ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 5, Number 2, Spring 1975

A SURVEY OF PERFECT CODES

J. H. VAN LINT

1. **Introduction.** In recent years there has been a lot of interest in so-called "perfect codes". Originally a topic in the theory of error-correcting codes, there are now connections to group theory, combinatorial configurations, covering problems and even diophantine number theory. As the results are spread over many fields and journals and since many of them are quite recent there has been a lot of duplication and more is to be expected. For this reason it seems worthwhile to write a survey of what is known (to this author) at the moment.

To introduce the subject and for further use in this survey we need a number of concepts from the theory of error-correcting codes which we now introduce briefly.

Consider a set F of q distinct symbols. We shall call this set the *alphabet*. By $\mathcal{R}^{(n)} : = F^n$ we denote the set of all n-tuples from F, i.e.

$$(1.1) \qquad \mathcal{R}^{(n)} : = \{(a_1, a_2, \cdots, a_n) \mid a_i \in F, i = 1, 2, \cdots, n\}.$$

In many cases we shall impose some algebraic structure, e.g., F will be a ring and $\mathcal{R}^{(n)}$ an F-module. If F is the field $\mathrm{GF}(q)$ we can consider $\mathcal{R}^{(n)}$ as an n-dimensional vector-space over F. We write $\boldsymbol{a} : = (a_1, a_2, \cdots, a_n)$ and use the words *vector* or *word* to denote the n-tuples from $\mathcal{R}^{(n)}$ (n is called the *block length* or *word length*). We also introduce a metric d in $\mathcal{R}^{(n)}$. In coding theory the most familiar metric is *Hamming-distance* defined by

$$(1.2) \qquad \mathrm{d}(\boldsymbol{x}, \boldsymbol{y}) : = \textit{the number of indices i for which } x_i \neq y_i.$$

In many cases one of the symbols of F is denoted by 0 (zero). We then define the *weight* $w(\boldsymbol{a})$ of a word $\boldsymbol{a}$ by

$$(1.3) \qquad w(\boldsymbol{a}) : = \textit{the number of indices i for which } a_i \neq 0.$$

Note that if $\mathbf{0} : = (0, 0, \cdots, 0)$ then $w(\boldsymbol{a}) = d(\boldsymbol{a}, \mathbf{0})$.

If $\boldsymbol{x} \in \mathcal{R}^{(n)}$ and $e \geqq 0$ is an integer we define the *sphere* $S(\boldsymbol{x}, e)$ with center $\boldsymbol{x}$ and radius e by

$$(1.4) \qquad S(\boldsymbol{x}, e) : = \{\boldsymbol{y} \in \mathcal{R}^{(n)} \mid d(\boldsymbol{x}, \boldsymbol{y}) \leqq e\}.$$

Received by the editors November 16, 1972.

Clearly

$$|S(\boldsymbol{x}, e)| = \sum_{i=0}^{e} \binom{n}{i}(q-1)^i. \tag{1.5}$$

Any subset C of $\mathcal{R}^{(n)}$ is called a *code.* If $F = \mathrm{GF}(q)$ and $\mathcal{R}^{(n)}$ is the n-dimensional vector-space over F then C is called a *linear code* (or (n, k)-code) if C is a k-dimensional linear subspace of $\mathcal{R}^{(n)}$. A slightly weaker concept is a *group code.* This name is used if $\mathcal{R}^{(n)}$ is an additive group and C a subgroup. A code C is an *e-error-correcting code* if

$$\forall_{x \in C} \forall_{y \in C} [(\boldsymbol{x} \neq \boldsymbol{y}) \Rightarrow d(\boldsymbol{x}, \boldsymbol{y}) \geqq 2e + 1], \tag{1.6}$$

i.e.,

$$\forall_{x \in C} \forall_{y \in C} [(\boldsymbol{x} \neq \boldsymbol{y}) \Rightarrow S(\boldsymbol{x}, e) \cap S(\boldsymbol{y}, e) = \emptyset]. \tag{1.7}$$

If for such an e-error-correcting code C the union of these spheres is $\mathcal{R}^{(n)}$, i.e.,

$$\mathcal{R}^{(n)} = \bigcup_{x \in C} S(\boldsymbol{x}, e) \tag{1.8}$$

then the code is called *perfect.* In this case there is, for every $\boldsymbol{y} \in \mathcal{R}^{(n)}$, a unique $\boldsymbol{x} \in C$ with $d(\boldsymbol{x}, \boldsymbol{y}) \leqq e$.

In the following we shall make use of some terminology from the theory of linear codes which we now introduce. If C is a linear code of dimension k and $\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_k$ form a basis of C then the matrix G with row-vectors $\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_k$ is called a *generator* matrix of C. A generator matrix H of the orthogonal complement $C^{\perp}$ of C in $\mathcal{R}^{(n)}$ is called a *parity-check* matrix of C. The orthogonal complement itself is called the *dual* code of C. Clearly we have

$$C = \{\boldsymbol{a} \in \mathcal{R}^{(n)} \mid \boldsymbol{a} = (b_1, b_2, \cdots, b_k) G ; b_i \in F, i = 1, 2, \cdots, k\} \tag{1.9}$$

and

$$C = \{\boldsymbol{a} \in \mathcal{R}^{(n)} \mid \boldsymbol{a}H^T = 0\}. \tag{1.10}$$

The error-correcting properties of a code do not change if we apply a permutation π of the places to $\mathcal{R}^{(n)}$, e.g., $\pi(a_1, a_2, \cdots, a_n) = (a_n, a_{n-1}, \cdots, a_1)$. The resulting codes are called *equivalent* codes. Sometimes the definition of equivalence is extended by also allowing a permutation of the symbols of F; (this will in general destroy linearity).

The main purpose of this survey is to discuss the connection of perfect codes to several other problems and to show how the problem of the existence of such perfect codes was completely solved in the case where F is a finite field. First, however, we wish to show how the concept of perfect code, as introduced above, can be generalized in several directions and how some analogous problems can be formulated.

Let $(\mathcal{R}, d)$ be a metric space (d the distance function) and $e > 0$. A subset $C \subset \mathcal{R}$ is called a *perfect e-code* if $\mathcal{R}$ is the disjoint union of the spheres of radius e (as in (1.8)) around the points of C. In this formulation we have a *sphere-packing* problem of a special nature. A rather natural generalization of the Hamming metric is the Lee-metric defined as follows when F is the ring of integers mod q:

$$(1.11) \qquad W_L(x) := \sum_{i=1}^{n} \min\{x_i, q - x_i\},$$

where the sum is taken in $\mathbf{Z}$, and

$$(1.12) \qquad d_L(x, y) := W_L(x - y).$$

Very little is known about perfect codes with this metric. (See § 8.)

A more complicated way to generalize perfect codes is the following. Start with n alphabets $F_1, F_2, \cdots, F_n$ and let $\mathcal{R} := F_1 \times F_2 \times \cdots \times F_n$. Define Hamming metric as in (1.2). Again, we can study perfect codes in $\mathcal{R}$. (See § 8.)

If $\mathcal{R}^{(n)}$ is n-dimensional vector-space over GF(q) and $C \subset \mathcal{R}^{(n)}$ is a perfect e-error-correcting code, then by (1.8) we have $\mathcal{R}^{(n)} = \mathrm{S}(\mathbf{0}, e) \oplus C$, a direct sum. We can now generalize the problem by varying the set S. If, e.g., we take S to include all vectors of weight $\leqq e$ and also some of the vectors of weight $e + 1$ then any solution C is called a *quasi-perfect* code. This class of codes contains codes which are called *nearly perfect*. These will be treated in § 8.

The geometrical problems of packing spheres in $\mathcal{R}^{(n)}$, resp. covering $\mathcal{R}^{(n)}$ with spheres meet in the case of perfect packings (coverings). Therefore it is to be expected that some results concerning perfect codes originate from the study of covering problems. Typical examples are perfect single-error-correcting codes which turned up several times in connection with the following group theory problem (Taussky and Todd [**65**]). Let G be an abelian group with base elements $g_1, g_2, \cdots, g_n$, all of order q. Let S be the set of all powers of the base elements, i.e., $\mathrm{S} = \{g_i^{\alpha} \mid i = 1, 2, \cdots, n; 0 \leqq \alpha < q\}$. Let H be a subset of G such that every element g of G can be written as $g = hs$ with $h \in H$, $s \in \mathrm{S}$. This is called a *group covering*. Taussky and Todd asked for the minimal number of elements in such a set H and whether H could be a subgroup. (See § 2.)

This survey is organized as follows. In § 2 we discuss perfect single-error-correcting codes. In section 3 we discuss the two known nontrivial perfect e-error-correcting codes with $e \geqq 2$. These are known as the Golay codes. We shall illustrate their connection with combinatorial theory and group theory. More connections between perfect codes and combinatorial theory will be discussed in § 4. The interesting properties of the known perfect codes have stimulated the search for more such codes. The obvious thing to do is to consider the necessary condition for the existence of such codes which follows from (1.8) by counting the number of elements on both sides. This leads to a number theoretic problem. The condition, known as the *sphere-packing condition*, is treated in § 5. A deeper theorem yielding a necessary condition for the existence of perfect codes is known as Lloyd's theorem. This is discussed in § 6. In the past few years an extensive study of the combined necessary conditions has led to a proof that all perfect codes over alphabets which are finite fields are known. We summarize the methods in § 7. Finally, in § 8, we shall discuss the generalizations mentioned earlier in this introduction.

2. **Perfect single-error-correcting codes.** Perfect single-error-correcting codes (s.e.c. codes) have been constructed for every field alphabet GF(q). They are known as Hamming codes (sometimes H-G codes, the G for Golay who contributed to the development of the idea first used by Hamming [28]). The codes have been rediscovered a number of times, e.g., as a solution of the problem of Taussky and Todd mentioned in the introduction (see later in this section). We mention the references Cocke [15], Golay [24], Losey [45], Mac Williams [47], Mauldon [49], Zaremba [72], [73].

Hamming codes are defined as follows. Let the m-dimensional vector-space $\mathcal{R}^{(m)}$ over GF(q) be interpreted as a model of the affine geometry AG(m, q). There are $n := (q^m - 1)/(q - 1)$ lines through the origin $\mathbf{0}$. On each of these we choose one non-zero vector. We take these vectors as columns of a matrix H (m rows, n columns). Consider H as the parity-check matrix of a linear code C in $\mathcal{R}^{(n)}$ (cf. (1.1), (1.10)). Since a linear combination of less than three columns of H is zero only if the coefficients are zero, the non-zero words of C all have weight $\geqq 3$. Hence C is an s.e.c. code ((1.6) holds with $e = 1$). C is a subspace of $\mathcal{R}^{(n)}$ with dimension $n - m$. By (1.5) we have $S(\mathbf{x}, 1) = q^m$ for $\mathbf{x} \in C$. Therefore we find from (1.6) that $|\bigcup_{\mathbf{x} \in C} S(\mathbf{x}, 1)| = q^{n-m}q^m = q^n = |\mathcal{R}^{(n)}|$, i.e., (1.7) holds and hence C is perfect! (For a generalization of this idea see § 8.)

The special case $q = 2$ is particularly elegant. We can choose the columns of H to be the binary representations of the integers $1, 2, \cdots, n$. If c is a vector in the Hamming code, i.e., $cH^T = 0$, and c' is obtained from c by changing the j-th coordinate of c (a single error) then $c'H^T$ is the binary representation of j (the place where the error occurs).

Definition (2.1). *If A_i denotes the number of code words of weight i in a code C then $A(z) := \sum_{i=0}^{n} A_i z^i$ is called the weight enumerator of C.*

If C is a perfect s.e.c. code of length n over an alphabet of q symbols (q not necessarily a prime power) then

$$(2.2)\qquad \begin{aligned} A(z) = \frac{1}{n(q-1)+1}\{&[1+(q-1)z]^{n} \\ &+ n(q-1)[1+(q-1)z]^{(n-1)/q}(1-z)^{(n(q-1)+1)/q}\}. \end{aligned}$$

This result is obtained by a straightforward counting argument (Peterson [53] p. 68; van Lint [41] p. 89).

Before looking at the problem of the existence of perfect s.e.c. codes in the case that $|F|$ is not a power of a prime we give an alternate description of Hamming codes, valid if q is a power of a prime, $n = (q^m - 1)/(q - 1)$ and $(n, q-1) = (m, q-1) = 1$. To do this we introduce the concept of a *cyclic code* which will turn up again later. A linear code C is called cyclic if

$$(2.3)\qquad (a_0, a_1, \cdots, a_{n-1}) \in C \Longleftrightarrow (a_{n-1}, a_0, a_1, \cdots, a_{n-2}) \in C.$$

If R denotes the ring of polynomials with coefficients in $\mathrm{GF}(q)$, i.e., $R := (\mathrm{GF}(q)[x], +,)$ and S is the ideal generated by $x^n - 1$, i.e., $S := ((\{x^n - 1\}), +,)$, then the residue class ring $R \bmod S$ is represented by the polynomials $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ of degree $< n$. As an additive group $R \bmod S$ is isomorphic to $\mathscr{R}^{(n)}$ and a cyclic code C corresponds to an ideal in $R \bmod S$ (cf. Peterson [53] p. 137; Berlekamp [12] p. 129; van Lint [41] p. 42). Now let α be a primitive element in $\mathrm{GF}(q^m)$. Then $\beta = \alpha^{q-1}$ is a primitive n-th root of unity in $\mathrm{GF}(q^m)$. The minimal polynomial (over $\mathrm{GF}(q)$) of β, which we call $g(x)$, has degree $\leqq m$. In $R \bmod S$ the polynomial $g(x)$ generates an ideal which corresponds to a cyclic code C of dimension $\geqq n - m$. If we represent $1, \beta, \beta^2, \cdots, \beta^{n-1}$ as vectors (with m coordinates) over $\mathrm{GF}(q)$ and take these vectors as columns of a matrix H then $\boldsymbol{a}H^T = 0$, where $\boldsymbol{a} := (a_0, a_1, \cdots, a_{n-1})$, means the same thing as $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$, i.e., $g(x)$ divides $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ and hence $\boldsymbol{a} \in C$. It is easily seen that the code C is equivalent to a

Hamming code as described earlier in this section. We remark that if $(n, q - 1) \neq 1$, Hamming codes can be described in a similar way by replacing $x^n - 1$ by $x^n - c$; c suitably chosen in $\mathrm{GF}(q)$.

There are no examples known of perfect s.e.c. codes in the case where $|F|$ is not a power of a prime (except of course the trivial example $n = 1$ and C any one-element subset of F). From (1.1), (1.5), (1.8) it is obvious that

$$1 + n(q - 1) \mid q^n \tag{2.4}$$

is a necessary condition for the existence of a perfect s.e.c. code of word length n over an alphabet of q symbols. (We remark that if $q = p^\alpha$, p prime then (2.4) implies that $1 + n(q - 1)$ is a power of q (cf. van Lint [41] p. 87). If $n = q + 1$ then (2.4) is satisfied. The first case to be studied then is $q = 6$, $n = 7$. Strangely enough, this is the only case for which it has been shown that there is no perfect s.e.c. code (cf. Golomb and Posner [25]). The curious exception is a consequence of the nonexistence of two orthogonal Latin squares of order 6. We return to this fact later in this section. If (2.4) holds and $n \equiv 1 \pmod{q}$ then all the coefficients in (2.2) are integers which means that no nonexistence theorem is to be expected from that direction.

If any such perfect codes exist they will be hard to construct. This is a consequence of a theorem of B. Lindström [37] which states that if $n = q + 1$, q is not a power of a prime, and C is a perfect s.e.c. code over an alphabet of q symbols, then C is not a group code! This was generalized by H. W. Lenstra Jr. [35] to:

Theorem (2.5). *Let G_i $(1 \leqq i \leqq n)$ be a group with underlying set F. Suppose there exists a subgroup $C \subset \Pi_{i=1}^n G_i$ such that the underlying set of C is a perfect e-error correcting code of block length n over F, with $e < n$. Then q is a power of a prime p and each G_i is abelian of type $(p, p, \cdots, p)$.*

In 1962 Ju. L. Vasil'ev produced nonlinear perfect s.e.c. codes. Later his construction was generalized. References are Lindström [37], Schönheim [58], Vasil'ev [69]. The results are combined in:

Theorem (2.6). *If q is a power of a prime, $n = (q^{m+1} - 1)/(q - 1)$, where $m \geqq 3$ if $q = 2$ and $m \geqq 2$ if $q \geqq 3$, then there exists a perfect single-error-correcting code of length n over $\mathrm{GF}(q)$ which is not equivalent to a linear code.*

In (2.6) equivalence includes permutation of the symbols of the alphabet. This concludes the discussion on construction and existence of perfect s.e.c. codes. We are left with

Problem (2.7). *Are there any perfect single-error-correcting codes over an alphabet F for which* $|F|$ *is not a power of a prime*?

It is worthwhile tc give a brief look at some interesting results connected with perfect s.e.c. codes discussed in a paper by Golomb and Posner [25]. Let us consider once again a Hamming code C of length $n = q + 1$ over GF(q). The dual $C^\perp$ of this code has dimension 2, i.e., $C^\perp$ consists of q^2 words of length $q + 1$. If, for $\boldsymbol{a} := (a_1, a_2, \cdots, a_n)$ and $\boldsymbol{b} := (b_1, b_2, \cdots, b_n)$, $(\boldsymbol{a} \neq \boldsymbol{b})$, $a_i = b_i$ and $a_j = b_j$ $(i \neq j)$ then $\boldsymbol{a}$ and $\boldsymbol{b}$ are both orthogonal to a word of weight 2. Since there are no words of weight 2 in C it follows that any 2 words $\boldsymbol{a}$ and $\boldsymbol{b}$ in $C^\perp$ have distance $\geqq n - 1 = q$. If we make a list of the q^2 words of $C^\perp$ (q^2 rows, $q + 1$ columns) then in any 2 columns of this list every pair (i, j) occurs once. Such a combinatorial object is called an *orthogonal array* OA$(q, q + 1)$ (cf. Hall [27]). It is well known that the existence of such an array is equivalent to the existence of a projective plane of order q. Now in this discussion we have assumed linearity of C but there is some reason to conjecture that the existence of a perfect s.e.c. code of length $n = q + 1$ is as hard to show as the existence of a projective plane of order q. For many other interesting connections between combinatorial theory and perfect codes we refer to the original paper (Golomb and Posner [25]).

In a *football pool* one wishes to forecast the outcome (win, lose or draw) of n football matches. To win second prize one must have $n - 1$ correct results. The question is what is the most efficient way of making a number of forecasts such that, no matter what the outcome of the matches, at least one of the forecasts will have $\geqq n - 1$ correct results. If $n = (3^m - 1)/2$ there is a solution with 3^{n-m} forecasts and this solution is provided by the Hamming code of length n over GF(3). It was this problem which led Taussky and Todd to their group theory problem mentioned in § 1. Further references: Stanton [62], Johnson [84].

Another amusing (old) problem connected to the Hamming code over GF(3) is the *penny-weighing problem*: Given a balance which can be used to determine whether two weights are equal, or which is heavier, and given a certain quantity of pennies, of which at most one may be heavier or lighter than the standard weight, it is asked to determine what paired assemblies of pennies should have their weight compared with each other, in order to find, with a minimum number of operations, which penny, if any, is too heavy or too light. It is also required that the weighing program be completely predetermined, and thus not affected by the results of the successive weighings. By now the connection to perfect codes should be obvious to the reader. For details we refer to Assmus and Mattson [10], Golay [24], van Lint [38].

3. **The Golay codes.** Obvious and trivial examples of perfect e-error-correcting codes with $e > 1$ are

(3.1) n arbitrary, q arbitrary, $e = n$, C consists of one word;

(3.2) n odd, $q = 2$, i.e., $F := \{0, 1\}$, C consists of the zero word and the all-one word. In this case $e = (n-1)/2$. The code is known as the *repetition code.*

The codes (3.1) and (3.2) are called *trivial* perfect codes. We exclude them from further discussion. There are two known non-trivial perfect e-error-correcting codes with $e > 1$. In this section we discuss representations and properties of these codes which have been shown to be unique (cf. (3.5)). The codes were first discussed by Golay [22]. Here we introduce them as *quadratic-residue codes* (cf. Berlekamp [12] p. 352; van Lint [41] p. 79). We refer to the introduction of cyclic codes in § 2 of this survey.

DEFINITION (3.3). Over GF(2) we have

$$\begin{aligned} x^{23} - 1 &= (x-1)(x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1) \\ &\quad \cdot (x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1) \\ &= (x-1)g_0(x)g_1(x). \end{aligned}$$

The polynomial $g_0(x)$ generates a (23, 12) cyclic code called the binary Golay code.

DEFINITION (3.4). Over GF(3) we have

$$\begin{aligned} x^{11} - 1 &= (x-1)(x^5 + x^4 - x^3 + x^2 - 1)(x^5 - x^3 + x^2 - x - 1) \\ &= (x-1)g_0(x)g_1(x). \end{aligned}$$

The polynomial $g_0(x)$ generates an (11, 6) cyclic code called the ternary Golay code.

There are several ways of showing that the minimum distance of the binary Golay code is 7 and that the minimum distance of the ternary Golay code is 5 (cf., e.g., van Lint [41]). For both codes (1.8) then follows by counting (cf. (1.5)). Hence the binary Golay code is a perfect 3-error-correcting code over GF(2) and the ternary Golay code is a perfect 2-error-correcting code over GF(3).

In the following theorem we call two codes equivalent if one is obtained from the other by a monomial transformation on the vector space $\mathscr{R}^{(n)}$, i.e., a linear mapping defined by a matrix DP where D is a diagonal matrix and P a permutation matrix. The following theorem is due to V. Pless [54] (see Comment (9.1)!):

THEOREM (3.5).

(i) *Every perfect* 2-*error-correcting code of word length* 11 *over* GF(3) *is equivalent to the ternary Golay code,* (*assuming linearity*),

(ii) *every perfect* 3-*error-correcting code of word length* 23 *over* GF(2) *is equivalent to the binary Golay code,* (*assuming linearity*).

In fact more is proved in the paper. For codes with the parameters of the Golay codes a number of properties are shown to be equivalent. One of these is the property of being perfect, another is equivalence with a Golay code. The proof depends on the following property that both of the Golay codes have. If C is an (n, k) code we call C^+ the *extended* code if $C^+ \subset \mathscr{R}^{(n+1)}$ is obtained by adding an extra coordinate to the words of C, which coordinate is a fixed linear combination of the remaining coordinates. Then C^+ is an $(n + 1, k)$ code. The most common extension is obtained by requiring that in the extended code every word is orthogonal to $(1, 1, \cdots, 1)$. Then it can be shown that the following is true.

THEOREM (3.6). *The extended Golay codes are self-dual if the original codes are suitably represented,* (cf. van Lint [41], Pless [54]).

This property was used by Goethals [20] to construct a simple decoding algorithm for the binary Golay code. For other decoding methods see Assmus and Mattson [10], Chien [14].

The following representations of the two Golay codes are often useful. For details we refer to Karlin [33], van Lint [41]. Let C_{11} be the circulant matrix of size 11 with first row (11011100010) and let C_5 be the circulant matrix of size 5 with first row $(0\ 1\ -1\ -1\ 1)$. Then

$$G_1 : = \begin{bmatrix} & 1\,1 \cdots 1 \\ \mathrm{I}_{12} & C_{11} \end{bmatrix}, \quad G_2 : = \begin{bmatrix} & 1\,1\,1\,1\,1 \\ I_6 & C_5 \end{bmatrix}$$

are generator matrices of the two Golay codes.

A particularly simple description of the binary Golay code was given by R. Turyn, cf. ref. [7]. Let H be the $(8, 4)$ code obtained by extending the $(7, 4)$ Hamming code. Numbering the positions from 1 to 8 we obtain the code H' by applying the permutation $(1, 7)\ (2, 6)\ (3, 5)$ to the positions. Then

$$V : = \{(a + c, b + c, a + b + c) \mid a \in H, b \in H, c \in H'\}$$

is a (24, 12) linear code over GF(2). By showing that this code has minimum distance 8 it follows from (3.5) that V is the extended binary Golay code. For details we refer to van Lint [41] p. 100.

For the sake of completeness we give the weight enumerators of the Golay codes. Obviously the fact that the codes are perfect is enough information to calculate these weight enumerators. Several other methods are faster. The weight enumerator of the binary Golay code is:

(3.6)

$$1 + 253\, z^{7} + 506\, z^{8} + 1288\, z^{11} + 1288\, z^{12} + 506\, z^{15} + 253\, z^{16} + z^{23};$$

the weight enumerator of the ternary Golay code is

$$1 + 132\, z^{5} + 132\, z^{6} + 330\, z^{8} + 110\, z^{9} + 24\, z^{11}. \tag{3.7}$$

Recently Goethals [20] obtained a new non-linear code, having 256 code words of length 16 at mutual distance at least 6 by considering a subset of the binary Golay code and dropping 8 coordinates. He showed that dropping one more coordinate gives a code equivalent to the Nordstrom-Robinson code (Nordstrom and Robinson [51]). Preparata [56] gave a method of extending a class of nonlinear 2-error-correcting codes which, when applied to the Nordstrom-Robinson code, produces the binary Golay code. This is Goethals' result obtained from the other direction. Other results obtained by considering a subset of the positions in the Golay codes will be mentioned in the next section.

Many interesting groups can be described by considering automorphism groups of certain combinatorial configurations, i.e., permutation groups on the elements of such a configuration which leave the configuration invariant. As an example one can consider a code and permute the coordinate places as we did in the definition of equivalence in § 1. Those permutations which leave the code invariant (as a subset of $\mathcal{R}^{(n)}$) form the *automorphism group* of the code. It was shown by Assmus and Mattson [4] that the automorphism groups of the extended Golay codes are the *Mathieu groups* M_{24} and M_{12}, (cf. also Berlekamp [12] p. 395; Paige [52]). The groups M_{11}, M_{22}, M_{23} appear as the automorphism groups of special tactical configurations called Steiner systems (see § 4) obtained from the Golay codes. Recent discoveries of new simple groups on the one hand and the connection between the Mathieu groups and the Golay codes on the other explain the interest of group theorists in the search for new perfect codes. The results to be discussed in § 7 were a disappointment for them. (Additional reference: Todd [93]).

4. **Perfect codes and combinatorial theory.** There are several connections between perfect codes and combinatorial theory. Most of these are applications in which error-correcting properties of the codes are not important but where the structure of the codes leads to interesting results. We mentioned a few of these results in § 2 (Golomb and Posner [25]).

DEFINITION (4.1). A *tactical configuration of type* λ; $t - d - n$ (also called a *t-design*) is a collection $\mathfrak{D}$ of d-subsets of an n-set S such that every t-subset of S is contained in exactly λ distinct members of $\mathfrak{D}$. To avoid trivial configurations one usually demands $0 < t < d < n$.

For the special case $t = 2$ the tactical configuration is called a *balanced incomplete block design.* In the case $\lambda = 1$ the tactical configuration is called a *Steiner system* of type (t, d, n). The following theorem illustrates the connection with perfect codes. We state the result only for binary codes. By adding the assumption of linearity it can be generalized to other alphabets (Assmus and Mattson [5]).

THEOREM (4.2). *Let V be a binary perfect e-error-correcting code of block length n and assume* $\mathbf{0} \in V$. *Then the collection* $\mathfrak{D}$ *of* $(2e + 1)$ *subsets D of* $\{1, 2, \cdots, n\}$ *for which there is a codeword in V with its nonzero coordinates in the positions of D is a Steiner system of type* $(e + 1, 2e + 1, n)$.

For a proof see van Lint [41] p. 95. A simple counting argument then leads to the following theorem.

THEOREM (4.3). *If a binary perfect e-error-correcting code of block length n exists then the numbers*

$$\binom{n-h}{e+1-h} \Big/ \binom{2e+1-h}{e+1-h}, \quad h = 0, 1, \cdots, e$$

are all integers.

This theorem has been used to show the non-existence of certain perfect codes. Now that the results of § 7 are known the theorem has lost its importance. Another theorem of the type of (4.2) is

THEOREM (4.4). *The codewords of weight* 8 *(interpreted as subsets of* $\{1, 2, \cdots, 24\}$*) in the extended binary Golay code form a Steiner system of type* $(5, 8, 24)$.

Goethals [20] derived several block designs from this Steiner system. For extensive treatment of this type of application of perfect codes cf. Assmus and Mattson [5], [6], [8], [9]; Paige [52]. The results of Assmus and Mattson were generalized to semilinear codes by J. Schönheim [59]. For a connection between tactical configurations and nearly perfect codes see § 8.

An interesting application of the ternary Golay code to graph theory is given in Berlekamp, van Lint and Seidel [13]. The paper is concerned with strongly regular graphs in which every adjacent pair of vertices is in exactly one triangle and every non-adjacent pair of vertices is in exactly one quadrangle. If n is the number of vertices of such a graph then one can show that n must be one of the integers 9, 99, 243, 6273 or 494019. The example for $n = 9$ is easily found. For $n = 243$ the ternary Golay code provided an example in the following way. The columns of the 5 by 11 parity check matrix H of the ternary Golay code are considered as points $\mathbf{x}_i$ $(i = 1, 2, \cdots, 11)$ in 5-dimensional vector space over GF(3). The vertices of the graph are $\mathbf{0}$, $\pm x_i$, $(i = 1, 2, \cdots, 11)$, and $\pm x_i \pm x_j, i \neq j$, $(i, j = 1, 2, \cdots, 11)$. If the difference of two vertices is $\pm \mathbf{x}_k$ they are called adjacent. It is easy to check that this graph has the required properties. For the other 3 values of n the problem is still open.

5. **The sphere-packing condition.** An obvious necessary condition for the existence of a perfect e-error-correcting code of word length n over an alphabet of q symbols (if q is a power of a prime p we write $q = p^\alpha$) is obtained from (1.5) and (1.8) in the same way as (2.4). The condition is

$$(5.1) \qquad \sum_{i=0}^{e} \binom{n}{i}(q-1)^i \mid q^n$$

and it is known as the *sphere-packing-condition.* If $q = p^\alpha$ it follows from (5.1) that

$$(5.2) \qquad \sum_{i=0}^{e} \binom{n}{i}(q-1)^i = q^k.$$

By expanding the power of $(q - 1)$ we find

$$(5.3) \qquad \sum_{j=0}^{e} (-1)^j q^j \binom{n}{j}\binom{n-j-1}{e-j} = (-1)^e q^k.$$

A counting argument of the same type as was used to derive (5.1) is the following. Consider a perfect e-error-correcting code and assume without loss of generality that $\mathbf{0}$ is in the code. All the other words of the code have weight at least $2e + 1$. Hence each word of weight $e + 1$ is at distance e from exactly one codeword of weight

$2e + 1$. Hence the number A_{2e+1} (cf. (2.1)) is $[\binom{n}{e+1}/\binom{2e+1}{e}](q-1)^{e+1}$ Hence

THEOREM (5.4). *A necessary condition for the existence of a perfect e-error-correcting code of block length n over an alphabet of q symbols is that*

$$[\tbinom{n}{e+1}/\tbinom{2e+1}{e}](q-1)^{e+1}$$

is an integer.

Note that $q = 2$ yields the case $h = 0$ in (4.3).

Extensive computer searches have been made to find solutions of (5.2) with $e > 1$. The ranges that were covered were:

(a) $e = 2$, q odd, $3 \leqq q \leqq 125$, $3 \leqq k \leqq 40000$ (Cohen [**16**]),

(b) $e \leqq 20$, $q = 2$, $n \leqq 2^{70}$ (McAndrew [**50**]),

(c) $e \leqq 1000$, $q \leqq 100$, $n \leqq 1000$ (van Lint [**38**]).

Excluding the parameters of trivial codes the computer searches yielded only the parameters of the Golay codes and $q = 2$, $e = 2$, $n = 90$. The last set is excluded by (4.3).

The first papers on nonexistence of perfect codes all started with the equation (5.2). The theorems are of two different types which we now discuss briefly. The first method is due to Shapiro and Slotnick [**61**]. They observed that if $q = 2$ and e is odd, then the left-hand side of (5.2) can be written as $(n + 1)R_e(n)/e!$, where $R_e(n)$ is a polynomial of degree $e - 1$ with integer coefficients. Therefore (5.2) implies that $n + 1 = 2^{\ell}b$, where $b \mid e!$, and substitution in $R_e(n)$ yields an equation for ℓ and b. It follows that the possible values of n are in a finite set. This had also been observed by Golay [**23**]. The method of Shapiro and Slotnick was also applied by Leont'ev [**36**]. By a modification of this same method and using only hand computation Johnson [**31**] showed there are no nontrivial binary perfect e-error-correcting codes for $5 \leqq e \leqq 29$, e odd. This was extended to $e \leqq 39$, e odd by James, Stanton and Cowan [**30**].

The other early nonexistence theorems all concern $e = 2$. For that case (5.2) can be interpreted as a quadratic equation in n. For this equation to have a solution in integers it is necessary that the diophantine equation $x^2 - (q^2 - 6q + 1) = 8q^k$ has a solution in integers. This diophantine equation can be treated by considering a suitable algebraic extension of Q or using continued fraction methods. The following cases were settled:

(a) $q = 5$, Engelman [**19**]

(b) $q \leqq 5$ (and $q = 6$, assuming linearity), Cohen [**16**]

(c) $7 \leqq q \leqq 9$, Alter [**1**], [**2**].

In each case no unknown solutions to (5.2) were found. Although as far as perfect codes are concerned the problem has been settled, the purely number-theoretic problem of finding all solutions of (5.2) remains open. (cf. also Alter [3]).

6. **Lloyd's theorem.** A necessary condition for the existence of a perfect binary code, deeper than (5.2), was found by Lloyd [44]. This theorem was generalized by F. J. MacWilliams [46] and recast by A. M. Gleason (cf. Assmus and Mattson [5]). Below we shall sketch a proof for the case $q = p^\alpha$ (p prime) as given in van Lint [41]. Recently it was shown by Delsarte [17] and Lenstra [35] that the theorem holds for all q. A polynomial which plays a role in the theorem has been shown by Delsarte to be connected with a sequence of orthogonal polynomials defined by Kravčuk in 1929 (cf. Szegö [64]).

Before formulating Lloyd's theorem we introduce the Kravčuk polynomials. We assume n is fixed.

Definition (6.1). The *Kravčuk polynomial $P_k(x)$ of degree k* is defined by

$$P_k(x) := \sum_{j=0}^{k} (-1)^j (q-1)^{k-j} \binom{x}{j} \binom{n-x}{k-j}, \quad 0 \leqq k \leqq n,$$

where

$$\binom{x}{j} := \frac{x(x-1)\cdots(x-j+1)}{j!}$$

The Kravčuk polynomials are connected to the MacWilliams transform for the weight enumerator of a code and its dual (cf. Berlekamp [12] 16.2) in the following way:

If $A(x, y) := \sum_{i=0}^{n} A_i x^i y^{n-i}$ then

$$B(x, y) := A(y - x, y + (q-1)x) = \sum_{i=0}^{n} B_k x^k y^{n-k}$$

where $B_k = \sum_{i=0}^{n} A_i P_k(i)$. The polynomials $P_k(x)$ satisfy the orthogonality conditions

$$(6.2) \quad \sum_{i=0}^{n} \binom{n}{i} (q-1)^i P_r(i) P_s(i) = \binom{n}{r} q^n (q-1)^r \delta_{rs}, 0 \leqq i \leqq n,$$

where δ_{rs} is the Kronecker symbol. (For further relations see Delsarte [17]).

Definition (6.3). *Lloyd's polynomial* $Q_e(x)$ is defined by

$$Q_e(x) := \sum_{k=0}^{e} P_k(x), \quad (0 \leqq e \leqq n).$$

The polynomial $Q_e(x)$ has degree e and can be written as

$$(6.5) \qquad Q_e(x) = \sum_{i=0}^{e} (-1)^i \binom{x-1}{i} \binom{n-x}{e-i} (q-1)^{e-i},$$

or

$$(6.6) \qquad Q_e(x) = (-1)^e \sum_{j=0}^{e} (-1)^j q^j \binom{n-x}{j} \binom{n-j-1}{e-j}.$$

Then we have

Theorem (6.7). *If a perfect e-error-correcting code of block length n over an alphabet of q symbols exists, then $Q_e(x)$ has e distinct integral zeros among* $1, 2, \cdots, n$.

Essentially the theorem depends on a counting argument. No structure of the alphabet is necessary and the perfect code need not be linear. The proof we sketch is for the case $q = p^\alpha$ in which case we can take GF(q) for our alphabet. This allows us to make certain simplifications but these are not essential (cf. Lenstra [35]).

Let $(\mathfrak{A}, \oplus, *)$ be the group ring of $\mathscr{R}^{(n)}$ over Q where we use $\oplus$ and $\mathbf{\Sigma}$ to distingusih formal addition from vector addition in $\mathscr{R}^{(n)}$. The set $\mathfrak{A}$ is

$$\mathfrak{A} := \left\{ \mathbf{\Sigma}_{x \in \mathscr{R}^{(n)}} \alpha_x x \mid \alpha_x \in Q \right\}.$$

In the following we identify any subset $C \subset \mathscr{R}^{(n)}$ with the element $\mathbf{\Sigma}_{c \in C}\, c$ of $\mathfrak{A}$. If C is a perfect e-error-correcting code and $S_e := S(\mathbf{0}, e)$ (cf. (1.4)) then

$$(6.8) \qquad S_e * C = \mathscr{R}^{(n)}.$$

If $v_i := (1, 1, \cdots, 1, 0, 0, \cdots, 0) \in \mathscr{R}^{(n)}$ is the vector for which the first i coordinates are 1 and the other coordinates are 0, then $C_i := \{c + v_i \mid c \in C\}$ is also a perfect code and C_i has minimum weight i $(0 \leqq i \leqq e)$. The elements $C_0, C_1, \cdots, C_e$ are linearly independent over Q. Let G be the group of all monomial transformations of $\mathscr{R}^{(n)}$. Then the mapping T defined by

$$(6.9)\qquad T\left(\sum \alpha_x x\right) := \frac{1}{|G|}\sum \alpha_x \sum_{\varphi\in G} \varphi(x)$$

is a homomorphism of $\mathfrak{A}$ into the $(n+1)$-dimensional subspace

$$\bar{\mathfrak{A}} := \left\{ \sum_{i=0}^{n} \alpha_i \left(\sum_{x\in\mathcal{R}^{(n)}, w(x)=i} x \right) \mid \alpha_i \in Q \right\}.$$

A straightforward calculation shows that $S_e(A) := S_e * A$ defines a linear transformation of $\bar{\mathfrak{A}}$ and that the e linearly independent elements $\bar{C}_i - \bar{C}_0$ $(i = 1, 2, \cdots, e)$ satisfy $S_e(\bar{C}_i - \bar{C}_0) = 0$. Hence the kernel K of S_e has dimension at least e. For the next step of the proof let χ be any non-trivial character on $(\mathrm{GF}(q), +)$. Then it is not hard to show that if we define $\chi_v : \mathcal{R}^{(n)} \rightarrow C^\times$ by $\chi_v(x) := \chi((x, v))$ and extend this in the obvious way to a linear functional on $\mathfrak{A}$, then the functionals $\chi_i := \chi_{v_i}$ span the space of all linear functionals on $\bar{\mathfrak{A}}$. A direct calculation shows that $\chi_w(S_e) = Q_e(w)$ for $w = 0, 1, \cdots, n$. Since $\chi_w(S_e)\chi_w(A) = 0$ for all A in K and the χ_w are linearly independent there must be at least (and therefore exactly) e integral values of w for which $Q_e(w)$ vanishes. Since $Q_e(0) \neq 0$ this proves the theorem.

We mention that these zeros of Q_e are exactly the weights of the words in the dual of the perfect code in case this code is linear. For this and details of the proof we refer to van Lint [41]. Lenstra's proof for arbitrary q follows the same pattern, replacing characters by suitable homomorphisms, etc. (also see Delsarte [78], [79]).

The original proof in Lloyd [44] reduced the counting argument to a differential equation. The necessary condition for the existence of a binary perfect e-error-correcting code then amounted to the vanishing of e of the coefficients of $(1 + x)^e(1 - x)^{n-1-e}$, expanded as a polynomial. Roos [57] proved the same formulation of Lloyd's theorem for $q = p$ in a purely algebraic way. The proof also depends on the idea of averaging over all translations of the code which is the basis of the proof we have sketched.

7. **Nonexistence theorems.** Although Lloyd [44] treated a few examples in his paper he did not use his theorem to prove the nonexistence of classes of perfect codes and the theorem remained unused for several years. Johnson [31] used Lloyd's theorem to give an alternate proof for the cases $q = 2$, $e = 2$ or 3 which had been settled by number theory methods (see § 5). In retrospect it is remarkable to see how simple the general treatment of $e = 2$ and $e = 3$, with no restriction on q, turned out to be. The proof for $e = 2$ (van Lint [39]) uses the sphere-packing condition and Lloyd's theorem

and the simple observation that $Q_e(0)$ is the left-hand side of (5.2), (cf. (6.5)). With this information on the product of the zeros of the quadratic polynomial $Q_2(x)$ it took only one page to show that there are no perfect 2-error-correcting codes with $q = p^\alpha > 3$, $n > 2$. The proof that the Golay code is the only nontrivial perfect 3-error-correcting code was even simpler. Two consecutive integers were found for which $Q_3(x)$ had different signs!

The method used for $e = 2$ depended on solving the quadratic equation $Q_2(x) = 0$. Of course this method did not look promising for $e > 3$. In fact only $e = 4$ looked feasible. The first nonexistence proof for the case $q = 2$, $e = 4$ was (unnecessarily) extremely complicated. In this proof (van Lint [42]) the equation $Q_4(x) = 0$ was solved explicitly. Lloyd's theorem then led to the condition that $(n - 1) \pm (3n - 7 \pm \sqrt{6n^2 - 30n + 40})^{1/2}$ is an even integer for all four choices of signs. The resulting set of diophantine equations was treated by using a method which had just been developed by Baker and Davenport [11]. This involved two hours computing time on ATLAS I. Although this was interesting as a second application of this method of Baker and Davenport this author soon realized that instead of using only Lloyd's theorem as he had done, the proof for $e = 4$ should also have exploited the connection between (5.2) and (6.5) as was done for $e = 2$ and $e = 3$. For $e = 4$ this connection implies that $Q_4(0)$ is a power of 2 and since the product of the zeros of $Q_4(x)$ is $3Q_4(0)/2$ three of the zeros of $Q_4(x)$ are powers of 2. This observation led to a proof in a few lines (van Lint [38]) that there are no nontrivial binary perfect 4-error-correcting codes.

At this point the idea which would lead to the proof that all perfect codes over finite fields are known had been born. The idea, mentioned above in the case $q = 2$, $e = 4$ was generalized by this author (van Lint [43]) to all q and $p > e$. Simultaneously Tietäväinen [66] observed that the method used by van Lint [39] for $e = 2$ and $e = 3$ could be generalized to $e = 4$, i.e., the restriction $q = 2$ which we used above is unnecessary.

Actually the whole idea of the nonexistence proofs is extremely simple. We have already remarked that $Q_e(0)$ is equal to the left-hand side of (5.2) and hence a power of q. By calculating the first two coefficients of $Q_e(x)$, we then know the sum and the product of the zeros of this polynomial:

$$x_1 + x_2 + \cdots + x_e = \frac{e(n-e)(q-1)}{q} + \frac{e(e+1)}{2}, \tag{7.1}$$

$$x_1 x_2 \cdots x_e = e!q^{k-e}. \tag{7.2}$$

Using the alternating character of the expression (6.5) a lower bound for the zeros of $Q_e(x)$ can be obtained. Combined with a relatively simple divisibility argument this was sufficient to prove the following theorem.

THEOREM (7.3). *If $e \geqq 3$, $q = p^\alpha$, $p > e$ then there is no nontrivial perfect e-error-correcting code over* GF(q).

For details we refer to van Lint [**41**], [**43**]. This method also works for $p < e$ if $p \nmid e$. For fixed e the theorem leaves only a finite number of values of p to be considered. These can all be treated by exactly the same method (and a little more care) as was shown in van Lint [**40**] for $e = 5, 6$ and 7.

To complete the nonexistence theorems a refinement was necessary. This was provided by Tietäväinen [**67**], [**68**]. The first new trick is an elegant application of a refined arithmetic-geometric mean inequality to (7.1) and (7.2). The second is the observation that (7.2) implies that for $p \leqq e$, there is at least one pair of zeros x_i, x_j with $x_i/x_j = p^\nu$, which is not difficult to prove. Finally small values of n are excluded by the Elias bound (cf. Berlekamp [**12**] ch. 13). These ideas combined with a skillful treatment of several inequalities led to the following theorem:

THEOREM (7.4). *If $e \geqq 4$, $q = p^\alpha$, $p \leqq e$ then there is no nontrivial perfect e-error-correcting code over* GF(q).

For details we refer to Tietäväinen [**68**]. Clearly (7.3) and (7.4) completely settle the problem of the existence of perfect codes over finite fields. In § 6 we mentioned that Lenstra [**35**] had shown Lloyd's theorem to be true for all q. The reason this has not led to new nonexistence theorems yet is the fact that if q is not a power of a prime then (5.2) must be replaced by (5.1) and (7.2) is no longer as useful. (See Comments (9.2) and (9.3)!)

8. **Generalizations.** In § 1 we introduced the Lee-metric (1.11, 1.12) (cf. Lee [**34**]). For this metric one can again study perfect codes and ask the same questions which have been treated for the Hamming metric. Very little is known about perfect codes for this metric. We mention:

THEOREM (8.1). *For any given t, there exists a perfect t-Lee-error-correcting code of block length $n = 2$ over the alphabet of integers* mod $q = 2t^2 + 2t + 1$ (cf. Berlekamp [**12**], ch. 13).

Golomb and Welch [**26**] conjectured that for $t > 1$, $n > 2$ and $q > 3$ there are no perfect Lee-error-correcting codes. They treated a number of special cases (namely $n = 3$, $t = 2$, and $n > 2$, $t > t_n$) but essentially the problem is still completely open.

Clearly the sphere-packing condition for the Lee metric is obtained in the same way as (5.1) namely by calculating $|S(0, e)|$ for the Lee metric. The result is

$$\sum_{i=0}^{t} 2^i \binom{n}{i}\binom{t}{i} \mid q^n, \quad (t \leqq (q-1)/2) \tag{8.2}$$

where t is the number of errors. In § 5 we saw that the sphere-packing bound alone has led to only a few nonexistence theorems. In fact it was only the combination with Lloyd's theorem which led to success. So we have

Problem (8.3). Is there an analog of Lloyd's theorem for perfect codes in the Lee metric? (See Comment (9.4)!)

The problem of sphere-packing with no gaps using a metric which is a combination of the Hamming and Lee metrics also occurs in a paper by S. K. Stein [63]. His results are similar to those of Golomb and Welch. (Also see Stein [90], [91]).

Herzog and Schonheim [29] have generalized the idea on which Hamming codes are based to construct perfect codes for $\mathscr{R} := F_1 \times F_2 \times \cdots \times F_n$ where each F_i is a field and Hamming metric is defined as in (1.2). Let the abelian group G be the union of n subgroups $G_1, G_2, \cdots, G_n$ which pairwise have only the zero element of G in common. Then $(x_1, x_2, \cdots, x_n) \rightarrow x_1 + x_2 + \cdots + x_n$ is a homomorphism of $\mathscr{R} := G_1 \times G_2 \times \cdots \times G_n$ into G. The kernel of this homomorphism is a group code in $\mathscr{R}$. It is easily seen that this code is single-error-correcting. This is the idea used in § 2 where AG(m, q) was written as the union of all lines through the origin. Herzog and Schonheim give an example of a perfect code in GF(4) × GF(2) × GF(2) × GF(2) × GF(2), namely

$$\begin{array}{ll}
(0,0,0,0,0) & (1,0,1,1,0) \\
(\beta,1,1,0,0) & (\alpha,0,1,0,1) \\
(\alpha,1,0,1,0) & (\beta,0,0,1,1) \\
(1,1,0,0,1) & (0,1,1,1,1),
\end{array} \tag{8.4}$$

where $\{0, 1, \alpha, \beta\} = \mathrm{GF}(4)$. We remark that in this example each element of GF(4) is followed by a complementary pair of words of a Hadamard code (cf. Peterson [53], § 5.7 and also [83], [86]).

Let $S^*(\mathbf{0}, e)$ be a subset of $\mathcal{R}^{(n)}$ with

$$(8.5)\qquad S(\mathbf{0}, e) \subset S^*(\mathbf{0}, e) \subset S^*(\mathbf{0}, e+1)$$

(where inclusions are strict). If an e-error-correcting code C has the property

$$(8.6)\qquad \mathcal{R}^{(n)} = \bigcup_{x \in C} (x + S^*(\mathbf{0}, e)), \quad \text{a disjoint union,}$$

then the code C is called *quasiperfect.* This generalizes (1.8). Such codes can be obtained, e.g., by dropping certain coordinates from all words of a Hamming code. There are very many quasiperfect codes. Apparently (8.6) is so much less restrictive than (1.8) that the resulting codes do not have such interesting properties. For a number of results we refer to Peterson [53], Wagner [70], [71], [94].

Recently Goethals and Snover [21] introduced the concept of *nearly perfect code.* Johnson [32] proved that for a binary code C of length n and minimum distance $2e + 1$ the following bound for the number of codewords holds

$$(8.7)\, |C| \left\{ \sum_{i=0}^{e} \binom{n}{i} + \frac{1}{\left[\frac{n}{e+1}\right]} \binom{n}{e} \left(\frac{n-e}{e+1} - \left[\frac{n-e}{e+1} \right] \right) \right\} \leqq 2^n.$$

Note that for a binary perfect code we have $(e + 1) \mid (n - e)$ by (4.3) and that equality holds in (8.7) (cf. (5.1), (5.2)). Now any code for which equality holds in (8.7) is called nearly perfect. This includes the perfect codes and the shortened Hamming codes and also the Preparata 2-error-correcting codes (Preparata [55]). Many of the properties of perfect codes discussed in this survey were generalized to nearly perfect codes by Goethals and Snover, e.g., theorem (4.2), (5.2) and Lloyd's theorem. We mention one example of such a generalization of (4.2).

THEOREM (8.8). *In any nearly perfect e-error-correcting code of length n, the codevectors at distance $d = 2e + 1$ from a given codevector determine an e-design with parameters* $[(n - e)/(e + 1)]$; (e, d, n). (cf. (4.1)).

The generalization of Lloyd's theorem is

THEOREM (8.9). *If a nearly perfect binary e-error-correcting code of block length n, with $n + 1 \not\equiv 0 \pmod{e + 1}$, exists, then*

$$Q_{e-1}(x) + \frac{1}{[(n+1)/(e+1)]} \{Q_{e+1}(x) - Q_{e-1}(x)\}$$

has $e + 1$ distinct integral zeros among $1, 2, \cdots, n$.

Of course this raises:

PROBLEM (8.10). Generalize (7.3) and (7.4) to nearly perfect codes.

The combinatorial theorems of which (8.8) is an example combined with the conjecture that there is no nontrivial 6-design justify the conjecture that all the nearly perfect codes are known. Similar results to those of Goethals and Snover were found independently by Semakov, Zinovjev and Zaitzev [60] in a paper on *uniformly packed codes*, a special type of quasiperfect codes. (See Comment (9.5)!)

In § 6 we mentioned that the e distinct integral zeros of $Q_e(x)$ in the case of a linear perfect code are exactly the distinct nonzero weights occurring in the dual code. This led Delsarte [18] to a generalization of the duals of perfect codes by considering codes with e distinct nonzero weights satisfying equality in a certain bound on the number of codewords. Besides the duals of perfect codes he found other examples. The most interesting fact from our point of view is that a generalization of Lloyd's theorem again holds. (See Comment (9.6)!)

It seems that in this area of combinatorics many more interesting results are to be expected. It is the hope of this author that the present survey will prevent unnecessary duplication of research and enable the interested readers to work on those problems which are open at this moment.

9. **Comments** (added in proof). In accordance with the last sentence of § 8 we add some comments on papers which appeared since the manuscript of this survey was submitted. We have added 23 references to the original list. Some of these are older papers of which this author was not aware. For drawing his attention to these papers and for several helpful suggestions concerning small changes in the survey the author wishes to thank many of the persons mentioned in the references.

COMMENT (9.1). In Theorem (3.5) linearity of the codes is assumed. In the meantime it has been shown by Snover [89] and by Delsarte and Goethals [80] that Theorem (3.5) holds even if linearity is not assumed.

COMMENT (9.2). Shortly after Tietäväinen, a proof very similar to his proof was found independently by V. A. Zinov'ev and V. K. Leont'ev [85], [95], [96].

COMMENT (9.3). Recently Tietäväinen [92] produced a nonexistence proof for perfect codes which is much shorter than his original proof. He excludes $q = 2$. In van Lint [87] it is shown that a slight modification makes the proof valid for $q = 2$. This paper also includes some information on the nonexistence of perfect codes when q is not a prime power.

COMMENT (9.4). The answer to Problem (8.3) is yes. A proof was recently provided by L. A. Bassalygo [74].

COMMENT (9.5). The original idea of uniformly packed codes has been generalized even further; cf. Bassalygo, Zaitzev and Zinov'ev [75]. Recently Goethals and van Tilborg have found a number of interesting sequences of uniformly packed codes. Their paper is in preparation. Also see van Lint [87].

COMMENT (9.6). A very interesting generalization of perfect codes in $\mathbf{R}^{(n)}$ is the concept of a perfect code in a graph as defined by Biggs [76], [77]. Also see Heden [82], Hammond and Smith [88]. A general theory containing nearly all the concepts treated in this survey is the theory of association schemes in coding theory. This was developed by Delsarte [78], [79]. Both of these papers are highly recommended to those readers who wish to gain more insight into the theory of perfect codes.

REFERENCES

1. R. Alter, *On the Nonexistence of Close-Packed Double Hamming-Error-Correcting Codes on $q = 7$ Symbols,* J. Comp. Syst. Sci. **2** (1968), 169–176.

2. ——, *On the Nonexistence of Perfect Double Hamming-Error-Correcting Codes on $q = 8$ and $q = 9$ Symbols,* Inf. and Control **13** (1968), 619–627.

3. ——, *On a Diophantine Equation Related to Perfect Codes,* Math. of Comp. **25** (1971), 621–624.

4. E. F. Assmus Jr. and H. F. Mattson, *Perfect Codes and the Mathieu Groups,* Archiv d. Math. **17** (1966), 121–135.

5. ——, *Cyclic Codes,* Report AFCRL-66-348 of the Applied Research Laboratory of Sylvania Electronic Systems, Waltham, Mass. (1966).

6. ——, *On the number of Inequivalent Steiner Triple Systems,* J. Comb. Theory **1** (1966), 301–305.

7. ——, *A simple construction of the binary Golay code,* Report AFCRL-67-0365 of the Applied Research Laboratory of Sylvania Electronic Systems, part VI (1967).

8. ——, *On Tactical Configurations and Error-Correcting Codes,* J. Comb. Theory **2** (1967), 243–257.

9. ——, New 5-Designs, J. Comb. Theory **6** (1969), 122–151.

10. ——, *Algebraic Theory of Codes* II, Report AFCRL-69-0461 of the Applied Research Laboratory of Sylvania Electronic Systems (1969).

11. A. Baker and H. Davenport, *The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$,* Quart. J. of Math. **20** (1968), 129–137.

12. E. R. Berlekamp, *Algebraic Coding Theory,* McGraw-Hill Book Comp., New York (1968).

13. E. R. Berlekamp, J. H. van Lint and J. J. Seidel, *A strongly regular graph derived from the perfect ternary Golay Code,* in J. N. Srivastava (ed.), *A Survey of Combinatorial Theory,* North Holland Publ. Comp., Amsterdam (1973).

14. R. T. Chien, *On Golay's perfect codes and step by step decoding,* IEEE Trans. Inform. Theory IT 12 (1966), 403-404.

15. J. Cocke, *Lossless symbol coding with nonprimes,* IEEE Trans. Inform. Theory, 5 (1959), 33-34.

16. E. L. Cohen, *A Note on Perfect Double Error-Correcting Codes on q Symbols,* Inf. and Control. 7 (1964), 381-384.

17. P. Delsarte, *Linear programming associated with coding theory,* Report R 182 of MBLE Research Laboratory, Bruxelles, Belgium (1971).

18. ———, *Four fundamental parameters of a code,* Report R 184 of MBLE Research Laboratory, Bruxelles, Belgium (1972).

19. C. Engelman, *On Close-Packed Double Error-Correcting Codes on P Symbols,* IRE Trans-Inform. Theory 7 (1961), 51-52.

20. J.-M. Goethals, *On the Golay Perfect Binary Code,* J. Comb. Theory 11 (1971), 178-186.

21. J.-M. Goethals and S. L. Snover, *Nearly Perfect Binary Codes,* Discrete Math. 3 (1972), 65-88.

22. M. J. E. Golay, *Notes on Digital Coding,* Proc. IRE 37 (1949), 657.

23. ———, *Binary Coding,* IEEE Trans. Inform. Theory IT 4 (1954), 23-28.

24. ———, *Notes on the Penny-Weighing Problem, Lossless Symbol Coding with Nonprimes, etc.,* IEEE Trans. Inform. Theory, IT 4 (1958), 103-109.

25. S. W. Golomb and E. C. Posner, *Rook Domains, Latin Squares, Affine Planes, and Error-Correcting Codes,* IEEE Trans. Inform. Theory IT 10 (1964), 196-208.

26. S. W. Golomb and L. R. Welch, *Algebraic Coding and the Lee Metric,* p. 175-194 of H. B. Mann, *Error-Correcting Codes,* John Wiley & Sons, Inc., New York (1968).

27. M. Hall Jr., *Combinatorial Theory,* Blaisdell Publishing Company, Waltham, Mass. (1967).

28. R. W. Hamming, *Error-Detecting and Error-Correcting Codes,* Bell System Tech. J. 29 (1950), 147-160.

29. M. Herzog and J. Schonheim, *Linear and Nonlinear Single-Error-Correcting Perfect Mixed Codes,* Inf. and Control 18 (1971), 364-368.

30. L. O. James, R. G. Stanton and D. D. Cowan, *A Problem in Coding Theory,* Proc. Louisiana Conf. on Combinatorics, Graph Theory and Computing (1970), 167-179 (Louisiana State Univ., Baton Rouge, Lo.).

31. S. M. Johnson, *On Perfect Error-Correcting Codes,* Memorandum RM-3403-PR of the Rand Corporation, Santa Monica, Cal. (1962).

32. ———, *A New Upper bound for Error-Correcting Codes,* IEEE Trans. Inform. Theory, IT 8 (1962), 203-207.

33. M. Karlin, *New Binary Coding Results by Circulants,* IEEE Trans. Inform. Theory IT 15 (1969), 81-92.

34. C. Y. Lee, *Some Properties of Nonbinary Error-Correcting Codes,* IEEE Trans. Inform. Theory IT 4 (1958), 77-82.

35. H. W. Lenstra Jr., *Two theorems on perfect codes,* Discrete Math. 3 (1972), 125-132.

36. V. K. Leont'ev, *On a Problem of Close-Packed Codes* (in Russian), Diskret. Analiz **2** (1964) 56–58.

37. B. Lindström, *On group and nongroup perfect codes in q symbols*, Math. Scand. **25** (1969), 149–158.

38. J. H. van Lint, 1967–1969 Report of the Discrete Mathematics group, Report 69-WSK-04 of the Technological University, Eindhoven, Netherlands (1969).

39. ———, *On the Nonexistence of Perfect* 2- *and* 3-*Hamming-Error-Correcting Codes over* GF(q), Inf. and Control **16** (1970), 396–401.

40. ———, *On the Nonexistence of Perfect* 5-, 6- *and* 7- *Hamming-Error-Correcting Codes over* GF(q), Report 70-WSK-06 of the Technological University, Eindhoven, Netherlands (1970).

41. ———, *Coding Theory*, Springer Verlag, Berlin-Heidelberg, New York (1971).

42. ———, *On the Nonexistence of Certain Perfect Codes*, Computers in Number Theory 277–282, Academic Press, London and New York (1971).

43. ———, *Nonexistence Theorems for Perfect Error-Correcting-Codes*, Computers in Algebra and Number Theory 89–95, SIAM-AMS Proceedings IV (1971).

44. S. P. Lloyd, *Binary Block Coding*, Bell System Tech. J. **36** (1957), 517–535.

45. G. Losey, *Note on a Theorem of Zaremba*, J. Comb. Theory **6** (1969), 208–209.

46. F. J. MacWilliams, Ph. D. Dissertation, Harvard University (1961).

47. ———, *An Historical Survey*, p. 3–13 of H. B. Mann, *Error-Correcting Codes*, John Wiley & Sons, Inc., New York (1968).

48. H. B. Mann, *Error-Correcting Codes*, John Wiley & Sons, Inc., New York (1968).

49. J. G. Mauldon, *Covering Theorems for Groups*, Quart. J. Math. **1** (1950), 284–287.

50. M. H. McAndrew, *An Algorithm for Solving a Polynomic Congruence and its Application to Error-Correcting Codes*, Math. of Comp. **19** (1965), 68–72.

51. A. W. Nordstrom and J. P. Robinson, *An Optimum Nonlinear Code*, Inform. and Control **11** (1967), 613–616.

52. L. J. Paige, *A Note on the Mathieu Groups*, Can. J. Math. **9** (1956), 15–18.

53. W. W. Peterson, *Error-Correcting Codes*, The M. I. T. Press, Cambridge, Mass. (1961).

54. V. Pless, *On the uniqueness of the Golay codes*, J. Comb. Theory **5** (1968), 215–228.

55. F. P. Preparata, *A Class of Optimum Nonlinear Double-Error-Correcting Codes*, Inform. and Control **13** (1968), 378–400.

56. ———, *A new look at the Golay* (23, 12) *code*, IEEE Trans. Inform. Theory IT **16** (1970), 510–511.

57. J. E. Roos, *An Algebraic Study of Group and Nongroup Error-Correcting Codes*, Inform. and Control **8** (1965), 195–214.

58. J. Schönheim, *On linear and nonlinear single-error-correcting q-nary perfect codes*, Inf. and Control **12** (1968), 23–26.

59. ———, *Semilinear Codes and some Combinatorial Applications of Them*, Inf. and Control **15** (1969), 61–66.

60. N. V. Semakov, N. A. Zinovjev and G. V. Zaitzev, *Uniformly Packed Codes* (in Russian), Problemy Peredachi Informatsii **7** (1971), 38–50.

61. H. S. Shapiro and D. S. Slotnick, *On the Mathematical Theory of Error-Correcting Codes*, IBM J. Res. Develop. **3** (1959), 25–34.

62. R. G. Stanton, *Covering theorems in groups* (or: How to win at football pools), Recent Progress in Combinatorics (Proc. Third Waterloo Conf. on Combina-

torics) 37–45, Academic Press, New York (1969).

63. S. K. Stein, *Factoring by Subsets*, Pac. J. Math. **22** (1967), 523–541.

64. G. Szegö, *Orthogonal Polynomials*, Am. Math. Soc. Coll. Publ. 23 (1959).

65. O. Taussky and J. Todd, *Covering Theorems for Groups*, Ann. Soc. Polon. Math. **2** (1948), 303–305.

66. A. Tietäväinen, *On the Nonexistence of Perfect 4-Hamming-Error-Correcting Codes*, Ann. Ac. Sci. Fennicae Ser. A. I (1970), 485.

67. ———, *On the Nonexistence of Perfect Codes over Finite Fields*, SIAM J. Appl. Math. **24** (1973), 88–96.

68. A. Tietäväinen and A. Perko, *There are No Unknown Perfect Binary Codes*, Ann. Univ. Turku, Ser. A. I (1971), 148.

69. Ju. L. Vasil'ev, *On nongroup close-packed codes* (in Russian), Probl. Kibernet **8** (1962), 337–339, translated in Probleme der Kybernetik **8** (1965), 375–378.

70. T. J. Wagner, *A Search Technique for Quasi-Perfect Codes*, Inf. and Control **9** (1966), 94–99.

71. ———, *A Remark Concerning the Existence of Binary Quasi-Perfect Codes*, IEEE Trans. Inform. Theory IT **12** (1966), 401.

72. S. K. Zaremba, *A Covering Theorem for Abelian Groups*, J. London Math. Soc. **26** (1950), 71–72.

73. ———, *Covering problems concerning Abelian Groups*, J. London Math Soc. **27** (1952), 242–246.

74. L. A. Bassalygo, *A Necessary condition for the Existence of Perfect Codes in the Lee Metric* (in Russian), Matematicheski Zametki **15** (1974), 313–320.

75. L. A. Bassalygo, G. V. Zaitzev, N. A. Zinov'ev, *On Uniformly Packed Codes* (in Russian), Problemy Peredachi Informatsii (1974), 9–14.

76. N. L. Biggs, *Perfect Codes in Graphs*, J. Comb. Theory B **15** (1973), 289–296.

77. ———, *Perfect Codes and Distance Transitive Graphs*, in *Combinatorics*, Proc. of the Third British Comb. Conf., Aberystwyth 1973, London Math. Soc. Lecture Notes 13 (F. P. McDonough and V. C. Mavron, eds.).

78. P. Delsarte, *An Algebraic Approach to the Association Schemes of Coding Theory*, Philips Res. Repts. Suppl. **10** (1973).

79. ———, *The Association Schemes of Coding Theory*, p. 139–157 in *Combinatorics* (M. Hall and J. H. van Lint, eds.), Mathematical Centre Tracts 55, Amsterdam, 1974.

80. P. Delsarte and J.-M. Goethals, *Unrestricted Codes with the Golay Parameters are Unique*, Report R 238, M.B.L.E. Research Laboratory, Brussels, 1973.

81. S. W. Golomb and L. R. Welch, *Perfect Codes in the Lee Metric and the Packing of Polyominoes*, SIAM J. Appl. Math. **18** (1970), 302–317.

82. O. Heden, *Perfect Codes in Antipodal Distance-Transitive Graphs*, Math. Institute of the Univ. of Stockholm preprint (1974).

83. M. Herzog and J. Schönheim, *Group Partition, Factorization and the Vector Covering Problem*, Can. Math. Bull. **15** (1972), 207–214.

84. S. M. Johnson, *A New Lower Bound for Coverings by Rook Domains*, Utilitas Math. **1** (1972), 121–140.

85. V. K. Leont'ev, *On the Existence of Densely Packed Codes* (in Russian), Problemy Kibernet. **15** (1965), 253–257.

86. B. Lindström, *Group Partitions and Mixed Perfect Codes*, Can. Math. Bull. (to appear).

87. J. H. van Lint, *Recent Results on Perfect Codes and Related Topics*,

p. 158–178 in *Combinatorics* (M. Hall and J. H. van Lint, eds.) Mathematical Centre Tracts 55, Amsterdam, 1974.

88. D. H. Smith and P. Hammond, *Perfect Codes in the Graphs* 0_k, J. Comb. Theory (to appear).

89. S. L. Snover, *The Uniqueness of the Nordstrom-Robinson and the Golay Binary Codes,* thesis, Michigan State Univ., 1973.

90. S. K. Stein, *A Symmetric Star Body that Tiles but not as a Lattice,* Proc. Am. Math. Soc. **36** (1972), 543–548.

91. ———, *Algebraic Tiling,* Am. Math. Monthly **81** (1974), 445–462.

92. A. Tietäväinen, *A Short Proof for the Nonexistence of Unknown Perfect Codes over GF*(q), $q > 2$, Ann. Acad. Sci. Fennicae A 580 (1974).

93. J. A. Todd, *A Representation of the Mathieu Group* M_{24} *as a Collineation Group,* Ann. di Mat. (IV) **71** (1966), 199–238.

94. T. J. Wagner, *Some Additional Quasi-Perfect Codes,* Inf. and Control **10** (1967), 334.

95. V. A. Zinov'ev and V. K. Leont'ev, *On Perfect Codes* (in Russian), Problemy Peredachi Informatsii **8** (1972), 26–35.

96. ———, *A Theorem on the Nonexistence of Perfect Codes over Finite Fields* (in Russian), Problemy Peredachii Informatsii (to appear).

TECHNICAL UNIVERSITY EINDHOVEN, EINDHOVEN, NETHERLANDS