CUBO A Mathematical Journal
Vol.11, Nº 02, (1–6). May 2009

Some Theoretical Issues Concerning Hamming Coding

Erika Griechisch
University of Pécs, College of Natural Sciences,
Institute of Mathematics and Informatics,
Ifjúság útja 6, Pécs, 7624, Hungary
email: `griechisch.erika@gmail.com`

ABSTRACT

The security of telecommunication largely depends on effective and safe coding. National security as well as the safety of the entire society also depends on how information is exchanged between government agencies. The security of information can also be guaranteed by a safe and effective coding system.

A Hamming code is a linear error-correcting code which can detect and correct single-bit errors. It can also detect, but not correct up to two simultaneous bit errors. For each integer $m > 1$ there is a code with the parameters $\{2^m - 1, 2^m - m - 1, 3\}$. The factorization of Abelian groups and the complete factor problem of 2-groups are closely related to the error-correcting Hamming codes. In this paper we will deal with the Rédei property of 2-groups.

RESUMEN

La seruridad en telecomunicaciones depende ampliamente de efectivos e seguros códigos. La seguridad nacional bien como la seguridad de la sociedad entera también depende de como la información es intercambiada entre agencias de govierno. La seguridad de información también puede ser garantizada por efectivos y seguros códigos.

Un código Hamming es un código linear error-corrección el cual puede detectar y corregir errores single-bit. Este puede también detectar, pero no corrigir dos errores bit simultaneos. Para todo entero $m > 1$ hay un código con los parametros $\{2^m - 1, 2^m - m - 1, 3\}$. La factorización de grupos abelianos y el problema de factor completo de 2-grupos son relativamente proximos de los códigos Hamming error-corrector. Este artículo trabaja con la propiedad de Rédei de 2-grupos.

Key words and phrases: *Factorization of Abelian groups, full-rank tiling, Rédei property, dancing link, exhaustive search.*

Math. Subj. Class.: *20K01, 05B45, 52C22, 68R05.*

1 Introduction

Let G be a finite Abelian group, with identity element e. Let $A_1, \ldots, A_n$ be given subsets of G. Then

$$A_1 \cdots A_n = \{a_1 \cdots a_n \mid a_i \in A_i\}$$

is a factorization of G, if $G = A_1 \cdots A_n$ and each $g \in G$ can be uniquely represented in the form $a_1 \cdots a_n$.

A subset A of G is normalized if $e \in A$. The factorization is called normalized if each factor is normalized,. Let $\langle A \rangle$ denote the smallest subgroup of G that contains A. It is called the span of A in G.

If G is a direct product of cyclic groups of order $t_1, \ldots, t_n$, then the type of G is $(t_1, \ldots, t_n)$. A group of type $(p, \ldots, p)$, where p is prime, is called an elementary-p-group, and the group of type $(t_1, \ldots, t_n)$, where each t_i is a power of p is called a p-group.

In this short paper we will restrict our attention to p-groups.

Definition 1. G has the Rédei property if from each normalized factorization $G = AB$ it follows that either $\langle A \rangle \neq G$ or $\langle B \rangle \neq G$.

In the special case, when $G = \{e\}$, G has the Rédei property by definition. The reason is the following. $\{e\}$ has only one factorization, namely $\{e\}\{e\}$. In this case $\langle A \rangle = \langle B \rangle = G$. In 1970 L. Rédei conjectured if $G = AB$ is a normalized factorization of G and G is of type (p, p, p), then either $\langle A \rangle \neq G$ or $\langle B \rangle \neq G$. This was published as problem 5 in [3].

The following facts are known about the Rédei property. Let p be a prime and let F_p be a family of p-groups whose types are depicted in Table 1 or a subgroup of such a group. Szabó proved in [4], that if G is a p-group with the Rédei property, then G is a member of the F_p family.

$p = 2$	$(2^\alpha, 2^\beta, 2, 2)$	$\alpha \geq 3, \beta \geq 2$
	$(2^\alpha, 2, 2, 2, 2, 2)$	$\alpha \geq 3$
	$(2^2, 2^2, 2, 2, 2, 2, 2, 2, 2)$	
$p = 3$	$(3^\alpha, 3^\beta, 3)$	$\alpha \geq 2, \beta \geq 2$
	$(3^\alpha, 3, 3, 3)$	$\alpha \geq 2$
	$(3, 3, 3, 3, 3)$	
$p \geq 5$	(p^α, p^β, p)	$\alpha \geq 1, \beta \geq 1$

Table 1: The F_p family

We will show, that a group of type $(4, 4, 2, 2)$ does not have the Rédei property. As a consequence of this fact is that the earlier list will change. This is the main result of this paper.

2 Mathematical Results

Lemma 1. Let G be a group of type $(4,4,2,2)$. Then G has a full-rank factorization.

Proof. Let x_1, x_2, y_1, y_2 be a basis of G, where $|x_1| = |x_2| = 4, |y_1| = |y_2| = 2$. Set

$$A = \{e, x_1, x_2, x_1x_2y_1, x_1x_2y_1, x_1x_2^2y_1y_2, x_1^2x_2y_1y_2, x_2y_1y_2, x_1^2x_2^2y_1y_2\}$$

and let

$$B = \{e, y_2, x_1x_2^2y_2, x_1x_2^3y_1, x_1^2x_2, x_1^2x_2^3y_2, x_1^3x_2y_1y_2, x_1^3x_2^2\}.$$

It can be easily verified, that the product AB is direct. For convenience we exhibited the elements A and B in Table 2 using only their exponents.

A	B
0000	0000
1000	0001
0100	1201
1110	1310
1101	2100
1211	2301
2111	3111
2211	3200

Table 2: Factors A and B

Table 3 summaries the elements of product AB.

Clearly $\langle A\rangle = \langle B\rangle = G$. Furthermore

$e, x_1 \in A \vdash x_1 \in \langle A\rangle$.
$e, x_2 \in A \vdash x_2 \in \langle A\rangle$.
$x_1, x_2 \in \langle A\rangle \vdash x_1x_2y_1 \in A \vdash y_1 \in \langle A\rangle$.
$x_1x_2y_2 \in A, x_1, x_2 \in \langle A\rangle \vdash y_2 \in \langle A\rangle$.

Thus $x_1, x_2, y_1, y_2 \in \langle A\rangle$ and so $\langle A\rangle = G$.

$e, y_2 \in B \vdash y_2 \in \langle B\rangle$.
$x_1x_2^2y_2, y_2 \in B \vdash x_1x_2^2 \in \langle B\rangle$.
$x_1^2x_2 \in B, x_1x_2^2 \in \langle B\rangle \vdash x_1^3x_2^3 \in \langle B\rangle$.
$x_1^3x_2^2 \in B, x_2 \in \langle B\rangle \vdash x_2 \in \langle B\rangle$.
$x_1x_2^2, x_2 \in \langle B\rangle \vdash x_1 \in \langle B\rangle$.
$x_1x_2^3y_1 \in B, x_1, x_2, y_2 \in \langle B\rangle \vdash y_1 \in \langle B\rangle$.

	0000	0001	1201	1310	2100	2301	3111	3200
0000	0000	0001	1201	1310	2100	2301	3111	3200
1000	1000	1001	2201	2310	3100	3301	0111	0200
0100	0100	0101	1301	1010	2200	2001	3211	3300
1110	1110	1111	2311	20000	3210	3011	0201	0310
1101	1101	1100	2300	2011	3201	3000	0210	0301
1211	1211	1210	2010	2101	3311	3110	0300	0011
2111	2111	2110	3310	3001	0211	0010	1200	1311
2211	2211	2210	3010	3101	0311	0110	1300	1011

Table 3: The product A and B

Similarly, $x_1, x_2, y_1, y_2 \in \langle B \rangle$ and therefore $\langle B \rangle = G$. □

Notice that the construction in Lemma 1 was accomplised by an exhaustive computer search using D.E. Knuth [1] dancing links algorithm.

Theorem 1 Let F_2' be a family of 2-groups whose types are given in Table 4 or a subgroup of such a group. If a 2-group G has the Rédei property, then G is a member of the F_2' family.

Proof. Let G be a group of type

$$(2^{\alpha(1)}, \ldots, 2^{\alpha(r)}, 2^{\beta(1)}, \ldots, 2^{\beta(s)}, 2^{\gamma(1)}, \ldots, 2^{\gamma(t)}),$$

where

$$\alpha(1) \geq \cdots \geq \alpha(r) \geq 3,$$

$$\beta(1) = \cdots = \beta(s) = 2,$$

$$\gamma(1) = \cdots = \gamma(t) = 1.$$

$(2^\alpha, 2^\beta, 2)$	$\alpha, \beta \geq 2$
$(2^\alpha, 2, 2, 2, 2, 2)$	$\alpha \geq 3$
$(2^2, 2, 2, 2, 2, 2, 2, 2, 2)$	

Table 4: The F_2' family

Suppose that G has the Rédei property. It is sufficient to shown that G is a member of F_2' family. If $r + s \geq 3$, then G has a subgroup H of type $(4, 4, 4)$. Now by [5], H has a full-rank factorization and so by Theorem 1 in [4] G also has a full-rank factorization. For the remaining part of the the proof we may assume that $0 \leq r + s \leq 2$.

We distinguish between the following cases listed in Table 5.

Case	r	s	t
1	0	0	≤ 9
2	0	1	≤ 8
3	0	2	≤ 1
4	1	0	≤ 4
5	1	1	≤ 1
6	2	0	≤ 1

Table 5: Cases

Case 1 If $r = 0, s = 0$ and $t \geq 10$, then G has a subgroup H of the type $(2, ..., 2)$. By [2], H admits a full-rank factorization and so does G as well. Thus $t \leq 9$ as required

Case 2 If $r = 0, s = 1$ and $t \geq 9$, then G has a subgroup of the type $(4, \overbrace{2, \ldots, 2}^{9})$, then G has a subgroup H of type $(\overbrace{2, \ldots, 2}^{10})$. By [2], H has a full-rank factorization so does G as well. Thus $t \leq 8$ as required.

Case 3 If $r = 0, s = 2$ and $t \geq 2$, then G has a subgroup of the type $(4, 4, 2, 2)$ which has full-rank factorization by Lemma 1. So G has a full-rank factorization also. Thus $t \leq 1$ as required.

Case 4 If $r = 1, s = 0, t \geq 5$, then G has a subgroup of the type $(8, 2, 2, 2, 2, 2)$ and this subgroup has full-rank factorization by [4]. So G also has a full-rank factorization. Thus $t \leq 4$ as required.

Case 5 If $r = 1, s = 1, t \geq 2$, then G has a subgroup of the type $(4, 4, 2, 2)$ which has full-rank factorization by Lemma 1. So G has a full-rank factorization also. Thus $t \leq 1$ as required.

Case 6 If $r = 2, s = 0, t \geq 2$, then G has a subgroup of the type $(8, 8, 2, 2)$ which has a subgroup of type $(4, 4, 2, 2)$. Thus G has a full-rank factorization by Lemma 1. Therefore $t \leq 1$ is required.

Thus the proof is completed. □

Acknowledgement

The help of Péter Császár providing the implementation of the exact cover algorithm, is highly appreciated.

Received: March 21, 2008. Revised: April 29, 2008.

References

[1] Knuth, D.E., *Dancing links, in Millennial Perspectives in Computer Science*, J. Davies, B. Roscoe, and J. Woodcock, Eds., Palgrave Macmillan, Basingstoke, 2000, pp. 187–214.

[2] Östergard, P.R.J. and Vardy, A., *Resolving the existence of full-rank tilings of binary Hamming spaces*, SIAM Journal of Discrete Mathematics, Vol. **18**, No. 2 (2004), pp. 382–387.

[3] Rédei, L., *Lückenhafte Polynome über Endlichen Körpern*, Birkhäuser Verlag, Basel 1970, (English translation: Lacunary Polynomials over Finite Fields, North-Holland, Amsterdam, 1973).

[4] Szabó, S., *Factoring finite Abelian groups by subsets with maximal span*, SIAM Journal of Discrete Mathematics, Vol. **20**, No. 4 (2006), pp. 920–931.

[5] Szabó, S., *Topics in Factorization of Abelian Groups*, Birkhäuser, 2004.