Variations on the McFarland and Spence Constructions of Difference Sets

K.T. Arasu*, Department of Mathematics and Statistics, Wright State University, Dayton, Ohio 45435, USA

and

Alexander Pott**, Mathematisches Institut der Universität Gießen, Arndtstraße 2, 35392 Gießen, Germany

Abstract: We give two new constructions of symmetric group divisible designs using divisible difference sets. These constructions generalize the McFarland and Spence constructions of symmetric designs.

Divisible designs are of interest in several parts of mathematics: The design theorist needs classes of divisible designs as "ingredients" for recursive constructions of designs. Statisticians use divisible designs in the design of experiments. Recently, divisible designs found applications in cryptography, see [9]. A **divisible design** is an incidence structure consisting of m·n points partitioned into m classes of size n each. Two distinct points are joined by exactly λ_1 or λ_2 blocks depending whether the two points are elements in the same point class or not. The block size is a constant number and usually called k. The design is **symmetric** if the dual structure is a divisible design with the same parameters. In many cases symmetric divisible designs are constructed as "developments" of **divisible difference sets**. A divisible difference sets D in a group G is a k-subset of G with the following properties: The group G contains a subgroup N of order n and index m. The list of differences d-d' ($d,d' \in D$) contains every nonzero element in N exactly λ_1 times and the elements in G\N exactly λ_2 times. We say that such a subset D is an **$(m,n,k,\lambda_1,\lambda_2)$-divisible difference set in G relative to N**. Using divisible difference sets it is quite easy to construct divisible designs. The points are just the elements of G and the blocks are the translates $D+g=\{d+g: d \in D\}$ of D.

Usually one requires that N is a normal subgroup of G. In this case one can show that the

*Research partially supported by NSA grant MDA 904-92-H-3057, NSF grant NCR-9200265 and by an Alexander-von-Humboldt fellowship. The author thanks the Mathematisches Institut der Universität Giessen for its hospitality during the time of this research.

**Current address: Institut für Mathematik, Universität Augsburg, 86135 Augsburg, Germany

corresponding divisible design is symmetric. However, it is not known whether any condition is required at all. No example of a non-symmetric divisible design is known that can be constructed from a group G with subgroup N as described above, see [2].

If $\lambda_1=\lambda_2(=\lambda)$ or n=1 the divisible difference set becomes a (v,k,λ)-difference set in the usual sense (v denotes the order of G) and the corresponding design is just a symmetric (v,k,λ)-design.

In this paper we want to describe a new construction of divisible difference sets (relative to a normal subgroup N) and therefore symmetric divisible designs. As special cases we obtain

- — difference sets due to McFarland [6],
- — difference sets due to Spence [8],
- — divisible difference sets due to Jungnickel (generalizing McFarland's construction) [3],
- — divisible difference sets due to Jungnickel (generalizing Spence's construction) [4].

Informally, we can describe these four constructions as follows. Take the hyperplanes in $V=GF(q)^n$ and a group G. We construct divisible difference sets in $V\times G$ in the following way: Combine the elements of G with different hyperplanes or complements of hyperplanes of V. The constructions mentioned above and in the sequel differ just by the choice of the subsets S, T and U (in G) which we combine with hyperplanes, complements of hyperplanes and with the entire group V.

We refer the reader to [2] for a source of many more constructions of divisible difference sets. Unfortunately, not many examples are known where $\lambda_1=0$, a situation which is of particular interest. Divisible difference sets with $\lambda_1=0$ are called **relative difference sets**.

In order to describe our constructions and to verify that they yield divisible difference sets we need some notation. We will work in the group ring $\mathbb{Z}G$ where G is written multiplicatively, and define

$$\left(\sum a_g g\right)^{(t)} := \sum a_g g^t$$

for integers t. A subset S of G will be identified with $S:=\sum_{g\in S} g$ in the group ring $\mathbb{Z}G$ and we denote this group ring element S, by abuse of notation. Using this notation we can translate the definition of a divisible difference set. A subset D of a group G is an $(m,n,k,\lambda_1,\lambda_2)$-divisible difference set in G relative to N if and only if

$$D\cdot D^{(-1)} = k + \lambda_1(N-1) + \lambda_2(G-N)$$

provided $|G|=mn$ and $|N|=n$. It is this group ring equation that we will check in the following constructions.

Theorem 2.1: Let q be a prime power and d a positive integer. Let $V=GF(q)^d$ and G any group of order $v=(q^d-1)/(q-1)$. Let D be a (v,r,λ)-difference set in G. Then there exists a divisible difference set R in $G\times V$ relative to V with parameters

$$m = \frac{q^d-1}{q-1},$$

$$n = q^d,$$

$$k = (v-r)\cdot q^{d-1} + r\cdot(q^d-q^{d-1}),$$

$$\lambda_1 = v\cdot q^{d-2} - q^{d-2} + r\cdot q^d - 2\cdot r\cdot q^{d-1},$$

$$\lambda_2 = v\cdot q^{d-2} + 2\cdot r\cdot(q^{d-1}-2q^{d-2}) + \lambda\cdot(q^d-4q^{d-1}+4q^{d-2}).$$

Proof. Let $H_1, H_2, \ldots, H_v$ be the hyperplanes of V (i.e. subgroups of order q^{d-1}). In the sequel we use the following three equations

$$H_i^2 = q^{d-1}\cdot H_i, \tag{1}$$

$$\sum_{i=1}^{v} H_i = q^{d-1} + \frac{q^{d-1}-1}{q-1}V, \tag{2}$$

$$H_iH_j = q^{d-2}\cdot V, \ i\neq j. \tag{3}$$

Enumerate the elements of D and G\D as follows:

$$D = \{g_1, g_2, \ldots, g_r\} \text{ and } G\backslash D = \{g_{r+1}, g_{r+2}, \ldots, g_v\}.$$

We assert that

$$R = \left(\bigcup_{i=r+1}^{v} g_iH_i\right) \cup \left(\bigcup_{i=1}^{r} g_i(V\backslash H_i)\right) \tag{4}$$

serves as the desired divisible difference set. Using our group ring notation, (4) can be rewritten as

$$R = \sum_{g_i\in G} g_iH_i + \sum_{g_i\in D} g_i(V-2H_i) \tag{5}$$

Define

$$A := \sum_{g_i\in G} g_iH_i \quad \text{and} \quad B := \sum_{g_i\in D} g_i(V-2H_i).$$

Then R=A+B and

$$R\cdot R^{(-1)} = A\cdot A^{(-1)} + A\cdot B^{(-1)} + A^{(-1)}\cdot B + B\cdot B^{(-1)}. \tag{6}$$

Consider

$$A\cdot A^{(-1)} = \left(\sum_{g_i\in G} g_iH_i\right)\cdot\left(\sum_{g_j\in G} g_j^{-1}H_j\right) = \sum_{g_i,g_j} g_ig_j^{-1}H_iH_j =$$

$$= \sum_i H_i^2 + \sum_{i\neq j} q^{d-2}\cdot g_ig_j^{-1}V \quad \text{(using (3))}$$

$$= q^{d-1}\cdot\left(q^{d-1} + \frac{q^{d-1}-1}{q-1}V\right) + q^{d-2}\cdot v\cdot(G-1)V \quad \text{(using (1) and (2)).}$$

Thus

$$A\cdot A^{(-1)} = q^{2d-2} - q^{d-2}\cdot V + v\cdot q^{d-2}\cdot G\times V. \tag{7}$$

Next let us look at

$$\begin{aligned} A\cdot B^{(-1)} + A^{(-1)}\cdot B &= \sum_{g_i\in G, g_j\in D} \left(g_i g_j^{-1}+g_i^{-1}g_j\right)H_i(V-2H_j) \\ &= \sum_{g_i\in D} 2H_i(V-2H_i) + \sum_{g_i\neq g_j, g_i\in G, g_j\in D} \left(g_i g_j^{-1}+g_i^{-1}g_j\right)H_i(V-2H_j) \\ &= \sum_{g_i\in D} 2\cdot(q^{d-1}V-2q^{d-1}H_i) + 2\cdot r\cdot(q^{d-1}-2q^{d-2})V(G-1) \\ &= -4\cdot q^{d-1}\sum_{g_i\in D} H_i + 4\cdot r\cdot q^{d-2}\cdot V + 2\cdot r\cdot(q^{d-1}-2q^{d-2})\cdot G\times V. \quad (8) \end{aligned}$$

Finally we calculate

$$\begin{aligned} B\cdot B^{(-1)} &= \sum_{g_i, g_j\in D} g_i g_j^{-1}(V-2H_i)(V-2H_j) \\ &= \sum_{g_i\in D} (V-2H_i)^2 + \lambda\cdot(V-2H_1)(V-2H_2)(G-1) \\ &= r\cdot(q^d-4\cdot q^{d-1})\cdot V + 4\cdot q^{d-1}\sum_{g_i\in D} H_i + \lambda\cdot(q^d-4q^{d-1}+4q^{d-2})\cdot V(G-1). \quad (9) \end{aligned}$$

Using (7),(8) and (9) in (6), we get

$$R\cdot R^{(-1)} = (k-\lambda_1) + (\lambda_1-\lambda_2)\cdot V + \lambda_2\cdot G\times V$$

where k, λ_1 and λ_2 are as stated in the theorem. Since R has coefficients 0 and 1, we can conclude that R "is" a divisible difference set with the desired parameters. □

Theorem 2.1 generalizes the Spence construction of difference sets. The set R is a difference set in G×V if and only if $\lambda_1=\lambda_2$, equivalently (after simplifying) $(r-\lambda)(q-2)^2=1$, i.e. $r-\lambda=1$ (or $v=r+1$) and $q=3$. This is exactly Spence's construction [8]: Take all but one of the hyperplanes and combine them with different elements in G and add the complement of the remaining hyperplane (combined with the remaining element of G). For some nonabelian examples of difference sets with these parameters we refer the interested reader to [5] and [7]. If we choose D to be a $(v,v-1,v-2)$-difference set (not necessarily $q=3$) we obtain the divisible difference sets in [4]. Unfortunately, Theorem 2.1 never produces relative difference sets as λ_1 is always greater than 0.

Now we are going to generalize the McFarland construction.

Theorem 2.2: Let q be a prime power and d a positive integer. Let $V=GF(q)^d$ and G be any group of order $v=1+(q^d-1)/(q-1)$. Let D be a (v,r,λ)-difference set in G with $1\notin D$. Assume that either $r=0$ or $r=v-1$ or $D\cup D^{(-1)}=G\setminus\{1\}$ and $D\cap D^{(-1)}=\emptyset$. Then there exists a divisible difference set E in G×V relative to V with parameters

$$m = 1+\frac{q^d-1}{q-1},$$
$$n = q^d,$$
$$k = q^{d-1}\cdot(v-r-1) + r\cdot(q^d-q^{d-1}),$$

$$\lambda_1 = r\cdot q^d - 2\cdot r\cdot q^{d-1} + \frac{q^{2d-2}-q^{d-1}}{q-1},$$

$$\lambda_2 = \frac{q^{2d-2}-q^{d-1}}{q-1} + \delta\cdot(q^{d-1}-2q^{d-2}) + \lambda\cdot(q^d-4q^{d-1}+4q^{d-2})$$

where $\delta=0$ if $r=0$, $\delta=2r-2$ if $r=v-1$ (hence $\delta=2v-4$) and $\delta=2r-1$ otherwise.

Proof. Let $H_1, H_2, \ldots, H_s$ be the hyperplanes of V ($s=(q^d-1)/(q-1)$). Write $D=\{g_1, g_2, \ldots, g_r\}$ and $G\setminus(D\cup\{1\})=\{g_{r+1}, g_{r+2}, \ldots, g_{v-1}\}$. We define

$$E := \bigcup_{i=1}^{r} g_i(V\setminus H_i) \cup \bigcup_{i=r+1}^{v-1} g_iH_i.$$

Let $A:=\sum_{g_i\in G\setminus\{1\}} g_iH_i$ and $B:=\sum_{g_i\in D} g_i(V-2H_i)$. As in the proof of Theorem 2.1 we will compute $A\cdot A^{(-1)}$, $A\cdot B^{(-1)}+B\cdot A^{(-1)}$ and $B\cdot B^{(-1)}$. The equation for $B\cdot B^{(-1)}$ is exactly the same as (9). The situation for $A\cdot B^{(-1)}+B\cdot A^{(-1)}$ is slightly different:

$$\begin{aligned} A\cdot B^{(-1)} + A^{(-1)}\cdot B &= \sum_{g_i\in G\setminus\{1\}, g_j\in D} (g_ig_j^{-1}+g_i^{-1}g_j)H_i(V-2H_j) \\ &= \sum_{g_i\in D} 2H_i(V-2H_i) + (2r(G-1)-D-D^{(-1)})\cdot(q^{d-1}-2q^{d-2})V \\ &= 2\cdot r\cdot q^{d-1}\cdot V - 4\cdot q^{d-1}\sum_{g_i\in D} H_i + \delta\cdot(G-1)\cdot(q^{d-1}-2q^{d-2})\cdot V \quad (10) \end{aligned}$$

Note that $D+D^{(-1)}=2(G-1)$ if $r=v-1$ and $D+D^{(-1)}=G-1$ if $D\cap D^{(-1)}=\emptyset$, $D\cup D^{(-1)}= G\setminus\{1\}$.

Without going into details we just state the result for $A\cdot A^{(-1)}$:

$$A\cdot A^{(-1)} = q^{2d-2} + \frac{q^{2d-2}-q^{d-1}}{q-1}G\times V. \qquad (11)$$

Using (9), (10) and (11), we get

$$E\cdot E^{(-1)} = (k-\lambda_1) + (\lambda_1-\lambda_2)\cdot V + \lambda_2\cdot(G\times V)$$

where k, λ_1, and λ_2 are as in the statement of Theorem 2.2. Since E has coefficients 0 and 1, it follows that E is the desired divisible difference set. □

If $r=0$ in the Theorem above, then E corresponds to the McFarland difference sets [6]. If $r=v-1$ we get the complements of the divisible difference sets in [3]. Now we want to discuss the case that $D\cup D^{(-1)}=G\setminus\{1\}$ and $D\cap D^{(-1)}=\emptyset$. If G is abelian, this implies that $|G|=p^x$ for some prime p ($p\equiv 3 \pmod 4$) and D is a $(p^x,(p^x-1)/2,(p^x-3)/4)$- difference set in G, see [1]. Difference sets with these parameters and the property $D\cup D^{(-1)}=G\setminus\{1\}$ exist, take just the squares in $GF(p^x)$. Thus Theorem 2.2 provides divisible difference sets if and only if

$$v = \frac{q^d-1}{q-1} + 1 = p^x \equiv 3 \pmod 4.$$

A few examples when this happens are for d=2 and q=5,9,17,25,29. In fact, whenever $q+2=p^x$, where q is a prime power, we get such examples with d=2.

References

[1] P. Camion and H.B. Mann, *Antisymmetric difference sets*, J. Number Th. **4** (1972), 266-268.

[2] D. Jungnickel, *On automorphism groups of divisible designs*, Can.J.Math. **24** (1982), 257-297.

[3] D. Jungnickel, *A new class of symmetric divisible designs*, Annals of Discrete Math. **34** (1987), 297-300.

[4] D. Jungnickel, *A new family of relative difference sets*, J.Comb.Th.(A) **52** (1989), 101-103.

[5] S.L. Ma, *A family of difference sets having -1 as an invariant*, Europ.J.Comb. **10** (1989), 207-209.

[6] R.L. McFarland, *A family of difference sets in non-cyclic groups*, J.Comb.Th. (A) **15** (1973), 1-10.

[7] M. Miyamoto, *A family of differnce sets having -1 as an invariant*, Hokkaido. Math.J. **12** (1983), 24-26.

[8] E. Spence, *A family of difference sets in non-cyclic groups*, J.Comb.Th. (A) **22** (1977), 103-106.

[9] D.R. Stinson, *Some constructions and bounds for authentication codes*, J. of Cryptology **1** (1988), 37-51

(Received 23/2/94)