Code over groups with arbitrary metrics

TECHNISCHE HOGESCHOOL EINDHOVEN
NEDERLAND
ONDERAFDELING DER WISKUNDE

EINDHOVEN UNIVERSITY OF TECHNOLOGY
THE NETHERLANDS
DEPARTMENT OF MATHEMATICS

Code over groups with arbitrary metrics

by

A. Bos

T.H. - Report 80-WSK-06

July 1980

Code over groups with arbitrary metrics

by

A.Bos

Abstract

A description is given of a method that produces codes over an abelian group with an arbitrary metric. For groups with the Hamming metric the method is known [6], but this paper gives a more general presentation, which makes the construction easier to understand.

0. Introduction

If A is a finite set, a subset of A^n is called a code over the alphabet A of length n. The Hamming distance between two elements x and y of A^n is the number of coordinates in which x and y differ. In case $0 \in A$ the weight w(x) of an element $x \in A^n$ is the number of non-zero coordinates of x.

If $A = \{0,1\}$ a code over A is called a binary code. If A is a finite field and C is a linear subspace of A^n, then C is a linear code. An (n,k,d)-code is a linear code of length n, dimension k and minimum distance d.

Let there be given a binary linear code C with parameters n, k and d and a (N,K,D)-code Γ over the field of 2^k elements. Let $\underline{a} = (a_1,\ldots,a_N)$, $a_i \in GF(2^k)$ be a typical code word of Γ. There exists a linear bijection between the elements of $GF(2^k)$ and the code words of C. Replacing each coordinate of codeword $\underline{a}$ by the corresponding binary n-tuple, we obtain a binary vector of length nN. The code obtained in this way has parameters nN, kK and dD and is called a concatenated code [5, Ch 10, § 11].

A generalization of this idea is given by Zinov'ev [6].
In this paper we give a further generalization generating codes over groups with arbitrary metrics.

In the first section we give the definitions needed, starting from scratch. In section two the main theorem is stated. The third section contains examples in the Hamming , the Lee and the Euclidean metric. In the last section some remarks are made.

1. Some definitions and properties

Let G be an additive group, finite or infinite, with a *metric* d, that is, a mapping $d : G \times G \to \mathbb{R}$ such that for all $a,b,c \in G$:
i) $d(a,b) \geq 0$; ii) $d(a,b) = 0$ iff $a = b$; iii) $d(a,b) = d(b,a)$ and
iv) $d(a,b) + d(b,c) \geq d(a,c)$.
A metric is called *translation invariant* if for all $x,a,b \in G$
$d(a+x, b+x) = d(a,b)$.

A *weight function* is a mapping $w : G \to \mathbb{R}$ such that for all $a,b \in G$: i) $w(a) \geq 0$; ii) $w(a) = 0$ iff $a = 0$; iii) $w(a) = w(-a)$ and
iv) $w(a) + w(b) \geq w(a+b)$.
Clearly, any weight function determines a translation invariant metric and vice versa by $d(a,b) = w(b-a)$ for all $a,b \in G$.
From now on all metrics under consideration are translation invariant.
As examples we mention only the Euclidean metric on $\mathbb{R}^n$, the Hamming or trivial metric on an arbitrary group and the Lee metric on $\mathbb{Z}/m\mathbb{Z}$.
The last one is defined by $d_L(a,b) := \min((a-b) \bmod m, (b-a) \bmod m)$ for $a,b \in \mathbb{Z}/m\mathbb{Z}$.
Let V be a finitely generated free module over G. Each element of V can be represented uniquely by m "coordinates" $g_1,\ldots,g_m \in G$. A metric and a weight function on V, also denoted by d and w respectively, are defined in terms of the metric on G by

$$d((g_1,\ldots,g_m), (h_1,\ldots,h_m)) := \sum_{i=1}^{m} d(g_i,h_i) \text{ and}$$

$$w((g_1,\ldots,g_m)) := \sum_{i=1}^{m} w(g_i).$$

A *code* C of length m over G is a subset of V with $0 \in C$ and

$d_C := \inf_{\substack{x \neq y \\ x,y \in C}} d(x,y)$, the *minimum distance*.

The minimum distance of the code $\{0\}$ is ∞ by definition.
A code is called a *linear* code if it is a submodule of V.
The *dimension* of a linear code is the number of generators of the code. For a linear code we have $d_C = \inf_{0 \neq x \in C} w(x)$.

For a subset $W \subset V$ and $a \in V$ we define

$$d(a,W) := \inf_{x \in W} d(a,x).$$

Let μ be a measure on V such that for $W \subseteq V$ with $|W| < \infty$
$\mu(W) = |W|$.
The *centerdensity* δ_C of a code C is defined by

$$\delta := \lim_{r \to \infty} \frac{\mu(B(0,r) \cap C)}{\mu(B(0,r))},$$

where B(0,r) is the open ball with radius r and center 0.

Note that for finite G and $C \subseteq G^m$, $\delta_C = \frac{|C|}{|G|^m}$.

The *density* Δ of a code C with minimum distance d_C is defined by $\Delta := \delta_C . \mu\,(B(0, \frac{d}{2}))$.

So for every code we have the *sphere packing condition* $\Delta \leq 1$.
A code is called *perfect* if equality is attained.

Lemma 1 : If G is finite and $C \subseteq V$ is a perfect code, then for all $x \in V$ we have $d(x,C) \leq \frac{1}{2} d_C$.

Proof : Since $\delta_C = |C| / |G|^m$, we must have the equality $|C| . |B(0, \frac{1}{2} d_C)| = |G|^m$, thus for all $x \in V$ $d(x,C) \leq \frac{1}{2} d_C$. □

Lemma 2 : Let C be a linear code in V. If $y \equiv x \pmod{C}$ then $d(y,C) \leq d(x,C)$.

Proof : $d(y,C) = \inf_{a \in C} d(y,a) = \inf_{a \in C} d(x+c,a) = \inf_{a \in C} d(x,a-c) =$

$= \inf_{b \in C} d(x,b) = d(x,C)$, where $y = x+c$ and $b = a-c$, $c \in C$. □

Corollary 3 : If C is a linear code in V, we can define a metric on $\overline{V} := V/C$ by $w(\overline{a}) := d(a,C)$ where $\overline{a} := a+C$.

3. Constructions of new codes

Theorem 4 : Let $C_1 \subseteq C_2$ be linear codes in V, $\overline{C}_2 := C_2/C_1$ and $\phi : \overline{C}_2 \to C_2$ be an injective homomorfism with $\phi\overline{\alpha} \in \overline{\alpha}$ for $\alpha \in C_2$;

Γ be a code of length n over $\overline{C}_2$ with minimum distance ε.

Then $B := \bigcup_{x \in \Gamma} (\phi^n x + C_1^n)$ is a code over G of length nm and with minimum distance $D = \min(\varepsilon, d_{C_1})$.

If $\overline{C}_2$ is finite, then $\delta_B = |\Gamma|(\delta_{C_1})^n$.

Proof : Notice that $d(\phi\overline{\alpha}, C_1) = w(\overline{\alpha})$ for $\alpha \in C_2$, since $\phi\overline{\alpha} \in \overline{\alpha}$.

Let $x_1, x_2 \in \Gamma$ be such that $x_1 - x_2 = (\overline{\alpha}_1, \ldots\ldots, \overline{\alpha}_n) \neq 0$ with $\overline{\alpha}_i \in \overline{C}_2$.

Then $d(x_1,x_2) = \sum_{i=1}^{n} w(\overline{\alpha}_i) \geq \varepsilon$.

Now we have

$$d(\phi^n x_1 + C_1^n, \phi^n x_2 + C_1^n) = d(\phi^n(x_1-x_2), C_1^n) =$$

$$= \sum_{i=1}^{n} d(\phi_i\overline{\alpha}_i, C_1) = \sum_{i=1}^{n} w(\overline{\alpha}_i) \geq \varepsilon .$$

Since $\delta_{C_1^n} = (\delta_{C_1})^n$ we get $\delta_B = |\Gamma|.(\delta_{C_1})^n$. □

Theorem 5 (Main theorem): Given a tower of linear codes C_i $(i=0,1,\ldots,k)$ of length m with minimum distance d_i, that is

$C_0 \subseteq C_1 \subseteq \ldots\ldots \subseteq C_k$, and injective homomorfisms $\phi_i : \overline{C}_i \to C_i$

such that $\phi_i \overline{\alpha}_i \in \overline{\alpha}_i$ for $\alpha_i \in C_i$, where $\overline{C}_i := C_i/C_{i-1}$ $(i=1,\ldots,k)$.

Further for each $i=1,\ldots,k$ a code Γ_i of length n over $\overline{C}_i$ and minimum distance ε_i is given. Then the new code

$$:= \bigcup_{(x_1,\ldots,x_k)\in \Gamma_1\times\ldots\times\Gamma_k} \left(\sum_{i=1}^{k} \phi_i^n x_i + C_0^n \right)$$

over G of length nm has minimum distance $D = \min(d_0, \varepsilon_1 \ldots, \varepsilon_k)$.

If for all $i=1,\ldots,k$ Γ_i is a linear code, then so is $\mathcal{B}$.

If for all $i=1,\ldots,k$ $\overline{C}_i$ is finite, then $\delta_{\mathcal{B}} = (\delta_{C_0})^n \prod_{i=1}^{k} |\Gamma_i|$.

Proof : Notice that if $\beta_i \in C_i$ for $i=r,r+1,\ldots,s$ then

$$d\Big(\sum_{i=r}^{s} \beta_i,\ C_{r-1}\Big) \geq d(\beta_s,\ C_{s-1}) \text{ since}$$

$$d(\beta_r + \beta_{r+1} + \ldots + \beta_s, C_{r-1}) = d(\beta_s, C_{r-1} - \beta_r - \beta_{r+1} - \ldots - \beta_{s-1}) \geq d(\beta_s, C_{s-1}).$$

For $i=1,\ldots,k$ let $x_i, y_i \in \Gamma_i$ such that $x_i - y_i = (\overline{\alpha}_{i1}, \ldots, \overline{\alpha}_{in})$

with $\overline{\alpha}_{ij} \in \overline{C}_i$. If we suppose that $x_i = y_i$ for $i=j+1,\ldots,k$

and $x_j \neq y_j$ $(j \geq 1)$ then

$$d\Big(\sum_{i=1}^{k} \phi_i(x_i - y_i),\ C_0^n\Big) = d\Big(\sum_{i=1}^{j} \phi_i(x_i - y_i),\ C_0^n\Big).$$

Furthermore

$$d\Big(\sum_{i=1}^{j} \phi_i(x_i - y_i), C_0^n\Big) = \sum_{r=1}^{n} d\Big(\sum_{i=1}^{j} \phi_i \overline{\alpha}_{ir}, C_0\Big) \geq \sum_{r=1}^{n} d(\phi_j \overline{\alpha}_{jr}, C_{j-1}) =$$

$$= \sum_{r=1}^{n} w(\overline{\alpha}_{jr}) \geq \varepsilon_j .$$

The second statement is obvious.

Since $\delta_{C_0^n} = (\delta_{C_0})^n$ we obtain $\delta_B = (\delta_{C_0})^n \prod_{i=1}^{k} |\Gamma_i|$ if all $|C_i| < \infty$.□

4. Examples

i) $G = \{0,1\}$ with the Hamming metric, $V = G^8$. Given the tower of codes $C_0 = (8,2^4,4) \subset C_1 = (8,2^7,2) \subset C_2 = (8,2^8,1)$.

Then $\overline{C}_1 \simeq G^3$ with twice the Hamming metric and $\overline{C}_2 \simeq G$.

Using $\Gamma_1 = (4,8^3,4)$ and $\Gamma_2 = (4,2^1,4)$ the optimal linear code $B = (32,2^{26},4)$ over G is obtained.

For more examples producing codes over GF(2) with the Hamming metric, see Zinov'ev [6].

ii) $G = \mathbb{R} = V$ with the Euclidean metric. Given the tower of codes

$C_0 = \mathbb{Z} \subset C_1 = \frac{1}{2}\mathbb{Z} \subset C_2 = \frac{1}{4}\mathbb{Z}$,

then $\overline{C}_1 \simeq \overline{C}_2 \simeq \{0,1\}$ with $\frac{1}{2}$ and $\frac{1}{4}$ times the Hamming metric respectively.

The codes $\Gamma_1 = (16,2^{11},4)$ and $\Gamma_2 = (16,2^1,1)$ produce a sphere packing in $\mathbb{R}^{16}$ with highest known center-density $\delta_B = 2^{-4}$.

For more examples of sphere packings constructed in this way, see Bos [2] .

iii) Let $m \geq 2$ and $G = \mathbb{Z}/2^m\mathbb{Z} = V$ with the Lee metric. The codes

$C_0 = (1,2^0,\infty) \subset C_2 = (1,2^1,2^{m-1}) \subset \ldots \subset C_i = (1,2^{m-i},2^i) \subset \ldots \subset C_m = (1,2^m,1)$

form a tower with $\overline{C}_i \simeq \{0,1\}$ with 2^i times the Hamming metric.

The binary i-th order RM-codes $\Gamma_i = (2^m, 2^{K_i}, 2^{m-i})$ with

$K_i = \sum_{j=1}^{i} \binom{m}{j}$ for i=1,2,.....,m produce the Lee code over $\mathbb{Z}/2^m\mathbb{Z}$

$B = (2^m, 2^K, 2^m)$ with $K = 2^m(\frac{m}{2} + 1)$.

This improves the (N,N^2,N) Lee codes over $\mathbb{Z}/N\mathbb{Z}$ in [4] for $N = 2^m$.

5. REMARKS

i) If d_1 and d_2 are two metrics on the group G such that for all $x,y \in G$ $d_1(x,y) \leq d_2(x,y)$, we say d_2 is a *stronger* metric than d_1.
If a code C has minimum distance d with respect to metric d_1, and minimum distance d' with respect to a stronger metric d_2, then one has $d' \geq d$. Since it is sometimes easier to find the minimum distance of codes for weaker metrics, this method can be used to give a lower bound for the minimum distance of codes for stronger metrics.
E.g. the Lee-metric on $\mathbb{Z}/m\mathbb{Z}$ is stronger than the Hamming metric on $\mathbb{Z}/m\mathbb{Z}$. So every Hamming-code over $\mathbb{Z}/m\mathbb{Z}$ is also a Lee-code over $\mathbb{Z}/m\mathbb{Z}$ although the estimate for the minimum distance can be rather poor.

ii) Theorem 4 and 5 can also be applied to codes (in a tower) of which one is the union of cosets of the other, without them being linear.
E.g. Zinov'ev [6] uses the tower of codes

$C_1 = (16,2^1,16) \subseteq C_2 = (16,2^5,8) \subseteq C_3 = (16,2^8,6) \subseteq C_4 = (16,2^{11},4)$,

to construct binary codes with minimum distance 24 and 30, although C_3 is the nonlinear extended Nordström-Robinson code.
The new codes are of course nonlinear.
To produce a good code one must try to find towers of codes that cannot be refined further and with metrics on the factor groups over which good codes exist.

iii) Given the binary codes $C_0 = (2,1,d) \subset C_1 = (2,2^2,1)$ with $d > 2$. Then $\overline{C}_1 \simeq \mathbb{Z}/4\mathbb{Z}$ with the Lee metric. So a code $\Gamma = (n,M,d)$ over $\overline{C}_1$ produces a $(2n,M,d)$-code over $\{0,1\}$. This is the inverse of a construction noticed by Lee [3]. He remarks that a binary $(2n,M,d)$-code produces an (n,M,d)-code over $\mathbb{Z}/4\mathbb{Z}$ with the Lee-metric by substituting 00 by 0, 01 by 1, 10 by 3 and 11 by 2.

iv) Following Blokh and Zyablov [1] it seems to me that for the codes constructed by theorem 4 and 5, cascade codes is a better name than concatenated codes.

REFERENCES

[1] E.L.Blokh & V.Y.Zyablov, "Coding of generalized cascade codes", Problemy Peredachi Inform., 10(1974), 45-50.

[2] A.Bos, "Spherepackings in high-dimensional space", (preprint).

[3] C.Y.Lee, "Some properties of non-binary error-correcting-codes", IRE Trans. Inf. Theory, IT-4 (1958), 77-82.

[4] Ch.Satyanarayana, "Lee metric codes over integer residue rings", IEEE IT-25 (1979), 250-254.

[5] F.J.MacWilliams & N.J.A.Sloane, "The theory of error-correcting codes", North-Holland, Amsterdam 1977.

[6] V.A.Zinov'ev, "Generalized concatenated codes", Problemi Peredachi Inform., 12 (1976), 5-15.