

## TWO THEOREMS ON PERFECT CODES

H.W. LENSTRA, Jr.

*Mathematical Institute, University of Amsterdam,  
Amsterdam, The Netherlands*

Received 17 March 1972

**Abstract.** Two theorems are proved on perfect codes. The first one states that Lloyd's theorem is true without the assumption that the number of symbols in the alphabet is a prime power. The second theorem asserts the impossibility of perfect group codes over non-prime-power-alphabets.

### §0. Introduction

Let  $V$  be a finite set,  $|V| = q \geq 2$ , and let  $1 \leq e \leq n$  be rational integers. We put  $N = \{1, 2, \dots, n\}$ . For  $v = (v_i)_{i=1}^n \in V^n$ ,  $v' = (v'_i)_{i=1}^n \in V^n$  we define  $d(v, v') = |\{i \in N \mid v_i \neq v'_i\}|$ . A *perfect  $e$ -error-correcting code of block length  $n$  over  $V$*  is a subset  $C \subset V^n$  such that for every  $v \in V^n$  there exists exactly one  $c \in C$  satisfying  $d(v, c) \leq e$ .

If  $q$  is a prime power, a necessary condition for the existence of such a code is given by Lloyd's theorem [6]. This theorem has recently been used to determine all  $n, e$  for which a perfect code over an alphabet  $V$  of  $q$  symbols,  $q$  a prime power, exists [5; 6].

In §1 I show that Lloyd's theorem holds for all  $q$ . The proof, which is modelled after [6, 5.4], makes use of some elementary notions from commutative algebra. A different proof has been obtained by P. Del-sarte [2]. It seems hard to use Lloyd's theorem to prove non-existence theorems for perfect codes over non-prime-power-alphabets.

In §2 I prove the following theorem: if  $G_i$  ( $1 \leq i \leq n$ ) is a group with underlying set  $V$ , and  $C \subset \prod_{i=1}^n G_i$  is a subgroup which as a subset of  $V^n$  is a perfect  $e$ -error-correcting code,  $e < n$ , then  $q$  is a prime power and each  $G_i$  is abelian of type  $(p, p, \dots, p)$ . A special case of this theorem was proved in [4].

### § 1. Lloyd's theorem

**Theorem 1.** *If a perfect  $e$ -error-correcting code of block length  $n$  over  $V$  exists then the polynomial*

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

where

$$\binom{a}{i} = \prod_{j=1}^i \frac{a-j+1}{j},$$

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

**Proof.** Let  $K$  be a field of characteristic zero, and let  $M$  be a  $K$ -vector space of dimension  $q^n$  with the elements of  $V^n$  as basis vectors:

$$M = \{ \sum_{v \in V^n} k_v \cdot v \mid k_v \in K \text{ for } v \in V^n \}.$$

If  $D \subset V^n$  is a subset, we denote  $\sum_{v \in D} v \in M$  by  $\Sigma D$ . Define the  $K$ -endomorphisms  $\phi_i$  ( $1 \leq i \leq n$ ) of  $M$  by

$$\phi_i(v) = \Sigma \{ v' = (v'_j)_{j=1}^n \in V^n \mid v'_j = v_j \text{ for all } j \neq i \},$$

$v = (v_j)_{j=1}^n \in V^n$ . One easily checks:

$$(1) \quad \phi_i \phi_j = \phi_j \phi_i \quad (1 \leq i \leq j \leq n),$$

$$(2) \quad \phi_i^2 = q \cdot \phi_i \quad (1 \leq i \leq n).$$

Let  $K[X_1, \dots, X_n]$  be the commutative polynomial ring in  $n$  symbols over  $K$ . The ideal generated by  $\{X_i^2 - qX_i \mid 1 \leq i \leq n\}$  is denoted by  $B$ , and  $R$  is the factor ring  $K[X_1, \dots, X_n]/B$ . By (1) there exists a  $K$ -linear ring homomorphism  $K[X_1, \dots, X_n] \rightarrow \text{End}_K(M)$  (the ring of  $K$ -endomorphisms of  $M$ ) mapping 1 to the identity and  $X_i$  to  $\phi_i$  ( $1 \leq i \leq n$ ). The kernel of this ring homomorphism contains  $B$ , by (2), so we obtain a ring homomorphism  $f: R \rightarrow \text{End}_K(M)$ , mapping  $x_i = (X_i \text{ mod } B) \in R$

to  $\phi_i$ . Therefore we can make  $M$  into an  $R$ -module by defining  $r \cdot m = f(r)(m)$  ( $r \in R, m \in M$ ) [I, II 1 1, 3, III 1]

Put  $y_I = \prod_{i \in I} (x_i - 1) \in R$  for  $I \subset N$ . Then

$$y_I \cdot v = \sum \{v' \in V^n \mid \text{if } j \in N, \text{ then } v_j = v'_j \iff j \notin I\},$$

$I \subset N, v \in V^n$ . Therefore,  $\{y_I \cdot v \mid I \subset N\} \subset M$  is linearly independent over  $K$ , for  $v \in V^n$ . Then certainly  $\{y_I \mid I \subset N\} \subset R$  is linearly independent over  $K$ . Moreover, it is easily shown that  $\{y_I \mid I \subset N\}$  generates  $R$  as a  $K$ -vector space. This proves  $\{y_I \mid I \subset N\}$  is a  $K$ -basis for  $R$ , and  $\dim_K(R) = 2^n$  (by  $\dim_K$  we mean dimension over  $K$ ).

The permutation group  $S_n$  on  $n$  symbols acts as a group of  $K$ -linear ring automorphisms on  $R$  by permuting  $\{x_i \mid i \in N\}$ . The set of invariants

$$A = \{r \in R \mid \sigma(r) = r \text{ for all } \sigma \in S_n\}$$

is a subring of  $R$ . Put

$$z_j = \sum_{I \subset N, |I|=j} y_I \text{ for } 0 \leq j \leq n$$

Then it is easy to see that  $\{z_j \mid 0 \leq j \leq n\}$  is a  $K$ -basis for  $A$ , and

$$(3) \quad z_j \cdot v = \sum \{v' \in V^n \mid d(v, v') = j\}, \quad 0 \leq j \leq n, v \in V^n$$

Since  $A$  is a subring of  $R$ ,  $M$  is also an  $A$ -module.

Choose  $u \in V^n$  arbitrary but fixed, and define  $w(v) = d(v, u)$  for  $v \in V^n$ . Let  $S_{V^n}$  be the full permutation group of  $V^n$ , and let  $G$  be the subgroup  $G = \{\sigma \in S_{V^n} \mid \sigma(u) = u, \text{ and } d(v, v') = d(\sigma(v), \sigma(v')) \text{ for all } v, v' \in V^n\}$ . By permuting the basis vectors,  $G$  acts  $K$ -linearly on  $M$ . This action is even  $A$ -linear, since for  $\sigma \in G, 0 \leq j \leq n, v \in V^n$  we have

$$\begin{aligned} \sigma(z_j \cdot v) &= \sigma(\sum \{v' \mid d(v, v') = j\}) = \sum \{\sigma(v') \mid d(v, v') = j\} \\ &= \sum \{v' \mid d(v, \sigma^{-1}(v')) = j\} = \sum \{v' \mid d(\sigma(v), v') = j\} \\ &= z_j \cdot \sigma(v) \end{aligned}$$

Therefore,  $M^G = \{m \in M \mid \sigma(m) = m \text{ for all } \sigma \in G\}$  is an  $A$ -submodule of  $M$ , and the map  $T: M \rightarrow M^G$ , defined by

$$T(m) = \sum_{\sigma \in G} \sigma(m),$$

is an  $A$ -homomorphism. We wish to determine the structure of  $M^G$  as an  $A$ -module.

It is not hard to see that the orbits of the  $G$ -action on  $V^n$  are  $\{\{v \in V^n \mid w(v) = j\} \mid 0 \leq j \leq n\}$ . Put

$$m_j = \sum \{v \in V^n \mid w(v) = j\} \in M, \quad 0 \leq j \leq n,$$

then it follows that  $\{m_j \mid 0 \leq j \leq n\}$  is a  $K$ -basis for  $M^G$ . Define the  $A$ -homomorphism

$$A \xrightarrow{\psi} M^G \quad \text{by} \quad \psi(a) = a \cdot u$$

(we consider  $A$  as an  $A$ -module by left multiplication, [1; 3]). Then

$$\psi(z_j) = z_j \cdot u = \sum \{v \in V^n \mid d(v, u) = j\} = m_j.$$

So  $\psi$  maps a  $K$ -basis for  $A$  one to one onto a  $K$ -basis for  $M^G$ . This implies that  $\psi$  is bijective. We have shown:

$$(4) \quad A \cong M^G \quad \text{as } A\text{-modules.}$$

Now suppose that a perfect  $e$ -error-correcting code  $C \subset V^n$  exists. Then one easily constructs  $e + 1$  perfect  $e$ -error-correcting codes  $C_0, \dots, C_e \subset V^n$  such that  $i \in w[C_i]$  ( $0 \leq i \leq e$ ). We first prove:

$$(5) \quad \{T(\sum C_i) \mid 0 \leq i \leq e\} \subset M^G \quad \text{is linearly independent over } K.$$

**Proof of (5).** Let  $T(\sum C_i) = \sum_{j=0}^n k_{ij} m_j$  ( $k_{ij} \in K$ ); since  $C_i$  is  $e$ -error-correcting, we have  $w[C_i] \cap \{0, 1, \dots, e\} = \{i\}$ ; therefore, if  $0 \leq i \leq e$ ,  $0 \leq j < e$ , the coefficient  $k_{ij}$  is nonzero if and only if  $i = j$ , and (5) follows.

Put

$$s = \sum_{j=0}^e z_j \in A .$$

By (3), the perfectness of  $C_i$  implies

$$s \cdot \Sigma C_i = \Sigma V^n, \quad 0 \leq i \leq e .$$

Applying the  $A$ -linear map  $T$  we find

$$s \cdot T(\Sigma C_i) = T(\Sigma V^n), \quad 0 \leq i \leq e .$$

Using (5) we conclude  $\dim_K \{m \in M^G \mid s \cdot m = 0\} \geq e$ , and by (4) this is the same as

$$(6) \quad \dim_K \{a \in A \mid s \cdot a = 0\} \geq e .$$

Therefore it seems useful to study the structure of  $A$ .

For  $I \subset N$  we define the ring homomorphism  $\chi_I: R \rightarrow K$  by

$$\chi_I(k) = k, \quad k \in K ,$$

$$\chi_I(x_i) = 0 \quad \text{if } i \in I ,$$

$$\chi_I(x_i) = q \quad \text{if } i \notin I .$$

The maximal ideals  $\ker(\chi_I)$  of  $R$  are mutually different, so  $\ker(\chi_I) + \ker(\chi_J) = R$  for  $I \neq J$ . By the Chinese remainder theorem [3, II.2; 1, I.8.11] it follows that the  $K$ -linear ring homomorphism

$$\chi = \prod_{I \subset N} \chi_I : R \rightarrow \prod_{I \subset N} K$$

is surjective (in  $\prod_{I \subset N} K$  addition and multiplication are defined componentwise); comparison of  $K$ -dimension shows that  $\chi$  is injective, so  $\chi$  is a ring isomorphism. For  $\sigma \in S_n$ ,  $I \subset N$ ,  $r \in R$  we have  $\chi_{\sigma[I]}(\sigma(r)) = \chi_I(r)$ . This implies: if  $I, J \subset N$  satisfy  $|I| = |J|$  then  $\chi_I$  and  $\chi_J$  have the same restriction to  $A$ . Therefore

$$\chi[A] \subset \{(k_J)_{J \subset N} \in \prod_{J \subset N} K \mid k_J = k_{J'} \text{ if } |J| = |J'|\},$$

and counting dimension over  $K$  shows that this inclusion is in fact an equality. Putting

$$I_x = \{1, 2, \dots, x\}, \quad \chi_x = \chi_{I_x} \upharpoonright A \quad (0 \leq x \leq n),$$

we conclude that

$$\chi' = \prod_{x=0}^n \chi_x : A \rightarrow \prod_{x=0}^n K$$

is a  $K$ -linear ring isomorphism.

For  $k = (k_x)_{x=0}^n \in \prod_{x=0}^n K$  we have obviously

$$\dim_K \{k' \in \prod_{x=0}^n K \mid k \cdot k' = 0\} = |\{x \mid 0 \leq x \leq n, k_x = 0\}|.$$

Putting  $k = \chi'(s)$  and using (6) we find:

$$(7) \quad |\{x \mid 0 \leq x \leq n, \chi_x(s) = 0\}| \geq e.$$

From the definitions we compute

$$\begin{aligned} \chi_x(z_j) &= \sum_{I \subset N, |I|=j} \chi_{I_x}(y_I) \\ &= \sum_{I \subset N, |I|=j} (-1)^{|I \cap I_x^c|} \cdot (q-1)^{|I - I_x|} \\ &= \sum_{i=0}^j \binom{x}{i} \binom{n-x}{j-i} (-1)^i (q-1)^{j-i}, \\ (8) \quad \chi_x(s) &= \sum_{j=0}^e \chi_x(z_j) \\ &= \sum_{i=0}^e (-1)^i \binom{n-x}{e-i} \binom{x-1}{i} (q-1)^{e-i} \\ &= P(x). \end{aligned}$$

Since  $P(0) = \sum_{i=0}^e \binom{n}{e-i} (q-1)^{e-i} \neq 0$ , Lloyd's theorem now follows from (7) and (8).

§2. Perfect group codes

**Theorem 2** Let  $G_i, 1 \leq i \leq n$ , be a group with underlying set  $V$ . Suppose there exists a subgroup  $C \subset \prod_{i=1}^n G_i$  such that the underlying set of  $C$  is a perfect  $e$ -error-correcting code of block length  $n$  over  $V$ , with  $e < n$ . Then  $q$  is a power of a prime  $p$  and each  $G_i$  is abelian of type  $(p, p, \dots, p)$ .

**Proof** Without loss of generality we may assume that the groups  $G_i$  have the same unit element  $1 \in V (1 < i \leq n)$ . Put  $u = (1)_{i=1}^n$ , and let  $w(g) = d(g, u)$  for  $g \in \prod_{i=1}^n G_i$ , as in §1.

Let  $C \subset \prod_{i=1}^n G_i$  be as in the statement of Theorem 2. Then  $u \in C$  since  $u$  is the unit element of  $\prod_{i=1}^n G_i$ . If

$$g = (g_i)_{i=1}^n \in \prod_{i=1}^n G_i$$

satisfies  $w(g) = e + 1$ , then the unique element  $c = (c_i)_{i=1}^n \in C$  for which  $d(g, c) \leq e$  cannot equal  $u$ , and therefore  $w(c) \geq 2e + 1$ . This is only compatible with  $w(g) = e + 1$  and  $d(g, c) \leq e$  if  $w(c) = 2e + 1$  and  $c_i = g_i$  for all  $i$  such that  $g_i \neq 1$ . We shall use this remark two times below.

Choose  $\alpha_2 \in G_2$  such that the order of  $\alpha_2$  in  $G_2$  is a prime number  $p$ , and choose  $\alpha_i \in G_i, \alpha_i \neq 1$ , for  $3 \leq i \leq e + 1$ . It is sufficient to prove

- (i) every  $\alpha \in G_1, \alpha \neq 1$ , has order  $p$  in  $G_1$ ,
- (ii)  $\alpha\beta = \beta\alpha$  for all  $\alpha, \beta \in G_1$ .

(i) Let  $\alpha \in G_1, \alpha \neq 1$ . Put

$$g = (\alpha, \alpha_2, \dots, \alpha_{e+1}, 1, \dots, 1) \in \prod_{i=1}^n G_i$$

Then  $w(g) = e + 1$ . By the above remark, some  $c \in C$  has the following shape

$$c = (\alpha, \alpha_2, \dots, \alpha_{e+1}, (\text{exactly } e \text{ of the remaining components } \neq 1))$$

Since  $C$  is a subgroup,  $c^p \in C$ , and

$$c^p = (\alpha^p, 1, (\text{at most } 2e - 1 \text{ of the remaining components } \neq 1))$$

Therefore  $w(c^p) \leq 2e$  which implies  $c^p = u$  and  $\alpha^p = 1$ .

(ii) Let  $\alpha, \beta \in G_1, \alpha \neq 1 \neq \beta$ . Put

$$g = (\alpha, \alpha_2, \dots, \alpha_{e+1}, 1, \dots, 1),$$

$$g' = (\beta, \alpha_2, \dots, \alpha_{e+1}, 1, \dots, 1).$$

The above remark yields  $c, c' \in C$  which look like

$$c = (\alpha, \alpha_2, \dots, \alpha_{e+1}, (\text{exactly } e \text{ of the remaining components } \neq 1))$$

$$c' = (\beta, \alpha_2, \dots, \alpha_{e+1}, (\text{exactly } e \text{ of the remaining components } \neq 1)).$$

Then  $d(cc', c'c) \leq e + 1$ , and since  $cc', c'c \in C$  it follows that  $cc' = c'c$  and  $\alpha\beta = \beta\alpha$ . This completes the proof of Theorem 2.

### References

- [1] N. Bourbaki, *Algebre I* (Hermann, Paris, 1970)
- [2] P. Delsarte, *Linear programming associated with coding theory*, MBL Res. Lab. Rept. R 182 (Brussels, 1971).
- [3] S. Lang, *Algebra* (Addison-Wesley, Reading, Mass, 1965)
- [4] B. Lindstrom, *On group and nongroup perfect codes in  $q$  symbols*, *Math. Scand* 25 (1969) 149–158.
- [5] A. Tietavainen, *On the non-existence of perfect codes over finite fields*, *SIAM J Appl Math.*, to appear.
- [6] J.H. van Lint, *Coding theory*, *Lectures Notes in Math* 201 (Springer, Berlin, 1971)