12-1992

Almost Difference Sets and Reversible Divisible Difference Sets

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

Recommended Citation

Davis, James A. "Almost Difference Sets and Reversible Divisible Difference Sets." *Archiv Der Mathematik* 59, no. 6 (December 1992): 595-602. doi: 10.1007/BF01194853.

Arch. Math., Vol. 59, 595-602 (1992)

0003-889X/92/5906-0595 $ 3.10/0

Almost difference sets and reversible divisible difference sets

By

JAMES A. DAVIS

1. Introduction. 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 called a $(m, n, k, \lambda_1, \lambda_2)$ divisible difference set (DDS) 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 $G - N$ exactly λ_2 times. Difference sets are used to generate designs, as described by [4] and [9]. D will be called an Almost Difference set (ADS) if λ_1 and λ_2 differ by 1. The reason why these are interesting involves their relationship to symmetric difference sets. A symmetric difference set is a DDS with $\lambda_1 = \lambda_2$, so the ADS are "almost" difference sets. Symmetric difference sets are becoming more and more difficult to construct, and this is as close as we can get with a divisible difference set.

One helpful way to view DDS is to consider the group ring $Z[G]$. We will abuse notation by associating to the subset A of G the element $A = \sum_{a \in A} a$ of the group ring. Similarly, we will write $A^{(-1)} = \sum_{a \in A} a^{-1}$. The definition of a DDS immediately yields the group ring equation $DD^{(-1)} = k + \lambda_1(N - 1) + \lambda_2(G - N)$. This is often a very simple way to check whether a subset of a group meets the properties of being a divisible difference set, and it has the advantage that it works in nonabelian cases. We will use this technique to check the second construction.

We now restrict our attention to abelian groups; in this case, characters of the group are simply homomorphisms from the group to the complex numbers (we are following the lead of Turyn [13]). Extending this homomorphism to the entire group ring yields a map from the group ring to a number field. The character sum for the character χ on the element D of the group ring yields 3 possible results: $\chi(D) = k$ if χ is the principal (all 1) character, $|\chi(D)| = \sqrt{k - \lambda_1}$ if χ is nonprincipal on N, and $|\chi(D)| = \sqrt{k - \lambda_1 + (\lambda_1 - \lambda_2)\, n}$ if χ is principal on N but nonprincipal on G. One other useful fact about characters is that if χ is a nonprincipal character on a group (or subgroup) H, then the character sum of χ over H will be 0. If we have a subset of the group that satisfies these character sums for every character χ, then that subset will be a DDS (this is because of the orthogonality relations for characters: see [13] for similar arguments). Thus, our strategy will be to come up with a "candidate" subset of the group, then use character theory to check that all the sums are correct. We will use this techniques to check the first construction.

One other condition that we will note in this paper involves the multiplier group of the difference set. We say that a difference set is *reversible* if $D^{(-1)} = D$. This is a nice property for a set to have because it has strong implications for all of the other multipliers. For symmetric difference sets, it is conjectured that there is only one non-Menon difference set with multiplier -1. Reversible DDSs have been the subject of much recent research, with both constructions and nonexistence results appearing in the literature. In particular, Ma [10, 11] has provided several nonexistence results based on number theoretic considerations on the parameters. Jungnickel [7, 8], and then Arasu, Jungnickel, and Pott [2] have provided constructions of reversible DDSs based on the constructions for reversible symmetric difference sets found in McFarland's paper [10]. Construction 2 will yield some new reversible DDSs that generalize the constructions found in these papers.

2. Construction 1. The first construction has connections to a familiar set of parameters from symmetric difference sets. Turyn [14] has constructed $(4 \cdot 3^{2a}, 2 \cdot 3^{2a} - 3^a, 3^{2a} - 3^a)$ in groups of the form $H \times EA(3^{2a})$ where H is either group of order 4, and $EA(3^{2a})$ is the elementary abelian group of order 3^{2a}. In an effort to find other groups that have difference sets with these parameters, this author constructed divisible difference sets, but these divisible difference sets did not have λ_1 close to λ_2 (see [5]). Since then, this author, together with Jedwab, Arasu, and Sehgal have constructed difference sets with the same parameters as Turyn's examples (see [1]). A minor adjustment of that difference set will yield an ADS.

Let G be the group of the form $H \times Z_{3^a}^2$ where H is either group of order 4. The generators of the 3^a parts are y and z, and we will write the elements of H as h_0, h_1, h_2, h_3. The subgroup N is the group $\langle y, z\rangle \cong Z_{3^a}^2$. We also want to label the cyclic subgroups of order 3^a in a careful way. We will use $D_{1,i} = \langle yz^i\rangle$, $i = 0, 1, \ldots, \frac{3^{a+1}-1}{3-1} - 2$ and $D_{j,1} = \langle y^{3j}z\rangle$, $j = 0, 1, \ldots, \frac{3^a - 1}{3-1} - 1$. It is worth noticing that $D_{1,m} = D_{1,m+3^a}$ and $D_{n,1} = D_{n+3^{a-1},1}$. Consider the set

$$D = \left(\bigcup_{k=0}^{2} h_k\left(\bigcup_{i=0}^{\frac{3^a-1}{3-1}-1} z^i D_{1,3i+k}\right)\right) \cup \left(h_3\left(\bigcup_{j=0}^{\frac{3^a-1}{3-1}-1} y^j D_{j,1}\right)\right).$$

This is the "candidate" subset; we claim that this is an ADS with the parameters $(4{,}3^{2a}, 2(3^{2a} - 3^a), 3^{2a} - 2 \cdot 3^a, 3^{2a} - 2 \cdot 3^a + 1)$. The only difference between this and the difference sets found in [1] is this construction is missing one coset of the $D_{i,j}$. The proof is broken down into the following sequence of lemmas (these are the essentially the same as found in [1], and we do not include the proofs here).

Lemma 2.1. *D has no repeated elements.*

This ensures us that we will have the correct number of elements in the difference set, and that there is no overlapping of the cosets.

Lemma 2.2. *If χ is a character of order 3^a on G/H, then χ is nonprincipal on all of the $D_{i,j}$ except one, where it is principal.*

This lemma declares that any character of order 3^a will have a character sum of 0 over all of the $D_{i,j}$ except one. Thus, the character sum over the entire set will be (in modulus) the size of that $D_{i,j}$, which is 3^a. The only difficulty in the proof involves cases when the $D_{i,j}$ shows up twice. In that case, the character sum will be $3^a\chi(z^i)(1 + \xi^{3^{a-1}})$, where ξ is a primitive 3^a root of unity. The modulus of that sum is 3^a, so it matches what is required. The next lemma describes the situation for all of the other characters that are nonprincipal on the forbidden subgroup $\langle y, z\rangle$.

Lemma 2.3. *If χ is a character of G/H that is nonprincipal but of order less than 3^a, then*

$$\sum_{i=0}^{3^a-1} \chi(z^i D_{1,3i+k}) = \sum_{j=0}^{3^a-1} \chi(y^j D_{j,1}) = 0$$

for every k except 1, where the character sum is 3^a in modulus.

Thus, the character sum is correct for all of the characters that are nonprincipal on $\langle y, z\rangle$. All that remains is to check the character sums for the characters that are principal on $\langle y, z\rangle$, but nonprincipal on H. Each of the cosets of $\langle y, z\rangle$ has $\frac{3^{2a}-3^a}{2}$ elements, so the character sum is $\frac{3^{2a}-3^a}{2}\sum_{i=0}^{3}\chi(h_i) = 0 = \sqrt{k-\lambda_1+(\lambda_1-\lambda_2)\,n}$, which is correct. The next lemma summarizes that result.

Lemma 2.4. *If χ is a nonprincipal character on G that is principal on $\langle y, z\rangle$, then $\chi(D) = 0$.*

Putting all this together, we get the following

Theorem 2.1. *D is a* $(4,3^{2a}, 2(3^{2a}-3^a), 3^{2a}-2\cdot 3^a, 3^{2a}-2\cdot 3^a+1)$ ADS *in G.*

This DDS generates a divisible design with the same parameters, and that design is semi-regular since $k^2 = (2(3^{2a}-3^a))^2 = 4\cdot 3^{2a}(3^a-1)^2 = mn\lambda_2$. The author has not found this set of parameters in the literature, so this seems to be a new set of parameters for a semi-regular design that is also an ADS.

3. Construction 2. Another set of parameters that have been studied extensively for regular difference sets are $\left(q^{d+1}\left(\frac{q^{d+1}-1}{q-1}+1\right), q^d\left(\frac{q^{d+1}-1}{q-1}\right), q^d\left(\frac{q^d-1}{q-1}\right)\right)$. The original construction of these difference sets can be found in McFarland's paper [10]. Dillon [6] modified this construction slightly, and it has been further generalized in [2, 7, 8]. All of these constructions have the same basic strategy: take all of the hyperplanes of an elementary abelian group $EA(q^{d+1})$ (call them $H_1, H_2, \ldots, H_{\frac{q^{d+1}-1}{q-1}}$), and attach a different coset representative to each hyperplane. We consider one further generalization of this construction; instead of using a difference set (as in [2] and [8]), we will use a DDS with the property that $k-\lambda_1 = 1$. Let A be a $(m, n, h, h-1, \lambda_2)$ DDS in a group H relative to a normal subgroup K, where $h = \frac{q^{d+1}-1}{q-1}$. If the elements of A are a_i, $i = 1, 2, \ldots, h$, then form the set $D = \bigcup_{i=1}^{h} a_i H_i$ of $H \times EA(q^{d+1})$.

Theorem 3.1. *D is a $\left(m, nq^{d+1}, q^d \frac{q^{d+1}-1}{q-1}, q^d\left(\frac{q^d-1}{q-1}\right), q^{d-1}\lambda_2\right)$ DDS in $H \times EA(q^{d+1})$ relative to $K \times EA(q^{d+1})$.*

Proof:

$$\begin{aligned} DD^{(-1)} &= \sum_{i=1}^{h} a_i H_i \sum_{j=1}^{h} H_j a_j^{-1} \\ &= q^d \sum_{i=1}^{h} a_i H_i a_i^{-1} + q^{d-1} EA(q^{d+1}) \sum_{i \neq j} a_i a_j^{-1} \\ &= q^d \left[h + \frac{q^d-1}{q-1}(EA(q^{d+1})-1)\right] \\ &\quad + q^{d-1} EA(q^{d+1}) \left[\left(\frac{q^{d+1}-1}{q-1} - 1\right)(K-1) + \lambda_2(H-K)\right] \\ &= q^d \frac{q^{d+1}-1}{q-1} + q^d \frac{q^d-1}{q-1}((K \times EA(q^{d+1}))-1) \\ &\quad + q^{d-1}\lambda_2(G-(K \times EA(q^{d+1}))). \end{aligned}$$

We had to require that the set A be a DDS with the property $k - \lambda_1 = 1$ in order to satisfy the equation $q^{d-1}\lambda_1 = q^d \frac{q^d-1}{q-1}$. □

This construction works even if H and K are nonabelian groups, and it will also work if this is not a direct product group, but we will need to put a Dillon-like condition on the permutation of the hyperplanes.

Thus, we need to investigate the DDS that have the property $k - \lambda_1 = 1$. The first case we will consider is called a *trivial* case. Let H be any group with a normal subgroup K. It is easy to see that the set $(H-K) \cup \{1\}$ is a $(m, n, (m-1)n+1, (m-1)n, (m-1)n-n+2)$ DDS in H relative to K. Since this is a DDS with the correct property, we get the following corollary.

Corollary 3.1. *Suppose that n is a divisor of $\frac{q^{d+1}-1}{q-1} - 1$, and that $m = \dfrac{\frac{q^{d+1}-1}{q-1}}{n} + 1$. If H is any group of order mn with a normal subgroup K of order n, then we will get a $\left(m, nq^{d+1}, q^d\left(\frac{q^{d+1}-1}{q-1}\right), q^d\left(\frac{q^d-1}{q-1}\right), q^{d-1}((m-1)n-n+2)\right)$ DDS in $H \times EA(q^{d+1})$ relative to $K \times EA(q^{d+1})$.*

We should make several comments about this construction. First, when $n = 2$, the parameters reduce to a difference set (since $\lambda_1 = \lambda_2$), and this construction is McFarland's original idea. Second, when $n = 1$, we get the construction found in [2] and [8]. It is semiregular since $k^2 = q^{2d}\left(\frac{q^{d+1}-1}{q-1}\right)^2 = \frac{q^{d+1}-1}{q-1} q^{d+1} q^{d-1} \frac{q^{d+1}-1}{q-1} = mn\lambda_2$. It is not an ADS in general, but it is when $d = 1$ (these parameters are found in [2]).

Corollary 3.2. *If H is a group of order $q+1$, then $h \times EA(q^2)$ will have a $(q+1, q^2, q(q+1), q, q+1)$ ADS.*

Another interesting case occurs when $q = 3^a$, $n = 3$, and $d = 1$:

Corollary 3.3. *D is a $(3^{a-1}+1, 3^{2a+1}, 3^a(3^a+1), 3^a, 3^a-1)$ ADS in G.*

This is not a semi-regular example, but it is the only example that the author is aware of that has $\lambda_2 = \lambda_1 - 1$.

Finally, we consider an important consequence of this result that does not relate to ADS, we can get reversible DDS.

Corollary 3.4. *If m and n are both powers of 2, then there is a reversible DDS with the parameters listed above.*

Proof: Let the group be $Z_2^{u+v} \times EA(q^{d+1})$, where $m = 2^u$, $n = 2^v$. Since every element of Z_2^{u+v} is fixed under inversion, and every hyperplane is fixed under inversion, it is clear that $D = D^{(-1)}$. $\square$

We list several examples of this below:

#	n	q	d	m	$(m, nq^{d+1}, q^d h, q^d \frac{q^d-1}{q-1}, q^{d-1}\lambda_2)$
1	2	5	2	16	(16, 250, 775, 150, 150)
2	1	3	1	4	(4, 9, 12, 3, 4)
3	1	7	1	8	(8, 49, 56, 7, 8)
4	1	31	1	32	(32, 961, 992, 31, 32)
5	4	3	2	4	(4, 108, 117, 36, 30)
6	8	7	2	8	(8, 2744, 2793, 392, 350)
7	32	31	2	32	(32, 953312, 954273, 30752, 29822)
8	8	3	4	16	(16, 1944, 9801, 3240, 3078)

Notice several things about this list. First, Example # 1 is the sporadic example of a (non-Menon) symmetric difference set that has multiplier -1. Examples # 2–4 come from [2]. Examples # 5–7 all have the property that $m = n$, and $q = n - 1$. Whenever $2^u - 1$ is a prime power, then the corollary will apply to $m = n = 2^u$, $q = 2^u - 1$, $d = 2$. Thus, we will also have examples of DDS with -1 multiplier like # 5–7 for $n = 128$ and $n = 8192$. Finally, Example # 8 shows that there are examples of these DDS with d greater than 2.

Before we look at an example using a nontrivial DDS, we can make two minor modifications in this construction that will give similar parameters. Let $S_i = EA(q^{d+1}) - H_i$, the complement of the i^{th} hyperplane in $EA(q^{d+1})$. The (trivial) DDS that we have been using for this construction is $A = \{1\} \cup (H - K)$. If $a_1 = 1$, then form the set $D = H_1 \cup \left(\bigcup_{i=2}^{h} a_i S_i \right)$. If the group H is abelian, then we can analyze this set using character theory. If χ is a nonprincipal character on $EA(q^{d+1})$, then χ will be nonprincipal on all the hyperplanes except 1, so the character sum will be 0 on all of those other hyperplanes. Since χ is nonprincipal on $EA(q^{d+1})$, it will have character sum of 0 on all of the S_i associated to those hyperplanes. On the one hyperplane that χ is principal on, the character sum will have modulus the size of the hyperplane over either H_i or S_i, which is q^d. If χ is principal on $EA(q^{d+1})$, but nonprincipal on K, then I claim that the sum over $\bigcup_{i=2}^{h} a_i S_i$ will be 0. Thus, the sum over D is the size of H_1, which is q^d. Finally, if χ is principal on $K \times EA(q^{d+1})$ but nonprincipal on H, then the character sum is $q^d(n(q-1)-1)$. This proves the following theorem.

Theorem 3.2. *There is a* $(m, nq^{d+1}, q^d(q^{d+1} - q + 1), q^d(q^d - 1)(q - 1), q^{d-1}(q - 1) \cdot (q(q^d - 1) - n(q - 1) + 2))$ DDS *in* $H \times EA(q^{d+1})$ *relative to* $K \times EA(q^{d+1})$.

I am not aware of any new ADS from this theorem, but there will be new reversible DDS similar to the ones in the table above, such as (4, 108, 225, 144, 108); (8, 2744, 16513, 14112, 12180); and (16, 1944, 19521, 12960, 12204).

One other modification that we can make is to consider any divisor of $\frac{q^{d+1}-1}{q-1} + 1$, say n. If $mn = \frac{q^{d+1}-1}{q-1} + 1$, and if H is any group of order mn with a normal subgroup K of order n, then label the elements of H as $h_0, h_1, \ldots, h_{mn-1}$ where the elements of K are the first n elements in this list. The set $D = \left(\bigcup_{i=1}^{n-1} h_i H_i \right) \cup \left(\bigcup_{i=n}^{mn-1} h_i S_i \right)$ is a $(m, nq^{d+1}, q^d((m-1)n(q-1) + (n-1)), q^d((m-1)n(q-1) + (n-1) - q^d), \lambda_1 - q^{d-1}(q-2)[n(q-2)+2])$ DDS in $H \times EA(q^{d+1})$ relative to $K \times EA(q^{d+1})$. If H is abelian, the easiest proof is character theoretic like the above proof (we do not include it here). There are reversible DDS with these parameters when $q = 5, d = 2$.

Theorem 3.3. *There are reversible* DDS *with the parameters* (32, 125, 3100, 2475, 2400); (16, 250, 3025, 2400, 2280); (8, 500, 2875, 2250, 2040); (4, 1000, 2575, 1950, 1560); *and* (2, 2000, 1975, 1350, 600).

The first of these is the complement of one of the DDS found in [2]; I think that the rest are new.

Finally, we consider applications of Theorem 3.1 that use nontrivial DDS with $k - \lambda_1 = 1$. In [3], the authors list all known nontrivial DDS with that property, and the list includes two families. The first set has the parameters $(q', n, 1 + n(q'-1)/2, n(q'-1)/2, 1 + n(q'-3)/4)$ for q' a prime $\equiv 3 \pmod 4$ and $n \geqq 2$. The second set has parameters $(q', 2, q', q'-1, (q'-1)/2)$ for q' a square of an odd prime power. In either of those cases, we want the size of the DDS to divide $\frac{q^{d+1}-1}{q-1}$. We will state the result, then give examples of the possible constructions.

Corollary 3.5. a. *If* $\frac{q^{d+1}-1}{q-1} \equiv 1 \left(\bmod \frac{q'-1}{2}\right)$ (*for* q *a prime power and* q' *a prime power* $\equiv 3 \pmod 4$)*, then there is a*

$$\left(q', n q^{d+1}, q^d\left(\frac{q^{d+1}-1}{q-1}\right), q^d\left(\frac{q^d-1}{q-1}\right), q^{d-1}\left(1+n\frac{q'-3}{4}\right)\right)$$

DDS *in the group* $EA(q') \times K \times EA(q^{d+1})$ *relative to* $K \times EA(q^{d+1})$.

b. *If* $\frac{q^{d+1}-1}{q-1}$ *is equal to a square of an odd prime power* q', *then there is a*

$$\left(\frac{q^{d+1}-1}{q-1}, 2q^{d+1}, q^d\left(\frac{q^{d+1}-1}{q-1}\right), q^d\left(\frac{q^d-1}{q-1}\right), \left(q^d\left(\frac{q^d-1}{q-1}\right)\right)\Big/2\right)$$

DDS *in* $EA(q') \times Z_2 \times EA(q^{d+1})$ *relative to* $Z_2 \times EA(q^{d+1})$.

Examples of the first include a (7, 8, 6, 2, 3) ADS and

$$\left(3, q^{d+2}\frac{q^d-1}{q-1}, q^d\frac{q^{d+1}-1}{q-1}, q^d\frac{q^d-1}{q-1}, q^{d-1}\left(1+q\frac{q^d-1}{q-1}\,\frac{\frac{q^{d+1}-1}{q-1}-3}{4}\right)\right)$$

for any prime power q. An example of the second would be (121, 486, 9801, 3240, 1620).

References

[1] K. T. Arasu, J. A. Davis, J. Jedwab, and S. K. Sehgal, New Constructions of Menon difference sets. J. Combin. Theory Ser. A, to appear.

[2] K. T. Arasu, D. Jungnickel, and A. Pott, Divisible difference sets with multiplier -1. J. Algebra **133**, 35–62 (1990).

[3] K. T. Arasu, D. Jungnickel, and A. Pott, Symmetric divisible designs with $k-\lambda_1=1$. Discrete Math., to appear.

[4] T. Beth, D. Jungnickel, and H. Lenz, Design Theory. Cambridge 1986.

[5] J. A. Davis, New constructions of divisible designs. Submitted.

[6] J. F. Dillon, Variations on a scheme by McFarland for noncyclic difference sets. J. Combin. Theory Ser. A **40**, 9–21 (1985).

[7] D. Jungnickel, On automorphism groups of divisible designs. Canad. J. Math., **34**, 257–297 (1982).

[8] D. Jungnickel, A new family of relative difference sets. J. Combin. Theory Ser. A **52**, 301–303 (1989).

[9] E. S. Lander, Symmetric designs: an algebraic approach. Cambridge 1983.

[10] S. L. Ma, On divisible difference sets which are fixed by the inverse. Arch. Math. **54**, 409–416 (1990).

[11] S. L. Ma, It Abelian divisible difference sets with multiplier -1, J. Combin. Theory Ser. A, to appear.

[12] R. L. McFarland, A family of difference sets in noncyclic groups. J. Combin. Theory Ser. A **15**, 1–10 (1973).

[13] R. J. TURYN, Character sums and difference sets. Pacific J. Math. **15**, 319–346 (1965).
[14] R. J. TURYN, A special class of Williamson matrices and difference sets. J. Combin. Theory Ser. A **36**, 111–115 (1984).

Eingegangen am 16. 8. 1991 *)

Anschrift des Autors:

James A. Davis
Department of Mathematics
and Computer Science
University of Richmond
Richmond, Virginia 23173
USA

*) Eine Neufassung ging am 20. 3. 1992 ein.