Automorphisms of constant weight codes and of divisible designs

Ralph-Hardo Schulz and Antonino Giorgio Spera

Abstract: We show that the automorphism group of a divisible design $\mathcal{D}$ is isomorhic to a subgroup H of index 1 or 2 in the automorphism group $\mathrm{Aut}\,\mathcal{C}(\mathcal{D})$ of the associated constant weight code. Only in very special cases, H is not the full automorphism group.

Keywords: Divisible design, constant weight code, CW-code, automorphism group.

Classification: **20B25**, 94B60, 05B30, 94B25.

1 Introduction

Binary constant weight codes have applications in synchronization of communication systems and as protocol sequence sets for multiuser channels; (see e.g. [NGM], [dRM]). Recently, the interest has been directed as well to non-binary constant weight codes. ETZION ([E]) considers optimal $(s+1)-$ary constant weight codes of length n and weight w and the associated geometric structures which have been called later (see [BWP]) "maximal distance designs" MD(t, w, n, s); these are $t-(s, w, 1)-$divisible designs with n point classes such that the code has minimal distance $d = 1 + 2(w - t)$. PHELPS & YIN ([PY]) have constructed MD$(2, 3, n, s)$ with $s \equiv 3 \pmod 6$ and BLAKE-WILSON & PHELPS ([BWP]) proved that the obvious necessary conditions for the existence of a MD$(2, 3, n, s)$ are asymptotically (in n) sufficient.
In the present article we investigate automorphisms of constant weight codes and related $(s, k, \lambda)-$divisible designs; (for definitions see section 2). We show that the automorphism group of a divisible design induces a subgroup H of the automorhism group $\mathrm{Aut}\,\mathcal{C}$ of the related constant weight code $\mathcal{C}$ and that $[\mathrm{Aut}\,\mathcal{C} : H] \leq 2$. Equality can hold only if $s = 1$ and $n = 2k$ (see section 3.1). Since the theory of divisible designs and their construction by groups is already developed (see e.g. [Hugh], [J$_i$], [BM], [Sch$_j$], [Sp$_i$], [SchSp$_i$] for $i = 1, 2, j = 1, \ldots, 5$), our investigation yields many examples of constant weight codes with large automorphism group (see section 4).

2 Constant weight codes and divisible designs

For the convenience of the reader, we repeat some definitions needed in this article.

2.1 Definitions

2.1.1 Constant weight codes

An $m-$ary *constant weight code (CW–code)* $\mathcal{C}$ of length n and weight w is defined as a set $\mathcal{C}$ with $\mathcal{C} \subseteq (\mathbb{Z}_m)^n$ fulfilling $w_H(c) = w$ for all $c \in \mathcal{C}$. (Here, as usual, one defines the *Hamming distance* $d_H(c, c')$ as the number of different components of c and c' und the *Hamming weight* $w_H(c)$ as $d_H(c, 0)$, the number of non–zero components of c. (See e.g. [McWS]).

2.1.2 Divisible designs and some of their properties

A $t-(s, k, \lambda_t)-$*divisible design*, ($t-$DD, group divisible design, groop divisible design, H–design)(cf.e.g.[BJL]) is an incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ consisting of a finite *"point set"* $\mathcal{P}$ and a *"block set"* $\mathcal{B} \subseteq \binom{\mathcal{P}}{k}$ for $1 < k < v := \mid \mathcal{P} \mid$ with a partition of $\mathcal{P}$ into *"point classes"* such that for fixed $s < v$ and $t \geq 2$

(i) $\mid \overline{p} \mid = s$ for each point class $\overline{p}$,

(ii) $[p, q] = 0$ for $\overline{p} = \overline{q}$ and $p \neq q$,

iii) $[T] = \lambda_t$ for every "transversal" $t-$subset T of $\mathcal{P}$.

(Here, $\overline{p}$ denotes the point class containing p and $[T]$ means the number of blocks incident with all points of T; and a transversal subset of $\mathcal{P}$ is a set containing at most one point from every point class).
By counting in two ways one can show $\lambda_{t-1} = \lambda_t(v - st + s)(k - t + 1)^{-1}$. Putting $r := \lambda_1, b := \lambda_0 = |\mathcal{B}|$ and $\lambda := \lambda_2$ one has in particular $r = \lambda(v - s)/(k - 1)$ and $b = \lambda v(v - s)/k(k - 1)$. The number of point classes is $n = v/s$.
Since any t–DD for $t > 2$ is as well a 2–DD we consider especially the case $t = 2$ and call the design an $(s, k, \lambda)-$ divisible design (in short DD).

2.1.3 Automorphisms

(a) An automorphism of an incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is by definition a permutation β of the set $\mathcal{P}$ with the property that $\beta(l) \in \mathcal{B}$ iff $l \in \mathcal{B}$. The group of all automorphisms of $\mathcal{D}$ with the composition as the group operation is denoted by $\mathrm{Aut}\,\mathcal{D}$.
(b) An automorphism of the set $\mathcal{A}^n$ of all words of length n over an alphabet $\mathcal{A}$ is defined as a mapping consisting of n permutations $\alpha_1, \ldots, \alpha_n$, where α_i is a permutation of the alphabet $\mathcal{A}$ in the i-th component, followed by a permutation α_0 of the components of $\mathcal{A}^n$. (Notice that sometimes, e.g. in [NKÖ], only permutations of the components are considered.)
(c) For a code $\mathcal{C} \subseteq \mathcal{A}^n$, the group $\mathrm{Aut}\,\mathcal{C}$ consists of all automorphisms α of $\mathcal{A}^n$ with $\alpha(\mathcal{C}) = \mathcal{C}$. Here again, the group operation is the composition.

2.2 Construction of CW–codes from divisible designs

(cf. [E] and, independently,[Sp_2], generalizing methods used for binary codes)
¿From a divisible design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ with n point classes we are going to construct an $(s+1)-$ary constant weight code $\mathcal{C} = \mathcal{C}(\mathcal{D})$ of length n. We are doing that in two steps.

2.2.1 The completion $\tilde{\mathcal{D}}$ of $\mathcal{D}$

To every point class G_i of $\mathcal{D}$ we attach a new *ideal point* O_i and define $\tilde{\mathcal{P}}$ as the union of $\mathcal{P}$ with the set of ideal points O_i , $i = 1, \dots, n$. With every block $l \in \mathcal{B}$ we associate a block $\tilde{l}$ by

$$\tilde{l} := l \cup \{O_i \,|\, l \text{ is not incident with a point of } G_i\}$$

and define $\tilde{\mathcal{B}} := \{\tilde{l} \,|\, l \in \mathcal{B}\}$. We call $\tilde{\mathcal{D}} := (\tilde{\mathcal{P}}, \tilde{\mathcal{B}})$ the completion of $\mathcal{D}$.

2.2.2 The constant weight code $\mathcal{C}(\mathcal{D})$

We introduce a special numbering of the point set of $\mathcal{D}$ and $\tilde{\mathcal{D}}$ respectively. As done already, we number the point classes $G_1, \dots, G_n$ by the elements $1, \dots, n$ of ${\mathbb{Z}_{n+1}}^* := \mathbb{Z}_{n+1} \setminus \{0\}$; and in each point class we number the proper points by $1, \dots, s$ from $\mathbb{Z}_{s+1} \setminus \{0\}$ and the ideal point by 0. So we have without loss of generality

$$\mathcal{P} = {\mathbb{Z}_{n+1}}^* \times {\mathbb{Z}_{s+1}}^* \;\text{ and }\; \tilde{\mathcal{P}} = {\mathbb{Z}_{n+1}}^* \times \mathbb{Z}_{s+1}$$

Every block $l \in \mathcal{B}$ is of the form $l = \{(i_1, j_{i_1}), \dots (i_k, j_{i_k})\}$ and the associated block $\tilde{l} \in \tilde{\mathcal{B}}$ can be written as $\{(u, j_u) | u = 1, \dots, n\}$ where $(u, j_u) = (u, 0)$ for $u \notin \{i_1, \dots, i_k\}$ (that means for u with $O_u \in \tilde{l}$). Now we define $c(l) = c(\tilde{l}) := j_1 j_2 \dots j_n$. (Remembering that any $n-$tuple is a mapping from $\{1, \dots, n\}$ to the components we even have $c(l) = \tilde{l}$.
Finally, we put $\mathcal{C}(\mathcal{D}) := \{c(l) | l \in \mathcal{B}\}$ and call it the code associated with the divisible design $\mathcal{D}$.

2.2.3 Properties of $\mathcal{C}(\mathcal{D})$

The code $\mathcal{C} := \mathcal{C}(\mathcal{D})$ of a $t-(s,k,\lambda)-$divisible design $\mathcal{D}$ with n point classes has the following properties.

(i) $\mathcal{C} \subseteq (\mathbb{Z}_{s+1})^n$.

(ii) $\mathcal{C}$ is a constant weight code with $w = k$.

(iii) For any t different positions $i_1, \dots, i_t$ and for any elements $j_1, \dots j_t \in \mathbb{Z}_{s+1} \setminus \{0\}$ there exist exactly λ_t words of $\mathcal{C}$ with coordinate j_u at position i_u for all $u = 1, \dots, t$.

2.2.4 Characterization

Conversely, to every code $\mathcal{C}$ with the properties 2.2.3 (i), (ii) and (iii) there exists (up to isomorphism) a unique $t-(s,k,\lambda_t)-$ divisible design $\mathcal{D}$ with n point classes and $\mathcal{C}(\mathcal{D}) \cong \mathcal{C}$.

In the next section, we investigate the relation between the automorphism groups of a divisible design $\mathcal{D}$ and the associated constant weight code $\mathcal{C}(\mathcal{D})$.

3 The automorphism group of $\mathcal{C}(\mathcal{D})$

3.1 Theorem

Let $\mathcal{D}$ be a divisible design and $\mathcal{C} = \mathcal{C}(\mathcal{D})$ the constant weight code related to $\mathcal{D}$. Then $Aut\mathcal{D}$ induces faithfully a group H of automorphisms of $\mathcal{C}$. Either $H = Aut\mathcal{C}$ and therefore $Aut\mathcal{D} \cong Aut\mathcal{C}$ or $\mathcal{D}$ is a 2-design with $v = 2k$ and $[\,Aut\mathcal{C} : H] = 2$.

Proof.
(i) Let $\gamma \in \mathrm{Aut}\,\mathcal{D}$ and let $\tilde{\mathcal{D}} = (\tilde{\mathcal{P}}, \tilde{\mathcal{B}})$ be the completion of $\mathcal{D}$ (in the sense of 2.2.1). As a maximal set of unjoined points of $\mathcal{D}$, each point class is mapped by γ onto a point class . Hence γ induces a permutation of the point classes and hereby a permutation $\gamma_0 \in S_n$ of the components of every word of $(\mathbb{Z}_{s+1})^n$. The restriction of γ to the extended point classes $\tilde{G}_i$ and $\tilde{G}_{\gamma_0(i)}$ yields a bijection $\gamma_i : \mathbb{Z}_{s+1} \longrightarrow \mathbb{Z}_{s+1}$ fixing 0 (for $i = 1, \ldots, n$). Alltogether, γ induces a bijection $\hat{\gamma} = \gamma_0 \circ (\gamma_1, \ldots, \gamma_n)$ of ${\mathbb{Z}_{s+1}}^n$ onto itself; this is an element of the wreath product $S_n \wr S_{s+1}$ (cf. e.g.[Hup]). The block $\tilde{l} = \{(i, j_i) | i = 1, \ldots, n\} \in \tilde{\mathcal{B}}$, corresponding to $c(l) = j_1 \ldots j_n \in \mathcal{C}$, is mapped onto $\widetilde{\gamma(l)} = \{(\gamma_0(i), \gamma_i(j_i)) | i = 1, \ldots, n\}$, a block corresponding to $c(\gamma(l)) = \hat{\gamma}(c(l))$. Thus $\hat{\gamma}(\mathcal{C}) \subseteq \mathcal{C}$. Using the injectivity of γ we get $\hat{\gamma} \in \mathrm{Aut}\,\mathcal{C}$ and $c \circ \gamma = \hat{\gamma} \circ c$.

(ii) The mapping $\gamma \mapsto \hat{\gamma}$ defines a homomorphism from $\mathrm{Aut}\,\mathcal{D}$ into $\mathrm{Aut}\,\mathcal{C}$. Its kernel is trivial since the identical automorhism of $\mathcal{C}$ does not move any point class and does not change the entries if any component. This shows $\mathrm{Aut}\,\mathcal{D} \cong H$ for a subgroup H of $\mathrm{Aut}\,\mathcal{C}$.

(iii) Conversely, let $\alpha \in \mathrm{Aut}\,\mathcal{C}$. By the definition of code automorphisms, α can be written as $\alpha = \alpha_0 \circ (\alpha_1, \ldots, \alpha_n)$ with $\alpha_0 \in S_n$ and $\alpha_i \in S_{s+1} (i = 1, \ldots, n)$, an element of the wreath product $S_n \wr S_{s+1}$. Now α can as well be interpreted as induced by a permutation of the set $\tilde{\mathcal{P}}$. The codewords and therefore the elements of $\tilde{\mathcal{B}}$ are permuted by α. So α corresponds to an automorphism $\tilde{\alpha} = \alpha_0 \circ (\tilde{\alpha}_1, \ldots \tilde{\alpha}_n)$ of $\tilde{\mathcal{D}}$. We show that either $\tilde{\alpha}_i$ fixes 0, the label of the ideal point O_i of the point class $G_i \subseteq \mathcal{P}$ for all $i = 1, \ldots, n$, so that all proper points are mapped onto proper points or that all proper points are mapped onto ideal points and vice versa.
When all proper points are permuted among themselves, the automorphism α of $\mathcal{C}$ is induced by a bijection of $\mathcal{P}$ preserving the set $\mathcal{B}$, that means by an automorphism of $\mathcal{D}$.
Therefore, suppose that there exists a point p of of a point class G_i which is mapped by $\tilde{\alpha}$ to $O_1 = (\alpha_0(i), 0)$. Since $\tilde{\alpha} \in \mathrm{Aut}\,\tilde{\mathcal{D}}$, we get $r = [p] = [O_1]$. All blocks of $\tilde{\mathcal{B}}$ intersect

the point class $\tilde{G}_{\alpha_0(i)}$, hence

$$(1) \qquad b \;=\; \sum_{q \in G_{\alpha_0(i)}} [q] + [O_1] = \;(s+1)\,r.$$

Distinguishing two cases, we first assume that there exists a point $q \in G_j$ with $i \neq j$ which is mapped to a proper point q'. Now $\lambda = [p,q] = [O_1, q']$; by considering $[q']$ we get

$$(2) \qquad r \;=\; (s+1)\lambda.$$

As mentioned in (2.1.2), the parameters of any divisible design satisfy the conditions

$$(3) \qquad r(k-1) \;=\; \lambda(v-s) \qquad \text{and} \qquad (4) \qquad vr \;=\; bk.$$

Substituting b in (4) according to equation (1) we get $v = k(s+1)$; but (3) and (2) imply

$$v = s + r(k-1)/\lambda = s + \lambda(s+1)(k-1)/\lambda = s + (s+1)(k-1) = k(s+1) - 1,$$

a contradiction.
In the second case, we suppose that there does not exist any $q \in \bigcup_{j \neq i} G_j$ which is mapped to a proper point. Since at most one proper point of a point class G_j can be mapped by $\tilde{\alpha}$ to the ideal point of $G_{\alpha_o(j)}$ this can only occur when $s = 1$ and all proper points are mapped to ideal points and vice versa. The blocks $\tilde{l}$ and $\tilde{\alpha}(\tilde{l})$ of $\tilde{\mathcal{B}}$ consist of k proper and $n-k$ ideal points, since $\mathcal{C}$ is a constant weight code; hence $n-k = k$. This shows that this case can only happen if $s = 1$ and $n = v = 2k$.
If $\tilde{\beta}$ is an element of $\mathrm{Aut}\,\tilde{\mathcal{D}}$ mapping – like $\tilde{\alpha}$ and $\tilde{\alpha}^{-1}$ – all proper points to ideal points and vice versa then $\tilde{\alpha}^{-1} \circ \tilde{\beta}$ permutes the proper points and is therefore an automorphism of $\mathcal{D}$. Hence $\mathrm{Aut}\,\tilde{\mathcal{D}} = \; \mathrm{Aut}\,\mathcal{D} \cup \tilde{\alpha} \circ \mathrm{Aut}\,\mathcal{D}$, showing $[\mathrm{Aut}\,\mathcal{C} : H] = 2$. □

3.2 Remark

a) In theorem 3.1, the second case can not be excluded. Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a $2-(2k, k, \lambda)-$design with the property that the complement in $\mathcal{P}$ of any block is again a block. The mapping $\tilde{\alpha}$ of $\tilde{\mathcal{D}}$ which maps every proper point to the related ideal point and vice versa is a bijection preserving $\tilde{\mathcal{B}}$, i.e an automorphism of $\tilde{\mathcal{D}}$ and therefore related to an automorphism of $\mathcal{C}(\mathcal{D})$. An example of such a 2-design where not all $k-$subsets are blocks is the following.

   $\mathcal{P} = \mathrm{GF}(8)$ and $\mathcal{B} = \{\{0, 1, \xi, \xi^3\} \cdot \xi^i | i = 0, \ldots, 6\} \cup \{\{\xi^2, \xi^4, \xi^5, \xi^6\} \cdot \xi^i | i = 0, \ldots, 6\}$

   for $\xi \neq 1 = \xi^7$ and $\xi^3 + \xi + 1 = 0$. This is a 2-design with parameters $k = 4, v = 8, \lambda = 3, r = 7$ and $b = 12$.

b) The parameters of the designs considered in the second case of theorem 3.1 and in part a) fulfill the equation (3') $r(k-1) = \lambda(2k-1)$. Since $\gcd(k-1, 2k-1) = 1$ this implies that $(k-1)$ is a divisor of λ and $(2k-1)$ a divisor of r. So $\lambda = 3$ and $r = 7$ in the example of part a) are minimal for $k = 4$.

c) Every $\alpha \in \mathrm{Aut}\,\mathcal{C}$ induces a permutation $\overline{\alpha}$ of the set $\mathcal{C}$ of codewords. In general, the homomorphism $\alpha \mapsto \overline{\alpha}$ need not to be injective as the permutations of the components of the repetition codes show. But in the situation considered here the following holds.

3.3 Corollary

If $\mathcal{C} = \mathcal{C}(\mathcal{D})$ *for a divisible design* $\mathcal{D}$ *and* $\alpha \in \mathrm{Aut}\,\mathcal{C}$ *then* $\alpha|_{\mathcal{C}} = \mathrm{id}$ *implies* $\alpha = \mathrm{id}$.

Proof.

As seen in the proof of 3.1 either there exists a $\gamma \in \mathrm{Aut}\,\mathcal{D}$ with $\hat{\gamma} = \alpha$ or α maps the set of proper points onto the set of ideal points. In the first case we get $\hat{\gamma}|_{\mathcal{C}} = \mathrm{id}$ from $\alpha|_{\mathcal{C}} = \mathrm{id}$ and therefore $\gamma|_{\mathcal{B}} = \mathrm{id}$; if $\mathcal{F} := \bigcap_{p \in l} l$ would contain a point different from p we would have $r = \lambda$, a contradiction; so the operation on the block set determines the operation on the point set; hence $\alpha|_{\mathcal{C}} = \mathrm{id}$ implies $\gamma = \mathrm{id}$.

In the second case, $\mathcal{D}$ is a 2-design with $v = 2k$, as seen above. Since any block $\tilde{l}$ is fixed under $\tilde{\alpha}$, the ideal points and the proper points of $\tilde{l}$ are interchanged. Let p be a proper point of a block $\tilde{l}_1$ and O its immagge under $\tilde{\alpha}$. If O is the ideal point of the class $G_i = \{q\}$, then we consider one of the blocks incident with p and q, say $\tilde{l}_2$. Its proper points are mapped to its ideal points too. But $\alpha(p) = O$ is not an ideal point of $\tilde{l}_2$ while p is a proper point of this block. This contradiction shows that, in the case considered, no automorhism fixing the elements of $\mathcal{C}$ can be of the second type. $\square$

4 Examples

Since automorphisms of divisible designs induce automorphisms of the associated CW–codes (see theorem 3.1), it is interesting to recall some constructions of divisible designs with large automorphism groups. Our listing is by no means complete, and the groups mentioned need not to be the full automorphism groups of the considered codes.

4.1 Divisible designs from relative difference sets

(For a survey see e.g.[J_2]).

If G is an (additively written) group of order mn and N a subgroup of order n of G, then a $k-$subset D of G is called an $(n, m, k, \lambda)-$*relative difference set* (RDS) if the multi–set of differences $d - d'$ $(d, d' \in D, d \neq d')$ contains each element of $G \setminus N$ exactly λ times and no element of $N \setminus \{0\}$.

One can show that the incidence structure $\operatorname{dev} D := (G, \{D + g \mid g \in G\})$, the *development* of D, is a divisible design with G as a *Singer group*, i.e. with G as an automorphism group acting regularly on both the point and block sets of $\operatorname{dev} D$. (Conversely, every divisible design with a Singer group can be represented in this way.) Aut of many possibilities, we mention
(i) the existence of a $(p^i, p^{i+j}, p^{i+j}, p^j)-$RDS (for i, j non–negative integers) in the elementary abelian group $G = \mathrm{EA}(p^{2i+j})$ for odd primes and in $G = \mathrm{EA}(2^j) \oplus \mathbb{Z}_4 \oplus \ldots \oplus \mathbb{Z}_4$ for $p = 2$ (Elliott & Butson , Jungnickel; cf. [J$_2$] 3.6) and
(ii) the existence of a $(q^2 - q, q^2 + q + 1, q^2, 1)-$RDS in the semidirect product of $\mathbb{Z}_{q^2+q+1}$ with $\mathbb{Z}_{q^2-q}$ for $q = 3$ or $q = 4$ (coming from a desarguesian projective plane with removed Baer subplane, see [J$_2$] 4.10).
The parameters of the constant weight codes associated with the divisible designs determined by these relative difference sets are:

i)	$n = p^{i+j}$,	$s + 1 = p^i + 1$,	$w = p^{i+j}$,	$\lambda = p^j$,	$\lvert\mathcal{C}\rvert = p^{2i+j}$
ii)	$n = q^2 + q + 1$,	$s + 1 = q^2 - q + 1$,	$w = q^2$,	$\lambda = 1$,	$\lvert\mathcal{C}\rvert = q^4 - q$.

4.2 Translation divisible designs

4.2.1 Definitions

([Sch$_2$], generalizing a method of André) Let $S = \{S_1, S_2, \ldots, S_r\} (\neq \emptyset\ )$ be an $H-(s, k, \lambda)$*–partition* of a finite group G, this means a set of proper subgroups $H, S_1, \ldots, S_r$ of G of order $\mid H \mid = s$ and $\mid S_i \mid = k > 1$ such that $S_i \cap H = 1$ (for all $i = 1, \ldots, r$) and that, for all $x \in G \setminus H$, there exist exactly λ groups S_i containing x. Then

$$\mathcal{D}(S) = (G, \{S_i\, g \mid g \in G,\ i = 1, \ldots r\})$$

is an $(s, k, \lambda)-$divisible design with point classes $\{Hg \mid g \in G\}$. Every $g_1 \in G$ defines an automorphism $g \mapsto gg_1$ (right translation) of $\mathcal{D}(S)$; and so we get $G \cong T \leq \operatorname{Aut} \mathcal{D}(G)$. Conversely, let $\mathcal{D}$ be an $(s, k, \lambda)-$translation divisible design (TTD), that means an $(s, k, \lambda)-$divisible design which possesses a subgoup T of its automorphism group (called *translation group)* which operates regularly on $\mathcal{P}$ and such that $\tau(l) = l$ or $\tau(l) \cap l = \emptyset$ for every $\tau \in T$ and every $l \in \mathcal{B}$. Then $\mathcal{B}$ can be represented by an $H-(s, k, \lambda)-$ partition in the way described.

4.2.2 Charakterisierung von TDD's

(cf. [BM], [Sch$_3$], [Sch$_4$])
The translation group T of an $(s, k, \lambda)-$TDD is either a $p-$group or a Frobenius group or an $HT(p)-$group (only for $\lambda = 1$ possible). We recall that a *Frobenius group* with complement H is a finite group F with subgroup $H \neq 1$ such that $H \cap g^{-1} H\, g = \{1\}$ for all $g \in F \setminus H$. And by an $HT(p)-$ *group* one denotes a finite group G which is neither a $p-$group nor a Frobenius group and has the property that the subgroup $H_p(G)$ generated by all elements of order different from p fulfills the equation $[G : H_p(G)] = p$. Conversely,

there exist examples for all three cases, see f.i. [J_1],[BM],[Sch_1] to [Sch_5]. Out of many possibilities we list the parameters of some CW–codes gained from TDD's.

(*i*) $n = q^{d-1}h, \quad s+1 = q^{m-d}+1, \quad w = q^{d-1}h, \quad \lambda \in \{1,\ldots,q^{m-d}\}, \quad |\mathcal{C}| = \lambda q^{2m-2d}$ with T a Frobenius group of order $q^{m-1}h$ (for every prime power q and all positive integers m, d, h, λ with $h\,|\,(q-1), h > 1, m/2 > d > 1$; see [$Sch_5$]3.4).

(*ii*) $n = p^{(m-1)d}, \quad s+1 = p^d+1, w = p^d, \lambda = 1, |\mathcal{C}| = p^{md}(p^{(m-1)d}-1)/(p^d-1)$ with T elementary abelian of order p^{md} (for p prime, cf. [Sch_3] 2.4a)

Notice that the examples of (i) come from transversal designs; so all codewords have only entries different from 0.

4.3 DD's from R–groups

(Generalizing a method of Hughes, see [Hug], to construct $t-$designs from $t-$homogenious permutation groups; compare as well with [NKÖ] and [JJ].)

4.3.1 Proposition ([Sp_1])

Let R be an equivalence relation on a finite set V of size v and let G be a finite $R-$group on V, i.e. a group G acting on V and permuting the equivalence classes among themselves; furthermore, let G be $t-R-$homogeneous i.e. with the property that any $R-$ transversal subset of V of size t can be mapped onto any other such transversal $t-$ subset. If B is an $R-$transversal subset of V of size k $(t < k < v)$, then we get an $t-(s,k,\lambda)-$divisible design $\mathcal{D}(B) := (V, B^G)$ by putting $B^G := \{g(B)|\, g \in G\}$. Notice that G induces an automorphism group on $\mathcal{D}(B)$ which is transitive, both on the block set and on the point set.

4.3.2 Corollary ([$SchSp_2$])

Let $\mathcal{T}$ be a finite translation plane of order q which admits a collineation group G acting 2-homogeneously on an orbit $\mathcal{O}$ of the line at infinity ℓ_∞ (with $|\mathcal{O}| \geq 2$). Let $\hat{\mathcal{O}}$ be the set of lines of $\mathcal{T}$ intersecting ℓ_∞ in $\mathcal{O}$ and R the equivalence relation on $\hat{\mathcal{O}}$ induced by the parallelism relation of $\mathcal{T}$. Then $\hat{G} = G \cdot T$ (where T denotes the translation group of $\mathcal{T}$) induces a $2-R-$homogeneous $R-$group on $\hat{\mathcal{O}}$. For any R-transversal k-subset B of $\hat{\mathcal{O}}$ with $2 \leq k \leq |\mathcal{O}|$ the incidence structure $\mathcal{D}(B) := (\hat{\mathcal{O}}, B^{\hat{G}})$ is an (s,k,λ)-divisible design with parameters $s = q$, k as chosen, $\lambda = \frac{k(k-1)b}{q^2|\mathcal{O}|(|\mathcal{O}|-1)}$, $v = q \cdot |\mathcal{O}|$ and $b = \frac{|\hat{G}|}{|\hat{G}_B|}$. Here, as usual, $\hat{G}_B$ denotes the setwise stabilizer of B.

4.3.3 Special cases

One gets examples for 4.3.1 and 4.3.2 by taking

1) $G =$ PSL$(2,q)$ for $q = 2^r$, a sharply $3-$transitive group of degree $q+1$, or

2) $\mathcal{O} = l_\infty$, G 2−transitive and $\mathcal{T}$ a desarguesian plane of order q with $G \cong \mathrm{PSL}(2,q)$ or $\mathcal{T}$ a Lüneburg plane of order q^2 for $q = 2^{2t+1}$ with G the Suzuki group $Sz(q)$ ([SchSp$_1$]) or

3) $\mathcal{O} \subset l_\infty$, $G \cong SL(2,q)$ and $\mathcal{T}$ a Hering plane of order q^2, an Ott–Schäffer plane of order q^2, a Kantor plane of type II of order q^3, the Dye–Kantor plane of order 8^3 or a Bartolone–Ostrom plane (see [SchSp$_2$]).

As parameters of related constant weight codes (with an automorphism group transitive on the set of codewords) one gets e.g.

1) $n = q+1, \quad s+1 = 2, w = k, \lambda = k(k-1)(q-1)/|G_B|, \quad |\mathcal{C}| = (q+1)q(q-1)/|G_B|$
$G = \mathrm{PSL}(2,q)$, $\lambda_3 = k(k-1)(k-2)/|G_B|$ (for $q = 2^r$ and start block B of size k, see [SchSp$_1$], Th.2).

2) $n = q^2, \quad s+1 = q^2+1, \quad w = q, \quad \lambda = q-1, \quad |\mathcal{C}| = q^5(q^2-1)$
$G = \mathrm{Sz}(q)$ (for $q = 2^{2t+1}$, $t > 0$, see [SchSp$_1$], Th. 2).

3) $n = q+1, \quad s+1 = q^2+1, \quad w = 4, \quad \lambda = 6(q-1)/u, \quad |\mathcal{C}| = (q^2-1)q^5/u$
$G = \mathrm{SL}(2,q)$ (for q a prime power and $u = 12$ in case $q \equiv 1 (\bmod 4)$ and $u = 6$ otherwise, cf. [SchSp$_2$] Th.2)

Acknowledgement:
We like to thank Martin Aigner for having asked the right question at the right time.

5 References

[BJL] Beth T., D. Jungnickel & H. Lenz: Design Theory. BI. Mannheim-Wien-Zürich, 1985.

[BM] Biliotti, M. & G. Micelli : On translation transversal designs. Rend. Sem. Mat. Univ. Padova **73** (1985) 217–229.

[BWP] Blake-Wilson, S. & K.T.Phelps: Constant weight codes and group divisibe designs. (Manuscript)

[dRM] da Rocha, V. C. jun. & J. L. Massey : A new approach to the design of codes for the binary adder channel. In Ganley, M. J. (ed.) Cryptography and coding III. Oxford: Clarendon Press, Inst. Math. Appl. Conf. Ser. **45** (1993) 179–185.

[E] Etzion, T.: Optimal constant weight codes over $\mathbb{Z}_k$ and generalized designs. Discrete Mathematics 169 (1997) 55–82.

[Hug] Hughes, D. R. : On t-designs and groups. Amer. J. Math. **87** (1965), 761-778.

[Hup] Huppert, B.: Endliche Gruppen I. Springer Verlag, Berlin-Heidelberg-New York 1967.

[JJ] Johnson, N. L. & V. Jha: Regulus codes. Discr. Math. **132** (1994) 97–106.

[$\mathbf{J}_1$] JUNGNICKEL, D. : Transversal designs associated with Frobenius groups. J. Geom. **17** (1981) 140–154.

[$\mathbf{J}_2$] JUNGNICKEL, D. : On automorphism groups of divisible designs. Can. J. Math. **34**/2 (1982) 257–297.

[**K**] KALLAHER, M. J. : Translation planes. In Buekenhout. F. (ed): Handbook of Indicence geometry. Elsevier 1995.

[**Lü**] LÜNEBURG, H.: Translation planes. Springer Verlag. Berlin- Heidelberg- New York 1980.

[**McWS**] MAC WILLIAMS, F.J. & N.J.A.SLOANE: The theory of error correcting codes. North-Holland. Amsterdam-New York-Oxford 1977.

[**NGM**] NGUYEN, Q. A. , L. GYÖRFI & J. L. MASSEY : Construction of binary constant–weight cyclic codes and cyclically permutable codes. IEEE Trans. Inf. Th. **38**/3 (1992) 940–949.

[**NKÖ**] NURMELA, K. J., M. K. KAIKKONEN & P. R. J. ÖSTERGÅRD: New constant weight codes from linear permutation groups. IEEE Trans. Inf. Th. **43**/5 (1997) 1623–1632.

[**PY**] PHELPS,K. & C.YIN: Generalized Steiner systems with block size three and group size $g \equiv 3\,(mod\ 6)$. J.Combin. Designs 5 (1997) 417–432.

[$\mathbf{Sch}_1$] SCHULZ, R.-H. Transversal designs and Hughes–Thompson groups. Mitt. Math. Sem. Giessen **65** (1984) 185–197.

[$\mathbf{Sch}_2$] SCHULZ, R.-H. Transversal designs and partitions associated with Frobenius groups. J. f. d. reine u. angew. Math. 355 (1985)153–162.

[$\mathbf{Sch}_3$] SCHULZ, R.-H. On the classification of translation group divisible designs. Europ. J. Comb. **6** (1985) 369–374.

[$\mathbf{Sch}_4$] SCHULZ, R.-H. On translation transversal designs with $\lambda > 1$. Arch. Math. 49.(1987)97–102.

[$\mathbf{Sch}_5$] SCHULZ, R.-H. On the existence of generalized triads related to transversal designs. Ars Combin. **25 B** (1988) 203–209.

[$\mathbf{SchSp}_1$] SCHULZ, R.-H. & A. G. SPERA: Divisible designs admitting a Suzuki group as an automorphism group. Bolletino U.M.I. (to appear).

[$\mathbf{SchSp}_2$] SCHULZ, R.-H. & A. G. SPERA: Construction of divisible designs from translation planes. Europ. J. Comb. (to appear).

[Sp$_1$] SPERA, A. G. : t-divisible designs from imprimitive permutation groups. Europ. J. Comb. **13** (1992), 409-417.

[Sp$_2$] SPERA, A. G. : Private communication with the second author. 1997.

Ralph-Hardo Schulz
2.Mathematisches Institut,
Freie Universität Berlin
Arnimallee 3
D–14195 Berlin (Germany).
e-mail: schulz@math.fu-berlin.de

Antonino Giorgio Spera
Dipartimento di Matematica ed applicazioni
Universitá di Palermo
Via Archirafi 34
I–90123 Palermo (Italy).
e-mail: spera@dipmat.math.unipa.it