Translation codes

P.G. Bonneau

INRIA

CENTRE DE ROCQUENCOURT

Institut National
de Recherche
en Informatique
et en Automatique

Domaine de Voluceau
Rocquencourt
BP105
78153 Le Chesnay Cedex
France

Tél. : (1) 39 63 55 11

Rapports de Recherche

N° 454

TRANSLATION CODES

Pierre G. BONNEAU

Novembre 1985

TRANSLATION CODES

Pierre G. BONNEAU

INRIA Rocquencourt

Domaine de Voluceau

BP No 105

78153-LE CHESNAY Cedex

FRANCE

TRANSLATION CODES

Mailing address : Pierre BONNEAU
34 rue S. Allende
92000 - NANTERRE
FRANCE

Summary : This paper deals with subgroups of finite product group (variable order group codes). More precisely, I give sufficient conditions under which a group code C is a translation one, that is, enjoies the following property : a codeword being chosen as the neutral, there exists exactly one family of group structures on the alphabets such that C is a subgroup of the corresponding product structure. I also generalize the following theorem of Lenstra : (constant order) group perfect codes must be elementary abelian. Finally, I prove that the quotient of a finite group by the intersection of its maximal proper normal subgroups is isomorphic to the direct product of some of its simple quotients.

Résumé : Cet article traite de sous-groupes de groupes finis produits (codes en groupe d'ordre variable). Plus précisement, nous donnons des conditions suffisantes pour qu'un code en groupe soit à translation, c'est à dire, vérifie la propriété suivante : un mot de code étant choisi comme élément neutre, il existe une famille unique de structures de groupe sur les alphabets telle que C soit un sous-groupe relativement à la structure produit. Nous généralisons également le théorème suivant de Lenstra : les codes parfaits en groupe (d'ordre constant) sont abéliens élémentaires. Enfin, nous prouvons que le quotient d'un groupe fini par l'intersection de ses sous-groupes distingués maximaux est isomorphe au produit direct de certains de ses quotients simples.

I INTRODUCTION

Translation codes were first defined in [2] (see also [3]). I needed to show that the group structures on some kinds of codes are intrinsic. My purpose was to classify these codes and to reduce the problems about their groups to problems of finite geometry . Here, I generalize this notion. In § III, I give new sufficient conditions under which a group code is a translation one. To that end, I define critical supports. They are also useful to strengthen a theorem of Lenstra. But the idea of critical support and the obvious fact that (the group structure on) a translation code is abelian are also used in § IV to prove purely group theorical results.

II PRELIMINARIES

First, I review some definitions and results which are mainly generalizations of those of [3] (with sometimes slight changes).

II.1. Generalized codes

II.1.a. The cardinality of a finite set X is denoted by $|X|$. Alternatively "X is a n-set" means "X is a finite set and $|X| = n$".

II.1.b. When P is a n-set with $n \geq 1$, and F_i, for each $i \in P$, are q_i-sets with $q_i \geq 2$, the (generalized) Hamming distance between $x,y \in \mathcal{H} = \prod_{i \in P} F_i$ is $d(x,y) = |i \in P, x_i \neq y_i|$ (x_i stands for the component of x on the position i, that is $x = (x_i)_{i \in P}$; I shall always use this notation when dealing with product sets). The classical case occurs when $q_i = q$ does not depend on i. It is studied in most of the references at the end of this paper.

II.1.c. In the general case, a code in $\mathcal{H}$ is a subset C of $\mathcal{H}$ with $|C| \geq 2$. Its elements are called codewords. I shall use the customary language of information theory : P is the set of positions, q_i is the order of $\mathcal{H}$ (or C) on the position i, F_i its alphabet of position i, n is the length of both $\mathcal{H}$ and C, and so on.

II.1.d. The minimum distance of a code C, (I shall denote it by d is the minimum value of the $d(c,c')$, $c \neq c' \in C$. When $x \in \mathcal{H}$, $d(x,C)$ stands for the minimum value of the $d(x,c)$, $c \in C$. The dual distance of $C \neq \mathcal{H}$ (I shall denote it by d') is the greatest integer δ such that, whenever J is a $(\delta-1)$-subset of P, and $y \in \prod_{j \in J} F_j$, the number of $c \in C$ with $c_j = y_j$ whenever $j \in J$ is $(\prod_{j \in J} q_j)^{-1} |C|$ (in other words, that number depends only on J and not on the particular choice of y). Remark that this definition agrees, in the classical case, with a characterization of Delsarte ([4] and [5]).

Let u be a codeword; $t > 0$ be an integer. I say that a subset X of $\mathcal{H}$ is a t-design at u when :

a) $0 < d(u,x) = d(u,x')$ whenever $x,x' \in X$;

b) there exists an integer $\lambda > 0$ such that whenever S is a t-subset of P, y_s, $s \in S$ are elements of F_s, $y_s \neq u_s$, then the number of $x \in X$ with $x_s = y_s$ whenever $s \in S$ is λ.

See e.g. [4], [5], [6], [11] for a study of design properties of codewords.

II.2. Groups and group codes

I shall use freely standard results and terminology when dealing with groups. Simply recall that $[G,G]$ is the subgroup of G spanned by the $x^{-1}y^{-1}xy$, $x,y \in G$. It is contained in every normal subgroup H of G such that G/H is commutative. See e.g. [7].

I also recall some notations about permutation groups and maps.

When $f : E \to F$ is a map, $x \in E$, xf stands for the image of x. Accordingly, when $g : F \to G$ is another map, fg stands for the map :

$$fg : E \to G$$
$$x \to (xf)g$$

and $(xf)g$ is simply denoted by xfg. The identity map is denoted by id on any set.

II.2.c. With the notations of I.1, let

$$\Lambda_i : F_i \times F_i \to F_i$$
$$(x,y) \to x \Lambda_i y$$

be group laws for every $i \in P$. I denote by Λ the product law on $\mathcal{H}$ (recall that Λ denotes also $(\Lambda_i)_{i\in P}$). I say that a code C in $\mathcal{H}$ is a Λ code, or alternatively, that Λ is a suitable family (with respect to C) when C is a subgroup of $\mathcal{H}$ ($\mathcal{H}$ being endowed with Λ). Note that a Λ code C is setwise invariant under the operation of the permutation group $T(\Lambda)$ whose elements are the

$$\Lambda c : \mathcal{H} \to \mathcal{H}$$
$$x \to x \Lambda c$$

II.2.d. When γ_i, $i \in P$, are permutations of the F_i, let γ denote the permutation

$$\gamma : \mathcal{H} \to \mathcal{H}$$
$$x \to (x_i\gamma_i)_{i\in P}$$

(remark that $(x_i\gamma_i)_{i\in P}$ may be denoted without any ambiguity $x\gamma$).

I say that γ is a nice map when either γ_i is fixed point free, either $\gamma_i = id$. Remark that the maps Λc (as defined in II.2.b.) are nice.

I say that Γ is a nice group (with respect to C) when the following conditions are satisfied :

(NG1) Γ is a permutation group on $\mathcal{H}$; every $\gamma \in \Gamma$ is a nice map;

(NG2) Γ preserves C and is transitive on it.

Assume that $d' \geq 2$ and that C admits a nice group Γ. Let u be any codeword. In [3], I have proved that, in the classical case (q_i does not depend on i), there exists exactly one suitable family Λ whose neutral is u and such that $\Gamma = T(\Lambda)$. The (quite easy) proof obviously extends to the general case. The geometric ideas beyond these concepts are explained in [2] and [3].

II.2.d. A code C is a group code when it admits at least one suitable family. A group code C is a translation code on the position i when : (i) whenever $a \in F_i$, there exists a codeword c with $c_i = a$;

(ii) the following equivalent [1] conditions hold : a) there exists $u \in C$ satisfying (*) : whenever

(1) The fact that these three conditions are equivalent ((i) being assumed) is left to the reader.

Λ, M are suitable families whose neutral is u, then $\Lambda_i = M_i$.

b) condition (*) holds whenever $u \in C$

c) when Γ, Γ' are nice groups, then for every $\gamma \in \Gamma$, there exists $\gamma' \in \Gamma'$ such that $\gamma_i = \gamma'_i$.

I say that a group code C is a translation code when it is a translation code on each of its positions (this definition is in accordance with that of [2] and [3] in the classical case).

Remark that, when a code C is a translation code on a position i, then for any suitable family Λ, Λ_i is abelian. Indeed, the opposite Λ^o of Λ is also a suitable family ($\Lambda^o(x,y) = \Lambda(y,x)$).

II.3. Supports, critical sets

II.3.a. With the previous notations, let C be a code. The supports (of C) are the $s(c,c') = \{i \in P, c_i \neq c'_i\}$, $c \neq c' \in C$. Let $i \in P$; I say that a support K is critical on i when $i \in K$, $|K| \geq 2$, and the following condition holds :

(Cr-i) let c,c' be two codewords. Assume that $c_\ell = c'_\ell$ whenever $\ell \notin K$ and $c_j = c'_j$ for at least one $j \in K$. Then $c_i = c'_i$.

I say that a support K is critical when $|K| \geq 2$ and

K is critical on all of its positions. Remark that when $d \geq 2$, a critical support is merely a minimum support with respect to set theorical inclusion.

II.3.b. Remark that, when C is a group code, then, for every $c \in C$ and every support K which is critical on one of its elements i, there exists a codeword c' such that $s(c,c') = K$. If one assumes moreover that C is linear (see e.g. [10], [11]), then, given $c \neq c'$, $a \neq c_i$, there exists such a c' with $c'_i = a$. Analogous remarks hold when critical on a position is replaced by critical.

III MAIN RESULTS FROM A CODING THEORIST POINT OF VIEW

Throughout this paragraph, I consider a code C. The context is that of (II.1).

III.1 I begin with a fundamental lemma. Here and in the next paragraph, it shall provide simple sufficient conditions in order that a code be a translation one on some position.

Lemma 1 : Consider a position i, and two codewords $u \neq c$. Assume that $K = s(u,c)$ is critical on i, and that for every $a \in F_i$, $a \neq u_i$, there exists a codeword b and a position $j \in K$ such that $b_i = a$ and $b_j = u_j$. Let γ, γ' be nice maps which preserve C and send u onto C. Then $\gamma_i = \gamma'_i$.

Proof : I must show that $a\gamma_i = a\gamma_i'$ whenever $a \in F_i$, $a \neq u_i$. So let b,j be like in the statement of the lemma. Remark that :

$(b\gamma)_j = (b\gamma')_j = c_j$

$(b\gamma)_\ell = (b\gamma')_\ell = b_\ell$ whenever $\ell \notin K$ (the last point holds because γ_ℓ and γ_ℓ' fix a point, so are the identity, see II.2.c.).

The conclusion follows thus from the definition (see II.3.a.).

Corollary 1 : Let Λ be a suitable family, i a position. Call u the neutral of Λ.

a) Assume that whenever $a \in F_i$, $a \neq u_i$, there exist both : * a codeword c such that $s(u,c) = K$ is critical on i and $c_i = a$

* a codeword b and a position $j \in K$ such that $b_i = a$ and $b_j = u_j$.

Then C is a translation code on the position i.

b) Assume that C is linear and that $d \geq 2$, $d' \geq 3$. Then C is a translation code.

c) Assume that the codewords c with $d(u,c) = d$ form a 1-design at u and that $d \geq 2$, $d' \geq 3$. Then C is a translation code.

Proof : Part a) is an obvious consequence of lemma 1. Parts b) and c) follow at once from it and from II.3.a.

Remark : Assume that q_i does not depend on i. Part b) is already proved (in a different way) in [3]. As a consequence of [1] e.g., "MDS" or "optimal" non trivial codes enjoy the assumption made in Part c). The conclusion, in this case, is proved in a different way in [3]. See chapter 5 of this thesis for other conditions in order that a group code be a translation one.

III.2. A generalization of a theorem of Lenstra

In [8], H.W. Lenstra has shown that perfect group codes must be elementary abelian (in the classical case where q_i does not depend on i). Here, I generalize this theorem in the next proposition. Because C is a translation code by (III.1) corollary 1, I shall write it additively.

Proposition 1 : Assume that C is a group code, that $d \geq 2$, and that whenever $i \neq j \in P$, $a \in F_i$, $b \in F_j$, $a \neq 0$, $b \neq 0$, there exist both :

a) $c \in C$ with $s(c,0)$ critical and $c_i = a$, $c_j = b$

b) $c' \in C$ with $c'_i = a$, $c'_j = 0$.

Then C is elementary abelian.

Proof : Let $i \in P$, p be a prime divisor of q_i, and consider another position $j \neq i$ and any $b \in F_j$, $b \neq 0$. Let $a \in F_i$ be an element of order p, c a codeword which enjoy the property a) in the statement of the proposition. Then $(pc)_k$ vanishes whenever $k \notin s(c,0)$ and also when $k = i$. So, because $s(c,0)$ is critical, $pc = 0$. This proves that $(pc)_j = pb = 0$.

Remarks : 1) Because property b) must hold whenever $i \neq j \in P$, $a \in F_i$, $C \neq \mathcal{H}$ and C is a group code, I could have stated it in another way : $d' \geq 3$.

2) I explain now why the assumptions of proposition 1 are satisfied by non trivial perfect group codes in the classical case. First the codewords x with $d(0,c) = d$ provide the codewords c that are required in a). This is an easy and well-known lemma. The fact that $d' \geq 3$ is far deeper. It follows from lemma 35 of ch. 6 § 10 of [11], and the fact that the lowest zero of the corresponding Lloyd polynomial is d'.

3) Assumption a) hold when the minimum weight codewords form a 2-design.

IV APPLICATION TO GROUP THEORY

IV.1 Some more notations

As previously, P stands for a finite non-void indexing set.

Let G be group of finite order, H_i , $i \in P$, be

proper normal subgroups of G. Let $\overline{g_i}$ denote the image of $g \in G$ under the canonical morphism $G \to G/H_i$. Set $G/H_i = F_i$. Then $C = \{(\overline{g_i})_{i\in P, g\in G}\}$ is a Λ code in $\prod_{i\in P} F_i$, where Λ stands for the obvious group law.

I say that a proper normal subgroup H of $\prod_{i\in P} F_i$ is a leader (resp. a plague) when G/H is simple (resp. is a non abelian simple group). One can also define leaders as maximal proper normal subgroups.

IV.2. Why may C be a non translation code ?

First, an easy lemma, which gives condition in order that one of the assumptions in lemma 1 holds.

Lemma 2 : a) Assume that H is a leader and that U is a normal subgroup of G with $U \not\subset H$. Then $UH = G$.

b) Assume that H_i is a plague and that when $j \neq i$, H_j is not a subgroup of H_i. Then, whenever $a \in F_i$, $a \neq 1$, there exists a codeword b with $b_i = a$, $b_j = 1$.

Proof : Part a) follows at once from the fact that UH is a normal subgroup of G which contains H properly. Thus, $H_iH_j = G$ under the hypothesis of b). So, let $g \in G$ be such that $\overline{g_i} = a$; $g = xy$ with $x \in H_i$, $y \in H_j$. Let $b = \bar{y}$, and check that b works.

Proposition 3 : Under the assumptions of lemma 2 $LH_i = G$, where $L = \bigcap_{j \neq i} H_j$

Proof : 1) In a first step, I show that when $1 \neq c \in C$, $s(1,c)$ is never critical on i.

Remark that C is not a translation code on i, because Λ_i is not abelian (II.2.d). So let Γ be a nice group (II.2.c) such that the subgroup $A = \{t \in T(\Lambda), \exists\, \gamma \in \Gamma, t_i = \gamma_i\}$ differs from Γ. Because of lemma 1 (III.1), A contains the set S of elements of $T(\Lambda)$ which send 1 onto a codeword c such that $s(1,c)$ is critical on i. Call B the permutation group on $\mathcal{H}$ which is spanned by S. This is obviously a normal subgroup of $T(\Lambda)$. Remark that A contains also $T' = \{t \in T(\Lambda), t_i = id\}$. Thus $BT' \subset A$ and BT' is a normal subgroup of $T(\Lambda)$. Because $T(\Lambda)/T' \simeq G/H_i$, thus is simple, and $A \neq T(\Lambda)$, I conclude that $BT' = T'$ and $S = \emptyset$.

2) Now remark that a support which is minimal among those which contain i must be a singleton (as I remarked in (II.3.a), the contrary implies that such a support is critical on i). Thus there exists $g \in G$ such that $\overline{g_i} \neq 1$ and $\overline{g_j} = 1$ whenever $j \neq 1$. The conclusion now follows from lemma 2 with $U = L$.

IV.3. A theorem about the structure of finite groups

Let $\mathfrak{M}$ be the set of leaders of G, and set $R = \bigcap_{H \in \mathfrak{M}} H$. A consequence of (IV.2) is

Theorem : There exists a subset $\mathfrak{N}$ of $\mathfrak{M}$ such that the obvious morphism $G/R \to \prod_{H \in \mathfrak{N}} G/H$ is an isomorphism.

Proof : I assume w. l.o.g. that $R = \{1\}$, and argue by induction on $|G|$. The conclusion is obvious when $|\mathfrak{M}| = 1$. Thus I assume that $|\mathfrak{M}| > 1$.

a) Suppose that G/H is abelian (thus cyclic of prime order) whenever $H \in \mathfrak{M}$. Because $[G,G] \subset H$ whenever $H \in \mathfrak{M}$ and $R = \{1\}$, $[G,G] = \{1\}$, that is : G is commutative. Now remark that when $x \in G$, p is a prime and $x^{p^2} = 1$, then $x^p = 1$. Indeed, choose any $H \in \mathfrak{M}$ with $x \notin H$. Set $|G/H| = q$. Because G/H is cyclic of order q and q is a prime, q divides p^2, thus $q = p$ and $x^p \in H$. But this is true for any $H \in \mathfrak{M}$, and $R = \{1\}$. Thus $x^p = 1$, as asserted. It follows that the Sylow subgroups of G are elementary abelian. Because G, as an abelian group, is the direct product of its Sylow subgroups, the conclusion of the theorem holds.

b) Suppose now that there exists $H \in \mathfrak{M}$ such that G/H is not abelian. Consider an arbitrary one to one and onto indexation $\begin{matrix} P \to \mathfrak{M} \\ j \to H_j \end{matrix}$. Call i the index such that $H_i = H$.

From proposition 2 of (IV.2), I get $G = HL$. But because $H \cap L = R = \{1\}$, and H, L are normal subgroups of G, $H \times L \to G$, $(h, \ell) \to h\ell$ is an isomorphism. The conclusion of the theorem follows from the induction hypothesis and the fact that when K is a leader of L, then HK is a leader of G.

BIBLIOGRAPHY

[1] P. BONNEAU : "Un renforcement de la formule d'énumération des poids des codes optimaux", C.R. Acad. Sc. Paris, t. 296 (1983) Série I, 863-864.

[2] P. BONNEAU : "The classification and the groups of additive perfect codes" (submitted to the Acts of the Colloquium AAECC, Toulouse 1984).

[3] P. BONNEAU : "Codes et Combinatoire", Thesis (Paris, 1984).

[4] Ph. DELSARTE : "An algebraic approach to the association schemes of coding theory", Philips Research Reports n° 10 (1973).

[5] Ph. DELSARTE : "Four fundamental parameters of a code and their combinatorial significance", Info. and Control, 23 (1973), 407-438.

[6] J.M. GOETHALS and H.C.A van TILBORG : "Uniformly packed codes", Philips Research Reports, 30 (1975), 9-36.

[7] D. GORENSTEIN : "Finite Groups", Harper & Row (1968).

[8] H.W. LENSTRA : "Two theorems on perfect codes", Discrete Math., 3 (1972) 125-132.

[9] J.H. van LINT : "A survey of perfect codes", Rocky Moutain J. of Mathematics, 5 (1975) 199-224.

[10] J.H. van LINT : "Introduction to coding theory", Springer (1982).

[11] F.J. Mac WILLIAMS and N.J.A. SLOANE : "The theory of error-correcting codes", North-Holland (1981).

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