MATH. SCAND. 37 (1975), 13–26

A GENERALISED LLOYD THEOREM AND MIXED PERFECT CODES

OLOF HEDEN

0. Introduction.

Denote by S the set $S_1 \times S_2 \times \ldots \times S_n$, where $S_i = \mathbf{Z}/p_i\mathbf{Z}$ for $i = 1, 2, \ldots, n$ and $\mathbf{Z}$ is the ring of integers. The numbers $p_1, p_2, \ldots, p_n$ are not necessarily prime numbers.

If T is a finite set, then $|T|$ is the cardinality of T. Let $s = (s_1, \ldots, s_n)$ and $t = (t_1, \ldots, t_n)$ be any two elements of S. The integer

$$d(s,t) = |\{i \mid s_i \neq t_i,\ i = 1, 2, \ldots, n\}|$$

is called the distance between s and t. Let $S_e(s)$ denote a sphere with center at s and radius e, that is

$$S_e(s) = \{t \in S \mid d(t,s) \leqq e\} .$$

A subset C of S is a perfect e-code if for any $t \in S$

$$|C \cap S_e(t)| = 1 .$$

If the numbers $p_1, p_2, \ldots, p_n$ are not equal, then a perfect e-code may be called a mixed perfect e-code.

In this paper we shall prove a theorem for mixed perfect e-codes that generalises a theorem of Lloyd, cf. [5], [6], [7] or [8]. We shall also prove that the following two conditions are necessary for the existence of a perfect e-code in S.

(i) If the prime p divides at least one of the numbers $p_1, \ldots, p_n$, then p divides $|S_e(0)|$.

(ii) Let p be a prime and $I_p = \{i \mid p \text{ divides } p_i\} \subseteq \{1, 2, \ldots, n\}$. If $I_p \neq \emptyset$ then $e > n - |I_p|$.

Suppose that $p_1 = p_2 = \ldots = p_n = q$ and that q is a prime power. Then all parameters n, e and q for which perfect e-codes exists are known, see [1]. If $p_i = p^{a_i}$, $i = 1, 2, \ldots, n$, (different a_i's) where p is a prime, then several perfect 1-codes are known, see [3] and [4]. In the general case, when the

Received October 14, 1974.

p_i's are arbitrary, no perfect e-code has been found and the non-existence has been proved only for a few cases, see [2].

Now, in many cases when the necessary condition given by the generalised Lloyd theorem is satisfied, then, by using (i) and (ii), it is possible to prove the non-existence of perfect e-codes. But, unfortunately, by these methods, we cannot say anything about the case $p_1=p_2=\ldots=p_n=q$, where q is not a prime power.

1. The algebra $K[X_1,\ldots,X_n]/(X_1^{p_1}-1,\ldots,X_n^{p_n}-1)$.

Let K be an infinite field that contains all primitive p_ith root's of unity. Let $K[X_1,\ldots,X_n]/(X_1^{p_1}-1,\ldots,X_n^{p_n}-1)$ denote the algebra over K generated by the monomials

$$X_1^{s_1}\ldots X_n^{s_n}, \quad (s_1,\ldots,s_n)\in S,$$

where multiplication is defined by

$$X_1^{s_1}\ldots X_n^{s_n}X_1^{t_1}\ldots X_n^{t_n} = X_1^{s_1+t_1}\ldots X_n^{s_n+t_n}.$$

s_i+t_i is the sum of s_i and t_i in S_i.

Let A and B be subsets of S. Then the sum $A+B$ is defined to be the set of all elements $c=a+b$ where $a\in A$ and $b\in B$, counted with multiplicities (note that in general c can be written in many ways as a sum). Note that we may represent A and B by the elements

$$A(X_1,\ldots,X_n) = \textstyle\sum_{s\in A} X_1^{s_1}\ldots X_n^{s_n}$$
$$B(X_1,\ldots,X_n) = \textstyle\sum_{t\in B} X_1^{t_1}\ldots X_n^{t_n}$$

of $K[X_1,\ldots,X_n]/(X_1^{p_1}-1,\ldots,X_n^{p_n}-1)$. Then $A+B$ is represented by the element

$$A(X_1,\ldots,X_n)B(X_1,\ldots,X_n)$$

of $K[X_1,\ldots,X_n]/(X_1^{p_1}-1,\ldots,X_n^{p_n}-1)$.

If C is a perfect e-code, then, as easily seen,

$$S_e(0)+C = S. \tag{1}$$

Since (1) is equivalent to

$$S_e(0)(X_1,\ldots,X_n)C(X_1,\ldots,X_n) = S(X_1,\ldots,X_n) \tag{2}$$

the following lemma and its corollary seem to be usefull in the study of perfect codes.

Let ϑ_i be a primitive p_ith root of unity. Denote by $y_t(X_1,\ldots,X_n)$, $t=(t_1,\ldots,t_n)\in S$, the following element of

$$K[X_1,\ldots,X_n]/(X_1^{p_1}-1,\ldots,X_n^{p_n}-1):$$
$$y_t(X_1,\ldots,X_n) = \prod_1^n (1+\vartheta_i^{t_i}X_i+\ldots+\vartheta_i^{(p_i-1)t_i}X_i^{p_i-1})/p_i\,.$$

LEMMA 1. *The vectors $y_t(X_1,\ldots,X_n)$, $t\in S$, is a base of*

$$K[X_1,\ldots,X_n]/(X_1^{p_1}-1,\ldots,X_n^{p_n}-1)$$

and

$$y_t(X_1,\ldots,X_n)y_{t'}(X_1,\ldots,X_n) = \begin{cases} y_t(X_1,\ldots,X_n) & \text{if } t=t' \\ 0 & \text{if } t\neq t' \end{cases}$$

PROOF. Since, for any pth root of unity ϑ,

$$1+\vartheta+\ldots+\vartheta^{p-1} = \begin{cases} p & \text{if } \vartheta=1 \\ 0 & \text{if } \vartheta\neq 1 \end{cases}$$

we find that

$$y_t(\vartheta_1^{-s_1},\ldots,\vartheta_n^{-s_n}) = \begin{cases} 1 & \text{if } (s_1,\ldots,s_n)=(t_1,\ldots,t_n) \\ 0 & \text{if } (s_1,\ldots,s_n)\neq(t_1,\ldots,t_n)\,. \end{cases}$$

Now suppose that there are elements $\alpha_t\in K$ such that

$$\textstyle\sum_{t\in S}\alpha_t y_t(X_1,\ldots,X_n) = 0\,.$$

If we put $X_i=\vartheta_i^{-t_i}$, $i=1,2,\ldots,n$, in the equality above, then we find that $\alpha_t=0$ for $t=(t_1,\ldots,t_n)$. We conclude that $\alpha_t=0$ for every $t\in S$ and, consequently, the vectors $y_t(X_1,\ldots,X_n)$ $t\in S$ are linearly independent. Since the dimension of $K[X_1,\ldots,X_n]/(X_1^{p_1}-1,\ldots,X_n^{p_n}-1)$ as vector-space over K is $|S|$ and the number of vectors $y_t(X_1,\ldots,X_n)$, $t\in S$, is $|S|$ we have now proved the first assertion of the lemma.

An easy computation shows that if $\vartheta^p=1$ and $q=p-1$, then

$$\begin{aligned}&(1+\vartheta^tX+\ldots+\vartheta^{qt}X^q)(1+\vartheta^{t'}X+\ldots+\vartheta^{qt'}X^q)\\ &\equiv (1+\vartheta^tX+\ldots+\vartheta^{qt}X^q)(1+\vartheta^{t'-t}+\ldots+\vartheta^{q(t'-t)}) \mod X^p-1\,.\end{aligned}$$

From that fact the second assertion of the lemma is easily deduced.

COROLLARY. *If the elements $A(X_1,\ldots,X_n)$, $B(X_1,\ldots,X_n)$ and $C(X_1,\ldots,X_n)$ of $K[X_1,\ldots,X_n]/(X_1^{p_1}-1,\ldots,X_n^{p_n}-1)$ satisfy*

$$A(X_1,\ldots,X_n)B(X_1,\ldots,X_n) = C(X_1,\ldots,X_n)\,, \tag{3}$$

then their coordinates α_t, β_t resp. γ_t in the base $y_t(X_1,\ldots,X_n)$, $t\in S$, satisfy

$$\alpha_t\beta_t = \gamma_t\,.$$

2. The weight enumerator.

Let $K[Z_1,\ldots,Z_k]$ denote the ring of polynomials in the variables $Z_1,\ldots,Z_k$ with coefficients in the field K. Consider this ring of polynomials and the algebra $K[X_1,\ldots,X_n]/(X_1^{p_1}-1,\ldots,X_n^{p_n}-1)$ as vectorspaces over K. We shall now define vectorspace homomorphisms from $K[X_1,\ldots,X_n]/(X_1^{p_1}-1,\ldots,X_n^{p_n}-1)$ to $K[Z_1,\ldots,Z_k]$ which we shall use later.

Let I be a subset of $\{1,2,\ldots,n\}$. Define the homomorphism f_I from $K[X_1,\ldots,X_n]/(X_1^{p_1}-1,\ldots,X_n^{p_n}-1)$ to $K[Z_1,\ldots,Z_n]$ by

$$f_I\colon \quad X_1^{s_1}\ldots X_n^{s_n} \mapsto Z_1^{d_1}\ldots Z_n^{d_n},$$

where

$$d_j = \begin{cases} s_j & \text{if } j \notin I \\ 0 & \text{if } j \in I \text{ and } s_j = 0 \\ 1 & \text{if } j \in I \text{ and } s_j \neq 0. \end{cases}$$

The image of the vectors $y_t(X_1,\ldots,X_n)$, $t \in S$, by the homomorphism f_I will be

$$(1/\textstyle\prod_1^n p_i)\prod_{j\notin I}(1+\vartheta_j^{t_j}X_j+\ldots+\vartheta_j^{(p_j-1)t_j}X_j^{p_j-1})\cdot \\ \cdot\prod_{j\in I}(1+(p_j-1)Z_j)^{1-d_j}(1-Z_j)^{d_j},$$

where if $j \in I$, then

$$d_j = \begin{cases} 0 & \text{if } t_j = 0 \\ 1 & \text{if } t_j \neq 0. \end{cases}$$

If $I=\{1,2,\ldots,n\}$, then we shall write f instead of f_I.

Let F denote a partition $A_1,\ldots,A_k$ of the set $\{1,2,\ldots,n\}$. Define the homomorphism g_F from $K[Z_1,\ldots,Z_n]$ to $K[Z_1,\ldots,Z_k]$ by

$$g_F\colon \quad Z_1^{d_1}\ldots Z_n^{d_n} \mapsto Z_1^{c_1}\ldots Z_k^{c_k},$$

where $c_i=\sum_{j\in A_i} d_j$. Suppose that $q_1,\ldots,q_k$ are integers such that if $i \in A_v$, then $p_i=q_v$. The image of $y_t(X_1,\ldots,X_n)$ by $g_F\circ f$ will be

$$g_F\circ f(y_t(X_1,\ldots,X_n)) = \textstyle\prod_1^k(1+(q_i-1)Z_i)^{n_i-d_i}(1-Z_i)^{d_i}, \tag{4}$$

where $n_i=|A_i|$ and $d_i=|\{j\in A_i \mid t_j\neq 0\}|$. We shall denote d_i by $w_i(t)$ and call it the ith weight of t. Let A be a subset of S. If A is represented by $A(X_1,\ldots,X_n)$ in $K[X_1,\ldots,X_n]/(X_1^{p_1}-1,\ldots,X_n^{p_n}-1)$, then

$$g_F\circ f(A(X_1,\ldots,X_n)) = \sum \delta[(c_1,\ldots,c_k),A]Z_1^{c_1}\ldots Z_k^{c_k},$$

where $\delta[(c_1,\ldots,c_k),A]$ is the number of elements of A, the ith weight of which equals c_i, $i=1,2,\ldots,k$. The polynomial $g_F\circ f(A(X_1,\ldots,X_n))$ is called the weight enumerator of A and will be denoted $A(Z_1,\ldots,Z_k)$.

Note that, by the homomorphisms f_I and $g_F \circ f$ polynomials of $K[X_1,\ldots,X_n]/(X_1^{p_1}-1,\ldots,X_n^{p_n}-1)$ with non-negative integer coefficients are mapped to polynomials of $K[Z_1,\ldots,Z_k]$ with non-negative integer coefficients. This fact shall be used in section 4 to prove some necessary conditions for the existence of perfect codes.

3. The Lloyd theorem.

Consider $K[X_1,\ldots,X_n]/(X_1^{p_1}-1,\ldots,X_n^{p_n}-1)$ as a vector space over K. Let $L(C(X):A(X))$ denote the subspace of

$$K[X_1,\ldots,X_n]/(X_1^{p_1}-1,\ldots,X_n^{p_n}-1)$$

spanned by the vectors $B(X_1,\ldots,X_n)$ satisfying (3). By using the corollary of Lemma 1 we may calculate the dimension of $L(C(X):A(X))$. If for some t, the tth coordinate in the base $y_t(X_1,\ldots,X_n)$, $t\in S$, of $A(X_1,\ldots,X_n)$ is zero and the tth coordinate of $C(X_1,\ldots,X_n)$ is nonzero, then it is impossible to find a vector $B(X_1,\ldots,X_n)$ satisfying (3). In this case we shall say that the dimension of $L(C(X):A(X))$ equals -1. In the other cases, then the dimension of $L(C(X):A(X))$ equals 1 plus the number of zero coordinates of $A(X_1,\ldots,X_n)$ in the base $y_t(X_1,\ldots,X_n)$, $t\in S$.

It may be seen that the vectors $B(X_1,\ldots,X_n)$ satisfying (3) are elements of an affine subspace of $K[X_1,\ldots,X_n]/(X_1^{p_1}-1,\ldots,X_n^{p_n}-1)$ of dimension $\big(\dim L(C(X):A(X))-1\big)$. But here we shall not use that fact.

Let $L(B(X);A,C)$ denote the subspace of

$$K[X_1,\ldots,X_n]/(X_1^{p_1}-1,\ldots,X_n^{p_n}-1)$$

spanned by the vectors $B(X_1,\ldots,X_n)$ which are the representation vectors of the sets B satisfying $A+B=C$.

LEMMA 2. *Let A and C be two subsets of S. If h is a vector space homomorphism from $K[X_1,\ldots,X_n]/(X_1^{p_1}-1,\ldots,X_n^{p_n}-1)$ to $K[Z_1,\ldots,Z_k]$, then*

$$\dim h\big(L(C(X):A(X))\big) \geqq \dim h\big(L(B(X);A,C)\big)\,.$$

PROOF. Since $L(B(X);A,C)\subseteqq L(C(X):A(X))$ and since h is a vector-space homomorphism, we find that lemma 2 is true.

Now we shall prove a generalisation of the Lloyd theorem. The proof will show how Lemma 2 and the corollary of Lemma 1 may be used to find necessary conditions for the existence of sets A, B and C satisfying $A+B=C$. But first we have to give some notations.

Let F be a partition $A_1,\ldots,A_k$ of $\{1,2,\ldots,n\}$ and $n_i=|A_i|$, $i=1,2,\ldots,k$. Denote by $P(F,e)$ the number

$$P(F,e) = |\{(s_1,\ldots,s_k) \mid s_1+\ldots+s_k\leqq e,\ s_i\in \mathbf{Z},\ \text{and } 0\leqq s_i\leqq n_i \text{ for } i=1,2,\ldots,k\}| .$$

Suppose that F and the numbers $q_1,\ldots,q_k$ are such that $i\in A_v$ implies that $p_i=q_v$, $v=1,2,\ldots,k$. Consider the polynomial

$$\prod_1^k (1+(q_i-1)Z_i)^{n_i-d_i}(1-Z_i)^{d_i} .$$

Denote the coefficient of the monomial $Z_1^{s_1}\ldots Z_k^{s_k}$ in this polynomial by

$$\delta[(s_1,\ldots,s_k),(d_1,\ldots,d_k),F] .$$

THEOREM 1. *Let F be as above. If a perfect e-code exists in S, then the number of distinct k-tuples $(d_1,\ldots,d_k)$, where d_i is an integer and $0\leqq d_i\leqq n_i$, $i=1,2,\ldots,k$, satisfying the equation*

$$0 = \sum_{s_1+\ldots+s_k\leqq e} \delta[(s_1,\ldots,s_k),(x_1,\ldots,x_k),F] \tag{5}$$

in the unknown $x_1,\ldots,x_k$ is greater than or equal to $P(F,e)-1$.

PROOF. We first intend to find the coordinates of $S_e(0)(X_1,\ldots,X_n)$ in the base $y_t(X_1,\ldots,X_n)$, $t\in S$. Denote by $\sigma_i(X)$ the polynomial

$$\sigma_i(X) = X+\ldots+X^{p_i-1} .$$

It is easily seen that

$$S_e(0)(X_1,\ldots,X_n) = 1+\sum_1^n \sigma_i(X_i)+\ldots+\sum_{i_1<\ldots<i_e} \sigma_{i_1}(X_{i_1})\ldots\sigma_{i_e}(X_{i_e}) .$$

The coordinate α_t, $t=(t_1,\ldots,t_n)$, of $S_e(0)(X_1,\ldots,X_n)$ is given by $S_e(0)(\vartheta_1^{-t_1},\ldots,\vartheta_n^{-t_n})$. Since

$$\sigma_i(\vartheta_i^{-t_i}) = \begin{cases} p_i-1 & \text{if } t_i=0 \\ -1 & \text{if } t_i\in\{1,2,\ldots,p_i-1\} , \end{cases}$$

we may conclude that

$$\alpha_t = \sum_{s_1+\ldots+s_n\leqq e} \delta[(s_1,\ldots,s_n),(d_1,\ldots,d_n),F_0] ,$$

where

$$d_i = \begin{cases} 0 & \text{if } t_i=0 \\ 1 & \text{if } t_i\neq 0 , \end{cases}$$

and F_0 is the partition $\{1\},\{2\},\ldots,\{n\}$ of $\{1,2,\ldots,n\}$. From this formula for α_t we find that

$$\alpha_t = \sum_{s_1+\ldots+s_k\leqq e} \delta[(s_1,\ldots,s_k),(d_1,\ldots,d_k),F] , \tag{6}$$

where $s_i \in \mathbf{Z}$, $0 \leqq s_i \leqq n_i$, and $d_i = w_i(t)$. Consequently if $C(X_1, \ldots, X_n)$ satisfies (2), then by the fact that $S(X_1, \ldots, X_n) = y_0(X_1, \ldots, X_n) \prod_1^n p_i$, the corollary of Lemma 1 and by (4) we get that

$$(7) \quad g_F \circ f(C(X_1, \ldots, X_n)) = (1/|S_e(0)|) \prod_1^k (1 + (q_i - 1)Z_i)^{n_i} + \sum B_d \prod_1^k (1 + (q_i - 1)Z_i)^{n_i - d_i} (1 - Z_i)^{d_i},$$

where $B_d = 0$, $d = (d_1, \ldots, d_k) \neq (0, \ldots, 0)$, if there is a $t \in S$ such that $w_i(t) = d_i$ and $\alpha_t \neq 0$. Observe that $\dim g_F \circ f\big(L(S(X) : S_e(0)(X))\big)$ is less than or equal to 1 plus the number of k-tuples $(d_1, \ldots, d_k)$ satisfying (5).

Now let $(s_1, \ldots, s_k)$ be a given k-tuple satisfying $s_1 + \ldots + s_k \leqq e$, $s_i \in \mathbf{Z}$, and $0 \leqq s_i \leqq n_i$. By adding a suitable element of S to a perfect e-code it is possible to find a perfect e-code C' whose representation vector $C'(X_1, \ldots, X_n)$ in $K[X_1, \ldots, X_n]/(X_1^{p_1} - 1, \ldots, X_n^{p_n} - 1)$ satisfies

$$g_F \circ f(C'(X_1, \ldots, X_n)) = Z_1^{s_1} \ldots Z_k^{s_k} + (\text{terms of degree} > e) .$$

Consequently

$$P(F, e) \leqq \dim g_F \circ f\big(L(C(X); S_e(0), S)\big) .$$

By using Lemma 2, then by (6) and (7) we have proved Theorem 1.

In the case $p_1 = p_2 = \ldots = p_n = p$ we can say even more about the zeros.

COROLLARY. *If a perfect e-code exists in S and $p_1 = \ldots = p_n = p$ then the number of distinct integer zeros d, $0 \leqq d \leqq n$, of the equation*

$$(8) \qquad \sum_0^e \operatorname{coeff}_{Z^s}(1 + (p-1)Z)^{n-x}(1 - Z)^x = 0$$

in the unknown x is equal to e.

PROOF. If $F = \{A\}$ and $A = \{1, 2, \ldots, n\}$, then $P(F, e) = e + 1$. Since the equation (8) is of degree e it has at most e zeros.

4. Applications.

We shall prove the following two theorems.

THEOREM 2. *If a perfect e-code exists in S and the prime p divides at least one of the numbers p_i, then p divides the number $|S_e(0)|$.*

THEOREM 3. *Let p be a prime and*

$$I_p = \{i \mid p \text{ divides } p_i\} \subseteqq \{1, 2, \ldots, n\} .$$

If a perfect e-code exists in S and $I_p \neq \emptyset$, then $e > n - |I_p|$.

But since the proofs of these theorems are very technical, we shall first use an example to show how the non-existence of a code can be proved by using Sections 1, 2 and 3.

EXAMPLE. Let $p_1=6$ and $p_2=\ldots=p_7=2$. Suppose that C is a perfect 1-code in $S=S_1\times S_2\times\ldots\times S_7$. Let F denote the partition $\{1\}, \{2,3,\ldots,7\}$ of the set $\{1,2,\ldots,7\}$. By (6) and (7) we get that

$$\begin{aligned} C(Z_1,Z_2) &= g_F\circ f(C(X_1,\ldots,X_7)) \\ &= 1/12(1+5Z_1)(1+Z_2)^6+B_1(1+5Z_1)(1-Z_2)^6+ \\ &\quad +B_2(1-Z_1)(1+Z_2)^3(1-Z_2)^3\,. \end{aligned}$$

Since $P(F,1)=3$ we can not use Lemma 2 to prove that no perfect 1-code exists in S. But if we substitute $Z_2=1$ in the polynomial $C(Z_1,Z_2)$, then we get that

$$C(Z_1,1) = 16/3\cdot(1+5Z_1)\,.$$

Since $C(X_1,\ldots,X_7)\in \mathbf{Z}[X_1,\ldots,X_7]$ we get that $C(Z_1,1)\in\mathbf{Z}[Z_1]$. Consequently we have a contradiction and there can not possibly exist any perfect 1-code in S.

Now we shall give some notations and lemmas that we shall use in the proofs of Theorem 3 and 4.

Let t be a m-tuple and I a subset of $\{1,2,\ldots,m\}$. Denote by $S(t,I)$ the set

$$S(t,I) = \{(s_1,\ldots,s_m) \mid s_i=t_i,\ i\notin I\}\,.$$

We note that for two m-tuples t and t' either $S(t,I)\cap S(t',I)=\emptyset$ or $S(t,I)=S(t',I)$.

LEMMA 3. *Suppose that* $C(X_1,\ldots,X_n)\in\mathbf{Z}[X_1,\ldots,X_n]$. *Let* α_t, $t\in S$, *be the coordinates of* $C(X_1,\ldots,X_n)$ *in the base* $y_t(X_1,\ldots,X_n)$, $t\in S$, *of* $K[X_1,\ldots,X_n]/({X_1}^{p_1}-1,\ldots,{X_n}^{p_n}-1)$. *Then for any n-tuple* t *and* $I\subseteqq\{1,2,\ldots,n\}$

$$(1/|S|)\textstyle\sum_{s\in S(t,I)}\alpha_s = \beta_t/\prod_{i\notin I}p_i\,,$$

where

$$\beta_t\in\mathbf{Z}[\vartheta_{i_1},\ldots,\vartheta_{i_k}]$$

and

$$\{i_1,i_2,\ldots,i_k\} = \{1,2,\ldots,n\}\setminus I\,.$$

PROOF. Substitute $X_i=0$ if $i\in I$ and $X_i=\vartheta_i^{-t_i}$ if $i\notin I$ in the polynomials $C(X_1,\ldots,X_n)$ and $y_s(X_1,\ldots,X_n)$, $s\in S$. We get that by this substitution

$$C(X_1,\ldots,X_n) = \beta_t\in\mathbf{Z}[\vartheta_{i_1},\ldots,\vartheta_{i_k}]$$

and that

$$y_{t'}(X_1,\ldots,X_n) = \begin{cases} 0 & \text{if } t' \notin S(t,I) \\ 1/\prod_{i\in I} p_i & \text{if } t' \in S(t,I) \end{cases}$$

Consequently

$$\sum_{s\in S} \alpha_s y_s(X_1,\ldots,X_n) = \sum_{s\in S(t,I)} \alpha_s / \prod_{i\in I} p_i ,$$

and Lemma 3 is proved.

LEMMA 4. *Suppose that* $C(X_1,\ldots,X_n)\in \mathbf{Z}[X_1,\ldots,X_n]$. *Let the elements* B_d *of* K *be such that*

$$C(Z_1,\ldots,Z_k) = \sum B_d \prod_1^k (1+(q_i-1)Z_i)^{n_i-d_i}(1-Z_i)^{d_i} .$$

Then for any k*-tuple* d *and* $I\subseteqq\{1,2,\ldots,k\}$

$$\sum_{d'\in S(d,I)} B_{d'} = \beta_d / \prod_{i\notin I} q_i^{n_i} ,$$

where

$$\beta_d \in \mathbf{Z}[\vartheta_{i_1},\ldots,\vartheta_{i_m}]$$

and

$$\{i_1,\ldots,i_m\} = \{1,2,\ldots,n\} \setminus \bigcup_{i\in I} A_i .$$

PROOF. Since $g_F \circ f(y_t(X_1,\ldots,X_n)) = g_F \circ f(y_{t'}(X_1,\ldots,X_n))$ if $w_i(t) = w_i(t')$, $i=1,2,\ldots,k$, we get that

$$B_d = (1/|S|) \sum_{t,\, w_i(t)=d_i} \alpha_t .$$

Consequently

$$\sum_{d'\in S(d,I)} B_{d'} = \sum_{t,\, w_i(t)=d_i,\, i\notin I} \alpha_t / |S| .$$

Let $S(t^{(1)},I)$, $S(t^{(2)},I),\ldots,S(t^{(m)},I)$ be a partition of $\{t\in S \mid w_i(t)=d_i,\ i\notin I\}$. We find that (cf. Lemma 3)

$$\sum_{d'\in S(d,I)} B_{d'} = \sum_{v=1}^{m} \beta_{t^{(v)}} / \prod_{i\notin I} q_i^{n_i} ,$$

and Lemma 4 is proved.

If we return to the example above we shall find, using Lemma 4, that $A_1 = b_1/64$ and $A_2 = b_2/64$ where b_1 and b_2 are integers. It is now easy to see that the constant of the polynomial $C(Z_1,Z_2)$ can never be an integer. Consequently there is no perfect 1-code in this particular S.

Since we have fixed the partition F we shall write

$$\delta[(s_1,\ldots,s_k),(d_1,\ldots,d_k)]$$

instead of $\delta[(s_1,\ldots,s_k),(d_1,\ldots,d_k),F]$. We shall use the notation

$$\delta[c_i,d_i] = \operatorname{coeff}_{Z_i^{c_i}}(1+(q_i-1)Z_i)^{n_i-d_i}(1-Z_i)^{d_i}$$

only when its meaning is clear. It follows from the definition of these symbols that if $c=(c_1,\ldots,c_k)$ and $d=(d_1,\ldots,d_k)$, then

$$\delta[c,d] = \prod_1^k \delta[c_i,d_i] .$$

LEMMA 5. *If p divides q_i, then*

$$\delta[c_i,d_i] \equiv \delta[c_i,d_i'] \mod p .$$

PROOF. Since for any g_i

$$(1+(q_i-1)Z_i)^{n_i-g_i}(1-Z_i)^{g_i} \equiv (1-Z_i)^{n_i} \mod p$$

we get that

$$(1+(q_i-1)Z_i)^{n_i-d_i}(1-Z_i)^{d_i} \equiv (1+(q_i-1)Z_i)^{n_i-d_i'}(1-Z_i)^{d_i'}$$

and Lemma 5 is proved.

If $c=(c_1,\ldots,c_k)$, then let $I(c)$ denote the k-tuple $(s_1,\ldots,s_k)$ where $s_i=0$ if $i\in I$ and $s_i=c_i$ if $i\notin I$. Let P denote the set

$$P = \{(s_1,\ldots,s_k) \mid s_i\in \mathbf{Z},\ 0\leqq s_i\leqq n_i \text{ and } s_1+\ldots+s_k\leqq e\} .$$

Let D denote the set

$$D = \{d\neq 0 \mid \textstyle\sum_{s\in P} \delta[s,d]=0\} .$$

Note that

$$\textstyle\sum_{s\in P} \delta[s,0] = |S_e(0)| . \tag{9}$$

From (7) we now deduce that if C satisfies (2), then

$$g_F\circ f(C(X_1,\ldots,X_n)) = (1/|S_e(0)|)\prod_1^k(1+(q_i-1)Z_i)^{n_i} + \textstyle\sum_{d\in D} B_d \prod_1^k (1+(q_i-1)Z_i)^{n_i-d_i}(1-Z_i)^{d_i} . \tag{10}$$

PROOF OF THEOREM 2. Let p be a prime and

$$I = \{i \mid p \text{ divides } q_i\} \subseteq \{1,2,\ldots,k\} .$$

Suppose that there exists a perfect e-code in S and that p does not divide $|S_e(0)|$. Since $|S_e(0)|>1$ and $g_F\circ f(C(X_1,\ldots,X_n))$ is a polynomial with integer coefficients we find by (10) that the set D is non-empty. So by (9) if $d\in D$, then

$$|S_e(0)| = \textstyle\sum_{s\in P}[\delta[s,0]-\delta[s,d]] .$$

Using Lemma 5 we find that

$$\begin{aligned}\delta[s,0]-\delta[s,d] &\equiv \textstyle\prod_1^k \delta[s_i,0]-\prod_1^k \delta[s_i,d_i] \\ &\equiv \textstyle\prod_{i\in I}\delta[s_i,0]\left[\prod_{i\notin I}\delta[s_i,0]-\prod_{i\notin I}\delta[s_i,d_i]\right] \mod p\,.\end{aligned}$$

We get that if $I=\{1,2,\ldots,k\}$ or $d_i=0$ for $i\notin I$, then p divides $\delta[s,0]-\delta[s,d]$ for every $s\in P$. Consequently I is a proper subset of $\{1,2,\ldots,k\}$ and

$$D\cap S(0,I)=\emptyset\,. \tag{11}$$

Let C be any perfect e-code. From (10) and the definitions of $\delta[s,C]$ and $\delta[s,d]$ we get the following relations:

$$\delta[s,C]=B_0\delta[s,0]+\textstyle\sum_{d\in D}B_d\delta[s,d],\quad s\in P\,. \tag{12}$$

Define $T(C)$ to be the integer

$$T(C)=\textstyle\sum_{s\in P}\left[-\delta[s,C]+\delta[I(s),C]\prod_{i\in I}\delta[s_i,0]\right].$$

We get that

$$T(C)=B_0T_0+\textstyle\sum_{d\in D}B_dT_d$$

where

$$\begin{aligned}T_d=\textstyle\sum_{s\in P}\Big[&\delta[s,0]-\delta[s,d]\\ &-\textstyle\prod_{i\in I}\delta[s_i,0]\left[\prod_{i\notin I}\delta[s_i,0]-\prod_{i\notin I}\delta[s_i,d_i]\right]\Big].\end{aligned}$$

By using Lemma 5 we find that

$$\begin{aligned}\delta[s,0]-\delta[s,d] &\equiv \textstyle\prod_1^k \delta[s_i,0]-\prod_1^k \delta[s_i,d_i] \\ &\equiv \textstyle\prod_{i\in I}\delta[s_i,0]\left[\prod_{i\notin I}\delta[s_i,0]-\prod_{i\notin I}\delta[s_i,d_i]\right] \mod p\,.\end{aligned} \tag{13}$$

Consequently, since each term in the sum T_d is divisible by p,

$$T_d\equiv 0 \mod p\,. \tag{14}$$

We also find that

$$\begin{aligned}&T_d+\textstyle\sum_{s\in P}\prod_{i\in I}\delta[s_i,0]\left[\prod_{i\notin I}\delta[s_i,0]-\prod_{i\notin I}\delta[s_i,d_i]\right]\\ &\qquad=\textstyle\sum_{s\in P}\delta[s,0]-\delta[s,d]=\begin{cases}|S_e(0)| & \text{if } d\in D\\ 0 & \text{if } d=0\,.\end{cases}\end{aligned}$$

Consequently

$$T_{d'}=T_d \text{ if } d,d'\in D \text{ and } d'\in S(d,I)\,. \tag{15}$$

Let $d^{(1)},\ldots,d^{(m)}$ be k-tuples such that

$$S(d^{(1)},I),S(d^{(2)},I),\ldots,S(d^{(m)},I)$$

is a partition of the set of k-tuples $(d_1,\ldots,d_k)$ satisfying $d_i\in\mathbf{Z}$ and $0\leqq d_i\leqq n_i$. Let J be a subset of $\{1,2,\ldots,m\}$ such that $S(d^{(i)},I)\cap D\neq\emptyset$

if and only if $i \in J$. We may suppose that $d^{(i)} \in D$ if $i \in J$. From the fact that $T_0 = 0$, (11), (15) we get that

$$\begin{aligned} T(C) &= B_0 T_0 + \sum_{d \in D} B_d T_d = \sum_{i=1}^{m} \sum_{d \in S(d^{(i)}, I) \cap D} B_d T_d \\ &= \sum_{i \in J} T_{d^{(i)}} \sum_{d \in S(d^{(i)}, I) \cap D} B_d \\ &= \sum_{i \in J} T_{d^{(i)}} \sum_{d \in S(d^{(i)}, I)} B_d = \sum_{i \in J} T_{d^{(i)}} \beta_{d^{(i)}} / \prod_{i \notin I} q_i^{n_i} , \end{aligned}$$

where by Lemma 4 since $C(X_1, \ldots, X_n) \in \mathsf{Z}[X_1, \ldots, X_n]$

$$\beta_{d^{(i)}} \in \mathsf{Z}[\vartheta_1, \ldots, \vartheta_n] .$$

Since p divides $T_{d^{(i)}}$, $i \in J$, (14), we find that

$$T(C) \prod_{i \notin I} q_i^{n_i} / p \in \mathsf{Z}[\vartheta_1, \ldots, \vartheta_n] .$$

Since all elements of $\mathsf{Z}[\vartheta_1, \ldots, \vartheta_n]$ are integral over Z we conclude that $T(C) \prod_{i \notin I} q_i^{n_i} / p \in \mathsf{Z}$. From the fact that the prime p does not divide q_i for $i \notin I$ we conclude that p divides $T(C)$.

Now we shall prove that there exists a perfect e-code C' in S such that $T(C')$ is not divisible by p. Let $s = (s_1, \ldots, s_n)$ be such that $w(s) = 1$ and $s_j = 0$ if $j \notin \bigcup_{i \in I} A_i$ and suppose that C is a perfect e-code. If c is an element of C, then the subset $C' = s - c + C$ of S is a perfect e-code that contains the element s. Since the minimum distance between the elements of C' is $2e+1$ we get that if $c' \in P$, then

$$\delta[c', C'] = \begin{cases} 0 & \text{if } c' \neq (w_1(s), \ldots, w_k(s)) \\ 1 & \text{if } c' = (w_1(s), \ldots, w_k(s)) . \end{cases}$$

It follows from the definition of $T(C')$ that $T(C') = -1$. This contradicts the fact that p divides $T(C)$ for every perfect e-code C in S. Consequently if there exists a perfect e-code in S, then p divides $|S_e(0)|$ and Theorem 2 is proved.

Proof of Theorem 3. Let p be a prime and

$$I = \{i \mid p \text{ divides } q_i\} \subseteq \{1, 2, \ldots, k\} .$$

Suppose that C is a perfect e-code in S. Consider the relations (12) and let $T(C)$ denote the integer

$$T(C) = \sum_{s \in P} \left[\prod_{i \in I} \delta[s_i, 0] \delta[I(s), C] - \prod_{1}^{k} \delta[s_i, 0] \delta[0, C] \right] .$$

We find that

$$T(C) = B_0 T_0 + \sum_{d \in D} B_d T_d ,$$

where $T_0 = 0$ and if $d \in D$, then

$$T_d = \sum_{s \in P} \left[\delta[s,0] - \delta[s,d] - \prod_{i \in I} \delta[s_i,0]\left[\prod_{i \notin I} \delta[s_i,0] - \prod_{i \notin I} \delta[s_i,d_i]\right]\right] - |S_e(0)| .$$

Since p divides $|S_e(0)|$, Theorem 2, we conclude using (13) that $T_d \equiv 0 \bmod p$ if $d \in D$. We also find that $T_d = T_{d'}$ if $d' \in S(d,1)$. So by similar arguments as those we used in the proof of Theorem 2 we find that p divides $T(C)$.

Suppose that $e \leqq n - |\bigcup_{i \in I} A_i|$. If a perfect e-code exists in S, then there will exist a perfect e-code C and an element $c \in C$ satisfying

$$\sum_{i \notin I} w_i(c) = e \text{ and } w_i(c) = 0 \text{ if } i \in I .$$

Since the minimum distance of C is $2e+1$ we find that

$$\delta[I(c'),C] = 0 \text{ if } c' \neq c \text{ and } (w_1(c'),\ldots,w_k(c')) \in P$$

and that $\delta[0,C] = 0$. Since $\delta[I(c),C] = 1$ we get that $T(C) = 1$. But this contradicts the fact that p divides $T(C)$ for every perfect e-code C of S. Consequently $e > n - |\bigcup_{i \in I} A_i|$ and Theorem 3 is proved.

The arguments in the proofs of Theorems 2 and 3 are in some cases helpful in the study of the existence of sets A and B satisfying

$$A + B = S . \tag{16}$$

For instance let A_1 and A_2 be a partition of the set $\{1,2,\ldots,n\}$ such that the prime p divides p_i iff $i \in A_1$. Let

$$A = \{s \in S \mid w_1(s) \leqq e_1 \text{ and } w_2(s) = 0\} \cup \{s \in S \mid w_2(s) \leqq e_2 \text{ and } w_1(s) = 0\} .$$

If $e_1 < |A_1|$ and $e_2 < |A_2|$, then it is possible to prove that there is no subset B of S satisfying (16).

But if A' and B' are subsets of $\times_{i \in A_1} S_i = S'$, A'' and B'' are subsets of $\times_{i \in A_2} S_i = S''$ satisfying $A' + B' = S'$ resp. $A'' + B'' = S''$, then $A' \times A'' + B' \times B'' = S' \times S''$.

Indeed it would be very interesting to know which subsets A and B of S satisfy (16).

By using the Sections 1, 2 and 3 I have found some other results that seem to be new. I hope to be able to discuss them in a forthcoming paper.

ACKNOWLEDGEMENT. I wish to thank B. Lindström for his kind interest and for his valuable criticisme of an earlier version of this paper. I also wish to mention that the paper [8] by J. E. Roos gave very much inspiration.

REFERENCES

1. A. Tietäväinen, *On the non existence of perfect codes over finite fields*, SIAM J. Appl. Math. 24 (1973), 88–96.
2. J. H. van Lint, *Recent results on perfect codes and related topics*, Proceedings of the Advanced Study Institute on Combinatorics, The Netherlands, 1974, Mathematical Centre Tracts 55, 1974, 158–178.
3. M. Herzog and J. Schönheim, *Group partition, factorization and the vector covering problem*, Canad. Math. Bull. 15 (2) (1972), 207–214.
4. B. Lindström, *Group partition and mixed perfect codes*, Canad. Math. Bull. (to appear).
5. S. P. Lloyd, *Binary block coding*, Bell System Tech. J. 36 (1957), 517–535.
6. H. W. Lenstra, Jr., *Two theorems on perfect codes*, Discrete Math. 3 (1972), 125–132.
7. P. Delsarte, *Bounds for unrestricted codes by the linear programming*, Philips Res. Rets. 27 (1972), 272–289.
8. J. E. Roos, *An algebraic study of group and nongroup error-correcting codes*, Information and Control 8 (1965), 195–214.

UNIVERSITY OF STOCKHOLM, SWEDEN