Perfect codes and group partitions

P.G. Bonneau

INRIA

CENTRE DE ROCQUENCOURT

Institut National
de Recherche
en Informatique
et en Automatique

Domaine de Voluceau
Rocquencourt
BP 105
78153 Le Chesnay Cedex
France

Tél. : (1) 39 63 55 11

Rapports de Recherche

N° 481

PERFECT CODES AND GROUP PARTITIONS

Pierre G. BONNEAU

Janvier 1986

PERFECT CODES AND

GROUP PARTITIONS

Pierre G. BONNEAU

INRIA - Rocquencourt
Domaine de Voluceau
B.P. N° 105
78153 - LE CHESNAY Cedex

FRANCE

PERFECT CODES AND GROUP PARTITIONS

Mailing Address : Pierre BONNEAU
INRIA Rocquencourt
Domaine de Voluceau
BP N° 105
78153 - LE CHESNAY Cedex
FRANCE

Summary : This paper deals with single error correcting perfect group codes, called GL codes. They are studied by mean of partitions of finite abelian groups. I generalize a result of B. Lindström who proved that some of these codes are not equivalent to Hamming ones. I prove that two GL codes are equivalent if and only if their associated partitions are isomorphic. In particular, non desarguesian partitions yield genuinely non linear GL codes. I use an alteration technique to construct such partitions, and thus I prove that whenever q is a prime power but not a prime, and m is an integer, $m \geq 3$, there exists a genuinely non linear GL code of length $\frac{q^m-1}{q-1}$ over an alphabet of size q.

Résumé : Cet article traite de codes parfaits en groupe correcteurs d'une erreur que nous appelons GL codes. Ils sont étudiés au moyen de partitions de groupes abeliens finis. Nous généralisons un résultat de B. Linström qui a prouvé que certains de ces codes n'étaient pas équivalents à des codes de Hamming. Nous prouvons que deux GL codes sont équivalents si et seulement si leurs partitions associées sont isomorphes. En particulier, des partitions non arguésiennes donnent lieu à des GL codes authentiquement non linéaires. Nous utilisons une technique d'altération pour construire de telles partitions, et prouvons ainsi que pour toute puissance première q qui n'est pas un nombre premier et pour tout entier $m \geq 3$, il existe un GL code authentiquement non linéaire dont la longueur est $\frac{q^m-1}{q-1}$ et la taille de l'alphabet q.

I - INTRODUCTION

This paper is devoted to perfect codes : given a finite set F and two positive integers n and e, a perfect e error correcting code in F^n is a subset C of F^n with the property that the "spheres" of radius e around the codewords (elements of C) are disjoint and fill F^n. The distance is the Hamming one, ie d(x,y) is the number of indices (positions) where the elements (words) $x,y \in F^n$ differ. The sphere of radius e around a word x is the set of y with $d(x,y) \leq e$. To avoid trivialities, I shall assume that $2e + 1 < n$ throughout the following discussion. This is also why I suppose $q \geq 2$, where q stands for the size of the alphabet F.

Let me give a short account on the existence problem. Van Lint's survey [6] is more detailed. For which parameters -I mean n, e and q - do there exist a perfect code ?

When e = 1 and q is a prime power, this problem is now completely solved. One must have $n = \frac{q^m-1}{q-1}$ for an integer $m \geq 2$. And when these conditions are fullfilled , there exists a Hamming code. These perfect codes were first constructed by Golay when q is a prime. Working in a slightly different setting, Zaremba [10] settled the general case. When q is not a prime power, only two facts are known : the obvious condition $1 + n(q-1)$ divides q^n must hold and there is no perfect code with parameters q = 6, n = 7, e = 1(see [9]).

When $e \geq 2$, only two perfect codes are known : the famous Golay ones ([8] chap. 20). The difficult Tietavaïnen and Van Lint theorem states that when q is a prime power, a perfect code must have the parameters of one of these codes. Recent work leads to the conjecture that the restriction on q can be removed.

In this paper, the existence problem will never be investigated. I confine attention to parameters for which a perfect code C is known to exist. Do there exist others ? A naïve answer is yes, because one can simply take the image of C by a map $F^n \longrightarrow F^n$ which preserves the distance.

Two codes that are image of each other by an isometry are called isometric or equivalent. I shall use basically "isometric" because "equivalent" has also been given a different meaning. It is known that each Golay code is "unique", that is every perfect code with the same parameters is equivalent to it. Thus, I restrict to the case when $e = 1$. Recall that q is a prime power, and $n = \frac{q^m-1}{q-1}$ for an integer $m \geq 2$. The Hamming codes are unique when $q = 2$, $m = 2,3$ and $q = 3$, $m = 2$. They are not unique for $q = 2$ and any $m \geq 4$. I refer you to [5] for the early history. This paper by B. Lindström has a very interesting feature : one can find in it not only constructions, but also a <u>proof</u> that the Hamming codes are not unique for infinitely many q : in fact every q which is not a prime, nor 4 and 8.

Lindström restricts to the case when m = 2, ie n = q+1, and to group codes : that is to subgroups of F^n, F being endowed with a group structure (incidentally he assumes that this group is elementary abelian, but remarks that other groups cannot give rise to perfect codes). He establishes a deep connection with translation planes by its use of Veblen-Wedderburn systems (quasifields). His two main results are :

- a description of every perfect group code up to isometry

- a necessary and sufficient condition under which a code is isometric to a Hamming one.

The present paper can be viewed as a continuation of Lindström's work. I restrict also to single error correcting perfect group codes, but release the assumption that m = 2. I give a geometrical description of these codes by mean of partitions of finite abelian groups. This has already been done in Herzog and Schönheim's paper [3]. But I prove also that the codes are isometric if and only if the associated partitions are isomorphic. I establish a connection between the isometry group of a code and the isomorphism group of the partition.

The paper is organized as follows : The second paragraph, entitled "Generalized Lindström codes and isometries" mainly intends to prove that two GL codes are equivalent if and only if they are equivalent as group codes. Group partitions are introduced in the third paragraph, where I show the existence of non desarguesian ones for a wide class of parameters. The fourth paragraph settles the main result about the connection between isometries of codes and isomorphisms of partitions.

II - ISOMETRIES AND GL CODES

The framework of the introduction is slightly changed for technical reasons. Although I am only interested in single error correcting perfect codes over alphabets of the same size q, I consider codes as subsets of product spaces $\prod_{i \in P} F_i$ where the F_i are finite sets of the same size $q \geq 2$ and P is a finite indexing set. I shall call sometimes an element of P a position, and when i is a position, F_i will be called the alphabet of position i. Every classical notion related to the Hamming distance will be generalized in an obvious way. But the F_i are not endowed in a unique way with group laws. By group law on a set S, I mean a map :

$$S \times S \longrightarrow S$$
$$(x,y) \longrightarrow x \Lambda y$$

which enjoies the usual axioms.

Definition 1 : A subset C of $\prod_{i \in P} F_i$ is a group code if there exists, for each position i, a group law Λ_i on F_i, so that C is a subgroup with respect to the product law. The family $(\Lambda_i)_{i \in P}$ is then called suitable with respect to C or simply suitable for short. A generalized Lindström code, or GL code, is a single error correcting perfect group code (it is assumed that the length, ie the size of P, is at least two).

The following result is a particular case of a theorem of Lenstra [4]. After the Zaremba-Schönheim construction [3,10], which relates GL codes to group partitions, it is equivalent to the fact that when a finite abelian group admits a partition, it must be elementary abelian, that is, isomorphic to a direct product of cyclic groups of the same prime order.

Proposition 1 : If $(\Lambda_i)_{i\in P}$ is a suitable family with respect to the GL code C then each Λ_i is elementary abelian.

Now, I investigate the relationship between GL codes and isometries. Except proposition 4, every result is already contained in my thesis [1], often as a very particular case.

The somewhat unusual notations in the following definition are explained in the remarks beneath.

Definition 2 : Let F_i, G_j be finite set of size q. The i runs through the indexing set P, the j through Q. For every bijective map $b : P \longrightarrow Q$ and every family $\sigma = (\sigma_i)_{i\in P}$ of bijective maps $\sigma_i : F_i \longrightarrow G_{ib}$, write $[\sigma, b]$ the map :

$$\prod_{i\in P} F_i \longrightarrow \prod_{j\in Q} G_j$$

$$m = (m_i)_{i\in P} \longrightarrow (m'_j)_{j\in Q}$$

where $m'_j = m_{jb^{-1}}\,\sigma_{jb^{-1}}$. An <u>isometry</u> is a map of the form $[\sigma, b]$ above. Two codes $C \subset \prod_{i\in P} F_i$, $D \subset \prod_{j\in Q} G_j$ are said <u>isometric</u> if there exists an isometry which maps C onto D.

<u>Remarks</u> : a) I shall use often similar notations for an element x of a product set, say $\prod_{i\in A} S_i$. Tacitly one has $x = (x_i)_{i\in A}$.

b) The maps will be often written at the right of the argument, e.g. $ib = b(i)$ and $m_{jb^{-1}}\,\sigma_{jb^{-1}} = \sigma_{jb^{-1}}(m_{jb^{-1}})$.

c) If f is an isometry which maps C onto D, I call it isometry from C onto D and write $f : C \longrightarrow D$.

Consider a GL code $C \subset \prod_{i\in P} F_i$, where each F_i is a set of size q. Choose a suitable family and write it additively.

Now, suppose that a code $D \subset \prod_{j\in Q} G_j$ is isometric to C. Obviously D is a perfect single error correcting code. Moreover D is a GL code too.

Indeed, let $f : C \longrightarrow D$ be an isometry. Write $f = [\sigma, b]$ like above. And define the group laws on each G_j in such a way that f is a group automorphism (recall that f is in fact a map $\prod_{i\in P} F_i \longrightarrow \prod_{j\in Q} G_j$). There is only one possibility :

$$G_j \times G_j \longrightarrow G_j$$

$$(x,y) \longmapsto (x\sigma_{jb-1}^{-1} + y\sigma_{jb-1}^{-1})\ \sigma_{jb-1}.$$

One checks easily that these are truly group laws on each G_j and that they form a suitable family with respect to D. Hence :

Proposition 2 : If a code is isometric to a GL code, then it is a GL code too.

Now I want to have more insight on the isometries between two GL codes, I ask the following question : what are the suitable families with respect to the GL code C ? A first result is obtained at once if one applies the previous discussion with D = C and with f of the following form :

$$\prod_{i\in P} F_i \longrightarrow \prod_{i\in P} F_i$$

$$x \longmapsto x + c$$

where c is a codeword.

Proposition 3 : Every codeword is the neutral of at least one suitable family.

Such a family is unique. I prove that fact now for the case when the neutral is 0. So, let $(\Lambda_i)_{i\in P}$ be a suitable family with respect to C and with neutral 0.

Let i be a position, a, a' be distinct non zero elements in F_i. Fix an arbitrary position $j \neq i$, and any b in F_j, $b \neq 0$. There is exactly one codeword m (resp.m') of weight 3 and such that :

$$\begin{cases} m_i = a, \; m'_i = a' \\ m_j = m'_j = b \end{cases}$$

Write k (resp.k') the remainding position where m (resp.m') does not vanish. Remark that $k \neq k'$, because, as $a \neq a'$, $d(m, m') \geq 3$.

Now, both $m + m'$ and $m \wedge m'$ (the codeword defined by $(m \wedge m')_i = m_i \wedge_i m'_i$ are examples of codewords c such that :

* $c_l = 0$ whenever l is a position and $l \notin \{i, j, k, k'\}$
* $c_k = m_k$
* $c_{k'} = m'_{k'}$

But there cannot exist two such codewords because the minimum distance of C is 3.

Hence $m + m' = m \Lambda m'$, and thus $a \Lambda_i a' = a + a'$. This last equality has been proved under the assumption that a, a' are distinct non zero elements of C. It is easy to extend it to the general case.

Proposition 4 : a) Let c be a codeword. There exist exactly

one suitable family with c as the neutral.

b) Let D be another GL code.

Write additively a suitable family with respect to D. Then every isometry $f : C \longrightarrow D$ that maps 0 onto 0 is a group isomorphism (with respect to the addively written laws).

Part b is a consequence of part a and of the discussion before proposition 2.

Codes for which part a and an additional, less important, assumption hold are studied in [1, 2] under the name of translation codes. The interested reader will find in [2] a generalization of proposition 1 and even of Lenstra's result.

III - PARTITION OF ABELIAN GROUPS

1) GENERALITIES

Let A be a finite abelian group, say of order v. A partition of A is a set Π of subgroups of A, called its members. The following properties are required :

(P1) Every member of Π has the same order, say k. Moreover, the non degeneracy assumption $1 < k < v$ holds.

(P2) Every element of A, except the neutral, belongs to exactly one element of Π.

I review now some background. The proofs can be found in [7].

The group A must be elementary abelian, that is isomorphic to a direct product of cyclic groups of the same prime order p. Accordingly, $v = p^d$, $k = p^r$ for integers d,r. Moreover $r \mid d$, say $d = rs$. I shall use a somewhat losely terminology when describing this situation : Π is of parameters p, r, s (in that order).

The kernel K of Π is the set of group endomorphisms α of A such that $\upsilon\,\alpha \subset \upsilon$ for every member υ of Π. This is obviously a subring of End A. More interesting is the fact that K is a field. Hence A can be viewed as a K linear space, and the members as subspaces. Obviously, they have the same dimension. When the members are lines, Π is called

desarguesian .

Now let Π, Π' be partitions of the finite abelian groups A, A' respectively. An isomorphism $f: \Pi \longrightarrow \Pi'$ is a group isomorphism $A \longrightarrow A'$ that maps every member of Π onto a member of Π'. Remark that two desarguesian partitions with the same parameters are isomorphic. When $r = 1$, every partition is desarguesian. Partitions with $s = 2$ are called spreads. They are closely related to translation planes. When $r \geq 2$, there exists a non desarguesian spread, with only two exceptions : $p = 2$, $r = 2$ and $p = 2$, $r = 3$ (see [7]).

2) NON DESARGUESIAN PARTITIONS.

Now, I prove a generalization of this last result : there exists always a non desarguesian partition with only the above exceptions. I argue as follows : given a partition Π of parameters p, r, s, I construct a class of partitions of parameters p, r, s+1 ; then I show that, when $r \geq 2$, some elements in the class are non desarguesian (even if Π is desarguesian). In fact, if Π is non desarguesian, every member of the constructed class are non desarguesian too.

Write $q = p^r$, and choose, for every member U of Π, a group isomorphism : $f_U : U \longrightarrow \mathbb{F}_q$, a finite field of order q.

Write again :

$$A' = A \times \mathbb{F}_q$$

$$\upsilon_\lambda = \{(x, xf_\upsilon \lambda), x \in \upsilon\} \quad (\lambda \in \mathbb{F}_q)$$

$$\Omega = \{(0, \lambda), \lambda \in \mathbb{F}_q\}$$

The above subgroups (υ_λ and Ω) are easily seen to form a partition Π' of the required parameters.

What is the kernel K' of Π' ? Identify A in the obvious way with a subgroup of A' ; it is a K' subspace of A', because it is the union of the υ_o . Another subspace is Ω. Hence, every element α of K' gives rise to two group automorphisms :

$$\alpha_1 : A \longrightarrow A$$

$$\alpha_2 : \mathbb{F}_q \longrightarrow \mathbb{F}_q$$

in such a way that $(x, \lambda)\ \alpha = (x\ \alpha_1;\ \lambda\ \alpha_2)$.

Obviously α_1 belongs to K and $\alpha \longrightarrow \alpha_1$ is a ring homomorphism (sending 1 onto 1). Because K and K' are both fields, this homomorphism is one to one. Hence if Π is non desarguesian, then so is Π'.

Now, assume that Π is desarguesian. I want to prove that Π' is non desarguesian, if the f_υ are properly chosen.I ask thus the question : what can be said about the f_υ if Π' is assumed desarguesian ? It will be sufficient to choose the f_υ in order that the answer fails.

Thus, assume that Π' is desarguesian. The following lemma will be useful :

LEMMA : Let E, F be linear spaces over a field, $g : E \longrightarrow F$ be a group homomorphism. The subgroup $\{(x, xg), x \in E\}$ is a subspace if and only if g is linear.

The proof is left over to the reader. I apply the lemma in the following situation :

* $E = \upsilon$ for any member υ of Π

* g is the map $\begin{array}{ccc} \upsilon & \longrightarrow & \mathbb{F}_q \\ x & \longmapsto & xf_\upsilon\lambda \end{array}$

for any $\lambda \neq 0$, $\lambda \in \mathbb{F}_q$.

This map, written g_λ, is linear. I fix υ a moment. Hence the map $h_\lambda : \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ x & \longrightarrow & x\lambda \end{array}$

is K' linear too (because $h_\lambda = g_1^{-1} g_\lambda$).

As $\mathbb{F}_q$ is a line, its linear automorphisms are the $k_\alpha : \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ x & \longmapsto & x\,\alpha_2 \end{array}$

where α runs through K'. Hence any h_λ is a k_α and there exists a field isomorphism $\sigma : K \longrightarrow \mathbb{F}_q$ such that $\alpha_2 = h_{\alpha\sigma}$ whenever $\alpha \in K$.

The K' linearity of f_U now means that $x \alpha f_U = x f_U \alpha^\sigma$ whenever $x \in U$, $\alpha \in K$.

Hence, to construct non desarguesian partitions, it is sufficient to choose the f_U in order that this last identity holds but with distinct σ as U runs through Π. This is clearly possible whenever $r \geq 2$.

IV - GENERALIZED LINDSTROM CODES AND GROUP PARTITIONS.

The idea of a relationship between group partitions and perfect codes (or something closely related to them) seems to go back to Zaremba's paper [10]. It was both deepened and clarified in [3]. Here, I study the relationship between isomorphisms of partitions and isometries of codes. Let me recall first the two basic constructions : detailed proofs can be found in [3].

1) Let Π be a partition of the abelian group A. Recall that the members of Π are elementary abelian of same order. Now, $C(\Pi) = \{(x_U)_{U\in\Pi}, x_U \in U , \sum_{U\in\Pi} x_U = 0\}$ is a GL-code in $\prod_{U\in\Pi} U$.

2) Let C be a GL code in $\prod_{i\in P} F_i$, where the alphabets F_i are endowed with elementary abelian group structures. I suppose that the F_i have the same order $q \geq 2$ and that C is a subgroup of $\prod_{i\in P} F_i$. Write $H = \prod_{i\in P} F_i$ and let U_i stands for the image of F_i under the quotient map $H \longrightarrow H/C$ (F_i is identified in the obvious way with a subgroup of H). I claim that the U_i form a partition of H/C.

I shall not give a detailed proof of the following theorem because this should be long and straightforward. The more important points of the proof are :

- a consequence of proposition 4 of § II : an isometry between two GL codes is the composition of a group translation and of a group isomorphism, these two codes

being endowed in an arbitrary way with suitable families.

- our study of non desarguesian partitions in § III.

- a rather technical argument to insure us that Π is in a natural way isomorphic to $\Pi(C(\Pi))$, and C isometric to $C(\Pi(C))$. First, remark that the second point is a consequence of the first when applied to the partition $\Pi(C)$. To obtain the isomorphism $\Pi \longrightarrow \Pi(C(\Pi))$, remark that $\prod_{U \in \Pi} U / C(\Pi)$ is isomorphic to A because the homorphism $\prod_{U \in \Pi} U \longrightarrow A$

$$(x_U) \longmapsto \sum_{U \in \Pi} x_U$$

is clearly onto and its kernel is $C(\Pi)$. Without any more detail, I state :

THEOREM : Let p be a prime, r, m be positive integers. Write $q = p^r$, $n = \frac{q^m - 1}{q-1}$. Assume $m \geq 2$.

a) If $r = 1$, every GL code is equivalent to a Hamming one. If $r \geq 2$, except when $m = 2$ and $q = 4,8$, there exist a GL code not equivalent to a Hamming one.

b) Let C, C' be GL codes. They are equivalent if and only if $\Pi(C)$ is isomorphic with $\Pi(C')$. Moreover, if C, C' are endowed with suitable families, every isometry which sends the neutral of C onto that of C' is a group isomorphism. Such isometries are in one to one and onto correspondance with the isomorphisms $\Pi(C) \longrightarrow \Pi(C')$.

c) Let Π, Π' be group partitions. They are equivalent if and only if $C(\Pi)$ is isometric to $C(\Pi')$. These codes being considered as subgroups of $\prod_{U\in\Pi} U$, $\prod_{U\in\Pi'} U$ respectively, there is a bijective correspondance between the isomorphisms $\Pi \longrightarrow \Pi'$ and the isometries $C(\Pi) \longrightarrow C(\Pi')$ which are group isomorphism too.

d) C is in a natural way isometric to $C(\Pi(C))$, Π is in a natural way isomorphic with $\Pi(C(\Pi))$.

e) If $C = C'$, resp. $\Pi = \Pi'$, the bijective correspondance considered in b and c are group automorphisms.

Remark : These correspondance are tacitly assumed to be the "most natural ones", that is

- in b, let f be an isometry $C \longrightarrow C'$ which sends the neutral of C onto that of C'. Then f is a group isomorphism $H \longrightarrow H'$ which maps C onto C' and one associates with it an isomorphism $H/C \longrightarrow H/C'$.

- in c, let ρ be an isomorphism $\Pi \longrightarrow \Pi'$; the associated isometry maps $(x_U)_{U\in\Pi}$ onto $(x_U\ \rho)$ suitably indexed.

BIBLIOGRAPHY

- 1 - BONNEAU P.G.
"Codes et Combinatoire"
Thèse de troisième cycle
Université Pierre et Marie Curie, Paris - 1984 -

- 2 - BONNEAU P.G.
"Translation Codes"
Submitted to Discrete Mathematics.

- 3 - HERZOG M. and SCHONHEIM J.
"Linear and non-linear single-error-correcting perfect mixed codes",
Info. Control., 18 - 1971 - 364-368.

- 4 - LENSTRA Jr H.W.
"Two theorems on perfect codes",
Discrete Math., 3 - 1972 - 125-132.

- 5 - LINDSTROM B.
"On group and nongroup perfect codes in q symbols",
Math. Scand., 25 - 1969 - 149-158.

- 6 - LINT J.H. Van
"A survey of perfect codes",
Rocky Mountain J. of Mathematics, 5 - 1975 - 199-224.

- 7 - LUNEBURG H.
"Translation planes",
Springer-Verlag - 1980 -

- 8 - MAC WILLIAMS F.J. and SLOANE N.J.A.,
"The theory of error-correcting codes"
(third printing) North-Holland - 1981 -

- 9 - SILVERMAN R.,
"A metrization for power sets with application to combinatorial analysis",
Canadian J. Math., 12 - 1960 - 158-176.

- 10 - ZAREMBA S.K.,
"Covering problems concerning abelian groups",
J. London Math. Soc., (2) 27 - 1952 - 242-246.

Imprimé en France
par
l'Institut National de Recherche en Informatique et en Automatique