Nonexistence theorems for perfect error-correcting codes

Nonexistence Theorems for Perfect Error-Correcting Codes

J. H. van Lint

1. **Introduction.** Let p be a prime, $q = p^\alpha$, $F = \mathrm{GF}(q)$ and let V be the vector space F^n. For any $x \in V$ we define the *weight* of x to be the number of nonzero components of x. The (Hamming-) distance $d(x, y)$ of two vectors x, y in V is defined to be the weight of $x-y$. If e is a positive integer we define the *sphere* $B_{x,e}$ by

$$B_{x,e} := \{y \in V \mid d(x, y) \leqq e\}.$$

A subset C of V is called an *e-error-correcting* code if

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

If furthermore $V = \cup_{x \in C} B_{x,e}$ the code is called *perfect*. In coding theory the vectors of C are called codewords; the dimension n of V is called the *block length* of the code.

The following perfect codes are known:

(a) Trivial perfect codes: If $e = n$ and C_1 consists of one word then C_1 is a perfect code. If $q = 2$, $n = 2e+1$ and C_2 consists of the words $(0, 0, \ldots, 0)$ and $(1, 1, \ldots, 1)$ then the code C_2 is perfect (repetition-code).

(b) Hamming codes: Perfect codes with $e = 1$. For a description cf. [4].

(c) Golay codes: There are two codes known as Golay codes, one with $e = 2, q = 3, n = 11$ and one with $e = 3, q = 2, n = 23$ (cf. [4]).

A necessary condition for the existence of a perfect code with parameters e, q, n is easily established. For each $x \in V$ the cardinality of the sphere $B_{x,e}$ is $\Sigma_{i=0}^{e} \binom{n}{i} (q-1)^i$. If a perfect code exists this number must be a divisor of the cardinality of V, which is q^n. Hence for some integer β

$$\sum_{i=0}^{e} \binom{n}{i} (q-1)^i = p^\beta.$$

AMS 1970 *subject classifications.* Primary 10B15, 94A10.

Since $\sum_{i=0}^{n} \binom{n}{i} (q-1)^i = q^n$ we find by subtraction

$$q^n - p^\beta \equiv 0 \pmod{q-1}.$$

This implies that p^β is a power of q. Hence:

(1.1) *If a perfect e-error-correcting code of block length n over* GF(q) *exists then there is an integer k such that* $\sum_{i=0}^{e} \binom{n}{i} (q-1)^i = q^k$.

A more complicated necessary condition for the existence of perfect codes was found by S. P. Lloyd in 1957 for the case $q = 2$ [**10**]. This was generalized by F. J. MacWilliams (1962) and later recast by A. M. Gleason (cf. [**3**]). The condition is:

(1.2) THEOREM (LLOYD, ETC.). *If a perfect e-error-correcting code of block length n over* GF(q) *exists then the polynomial*

$$P_e(x) := \sum_{i=0}^{e} (-1)^i \binom{n-x}{e-i} \binom{x-1}{i} (q-1)^{e-i},$$

where $\binom{a}{i} := a(a-1)\cdots(a-i+1)/i!$, *has e distinct integral zeros among* $1, 2, \ldots, n-1$.

2. **Survey of results on nonexistence of perfect codes.** Several authors have studied perfect codes and proved nonexistence theorems. Nearly all the results are based on (1.1) only. Very often part of the work depended on the use of computers. It has been proved a number of times that $e = 2$, $q = 2$, $n = 90$ satisfy the condition in (1.1) but that there is no perfect code with these parameters (cf. [**6**]). Using known theorems on diophantine equations E. L. Cohen [**5**] showed that for $e = 2$ and $q < 6$ the equation in (1.1) has no other solutions than the known ones. Also using numbertheoretical methods R. Alter ([**1**], [**2**]) treated $e = 2$, $7 \leqq q \leqq 9$ and proved that there are no perfect codes with these parameters except the ones mentioned above. A fairly easy case is: e odd, $q = 2$. For these values the left-hand side of the equation in (1.1) is a polynomial in n which is divisible by $n+1$ and then all solutions are easily found (Shapiro and Slotnick [**12**]). This has been done for $e < 20$ and no new perfect codes were found.

Computer searches were carried out by E. L. Cohen [**5**] for $e = 2$, $3 \leqq q$ (odd) $\leqq 125$, $3 \leqq k \leqq 40000$ (parameters in (1.1)); by M. H. McAndrew [**11**] for $e \leqq 20$, $n \leqq 2^{70}$ and in 1968 by this author for $e \leqq 1000$, $q \leqq 100$, $n \leqq 1000$ (cf. [**7**], [**8**]). In no case was a new perfect code found.

The results mentioned above are complete for binary 2- and 3-error-correcting codes, but not for $e = 4$. The latter were treated by using (1.2) (cf. [**7**]). The method used was one applied by A. Baker and H. Davenport for a completely different problem in the theory of diophantine equations. It involved over 2 hours of computing time. Exactly the same program was used for the coding theory problem!

Since then the author has found the following theorems (cf. [**9**]):

(2.1) THEOREM. *For $q = p^\alpha > 3$ there is no perfect 2-error-correcting code over the alphabet* GF(q) *with block length $n > 2$.*

(2.2) THEOREM. *The only perfect 3-error-correcting codes of block length $n > 3$ over* GF(q) *are the binary repetition code of block length 7 and the* (23, 12)*-Golay code.*

The new approach which led to these theorems was combining conditions (1.1) and (1.2). The proofs do not require computer searches.

In the following section we continue these investigations and prove new nonexistence theorems for perfect codes.

3. **New nonexistence theorems.** Since the question of existence of perfect 2- and 3-error-correcting codes has been settled ((2.1) and (2.2)), we restrict ourselves in this section to $e \geqq 4$. We shall exclude the trivial case $n = e$ from now on. From (1.1) it then follows that $k < n$ and also $k > e$ (since $\binom{n}{i} > \binom{e}{i}$ for $i \neq 0$). Summarizing, from now on:

$$n > k > e \geqq 4. \tag{3.1}$$

Now assume that a perfect code with parameters e, q, n exists. Then (1.1) and (1.2) are satisfied. Let x_i ($1 \leqq i \leqq e$) be the zeros of P_e arranged according to magnitude. By (1.2) we have

$$1 \leqq x_1 < x_2 < \cdots < x_e \leqq n-1.$$

LEMMA 1. *The zeros of P_e satisfy the relations*:

$$x_1 + x_2 + \cdots + x_e = e(n-e)(q-1)/q + e(e+1)/2, \tag{3.2}$$

$$x_1 x_2 \cdots x_e = e!\, q^{k_1}, \qquad \text{with } k_1 := k-e, \tag{3.3}$$

$$x_1 \geqq ((n-e+1)(q-1)+e)/((q-1)+e). \tag{3.4}$$

PROOF. By (1.1) and (1.2) we have

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

The coefficient of x^e in $P_e(x)$ is

$$\sum_{i=0}^{e} (-1)^i \frac{(-1)^{e-i}}{(e-i)!}\frac{1}{i!}(q-1)^{e-i} = \frac{(-1)^e}{e!} \sum_{i=0}^{e} \binom{e}{i} (q-1)^i = \frac{(-1)^e q^e}{e!}.$$

In the same way we find the coefficient of x^{e-1} to be

$$\sum_{i=0}^{e} \frac{(-1)^e (q-1)^{e-i}}{(e-i)!\, i!} \left\{ - \sum_{j=0}^{e-i-1} (n-j) - \sum_{j=1}^{i} j \right\}$$

$$= \frac{(-1)^{e-1}}{e!} q^{e-1} \{ e(n-e)(q-1) + \tfrac{1}{2} e(e+1)q \}.$$

From the coefficients of x^e, x^{e-1} and x^0 in $P_e(x)$ the sum and product of the zeros are found, proving (3.2) and (3.3).

To prove (3.4) we first remark that if a is a positive integer then $\binom{a}{i} = (a(a-1)\cdots(a-i+1))/i! \geqq 0$ because a negative factor in the numerator occurs only if some other factor is 0. Next we remark that if all terms in the sum defining $P_e(x)$ are zero for some value of x then $n = e$ which we have already excluded. Therefore this sum is an alternating sum with nonnegative terms (assuming that x is an integer). These terms decrease in absolute value if $x < ((n-e+1)(q-1)+e)/((q-1)+e)$. This proves (3.4).

From (3.1) we find as a corollary:

$$e(n-e) \equiv 0 \pmod{q}. \tag{3.5}$$

LEMMA 2. *If a nontrivial perfect e-error-correcting code of block length n over* GF(q) *exists, then*

$$q \leqq e(n-e-1)+1. \tag{3.6}$$

PROOF. Since by (1.2) the zeros $x_1, x_2, \ldots, x_e$ are different we have $x_1 \leqq n-e$. If we combine this with (3.4) then (3.6) follows.

REMARK. The argument we used to prove (3.4) can also be employed to give a sharper upper bound on x_e which would then lead to a slightly better inequality than (3.6). Much stronger inequalities can easily be proved!

We are now in a position to prove our first theorem.

THEOREM 1. *If $e \geqq 4$, $q = p^\alpha$ with $p > e$, then there is no nontrivial perfect e-error-correcting code over* GF(q).

PROOF. From (1.1) we find by expanding $(q-1)^i$ in powers of q:

$$\sum_{j=0}^{e} (-1)^j q^j \binom{n}{j}\binom{n-j-1}{e-j} = (-1)^e q^k \tag{3.7}$$

where $k > e$. Since $p > e$ we find from (3.5) that $q \mid (n-e)$. Furthermore, in the binomial coefficients in (3.7) the factor p does not occur in the denominator but for every $j < e$ the factor $(n-e)$ occurs in the numerator of $\binom{n-j-1}{e-j}$. Since $q \mid (n-e)$ and $p > e$ it follows that $p \nmid (n-i)$ for $0 \leqq i < e$. If p^σ is the highest power of p dividing $n-e$ then $p^{\alpha j+\sigma}$ is the highest power of p dividing the jth term on the left-hand side of (3.7) ($j = 0, 1, \ldots, e-1$) whereas $p^{\alpha e}$ is the highest power of p dividing the last term. Since $k > e$ we must have $\sigma = \alpha e$. This implies that the first term on the right-hand side of (3.2) is divisible by q^{e-1} whereas the second term contains a factor p only if $e+1 = p$. It is therefore not possible that all the zeros of P_e are divisible by p^2 and if $p \neq e+1$ then it is even impossible that all the zeros are divisible by p. Hence at least one of the zeros is a divisor of $(e+1)!$ (by (3.3)). It follows that $x_1 \leqq (e+1)!$. Since $q^e \mid (n-e)$ we have $n-e \geqq (e+1)^e$. Substituting these inequalities in (3.4) we find $(e+1)! \geqq 1+\frac{1}{2}(e+1)^e$ which is false for $e \geqq 3$. This completes the proof.

We now consider primes $p \leqq e$. Several cases have to be treated separately.

THEOREM 2. *If $e \geqq 4$, $q = p^\alpha > e$ with $p < e$, $p \nmid e$ then there is no nontrivial perfect e-error-correcting code over* GF(q).

PROOF. Once again (3.5) implies $q \mid (n-e)$. The quotient of two consecutive terms in (3.7) is

$$-q((n-j)(e-j))/(j+1)(n-j-1) \qquad (0 \leqq j \leqq e-1).$$

Now, since $p \nmid e$ and $p \mid (n-e)$, i.e. $p \nmid n$, at most one of the terms in the denominator of this quotient is divisible by p and since $q = p^\alpha > e$ and $q \mid (n-e)$ we see that the highest power of p dividing the denominator is less than q if $j \neq e-1$. Again let $p^\sigma \| (n-e)$. Then, since $q \mid (n-e)$ and $q > e$ in

$$(n-1)(n-2)\cdots(n-e+1)/(e-1)(e-2)\cdots 1$$

numerator and denominator are divisible by the same power of p. Therefore $p^\sigma \| \binom{n-1}{e}$. In the same way we see that the last term of the sum in (3.7) is exactly divisible by $p^{\alpha e}$. All the terms of this sum except the last are divisible by a higher power of p than the first term as was shown above. Since the right-hand side of (3.7) is divisible by q^{e+1} we must have $\sigma = \alpha e$. Just as in Theorem 1 we see that if all the zeros of P_e are divisible by a power of p then this power of p is a divisor of $(e+1)$. In the same way as in Theorem 1 this leads to a contradiction, completing the proof of Theorem 2.

In the following case the counting of the number of factors p in numerator and denominator of the binomial coefficients of (3.7) is more difficult. The result is now somewhat weaker.

THEOREM 3. *Let $p \mid e$, $q = p^\alpha$ and let $q > e$ if $p > 2$, $q > 2e$ if $p = 2$. Define*

$$M_p(e) := 2e! + e - 1 \qquad \text{if } p > 2,$$
$$:= ((e-1)!)_1 e + e - 1 \qquad \text{if } p = 2 \quad (a_1 \text{ denotes the odd part of } a).$$

If a nontrivial perfect e-error-correcting code of block length n over GF(q) *exists then $n < M_p(e)$.*

PROOF. Suppose all the zeros of P_e are divisible by a higher power of p than is contained in $\frac{1}{2}e(e+1)$. Then in (3.2) the two terms on the right-hand side are divisible by the same power of p and therefore $p^\alpha \| 2(n-e)$. Assume $p > 2$. Then, just as in the proof of Theorem 2, we see that numerator and denominator of

$$(n-1)(n-2)\cdots(n-e+1)/(e-1)(e-2)\cdots 1$$

are divisible by the same power of p and hence $q \nmid \binom{n-1}{e}$ contradicting (3.7). If $p = 2$ the same reasoning applies because in that case $p^{\alpha-1} \| (n-e)$ and $p^{\alpha-1} = \frac{1}{2}q > e$.

Since we found a contradiction, the original assumption was false, i.e. there is a zero of P_e which is not divisible by a higher power of p than $\frac{1}{2}e(e+1)$. If

$p > 2$ this means that $x_1 \leqq e!$ and if $p = 2$ this means that $x_1 \leqq ((e-1)!)_1(\frac{1}{2}e)$. The theorem now follows from (3.4).

REMARK. In the case considered in Theorem 3 the bound on n together with (3.6) gives a bound on q.

The three theorems treated in this section do not cover all possibilities. By treating an example we shall show in the following section that the methods used in the proofs of our theorems are also applicable in the remaining cases. The possibilities left open are covered by the computer search mentioned in §2. Summarizing, the result of our investigation is:

THEOREM 4. *For any e, the values of n and q for which* (1.1) *and* (1.2) *are satisfied can be found by a computer search.*

At the moment we cannot do without the computer search but the investigation is being continued in the hope of ultimately proving that there are no more perfect codes at all besides the known ones.

4. **Nonexistence of perfect 4-error-correcting codes.** As an application of the theorems and methods of §3 we shall now prove:

THEOREM 5. *There is no nontrivial perfect 4-error-correcting code over the alphabet* GF(q).

PROOF. By Theorem 1 it is sufficient to consider $q = p^\alpha$ where $p = 2$ or 3.

If $p = 3$ then by Theorem 2 we need only consider $q = p = 3$. We now proceed by the same method as used in the proofs of the preceding section. By (3.5) we have $n \equiv 1 \pmod 3$. For $j \geqq 2$ the terms in the sum in (3.7) are clearly divisible by 81 and so is the right-hand side. Therefore the sum of the first two terms on the left-hand side of (3.7) must be divisible by 81 which implies $n \equiv 4 \pmod 9$. But then by (3.2) the sum $x_1 + x_2 + x_3 + x_4$ is not divisible by 3 and therefore (3.3) implies that $x_1 \leqq 8$. Then from (3.4) it follows that $n \leqq 25$. In [8] it was shown that for $e = 4$, $q = 3$, $5 \leqq n \leqq 25$ no perfect codes exist.

It remains to consider $p = 2$. The cases $q = 2, 4, 8$ have to be treated separately. If $q = 2^\alpha > 8$ then by Theorem 3 we have $n < 15$ and by (3.6) we find $q \leqq 37$, i.e. $q = 16$ or 32. All these cases were also excluded in [8].

If $q = 8$ then by (3.5) n is even. Therefore all terms in (3.7) with $j > 0$ are divisible by 64 which implies that the term with $j = 0$ must also be divisible by 64. This means that $n \equiv 2$ or $4 \pmod{2^8}$. From (3.2) we see that there must be a zero of P_4 which is not divisible by 4 and from (3.3) we then see that $x_1 \leqq 6$ which together with (3.4) implies $n \leqq 11$, and hence $n = 4$ (trivial code).

If $q = 4$ the reasoning is analogous. From (3.7) we find that $n \equiv 1, 2, 3$ or $4 \pmod{16}$. From (3.2) it then follows that the sum of the zeros of P_4 is $\equiv 1, 4, 7$ or $10 \pmod{16}$. Then by (3.3) we see that $x_1 \leqq 12$ and from (3.4) we find $n \leqq 29$. The cases $e = q = 4$, $5 \leqq n \leqq 29$ were excluded in [8].

We could leave out $q = 2$ since it was treated separately in [8] but we shall show that the reasoning used above is applicable in this case. The first two

terms of (3.7) sum to $\frac{1}{24}(n-2)(n-3)(n-4)(7n+1)$ and this number must be divisible by 4. It follows that $n \equiv 2, 3, 4$ or 9 (mod 16). By (3.2) at least one zero is not divisible by 16 and hence by (3.3) $x_1 \leqq 24$. Then (3.4) yields $n \leqq 119$ and once again we can refer to [**8**].

This completes the proof of Theorem 5.

We have given all the details of the proof of Theorem 5 in order to justify the claim of Theorem 4. We remark that nonexistence of perfect 5- and 6-error-correcting codes can be proved in the same way with no essentially new difficulties. Since the details reveal nothing new and are quite tedious we shall omit them here and publish these separately as a report of the Technological University Eindhoven. (All the T.H.E.-Reports are available on request.)

REFERENCES

1. R. Alter, *On the nonexistence of close-packed double Hamming-error-correcting codes on $q = 7$ symbols*, J. Comput. System. Sci. **2** (1968), 169–176. MR **39** # 1227.

2. ———, *On the nonexistence of perfect double Hamming-error-correcting codes on $q = 8$ and $q = 9$ symbols*, Information and Control **13** (1968), 619–627. MR **39** # 1226.

3. E. F. Assmus, H. F. Mattson and R. Turyn, *Cyclic codes*, Report AFCRL-66-348 of the Applied Research Laboratory of Sylvania Electronic Systems, 40 Sylvan Road, Walthan, Mass. 02154.

4. E. R. Berlekamp, *Algebraic coding theory*, McGraw-Hill, New York, 1968. MR **38** # 6873.

5. E. L. Cohen, *A note on perfect double error-correcting codes on q symbols*, Information and Control **7**(1964), 381–384. MR **29** #5656.

6. M. J. E. Golay, *Notes on digital coding*, Proc. IRE **37** (1949), 657.

7. J. H. van Lint, *On the nonexistence of certain perfect codes*, Proc. Sympos. on Computers in Number Theory, Oxford, 1969.

8. ———, 1967–1969 *report of the discrete mathematics group*, Report 69-WSK-04, Technological University, Eindhoven.

9. ———, *On the nonexistence of perfect 2- and 3-Hamming-error-correcting codes over* GF(q), Information and Control **16** (1970), 396–401.

10. S. P. Lloyd, *Binary block coding*, Bell System Tech. J. **36** (1957), 517–535. MR **19**, 465.

11. M. H. McAndrew, *An algorithm for solving a polynomic congruence and its application to error-correcting codes*, Math. Comp. **19** (1965), 68–72. MR **30** # 4612.

12. H. S. Shapiro and D. L. Slotnick, *On the mathematical theory of error-correcting codes*, IBM J. Res. Develop. **3** (1959), 25–34. MR **20** #5092.

TECHNISCHE HOGESCHOOL, EINDHOVEN, THE NETHERLANDS