Uniqueness of Some Cyclic Projective Planes

Yiwei Huang
Division of Mathematical Sciences
School of Physical & Mathematical Sciences
Nanyang Technological University
Singapore 637371
Singapore

Bernhard Schmidt
Division of Mathematical Sciences
School of Physical & Mathematical Sciences
Nanyang Technological University
Singapore 637371
bernhard@ntu.edu.sg

January 15, 2008

Abstract

For $n < 41$ and for $n \in \{121, 125, 128, 169, 256, 1024\}$, every cyclic projective plane of order n is desarguesian. In particular, the cyclic group of order $1,049,601$ contains a unique nontrivial difference set, up to equivalence.

1 Introduction

A *finite projective plane* $\Pi = (\mathcal{P}, \mathcal{L})$ *of order* n consists of an (n^2+n+1)-set $\mathcal{P}$, whose elements are called *points*, and an (n^2+n+1)-set $\mathcal{L}$ of $(n+1)$-subsets of $\mathcal{P}$, whose elements are called *lines*, such that any two points are contained in exactly one line. A *collineation* of Π is a bijection $\alpha : \mathcal{P} \to \mathcal{P}$ such that $\{p^\alpha : p \in L\}$ is a line for every $L \in \mathcal{L}$. Two projective planes $(\mathcal{P}, \mathcal{L})$ and $(\mathcal{P}', \mathcal{L}')$ are called *isomorphic* if there is a bijection $\gamma : \mathcal{P} \to \mathcal{P}'$ such that $\{p^\gamma : p \in L\} \in \mathcal{L}'$ for all $L \in \mathcal{L}$.

Let $\Pi = (\mathcal{P}, \mathcal{L})$ be a projective plane of order n. If there is a collineation α of Π such that, for all $p, q \in \mathcal{P}$, there is exactly one $i \in \{0, ..., n^2+n\}$ with $p^{\alpha^i} = q$, then Π is called *cyclic projective plane.* In this case, α generates a cyclic group of collineations order n^2+n+1 which is called a *Singer cycle* of Π.

For every prime power q, a projective plane of order q, denoted by $\mathrm{PG}(2, q)$, can be constructed as follows. The points are the one-dimensional, and the lines are the two-dimensional subspaces of $\mathbb{F}_{q^3}$, viewed as an $\mathbb{F}_q$-vector space. Incidence is given by set-theoretic containment. A projective plane isomorphic to $\mathrm{PG}(2, q)$ is called *desarguesian.* It was discovered by Singer [12] that all desarguesian projective planes are cyclic. This can be seen as follows. Let α be a collineation of $\mathrm{PG}(2, q)$ induced by multiplication with a primitive element of $\mathbb{F}_{q^3}$. Then $\langle \alpha \rangle$ is a Singer cycle of $\mathrm{PG}(2, q)$.

Singer [12] introduced the notion of *difference sets* to describe cyclic projective planes. In today's language, a *planar difference of order n* is an $(n+1)$-subset D of a group G of order n^2+n+1 such that every nonidentity element g of G has exactly one representation $g = d_1 d_2^{-1}$ with $d_1, d_2 \in D$. If G is a cyclic group, then D is called a *cyclic planar difference set.* The following are straightforward to verify.

(a) If D is a cyclic planar difference set of order n in a cyclic group G, then $(G, \{\{dg : d \in D\} : g \in G\})$ is a cyclic projective plane of order n.

(b) If $\Pi = (\mathcal{P}, \mathcal{L})$ is a cyclic projective plane with Singer cycle $\langle \alpha \rangle$, and $p \in \mathcal{P}$, $L \in \mathcal{L}$ are arbitrary, then $\{\alpha^i : p^{\alpha^i} \in L\}$ is a cyclic planar difference set in $\langle \alpha \rangle$.

A difference set arising from the Singer cycle of $\mathrm{PG}(2, q)$ via construction (b) is called a *Singer difference set.*

Let G and H be cyclic groups of the same order, and let $D \subset G$, $E \subset H$ be planar difference sets. Then D and E are called *equivalent* if there are an isomorphism $\alpha : G \to H$ and $h \in H$ such that $E = \{hd^\alpha : d \in D\}$. In this case, the projective planes arising from D and E by construction (a) are isomorphic. An isomorphism of these planes is given by $G \to H,\ x \mapsto hx^\alpha$.

Singer [12] stated that "it seems to be true" that any two cyclic planar difference of the same order are equivalent. The *prime power conjecture* asserts that the order of any finite projective plane must be a prime power. Combining Singer's conjecture with the prime power conjecture gives the following.

Conjecture 1 *Every finite cyclic projective plane is desarguesian.*

Conjecture 1 is sometimes attributed to Singer, though, as a matter of fact, Singer did not conjecture that the order of a cyclic projective plane must be a prime power. Anyway, Conjecture 1 is equivalent to the combination of the following statements.

(i) Every cyclic finite projective plane has prime power order.

(ii) The cyclic projective planes of prime power order are all isomorphic.

Statement (i) has been verified by Baumert and Gordon [1, 6] for all orders up to $2 \cdot 10^9$. It also has been verified for several infinite classes of orders [2]. On the other hand, the results on (ii) do not go further than order 81 and date back to the work of Hall [9] and Bruck [3]. Assertion (ii) was proved by Hall [9] for orders 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 25, 27, and 32 with the help of a computer.

In our view, the known evidence for Conjecture 1 is quite flimsy. It seems that Bruck [3] actually was searching for counterexamples. However, he was not successful, but verified Conjecture 1 for orders 49, 64, and 81. The following statement of Bruck [3] inspired our work.

> *"It appears to the author that the present results could be extended considerably ... to find what might be called 'counter-examples'."*

We will show that the first part of Bruck's statement is correct – unfortunately, we had no success with the second part. We will verify (ii) for orders less than 41 and orders $121, 125, 128, 169, 256, 1024$.

We will show that this, in particular, implies the uniqueness of a nontrivial difference set in the cyclic group of order $1,049,601$, up to equivalence. To our knowledge, this is by far the largest group which contains a difference set, and for which all difference sets in the group have been classified.

Our main theorems partially rely on extensive computer searches. An independent verification of our results is highly desirable. Therefore, we attach great value to describing our algorithms precisely, and to present the results in a form suitable for easy verification. Furthermore, we tried to keep the paper as self-contained as possible.

2 Preliminaries

We will always identify a subset A of a group G with the element $\sum_{g \in A} g$ of the integral group ring $\mathbb{Z}[G]$. For $\alpha \in \mathbb{Z}$ and the identity element 1 of G, we simply write α for the group ring element $\alpha 1$. For $B = \sum_{g \in G} b_g g \in \mathbb{Z}[G]$ and $t \in \mathbb{Z}$, we write $B^{(t)} := \sum_{g \in G} b_g g^t$. A group homomorphism $G \to H$ is always assumed to be extended to a homomorphism $\mathbb{Z}[G] \to \mathbb{Z}[H]$ by linearity. For $X \in \mathbb{Z}[G]$ and $g \in G$, the group ring element Xg is called a *translate* of X. In the group ring language, cyclic planar difference sets can be characterized as follows.

Result 2 *Let G be a cyclic group of order n^2+n+1. An $(n+1)$-subset D of G is a cyclic planar difference set if and only if*

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

Homomorphic images of difference sets satisfy a similar group ring equation and thus are extremely useful.

Result 3 *Let G be a cyclic group of order n^2+n+1, and D be planar difference set in G. Let U be a subgroup of G, and let $\rho : G \to G/U$ denote the natural epimorphism. Then*

$$\rho(D)\rho(D)^{(-1)} = n + |U|(G/U). \tag{2}$$

By [8] and [11], we have the following.

Result 4 *Let n be a power of a prime p. Every cyclic planar difference set of order n is equivalent to a planar difference set D with $D^{(p)} = D$.*

If any counterexample for Conjecture 1 exists, then it necessarily corresponds to a cyclic planar difference set which is not equivalent to a Singer difference set of a desarguesian projective plane. On the other hand, in general, the inequivalence of two difference sets does *not* imply that the corresponding designs are non-isomorphic. However, as the following result shows, this implication *does* hold if one of difference sets in question is a Singer difference set of a desarguesian plane. It seems that the validity of this result tacitly has been assumed in some papers, but apparently no proof has been published.

Proposition 5 *Let q be a prime power, and let D be a cyclic planar difference set of order q which is not equivalent to a Singer difference set. Then the projective plane generated by D is non-desarguesian.*

Proof Let $v = q^2+q+1$ and let G be a cyclic group of order v containing D. Assume that D generates a desarguesian plane Π. Then G can be considered as a collineation group of Π and hence as a subgroup of $P\Gamma L(2,q)$ acting sharply transitively on the points of Π, see [4]. By a result of Ellers and Karzel [5] (see [4, p. 34]), G actually must be a subgroup of $PGL(2,q)$, since G is abelian. Let E be a Singer difference set of Π, and let H be the cyclic subgroup of $PGL(2,q)$ containing E. By [10, Cor. 4.7.], the subgroups G and H are conjugate in $PGL(2,q)$, i.e., there is $\sigma \in PGL(2,q)$ with $H = \sigma^{-1}G\sigma$. Let L be an arbitrary line of Π, and let P be an arbitrary point of L. Then P^σ is a point on the line L^σ. By replacing D, respectively E, by translates, if necessary, we can assume $D = \{g \in G : P^g \in L\}$, respectively, $E = \{h \in H : P^{\sigma h} \in L^\sigma\}$. Hence we get

$$\begin{array}{rcl} E & = & \{h \in H : P^{\sigma h} \in L^\sigma\} \\ & = & \{\sigma^{-1}g\sigma : g \in G, P^{\sigma(\sigma^{-1}g\sigma)} \in L^\sigma\} \\ & = & \{\sigma^{-1}g\sigma : g \in G, P^g \in L\} \\ & = & \sigma^{-1}D\sigma. \end{array}$$

Since conjugation with σ induces an isomorphism $G \to H$, this shows that D and E are equivalent, a contradiction. □

3 Cyclic planes of square order

3.1 The results of Bruck

The following Results 6-10 are contained in [3]. For the convenience of the reader, we include proofs, since our notation differs from [3].

Throughout this section, we use the following notation. Let q be a prime power, and let G be a cyclic group of order q^4+q^2+1. We write $m = q^3$, $s = q^2-q+1$, and $t = q^2+q+1$.

Result 6 *Let D be a planar difference set of order q^2 in G, and assume $D^{(m)} = D$. Let U be the subgroup of G of order t. Then $D \cap U$ is a planar difference set in U.*

Proof For $g \in G$ we write $Dg = \{dg : d \in D\}$. Let $\mathcal{L} := \{Dg : g \in G, (Dg)^{(m)} = Dg\}$. Note that $U = \{g \in G : g^m = g\}$ and $\mathcal{L} = \{Du : u \in U\}$. For $u \in U$, we write $\mathcal{L}_u = \{L \in \mathcal{L} : u \in L\}$. Let $w \in U$ and $M \in \mathcal{L} \setminus \mathcal{L}_w$ be arbitrary. It is straightforward to verify that the map $\mathcal{L}_w \to M \cap U$ sending $L \in \mathcal{L}_w$ to the unique point in $L \cap M$ is a well defined bijection. Using this fact repeatedly, we see that there is a positive integer x such that $|\mathcal{L}_u| = x$ for all $u \in U$ and $|L \cap U| = x$ for all $L \in \mathcal{L}$. Now fix some $u \in U$. Since the lines in $\mathcal{L}_u$ cover each point in $U \setminus \{u\}$ exactly once, we get $q^2 + q = x(x-1)$ and thus $x = q+1$. Since $D \in \mathcal{L}$ by assumption, we infer $|D \cap U| = q+1$. Hence $D \cap U$ is a planar difference set in U. □

Result 7 *Write $G = \langle\sigma\rangle\langle\tau\rangle$ where σ has order s and τ has order t. Let D be a planar difference set in G satisfying $D^{(m)} = D$. Then there is a function $f_D : \{1, ..., s-1\} \to \{0, ..., t-1\}$ such that*

$$D = \bar{D} + \sum_{x=1}^{s-1} \sigma^x \tau^{f_D(x)} \tag{3}$$

where $\bar{D} = D \cap \langle\tau\rangle$.

Proof Recall that $\bar{D}$ is a planar difference set in $\langle\tau\rangle$ by Result 6. Since $\bar{D}\bar{D}^{(-1)}$ covers all elements of $\langle\tau\rangle$, the elements of $D \setminus \bar{D}$ must all belong to different cosets $\neq \langle\tau\rangle$ of $\langle\tau\rangle$ in G. Since there are exactly $s-1$ such cosets and $|D \setminus \bar{D}| = s-1$, the elements of $D \setminus \bar{D}$ represent each coset $\neq \langle\tau\rangle$ of $\langle\tau\rangle$ in G exactly once. This implies the assertion. □

Throughout the rest of Section 3, we use the notation introduced in Result 7. For a positive integer r and an integer y, we write

$$[y]_r = \min\{z \in \mathbb{N} : z \equiv y \pmod{r}\}.$$

Result 8 *Assume $D^{(k)} = D$ for some integer k with $(k, st) = 1$. Then*

$$f_D([kx]_s) \equiv k f_D(x) \pmod{t}$$

for all $x \in \mathbb{Z}$, $x \neq 0$. In particular, if $D^{(p)} = D$, then $f_D([-x]_s) \equiv f_D(x) \pmod{t}$ for all $x \neq 0$.

Proof By (3) we have

$$\begin{aligned} \bar{D}^{(k)} + \sum_{x=1}^{s-1} \sigma^{kx} \tau^{k f_D(x)} &= \bar{D} + \sum_{x=1}^{s-1} \sigma^x \tau^{f_D(x)} \\ &= \bar{D} + \sum_{x=1}^{s-1} \sigma^{kx} \tau^{f_D([kx]_s)}. \end{aligned}$$

This implies

$$\sum_{x=1}^{s-1} \sigma^{kx} \tau^{k f_D(x)} = \sum_{x=1}^{s-1} \sigma^{kx} \tau^{f_D([kx]_s)}$$

and thus $f_D([kx]_s) \equiv k f_D(x) \pmod{t}$ for all $x \neq 0$.

Recall $m = q^3$. If $D^{(p)} = D$, then $D^{(m)} = D$, and thus $f_D([-x]_s) \equiv f_D([mx]_s) \equiv m f_D(x) \equiv f_D(x) \pmod{t}$. □

Result 9 *Define $E \subset \{0, ..., t-1\}$ by $D \cap \langle \tau \rangle = \sum_{d \in E} \tau^d$. The set D given by* (3) *is a planar difference set if and only if for each $x = 1, ..., s-1$ the following holds. The t numbers*

$$\begin{array}{l} f_D(x) - d, \ d \in E, \\ d - f_D(x), \ d \in E, \\ f_D([x+y]_s) - f_D(y), \ y = 1, ..., s-1, \ y \not\equiv -x \pmod{s}, \end{array} \qquad (4)$$

are pairwise distinct modulo t.

Proof

$$\begin{aligned} DD^{(-1)} &= \bar{D}\bar{D}^{(-1)} + \bar{D} \sum_{x=1}^{s-1} \sigma^{-x} \tau^{-f_D(x)} + \bar{D}^{(-1)} \sum_{x=1}^{s-1} \sigma^{x} \tau^{f_D(x)} \\ &+ \sum_{x,y=1}^{s-1} \sigma^{x-y} \tau^{f_D(x) - f_D(y)} \\ &= q + \langle \tau \rangle + \sum_{x=1}^{s-1} \sum_{d \in E} \sigma^{-x} \tau^{d - f_D(x)} + \sum_{x=1}^{s-1} \sum_{d \in E} \sigma^{x} \tau^{f_D(x) - d} \\ &+ s - 1 + \sum_{z=1}^{s-1} \sigma^z \sum_{\substack{y=1 \\ y \not\equiv -z \bmod s}}^{s-1} \tau^{f_D([z+y]_s) - f_D(y)} \\ &= q^2 + \langle \tau \rangle + \sum_{x=1}^{s-1} \sigma^x \left(\sum_{d \in E} \tau^{d - f_D(x)} + \sum_{d \in E} \tau^{f_D(x) - d} + \sum_{\substack{y=1 \\ y \not\equiv -z \bmod s}}^{s-1} \tau^{f_D([x+y]_s) - f_D(y)} \right) \end{aligned}$$

Condition (4) holds if and only if the term in the parenthesis equals $\langle \tau \rangle$ for all $x \neq 0$. This implies the assertion. □

Result 10 *For $S \subset \langle \tau \rangle$, define*

$$K(S) := \{k \in \{0, ..., t-1\} : \tau^{2k} \neq d_1 d_2 \text{ for all } d_1, d_2 \in S\}.$$

Recall $\bar{D} = D \cap \langle \tau \rangle$. The range of f_D is $K(\bar{D})$. Furthermore, $|K(\bar{D})| = (s-1)/2$, and f_D is a two-to-one map.

Proof Let $x \in \{1, ..., s-1\}$ be arbitrary. Then

$$\tau^{f_D(x)} d_1^{-1} \neq d_2 \tau^{-f_D(x)} \text{ for all } d_1, d_2 \in \bar{D}$$

by Result 9. Hence the range of f_D is a subset of $K(\bar{D})$.

Let $x, y \in \{1, ..., s-1\}$ with $x \not\equiv \pm y \bmod s$ be arbitrary. Define $a, b \in \{0, ..., s-1\}$ by $x \equiv a + b \pmod{s}$ and $y \equiv a - b \pmod{s}$. Then $a, b \not\equiv 0 \pmod{s}$ and $a \not\equiv \pm b \pmod{s}$. Note that $f_D([-b]_s) \equiv f_D(b) \pmod{t}$ by Result 8. Hence

$$f_D([a+b]_s) - f_D(b) \not\equiv f_D([a-b]_s) - f_D(b) \pmod{t}$$

by Result 9. Since $[a+b]_s = x$ and $[a-b]_s = y$, this implies $f_D(x) \not\equiv f_D(y) \pmod{t}$. Since $f_D(x) \equiv f_D([-x]_s) \pmod{t}$, this shows that f_D is a two-to-one mapping. Hence the range of f_D has exactly $(s-1)/2$ elements.

It remains to show $|K(\bar{D})| = (s-1)/2$. Assume that $d_1 d_2 = d_3 d_4$ with $d_i \in \bar{D}$ for $i = 1, 2, 3, 4$. Then $d_1 d_3^{-1} = d_4 d_2^{-1}$. Since $\bar{D}$ is a planar difference set, this implies $d_1 = d_4$ and $d_3 = d_2$ or $d_1 = d_3$ and $d_4 = d_2$, i.e., $\{d_1, d_2\} = \{d_3, d_4\}$. Hence $|K(\bar{D})|$ is the t minus the number of unordered pairs of elements from $\bar{D}$, i.e., $t - (q+1)(q+2)/2 = (s-1)/2$. □

3.2 Cyclic planes of orders 121, 169, 256, and 1024

In this section, we prove some general auxiliary results on cyclic projective planes of square order, and describe the implementation of complete searches for cyclic projective planes of orders 121, 169, 256, and 1024. Our searches are based on the results of Section 3.1 and the following result of Hall [8].

Result 11 *Every cyclic projective plane of order at most* 16 *and of order* 32 *is desarguesian.*

Throughout this section, we use the notation introduced in Section 3.1. We write $q = p^a$ where p is a prime. Recall that $G = \langle\sigma\rangle\langle\tau\rangle$ denotes a cyclic group of order $q^4 + q^2 + 1$, and σ, respectively τ, is an element of G or order $s = q^2 - q + 1$, respectively $t = q^2 + q + 1$.

Lemma 12 *Let $q = p^a$ where p is a prime and $q \leq 16$ or $q = 32$. Let D_q be an arbitrary planar difference set of order q in $\langle\tau\rangle$ satisfying $D_q^{(p)} = D_q$. Any cyclic planar difference set of order q^2 is equivalent to a difference set D satisfying*

$$D^{(p)} = D \text{ and } D \cap \langle\tau\rangle = D_q. \tag{5}$$

Proof Let F be a cyclic planar difference set of order q^2. Result 4 shows that F is equivalent to a difference set F_1 with $F_1^{(p)} = F_1$. Proposition 5, Result 6, and Result 11 imply that $F_1 \cap \langle\tau\rangle$ and D_q are equivalent difference sets. Hence there are $g \in \langle\tau\rangle$ and an integer r with $(r, t) = 1$ such that $(F_1 \cap \langle\tau\rangle)^{(r)} g = D_q$. Since $F_1^{(p)} = F_1$ and $D_q^{(p)} = D_q$, we have $g = 1$. Hence $D = F_1^{(r)}$ satisfies (5). □

From now on, let D be a cyclic planar difference set of order q^2 in G satisfying (5), let f_D be the corresponding function defined in Result 7, and let $K(\bar{D})$ be defined as in Result 10.

Let r be any positive integer. We define an *r-cycle* as an orbit of multiplication with p mod r on $\{0, ..., r-1\}$, i.e., a subset of $\{0, ..., r-1\}$ of the form $\{[xp^i]_r : i \in \mathbb{N}\}$ for some $x \in \{0, ..., r-1\}$.

Since D satisfies (5), we infer that $K(\bar{D})$ is a union of t-cycles. A t-cycle contained in $K(\bar{D})$ is called a *$K(\bar{D})$-cycle.*

Lemma 13 *Let O be any s-cycle. Then $f_D(O)$ is a $K(\bar{D})$-cycle, and*

$$O \to f_D(O), x \mapsto f_D(x)$$

is a two-to-one map. Furthermore, the map F_D from the set of s-cycles $\neq \{0\}$ to the set of $K(\bar{D})$-cycles induced by f_D is a bijection.

Proof Since $D^{(p)} = D$, Result 8 shows that $f_D(O)$ is a $K(\bar{D})$-cycle for every s-cycle O. By Result 10, the map F_D is surjective. Let $x, y \in \{0, ..., s-1\}$ with $f_D(x) = f_D(y)$. By the proof of Result 10, this implies $x \equiv -y \pmod{s}$. Since $q^3 \equiv -1 \pmod{s}$, the elements x and y are contained in the same s-cycle. This shows that F_D is injective. Since f_D is a two-to-one map by Result 10, we infer that $O \to f_D(O), x \mapsto f_D(x)$ is also a two-to-one map for each s-cycle O. □

Lemma 14 *If $q \equiv 2 \pmod 3$, then there is an s-cycle O containing exactly two elements, and we have $f_D(x) = 0$ for $x \in O$.*

Proof Since $q \equiv 2 \pmod 3$, we have $s \equiv 0 \pmod 3$, and $O = \{s/3, 2s/3\}$ is an s-cycle. Since $O \to f_D(O), x \mapsto f_D(x)$ is a two-to-one map, $f_D(O)$ is a $K(\bar{D})$-cycle containing only one element. Hence $f_D(x) = 0$ for $x \in O$. □

Let $\mathbb{Z}_s^*$ denote the multiplicative group of integers mod s. Note that $\mathbb{Z}_s^*$ acts by multiplication mod s on the set $\{1, ..., s-1\}$, and this induces an action of $\mathbb{Z}_s^*$ on the set of s-cycles.

Lemma 15 *Let $M = M_1 \cup \cdots \cup M_c$ be the set of s-cycles, where $M_1,...,M_c$ are the orbits of the $\mathbb{Z}_s^*$ action on M. For $i = 1,...,c$, let $O_i \in M_i$ and $x_i \in O_i$ be arbitrary. Let O be any $K(\bar{D})$-cycle, and let $y \in O$ be arbitrary.*

Let E be an arbitrary cyclic planar difference set of order q^2. Then there is $j \in \{1,...,c\}$ with $|O_j| = 2|O|$ such that E is equivalent to a difference set D satisfying (5) *and $f_D(x_j) = y$.*

Proof Let D be any cyclic planar difference set of order q^2 satisfying (5). It suffices to show that there are $j \in \{1,...,c\}$ and positive integer r coprime to st with $f_{D^{(r)}}(x_j) = y$. Since O is contained in $K(\bar{D})$, and $K(\bar{D})$ is the range of f_D, there is $x \in \{1,...,s-1\}$ with $f_D(x) = y$. Let $s(x)$ denote the s-cycle containing x. Then $s(x) \to O, z \mapsto f(z)$ is a two-to-one map by Lemma 13. Hence $|s(x)| = 2|O|$. Furthermore, by the definition of the x_i, there are $j \in \{1,...,c\}$ and an integer r with $(r,s) = 1$, $r \equiv 1 \pmod t$, and $rx \equiv x_j \pmod s$. Note $|O_j| = |s(x)| = 2|O|$. Moreover,

$$D^{(r)} = D_q + \sum_{z=1}^{s-1} \sigma^{rz}\tau^{f_D(z)} = D_q + \sum_{z=1}^{s-1} \sigma^{z}\tau^{f_D([r_1 z]_s)}$$

where r_1 is an integer with $rr_1 \equiv 1 \pmod s$. This implies $f_{D^{(r)}}(x_j) = f_D([r_1 x_j]_s) = f_D(x) = y$. □

Proposition 16 *Assume that s is a prime, and let D_q be an arbitrary planar difference set of order q in $\langle\tau\rangle$ with $D_q^{(p)} = D_q$. Let $y \in K(D_q)$ be arbitrary. Then every cyclic planar difference set of order q^2 is equivalent to a difference set D satisfying* (5) *and $f_D(1) = y$. Furthermore, any two distinct difference sets D satisfying* (5) *and $f_D(1) = y$ are inequivalent.*

Proof Note that we have $c = 1$ in Lemma 15 since s is a prime. Thus, choosing $x_j = 1$ in Lemma 15 shows that every cyclic planar difference set of order q^2 is equivalent to a difference set D satisfying (5) and $f_D(1) = y$. Now let D and D' be any two distinct difference sets satisfying (5) and $f_D(1) = f_{D'}(1) = y$. Assume that D and D' are equivalent. Then there are $g \in G$ and $r \in \mathbb{Z}$ with $(r, st) = 1$ and

$$D' = gD^{(r)}. \tag{6}$$

Since $\langle\tau\rangle$ is the only coset of $\langle\tau\rangle$ which contains more than one element of D, respectively D', this implies $g \in \langle\tau\rangle$. Hence (6) implies $D_q = gD_q^{(r)}$. By a result of [7], we have $r \equiv p^j \pmod t$ for some $j \in \mathbb{N}$. Since $D_q^{(p)} = D_q$, we get $D_q = gD_q$ and thus $g = 1$. Hence $D' = D^{(r)}$. Let $r_1 \in \{1, ..., s-1\}$ with $rr_1 \equiv 1 \pmod{s}$. By (3) and since $D' = D^{(r)}$, we have $f_{D'}(1) \equiv rf_D(r_1) \equiv p^j f_D(r_1) \pmod{t}$. In view of Result 8 and $f_D(1) = f_{D'}(1) = y$, this implies $f_D([p^j r_1]_s) = f_D(1)$. From Results 8 and 10 , we conclude $\pm p^j r_1 \equiv 1 \pmod{s}$ and thus $r \equiv \pm p^j \pmod{s}$. Recall $r \equiv p^j \pmod{t}$, $q^3 \equiv -1 \pmod{s}$, and $q^3 \equiv 1 \pmod{t}$. We infer $r \equiv p^e \pmod{st}$ for some positive integer e. But this implies $D' = D$, a contradiction. □

Proposition 16 is very useful since it shows that, in the case where D_q is unique up to equivalence and s is a prime, the number of nonisomorphic cyclic projective planes of order q^2 coincides with the number of functions f satisfying Result 9 with $D \cap \langle\tau\rangle = D_q$, Result 8 for $k = p^j$, $j \in \mathbb{N}$, and $f_D(1) = y$. Thus, in this case, all cyclic projective planes of order q^2 are desarguesian if and only if a function f_D satisfying these conditions is unique.

The following gives a similar result for the case where $s/3$ is a prime. The proof is similar to, but more tedious than the proof of Proposition 16 and is skipped.

Proposition 17 *Assume that $s = 3r$ where $r > 3$ is a prime, and let D_q be an arbitrary planar difference set of order q in $\langle\tau\rangle$ with $D_q^{(p)} = D_q$. Let $A \subset \{1, ..., s-1\}$ with $|A| = r - 1$ such that*

$$A \cup \{[(r+1)a]_s : a \in A\} = \{x \in \{1, ..., s-1\} : (x, s) = 1\}.$$

Let $y \in K(D_q)$ be arbitrary.

Every cyclic planar difference set of order q^2 is equivalent to a difference set D satisfying (5) *and one of the following conditions.*

(i) $f_D(1) = y$,

(ii) $f_D(3) = y$ *and* $f_D(a) = \min\{f_D(x) : x \in \{1, ..., s-1\}, (x, s) = 1\}$ *for some* $a \in A$.

Furthermore, any two distinct difference sets D satisfying (5) *and one of the conditions (i) or (ii) are inequivalent.*

Before describing our algorithm, we introduce some notation. By D_q we denote an arbitrary planar difference set of order q in $\langle\tau\rangle$ with $D_q^{(p)} = D_q$, and define $E \subset \{0, ..., t-1\}$ by $D_q \cap \langle\tau\rangle = \sum_{d \in E} \tau^d$. We consider the following modification of the condition in Result 9.

Let M be a subset of $\{1, ..., s-1\}$, and let $f : \{1, ..., s-1\} \to \{0, ..., t-1\}$ be a function. For $x \in \{1, ..., s-1\}$ we define a multiset M_x by

$$M_x = \begin{cases} \bigcup_{d \in E} \{[f(x) - d]_t, [d - f(x)]_t\}, & \text{if } x \in M, \\ \emptyset, & \text{if } x \notin M. \end{cases}$$

We say that the *condition $C(M)$ is satisfied for f* if, for every $x = 1, ..., s-1$, the multiset

$$M_x \cup \{[f(x+y) - f(y)]_s : y \in M,\ x+y \in M\}$$

does not contain any element with multiplicity ≥ 2.

For $y \in K(D_q)$, let $K(y)$ denote the $K(D_q)$-cycle containing y. For $a \in \{1, ..., s-1\}$, let $s(a)$ denote the s-cycle containing a.

The correctness of the following algorithm follows from the results of Section 3.1 and Lemma 14.

Algorithm 18

Input: $q = p^a$ where p is a prime, a planar difference set D_q of order q in $\langle \tau \rangle$ with $D_q^{(p)} = D_q$, an s-cycle S with $|S| > 2$, and a k-cycle K with $|K| = |S|/2$

Output: A set $\mathcal{S}$ such that every cyclic planar difference set D of order q^2 with $D \cap \langle \tau \rangle = D_q$ and $f_D(S) = K$ is equivalent to an element of $\mathcal{S}$

Initialization:

1. $\mathcal{S} := \emptyset$; $M := \emptyset$.

2. Let $\{S_1, ..., S_b\}$ be the set of all s-cycles, and choose the numbering such that $S_1 = S$ and $S_b = \min\{|S_i| := i = 1, ..., b\}$. For $i = 1, ..., b$, choose $s_i \in S_i$ arbitrarily.

3. If $q \not\equiv 2 \pmod 3$, set $c := b$. If $q \equiv 2 \pmod 3$, set $c := b-1$, $f(x) := 0$ for $x \in S_b$ and $M := M \cup S_b$.

4. Choose $y \in K$ arbitrarily, set $f([p^i s_1]_s) := [p^i y]_t$, $i = 0, ..., |S|-1$, and $M := M \cup S$.

5. Set $R := K(D_q) \setminus (K \cup \{0\})$, and $L := 2$.

Main Step:

(i) If $L = c + 1$, then add $D_q \cup \bigcup_{i=1}^{s-1} \sigma^x \tau^{f(x)}$ to $\mathcal{S}$, set $L := L - 1$, $R := R \cup K(f(s_L))$, $M := M \setminus S_L$.

(ii) Repeat until $L = 1$ or $f(s_L) < \max(R)$:
Set $f(s_L) := -1$, $L := L - 1$, $R := R \cup K(f(s_L))$, $M := M \setminus S_L$.

(iii) If $L = 1$, then terminate and output $\mathcal{S}$.

(iv) Set $y := \min\{r \in R : r > f(s_L)\}$ and $f([p^i s_L]_s) := [p^i y]_t$ for $i = 0, ..., |S_L| - 1$.

(v) Set $M' := M \cup S_L$. If $C(M')$ holds for f, then set $M := M'$, $R := R \setminus K(y)$, $L := L + 1$.

(vi) Go to step (i).

We now describe the application of Algorithm 18 to the cases $q = 11$, 13, 16, and 32. The difference set $D_q \subset \langle \tau \rangle$ will be specified by giving the set $E \subset \{0, ..., t-1\}$ with $D_q = \sum_{d \in E} \tau^d$. The functions $f : \{1, ..., s-1\} \to K(D_q)$ computed by Algorithm 18 are given in the form $f(1) \cdots f(s-1)$ (values separated by spaces).

1. $q = 11$. We choose $E = \{1, 11, 16, 40, 41, 43, 52, 60, 74, 78, 121, 128\}$. Since $s = 3 \cdot 37$, we can apply Proposition 17. We take $y = 4$ and choose A such that $4 \in A$ and thus $41 = [4(1 + s/3)]_s \notin A$. The application of Algorithm 18 shows that there is no cyclic planar difference set D of order 11^2 satisfying (5) and $f_D(1) = y$. Moreover, there is a unique D satisfying (5), $f_D(3) = 4$, and $f_D(4) = \min\{f_D(x) : x \in \{1, ..., s-1\}, (x, s) = 1\}$. According to Proposition 17, this shows that there is exactly one cyclic planar difference set of order 11^2, up to equivalence. The following are the values of the unique function f_D for which (5) holds, and which satisfies $f_D(3) = 4$, and $f_D(4) = \min\{f_D(x) : x \in \{1, ..., s-1\}, (x, s) = 1\}$.

13 17 4 5 71 105 32 25 30 110 10 64 115 77 29 12 88 120 83 62 39 54 9 123 36 119 129 100 7 85 99 68 44 86 37 89 0 35 51 73 15 23 49 55 91 132 112 48 122 79 70 8 130 53 116 116 53 130 8 70 79 122 48 112 132 91 55 49 23 15 73 51 35 0 89 37 86 44 68 99 85 7 100 129 119 36 123 9 54 39 62 83 120 88 12 29 77 115 64 10 110 30 25 32 105 71 5 4 17 13

2. $q = 13$. Let $E = \{0, 2, 3, 10, 26, 39, 43, 61, 109, 121, 130, 136, 141, 155\}$. Since $s = 157$ is a prime, we can apply Proposition 16. We take $y = 8$. The application of Algorithm 18 shows that there is exactly one cyclic planar difference set D of order 13^2 satisfying (5) and $f_D(1) = y$. According to Proposition 16, this shows that there is exactly one cyclic planar difference set of order 13^2, up to equivalence. The following are the values of the unique function f_D for which (5) holds, and which satisfies $f_D(1) = 8$.

8 84 15 83 19 35 25 53 38 11 57 71 104 9 134 87 96 55 42 46 20 154 137 105 117 177 143 172 48 102 58 129 149 60 63 156 29 95 12 128 77 107 27 67 171 36 120 119 17 40 33 164 140 49 30 139 160 103 145 100 173 86 75 150 64 142 180 22 168 24 144 59 16 88 110 45 166 89 89 166 45 110 88 16 59 144 24 168 22 180 142 64 150 75 86 173 100 145 103 160 139 30 49 140 164 33 40 17 119 120 36 171 67 27 107 77 128 12 95 29 156 63 60 149 129 58 102 48 172 143 177 117 105 137 154 20 46 42 55 96 87 134 9 104 71 57 11 38 53 25 35 19 83 15 84 8

3. $q = 16$. Let
$E = \{39, 78, 156, 91, 182, 17, 34, 68, 136, 272, 271, 269, 265, 257, 241, 209, 145\}$. Since $s = 241$ is a prime, we can apply Proposition 16. We take $y = 3$. The application of Algorithm 18 shows that there is exactly one cyclic planar difference set D of order 16^2 satisfying (5) and $f_D(1) = y$. According to Proposition 16, this shows that there is exactly one cyclic planar difference set of order 16^2, up to equivalence. The following are the values of the unique function f_D for which (5) holds, and which satisfies $f_D(1) = 3$.

3 6 50 12 198 100 185 24 238 123 20 200 157 97 222 48 187 203 188 246 163 40 167 127 63 41 42 194 98 171 262 96 55 101 71 133 116 103 22 219 231 53 158 80 242 61 245 254 197 126 29 82 161 84 109 115 244 196 186 69 149 251 5 192 47 110 147 202 86 142 176 266 212 232 183 206 105 44 114 165 57 189 228 106 88 43 210 160 139 211 93 122 191 217 151 235 259 121 79 252 11 58 172 164 131 49 21 168 220 218 94 230 111 215 10 119 229 99 25 138 138 25 99 229 119 10 215 111 230 94 218 220 168 21 49 131 164 172 58 11 252 79 121 259 235 151 217 191 122 93 211 139 160 210 43 88 106 228 189 57 165 114 44 105 206 183 232 212 266 176 142 86 202 147 110 47 192 5 251 149 69 186 196 244 115 109 84 161 82 29 126 197 254 245 61 242 80 158 53 231 219 22 103 116 133 71 101 55 96 262 171 98 194 42 41 63 127 167 40 163 246 188 203 187 48 222 97 157 200 20 123 238 24 185 100 198 12 50 6 3

3. $q = 32$. Let
$E = \{1, 2, 4, 8, 16, 32, 55, 64, 110, 128, 139, 220, 256, 278, 299, 339, 349, 440, 453, 512, 529, 556, 598, 678, 698, 703, 755, 793, 880, 906, 925, 991, 1024\}$. Since $s =$

$3 \cdot 331$, we can apply Proposition 17. We take $y = 297$ and choose A such that $113 \in A$ and thus $775 = [113(1+s/3)]_s \notin A$. The application of Algorithm 18 shows that there is no cyclic planar difference set D of order 32^2 satisfying (5) and $f_D(1) = y$. Moreover, there is a unique D satisfying (5), $f_D(3) = 297$, and $f_D(113) = \min\{f_D(x) : x \in \{1, ..., s-1\}, (x, s) = 1\}$. According to Proposition 17, this shows that there is exactly one cyclic planar difference set of order 32^2, up to equivalence. The following are representatives of the values of the unique function f_D for which (5) holds, and which satisfies $f_D(3) = 297$, and $f_D(113) = \min\{f_D(x) : x \in \{1, ..., s-1\}, (x, s) = 1\}$. The remaining values of f_D can be determined by Result 8.

x	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	37	41	43	45	49	51	53	55	57	67	69	71	73	75	83	87	103	149	331
$f(x)$	168	297	594	1012	161	251	675	832	1030	823	659	984	432	1020	871	370	497	318	597	601	843	50	67	966	746	369	587	820	869	499	540	408	493	0

These results lead to the following.

Theorem 19 *Let q be a prime power such that $q \leq 16$ or $q = 32$. Then every cyclic projective plane of order q^2 is desarguesian.*

Proof For $q \leq 9$, this was shown by Bruck [3]. The cases $q = 11, 13, 16, 32$ have been dealt with above. □

Remark 20 Using Algorithm 18, we have independently verified all results of Bruck [3].

Corollary 21 *The cyclic group of order $v = 1,049,601$ contains a unique nontrivial difference set, up to equivalence.*

Proof It is straightforward the check that, up to taking complements, we have $k \in \{1025, 460800, 461825\}$ if a (v, k, λ) difference set exists (see [2] for the definitions). Note that $v = q^2 + q + 1$ where $q = 1024$. Theorem 19 and Proposition 5 imply that there is a unique (v, k, λ) difference with $k = 1025$ cyclic group of order v. The Mann Test (see [2]) shows that there is no (v, k, λ) difference with $k \in \{460800, 461825\}$ in this group. □

4 Cyclic planes of nonsquare order

In this section, we use a depth first search algorithm together with homomorphic images to search for cyclic planes of order less than 41 and of orders 125 and 128. We first introduce some notation.

Let D be a subset of a cyclic group. We say that the condition $\Gamma(D)$ holds if $d_1 d_2^{-1} \neq d_3 d_4^{-1}$ for all $d_1, ..., d_4 \in D$ with $d_1 \neq d_2$.

Algorithm 22 (Depth first search for cyclic planes)

Input: $q = p^a$ where p is prime.

Output: A set $\mathcal{S}$ such that every cyclic planar difference set of order q is equivalent to an element of $\mathcal{S}$

Initialization:

1. Let G be a cyclic group of order $q^2 + q + 1$, and let O_1,...,O_t be the orbits of $x \mapsto x^p$ on G.
2. Set $\mathcal{S} := \emptyset$, $D := \emptyset$, $L := 1$, and $f(x) := 0$, $x = 1, ..., t$.

Main Step:

(i) If $|D| = q + 1$, then set $\mathcal{S} := \mathcal{S} \cup \{D\}$, $L := L - 1$, $D := D \setminus O_{f(L)}$.

(ii) Repeat until $L = 0$ or $f(L) < t$:
$f(L) := 0$, $L := L - 1$. If $L > 0$, then set $D := D \setminus O_{f(L)}$.

(iii) If $L = 0$, then output $\mathcal{S}$ and terminate the execution of the algorithm.

(iv) Set $y := f(L) + 1$. If $f(L) > 0$, then set $E := (D \setminus O_{f(L)}) \cup O_y$. If $f(L) = 0$, then set $E := D \cup O_y$.

(v) Set $f(L) := f(L) + 1$.

(vi) If $\Gamma(E)$ holds, then set $D := E$, $L := L + 1$.

(vii) Go to step (i).

The correctness of Algorithm 22 can be proved using the definition of a planar difference set and Result 4. For $q \leq 19$ and $q = 128$, a straightforward implementation of Algorithm 22 on a PC is sufficient to find all planar difference sets of order q up to equivalence. All difference sets found are equivalent to Singer difference sets. Thus all cyclic projective planes of order at most 19 and of order 128 are desarguesian.

For $q = 23, 29, 31, 37, 125$, we can use the results below to speed up Algorithm 22.

We first introduce some notation. Let $q = p^a$ where p is a prime, $v = q^2 + q + 1$, and let $G = \langle g \rangle$ be a cyclic group of order v. Let u be a divisor of v and $x \in \{0, ..., u-1\}$. We set

$$\mathcal{O}(x, q, u) = \{\{g^{yp^t} : t \in \mathbb{N}\} : y \in \mathbb{Z},\ y \equiv x \pmod{u}\}.$$

The elements of $\mathcal{O}(x, q, u)$ will be called *orbits* since they are orbits of the map $z \mapsto z^p$ on G.

Lemma 23 *Let $q = 23$, $v = q^2 + q + 1$, and let $G = \langle g \rangle$ be a cyclic group of order v. Every planar difference set of order q in G is equivalent to a difference set D with $D = D^{(q)}$ which contains $\{g, g^{23}, g^{489}\}$, two further orbits in $\mathcal{O}(1, 23, 7)$ and five orbits in $\mathcal{O}(3, 23, 7)$.*

Proof By Result 4 we can assume $D = D^{(23)}$. Let U be the subgroup of G of order 79. Let $\rho : G \to G/U$ be the natural epimorphism, and write $\rho(D) = \sum_{i=0}^{6} a_i h^i$ where $a_i \in \mathbb{Z}$ and h is a generator of G/U. As $D^{(23)} = D$, we have $\rho(D)^{(2)} = \rho(D)$, and thus $a_1 = a_2 = a_4$ and $a_3 = a_6 = a_5$. Since $|D| = 24$, we have $\sum a_i = 24$. Comparing the coefficient of the identity element in (2), we get $\sum a_i^2 = 23 + 79 = 102$. The only solutions to these conditions are $a_0 = 0$, $a_1 = a_2 = a_4 = 3$, $a_3 = a_6 = a_5 = 5$ and $a_0 = 0$, $a_1 = a_2 = a_4 = 5$, $a_3 = a_6 = a_5 = 3$. Replacing D by $D^{(3)}$, if necessary, we can assume $a_0 = 0$, $a_1 = a_2 = a_4 = 3$, and $a_3 = a_6 = a_5 = 5$. Note that every orbit in $\mathcal{O}(1, 23, 7)$ contained in D contributes exactly 1 to a_1, a_2, and a_4. Similarly, every orbit in $\mathcal{O}(3, 23, 7)$ contained in D contributes exactly 1 to a_3, a_6, and a_5. Thus D consists of three orbit in $\mathcal{O}(1, 23, 7)$ and five orbit in $\mathcal{O}(3, 23, 7)$. At least one element of $\mathcal{O}(1, 23, 7)$ contained in D, say O, contains a group element g^x with $(x, 533) = 1$. Thus there is an integer y with $y \equiv 1 \pmod 7$ and $(y, 533) = 1$ such that $g^y \in O$. Let t be an integer with $t \equiv 1 \pmod{7}$ and $ty \equiv 1 \pmod{79}$. Replacing D by $D^{(t)}$, if necessary, we can assume $g^{ty} = g \in D$. Since $D = D^{(23)}$, this implies $\{g, g^{23}, g^{489}\} \subset D$. □

Lemma 24 *Let $q = 29$, $v = q^2 + q + 1$, and let $G = \langle g \rangle$ be a cyclic group of order v. Every planar difference set of order q in G is equivalent to a difference set D with $D = D^{(q)}$ which contains $\{g^2, g^{58}, g^{811}\}$, one further orbit in $\mathcal{O}(2, 29, 13)$, three orbits in $\mathcal{O}(0, 29, 13)$, three orbits in $\mathcal{O}(4, 29, 13)$, and four orbits in $\mathcal{O}(7, 29, 13)$.*

Proof By Result 4 we can assume $D = D^{(29)}$. Let U be the subgroup of G of order 67. Let $\rho : G \to G/U$ be the natural epimorphism, and write $\rho(D) = \sum_{i=0}^{12} a_i h^i$ where $a_i \in \mathbb{Z}$ and h is a generator of G/U. As $D^{(29)} = D$, we have $\rho(D)^{(3)} = \rho(D)$, and thus $a_1 = a_3 = a_9$, $a_2 = a_6 = a_5$, $a_4 = a_{12} = a_{10}$, and $a_7 = a_8 = a_{11}$. Since $|D| = 30$, we have $\sum a_i = 30$. Comparing the coefficient of the identity element in (2), we get $\sum a_i^2 = 29 + 67 = 96$. There are exactly 30 solutions $(a_0, ..., a_{12})$ to these conditions, and the only solutions which satisfy (2) are given in the following table (the values of the other a_i's can be deduced from the equations above).

a_0	a_1	a_2	a_4	a_7
3	0	2	3	4
3	4	0	2	3
3	3	4	0	2
3	2	3	4	0

Replacing D by $D^{(2)}$, $D^{(4)}$, or $D^{(8)}$, if necessary, we can assume $a_0 = 3$, $a_1 = 0$, $a_2 = 2$, $a_4 = 3$, and $a_7 = 4$. Note that, for $x \in \{0, 1, 2, 4, 7\}$ every orbit in $\mathcal{O}(x, 29, 13)$ contained in D contributes exactly 1 to a_x. This implies that D contains three orbits in $\mathcal{O}(0, 29, 13)$, two orbits in $\mathcal{O}(2, 29, 13)$, three orbits in $\mathcal{O}(4, 29, 13)$, and four orbits in $\mathcal{O}(7, 29, 13)$.

At least one orbit in $\mathcal{O}(2, 29, 13)$ contained in D, say O, contains an element g^x with $(x, 871) = 1$. Thus there is an integer y with $y \equiv 2 \pmod{13}$ and $(y, 871) = 1$ such that $g^y \in O$. Let t be an integer with $t \equiv 1 \pmod{13}$ and $ty \equiv 2 \pmod{67}$. Replacing D by $D^{(t)}$, if necessary, we can assume $g^{ty} = g^2 \in D$. Since $D = D^{(29)}$, this implies $\{g^2, g^{58}, g^{811}\} \subset D$. $\square$

The following three lemmas can be proved by similar arguments, and we skip their proof.

Lemma 25 *Let $q = 31$, $v = q^2 + q + 1$, and let $G = \langle g \rangle$ be a cyclic group of order v. Every planar difference set of order q in G is equivalent to a difference set D with $D = D^{(q)}$ which contains $\{g^{331}, g^{662}\}$, four orbits in $\mathcal{O}(0, 31, 3)$ different from $\{1\}$, four orbits in $\mathcal{O}(1, 31, 3)$ different from $\{g^{331}\}$, and two orbits in $\mathcal{O}(2, 31, 3)$ different from $\{g^{662}\}$.*

Lemma 26 *Let $q = 37$, $v = q^2 + q + 1$, and let $G = \langle g \rangle$ be a cyclic group of order v. Every planar difference set of order q in G is equivalent to a difference set D with $D = D^{(q)}$ which contains $\{g^{469}, g^{938}\}$ and satisfies one of the following conditions.*

(*i*) *For* $x \in \{4, 6, 17, 18, 25, 27, 30, 41\}$*, the difference set* D *contains* $N(x)$ *orbits in* $\mathcal{O}(x, 37, 67)$ *where* $N(x)$ *is given in the following table.*

x	4	6	15	17	18	25	27	30	41
$f(x)$	2	1	2	2	1	1	1	1	1

(*ii*) *The difference set* D *contains one orbit in* $\mathcal{O}(0, 37, 67)$ *different from* $\{0\}$*,* $\{g^{469}\}$*, and* $\{g^{938}\}$ *and exactly one orbit from* $\mathcal{O}(x, 37, 67)$ *for each* $x \in \{2, 3, 5, 8, 12, 18, 27, 30, 32, 34, 41\}$.

Lemma 27 *Let* $q = 125$*,* $v = q^2 + q + 1$*, and let* $G = \langle g \rangle$ *be a cyclic group of order* v*. Every planar difference set of order* q *in* G *is equivalent to a difference set* D *with* $D = D^{(5)}$ *which contains exactly two orbits from* $\mathcal{O}(1, 125, 829)$*.*

Using Lemmas 23-27 to reduce the number of choices for the orbits in Algorithm 22 dramatically narrows the search space. For instance, a complete search for cyclic projective planes of order 37 using Lemma 26 takes less than three seconds on a PC. Straightforward implementations show that all cyclic planar difference sets of orders 23, 29, 31, 37, and 125 are equivalent to Singer difference sets. Summarizing the results of this section, we have the following.

Theorem 28 *Every cyclic projective plane of order at most* 37 *and of order* 125 *or* 128 *is desarguesian.*

References

[1] L.D. Baumert, D.M. Gordon: On the existence of cyclic difference sets with small parameters. *In: High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, Fields Inst. Commun. **41** (2004), 61-68.

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

[3] R.H. Bruck: Quadratic Extensions of Cyclic Planes. *Proc. Sympos. appl. Math.* **10** (1960), 15-44.

[4] P. Dembowski: *Finite geometries. Repr. of the 1968 ed.* Springer (1997).

[5] E. Ellers, H. Karzel: Endliche Inzidenzgruppen. *Abh. Math. Semin. Univ. Hamb.* **27** (1964), 250-264.

[6] D.M. Gordon: The prime power conjecture is true for $n < 2,000,000$. *J. Comb.* **1** (1994), 101-107.

[7] B. Gordon, W.H. Mills, L.R. Welch: Some new difference sets. Canad. J. Math. 14 1962 614–625.

[8] M. Hall: Cyclic projective planes. *Duke Math. J.* **14** (1947), 1079-1090.

[9] M. Hall: A survey of difference sets. *Proc. Am. Math. Soc.* **7** (1957), 975-986.

[10] J.W.P. Hirschfeld: *Projective geometries over finite fields. 2nd ed. Oxford Mathematical Monographs.* Clarendon Press 1998.

[11] R.L. McFarland, B.F. Rice: Translates and multipliers of abelian difference sets. *Proc.Amer. Math. Soc.* **68** (1978), 375-379.

[12] J. Singer: A theorem in finite projective geometry and some applications to number theory. *Trans. Amer. Math. Soc.* **43** (1938), 377-385.