Riv. Mat. Univ. Parma (4) 17 (1991), 325-331

P. R. FUCHS (*)

A decoding method for planar near-ring codes (**)

Introduction

Let N be a near-ring and $n, m \in N$. Define *an equivalence relation* $\equiv$ *on* N by $n \equiv m$ if $kn = km$ for all $k \in N$. Then N is called *planar* if there are at least 3 equivalence classes w.r.t. $\equiv$ and every equation of the form $xn = xm + k$, where $n, m, k \in N$, $n \not\equiv m$, has a unique solution.

To construct a planar near-ring on a group G is nothing else than to construct a group of fixed point free automorphisms on G. For if N is planar and $n \in N$, $n \not\equiv 0$, then ϕ_n: $N \to N$, $\phi_n(k) = kn$, $k \in N$,is a f.p.f. automorphism, i.e. if $\phi_n(k) = k$ for some $k \in N$ then $k = 0$ or ϕ_n is the identity map on N. Moreover, $\Phi = \{\phi_n | n \not\equiv 0\}$ forms a group. The order of Φ is equal to $|N/_{\equiv}|$, the number of equivalence classes w.r.t. $\equiv$. Conversely, if Φ is a f.p.f. group of automorphisms on a group G and $R = \{\gamma_i | i \in I\}$ is a (not necessarily complete) set of representatives of the orbits $\Phi\gamma$, then $(G, +, \cdot_R)$ forms a planar near-ring if we define $\gamma \cdot_R \delta = 0$ for $\delta \notin \cup\{\Phi\gamma_i | i \in I\}$ and $\gamma \cdot_R \delta = \phi(\gamma)$, if $\delta \in \Phi\gamma_i$ for some $i \in I$ and $\phi \in \Phi$ is the (unique) automorphism which maps γ_i into δ. All of these results are well-known and mainly due to Ferrero $[2]_1$.

Example 1. As a specific example due to J. R. Clay $[1]_1$ let F be a finite field and let U be a subgroup of F^*. Then U acts as a group of f.p.f. automorphisms by right multiplication. The nonzero orbits are just the cosets of U in F^*. By our construction above we obtain a planar near-ring.

Due to several connections with geometry and combinatorics planar near-rings have received a lot of interest. In all of the following we let N be a finite inte-

(*) Indirizzo: Department of Mathematics, Johannes Kepler University, A-4040 Linz.

(**) MR classification: 16Y30, 14B35; 05B05. – Ricevuto: 2-X-1991.

gral planar near-ring and let Φ denote the f.p.f. automorphism group associated with N. Also, N^* shall denote the set $N \setminus \{0\}$. Then N gives rise to a balanced incomplete block design as follows.

Theorem 2 (Clay [1]$_2$ Thm. 2). *Let N be a finite integral planar near-ring and $\mathcal{B} = \{nN^* + m \mid n,\ m \in N,\ n \neq 0\}$. Then $(N, \mathcal{B})$ is a* BIBD *with parameters* $v = |N|,\ k = |\Phi| = |N/_{\equiv}|,\ b = \dfrac{v(v-1)}{k},\ r = v-1,\ \lambda = k-1.$

Sets of the form $nN^* + m$ are called *blocks*. The number of blocks b in Theorem 2 is evident from the following result.

Theorem 3 (Clay [1]$_2$ Prop. 1). *Let $nN^* + m$, $pN^* + q$ be blocks. Then $nN^* + m = pN^* + q$ if and only if $m = q$ and $nN^* = pN^*$.*

There are several other ways to obtain a BIBD from a planar near-ring. For instance, it was shown by Ferrero [2]$_2$ that $(N, \mathcal{B})$ with $\mathcal{B} = \{nN + m \mid n \in N^*\}$ «often», but not always forms a BIBD.

We now associate two different codes to the BIBD obtained in Theorem 2.

(1) *The row code $\mathcal{C}_1(N)$.*

Here we associate to each block $B = nN^* + m$ a function $c_B : N \to \{0, 1\}$, where $c_B(p) = 1$ if $p \in B$ and $c_B(p) = 0$ otherwise. Then $\mathcal{C}_1(N) = \{c_B \mid B \in \mathcal{B}\} \subseteq \{0,\ 1\}^N$. All $c_B \in \mathcal{C}_1(N)$ have weight k, i.e. $|\{p \mid c_B(p) = 1\}| = k$.

(2) *The column code $\mathcal{C}_2(N)$.*

For the column code we associate to each point $p \in N$ a function $c_p : \mathcal{B} \to \{0, 1\}$, where $c_p(B) = 1$ if $p \in B$ and $c_p(B) = 0$ otherwise. Then $\mathcal{C}_2(N) = \{c_p \mid p \in N\} \subseteq \{0, 1\}^{\mathcal{B}}$. All $c_p \in \mathcal{C}_2(N)$ have weight r.

A study of these (nonlinear) codes has been initiated in [3] and [4]. In this paper we are concerned with decoding methods for $\mathcal{C}_1$ and C_2.

First we consider the row code $\mathcal{C}_1(N)$. Let $N = \{p_1, \ldots, p_v\}$ and $\mathcal{B} = \{B_1, \ldots, B_b\}$ be any enumeration of the points and the blocks. Later on we find it convenient to work with a special enumeration of the points. The $b \times v$ incidence matrix $A = (\alpha_{ij})$ of the design $(N, \mathcal{B})$ is then defined by $\alpha_{ij} = 1$ if $p_j \in B_i$ and

$\alpha_{ij} = 0$ otherwise. Thus each codeword $c_B \in \mathcal{C}_1(N)$ can be represented as a row of the incidence matrix A. It is easy to find the minimal distance $d_{\min}$ and the error-correction capability of $\mathcal{C}_1(N)$.

Proposition 4 ([3], Prop. 1.1). *Let* $\mu = \max\{|B_1 \cap B_2| \,|\, B_1, B_2 \in \mathcal{B}, B_1 \neq B_2\}$. *Then*: (1) $d_{\min} = 2(k-\mu)$. (2) $e \leqslant k - \mu - 1$ *errors can be corrected.*

Now suppose that we send a codeword c_B, $B = nN^* + m$, $n \neq 0$, through a channel. The receiver on the other side of the channel obtains a possibly different sequence $c \in \{0, 1\}^N$. His task is to determine n, m. For each $p \in N$ such that $c(p) = 1$ one obtains an equation $p = nl + m = \phi_l(n) + m$ for the unknown pair (n, m). Let E denote the set of all those equations. If errors have occured in the transmission, then E will be inconsistent. But from Proposition 4 we know that if the number of errors is less than or equal $k - \mu - 1$, then n, m can be recovered. Thus we have to look for a solvable subsystem whose unique solution is (n, m). For a real number x let $[x]$ denote the least integer $z \geqslant x$.

Proposition 5. *Let* c *denotes the received sequence and let* $z = |\{p | c(p) = 1\}|$. *Suppose that not more than* $k - \mu - 1$ *errors have been made. Then*: (1) $2k - \mu - 1 \geqslant z \geqslant \mu + 1$. (2) *Every subsystem* $E' \subseteq E$ *with* $|E'| \geqslant [\frac{z+\mu+1}{2}]$ *has at most one solution* (s, t). (3) *There exists a solvable subsystem* $E' \subseteq E$ *with* $|E'| \geqslant [\frac{z+\mu+1}{2}]$. *If* (n, m) *is the solution of any such system* E', *then* c_B, *where* $B = nN^* + m$, *has been sent.*

Proof. Let c_B, $B = nN^* + m$, $n \neq 0$, denote the transmitted codeword.

(1) If $z < \mu + 1$, then $c_B(p) = 1$ and $c(p) = 0$ for more than $k - \mu - 1$ points p, since c_B has weight k. If $z > 2k - \mu - 1$, then $c_B(p) = 0$ and $c(p) = 1$ for more than $k - \mu - 1$ points p.

(2) Suppose (s_1, t_1), (s_2, t_2) are both solutions of E'. Then there exists at least $[\frac{z+\mu+1}{2}]$ points p such that $p \in (s_1 N^* + t_1) \cap (s_2 N^* + t_2)$. By (1) $z \geqslant \mu + 1$, hence $[\frac{z+\mu+1}{2}] \geqslant \mu + 1$, a contradiction.

(3) Let $z' \leqslant z$ denote the number of points p such that $c_B(p) = c(p) = 1$. Then the number e of errors made in the transmission is given by $e = z - z' + k - z' \leqslant k - \mu - 1$. Thus $z' \geqslant [\frac{z+\mu+1}{2}]$. These z' points determine a

set $E' \subseteq E$ of equations for which (n, m) is the (unique) solution. It sufficies to show that the distance $d(c, c_B)$ between c and c_B is less than or equal to $k-\mu-1$. Since (n, m) solves E', there are at most $z-[\frac{z+\mu+1}{2}]$ points p such that $c(p)=1$ and $c_B(p)=0$. Also there are at most $k-[\frac{z+\mu+1}{2}]$ points p such that $c(p)=0$ and $c_B(p)=1$. Consequently $d(c, c_B) \leqslant z-[\frac{z+\mu+1}{2}] + k - [\frac{z+\mu+1}{2}] \leqslant k-\mu-1$.

The following example shows that in general we have to take a solvable subsystem E' with at least $[\frac{z+\mu+1}{2}]$ equations in order to decode correctly.

Example 6. Let F denote the prime field with 13 elements and $U=\{8, 12, 5, 1\} \leqslant F^*$. According to Example 1 we obtain a planar near-ring N and therefore a BIBD with parameters $(v, b, r, k, \lambda)=(13, 39, 12, 4, 3)$ by Theorem 2. Thus $\mathcal{C}_1(N)$ consists of 39 codewords of length 13 and weight 4. By Table III in Clay $[1]_2$ N is a «circular» planar near-ring which means that 3 points determine a unique block. Consequently $\mu=2$ and $\mathcal{C}_1(N)$ is a single error-correcting code. Consider the block $B := 2N^*+1 \doteq 2\cdot U+1=\{4, 12, 11, 3\}$. If we let $p_1=0$, $p_2=1, \ldots, p_{13}=12$, then c_B corresponds to the sequence 0001100000011. Suppose that we receive 0011100000011, i.e. one error has been made. Then the three equations $2=\phi_1(s)+t$, $3=\phi_2(s)+t$, $11=\phi_3(s)+t$ form a solvable subsystem E'. Since $2, 3, 11 \in 3\cdot U$ and N is circular $3\cdot U \neq 2\cdot U+1$ is its unique solution. Thus we need at least $[\frac{z+\mu+1}{2}]=4$ equations to decode correctly.

Now let $\mathcal{F}=\{F\}$ be a fibration on the group $(N, +)$, i.e. $\mathcal{F}$ has the following properties:

(1) Each $F \in \mathcal{F}$ is a subgroup of $(N, +)$ and $F \neq \{0\}$. (2) $\cup\{F | F \in \mathcal{F}\}=G$. (3) For each $F, F' \in \mathcal{F}$ either $F=F'$ or $F \cap F'=\{0\}$ holds.

Further we require that $\mathcal{F}$ is Φ-invariant, i.e. $\Phi(F) \subseteq F$ for every $F \in \mathcal{F}$. Thus, each $F \in \mathcal{F}$ is a union of orbits w.r.t. the action of Φ. It will be evident from our next results that the number of orbits in each fiber $F \in \mathcal{F}$ should be as small as possible. Once we have chosen such a suitable fibration $\mathcal{F}=\{F_1, \ldots, F_t\}$, where

$F_i = \cup\{n_{ij}N \mid 1 \leqslant j \leqslant j_i\}$, $1 \leqslant i \leqslant t$, we can list the points blockwise as follows

$$\begin{array}{ccc} & F_1^* & F_{0t}^* \\ 0 & n_{11}N^* \cdots\cdots n_{1j_1}N^* \cdots\cdots\cdots\cdots & n_{t1}N^* \cdots\cdots n_{tj_t}N^*. \end{array}$$

According to this enumeration of the points we define the $b \times v$ incidence matrix of our design $(N, \mathscr{B})$. As far as the row code is concerned one can use any enumeration of the blocks.

Now suppose that c_B, $B = nN^* + m$ is the transmitted codeword and that c has been received. As before let $E = \{p \mid c(p) = 1\} = \{p_1 \ldots p_z\}$. Also let $E^* = \{p \in E \mid c(p) = 1 \text{ is correct}\}$ and $e_i = |\{p \in F_i \mid c(p) = 1\}|$, $1 \leqslant i \leqslant t$. Using the above enumeration of the points it is easy to determine whethern n, m belong to a common fiber or not.

Theorem 7. *If n, m belong to a common fiber, then $e_j \geqslant [\frac{z+\mu+1}{2}]$ for some $1 \leqslant j \leqslant t$. Conversely, if $e_i \geqslant [\frac{z+\mu+1}{2}]$, then n, $m \in F_i$.*

Proof. If $n, m \in F_j$ then $c_B(p) = 0$ for all $p \notin F_j$. By Proposition 5 $|E^*| \geqslant [\frac{z+\mu+1}{2}]$, hence $e_j \geqslant [\frac{z+\mu+1}{2}]$. Now suppose that $e_i \geqslant [\frac{z+\mu+1}{2}]$, but either n or m is not an element of F_i. Let p_1, $p_2 \in (nN^* + m) \cap F_i$, say $p_1 = \phi_1(n) + m$, $p_2 = \phi_2(n) + m$. Then $p_1 - p_2 = (\phi_1 - \phi_2)(n) \in F_i$. If $n \notin F_i$, then, since all fibers are Φ-invariant, we have that $(\phi_1 - \phi_2)(n) = 0$, hence $p_1 = p_2$. If $n \in F_i$, then by our assumption $m \notin F_i$, hence $(nN^* + m) \cap F_i = \phi$, since $m \neq 0$. In any case $|(nN^* + m) \cap F_i| \leqslant 1$. Since $|E^*| \geqslant [\frac{z+\mu+1}{2}]$, we obtain that $z = |E| \geqslant [\frac{z+\mu+1}{2}] + [\frac{z+\mu+1}{2}] - 1 \geqslant z + \mu > z$, a contradiction. Consequently n, $m \in F_i$.

After this preliminary result, we show how n, m can be recovered. Let $p_i \in E$, $1 \leqslant i \leqslant z$ and let $E_i = E - p_i$. If $p_i \in E^*$, then $p_i = \phi(n) + m$ for some $\phi \in \Phi$, hence $E^* - p_i \subseteq nN^* - \phi(n)$. Suppose that $n \in F$. Since $|E^* - p_i| = |E^*| \geqslant [\frac{z+\mu+1}{2}]$ it follows that $|E_i \cap F| \geqslant [\frac{z+\mu+1}{2}]$. Thus we have established the existence of $1 \leqslant i \leqslant z$ and $F \in \mathscr{F}$ such that $|E_i \cap F| \geqslant [\frac{z+\mu+1}{2}]$. We now have the following

Theorem 8. *If $|E_i \cap F| \geqslant [\frac{z+\mu+1}{2}]$ for some $1 \leqslant i \leqslant z$, then there exists* *exactly one* $f \in F$ *such that* $|(E_i+f) \cap aN^*| \geqslant [\frac{z+\mu+1}{2}]$ *for some* $a \in N^*$. *In this case* $m = -f + p_i$ *and* $aN^* = nN^*$.

Proof. We can write p_i as $p_i = \phi(b) + m$ for some $b \in N$. Then $E^* - p_i \subseteq nN^* - \phi(b)$. If $b \notin F$, we can proceed like in the proof of Theorem 7 to show that $|(nN^* - \phi(b)) \cap F| \leqslant 1$ and get a contradiction. Thus $\phi(b) \in F$ and we have established the existence of $f \in F$ as claimed in the statement of the theorem. Now suppose that $|(E_i+f) \cap aN^*| \geqslant [\frac{z+\mu+1}{2}]$ for $f \in F$ and $a \in N^*$.

If $p \in E^*$, then $p - p_i + f \in nN^* - \phi(b) + f$, hence $|(E_i+f) \cap (nN^* - \phi(b) + f)| \geqslant [\frac{z+\mu+1}{2}]$. Suppose that $aN^* \neq nN^*$ or $f \neq \phi(b)$. Then $|aN^* \cap (nN^* - \phi(b) + f)| \leqslant \mu$ by Theorem 3. By our assumption $|(E_i+f) \cap aN^*| \geqslant [\frac{z+\mu+1}{2}]$, hence $|E_i+f| = |E| = z \geqslant [\frac{z+\mu+1}{2}] + [\frac{z+\mu+1}{2}] - \mu \geqslant z+1$, a contradiction. Consequently $aN^* = nN^*$ and $\phi(b) = f$, hence $-f + p_i = m$.

Provided that all fibres are small, the element $f \in F$ in Theorem 8 can be readily found. Finally we turn to the columm code $\mathcal{C}_2(N)$. Its error-correction capability is given by the following

Proposition 9 ([3], Prop.1.2). (1) $d_{\min} = 2(r - \lambda)$. (2) $e \leqslant r - \lambda - 1$ *errors can be corrected.*

Now suppose that the codeword $c_p \in \mathcal{C}_2(N)$ has been emitted and that c is the received message.

Let $E = \{B | c(B) = 1\}$. For each $B \in E$, $B = nN^* + m$ we obtain an equation $p = \phi(n) + m$ for the unknown point p. Let us denote this set of equations also by E. The following result is similar to Proposition 5, so its proof shall be omitted.

Proposition 10. *Let* $z = |E|$ *and suppose that not more than* $r - \lambda - 1$ *errors have been made. Then:* (1) $2r - \lambda - 1 \geqslant z \geqslant \lambda + 1$. (2) *Every subsystem* $E' \subseteq E$ *with* $|E'| \geqslant [\frac{z+\lambda+1}{2}]$ *equations has at most one solution* $q \in N$. (3) *There exists a solvable subsystem* $E' \subseteq E$ *with* $[\frac{z+\lambda+1}{2}]$ *equations. If* p *is the solution of any such system* E', *then the codeword* c_p *has been sent.*

Proposition 10 leads us to the following decoding algoritm: Let $E = \{B | c(B) = 1\} =: \{n_1 N^* + m_1, \ldots, n_z N^* + m_z\}$ and $E^* = \{B | c(B) = 1$ is correct}. Consider the set of propositions

$$(*) \qquad \phi(n_1) + m_1 - m_2 \in n_2 N^* \ \dots \ \phi(n_1) + m_1 - m_z \in n_z N^*$$

where $\phi \in \Phi$. By Proposition 10, $n_1 N^* + m_1 \in E^*$ if and only if there exists an element $\phi \in \Phi$ such that ϕ solves at least $[\frac{z+\lambda+1}{2}]$ propositions from (*). In this case Proposition 10 (3) tells us that $p = \phi(n_1) + m_1$ is the unknown point, i.e. c_p has been transmitted. If it is impossible to solve $[\frac{z+\lambda+1}{2}]$ equations for any $\phi \in \Phi$, then $n_1 N^* + m_1 \notin E^*$. Thus one can replace $c(n_1 N^* + m_1) = 1$ by $c(n_1 N^* + m_1) = 0$ and move on to the next block $n_2 N^* + m_2$ in order to repeat the same procedure, etc. If $|\Phi|$ (and therefore every orbit) is reasonably small, then the above method turns out to be fairly quick.

References

[1] J. R. CLAY: [•]$_1$ *Generating balanced incomplete block designs from planar near-rings*, J. Algebra 22 (1972), 319-331; [•]$_2$ *Circular block designs from planar near-rings*, Ann. Discr. Math. 37 (1988), 95-106.

[2] G. FERRERO: [•]$_1$ *Classificazione e costruzioni degli stems p-singolari*, Ist. Lombardo Accad. Sci Lett. Rend. A **102** (1968), 597-613; [•]$_2$ *Stems planari e* BIB-*disegni*, Riv. Mat. Univ. Parma **11** (1970), 79-96.

[3] P. FUCHS, G. HOFER and G. PILZ, *Codes from planar near-rings*, IEEE Trans. Inform. Theory **36** (1990), 647-651.

[4] G. PILZ, *Codes, Frobenius groups and near-rings*, submitted.

Abstract

Using planar near-rings J. R. Clay and G. Ferrero constructed BIB-*designs of high efficiency. For instance, if N is a finite integral planar near-ring, then the set of blocks* $\mathcal{B} = \{nN^* + m | n, \ m \in N, \ n \neq 0\}$ *always forms a* BIBD. *By taking either the rows or the columns of the incidence matrix of such a* BIBD *one can obtain nonlinear codes. The purpose of this paper is to develop decoding algorithms for these codes.*

* * *