10-1993

A Note on New Semi-Regular Divisible Difference Sets

James A. Davis
University of Richmond, jdavis@richmond.edu

Jonathan Jedwab

Recommended Citation
Davis, James A., and Jonathan Jedwab. "A Note on New Semi-Regular Divisible Difference Sets." *Designs, Codes, and Cryptography* 3, no. 4 (October 1993): 379-81. doi: 10.1007/BF01418532.

Designs, Codes and Cryptography, 3, 379–381 (1993)

A Note on New Semi-Regular Divisible Difference Sets

JAMES A. DAVIS*
Department of Mathematics, University of Richmond, Richmond, VA 23173

JONATHAN JEDWAB
Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol, BS12 6QZ, U.K.

Communicated by D. Jungnickel
Received October 12, 1992; Revised

Abstract. We give a construction for new families of semi-regular divisible difference sets. The construction is a variation of McFarland's scheme [5] for noncyclic difference sets.

Let G be a group of order mn and N a subgroup of G of order n. If D is a k-subset of G then D is a $(m, n, k, \lambda_1, \lambda_2)$ *divisible difference set* in G relative to N provided that the differences dd'^{-1} for $d, d' \in D, d \neq d'$, contain every nonidentity element of N exactly λ_1 times and every element of $G \backslash N$ exactly λ_2 times. If $k > \lambda_1$ and $k^2 = mn\lambda_2$, then the divisible difference set is called *semi-regular*. Families of semi-regular divisible difference sets with $\lambda_1 \neq 0$ are rare, as mentioned in [4]. If $\lambda_1 = \lambda_2$ then D is a (mn, k, λ_1) *difference set* in G.

One way to check if a subset of a group is a divisible difference set is to use the group ring equation. If we abuse notation by writing $D = \Sigma_{d \in D} d$ and $D^{(-1)} = \Sigma_{d \in D} d^{-1}$ then the definition of a divisible difference set is equivalent to the equation $DD^{(-1)} = k + \lambda_1(N - 1) + \lambda_2(G - N)$ in the group ring $Z[G]$ (see [2], [3] for examples of this technique).

In this paper, we will construct semi-regular divisible difference sets with new sets of parameters. The construction is similar to those found in [1], [2], [3]. We start with the group $E = EA(q^{d+1})$, the elementary Abelian group with q^{d+1} elements, where q is a prime power. We will view E as a vector space of dimension $d + 1$ over $GF(q)$. A hyperplane of E is a subspace of dimension d; a standard counting argument shows that E contains $(q^{d+1} - 1)/(q - 1)$ hyperplanes. Label these hyperplanes H_i for $i = 1, \ldots, (q^{d+1} - 1)/(q - 1)$ and note that $E/H_i \cong EA(q)$ for each i. Suppose $EA(q)$ supports a (q, k', λ') difference set. Then for each i form the set $D_i = \cup_{j=1}^{k'} a_{ij}H_i \subset E$ (regarding each $a_{ij}H_i$ as a subset of E), where $\{a_{ij}H_i : j = 1, \ldots, k'\}$ is a (q, k', λ') difference set in E/H_i (regarding each $a_{ij}H_i$ as an element of E/H_i). Suppose M is an Abelian group containing a $(m, (q^{d+1} - 1)/(q - 1), \lambda'')$ difference set $\{b_i : i = 1, \ldots, (q^{d+1} - 1)/(q - 1)\}$. Then form the set $D = \cup_{i=1}^{(q^{d+1}-1)/(q-1)} b_iD_i \subset M \times E$. The set D thus constructed is a divisible difference set:

*This work is partially supported by NSA grant # MDA 904-92-H-3067.

THEOREM 1. *Let q be a prime power. If there exists a $(m, (q^{d+1} - 1)/(q - 1), \lambda'')$ difference set in an Abelian group M and a (q, k', λ') difference set in $EA(q)$, then there exists a $(m, q^{d+1}, q^d((q^{d+1} - 1)/(q - 1))k', q^d(((q^{d+1} - 1)/(q - 1))k' - q^d(k' - \lambda')), q^{d-1}k'^2\lambda'')$ divisible difference set in $G = M \times EA(q^{d+1})$ relative to $EA(q^{d+1})$.*

Proof. We work in the group ring $Z[E]$. For hyperplanes H_i, $H_{i'}$ of E the expression $H_iH_{i'}$ in $Z[E]$ is equal to q^dH_i if $i = i'$ and $q^{d-1}E$ if $i \neq i'$. Since $\{a_{ij}H_i\}$ is a (q, k', λ') difference set in E/H_i, it follows that in $Z[E]$ we have $D_iD_i^{(-1)} = q^d\Sigma_{j,j'}a_{ij}a_{ij'}^{-1}H_i = q^d(k'H_i + \lambda'(E - H_i))$. Also note that $\Sigma_iH_i = (q^{d+1} - 1)/(q - 1) + (q^d - 1)/(q - 1)(E - 1)$. The proof involves a separation into cases based on $i = i'$ and $i \neq i'$:

$$\begin{aligned} DD^{(-1)} &= \sum_{i=1}^{(q^{d+1}-1)/(q-1)} \sum_{j=1}^{k'} b_ia_{ij}H_i \sum_{i'=1}^{(q^{d+1}-1)/(q-1)} \sum_{j'=1}^{k'} H_{i'}a_{i'j'}^{-1}b_{i'}^{-1} \\ &= q^d \sum_i \sum_{j,j'} a_{ij}a_{ij'}^{-1}H_i + q^{d-1} \sum_{i\neq i'} b_ib_{i'}^{-1} \sum_{j,j'} a_{ij}a_{i'j'}^{-1}E \\ &= q^d \sum_i (k'H_i + \lambda'(E - H_i)) + q^{d-1}k'^2E \sum_{i\neq i'} b_ib_{i'}^{-1} \\ &= q^d(k' - \lambda') \sum_i H_i + q^d\lambda' \frac{q^{d+1} - 1}{q - 1} E + q^{d-1}k'^2E\lambda''(M - 1) \\ &= q^dk' \frac{q^{d+1} - 1}{q - 1} + q^d \left(\frac{q^{d+1} - 1}{q - 1} k' - q^d(k' - \lambda') \right) (E - 1) \\ &\qquad + q^{d-1}k'^2\lambda''(G - E) \end{aligned}$$

□

A divisible difference set with the parameters of Theorem 1 can also be constructed in any group containing a normal subgroup isomorphic to E, using a similar adaption of the above method to that introduced by Dillon [3] to modify the scheme of McFarland [5].

The parameters in Theorem 1 are not semiregular in general, but they are in the special case when the difference set $\{b_i\}$ is trivially the whole of M:

COROLLARY 1. *If $m = (q^{d+1} - 1)/(q - 1)$, then the divisible difference set is semi-regular.*

Proof. $k^2 = q^{2d}((q^{d+1} - 1)/(q - 1))^2k'^2 = ((q^{d+1} - 1)/(q - 1))(q^{d+1})(q^{d-1}k'^2((q^{d+1} - 1)/(q - 1))) = mn\lambda_2$. □

For example, if we choose $q = 7$, $k' = 3$, $\lambda' = 1$, and $d = 1$, then the corollary shows the existence of a (8, 49, 168, 70, 72) semi-regular divisible difference set in $M \times EA(49)$, where M is any group of order 8 (including nonabelian). Known existence results for (q, k', λ') difference sets in $EA(q)$ provide many examples for the construction of Corollary 1. In the case $q \equiv 3 \pmod 4$ there exists a $(q, (q - 1)/2, (q - 2)/4)$ difference set. In the case $q \equiv 1 \pmod 4$ there are examples such as (13, 4, 1) and (73, 9, 1) in the projective planes, as well as others such as (37, 9, 2).

References

1. K.T. Arasu, D. Jungnickel, and A. Pott, Divisible difference sets with multiplier −1, *J. Algebra*, Vol. 133, (1990) pp. 35–62.
2. J.A. Davis, Almost difference sets and reversible divisible difference sets, *Archiv der Mathematik*. To appear.
3. J.F. Dillon, Variations on a scheme of McFarland for noncyclic difference sets, *J. Combin. Theory* (A), Vol. 40, (1985) pp. 9–21.
4. D. Jungnickel, On automorphism groups of divisible designs, *Canad. J. Math.*, Vol. 325, (1982) pp. 257–297.
5. R.L. McFarland, A family of difference sets in non-cyclic groups, *J. Combin. Theory* (A), Vol. 15, (1973) pp. 1–10.