5, pp. 215–228, Nov. 1968.

[11] ——, "A classification of self-orthogonal codes over GF(2)," to be published.

[12] J.-P. Serre, *Cours d'Arithmétique*. Paris: Presses Univ. France, 1970.

[13] J. G. Thompson, "A note on a theorem of Gleason," to be published.