ANNALES ACADEMIAE SCIENTIARUM FENNICAE

Series A

I. MATHEMATICA

485

ON THE NONEXISTENCE OF PERFECT 4-HAMMING-ERROR-CORRECTING CODES

BY

AIMO TIETÄVÄINEN

HELSINKI 1970
SUOMALAINEN TIEDEAKATEMIA

doi:10.5186/aasfm.1971.485

Communicated 13 November 1970 by K. Inkeri

KESKUSKIRJAPAINO
HELSINKI 1970

On the nonexistence of perfect 4-Hamming-error-correcting codes

1. Introduction. Let $K = GF(q)$ be the finite field of $q = p^r$ elements where p is a prime. Let V be the vector space K^n. For $\mathbf{a} \in V$, let $\|\mathbf{a}\|$ be the number of nonzero components of $\mathbf{a}$. The sphere of centre $\mathbf{a}$ and radius e is defined as the set

$$B(\mathbf{a}, e) = \{ \mathbf{x} \in V \mid \|\mathbf{x} - \mathbf{a}\| \leqq e \} .$$

A subset C of V is called a perfect (or close-packed) e-(Hamming-)error-correcting code if

(i) $\bigcup_{\mathbf{a} \in C} B(\mathbf{a}, e) = V$

and

(ii) $\mathbf{a} \in C$, $\mathbf{b} \in C$, $\mathbf{a} \neq \mathbf{b}$ implies $B(\mathbf{a}, e) \cap B(\mathbf{b}, e) = \emptyset$.

The dimension n of V is called the block length of C.

A perfect e-error-correcting code of block length n is called trivial if $e = n$ (one-word code) or if $q = 2$ and $n = 2e + 1$ (repetition code of two words). For every q, there is an infinity of nontrivial perfect 1-error-correcting codes. Nontrivial perfect e-error-correcting codes with $e > 1$ are known only for $e = 2$, $q = 3$, $n = 11$, and $e = 3$, $q = 2$, $n = 23$. Both of them are called Golay codes (see [3], pp. 302—309). It was proved in 1968 or earlier (see [4], [1], [2] and references in [1]) that there are no unknown perfect 2-error-correcting codes for $q \leqq 9$. In his paper [5] van Lint proved the nonexistence of unknown perfect e-error-correcting codes in cases $e = 2$ and $e = 3$ for all q. The purpose of this note is to extend that result to the case that $e = 4$. We shall hence prove the following

Theorem. *There are no nontrivial perfect 4-error-correcting codes over finite fields.*

2. Lemma. In the proof of this theorem we shall use the following

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

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

where

$$\binom{x}{i} = x(x-1) \ldots (x-i+1)/i\,! ,$$

has e *distinct integral zeros among* $1, 2, \ldots, n-1$.

This lemma, which is due to Lloyd [6] in case $q = 2$, is here in the form in which van Lint gave it in [5].

3. Proof of Theorem. Assume the contrary: there exists a nontrivial perfect 4-error-correcting code with block length n over $GF(q)$. Because the case $q = 2$ has been considered by van Lint (see [5], p. 399) and because the trivial perfect codes are excluded, we may suppose that $q \geqq 3$ and $n \geqq 5$.

By the equation (1)

$$24q^{-4}P_4(x) = x^4 - A_1x^3 + A_2x^2 - A_3x + A_4$$

where

(2) $$A_1 = 4n - 6 - (4n - 16)q^{-1}$$

and

(3) $$A_4 = 24q^{-4} \sum_{i=0}^{4} \binom{n}{4-i} (q-1)^{4-i} .$$

On the other hand, van Lint ([5], the eq. (2.2)) has shown that there exists a positive integer k such that

(4) $$\sum_{i=0}^{4} \binom{n}{4-i} (q-1)^{4-i} = q^k .$$

Furthermore, we know that

(5) $$x_1 + x_2 + x_3 + x_4 = A_1$$

and

(6) $$x_1x_2x_3x_4 = A_4$$

where x_1 , x_2 , x_3 and x_4 $(x_1 < x_2 < x_3 < x_4)$ are the zeros of $P_4(x)$. A combination of the equations (6), (3), (4) and $q = p^r$ gives the result

(7) $$x_1x_2x_3x_4 = 24p^{(k-4)r} .$$

In the rest of this paper we shall show, by means of some easy but rather lengthy calculations, that the number $X = (x_1 + x_2 + x_3 + x_4)/x_4$ is, by (7), considerably smaller than 4 and, moreover, that this result with the inequality $x_4 \leqq n - 1$ and with the equations (5) and (2) leads to a contradiction.

If $p = 2$, one of the numbers x_i, say x_j, is of the form $3 \cdot 2^\alpha$, the others are powers of 2. If $j = 1$, $X \leqq 31/16$; if $j = 2$, $X \leqq 17/8$; if $j = 3$, $X \leqq 5/2$; if $j = 4$, $X \leqq 13/6$. Consequently $X \leqq 5/2$ for $p = 2$. Hence

$$A_1 \leqq 5(n - 1)/2 . \tag{8}$$

On the other hand, it follows from the equation (2) and from the inequality $q \geqq 4$ that

$$A_1 \geqq 4n - 6 - (4n - 16)/4 = 3n - 2 . \tag{9}$$

The inequalities (8) and (9) imply $n \leqq -1$ which is impossible.

If $p = 3$, $x_1 x_2 x_3 x_4$ is of the form $8 \cdot 3^\alpha$. If one of the factors x_i is divisible by 8 then $X \leqq 7/3$. If one factor is divisible by 4 and another by 2 then $X \leqq 5/2$. In the case that only one of the x_i's is not divisible by 2 we find the result $X < 2$. Using the inequalities $X \leqq 5/2$, $x_4 \leqq n - 1$ and

$$x_1 + x_2 + x_3 + x_4 \geqq 4n - 6 - (4n - 16)/3$$

we get the impossibility

$$5(n - 1)/2 \geqq (8n - 2)/3 .$$

If $p = 5$, $x_1 x_2 x_3 x_4$ is of the form $2^3 \cdot 3 \cdot 5^\alpha$ and therefore one of the factors is of the form $2^\beta \cdot 3 \cdot 5^\gamma$ and the others are of the form $2^\delta \cdot 5^\varepsilon$. Using this result it is possible to see that $X \leqq 79/25$. Hence we get the impossibility

$$79(n - 1)/25 \geqq (16n - 14)/5 .$$

If $p \geqq 7$, we may see that $X \leqq 25/8$. This implies the inequality

$$25(n - 1)/8 \geqq (24n - 26)/7$$

which is impossible since $n > 4$.

Note added December 7, 1970. Prof. J. H. van Lint announced to me to-day that he has recently extended his result to the case that $e = 4$ (Nonexistence theorems for perfect error-correcting codes, to appear in the proceedings of the A.M.S. Symposium in Algebra and Number Theory 1970) and even to cases $e = 5$, $e = 6$ and $e = 7$ (On the nonexistence of perfect 5-, 6- and 7-Hamming-error-correcting codes over $GF(q)$. — Report 70-WSK-06, Technological University Eindhoven). His method differs considerably from that of this paper.

References

[1] ALTER, R.: On the nonexistence of close-packed double Hamming-error-correcting codes on $q = 7$ symbols.— J. Comput. System Sci. 2 (1968), 169—176.

[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.

[3] BERLEKAMP, E. R.: Algebraic coding theory. McGraw-Hill (1968).

[4] COHEN, E. L.: A note on perfect double error-correcting codes on q symbols. — Information and Control 7 (1964), 381—384.

[5] VAN LINT, J. H.: On the nonexistence of perfect 2- and 3-Hamming-error-correcting codes over $GF(q)$. — Information and Control 16 (1970), 396—401.

[6] LLOYD, S. P.: Binary block coding. — Bell System Tech. J. 36 (1957), 517—535.

Printed December 1970