stichting
mathematisch
centrum

MC

DEPARTMENT OF PURE MATHEMATICS

ZW 65/76 JANUARY

E. WATTEL

A NOTE ON PERFECT MIXED LEE CODES AND FINITE ABELIAN GROUPS

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

A note on perfect mixed Lee codes and finite abelian groups

by

E. Wattel

ABSTRACT

In this paper it is shown that there exists a one-to-one mapping between the class of finite abelian groups and the perfect single error correcting mixed Lee codes. This mapping is a functorial isomorphism on the skeletons of the categories.

KEY WORDS & PHRASES: *Lee codes, perfect codes*

1. INTRODUCTION

The main purpose of this paper is to show that there exists a decent one-to-one mapping from the class of finite abelian groups into the collection of single error correcting mixed Lee codes.

The crucial point in the proof is that the elements of a word space of a single error correcting group code can be partitioned into cosets with respect to the code. These cosets constitute a finite abelian group, which is called the *error pattern group*.

Among the codes with the same error pattern group there exists a minimal one which will be called a *primitive* code. The primitive code of a given error pattern group can be constructed directly from the group, and primitive group codes can be directly recognized by a simple internal characterization.

The ideas of error patterns and primitive codes apply to other types of codes, but correspondences which are as simple as the one described here are rare.

2. BASIC NOTIONS

2.1. DEFINITIONS. The finite abelian group $\mathbb{Z}_a$ of integers modulo a with the usual cyclic distance function is called the *Lee alphabet* A with a elements. Elements of an alphabet are also called *letters*.

Since all groups under observation are abelian we denote unit elements by 0 (or 0^* etc.) and group operations by additions (and subtractions). Repeated addition of a fixed element of a group is denoted by multiplication by an integer.

A *word space* W is a finite direct product of (not necessarily isomorphic) alphabets $\{A_i \mid i = 1,2,\ldots,n\}$. If $W = \Pi_{i=1}^{n} A_i$, then n is called the *word length* and members of W are called words. Word spaces W will be supplied with the *Lee distance function* ρ defined as follows: if

$$x = (x_i)_{i=1}^{n} \quad \text{and} \quad y = (y_i)_{i=1}^{n}, \qquad x \in W, \quad y \in W,$$

then

$$\rho(x,y) = \sum_{i=1}^{n} \rho_i(x_i,y_i),$$

in which ρ_i refers to the distance function in A_i. So, the distance between two words in W equals the sum of the distances between the corresponding letters.

A *code* C in W is a subgroup of W; the members of C are called *code words*. A code in a word space with Lee distance function is called a *Lee code*. If the factors A_i are not all isomorphic, then the code is called *mixed*.

2.2. CONVENTIONS. We will use the following notational conventions: $\mathbb{N}$ is the set of natural numbers; $\mathbb{Z}_a$ is the group of integers modulo a; δ_{ij} is the Kronecker symbol: $\delta_{ij} = 0$ iff $i \neq j$, $\delta_{ij} = 1$ iff $i = j$. Elements of the word space with all coordinates zero except for the j^{th}, which is 1, will be denoted by d_j:

$$d_j = (\delta_{ji})_{i=1}^{n} \in W.$$

Also,

$$D = \{d_j \mid j = 1,2,\ldots,n\};$$

D is a set of generators of W.

The minimal subgroup of a group which contains a given set A will be called the *hull* of A, and will be denoted by $H(A)$.

For $e \in \mathbb{N}$ and $w \in W$ we define the e-*sphere at* w by:

$$S_e(w) = \{x \mid x \in W \ \& \ \rho(w,x) \leq e\}.$$

2.3. DEFINITIONS. If the e-spheres at code words of C are pairwise disjoint, but the e + 1 spheres are not, then C is said to be an e-*error correcting* code in W.

An e-error correcting code C is *perfect* whenever the e-spheres at the code words are pairwise disjoint and cover the space W.

2.4. DEFINITIONS. The *error-pattern group* of a code C is the group W/C supplied with a distance function ρ' defined as follows: if g_1, g_2 are cosets in W with respect to C, then

$$\rho'(g_1,g_2) = \min\{\rho(x,y) \mid x \in g_1;\ y \in g_2\}.$$

A code is called *primitive* when it contains no code words with precisely one letter different from 0 (i.e. $C \cap \{md \mid m \in N;\ d \in D\} \equiv \{0\}$).

2.5. DEFINITIONS. If (W,C,ρ) and (W^*,C^*,ρ^*) are Lee codes, and if $h: W \to W^*$ is a group homomorphism such that $h: C \to C^*$ and

$$\rho(x,y) \geq \rho^*(h(x), h(y)) \qquad \text{for all } x \text{ and } y \text{ in } W,$$

then h is called a *code homomorphism* from (W,C,ρ) *into* (W^*,C^*,ρ^*).

If $\rho(x,y) = \rho^*(h(x), h(y))$ for all $x,y \in W$, then the function h is clearly one-to-one and we have a *code isomorphism* of (W,C,ρ) into (W^*,C^*,ρ^*).

If, moreover, $W^* = h[W]$, then we have a homomorphism (resp. isomorphism) h of (W,C,ρ) *onto* (W^*,C^*,ρ^*).

This is intended to provide the injections, surjections, bijections and objections for the category-theory practitioners.

Note that for all $d_j \in D$ and for all code homomorphisms h we have that $h(d_j)$ is either $\pm d_k^* \in D^*$ or $0^* \in W^*$. If, in particular, h defines a one-to-one correspondence between D and D^* and $h^{-1}(0^*) \subset C$, then we say that (W,C,ρ) is a *compound multiple* of (W^*,C^*,ρ^*).

In the following proposition we will show that every mixed Lee code is a compound multiple of a primitive code.

2.6. PROPOSITION. *Every (mixed) Lee group code can be mapped homomorphically onto a primitive Lee code with an isomorphic error pattern group. Moreover, every mixed Lee code is determined by its primitive code and its collection of code words with one letter different from* 0.

PROOF.

(1) Let $H = H(C \cap \{md \mid m \in \mathbb{N};\ d \in D\})$ (this is the hull of all the code words with one letter different from 0). From the isomorphism theorems we find that

$$W/C \cong (W/H)/(C/H),$$

since H is clearly a subgroup of C. Also the distances ρ' in W/C and ρ'' in (W/H)/(C/H) are clearly isomorphic.

Next we show that W/H is a direct product of Lee alphabets. Define for every j:

$$H_j = C \cap \{md_j \mid m \in \mathbb{N}\}.$$

Now $\Pi_{j=1}^{n} H_j = H$, and A_j/H_j is again a cyclic group. A_j is cyclic for every alphabet A_j, and has the cyclic distance function. Therefore

$$W/H = \prod_{j=1}^{n} A_j/H_j,$$

and C/H is a code in this word space which is clearly primitive.

(2) Conversely, let (W,C,ρ) be primitive, and let $W = \Pi_{i=1}^{n} A_i$ with A_i a cyclic group of order a(i). Then we can construct $A_i^* = \mathbb{Z}_{a(i)m(i)}$ for $m(i) \in \mathbb{N}$; $W^* = \Pi_{i=1}^{n} A_i^*$ and

$$C^* = H\Big(C \cup \{a(i)d_i^* \mid d_i^* \in D^* \subset W^*\}\Big).$$

In this way we can obtain any compound multiple of (W,C,ρ). The subgroup H of part (1) can now be found as: $H(\{a(i)d_i^* \mid d_i^* \in D^*\})$. □

We can obtain isomorphic images of codes by reordering and reflecting some of the alphabets on the word space.

It is not hard to see from the definitions 2.5 that in this way all possible isomorphisms are obtained.

3. PRIMITIVE PERFECT SINGLE ERROR CORRECTING CODES

The simplest type of error pattern group which is possible is a finite abelian group with the trivial distance function: $\rho(\alpha,\beta) = 1$ iff $\alpha \neq \beta$ and $\rho(\alpha,\alpha) = 0$. We show that for each finite abelian group with this distance function there is a primitive perfect single error correcting code which is unique up to isomorphism.

3.1. DEFINITION. A *half set* S of a group G is a subset of G with the following two properties:
(i) for every $x \in G$, $x \neq 0$, either $x \in S$ or $-x \in S$, but not both;
(ii) $0 \notin S$; every order 2 element of G is in S.

3.2. THEOREM. *Every finite abelian group with trivial distance function is the error pattern group of a primitive perfect single error correcting mixed Lee code, and every perfect single error correcting primitive mixed Lee code has an error pattern group which is finite abelian with trivial distance function. Moreover, this correspondence is unique up to isomorphism.*

PROOF.
a) Let (W,C,ρ) be a perfect single error correcting mixed Lee code. Then W/C is an abelian group. Let α and β be two different cosets; then

$$\rho'(\alpha,\beta) = \min_{W} \{\rho(C,W) \mid W \in \alpha - \beta\}.$$

Since C is perfect single error correcting this minimum is 0 iff $\alpha - \beta = C$, and 1 otherwise. Therefore, every code of this type has a well-defined error pattern group with trivial distance function.

b) Let G be a finite abelian group. Let $S = \{\alpha_i\}_{i=1}^{n}$ be any half set of G. Then

$$n = \#(S) = \tfrac{1}{2}\left[\#(G) + (\#\{x \in G \mid 2x = 0'\})\right] - 1.$$

In this way we have indexed the half set. Assume that the order of α_i in G is a(i) for $1 \le i \le n$.
To each α_i in S we assign a Lee alphabet $A_i \cong \mathbb{Z}_{a(i)}$ and we construct a word space by

$$W = \prod_{i=1}^{n} A_i.$$

Thus, $x \in W \Leftrightarrow x = (x_i)_{i=1}^{n}$ with $x_i \in \mathbb{Z}_{a(i)}$ for i=1,2,...,n. There exists an evaluation mapping from W into G:

$$f: W \to G,$$
$$f(x) = \sum_{i=1}^{n} x_i \alpha_i.$$

(Compare with definitions 2.1. The x_i can be considered to be integers). The mapping f is a group homomorphism if W is considered to be a direct product of the abelian groups A_i.
If we put $C = f^{-1}(0')$, then $G \cong W/C$, and we claim that C is a primitive perfect single error correcting code in W.
Firstly we prove primitivity. Suppose that $(x_i)_{i=1}^{n} = m.d_j \in C$ for m integer and $d_j \in D$. Then $\Sigma_{i=1}^{n} x_i \alpha_i = m.\alpha_j = 0' \in G$. Therefore, a(j) divides m, i.e., $m \equiv 0 \bmod a(j)$, and $m.d_j = 0 \in W$.
Next we prove that the unit spheres at code words form a partition of W. Observe that

$$S_1(0) = \{0\} \cup \{\pm d_j \mid d_j \in D\},$$
$$f(0) = 0', \quad f(d_j) = \alpha_j \text{ and } f(-d_j) = -\alpha_j.$$

We conclude that f: $S_1(0) \to G$ is one-to-one and onto. Therefore $S_1(0)$ is a complete system of representatives of the cosets in W with respect to C. We conclude that $\{S_1(c) \mid c \in C\}$ covers the word space W.
In order to prove that C is one error correcting we show that no member of W can be in two different unit spheres at code words. Suppose that $x \in S_1(c')$ and $x \in S_1(c'')$. Then

$$\rho(c',c'') \leq \rho(x,c') + \rho(x,c'') \leq 2.$$

Define $c = c' - c''$. Then $c \in C$ with $\rho(c,0) \leq 2$ and we have already seen that $c \neq md_j$ for any $m \in \mathbb{Z}$ and $d_j \in D$. Therefore c has to be of the form: $\pm d_i \pm d_j$. This means that $\pm \alpha_i \pm \alpha_j = 0' \in G$; thus $\alpha_i = \pm \alpha_j$, but now α_i and α_j cannot be different members of S. This gives a contradiction. So the unit spheres at code words indeed form a partition of W, and so C is both perfect and single error correcting.

c) In order to show that the above construction is unique up to isomorphism, we observe that the half set S is determined completely by $D \subset W$, and the indexing of S corresponds to the arrangment of the coordinates of W. One-to-one correspondences between two half sets which map each element onto an element of the same order can be extended to code isomorphisms between the corresponding codes. □

3.3. PROPOSITION. *If we have a homomorphism* h *between two single error correcting perfect codes, then the induced mapping* $\tilde{h}$ *between the error patterns of the codes is a group homomorphism.*

PROOF. This is just a reformulation of a well-known fact in group theory. □

3.4. PROPOSITION. *If* G *and* G^* *are finite abelian groups and* $\tilde{h}$ *is a homomorphism from* G *into* G^*, *then there exist two codes* (W,C,ρ) *and* (W^*,C^*,ρ^*) *which are primitive and perfect single error correcting, whose error-pattern groups are precisely* G *and* G^*, *and which admit a code homomorphism* h *from* (W,C,ρ) *into* (W^*,C^*,ρ^*) *such that* $\tilde{h}$ *is the induced mapping between their error-pattern groups.*

PROOF. Let S^* be a half set in G^*. Then for all $g \in G$

$$\#(\tilde{h}^{-1}(S^* \cup \{0^*\}) \cap \{g,-g\}) \geq 1,$$

and thus $\tilde{h}^{-1}(S^* \cup \{0^*\})$ can be restricted to a half set S of G.

Obviously, $\tilde{h}(S \setminus \tilde{h}^{-1}(S^*)) = 0^{*\prime} \in G^*$.

Now we construct the codes (W,C,ρ) and (W^*,C^*,ρ^*) from G (resp. G^*) and S (resp. S^*) in the same way as in the proof of Theorem 3.2.

C (resp. C^*) is the kernel of a homomorphism f (resp. f^*) from W (resp. W^*) onto G (resp. G^*).

We construct $h: W \to W^*$ in the following way: As in the proof of 3.2, $f: D \to S$ and $f^*: D^* \to S^*$ are one-to-one and onto. Therefore the mapping $\tilde{h}: S \to S^* \cup \{0^*\}$ induces a mapping $h: D \to (D^* \cup \{0^*\}) \subset W^*$, defined by $h(d_j) = f^{-1}\tilde{h}f(d_j) \cap D^*$ if it exists, and 0^* otherwise.

Since D is a set of generators of W, the mapping h(D) can be extended homomorphically to W. Clearly $\tilde{h}$ is the induced mapping of h on W, since this is already the case on the generators D. Therefore, also, $C = f^{-1}(0') \subset W$ is mapped homomorphically into $C^* = f^{*-1}(0^{*\prime}) \subset W^*$, and since h is nonexpanding on the generators of W it is clear that

$$\rho^*(h(w), h(\tilde{w})) \leq \rho(w,\tilde{w}) \qquad \text{for } w,\tilde{w} \in W.$$

Our conclusion is that we have a code homomorphism between (W,C,ρ) and (W^*,C^*,ρ^*).

The proof and the construction of this proposition is closely related to the five-lemma in category theory (cf. [5]):

$$\begin{array}{ccccccccc} 0 & \hookrightarrow & C & \hookrightarrow & W & \overset{f}{\twoheadrightarrow} & G & \to & 0' \\ & & \downarrow h & & \downarrow h & & \downarrow \tilde{h} & & \\ 0^* & \hookrightarrow & C^* & \hookrightarrow & W^* & \overset{f^*}{\to} & G^* & \to & 0^{*\prime}. \end{array} \quad \square$$

3.5. CONCLUSIONS. If we consider the skeletons of the category of finite abelian groups and the category of primitive perfect single error correcting mixed Lee codes, then they turn out to be isomorphic. Theorem 3.2 and Propositions 3.3 and 3.4 describe the functors which establish the

isomorphism.

In practice this means that constructions like products and quotients, which are possible in finite abelian groups, can be copied and translated into terms of perfect single error correcting mixed Lee codes.

4. REFERENCES.

[1] HALL Jr., M., *The Theory of Groups* (McMillan, New York, 1959).

[2] LEE, C.Y., *Some properties of non-binary error correcting codes*, IRE Transactions IT(4) (1958) 77-82.

[3] PETERSEN, W.W., *Error correcting codes*, M.I.T. (1961).

[4] POST, K.A., *Nonexistence theorems on perfect Lee codes over large alphabets*, Information & Control 29-4 (1975) 369-380.

[5] HERRLICH, H. & G.E. STRECKER, *Category Theory* (Allyn and Bacon, Boston, Mass., 1973).