Can, J. Math., Vol. XXVII, No. 4, 1975, pp. 819–826

RACINE MINIMUM D'UN GROUPE ELEMENTAIRE ABELIEN

MIKHAIL DEZA

Soit L un groupe abélien élémentaire d'ordre p^n (p est un premier, n est un entier positif). Soient (a) le groupe cyclique d'élément $a \in L$, $|A|$ le nombre des éléments de l'ensemble $A \subset L$. Nous appellerons l'ensemble $B \subset L$ *racine du groupe* L si pour tout a, $\{0\} \neq a \in L$, il existe b_1, $b_2 \in B$ ($b_1 \neq b_2$) tels que $b_1 - b_2 \in (a)$. (A ce propos, il est évident que si B est une racine de L, l'ensemble $B_{st}{}^* = \{b_i{}^* = sb_i + t/b_i \in B\}$, où sont donnés s, $t \in L$, $(s) \neq (0)$, (c'est-à-dire $B_{st}{}^*$ est le résultat de l'affinité de B) est également racine de L.) Nous appellerons la racine B *minimum* et désignerons $|B|$ par $\beta(L)$ si tout autre racine contient au minimum $|B|$ éléments. Voici les exemples de racines minimum du L pour $L = F_2{}^n$, $n = 1, 2, 3, 4, 5$ et pour $L = F_3{}^3$:

$\{0, 1\}$; $\{00, 01, 10\}$; $\{000, 001, 010, 100, 111\}$;
$\{0000, 0001, 0010, 0100, 1000, 1111\}$;
$\{00000, 00001, 00010, 00100, 01000, 10000, 00011, 00101, 00110, 11111\}$;
$\{000, 001, 010, 100, 111, 222\}$.

LEMME 1. *On a*

$$\tfrac{1}{2} + \left[\tfrac{1}{4} + 2 \sum_{0 \leqq i \leqq n-1} p^i\right]^{1/2} \leqq \beta(L) \leqq p^{[n/2]} + p^{n-[n/2]} - 1.$$

En effet, soit $\bar{L}_0$ un sous-groupe d'ordre $p^{[n/2]}$ du groupe L, $\tilde{L}_0$ un sous-groupe tel que $\bar{L}_0 \cap \tilde{L}_0 = (0)$, $\bar{L}_0 + \tilde{L}_0 = L$. L'ensemble $\bar{L}_0 \cup \tilde{L}_0$ est évidemment une racine, donc, $\beta(L) \leqq |\bar{L}_0 \cup \tilde{L}_0|$, d'où découle l'estimation supérieure. Soit B la racine minimale. Il est clair que $\bigcup_{b_1, b_2 \in B} (b_1 - b_2) = L$. Mais dans $\bigcup_{b_1, b_2 \in B} (b_1 - b_2)$ on trouve au plus $\binom{|B|}{2}(p-1)$ éléments non-nuls ; donc

$$\binom{|B|}{2}(p-1) \geqq |L| - 1, \quad \binom{\beta}{2} \geqq p^{n-1} + \ldots + p + 1,$$

d'où découle l'estimation inférieure.

Si $L = F_2{}^n$, l'estimation supérieure du lemme est obtenue pour $n = 1, 2, 3$; pour $n > 4$, dans cette estimation on peut poser le signe d'inégalité rigoureuse puisque, à la place de la racine $\bar{L}_0 \cup \tilde{L}_0$ on peut prendre la racine

$$(\tilde{L}_0 \backslash \{a_1\}) \cup (\bar{L}_0 \backslash \{a_2\}) \cup \{a_1 + a_2\},$$

Reçu le 12 octobre, 1973 et sous forme revisée, le 21 août, 1974.

où sont fixés des éléments non-nuls $a_1 \in \bar{L}_0$, $a_2 \in \tilde{L}_0$). Si $L = F_2{}^n$, l'estimation inférieure du lemme est obtenue si et seulement si $n = 1, 2, 4$ (à ce propos, pour tout L la racine minimum est un (v, k, λ)-ensemble de groupe de différence, où $v = |L|$, $k = \beta(L)$, $\lambda = 1$ si et seulement si on obtient l'estimation inférieure du lemme). Si $L = F_2{}^n$, $n \geqq 3$ alors on peut montrer que parmi les racines minimum il en existe une qui contient toutes les n-suites à une unité, la n-suite à n unités et la n-suite à n zéros.

Le fait que le nombre $\beta(L)$ ait l'ordre du nombre $|L|^{\frac{1}{2}}$ (par le lemme il est aisé de voir que $(2/(p-1))^{\frac{1}{2}} |L|^{\frac{1}{2}} < \beta(L) < ((p+1)/p^{\frac{1}{2}})|L|^{\frac{1}{2}}$ pour $|L| \neq 2$) souligne l'analogie entre la notion de racine de groupe et celle de racine carrée du nombre. (Cette analogie apparaît aussi dans le fait que pour $p = 2$, B est une racine si et seulement si $B + B = L$.) On peut, pour $L = F_2{}^n$, appeler *racine* de *k-ième degré d'un groupe* L, un ensemble $B \subset L$, tel que $B + \ldots + B = L$, où B est pris en qualité de terme k fois. Ce faisant, il est facile de généraliser le lemme et pour une cardinalité $\beta_k(L)$ de racine *minimum* de degré k nous obtenons $\beta_k(L) \sim |L|^{1/k}$.

Montrons l'analogie de ce lemme, pour $L = F_2{}^n$, avec le résultat suivant de Rohrbach (cf. [**3**], p. 130) dans la théorie additive des nombres: soit $0 \leqq a_1 < \ldots < a_q \leqq m$ une suite d'entiers telle que chacun des entiers de $[0, m]$ soit représentable sous la forme $a_i + a_j$, et soit $g(n) = \min q$; alors $(2m)^{\frac{1}{2}} \leqq g(m) \leqq 2(m)^{\frac{1}{2}}$. Pour $L = F_2{}^n$, il est aisé de formuler le lemme de la façon suivante: soit $m = 2^n - 1$, soit $0 \leqq a_1 < \ldots < a_q \leqq m$ une suite d'entiers telle que chacun des entiers de $[0, m]$ puisse être représentable sous la forme $a_i \dot{+} a_j$ (si

$$a_t = \sum_{0 \leqq s \leqq n-1} a_{ts} 2^s$$

est une notation binaire d'entier a_t, définissons ainsi la somme

$$a_t \dot{+} a_j = \sum_{0 \leqq s \leqq n-1} |a_{ts} - a_{js}| 2^s)$$

et soit $\dot{g}(m) = \min q$; alors, $\dot{g}(m) = \beta(L)$, où $L = F_2{}^n$, et, donc,

$$(2m + 1/4)^{\frac{1}{2}} + 1/2 \leqq \dot{g}(m) \leqq \begin{cases} 2(m+1)^{\frac{1}{2}} - 1, \text{ si } 1g_2(m+1) \text{ est pair} \\ 3/2^{\frac{1}{2}}(m+1)^{\frac{1}{2}} - 1, \text{ si } 1g_2(m+1) \text{ est impair.} \end{cases}$$

Enfin, la notion de racine minimum est analogue à certains problèmes de combinatoire pour un groupe abélien fini G, envisagés dans [**2**] et dans les chapitres 1, 9 de [**5**]. Par exemple, le nombre $c(G)$ examiné dans [**2**] (c'est le min $|S|$, où

$$\left\{ \sum_{a_i \in S} \epsilon_i a_i / \text{tous les } \epsilon_i = 0, 1 \right\} = G$$

coïncide pour $G = F_2{}^n$ avec le nombre $\beta_k(G)$ envisagé ci-dessus, où $k = \beta_k(G)$.

https://doi.org/10.4153/CJM-1975-089-3 Published online by Cambridge University Press

Maintenant, montrons dans le Théorème 1 les estimations inférieures du "rôle relatif" $|\hat{B}_1| = |L\backslash(B\backslash B_1 + B\backslash B_1)|$ de tout propre sous-ensemble B_1, $B_1 \subset B$, d'une racine minimum du groupe $L = F_2{}^n$. Démontrons, pour commencer, un lemme algébrique. On donne une k-aire opération $\alpha(g_1, \ldots, g_k)$, $k \geqq 2$; appellerons l'ensemble G un *α-système*, si $|G| < k$, ou si $|G| \geqq k$ et pour tous *différents* $g_1, \ldots, g_k \in G$ on a $\alpha(g_1, \ldots, g_k) \in G$. Dans le Théorème I nous utiliserons seulement le cas trés particulier, où α-système est le groupe $F_2{}^n$; mais ci-dessous Lemme 2 prouve pour α-système par ce que la preuve n'est pas plus longue dans le cas gènèral et que la Lemme 2 a peut étre un intèrét en soi. Pour tout $F \subset G$, appelons *constructive* la représentation $F = \{a_1, \ldots, a_{kf}\} \cup F'$, où

(a) les éléments $a_1, \ldots, a_{kf}$ sont distincts;

(b) $\alpha(a_{kt-k+1}, \ldots, a_{kt}) \in (G\backslash F) \cup \{a_1, \ldots, a_{kt-k}\}$ pour $1 \leqq i \leqq f$;

(c) F' est un α-système.

LEMME 2. *Tout sous-ensemble fini d'un α-système a une représentation constructive.*

En effet, soient un α-système G et $F \subset G$. Pour tout entier $i \geqq 1$ définissons par induction l'ensemble F_i et la k-suite d'éléments distincts $(a_{kt-k+1}, \ldots, a_{kt})$ de la manière suivante: $F_i = F$ pour $i = 1$; si F_i n'est pas un α-système, alors $(a_{kt-k+1}, \ldots, a_{kt})$ est une k-suite d'éléments distincts de F_i telle que $\alpha(a_{kt-k+1}, \ldots, a_{kt}) \notin F_i$, et $F_{i+1} = F_i\backslash\{a_{kt-k+1}, \ldots, a_{kt}\}$. On a $|F_{i+1}| < |F_i|$ mais $|F_1| = |F| < \infty$ et donc, il existe un entier $z \geqq 1$, tel que F_z est un α-système. Posant $f = z$, $F' = F_z$, nous obtenons une représentation constructive (les propriétés (a), (c) sont évidentes; nous obtenons (b) puisque $F_i = F\backslash\{a_1, \ldots, a_{kt-k}\}$ et, plus loin,

$$\alpha(a_{kt-k+1}, \ldots, a_{kt}) \notin F_i \Leftrightarrow \alpha(a_{kt-k+1}, \ldots, a_{kt}) \in (G\backslash F) \cup \{a_1, \ldots, a_{kt-k}\},$$

puisque G est un α-système).

Remarquons qu'en général une k-suite $(a_{kt-k+1}, \ldots, a_{kt-k})$ peut ne pas être unique et que donc, une représentation constructive peut ne pas être unique. Remarquons également que F' peut ne pas être un α-système maximal de F; par exemple, si $F = G_1 \cup \ldots \cup G_k$ (où $G_1, \ldots, G_k$ sont des α-systèmes, $|G_1| = \ldots = |G_k| \geqq 1$ et $-1 + |G_1 \cup \ldots \cup G_k| = k|G_1| - k$), alors on a une représentation constructive avec $F' = \emptyset \neq G_1$.

Soient maintenant une racine minimum B du groupe $L = F_2{}^n$ et son propre sous-ensemble $B_1 \subset B$; désignons $\hat{B}_1 = L\backslash(B\backslash B_1 + B\backslash B_1)$. Soit une représentation constructive $\hat{B}_1 = \{a_1, \ldots, a_{2f}\} \cup F'$ (elle existe d'après le lemme 2 pour un α-système $G = F_2{}^n$, où l'opération α est une addition du groupe $F_2{}^n$); il est clair que $V = F' \cup (0)$ est un sous-groupe de $F_2{}^n$, puisque a, $b \in V \Rightarrow a + b \in V$ en vertu de (c) et $a + b = a - b$ en vertu de $b \in F_2{}^n \Rightarrow b + b = 0$. On donne une représentation $\hat{B}_1 \cup (0) = G_1 \cup \ldots \cup G_t$ sous forme d'une réunion de sous-groupes de $F_2{}^n$ se recoupant par paire uniquement au zéro (une telle représentation existe toujours et peut ne pas être unique).

THÉORÈME 1. *On a*

(1) $|B_1| \leqq f + \beta(V) - 1 = \frac{1}{2}(|\hat{B}_1| - |V| + 2\beta(V) - 1) \leqq \frac{1}{2}(|\hat{B}_1| + 1)$;

(2) $|B_1| \leqq \beta(G_1) + \ldots + \beta(G_t) - t$.

En effet, démontrons (2) pour commencer. Soient $T_1, \ldots, T_t$ des racines minimum de groupes $G_1, \ldots, G_t$, respectivement et désignons $T_1 \cup \ldots \cup T_t = T$. Il est clair que $T + T = G_1 \cup \ldots \cup G_t = \hat{B}_1 \cup (0) = L\backslash(B\backslash B_1 + B\backslash B_1) \cup (0)$ et $T \cup (B\backslash B_1)$ est une racine de $L = F_2{}^n$. Donc, $|B| \leqq |T \cup (B\backslash B_1)|$. Sans perdre la généralité, posons que $\{0\} \in \bigcap_{1 \leqq i \leqq t} T_i$; pour un $a^* \in B\backslash B_1$ en remplaçant tous les T_i, $1 \leqq i \leqq t$, par $T_i{}^* = \{a + a^*/a \in T_i\}$ nous obtenons tous $T_i{}^* + T_i{}^* = T_i + T_i = G_i$ et $a^* \in (B\backslash B_1) \cap \bigcap_{1 \leqq i \leqq t} T_i{}^*$. Nous obtenons $|B_1| \leqq |T_1| + \ldots + |T_t| - t$, c'est-à-dire l'estimation (2).

L'égalité de (1) découle de ce que $|\hat{B}_1| = 2f + |V| - 1$. L'inégalité de (1) à droite découle du Lemme 1. (A ce propos, elle se transforme en égalité si et seulement si le groupe V contient 2, 4 ou 8 éléments.) Pour démontrer l'inégalité de (1) à gauche désignons par T une racine minimum de groupe V et *supposons* qu'il existe un ensemble S tel que $|S \cup (B\backslash B_1)| \leqq f + |B\backslash B_1|$, $S + S \supset \hat{B}_1\backslash F'$. Alors $S \cup (B\backslash B_1) \cup T$ est une racine de $L = F_2{}^n$, puisque $(\hat{B}_1\backslash F') \cup ((B\backslash B_1) + (B\backslash B_1)) \cup V = F_2{}^n$; donc,

$$|B| \leqq |S \cup (B\backslash B_1) \cup T| \leqq f + |B| - |B_1| + \beta(V) - 1$$

et (1) est démontré. (Le terme -1 apparaît, puisque en prenant certains $a_1{}^* \in B\backslash B_1$, $a_2{}^* \in T$ et en remplaçant T par $T^* = \{a + a_1{}^* + a_2{}^*/a \in T\}$, nous obtenons $T^* + T^* = T + T = V$ et $a_1{}^* \in (B\backslash B_1) \cap T^*$.) Ainsi, pour démontrer le théorème il ne reste qu'à construire l'ensemble S.

Pour cela, utilisons les propriétés de l'ensemble ordonné $\{a_1, \ldots, a_{2f}\} = \hat{B}_1\backslash F'$. Désignons $B\backslash B_1 = C = \{c_{2f+1}, \ldots, c_{2f+|C|}\}$. Pour la représentation constructive envisagée on a $G\backslash F = F_2{}^n\backslash\hat{B}_1 = F_2{}^n\backslash(F_2{}^n\backslash(B\backslash B_1 + B\backslash B_1)) = C + C$ et, en vertu de b) on a (pour chaque $1 \leqq i \leqq f$) $i \in I$ ou $i \in J$, où nous définissons

$$i \in I \Leftrightarrow a_{2i-1} + a_{2i} \in C + C, \qquad i \in J \Leftrightarrow a_{2i-1} + a_{2i} \in \{a_1, \ldots, a_{2i-2}\}.$$

Désignons par α_i un nombre j (en général non unique) tel que $a_{2i-1} + a_{2i} + c_{\alpha_i} \in C$ pour $i \in I$, $a_{2i-1} + a_{2i} \in \{a_{2\alpha_i-1}, a_{2\alpha_i}\}$ pour $i \in J$. Il est clair que $i \in I$ pour $i = 1$ et que $\alpha_i < i$ pour $i \in J$, puisque au cas contraire

$$\{a_1, \ldots, a_{2i-2}\} \cap \{a_{2i-1}, \ldots, a_{2f}\} = (0),$$

ce qui contredit la propriété (a) de la représentation constructive. (A ce propos, remarquons ici que des propriétés (a), (b) il découle aisément $\{a_1, \ldots, a_{2f}\} \cap (0) = \emptyset$ pour la représentation constructive d'un sous-ensemble fini de tout groupe G.) Ainsi, nous pouvons donner la définition suivante par induction

$$s_i = a_{2i-1} + c_{\alpha_i} \text{ pour } i \in I, \qquad s_i = a_{2i-1} + s_{\alpha_i} \text{ pour } i \in J.$$

Désignons

$$S = \left(\bigcup_{i \in I} \{s_i, c_{\alpha_i}, a_{2i-1} + a_{2i} + c_{\alpha_i}\} \right) \cup \left(\bigcup_{i \in J} \{s_i\} \right).$$

Par commodité, introduisons encore les désignations $\alpha_i^2 = \alpha_{\alpha_i}$ pour $\alpha_i \in J$, α_i^2 est le numéro de l'élément $a_{2i-1} + a_{2i} + c_{\alpha_i}$ dans C pour $\alpha_i \in I$; désignons également $s_j = c_j$ pour $2f \leqq j \leqq 2f + |C|$. Alors nous obtenons

$$S = \{s_1, \ldots, s_f\} \cup \left(\bigcup_{i \in I} \{s_{\alpha_i}, s_{\alpha_i^2}\} \right), \quad s_i = a_{2i-1} + s_{\alpha_i} \quad \text{pour } 1 \leqq i \leqq f.$$

Il est clair que $|S \cup (B \backslash B_1)| \leqq f + |C| = f + |B| - |B_1|$, puisque $s_{\alpha_i}, s_{\alpha_i^2} \in C = B \backslash B_1$ pour $i \in I$. Il reste à montrer que

$$S + S \supset \hat{B}_1 / F' = \{a_1, \ldots, a_{2f}\}.$$

Pour $1 \leqq i \leqq f$ on a $s_i + s_{\alpha_i} = (a_{2i-1} + s_{\alpha_i}) + s_{\alpha_i} = a_{2i-1}$. Dans le cas restant $i \in J$ envisageons deux possibilités:

$$i \in J_1 \Leftrightarrow a_{2i-1} + a_{2i} = a_{2\alpha_i - 1}, \qquad i \in J_2 \Leftrightarrow a_{2i-1} + a_{2i} = a_{2\alpha_i}.$$

Pour $i \in J_1$ on a $s_i + s_{\alpha_i^2} = (a_{2i-1} + s_{\alpha_i}) + (s_{\alpha_i} - a_{2\alpha_i - 1}) = a_{2i}$. Pour $i \in J_2$ on a $s_i + (s_{\alpha_i} - a_{2\alpha_i}) = (s_i + s_{\alpha_i}) - a_{2\alpha_i} = a_{2i-1} - a_{2\alpha_i} = a_{2i}$ et, donc, il reste à démontrer que $s_{\alpha_i} - a_{2\alpha_i} \in S$. Pour $\alpha_i \in I$ ou $\in J_1$, c'est évident puisque $s_{\alpha_i} - a_{2\alpha_i} = (a_{2\alpha_i - 1} + c_{\alpha_i^2}) - a_{2\alpha_i} = c_{\alpha_i^2} + (c_{\alpha_i^2} + c_{\alpha_i^3}) = s_{\alpha_i^3} \in S$ ou $s_{\alpha_i} - a_{2\alpha_i} = s_{\alpha_i} - (a_{2\alpha_i^2 - 1} - a_{2\alpha_i - 1}) = s_{\alpha_i^2} - a_{2\alpha_i^2 - 1} = s_{\alpha_i^3} \in S$. Pour $\alpha_i \in J_2$ on a $s_{\alpha_i} - a_{2\alpha_i} = s_{\alpha_i} - (a_{2\alpha_i^2} - a_{2\alpha_i - 1}) = s_{\alpha_i^2} - a_{2\alpha_i^2} = \ldots = s_{\alpha_i^\mu} - a_{2\alpha_i^\mu}$, où $\alpha_i^u \in (I \cup J) \backslash J_2 = I \cup J_1$ (u existe, puisque $j \in J \Rightarrow \alpha_j < j$). (Il est clair que plus haut par α_i^3 on désigne $\alpha_{\alpha_i^2}$.) Ainsi, $S + S \supset \{a_1, \ldots, a_{2f}\}$ et le théorème est démontré. (Remarquons que $a_{2i-1} = s_i + s_{\alpha_i}$ pour tous $1 \leqq i \leqq f$, mais $a_{2i} = s_i + s_{\alpha_i^2}$ uniquement pour $1 \leqq i \leqq f$, $i \notin J_2$.)

D'après $\hat{B}_1 = L \backslash (B \backslash B_1)^2 = B^2 \backslash (B \backslash B_1)^2 = (B + B_1) \backslash ((B + B_1) \cap (B \backslash B_1)^2)$ on voit que l'estimation (1) (on a en vue $|\hat{B}_1| \geqq 2|B_1| - 1$) peut être considérablement renforcée dans des cas particuliers. Mais les deux estimations (1), (2) se transforment en égalité, par exemple, pour $B = \{00, 01, 10\}$, $B_1 = \{01, 10\}$, puisqu'ici $\hat{B}_1 = \{01, 10, 11\}$. (2) est plus fort que (1) pour $\min |G_i| > 2^3$ et plus faible que (1) pour $[\max |G_i|, |B_1|] \ni 2^1$ ou 2^2 ou 2^3 (pour cela, il suffit de remarquer que pour $|G_1| = \ldots = |G_t| = 2^q$ l'estimation (2) prend la forme $|B_1| \leqq t(\beta(G_1) - 1) = |\hat{B}_1|(2^q - 1)^{-1}(\beta(G_1) - 1)$, d'où, à l'aide du lemma 1 et du tableau des racines connues nous obtenons

$$|B_1| \leqq |\hat{B}_1|(2^q - 1)^{-1}(2^{[q/2]} + 2^{q-[q/2]} - 3)$$

pour $q \geqq 6$ et $|B_1|/|\hat{B}_1| \leqq 1, 2/3, 4/7, 1/3, 9/31$ pour $q = 1, 2, 3, 4, 5$.) De $\{0\} \in B \backslash B_1$,

$$|B \backslash B_1| \leqq |(B \backslash B_1)^2| \leqq \binom{|B \backslash B_1|}{2} + 1,$$

$|B\backslash B_1| = \beta(L) - |B_1|$, $|\hat{B}_1| = 2^n - |(B\backslash B_1)^2|$ il découle que

$$(3) \quad 2^n - \beta(L) + |B_1| \geqq |\hat{B}_1| \geqq 2^n - 1 - \binom{\beta(L) - |B_1|}{2}.$$

Pour comparer les estimations (1), (3) remarquons que, par exemple, pour $n = 5$ on a

$$2^n - 1 - \binom{\beta(L) - |B_1|}{2} \leqq 2|B_1| - 1 \Leftrightarrow |B_1| \leqq 2.$$

On peut étendre le Théorème 1 à n'importe quel groupe élémentaire abélien L d'ordre p^n, en définissant, en qualité de "rôle relatif" du sous-ensemble B_1, $(0) \not\subseteq B_1 \subset B$ de racine minimum B de L, le nombre $|\hat{B}_1|$, où $\hat{B}_1$ est tout ensemble minimum tel que

$$\{0\} \neq a \in L, \qquad (a) \cap (B\backslash B_1 - B\backslash B_1) = (0) \Rightarrow (a) \cap \hat{B}_1 \neq (0).$$

Il n'est pas difficile en généralisant le Lemme 2 de montrer qu'il existe une *représentation constructive* $\hat{B}_1 = \{a_1, \ldots, a_{2f}\} \cup F'$, où

(b′) pour tout $1 \leqq i \leqq f$ il existe un entier $k_i > 0$, tel que

$$k_i(a_{2i-1} - a_{2i}) \in (B\backslash B_1 - B\backslash B_1) \cup \{a_1, \ldots, a_{2i-2}\};$$

(c′) $a, b \in F' \Rightarrow (a - b) \cap F' \neq \emptyset$ (c'est-à-dire $V = \bigcup_{v \in F'} (v)$ est un groupe).
On peut démontrer que

$$(1') \quad |B_1| \leqq f + \beta(V) - 1 = \tfrac{1}{2}(|\hat{B}_1| - (|V| - 1)/(p - 1) + 2\beta(V) - 2).$$

(L'égalité découle de $|\hat{B}_1| = 2f + (|V| - 1)/(p - 1)$; l'inégalité est démontrée par analogie avec le théorème 1, mais cette méthode est plus encombrante.) Si $\bigcup_{a \in B_1} (a) = G_1 \cup \ldots \cup G_t$ est une représentation sous forme d'une réunion de sous-groupes se recoupant par paire uniquement au zéro, alors nous obtenons facilement la généralisation

$$(2') \quad |B_1| \leqq \beta(G_1) + \ldots + \beta(G_t) - t.$$

Indiquons une autre orientation de la généralisation du Théorème 1. Appelons *factorisation* du groupe $L = F_2{}^n$ la famille $A = \{A_1, \ldots, A_k\}$, où $A_1, \ldots, A_k \subset L$ et $A_1 + \ldots + A_k = L$. Soit une k-suite de positives $d = (d_1, \ldots, d_k)$; si $d_1|A_1| + \ldots + d_k|A_k| = \min$, alors appelons A factorisation *d-minimum*. (Pour $A_1 = \ldots = A_k$, $d_1 = \ldots = d_k > 0$, la factorisation correspond à une racine minimum de degré k de $L = F_2{}^n$). Soit encore une famille $A' = \{A_1', \ldots, A\}$ telle que $A_1' \subset A_1, \ldots, A_k' \subset A_k$; appelons "rôle relatif A' dans A'' le nombre $|(A, A')| = |L\backslash((A_1\backslash A_1') + \ldots + (A_k\backslash A_k'))|$ (ici, A, A', (A, A') sont analogues à B, B_1, $\hat{B}_1$ du Théorème 1). Généralisant le lemme 1, on peut obtenir une généralisation de (1), (2). Par exemple, si

$$(A, A') \cup (0) = G_1 \cup \ldots \cup G_t$$

et pour $1 \leqq i \leqq t$, $A_{i1}, \ldots, A_{ik}$ est une factorisation d-minimum de G_i, alors

$$(2'') \quad d_1|A_1'| + \ldots + d_k|A_k'| \leqq d_1 \sum_{1 \leqq j \leqq t} |A_{j1}| + \ldots + d_k \sum_{1 \leqq j \leqq t} |A_{jk}|.$$

Envisageons maintenant l'application de la notion de racine de groupe à un problème de la théorie algébrique des codes correcteurs. On présente à l'entrée du canal de transmission des éléments de l'ensemble X, tandis qu'à la sortie parviennent des éléments $x + y$ où $x \in X$ et $y \in Y$. Soit $(0) \subset X$, $Y \subset I$ nous appellerons X le *code* et Y le *bruit additif*. Si $x_1 + y_1 \neq x_2 + y_2$ pour tous $x_1, x_2 \in X$ et $y_1, y_2 \in Y$ $(x_1 \neq x_2)$, alors nous appellerons X *code correcteur du bruit* Y (dans ce cas, $X - X \cap Y - Y = (0)$ et un décodage régulier est possible à la sortie du canal). Un sous-ensemble du groupe L, corrigeant le bruit Y et ayant le nombre maximum d'éléments est désigné par $C(Y)$. On donne un entier m $(m > 1)$. Un bruit Y, tel que $|Y| = m$ et que le nombre $|C(Y)|$ est minimum, est appelé *m-bruit le pire* (pour correction).

Maintenant le nombre m et le m-bruit le pire Y sont fixés; $\bar{L}$ est le sous-groupe maximum de L, corrigeant Y; $\tilde{L}$ est un groupe tel que $\bar{L} \cap \tilde{L} = (0)$ et $\bar{L} + \tilde{L} = L$. Tout élément $a \in L$ est uniquement représentable sous la forme $a = \bar{a} + \tilde{a}$, où $\bar{a} \in \bar{L}$, $\tilde{a} \in \tilde{L}$. Soit $\tilde{Y}$ l'ensemble de tous les $\tilde{a}$ où $a \in Y$; C est un sous-ensemble maximum du groupe $\tilde{L}$ corrigeant $\tilde{Y}$.

THÉORÈME 2. *L'ensemble $\tilde{Y}$ est à la fois m-bruit le pire et une racine du groupe $\tilde{L}$. Ce faisant, $C + \bar{L} = C(\tilde{Y}) = C(Y)$.*

(a) Nous montrerons pour commencer que le code $C + \bar{L}$ corrige le bruit Y_2. Au cas contraire, il existe $c_1, c_2 \in C + \bar{L}$ et $y_1, y_2 \in Y (y_1 \neq y_2)$ tels que $c_1 + y_1 = c_2 + y_2$. Alors $(\bar{c}_1 + \tilde{c}_1) + (\bar{y}_1 + \tilde{y}_1) = (\bar{c}_2 + \tilde{c}_2) + (y_2 + \tilde{y}_2)$ d'où $(\bar{c}_1 + \bar{y}_1) - (\bar{c}_2 + \bar{y}_2) = (\tilde{c}_2 + \tilde{y}_2) - (\tilde{c}_1 + \tilde{y}_1)$. Mais la partie gauche $\in \bar{L}$, la partie droite $\in \tilde{L}$ et $\bar{L} \cap \tilde{L} = (0)$; donc, $\tilde{c}_2 + \tilde{y}_2 = \tilde{c}_1 + \tilde{y}_1$. Mais $\tilde{c}_2, \tilde{c}_1 \in C$ et $\tilde{y}_2, \tilde{y}_1 \in \tilde{Y}$, et le code C corrige le bruit $\tilde{Y}$; donc, $\tilde{y}_2 = \tilde{y}_1$, d'où $y_1 - \bar{y}_1 = y_2 - \bar{y}_2$ et l'égalité $\bar{c}_1 + \bar{y}_1 = \bar{c}_2 + \bar{y}_2$ se transforme en $\bar{c}_1 + y_1 = \bar{c}_2 + y_2$. Mais $\bar{c}_1, \bar{c}_2 \in L$ et $y_1, y_2 \in Y$, et le code $\bar{L}$ corrige le bruit Y; donc $y_1 = y_2$. La contradiction qui en résulte montre que le code $C + \bar{L}$ corrige le bruit Y.

(b) Montrons que $C + \bar{L} = C(\tilde{Y})$. Pour tout $\bar{a} \in \bar{L}$ nous désignerons $R(\bar{a}) = C(\tilde{Y}) \cap (\bar{a} + \tilde{L})$ et $\tilde{R}(\bar{a})$ comme l'ensemble de tous les $\tilde{r}$ où $r \in R(\bar{a})$. Il est évident que $|R(\bar{a})| = |\tilde{R}(\bar{a})|$. Mais $\tilde{R}(\bar{a}) \subset \tilde{L}$ et le code $\tilde{R}(\bar{a})$ corrige le bruit $\tilde{Y}$; donc, $|\tilde{R}(\bar{a})| \leqq |C|$, puisque $|C|$ est maximal. Nous obtenons

$$|C(\tilde{Y})| = \sum_{\bar{a} \in \bar{L}} |R(\bar{a})| = \sum_{\bar{a} \in \bar{L}} |\tilde{R}(\bar{a})| \leqq |C| \cdot |\bar{L}| = |C + \bar{L}|.$$

Mais le code $C + \bar{L}$ corrige le bruit $\tilde{Y}$ en vertu de la définition de C et de $\bar{L}$. Donc, $C + \bar{L} = C(\tilde{Y})$.

(c) Montrons que $\tilde{Y}$ est le m-bruit le pire et que $C(Y) = C + \bar{L}$. On a $|\tilde{Y}| = |Y| = m$ puisqu'au cas $|\tilde{Y}| < |Y|$ il existerait $y_1, y_2 \in Y$ $(y_1 \neq y_2)$ tels que $\tilde{y}_1 = \tilde{y}_2$, d'où $y_1 - y_2 = \bar{y}_1 - \bar{y}_2 \in \bar{L}$ et le groupe $\bar{L}$ ne corrigerait pas le bruit Y. D'après $a)$, $b)$ on voit que $|C(\tilde{Y})| = |C + \bar{L}| \leqq |C(Y)|$. Mais $|C(Y)| \leqq |C(\tilde{Y})|$ puisque $|\tilde{Y}| = m$ et Y est le m-bruit le pire. Donc, $C(Y) = C + \bar{L}$ et $\tilde{Y}$ est la m-bruit le pire.

(d) Le sous-ensemble $\tilde{Y}$ du groupe $\tilde{L}$ est sa racine, puisque au cas contraire il existerait un élément $\tilde{y}(\{0\} \neq \tilde{y} \in \tilde{L})$ tel que $(\tilde{Y} - \tilde{Y}) \cap (\tilde{y}) = (0)$ d'où

$(Y - Y) \cap (\bar{L} + (\tilde{y})) = (0)$ (c'est-à-dire que le groupe $\bar{L} + (\tilde{y})$ corrigerait le bruit Y) ce qui contredit la maximalité du groupe $\bar{L}$ corrigeant Y. Le Théorème 2 est démontré.

Il est facile de vérifier que pour $p = 2$ on a $|\tilde{L}| = \max |L_1|$ où $\beta(L_1) \leqq m$ (L_1 est un sous-groupe du groupe L); plus loin, $C = (0)$ et donc $C(\tilde{Y}) = \bar{L}$, $|C(\tilde{Y})| = |L|/|\tilde{L}|$, c'est-à-dire que $|C(\tilde{Y})|$ est un degré de 2. Ainsi, $|\tilde{Y}| = m$, $\tilde{Y} \subset L$, $\tilde{Y} + \tilde{Y} = \tilde{L}$, $|\tilde{L}| = \max |L_1|$ (où $\beta(L_1) \leqq m$). L'analogie avec la règle stratégique bien connue de minimisation de la possibilité de pénétration de l'adversaire au moyen d'une bonne disposition des ressources de défense données saute aux yeux (ici: minimisation du nombre d'éléments du code correcteur au moyen d'une disposition des m éléments du bruit). L'une des meilleures dispositions est la suivante: concentrer tous les m éléments dans la partie maximale du "front" (sous-groupe) et de façon que la "défense" de cette partie soit complètement assurée (aucun code non-nul dans ce sous-groupe ne pourra corriger, surmonter le bruit).

Il est aisé de démontrer le théorème analogue au Théorème 2, pour un m-bruit le pire à *détecter* (on dit que le code X *détecte* le bruit additif Y si $(X - X) \cap Y = (0)$). Précisément, parmi les m-bruits les pires pour détection, il existe un bruit $\tilde{Y}_1$ qui est *la racine de* 1-*ier degré* d'un sous-groupe $\tilde{L}$ de L (c'est-à-dire $Y' \cap ((a) \setminus (0)) \neq \emptyset$ pour $(0) \neq (a) \subset \tilde{L}'$). Ensuite, si on introduit par analogie la notion de *m-bruit le meilleur*, on peut montrer que le problème (dans le cas de détection) se ramène à la recherche pour un sous-ensemble donné A, $(0) \subset A \subset L$ et $|A| = m$ d'un groupe maximum $F(A)$ tel que $F(A) \subset A$; on peut montrer que si $F(A) \neq (0)$ alors $|F(A)| \geqq |L|/(|L| - |A| + 1)$ et que cette estimation est obtenue.

Ce travail est le développement de certains résultats de [1].

L'auteur exprime sa reconnaissance aux professeurs P. Camion et H. Hanani pour leurs précieuses remarques.

Bibliographie

1. M. Deza, *Codage dans les conditions d'un bruit additif arbitraire* (en russe), thèse soutenue au TSEMI de l'Académie des Sciences de l'URSS, Moscou, 1965
2. G. T. Diderrich and H. B. Mann, *Combinatorial problems in finite abelian groups*, A survey of combinatorial theory (J. N. Srivastava et al., eds., North-Holland Publ. Co., 1973, ch. 10, pp. 95–100).
3. P. Erdös, *Problems and results on combinatorial number theory*, A survey of combinatorial theory (J. N. Srivastava et al., eds., 1973, ch. 12, pp. 117–138).
4. P. Erdös and L. Moser, Calgary Conference (Gordon and Breach, New York, 1969, p. 506).
5. H. B. Mann, *Addition theorems* (Interscience Publishers, New York, 1965).

C.N.R.S.
Université Paris VII, U.E.R. de Mathématiques,
75005 Paris, France