Nonexistence Results on Chen and Davis-Jedwab Difference Sets

Bernhard Schmidt
Mathematisches Institut
Universität Augsburg
Universitätsstraße 15
86135 Augsburg
Germany

April 25, 2001

Proposed running head:

Nonexistence of Difference Sets

Author's address:

Bernhard Schmidt
Mathematisches Institut
Universität Augsburg
Universitätsstraße 15
86135 Augsburg
Germany

Abstract

We consider difference sets that have the parameters of the two series contructed recently by Chen respectively Davis and Jedwab. We show that the exponent bound following from the results of Turyn cannot be attained for these parameter series. In some cases this leads to a necessary and sufficient condition for the existence of such difference sets.

1 Introduction

A $(\mathbf{v},\mathbf{k},\lambda)$**-difference set** in a group G of order v is a k-subset D of G such that every nonidentity element g of G has exactly λ representations $g = d_1d_2^{-1}$ with $d_1, d_2 \in D$. In this paper, we only consider **abelian difference sets**, i.e. difference sets in abelian groups.
Recently, two new parameter series for difference sets were discovered by Chen (submitted) and Davis, Jedwab (1996). Chen's difference sets have parameters

$$\begin{aligned}
v &= 4q^{2t}\frac{q^{2t}-1}{q^2-1},\\
k &= q^{2t-1}[\frac{2(q^{2t}-1)}{q+1}+1],\\
\lambda &= q^{2t-1}(q-1)\frac{q^{2t-1}+1}{q+1},\\
n &= q^{4t-2},
\end{aligned}$$

where $q = p^f$ is a power of 3 or a square of an odd prime power and t is any positive integer. For $t = 1$, such a difference set is a Hadamard difference set. Any difference set with the above parameters (for any prime power q) and $t \geq 2$ will be called a **Chen difference set**. Chen's examples all have an elementary abelian Sylow p-subgroup; we will show that this is forced in some cases. However, in general there remains a large gap between the known necessary and sufficient conditions on the existence of Chen difference sets. I do not know if the exponent bound obtained in this paper can be improved. The other recent series of difference sets constructed by Davis and Jedwab has parameters

$$\begin{array}{rcl} v & = & 2^{2t+2}(2^{2t}-1)/3, \\ k & = & 2^{2t-1}(2^{2t+1}+1)/3, \\ \lambda & = & 2^{2t-1}(2^{2t-1}+1)/3, \\ n & = & 2^{4t-2}, \end{array}$$

where $t \geq 2$ is a positive integer. Any difference set with these parameters will be called a **Davis-Jedwab difference set**. Note that Davis-Jedwab difference sets are also Chen difference sets (put $q = 2$). Davis and Jedwab (1996) constructed Davis-Jedwab difference sets in all abelian groups of order $2^{2t+2}(2^{2t}-1)/3$ which have a Sylow 2-subgroup S_2 of exponent at most 4, with the single exception of $t = 2$ and $S_2 \cong \mathbf{Z}_4^3$. We will show that the condition $\exp(S_2) \leq 4$ is also necessary for the existence abelian Davis-Jedwab difference sets with the so-called character divisibility property.
Here we say that an (v, k, λ)-difference set D of square order $n = k - \lambda$ in an abelian group G has the **character divisibility property (CD property)** if the character value $\chi(D)$ is divisible by $\sqrt{n}$ for all nontrivial characters χ of G, see Jungnickel, Schmidt (to appear).
We emphasize that the CD property is a very natural assumption which is satisfied by all known difference sets with $\gcd(v, n) > 1$. Difference sets with $\gcd(v, n) > 1$ without the CD property - if they exist - must be difference sets of a completely new type. Therefore, it is reasonable to consider these two types of difference sets separately.

2 Preliminaries

Let us collect some results which will be needed in the following sections. Throughout the paper, we will use following notation. Let G be a finite abelian group. We identify a subset A of G with the element $\sum_{g \in A} g$ of the group ring $\mathbf{Z}G$. For $B = \sum_{g \in G} b_g g \in \mathbf{Z}G$ we write $|B| := \sum_{g \in G} b_g$ and $B^{(-1)} := \sum_{g \in G} b_g g^{-1}$. Let U be a subgroup of G; the natural epimorphism $G \to G/U$ is always assumed to be extended to $\mathbf{Z}G$ by linearity and is denoted by ρ_U. Furthermore, we write $G_U := G/U$. If D is a subset of G with $\rho_U(D) = \sum_{g \in G_U} d_g g$ then the numbers $d_g = |D \cap Ug|$ are called coefficients of $\rho_U(D)$ or intersection numbers of D with respect to U.

The following lemma is a direct consequence of the definition of a difference set.

Lemma 2.1 *Let D be a (v,k,λ)-difference set in an abelian group G, and let U be a subgroup of G. Then*

$$\rho_U(D)\rho_U(D)^{(-1)} = n + |U|\lambda G_U,$$

and hence

$$\chi(\rho_U(D))\overline{\chi(\rho_U(D))} = n$$

for every nontrivial character χ of G_U.

Definition 2.2 *A prime p is called self-conjugate modulo a positive integer m if there is a positive integer j with*

$$p^j \equiv -1 \bmod m',$$

where $m = p^a m'$ with $(m',p) = 1$.

Lemma 2.3 (Turyn (1965)) *Let ξ be a complex m-th root of unity, and let t be an integer which is self-conjugate modulo m. If $A \in \mathbf{Z}[\xi]$ and*

$$A\overline{A} \equiv 0 \bmod t^{2a}$$

for a positive integer a then

$$A \equiv 0 \bmod t^a.$$

As usual in papers on the existence of difference sets with $(v,n) > 1$, Ma's Lemma will be the essential tool.

Lemma 2.4 (Ma (1985)) *Let p be a prime, and let G be a finite abelian group with cyclic Sylow p-subgroup. If $Y \in \mathbf{Z}G$ satisfies the condition*

$$\chi(Y) \equiv 0 \ mod \ p^a$$

for all nontrivial characters χ of G then there are $X_1, X_2 \in \mathbf{Z}G$ with

$$Y = p^a X_1 + P X_2,$$

where P is the unique subgroup of order p of G.
Furthermore, the coefficients of X_1 and X_2 can be chosen to be nonnegative if Y has nonnegative coefficients.

The next lemma is a consequence of the inversion formula, see Curtis, Reiner (1962).

Lemma 2.5 *Let G be a finite abelian group, and let t be a postive integer. If $B \in \mathbf{Z}G$ with*

$$\chi(B) \equiv 0 \bmod t$$

for all characters of G then

$$B \equiv 0 \bmod t/(|G|, t).$$

Finally, we recall the central result of Turyn's classical paper [Turyn (1965, Theorem 6)]. By G^* we denote the character group of G.

Theorem 2.6 *Let D be any subset of an abelian group G, and let m be a positive integer such that $\chi\chi_1(D) \equiv 0 \bmod m$ for all χ in a subgroup H of G^*, $(|H|, m) = 1$, where χ_1 is a character of G of order $w > 1$ and $|H \cap \langle\chi_1\rangle| = 1$ and assume $\chi\chi_1(D) \neq 0$ for some $\chi \in H$. Then*

$$2^{r-1}|G| \geq mw|H|,$$

where r is the number of distinct prime divisors of w.

3 Chen difference sets

In this section, we will improve the exponent bound which follows from Theorem 2.6 in the case of Chen difference sets with odd q. In some cases, this will give a necessary and sufficient condition for the existence of these difference sets. We will use arguments similar to those of Arasu, Davis, Jedwab (1995). A very nice description of this method can be found in Pott (1995). As a consequence of Turyn's result we have the following.

Proposition 3.1 *Let $q = p^f$ be a prime power, and let G be an abelian group of order $4q^{2t}\frac{q^{2t}-1}{q^2-1}$ containing a Chen difference set D having the CD property. Denote the Sylow p-subgroup of G by S_p. Then the following hold.*
a) If p is odd then $exp(S_p) \leq q$.
b) If $p = 2$ then $exp(S_2) \leq 4q$.

Proof
a) Put $m = q^{2t-1}$, $|H| = 4\frac{q^{2t}-1}{q^2-1}$ and $w = \exp(S_p)$ in Theorem 2.6.
b) Put $m = q^{2t-1}$, $|H| = \frac{q^{2t}-1}{q^2-1}$ and $w = \exp(S_2)$ in Theorem 2.6. □

Remark
Because of Lemma 2.3, in the following cases every abelian Chen difference set must have the CD property.
a) q odd, $t = 2$ and the Sylow 2-subgroup of G is isomorphic to $\mathbf{Z}_2^3$ (note that 8 is the exact divisor of $|G| = 4q^4(q^2+1)$).
b) q even, $t = 2$.

We will improve the exponent bound following from Turyn's theorem by the following result.

Theorem 3.2 *Let $q = p^f$ be an odd prime power, and let G be an abelian group of order $4q^{2t}\frac{q^{2t}-1}{q^2-1}$, $f, t \geq 2$, containing a Chen difference set D having the CD property. Denote the Sylow p-subgroup of G by S_p. Then* $\exp(S_p) \leq p^{f-1}$.

Corollary 3.3 *Let $q = p^f$ be an odd prime power, and let G be an abelian group of order $4q^4(q^2+1)$. If the Sylow 2-subgroup S_2 is isomorphic to $\mathbf{Z}_2^3$ and a Chen difference set exists in G then the exponent of the Sylow p-subgroup S_p of G is at most p^{f-1}. In particular, if $f = 2$ and $S_2 \cong \mathbf{Z}_2^3$ then a Chen difference set in G exists if and only if S_p is elementary abelian.*

Proof of Theorem 3.2
Assume $S_p = \mathbf{Z}_q \times H$ where $\mathbf{Z}_q$ is a cyclic group of order q and H is a subgroup of S_p of order q^{2t-1}. We will use the notation introduced in Section 2. Let K be any complement of $\mathbf{Z}_q$ in S_p. By Ma's Lemma, we have

$$\rho_K(D) = q^{2t-1}X + PY, \tag{1}$$

where X, Y are elements of $\mathbf{Z}G_K$ having nonnegative coefficients and P is the subgroup of G_K of order p. Obviously, X can be viewed as a subset of G_K, and we can assume that no coset of P is contained in X. We write $w_g = |X \cap Pg|$ for $g \in G_K$ and $Y = \sum_{g \in T} a_g g$, where T is a set of distinct coset representatives of P in G_K. In view of (1), the coefficient of 1 in

$\rho_K(D)\rho_K(D)^{(-1)}$ is $p\sum a_g^2 + q^{4t-2}\sum w_g$. Hence Lemma 2.1 gives us

$$p\sum a_g^2 + q^{4t-2}\sum w_g = q^{4t-2} + q^{2t-1}\lambda. \tag{2}$$

Let L be the preimage of P under ρ_K. From (1) we see that the coefficient of 1 in $\rho_L(D)\rho_L(D)^{(-1)}$ is $p^2\sum a_g^2 + q^{4t-2}\sum w_g^2$. Hence Lemma 2.1 implies

$$p^2\sum a_g^2 + q^{4t-2}\sum w_g^2 = q^{4t-2} + pq^{2t-1}\lambda. \tag{3}$$

From (2) and (3) we infer

$$\sum_{g\in T}(pw_g - w_g^2) = p-1. \tag{4}$$

Since $0 \le w_g \le p-1$, we conclude that $w_h = 1$ or $p-1$ for one h and $w_g = 0$ for all $g \neq h$.

Now, fix any complement of $\mathbf{Z}_q$ in S_p, say H. From Lemma 2.5 we know that $\rho_H(D)$ is divible by q^{2t-2}, say $\rho_H(D) = q^{2t-2}u = \sum_{g\in G_H} b_g g$. Then by Lemma 2.1

$$uu^{(-1)} = q^2 + q^2(q-1)\frac{q^{2t-1}+1}{q+1}G_H,$$

hence $\sum b_g^2 = q^2 + q^2(q-1)\frac{q^{2t-1}+1}{q+1}$. Also, $\sum b_g = q(\frac{2(q^{2t}-1)}{q+1}+1)$ and $|G_H| = 4q\frac{(q^{2t}-1)}{q^2-1}$.

Let us define $c_g = b_g - (q-1)/2$. The point of this transformation is the nice formula

$$\sum_{g\in G_H} c_g^2 = q^2, \tag{5}$$

which is easily proved using the expressions for $\sum b_g$, $\sum b_g^2$ and $|G_H|$.

Since $\exp(H) \le q$ and $t \ge 2$, the rank of H must be at least three. Let $g_1, ..., g_r$, $r \ge 3$, be a basis of H, and let

$$K_{ijk} = \langle g_1 z^i, g_2 z^j, g_3 z^k, g_4, ..., g_r\rangle$$

for $i, j, k = 0, ..., p-1$, where z is an element of order p of $\mathbf{Z}_q$. Then each K_{ijk} is a complement of $\mathbf{Z}_q$ in S_p and $K_{ijk}K_{i'j'k'} = H\langle z\rangle$ for all $(i,j,k) \neq (i',j',k')$. From the conclusion following (4), we know that for every triple (i,j,k) there is a coset L_{ijk} of $K_{ijk}\langle z\rangle = H\langle z\rangle$ such that either

(i) there is a coset of K_{ijk} in L_{ijk} which is completely contained in D and all other cosets of K_{ijk} in L_{ijk} have an empty intersection with D or
(ii) there are $p-1$ cosets of K_{ijk} in L_{ijk} which are completely contained in D and the remaining coset has an empty intersection with D.

We conclude $L_{ijk} \neq L_{i'j'k'}$ for $(i,j,k) \neq (i',j',k')$. Otherwise $L_{ijk} = L_{i'j'k'}$ would have to be contained in D since every coset of K_{ijk} in L_{ijk} meets every coset of $K_{i'j'k'}$ in L_{ijk}.
Furthermore, we observe that every coset L_{ijk}, $(i,j,k) \neq (0,0,0)$, leads to p coefficients $b_g = p^{f-1}$ or $b_g = (p-1)p^{f-1}$ in $u = \rho_H(D)/q^{2t-2}$.
If $b_g = p^{f-1}$ then $c_g = \frac{1}{2}(-(p-2)p^{f-1}+1)$, and if $b_g = (p-1)p^{f-1}$ then $c_g = \frac{1}{2}((p-2)p^{f-1}+1)$. In both cases, we have $|c_g| \geq \frac{1}{2}((p-2)p^{f-1}-1)$. We also know that $b_g = q$ for at least one g since there is a $w_g \geq 1$. As there are (p^3-1) cosets L_{ijk}, $(i,j,k) \neq (0,0,0)$, it follows that

$$4\sum_{g\in G_H} c_g^2 \geq (q+1)^2 + (p^3-1)p[(p-2)p^{f-1}-1]^2. \qquad (6)$$

For $p=3$ and $f=2$, we get $4\sum_{g\in G_H} c_g^2 \geq 100 + 26\cdot 3\cdot 4 = 412$ which yields a contradiction since $4\sum_{g\in G_H} c_g^2 = 4q^2 = 324$ by (5). However, for $(p,f) \neq (3,2)$ we get

$$\begin{aligned} 4\sum_{g\in G_H} c_g^2 &> (p^3-1)p(p^{f-1}-1)^2 \\ &> (p^3-1)q(p^{f-1}-2) \\ &= q(p^{f+2}-p^{f-1}-2p^3+2) \\ &= q^2(p^2-1/p-2p^{3-f}+2/p^f) \\ &> 4q^2 \end{aligned}$$

(the last step uses $(p,f) \neq (3,2)$). This again contradicts (5). □

Remarks

a) The estimates used in the proof of Theorem 3.2 are rather crude. However, it seems to be unclear if this can be viewed as an evidence for a possible improvement of the exponent bound.
b) A brief look at the proof of Theorem 3.2 shows that the method does not work for $p=2$. In the next section, we present a method for $p=2$, $f=1$. It remains an open question if the exponent bound in Proposition 3.1 b) can be attained for $p=2$, $f>1$.

4 Davis-Jedwab difference sets

It was already mentioned that Davis-Jedwab difference sets exist in in all abelian groups of order $2^{2t+2}(2^{2t}-1)/3$, $t \geq 2$, which have a Sylow 2-subgroup S_2 of exponent at most 4, with the single possible exception of $t = 2$ and $S_2 \cong \mathbf{Z}_4^3$. In Ma, Schmidt (submitted), it was shown that for $t = 2$ an abelian group containing a Davis-Jedwab difference set must have a Sylow 2-subgroup of exponent at most 4. The following theorem is a generalization of this result.

Theorem 4.1 *Let G be an abelian group of order $2^{2t+2}(2^{2t}-1)/3$, $t \geq 2$, with Sylow 2-subgroup S_2. With the possible exception of $t = 2$ and $S_2 \cong \mathbf{Z}_4^3$, a Davis-Jedwab difference set D in G that has the CD property exists if and only if* $\exp(S_2) \leq 4$.

Remark
For $t = 2$ in Theorem 4.1 the CD property is always is satisfied, see Lemma 2.3. It is not known wether the CD property can be forced for $t > 2$ or acts as a wonderbra on Theorem 4.1.

Proof of Theorem 4.1
Putting $m = 2^{2t-1}$, $w = \exp(S_2)$ and $|H| = (2^{2t}-1)/3$ in Theorem 2.6 we conclude $\exp(S_2) \leq 8$. It remains to show $\exp(S_2) \neq 8$. Assume the contrary and write $S_2 = \mathbf{Z}_8 \times H$, where $\mathbf{Z}_8$ is cyclic of order 8 and $\exp(H) \leq 8$. If $\text{rank}(H) = 1$ then $t = 2$ and $S_2 \cong \mathbf{Z}_8^2$. However, this case was already excluded by Arasu, Sehgal (1995), see also Ma, Schmidt (1995, Corollary 3.3). Hence we can assume $\text{rank}(H) \geq 2$.
Let U be any be any complement of $\mathbf{Z}_8$ in S_2. From Lemma 2.5 we get $\rho_U(D) \equiv 0 \bmod 2^{2t-4}$, say $\rho_U(D) = 2^{2t-4}w_U$, $w_U = \sum_{g \in G_U} a_g g$, and Ma's Lemma gives

$$w_U = 8X + PY, \tag{7}$$

where P is the subgroup of order 2 in G_U and X, Y are elements of $\mathbf{Z}G_U$ with nonnegative coefficients. Since $\rho(D)$ cannot have coefficients greater than $|U| = 2^{2t-1}$, we conclude $|X \cap PY| = 0$.
Applying a character of order 8 to the equation

$$w_U w_U^{(-1)} = 64(1 + \frac{2^{2t-1}+1}{3} G_U) \tag{8}$$

following from Lemma 2.1, we see $|X_0| \geq 1$. Furthermore, we know that

$$\begin{aligned} |G_U| &= 8(2^{2t}-1)/3, \\ \sum a_g &= 8(2^{2t+1}+1)/3, \\ \sum a_g^2 &= 64(1+\frac{2^{2t-1}+1}{3}). \end{aligned}$$

The formula for $\sum a_g^2$ follows by comparing the coefficient of 1 in (8).
We define $b_g = a_g - 2$. Then a calculation using the formulae for $|G_U|$, $\sum a_g$ and $\sum a_g^2$ gives

$$\sum b_g^2 = 64. \tag{9}$$

If $|X| \geq 2$ then $\sum b_g^2 \geq 72$ which is impossible. Thus $|X| = 1$. Let z be the element of order 2 of $\mathbf{Z}_8$. Since $|X \cap PY| = 0$ we conclude that
$(*)$ for every complement U of $\mathbf{Z}_8$ in S_2 there is a coset L_U of $U\langle z\rangle$ such that one coset of U in L_U is completely contained in D and the other has empty intersection with D.
Write $H =< g_1, g_2 > \times K$ where possibly $|K| = 1$. Let $U_{ij} =< g_1z^i, g_2z^j > \times K$, $i,j = 0,1$. By $(*)$, obviously $L_{U_{ij}} \neq L_{U_{i'j'}}$ for $(i,j) \neq (i',j')$. Furthermore, the cosets $L_{U_{ij}}$, $(i,j) \neq (0,0)$, imply 6 coefficients 4 in w_H since every $L_{U_{ij}}$, $(i,j) \neq (0,0)$, is the union of two cosets of H which both intersect each of the two cosets of U_{ij} in $L_{U_{ij}}$ in exactly 4 elements.
Now, we will derive a contradiction to (9) for $U = H$. We know from above that w_H has one coefficient 8 and at least 6 coefficients 4. Let $\{a_g : g \in T\}$ be the remaining coefficients of w_H. Since

$$\begin{aligned} \sum_{g\in T} b_g &= |w_H| - (8 + 4\cdot 6) - 2(|G_H| - 7) \\ &= -10 \end{aligned}$$

we infer $\sum_{g\in T} b_g^2 \geq 10$. Thus

$$\begin{aligned} \sum b_g^2 &\geq (8-2)^2 + 6(4-2)^2 + 10 \\ &= 70, \end{aligned}$$

a contradiction to (9). □

5 References

K.T. Arasu, J.A. Davis, J. Jedwab, A nonexistence result for abelian Menon difference sets using perfect binary arrays, *Combinatorica*, **15** (1995), 311-317.

K.T. Arasu, J.A. Davis, J. Jedwab, S.L. Ma, R.L. McFarland, Exponent bounds for a family of abelian difference sets, In: *Groups, Difference Sets, and the Monster, Eds. K.T. Arasu, J.F. Dillon, K. Harada, S.K. Sehgal, R.L. Solomon*, DeGruyter Verlag, Berlin/New York (1996), 129-143.

K.T. Arasu, S.K. Sehgal, Difference sets in abelian groups of p-rank two, *Designs, Codes and Cryptography* **5** (1995), 5-12.

Y.Q. Chen, On the Existence of Abelian Hadamard Difference Sets and Generalized Hadamard Difference Sets, submitted.

C.W. Curtis, I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Wiley, New York, London (1962).

J.A. Davis, J. Jedwab: A unifying construction of difference sets. *Technical Report HPL-96-31*, Hewlett-Packard Labs., Bristol (1996).

D. Jungnickel, B. Schmidt, Difference Sets: An Update, to appear.

S.L. Ma, Polynomial addition sets, Ph.D. thesis, University of Hong Kong (1985).

S.L. Ma, B. Schmidt, On (p^a, p, p^a, p^{a-1})-Relative Difference Sets, *Designs, Codes and Cryptography* **6** (1995), 57-71.

S.L. Ma, B. Schmidt, A sharp exponent bound for McFarland difference sets with $p = 2$, submitted.

A. Pott, Finite geometry and character theory, Springer, New York (1995).

R.J. Turyn, Character sums and difference sets, *Pacific J. Math.* **15** (1965), 319-346.