stichting
mathematisch
centrum

MC

AFDELING ZUIVERE WISKUNDE ZN 59/75 MARCH

H.W. LENSTRA, Jr.

NECESSARY CONDITIONS FOR THE EXISTENCE OF PERFECT LEE CODES

2e boerhaavestraat 49 amsterdam

Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O), by the Municipality of Amsterdam, by the University of Amsterdam, by the Free University at Amsterdam, and by industries.

AMS(MOS) subject classification scheme (1970): 94A10, 05B99.

Necessary conditions for the existence of perfect Lee codes

by

H.W. Lenstra, Jr.

ABSTRACT

Necessary conditions for the existence of perfect Lee codes are obtained.

KEY WORDS & PHRASES: *Perfect code, Lee metric.*

Necessary conditions for the existence of perfect Lee codes

by

H.W. Lenstra, Jr.

1. INTRODUCTION

Let q, m, e be integers, with $q \geq 2$, $m \geq 1$ and $e \geq 0$. We denote by $\mathbb{Z}/q\mathbb{Z}$ the ring of integers modulo q. For $x \in \mathbb{Z}/q\mathbb{Z}$, let $|x| = \min\{|y| \mid y \in \mathbb{Z}, x = (y \bmod q)\}$.

Let X denote the m-fold cartesian product

$$X = (\mathbb{Z}/q\mathbb{Z}) \times \dots \times (\mathbb{Z}/q\mathbb{Z}).$$

This is an abelian group of order q^m, which we write additively. We endow X with a metric d by

$$d((x_i)_{i=1}^m, (y_i)_{i=1}^m) = \sum_{i=1}^m |x_i - y_i|,$$

the so-called *Lee metric*.

A *perfect code of order* e is a subset C of X with the property that for every $x \in X$ there exists a unique $c \in C$ for which $d(x,c) \leq e$. We are interested in obtaining necessary conditions for the existence of such a code.

Put

$$S_e = \{s \in X \mid d(0,s) \leq e\}.$$

Clearly, a subset $C \subset X$ is a perfect code of order e if and only if every $x \in X$ has a unique decomposition $x = c + s$, with $c \in C$ and $s \in S_e$.

By G we denote the group of group automorphisms of X which are at the same time isometries. Clearly, $\#G = 2^m.m!$ for $q > 2$ and $\#G = m!$ for $q=2$. Notice $\sigma S_e = S_e$ for every $\sigma \in G$.

Let ξ_q be a fixed primitive q-th root of unity in $\mathbb{C}$. We define a pairing $<,>: X \times X \to \mathbb{C}$ by

$$<(x_i)_{i=1}^m, (y_i)_{i=1}^m> = \xi_q^{\sum_{1\leq i\leq m} x_i y_i}.$$

We have $<\sigma x,\sigma y> = <x,y>$ for all $\sigma \in G$, $x,y \in X$.

Let

$$T_e = \{0\} \cup \{x \in X \mid \sum_{s\in S_e} <x,s> = 0\} \subset X.$$

For all $\sigma \in G$ we have $\sigma T_e = T_e$. The set T_e does not depend on the choice of ξ_q, since all primitive q-th roots of unity are conjugate over $\mathbb{Q}$. For the same reason, T_e is closed under multiplication by integers which are relatively prime to q, but we will not use this.

If a group H acts on a set S, then the orbit space is denoted by S/H.

THEOREM 1. *Suppose a perfect code of order* e *exists in* X. *Then* $\#(T_e/H) \geq \#(S_e/H)$ *for all subgroups* $H \subset G$.

The case $H = G$ of this theorem is equivalent to the "Lloyd"-theorem which has been proved by L.A. BASSALYGO [1].

THEOREM 2. *Suppose a perfect code of order* e *exists in* X. *Then* $\#S_e$ *divides* $\#<T_e>$, *where* $<T_e>$ *denotes the subgroup of* X *generated by* T_e. *More precisely, if*

$$Y_e = \{y \in X \mid <t,y> = 1 \text{ for all } t \in T_e\}$$

then Y_e *is a subgroup of* X *of index equal to* $\#<T_e>$, *and every perfect code of order* e *in* X *is periodic modulo* Y_e *(i.e.: a union of cosets of* Y_e*).*

Theorem 2 generalizes the "sphere packing bound" $\#S_e | q^m$, since $\#<T_e>$ obviously divides $\#X = q^m$.

THEOREM 3. *Suppose* q *is prime, and* $\#S_e = q$. *Then there exists a perfect code* $C \subset X$ *of order* e *if and only if there exists a subgroup* $C \subset X$ *whose underlying set is a perfect code of order* e.

Section 2 gives some illustrations of theorems 1, 2 and 3, and section 3 contains the proofs. The pleasure of formulating and proving analogues of these theorems for other situations (mixed perfect Lee-codes, for example) is left to the reader.

2. EXAMPLES.

We only consider examples which satisfy the sphere packing bound $\#S_e | q^m$.

(2.1) q=5, m=2, e=1. It is easily seen that in this case a perfect code exists. We have

$$S_1 = \{(0,0),\ (\pm 1,0),\ (0,\pm 1)\} \subset (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) = X.$$

Let $x = (a,b) \in X$, $x \neq (0,0)$. Then $x \in T_1$ if and only if $1 + \xi_5^a + \xi_5^{-a} + \xi_5^b + \xi_5^{-b} = 0$. Using that $X^4 + X^3 + X^2 + X + 1$ is the irreducible polynomial of ξ_5 over $\mathbb{Q}$ one arrives at

$$T_1 = \{(0,0),\ (\pm 2,\pm 1),\ (\pm 1,\pm 2)\}.$$

Thus we see $\#T_1 = 9 > 5 = \#S_1$ and $\#(T_1/G) = 2 = \#(S_1/G)$, in accordance with theorem 1.

(2.2) q=13, m=2, e=2. Also in this case a perfect code exists. One finds that T_2 is the union of the G-orbits containing

$$(0,0),\ (1,5),\ (2,3),\ (4,6).$$

Hence $\#(T_2/G) = 4 = \#(S_2/G)$.

(2.3) q=41, m=4, e=2 or q=61, m=5, e=2. It has been shown by E. Wattel that no perfect group code exists with these parameters. Since $\#S_2 = q$ is prime, it follows from theorem 3 that no perfect code at all exists in these cases.

(2.4) q=85, m=6, e=2. Using the methods of [2] and computer results kindly provided by A.E. Brouwer I checked that T_2 consists of the G-orbits of

$$(0, 0, 0, 0, 0, 0),$$
$$(0, 0, 17, 17, 34, 34),$$
$$(0, 17, 17, 17, 17, 34),$$
$$(0, 34, 34, 34, 34, 17).$$

Hence $\#(T_2/G) = 4 = \#(S_2/G)$ so the necessary condition of Bassalygo's theorem is satisfied (the case H=G of theorem 1). But by theorem 2 no perfect code exists in this case, since $\#S_2 = 85$ does not divide $\#\langle T_2\rangle = 5^6$.

(2.5)(Bassalygo) q=5, m≥2, e=2. If a perfect code exists, then theorem 1 (with H=G) and the sphere packing bound imply

$$\#(T_2/G) \geq 4,$$
$$m^2 + (m+1)^2 = 5^k \quad \text{(for some } k\in\mathbb{Z}).$$

It can be shown that this leads to a contradiction [1], so no perfect code with these parameters exists.

3. PROOFS.

The group ring. Let $\mathbb{C}[X]$ be the group ring of X over $\mathbb{C}$; so $\mathbb{C}[X]$ has, as a $\mathbb{C}$-vector space, a basis $\{e_x \mid x \in X\}$, and the multiplication is determined by $e_x . e_y = e_{x+y}$. For each $x \in X$ there is a ring homomorphism

$$\langle x,-\rangle : \mathbb{C}[X] \to \mathbb{C}$$
$$\langle x, \textstyle\sum_{y\in X} \lambda_y e_y\rangle = \sum_{y\in X} \lambda_y \langle x,y\rangle \quad (\lambda_y \in \mathbb{C})$$

and it is well known that the map

$$\mathbb{C}[X] \to \mathbb{C}^X$$
$$f \mapsto (\langle x,f\rangle)_{x\in X}$$

is an isomorphism of $\mathbb{C}$-algebras; here $\mathbb{C}^X$ is the product of $\#X$ copies of $\mathbb{C}$, with addition and multiplication performed componentwise.

For a subset D of X, we denote the element $\sum_{x\in D} e_x$ of $\mathbb{C}[X]$ by $\sum D$.

The group G acts on $\mathbb{C}[X]$ in a natural way as a group of algebra automorphisms, by permutation of the basis vectors e_x. We have $\langle\sigma x,\sigma f\rangle = \langle x,f\rangle$ for $x \in X$, $f \in \mathbb{C}[X]$, $\sigma \in G$.

For a subgroup $H \subset G$ we define $\mathbb{C}[X]^H = \{f \in \mathbb{C}[X] \mid \forall\sigma\in H\colon \sigma f = f\}$. Clearly, $\{\sum\bar{y} \mid \bar{y} \in X/H\}$ is a basis for $\mathbb{C}[X]^H$. Let $f \in \mathbb{C}[X]^H$. Then for $x \in X$ and $\sigma \in H$ we have $\langle\sigma x,f\rangle = \langle\sigma x,\sigma f\rangle = \langle x,f\rangle$, so $\langle x,f\rangle$ only depends on the H-orbit $\bar{x}$ of x. Hence for $f \in \mathbb{C}[X]^H$, $\bar{x} \in X/H$ we can define $\langle\bar{x},f\rangle = \langle x,f\rangle$, where $x \in \bar{x}$. This gives us a ring homomorphism

(3.1) $$\mathbb{C}[X]^H \to \mathbb{C}^{X/H}$$
$$f \mapsto (\langle\bar{x},f\rangle)_{\bar{x}\in X/H}$$

which is easily proved to be an isomorphism (e.g.: injectivity follows from injectivity of $\mathbb{C}[X] \to \mathbb{C}^X$, and surjectivity by comparison of dimensions).

Perfect codes. A subset $C \subset X$ is a perfect code of order e if and only if the relation

(3.2) $$(\textstyle\sum S_e)\cdot(\sum C) = \sum X$$

holds in $\mathbb{C}[X]$. From this we deduce:

(3.3) LEMMA. *Let* $x \in X$, $x \notin T_e$. *Then* $\langle x, \sum C\rangle = 0$ *for every perfect code* $C \subset X$ *of order* e.

PROOF. Applying the ring homomorphism $\langle x,-\rangle$ to (3.2) we find

$$\langle x, \textstyle\sum S_e\rangle \cdot \langle x, \sum C\rangle = \langle x, \sum X\rangle \quad \text{(in } \mathbb{C}\text{)}.$$

Because of $x \notin T_e$ we have $x \neq 0$ so

$$<x, \sum X> = \sum_{y \in X} <x,y> = 0$$

while further $x \notin T_e$ implies

$$<x, \sum S_e> = \sum_{s \in S_e} <x,s> \neq 0.$$

We conclude $<x, \sum C> = 0$, as required. □

Let $H \subset G$ be a subgroup, and for $f \in \mathbb{C}[X]$ define

$$t_H(f) = \sum_{\sigma \in H} \sigma(f).$$

Clearly, t_H is a linear map from $\mathbb{C}[X]$ to $\mathbb{C}[X]^H$. Generalizing (3.3) we have:

<u>(3.4) LEMMA</u>. *Let* $\bar{x} \in X/H$, $\bar{x} \notin T_e/H$. *Then* $<\bar{x}, t_H(\sum C)> = 0$ *for every perfect code* $C \subset X$ *of order* e.

<u>PROOF</u>. For $x \in \bar{x}$ we have

$$<\bar{x}, t_H(\sum C)> = <x, \sum_{\sigma \in H} \sigma(\sum C)> = \sum_{\sigma \in H} <\sigma^{-1}x, \sum C>$$

and by (3.3) we have $<\sigma^{-1}x, \sum C> = 0$ for each $\sigma \in H$. □

From the isomorphism (3.1) and lemma (3.4) we conclude:

(3.5). The $\mathbb{C}$-vector space spanned by $\{t_H(\sum C) \mid C \subset X$ is a perfect code of order $e\}$ has dimension at most $\#(T_e/H)$, for every subgroup $H \subset G$.

<u>PROOF OF THEOREM 1</u>. Suppose a perfect code $C \subset X$ of order e exists. Notice that such a C has exactly one element in common with S_e.

For every orbit $\bar{x} \in S_e/H$, one can find, by translation, a perfect code $C_{\bar{x}} \subset X$ of order e such that the unique element of $C_{\bar{x}} \cap S_e$ is contained in $\bar{x}$. Writing $t_H(\sum C_{\bar{x}})$ on the basis $\{\sum \bar{y} \mid \bar{y} \in X/H\}$ of $\mathbb{C}[X]^H$:

$$t_H(\sum C_{\bar{x}}) = \sum_{\bar{y} \in X/H} \lambda_{\bar{y}} \cdot (\sum \bar{y}), \quad (\lambda_{\bar{y}} \in \mathbb{C}),$$

we then find

$$\lambda_{\bar{y}} = 0 \quad \text{for } \bar{y} \in S_e/H,\ \bar{y} \neq \bar{x},$$

$$\lambda_{\bar{x}} > 0$$

(more precisely, $\lambda_{\bar{x}} = {}^{\#}H/{}^{\#}\bar{x}$). It follows that $\{t_H(\sum C_{\bar{x}}) \mid \bar{x} \in S_e/H\}$ spans a $\mathbb{C}$-vector space of dimension ${}^{\#}(S_e/H)$. Hence (3.5) implies ${}^{\#}(S_e/H) \leq {}^{\#}(T_e/H)$, as required. □

PROOF OF THEOREM 2. By the duality theory of finite abelian groups Y_e is a subgroup of X of index ${}^{\#}\langle T_e\rangle$. Let

$$V_e = \{f \in \mathbb{C}[X] \mid \langle x,f\rangle = 0 \text{ for all } x \in X,\ x \notin \langle T_e\rangle\}.$$

We claim

$$V_e = \{\textstyle\sum_{\bar{t} \in X/Y_e} \lambda_{\bar{t}}\cdot(\sum \bar{t}) \mid \lambda_{\bar{t}} \in \mathbb{C} \text{ for } \bar{t} \in X/Y_e\}.$$

In fact, the inclusion $\supset$ follows from a direct calculation, and equality follows by comparison of dimensions.

Let $C \subset X$ be a perfect code of order e. Then $\sum C \in V_e$ by lemma (3.3) and the definition of V_e, so our claim says

$$\textstyle\sum C = \sum_{\bar{t} \in X/Y_e} \lambda_{\bar{t}}\cdot(\sum \bar{t})$$

for certain complex numbers $\lambda_{\bar{t}}$. This exactly means that C is periodic modulo Y_e. In particular, ${}^{\#}Y_e$ divides ${}^{\#}C$, and since ${}^{\#}C.\ {}^{\#}S_e = {}^{\#}X$ it follows that ${}^{\#}S_e$ divides ${}^{\#}X/{}^{\#}Y_e = {}^{\#}\langle T_e\rangle$. □

PROOF OF THEOREM 3. We need only prove the "only if"-part. From theorem 1 we see ${}^{\#}T_e \geq {}^{\#}S_e > 1$ so there exists $x \in T_e$, $x \neq 0$. Hence

(3.6) $$\textstyle\sum_{s \in S_e} \langle x, s\rangle = 0$$

8

for some $x \in X$. Thus we have a sum of q q-th roots of unity which vanishes. Using the irreducibility of the polynomial $X^{q-1} + \ldots + X + 1$ over $\mathbb{Q}$ (since q is prime) one easily sees that (3.6) is equivalent to:

(3.7) for each $i \in \{0,1,\ldots,q-1\}$ there is a unique $s \in S_e$ with $<x,s> = \xi_q^i$.

Now let C be the kernel of the group homomorphism $X \to \{\xi_q^i \mid 0 \le i < q\}$ which sends y to $<x,y>$. Then (3.7) is equivalent to:

for each $y \in X$ there is a unique $s \in S_e$ with $y - s \in C$.

It follows that C is a perfect code of order e. □

More generally, one can prove, using theorems 1 and 2 and the methods of [2]:

<u>COROLLARY</u>. *Suppose* $\#S_e = p$ *is prime, and suppose that there exists at most one prime dividing* q *which is smaller than* p*. Then there exists a perfect code* $C \subset X$ *of order* e *if and only if there exists a subgroup* $C \subset X$ *whose underlying set is a perfect code of order* e*. Moreover, every perfect code* $C \subset X$ *of order* e *is periodic modulo* pX.

REFERENCES.

[1] BASSALYGO, L.A., *A necessary condition for the existence of perfect codes in the Lee metric*, Mat. Zametki <u>15</u> (1974), 313-320 (russian).

[2] MANN, H.B., *On linear relations between roots of unity*, Mathematika <u>12</u> (1965), 107-117.