Asymptotic Nonexistence of Difference Sets in Dihedral Groups

Ka Hin Leung
Department of Mathematics
National University of Singapore
Kent Ridge, Singapore 119260
Republic of Singapore

Bernhard Schmidt
Institut für Mathematik
Universität Augsburg
86135 Augsburg
Germany

April 26, 2001

Abstract

We prove that for any primes p_1,...,p_s there are only finitely many numbers $\prod_{i=1}^{s} p_i^{\alpha_i}$, $\alpha_i \in \mathbb{Z}^+$, which can be orders of dihedral difference sets. We show that, with the possible exception of $n = 540, 225$, there is no difference set of order n with $1 < n \leq 10^6$ in any dihedral group.

1 Introduction

Almost all known results on difference sets need severe restrictions on the parameters. The main purpose of this paper is to provide an asymptotic nonexistence result free from any assumptions on the parameters. The only assumption we make is that the underlying group is dihedral.

Difference sets originally mainly were studied in cyclic groups where they exist in abundance. For example, for any prime power n, there is a difference set in the cylic group of order n^2+n+1, namely, the so-called **Singer difference set**, see [2]. It is a very interesting phenomenon that the situation changes completely if one switches from cyclic groups to dihedral groups. No nontrivial difference set in any dihedral group has been found yet.

Conjecture 1 *There is no nontrivial difference set in any dihedral group.*

In the next section, we will see the reason for the probable nonexistence of dihedral difference sets: Putative difference sets in dihedral groups can be decomposed into two "orthogonal parts" corresponding to the two cosets of the subgroup of index two. The orthogonality of these two parts seems to be a too strong condition to admit solutions. It can be checked that a similar decomposition is impossible for all known difference sets in *cyclic* groups. This explains why difference sets in cyclic groups and dihedral groups behave so differently.

Difference sets in dihedral groups were thoroughly studied in [3]. The main result obtained there is the following.

Result 2 *If there is a nontrivial difference set of order n in a dihedral group, then $n=u^2$ for an odd integer u and $\varphi(u)/u<1/2$ where φ denotes the Euler totient function. In particular, u has at least three distinct prime divisors, and if u has exactly three distinct prime divisors p_1,p_2,p_3, then*

$$\{p_1,p_2,p_3\}\in\{\{3,5,7\},\{3,5,11\},\{3,5,13\}\}.$$

The main result we obtain in the present paper is quite different and of aymptotic nature: For any primes $p_1,...,p_s$ there are at most finitely many n of the form $\prod_{i=1}^{s}p_i^{\alpha_i}$, $a_i\in\mathbb{Z}^+$, which can be orders of difference sets in dihedral groups.

The central tool for the proof is the general bound on the absolute value of cyclotomic integers from [6, Thm. 4.2]. A combination of this bound with a substantial refinement of the arguments in [3] and careful number theoretic analysis yields the desired result. A similar asymptotic result for Hadamard difference sets has been obtained in [5, Thm. 6.1], but there the proof follows directly from the bound for the algebraic integers whereas the asymptotic result of the present paper needs substantial additional analysis.

In the final section, we obtain a nonexistence result for dihedral difference sets which is particularly useful for small cases. We use it to show that with one possible exception there is no dihedral difference set of order $n \leq 10^6$.

2 Preliminaries

In this section, we review the known facts which are needed in this paper. Let G be a multiplicatively written group of order v. A (v, k, λ, n) **difference set** is a k-subset D of G such that any nonidentity element of G has exactly λ representations as a quotient of two elements of D. The nonnegative integer $n = k - \lambda$ is called the **order** of D. We will only consider **nontrivial** difference sets, i.e. difference sets with $n > 1$. We also will assume $k < v/2$ which is possible without loss of generality since D is a (v, k, λ, n) difference set in G if and only if $G \setminus D$ is a $(v, v-k, v-2k+\lambda)$-difference set in G.

Given a difference set D, one can construct a finite geometry with point set G and block set $\{Dg : g \in G\}$ with the property that any two blocks meet in exactly λ points, see [2]. A difference set thus should be viewed as a concise description of a finite geometry.

When we study difference sets in a group G, we usually use the language of the group ring $\mathbb{Z}[G]$. For $X = \sum a_g g \in \mathbb{Z}[G]$ we write $|X| = \sum a_g$ and $X^{(t)} = \sum a_g g^t$. Let 1 be the identity element of G. For $r \in \mathbb{Z}$ we write r for the group ring element $r \cdot 1$, and for $S \subset G$ we write S instead of $\sum_{g \in S} g$. Using the group ring notation, a k-subset of a group G of order v is a (v, k, λ, n)-difference set in G if and only if

$$DD^{(-1)} = n + \lambda G$$

in $\mathbb{Z}[G]$. The following lemma from [3] is crucial for the study of difference sets in dihedral groups.

Lemma 3 *Let $D_m = \langle g, h | g^2 = h^m = ghgh = 1 \rangle$ denote the dihedral group of order $2m$ and write $C_m = \langle h \rangle$. There is a $(2m, k, \lambda, n)$ difference set in D_m if and only if there are $A, B \subset C_m$ with $|A| + |B| = k$ and*

$$AA^{(-1)} + BB^{(-1)} = \lambda C_m + n, \tag{1}$$

$$2AB \; = \; \lambda C_m. \qquad (2)$$

Proof Let D be a k-subset of D_m and write $D = A + Bg$ with $A, B \subset C_m$. A straightforward computation shows that $DD^{(-1)} = n + \lambda D_m$ if and only if (1) and (2) hold. □

By G^* we denote group of all characters $\chi : G \to \mathbb{C}$ of a finite abelian group G. The trivial character is denoted by χ_0. For a subgroup H of G^* we write

$$H^\perp = \{g \in G : \chi(g) = 1 \text{ for all } \chi \in H\}$$

and

$$U^\perp = \{\chi \in G^* : \chi(g) = 1 \text{ for all } g \in U\}.$$

for a subgroup U of G. Note that $\chi(g)$ is a complex t-th root of unity for all $\chi \in G^*$ and all $g \in G$ where $t = \exp G$. We write $\xi_t = e^{2\pi i/t}$. Any character can be extended naturally to a mapping $\mathbb{Z}[G] \to \mathbb{Z}[\xi_t]$ by linearity. For the basics on characters and difference sets, we refer the reader to [2, VI. §3]. We will make repeated use of the following.

Result 4 (Fourier inversion) *Let G be a finite abelian group and $A = \sum_{g\in G} a_g g \in \mathbb{Z}[G]$. Then the coefficients a_g are determined by the character values of A through*

$$a_g = \frac{1}{|G|} \sum_{\chi \in G^*} \chi(Ag^{-1}).$$

From Lemma 3 and the Fourier inversion we get the following.

Corollary 5 *There is a $(2m, k, \lambda, n)$ difference set in D_m if and only if there are $A, B \subset C_m$ with*

$$|A| + |B| = k \quad \text{and} \quad 2|A||B| = \lambda m$$

such that

$$\chi(A)\chi(B) = 0 \quad \text{and} \quad |\chi(A)|^2 + |\chi(B)|^2 = n$$

for every $\chi \in C_m^* \setminus \{\chi_0\}$.

The condition $\chi(A)\chi(B) = 0$ is the reason why we call the pieces A and B "orthogonal". Note that we can assume $|A| < |B|$ by replacing D by Dg if necessary which we will do from now on. The following essentially is a reformulation of [3, Thm. 2, Cor. 3] and gives an important restriction on the parameters of difference sets in dihedral groups.

Lemma 6 *Assume the existence of a $(2m, k, \lambda, n)$ difference set $D = A \cup Bg$ in D_m. Write $a = |A|$ and $b = |B|$ where $a < b$. Then $n = u^2$ for an odd integer $u > 1$, and there is an even divisor $c \le u - 1$ of $(u^2 - 1)/2$ such that*

$$\begin{aligned}
m &= \frac{u[(u+c)^2 - 1]}{2c} \\
n &= u^2 \\
a &= u(u+c-1)/2 \\
b &= u(u+c+1)/2 \\
k &= u(u+c) \\
\lambda &= uc.
\end{aligned}$$

Proof Put $u = b - a$ and $c = \lambda/u$. By Lemma 3 we have $a^2 + b^2 = \lambda m + n$ and $2ab = \lambda m$. Thus $n = u^2$. In particular, $u > 1$ since $n > 1$. Moreover, we have $a + b = k = n + \lambda = u(u + c)$ and this together with $u = b - a$ gives the formulas for a and b. We then get the formula for m from $2ab = \lambda m = ucm$. Furthermore, $n + \lambda = u(u + c)$ shows that λ is divisible by u. Thus c is an integer. For the proof of the fact that u is odd, we refer to [3, Cor. 3]. By the formula for m, we see that $(u + c)^2 - 1$ is even. Thus, c must be even and hence λ is also even. We recall that we assume $k < v/2$ for a (v, k, λ, n) difference set. Since $k(k - 1) = \lambda(v - 1)$ we have $\lambda < n$. This implies $c < u$. In [3, Thm. 2] it is shown that u divides m. Thus $2c$ divides $(u + c)^2 - 1$ and thus $u^2 - 1$ since c is even. □

Let $D = A \cup Bg$ be a difference set in D_m as in Lemma 3. Using Corollary 5, we can partition the nontrivial characters of C_m into two disjoint sets **A** and **B** as follows.

$$\mathbf{A} := \{\chi \in C_m^* : |\chi(A)|^2 = n\}, \ \mathbf{B} := \{\chi \in C_m^* : |\chi(B)|^2 = n\}.$$

In [3, Thm. 4] and its proof the following was shown.

Result 7 *Either* $\mathbf{A}$ *or* $\mathbf{B}$ *is a union of cosets of the subgroup of* C_m^* *of order* $m/(m,n)$*. Furthermore,*

$$\begin{aligned} |\mathbf{A}| &= (ma - a^2)/n, \\ |\mathbf{B}| &= (mb - b^2)/n. \end{aligned}$$

Let U_m *be the group of units modulo* m*. Then* U_m *acts on* C_m^* *by* $\chi \mapsto \chi^l$ *for* $l \in U_m$*. Both* $\mathbf{A}$ *and* $\mathbf{B}$ *are unions of orbits of* U_m *on* C_m^**.*

Now we state the results on cyclotomic integers from [5, 6] we will use. We first need a definition.

Definition 8 *Let* m*,* n *be positive integers, and let* $m = \prod_{i=1}^t p_i{}^{c_i}$ *be the prime power decomposition of* m*. For a prime* q *write*

$$m_q := \begin{cases} \prod_{p_i \neq q} p_i & \text{if } m \text{ is odd or } q = 2, \\ 4\prod_{p_i \neq 2,q} p_i & \text{otherwise.} \end{cases}$$

Let $\mathbf{D}(n)$ *be the set of prime divisors of* n*. For* $q \in \mathbf{D}(n)$ *and* $i \in \{1,...,t\}$*, let* $B(q,i)$ *be the smallest positive integer such that one of the following conditions is satisfied.*
(a) $q = p_i$ *and if* $p_i = 2$ *then* $B(q,i) \neq 1$*,*
(b) $B(q,i) = c_i$*,*
(c) $q \neq p_i$ *and* $q^{\mathrm{ord}_{m_q}(q)} \not\equiv 1 \pmod{p_i^{B(q,i)+1}}$*.*
For $i = 1,...,t$ *let* $b_i := \max\{B(q,i) : \ q \in \mathbf{D}(n)\}$*. We define*

$$F(m,n) := \prod_{i=1}^t p_i^{b_i}.$$

The properties of the function $F(m,n)$ just defined are crucial for the proof of our asymptotic result in the next section. Note that $F(m,n)$ and m have the same prime divisors since b_i is positive for all i. The following result was proved in [5].

Result 9 *Assume* $X\overline{X} = n$ *for* $X \in \mathbb{Z}[\xi_m]$ *where* n *and* m *are positive integers. Then*

$$X\xi_m^j \in \mathbb{Z}[\xi_{F(m,n)}]$$

for some j*.*

The next result essentially is contained in [6].

Result 10 *Let X be of the form*

$$X=\sum_{i=0}^{m-1} a_i\xi_m^i$$

with $0\le a_i\le C$ for some constant C. Let f be a divisor of m which has the same prime divisors as m. If $X\in\mathbb{Z}[\xi_f]$ and if $n:=X\overline{X}$ is an integer, then

$$n\le\frac{C^2f^2}{4\varphi(f)}.$$

Proof The proof is the same as that of Theorem 4.2 of [6], we only have to replace $F(m,n)$ there by f. □

Corollary 11 *If a difference set D of order n exists in the dihedral group of order $2m$, then*

$$4n\le\frac{m}{\varphi(m)}F(m,n).$$

Proof Write $D=A\cup Bg$ with $A,B\subset C_m$. Let χ be a character of C_m order m. By Corollary 5 we have $|\chi(A)|^2=n$ or $|\chi(B)|^2=n$. We only treat the case $|\chi(A)|^2=n$, the other case is similar. Note $\chi(A)=\sum_{i=0}^{m-1}a_i\xi_m^i$ with $0\le a_i\le 1$. Furthermore, $F(m,n)/\varphi(F(m,n))=m/\varphi(m)$ since m and $F(m,n)$ have the same prime divisors. Thus the assertion follows from Results 9 and 10. □

3 Asymptotic nonexistence

In this section, we prove that for any primes p_1,...,p_s there are only finitely many numbers $\prod_{i=1}^{s}p_i^{\alpha_i}$, $\alpha_i\in\mathbb{Z}^+$, which can be orders of dihedral difference sets. We start with a general lemma. By $[x]$ we denote the largest integer $\le x$.

Lemma 12 *Let G be a finite abelian group, and let X be an element of $\mathbb{Z}[G]$ with nonnegative coefficients. Assume that $|\chi(X)|^2 \in \{0, n\}$ for some positive integer n and all nontrivial characters χ of G. Let N be the number of nontrivial characters χ with $|\chi(X)|^2 = n$. Then*

$$N \geq \frac{\epsilon(1-\epsilon)|G|^2}{n}$$

where $\epsilon = |X|/|G| - [|X|/|G|]$.

Proof Write $X = \sum a_g g$ with $a_g \in \mathbb{Z}_0^+$ and $|G| = v$, $|X| = x$. Then $x/v = y + \epsilon$ where $y = [x/v]$. The minimum of $\sum a_g^2$ under the conditions $\sum a_g = x$, $a_g \in \mathbb{Z}_0^+$, is attained if and only if $a_g \in \{y, y+1\}$ for all $g \in G$, see [4]. In that case, the number of g's with $a_g = y+1$ is ϵv. Hence $\sum a_g^2 = (1-\epsilon)vy^2 + \epsilon v(y+1)^2 = x^2/v + v\epsilon(1-\epsilon)$. Thus for *all* $a_g \in \mathbb{Z}_0^+$ with $\sum a_g = x$ we get

$$\sum a_g^2 \geq \frac{x^2}{v} + v\epsilon(1-\epsilon). \tag{3}$$

On the other hand, since $\sum a_g^2$ is the coefficient of 1 in $XX^{(-1)}$, we have

$$\sum a_g^2 \leq \frac{1}{v}[x^2 + Nn] \tag{4}$$

by the Fourier inversion formula. The lemma follows by combining (3) and (4). □

Notation 13 The following notation will be used throughout this section. In the situation of Lemma 6, write $2c = 2^{\alpha+\beta}c_1c_2$ where c_1, c_2 are odd divisors of $u-1$ and $u+1$ respectively and $2^\alpha \mid (u-1)$, $2^\beta \mid (u+1)$. As c is even, we may assume $\alpha \geq 1$ and $\beta \geq 1$. Write $u-1 = 2^\alpha c_1 d_1$ and $u+1 = 2^\beta c_2 d_2$. Then $u-1+c = 2^\alpha c_1(d_1 + 2^{\beta-1}c_2)$ and $u+1+c = 2^\beta c_2(d_2 + 2^{\alpha-1}c_1)$. Next, we write $d_1 + 2^{\beta-1}c_2 = u_1 t_1$ and $d_2 + 2^{\alpha-1}c_1 = u_2 t_2$ where t_1 and t_2 are the greatest divisors of $d_1 + 2^{\beta-1}c_2$ respectively $d_2 + 2^{\alpha-1}c_1$ which are relatively prime to u. In particular, we deduce that $m = uu_1u_2t_1t_2$. For the convenience of the reader we give a table of the necessary identities.

$$\begin{aligned} c &= 2^{\alpha+\beta-1}c_1c_2 \\ u-1 &= 2^{\alpha}c_1d_1 \\ u+1 &= 2^{\beta}c_2d_2 \\ d_1+2^{\beta-1}c_2 &= u_1t_1 \\ d_2+2^{\alpha-1}c_1 &= u_2t_2 \\ u+c-1 &= 2^{\alpha}c_1u_1t_1 \\ u+c+1 &= 2^{\beta}c_2u_2t_2 \\ m &= uu_1u_2t_1t_2 \end{aligned}$$

Lemma 14 *Either a or b is divisible by $m/(m,n)$. We have $t_1 = 1$ or $t_2 = 1$. More precisely, we have $t_1 = 1$ if $m/(m,n)$ divides b and $t_2 = 1$ if $m/(m,n)$ divides a. With m' denoting the largest divisor of m coprime to u, we have $m' = t_1t_2 < u$.*

Proof We first show $m/(m,n)$ divides a or b. Let H be the subgroup of C_m of order (m,n). By Result 7 we have $\chi(A) = 0$ for all $\chi \in H^{\perp} \setminus \{\chi_0\}$ or $\chi(B) = 0$ for all $\chi \in H^{\perp} \setminus \{\chi_0\}$. Let $\rho : C_m \to C_m/H$ be the canonical epimorphism. Then, by the Fourier inversion formula, $\rho(A)$ or $\rho(B)$ is a multiple of C_m/H. Thus $|C_m/H| = m/(m,n)$ divides a or b.
Note that $m' = t_1t_2$ by definition. Suppose that $m/(m,n)$ divides $a = u(u+c-1)/2$. Then t_2 divides a. Since t_2 divides b by definition, it also divides $u = b-a$. As $(t_2,u) = 1$ we conclude $t_2 = 1$. Since $t_1 \mid (u+c-1)/2$ and $c < u$, we get $t_1t_2 < u$. The same argument works in the case that $m/(m,n)$ divides b. □

Theorem 15 *Write $u = \prod_{i=1}^{r} p_i^{\alpha_i}$ where the p_i's are distinct primes. Then $u/c < \prod_{i=1}^{r} p_i$. Moreover, if s is the largest integer such that $u/c > p_1p_2\cdots p_s$, then*

$$2\varphi(u) \le \varphi(P)u/P + 2^s c \tag{5}$$

where $P = \prod_{i=1}^{s} p_i$.

Proof For convenience, we denote the unique subgroup of order d of C_m by $G(d)$. By assumption we have $u > cP$. Let $d > 1$ be a divisor of P. Then $d < u/c$ and thus

$$a/(m/d) = ad/m < au/cm = u/(u+c+1) < 1. \tag{6}$$

Let $\rho : C_m \to C_m/G(d)$ be the canonical epimorphism. Note that the character values of $\rho(A)$ are exactly the values $\chi(A)$, $\chi \in G(d)^\perp$. From Lemma 12 with $X = \rho(A)$, $G = G(d)$ and $\epsilon = ad/m$ we get

$$u^2|\mathbf{A} \cap G(d)^\perp| \geq a(\frac{m}{d} - a).$$

Hence

$$|\mathbf{A} \cap G(d)^\perp| \geq (\frac{1}{2} + \frac{c-1}{2u})(\frac{m}{d} - \frac{u(u+c-1)}{2}). \tag{7}$$

Since $(c-1)/2u$ and $(m/d - u(u+c-1)/2)$ are both positive, we get

$$|\mathbf{A} \cap G(d)^\perp| > \frac{m}{2d} - \frac{u(u+c-1)}{4}. \tag{8}$$

Since $u(u+c-1)/4 < (u+c-1)^2/4 = mc/(2u)$ we get

$$|\mathbf{A} \cap G(d)^\perp| \geq \frac{m}{2d} - \frac{mc}{2u} \tag{9}$$

from (8). Similarly, we derive

$$|\mathbf{B} \cap G(d)^\perp| \geq \frac{m}{2d} - \frac{mc}{2u}$$

and thus

$$|\mathbf{A} \cap G(d)^\perp| < \frac{m}{2d} - \frac{mc}{2u} \tag{10}$$

since $|\mathbf{A} \cap G(d)^\perp| = \frac{m}{d} - |\mathbf{B} \cap G(d)^\perp| - 1$.
Let μ denote the Möbius function. Write $U = \cup_{i=1}^s G(p_i)^\perp$. Using (9), (10), inclusion-exclusion, and the well known formula $\varphi(P)/P = \sum_{d|P} \mu(d)/d$ we get

$$|\mathbf{A} \cap U| \quad = \quad \sum_{d|P,\ d>1} -\mu(d)|\mathbf{A} \cap G(d)^\perp|$$

$$\begin{aligned} &\geq \sum_{d|P,\ d>1} (-\mu(d)\frac{m}{2d} - \frac{mc}{2u}) \\ &= -\frac{m}{2}(\sum_{d|P,\ d>1} \frac{\mu(d)}{d}) - 2^{s-1}\frac{mc}{u} \\ &= \frac{m}{2}(1 - \frac{\varphi(P)}{P}) - 2^{s-1}\frac{mc}{u}. \end{aligned}$$

In the same way we estimate $|\mathbf{B} \cap U|$ and get

$$\min(|\mathbf{A} \cap U|, |\mathbf{B} \cap U|) \geq \frac{m}{2}(1 - \frac{\varphi(P)}{P}) - 2^{s-1}\frac{mc}{u}. \tag{11}$$

Let χ be a character of C_m of order m, and let W be the subgroup of C_m^* of order $m/(m,n)$. By Result 7 the set

$$S := \bigcup_{\substack{i=1 \\ (i,m)=1}}^{m-1} W\chi^i$$

is contained either in $\mathbf{A}$ or $\mathbf{B}$. Note $|S| = \varphi((m,n))|W| = m\varphi(n)/n$. Now we are going to show that $S \cap U = \emptyset$. We claim that for any character $\tau \in W$, τ is trivial on $G(p_j)$ for $j = 1, \dots, s$. Note that the claim is obvious if p_j does not divide the order of τ. In case that p_j divides the order of τ, we observe that $p_j \mid (m/|W|)$ also, so τ must also be trivial on $G(p_j)$. Now, as χ^i is nontrivial on $G(p_j)$ for all i with $(i,m) = 1$ and $j = 1, \dots, s$, we conclude $W\chi^i \cap U = \emptyset$ for $(i,m) = 1$. Hence, $S \cap U = \emptyset$. Thus together with (11) we get

$$\begin{aligned} \max(|\mathbf{A}|, |\mathbf{B}|) &\geq m\varphi(n)/n + \frac{m}{2}(1 - \frac{\varphi(P)}{P}) - 2^{s-1}\frac{mc}{u} \\ &= \frac{m}{2}[1 + \frac{2\varphi(u)}{u} - \frac{\varphi(P)}{P} - \frac{2^s c}{u}]. \end{aligned}$$

Using Result 7 it is straightforward to check that

$$|\mathbf{A}| < |\mathbf{B}| < \frac{m}{2} + \frac{m}{2u}.$$

Combining the last two estimates gives

$$\frac{m}{2}[\frac{2\varphi(u)}{u} - \frac{\varphi(P)}{P} - \frac{2^s c}{u}] < \frac{m}{2u}$$

and thus $2\varphi(u) - \varphi(P)u/P - 2^s c < 1$. Since $2\varphi(u) - \varphi(P)u/P - 2^s c$ is an integer, this implies (5).
It remains to show that $r = s$ is impossible. When $r = s$, then $\varphi(P)/P = \varphi(u)/u$. Recall $u/c > P$. Since $r \geq 3$, we get $2^r c < 2^r u/P = 2^r[u/(\varphi(u)P)]\varphi(u) = 2^r(\prod_{i=1}^r (p_i - 1)^{-1})\varphi(u) \leq 2^3 \cdot 2^{-1} \cdot 4^{-1} \cdot 6^{-1}\varphi(u) = \varphi(u)/6$. Now (5) gives the contradiction $2\varphi(u) < \varphi(u) + \varphi(u)/6$. Hence $s < r$. □

We will need the following properties of the function F from Definition 8. For a prime p and an integer y we write $p^a \parallel y$ if $p^a \mid y$ and $p^{a+1} \not| \, y$.

Lemma 16 *Let r, s, x be positive integers where x is coprime to rs. Then*
a) $F(r,s)$ divides r,
b) $F(rx,s)$ divides $x \gcd(e,r)F(r,s)$ where e is the exponent of the group $\mathbb{Z}_x^*$.

Proof Part a holds because of condition b in Definition 8. For part b, let p_i be a prime divisor of rx and define b_i by $p_i^{b_i} \parallel F(rx,s)$. We have to show $p_i^{b_i} \mid x \gcd(e,r)F(r,s)$. If $p_i \mid x$ then $p_i^{b_i} \mid x$ by part a, and we are finished. Thus let $p_i \mid r$. Define b_i', a and c_i by $p_i^{b_i'} \parallel F(r,s)$, $p_i^a \parallel e$ and $p_i^{c_i} \parallel r$. Since $b_i \leq c_i$ by part a, it suffices to show $b_i \leq b_i' + a$. Let $\mathbf{D}(s)$ be the set of prime divisors of s, and let $q \in \mathbf{D}(s)$. Let $B(i,q)$, $B(i,q)'$ be the numbers defined in Definition 8 when applied to $F(rx,s)$ respectively $F(r,s)$. By Definition 8 applied to $F(r,s)$ one of the following cases holds.

Case 1 $q = p_i$ and $(p_i, B(i,q)') \neq (2,1)$. Then $B(i,q) \leq B(i,q)'$ by Definition 8, condition a, applied to $F(rx,s)$.

Case 2 $B(i,q)' = c_i$. Then $B(i,q) \leq B(i,q)'$ since $B(i,q) \leq c_i$ by Definition 8, condition b, applied to $F(rx,s)$.

Case 3 $q \neq p_i$ and

$$q^{\Gamma'} \not\equiv 1 \pmod{p_i^{B(i,q)'+1}} \tag{12}$$

where $\Gamma' = \mathrm{ord}_{m_q'}(q)$ and

$$m_q' = \begin{cases} \prod_{p_j \mid r,\ p_j \neq q} p_j & \text{if r is odd or } q = 2, \\ 4\prod_{p_j \mid r,\ p_j \neq 2,q} p_j & \text{otherwise.} \end{cases}$$

Note that

$$q^{\Gamma'} \equiv 1 \pmod{p_i} \text{ and } q^{\Gamma'} \equiv 1 \pmod{4} \text{ if } r \equiv 0 \bmod 2 \text{ and } q \neq 2. \tag{13}$$

Let Γ be defined as Γ' only with r replaced by rx. Then $\Gamma \mid e\Gamma'$ where $e = \exp \mathbb{Z}_x^*$. Now (12), (13), $\Gamma \mid e\Gamma'$, and $p_i^{a+1} \not| \, e$ imply

$$q^\Gamma \not\equiv 1 \pmod{p_i^{B(i,q)'+a+1}}.$$

Thus $B(i,q) \leq B(i,q)' + a$ by Definition 8, condition c, applied to $F(r,s)$. In summary, we have shown $B(i,q) \leq B(i,q)' + a$ for all $q \in \mathbf{D}(s)$ in every possible case. Thus

$$b_i = \max\{B(i,q) : q \in \mathbf{D}(s)\} \leq a + \max\{B(i,q)' : q \in \mathbf{D}(s)\} = b_i' + a$$

concluding the proof. □

Lemma 17 *Let $p_1, ..., p_t$ be any primes. Then there is a constant $K \in \mathbb{Z}^+$ only depending on the p_i such that $F(r,s) \mid K$ for all r and s which are products of powers of the p_i.*

Proof We use the notation of Definition 8. Write $T := \prod_{i=1}^t p_i$. Let $i \in \{1, ..., t\}$ and $q \in \mathbf{D}(s)$ be arbitrary. If $q = p_i$, then $B(i,q) \leq 2$ by Definition 8, condition a. Note that $m_q \leq 2T$ and thus $q^{\mathrm{ord}_{m_q}(q)} < T^{2T}$. Hence, as a very crude estimate, $B(q,i) < T^{2T}$ by Definition 8, condition c, if $q \neq p_i$. This implies

$$F(r,s) \mid T^{T^{2T}}.$$

□

Lemma 18 *Let s be a positive integer and $x \in \mathbb{R}$ with $x \geq 2s$. Then*

$$\left((1 + \frac{1}{x})^s - 1 \right) x < 2s.$$

Proof This follows from $(1+1/x)^s < \sum_{i=0}^s (s/x)^i = 1 + (s/x) \sum_{i=0}^{s-1} (s/x)^i \leq 1 + (s/x) \sum_{i=0}^{s-1} (1/2)^i < 1 + 2s/x$. □

Theorem 19 *Let $p_1, \ldots, p_r$ be distinct primes. There are only finitely many u's of the form $\prod_{i=1}^r p_i^{\alpha_i}$ for which a dihedral difference set of order u^2 can exist.*

Proof It will be sufficient to deal with the case where $\alpha_i \geq 1$ for all i. We will only treat the case $t_1 = 1$. The case $t_2 = 1$ can be done in exactly the same way by adjusting some signs and indices.

In the following, when we say that a number x depending on u "is bounded" we mean that there is a constant K such that $x \leq K$ for all u of the form $\prod_{i=1}^{r} p_i^{\alpha_i}$. In this sense, Theorem 15 shows that u/c is bounded.

Recall that $m = uu_1u_2t_1t_2 = uu_1u_2t_2$ where $t_2 = m' < u$ is the largest divisor of m coprime to u. Let e be the exponent of the group $\mathbb{Z}_{t_2}^*$ and $P = \gcd(e, uu_1u_2)$. Write $t_2 = \prod q_j^{\alpha_j}$ where the q_j's are primes, and let L be the least common multiple of all the $(q_j - 1)$'s. Then $P = \gcd(L, uu_1u_2)$ as t_2 and u are relatively prime. Thus, for each i, there exists a j_i such that the highest powers of p_i dividing P respectively $q_{j_i} - 1$ are equal. Hence, we may rearrange the q_j's such that $P \mid \gcd(\prod_{j=1}^{s}(q_j - 1), uu_1u_2)$, $s \leq r$ and $q_1 < \cdots < q_s$.

Write $F(m, u) = Mu'$ where M is the largest divisor of $F(m, u)$ relatively prime to u. By Lemma 16 we have $M \mid t_2$ and $u' \mid F(u_1u_2u, u) \cdot P$. By Corollary 11, we get

$$4 \leq \frac{M^2 u'^2}{\varphi(M)\varphi(u')u^2} = \frac{u'}{\varphi(u')} \cdot \frac{u'}{\varphi(M)} \cdot \frac{M^2}{u^2}.$$

Write $t_2 = Y \prod_{i=1}^{s} q_i$. Since $M \mid t_2$, we have $M^2/\varphi(M) \leq t_2^2/\varphi(t_2)$. Furthermore, $\varphi(t_2) \geq \varphi(Y)\varphi(q_1 \cdots q_s)$. On the other hand, as u and u' have the same set of prime factors, $u/\varphi(u) = u'/\varphi(u')$. Therefore, we obtain

$$4 \leq \frac{u}{\varphi(u)} \cdot \frac{u'}{\varphi(Y)\varphi(q_1 \cdots q_s)} \cdot \frac{t_2^2}{u^2}. \tag{14}$$

By Lemma 17 there is a constant E such that $F(u_1u_2u, u) \mid E$ for all u's which are products of powers of the p_i. Since $u' \mid F(u_1u_2u, u) \cdot P$, we have $u' \mid EP$. Using $t_2 < u$, $P \mid \varphi(q_1 \cdots q_s)$ and (14) we get $4u/t_2 < (u/\varphi(u)) \cdot (E/\varphi(Y))$ and thus

$$\frac{u}{t_2} \text{ is bounded.} \tag{15}$$

Combining (14) with the fact that $u \geq (u+c+1)/2 = 2^{\beta-1}c_2u_2t_2$, we deduce

$$4 \leq \frac{u}{\varphi(u)} \cdot \frac{u'}{\varphi(q_1 \cdots q_s)} \cdot \frac{1}{\varphi(Y)2^{2\beta-2}c_2^2u_2^2}. \tag{16}$$

Since $u' \mid EP$ we can replace u' by EP in (16) and get

$$\frac{\varphi(q_1\cdots q_s)}{P} \le \frac{u}{\varphi(u)}\cdot\frac{E}{\varphi(Y)2^{2\beta}c_2^2u_2^2}. \tag{17}$$

From (17), we see that $\varphi(q_1\cdots q_s)/P$ is bounded. Also, since $P \mid \varphi(q_1\cdots q_s)$ we see from (17) that $\varphi(Y)$ is bounded. Thus

$$Y \text{ is bounded.} \tag{18}$$

We shall see later that (17) actually also forces all q_i's to be bounded. Using our table of identities in Notation 13, we obtain $d_1 2^\beta c_2 u_2 t_2 = d_1(u+c+1) = d_1(u+c-1) + 2d_1 = [(u-1)2^{-\alpha}c_1^{-1}][2^\alpha c_1 u_1] + 2d_1 = (u-1)u_1 + 2d_1 = uu_1 - (u_1 - d_1) + d_1 = uu_1 - 2^{\beta-1}c_2 + d_1$. Hence

$$d_1 2^\beta c_2 u_2 t_2 = uu_1 + d_1 - 2^{\beta-1}. \tag{19}$$

For $1 \le \ell \le s$, we define

$$Q(\ell) = \gcd(\prod_{i=\ell}^{s}(q_i - 1), uu_1).$$

Note that $Q(1) \ge P/u_2$. As u is odd, $Q(\ell) \ge Q(1)\prod_{i=1}^{\ell-1}\frac{2}{q_i-1}$ where $\prod_{i=1}^{\ell-1}\frac{2}{q_i-1}$ is defined to be 1 if $\ell = 1$. Thus

$$Q(\ell) \ge \frac{P}{u_2}\cdot\prod_{i=1}^{\ell}\frac{2}{q_i-1}. \tag{20}$$

By (19) and the definition of $Q(\ell)$ we have

$$d_1 - 2^{\beta-1}c_2 \equiv d_1 2^\beta c_2 u_2 t_2 \equiv d_1 2^\beta c_2 u_2[t_2 - Y(\prod_{i=1}^{\ell-1} q_i)(q_\ell - 1)\cdots(q_s - 1)] \bmod Q(\ell).$$

(Here it is understood that when $\ell = 1$, $\prod_{i=1}^{\ell-1} q_i = 1$.)
Since $|d_1 - 2^{\beta-1}c_2| < d_1 2^\beta c_2 u_2$, we conclude that

$$d_1 2^\beta c_2 u_2[t_2 - Y(\prod_{i=1}^{\ell-1} q_i)(q_\ell - 1)\cdots(q_s - 1)] - (d_1 - 2^{\beta-1}c_2)$$

is positive and thus $\geq Q(\ell)$. This implies

$$d_1 2^\beta c_2 u_2 [t_2 + 1 - Y(\prod_{i=1}^{\ell-1} q_i)(q_\ell - 1)\cdots(q_s - 1)] > Q(\ell). \qquad (21)$$

Recall $t_2 = Y\prod_{i=1}^{s} q_i$. Now suppose that $q_\ell \geq 2s+1$. Then we get

$$0 < q_\ell \cdots q_s - \varphi(q_\ell \cdots q_s) < [(1+\frac{1}{q_\ell - 1})^s - 1](q_\ell - 1)\cdots(q_s - 1) < 2s(q_{\ell+1}-1)\cdots(q_s-1)$$

using Lemma 18 with $x = q_\ell - 1$ and the fact that the $q_i's$ are ascending. Here the product on the right hand side has to be interpreted as 1 if $l = s$. In particular, we have

$$d_1 2^\beta c_2 u_2 [t_2 + 1 - Y(\prod_{i=1}^{\ell-1} q_i)(q_\ell - 1)\cdots(q_s - 1)] \leq d_1 2^\beta c_2 u_2 Y(\prod_{i=1}^{\ell-1} q_i)(2s)(q_{\ell+1}-1)\cdots(q_s-1).$$

Combining this with (21), we get

$$Q(\ell) < d_1 2^\beta c_2 u_2 Y(2s)(\prod_{i=1}^{\ell-1} q_i)(q_{\ell+1}-1)\cdots(q_s-1).$$

Together with (20) this gives

$$\frac{P}{u_2}\cdot\prod_{i=1}^{\ell-1}\frac{2}{q_i - 1} < d_1 2^\beta c_2 u_2 Y(2s)(\prod_{i=1}^{\ell-1} q_i)(q_{\ell+1}-1)\cdots(q_s-1).$$

Therefore,

$$q_\ell - 1 \leq d_1 2^\beta c_2 u_2^2 Y(2s)\frac{\varphi(q_1\cdots q_s)}{P}\prod_{i=1}^{\ell-1}\frac{q_i}{2}.$$

Combining this with (17), we obtain

$$q_\ell - 1 \leq d_1 2^\beta c_2 u_2^2 Y(2s)\frac{u}{\varphi(u)}\cdot\frac{E}{\varphi(Y)2^{2\beta}c_2^2 u_2^2}\prod_{i=1}^{\ell-1}\frac{q_i}{2} = sE\cdot\frac{d_1}{2^{\beta-1}c_2}\cdot\frac{Y}{\varphi(Y)}\cdot\frac{u}{\varphi(u)}\cdot\prod_{i=1}^{\ell-1}\frac{q_i}{2}.$$

Recalling that $d_1/(2^{\beta-1}c_2) = (u-1)/(2^{\beta-1}c_2 2^{\alpha}c_1) = (u-1)/c$ is bounded by Theorem 15 and using (18) we conclude that $q_\ell \prod_{i=1}^{\ell-1} q_i^{-1}$ is bounded if $q_\ell \geq 2s+1$. Using induction on ℓ, this shows that all q_i's are bounded. By (18) this shows that t_2 is bounded. Finally, (15) now implies that u is bounded, too. □

4 Further nonexistence results

After the asymptotic analysis of the last section, we now provide a result which is useful in dealing with cases where n is small. We will also update the list of open cases with $n \leq 10^6$ from [3]. We will need the following well known results of Turyn's [7].

Definition 20 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 $(m', p) = 1$. A composite integer t is called self-conjugate modulo m if every prime divisor of t is self-conjugate modulo m.

Result 21 *Let $X \in \mathbb{Z}[\xi_t]$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_t)/\mathbb{Q})$. If $r := |X|^2 \in \mathbb{Z}^+$ and if σ fixes all prime ideals dividing r, then $X^\sigma = \epsilon X$ where ϵ is a root of unity.*

Result 22 *Let a be self-conjugate modulo m. If $X \in \mathbb{Z}[\xi_m]$ with*

$$|X|^2 \equiv 0 \bmod a^2,$$

then $X \equiv 0 \bmod a$.

Result 23 *Let G be an abelian group of order v, let ω be a character of G of order v_1, and let H be a subgroup of G^* of order v_2 where $(v_1, v_2) = 1$. Assume that there is a subset A of G such that $\tau(A) \equiv 0 \pmod{r}$ for some integer r and all $\tau \in H\omega$, and that $\tau(A) \neq 0$ for some $\tau \in H\omega$. Then*

$$2^{t-1}v \geq r v_1 v_2$$

where t is the number of distinct prime divisors of v_1.

The following is an immediate consequence of the orthogonality relations, see [2, p. 314].

Lemma 24 *Let G be an abelian group. Let $D \subset G$, let $\omega \in G^*$ and let H be a subgroup of G^*. Then*

$$\omega(D \cap H^{\perp}) = \frac{1}{|H|} \sum_{\tau \in H} \omega\tau(D).$$

Theorem 25 *Assume the existence of a $(2m, k, \lambda, u^2)$ difference set in D_m where u is odd. Let T be a set of prime divisors p of u with $p^2 \not| \; m$ such that for every $p \in T$ at least one of the following conditions is satisfied.*

a) There is a divisor l of u/p which is self-conjugate modulo m/p such that $l > 2^{t-2}$ where t is the number of prime divisors of u.
b) $4u^2/p^2 > F(m/p, u/p)^2/\varphi(F(m/p, u/p))$.
c) $F(m/p, u/p) \equiv 4 \pmod 8$, $q \equiv 3 \pmod 4$ for all prime divisors q of u/p, and $8u^2/p^2 > F(m/p, u/p)^2/\varphi(F(m/p, u/p))$.

Then

$$\frac{n}{\varphi(n)} > 2\left(1 + \sum_{p \in T} \frac{1}{p-1}\right).$$

Proof Let **A**, **B** be defined as in Result 7. Let χ be a character of C_m of order m and assume $\chi \in \mathbf{A}$. Let $p \in T$ and write $\chi = \gamma\chi'$ where γ has order p and χ' is of order m/p. Note that p and m/p are coprime by assumption. We will show $\chi' \in A$.
Assume the contrary, i.e. $|\chi'(B)| = u$. Since $\chi(B) = 0$ and since B is a union of orbits of U_m by Result 7 we have $\chi'\gamma^i(B) = 0$ for $i = 1, ..., p-1$. Now Lemma 24 implies $p\chi'(B \cap \gamma^{\perp}) = \sum_{i=0}^{p-1} \chi'\gamma^i(B) = \chi'(B)$. Let $X := B \cap \gamma^{\perp}$. Then $\chi'(X) = \sum_{i=0}^{m/p-1} x_i \xi_{m/p}^i$ with $x_i \in \{0, 1\}$ and $|\chi'(X)| = u/p$ since $|\chi'(B)| = u$. Applying Result 10 to $\chi'(X)$, we get

$$\frac{u^2}{p^2} \leq \frac{F(m/p, u/p)^2}{4\varphi(F(m/p, u/p))}$$

and thus condition b of Theorem 25 cannot hold.
Now let l be a divisor of u/p which is self-conjugate modulo m/p. Let w' be the largest divisor of m/p coprime to u. Note that w' divides $m/(m, n)$. Let

W respectively W' be the subgroup of order $m/(m,n)$ respectively w' of C_m^*. Since $\chi \in \mathbf{A}$ and since $\mathbf{A}$ is a union of cosets of W and possibly $W \setminus \{\chi_0\}$, we in particular get $\chi\psi \in \mathbf{A}$ for all $\psi \in W'$. In the same way as we did for $\chi'(X)$, we conclude $|\chi'\psi(X)| = u/p$ for all $\psi \in W'$. Since l is self-conjugate modulo m/p, Result 22 implies

$$\chi'\psi(X) \equiv 0 \pmod{l} \tag{22}$$

for all $\psi \in W'$. Note that the coset $W'\chi'$ contains a unique character η of order $m/(pw')$. Since $W'\chi' = W'\eta$ we get

$$\eta\psi(X) \equiv 0 \pmod{l}$$

for all $\psi \in W'$ from (22). Now we apply Result 23 with $G = \tau^\perp$, $v = m/p$, $A = X$, $H = W'$, $\omega = \eta$, $v_1 = m/(pw')$, $v_2 = w'$, $r = l$ and get

$$2^{s-1}(m/p) \geq l(m/(pw'))(w') = lm/p$$

where s is the number of prime divisors of $m/(pw')$. Since $s = t-1$, this shows that condition a of Theorem 25 also cannot hold.

Thus condition c must be satisfied. By Result 9, we can assume $\chi'(X) \in \mathbb{Z}[\xi_f]$ where $f = F(m/p, u/p) \equiv 4 \pmod{8}$. Write $J := \chi'(X) = Y + iZ$ with $Y, Z \in \mathbb{Z}[\xi_{f/4}]$. Since all prime divisors of u/p are $\equiv 3 \pmod{4}$, the automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_f)/\mathbb{Q})$ defined by $i^\sigma = -i$ and $\xi_{f/4}^\sigma = \xi_{f/4}$ fixes all prime ideals above u/p in $\mathbb{Z}[\xi_f]$, see [2, VI. Thm. 15.2]. Thus $J^\sigma = \epsilon J$ where ϵ is a root of unity by Result 21. Since $\epsilon \in \mathbb{Z}[\xi_f]$ and $f \equiv 0 \pmod{4}$, we have $\epsilon = \xi_f^l$ for some l. Applying σ to to $J^\sigma = \epsilon J$, we get $\epsilon\epsilon^\sigma = 1$. Thus $\epsilon = i^j$ with $j \in \{0, ..., 3\}$. If $\epsilon = i$, then $J^\sigma = Y - iZ = iY - Z$. Thus $Y = -Z$ and $J = (1-i)Y$. But this implies that $|J|^2$ is divisible by 2 which is impossible since u is odd. Similarly, $\epsilon = -i$ is impossible. If $\epsilon = -1$, then $J^\sigma = Y - iZ = -Y - iZ$ and thus $Y = 0$. If $j = 0$, then $Z = 0$. In any case, we have shown that $\chi'(X)$ times a root of unity lies in $\mathbb{Z}[\xi_{f/2}]$. Since $|\chi'(X)| = u/p$, Result 10 now shows $u^2/p^2 \leq (f/2)^2/4\varphi(f/2) = f^2/8\varphi(f)$. Thus condition c of Theorem 25 also cannot hold, a contradiction.

Hence we have shown that $\chi \in \mathbf{A}$ implies $\chi' \in \mathbf{A}$. In the same way, it follows that $\chi \in \mathbf{B}$ implies $\chi' \in \mathbf{B}$. Let W be the subgroup of order $m/(m,n)$ of C_m^*. Recall that both $\mathbf{A}$ and $\mathbf{B}$ are unions of cosets of W and possibly $W \setminus \{\chi_0\}$. By what we have shown, $\chi \in \mathbf{A}$ and $\chi^p \in \mathbf{A}$ for all $p \in T$ or $\chi \in \mathbf{B}$ and $\chi^p \in \mathbf{B}$ for all $p \in T$.

Let $S \subset C_m^*$ be the union of all cosets $W\chi^s$, $W\chi^{pw_p}$, $1 \leq s < m$, $(s,m) = 1$, $1 \leq w_p < m/p$, $(w_p, m/p) = 1$, $p \in T$. Note $\varphi((m,n))/(m,n) = \varphi(n)/n$. Thus we have

$$\begin{aligned} |S| &= \frac{m}{(m,n)}\varphi((m,n)) + \sum_{p \in T}\left(\frac{m}{(m,n)}\varphi((m,n)/p)\right) \\ &= \frac{m\varphi(n)}{n}\left[1 + \sum_{p \in T}\frac{1}{p-1}\right]. \end{aligned}$$

By what we have shown, $S \subset \mathbf{A}$ or $S \subset \mathbf{B}$. Result 7 implies $|\mathbf{A}| < m/2 < |\mathbf{B}|$ and $|\mathbf{B}| - |\mathbf{A}| < m/u$. Write $y := 1 + \sum_{p \in T}\frac{1}{p-1}$. Suppose $2y \geq n/\varphi(n)$. Then $|S| = ym\varphi(n)/n \geq m/2$ and thus $S \subset \mathbf{B}$. Note $n/\varphi(n) = u/\varphi(u)$. We have $2y\varphi(u) \geq n\varphi(u)/\varphi(n) = u$. Since u is odd and $y\varphi(u)$ in an integer, this implies $2y\varphi(u) > u$. Hence $|\mathbf{B}| - |\mathbf{A}| > 2|S| - m = [2y\varphi(u) - u]m/u \geq m/u$, a contradiction. Thus $2y < n/\varphi(n)$ proving the assertion. □

Corollary 26 *With the possible exception of $u = 735$ there is no difference set of order $u^2 \leq 10^6$ in any dihedral group.*

Proof Assume the existence of a difference set of order $u^2 \leq 10^6$ in D_m. In [3] it is shown that only the following cases are possible.

u	105	315	525	735	945
m	24885	223020	620550	1214955	2010015

For $u = 105$ we apply Theorem 25 with $p = 5$ and $l = 3$. Since 3 is self-conjugate modulo 24885/5, condition a of Theorem 25 is satisfied. Thus $35/16 = 105/\varphi(105) > 2(1 + 1/4) = 5/2$, a contradiction. Thus $u \neq 105$.
In the case $u = 315$ we have $F(m,u) = m/3$. Thus Corollary 11 gives $396900 = 4n \leq m^2/(3\varphi(m)) < 340000$, a contradiction. Thus $u \neq 315$.
For $u = 525$ take $p = 7$ in Theorem 25. Note $F(m/7, u/7) = m/(7 \cdot 15)$. Thus $F(m/7,u/7)^2/\varphi(F(m/7,u/7)) < 4u^2/7^2$, i.e. condition b of Theorem 25 is satisfied. Hence $35/16 = u/\varphi(u) > 2(1 + 1/6)$, a contradiction. Thus $u \neq 525$.
For $u = 945$ we have $F(m,u) = m/9$ and like for $u = 315$ we get a contradiction by Corollary 11. Thus $u \neq 945$. □

In view of Result 2, the following is of interest.

Remark 27 Using Corollary 11, Theorem 19, Theorem 25, some additional calculations, and a computer search the following can be shown: With the possible exception of $u = 735$, there is no difference set of order u^2 with $u = 3^a 5^b 7^c$ for any positive integers a, b, c in any dihedral group.

References

[1] L.D. Baumert: *Cyclic Difference Sets.* Lecture Notes 182, Springer, Berlin/Heidelberg/New York 1971.

[2] T. Beth, D. Jungnickel, H. Lenz: *Design Theory* (2nd edition). Cambridge University Press, Cambridge 1999.

[3] K.H. Leung, S.L. Ma, Y.L. Wong: Difference sets in dihedral groups. Des. Codes Crypt. **1** (1992), 333-338.

[4] R.L. McFarland: Sub-difference sets of Hadamard difference sets. *J. Comb. Theory Ser. A* **54** (1990), 112-122.

[5] B. Schmidt: Cyclotomic integers and finite geometry. *J. Am. Math. Soc.* **12** (1999), 929-952.

[6] B. Schmidt: Towards Ryser's conjecture. Proc. Third European Congress of Mathematics (2000).

[7] R.J. Turyn: Character sums and difference sets. Pacific J. Math. 15 (1965), 319-346.