FINITE FIELDS AND THEIR APPLICATIONS **3,** 300–313 (1997)
ARTICLE NO. FF970187

Cyclotomic Conditions Leading to New Steiner 2-Designs

Marco Buratti

Universita' de L'Aquila, Dipartimento di Ingegneria Elettrica,
I-67040 Poggio di Roio (Aq), Italy
E-mail: buratti@mat.uniroma1.it

Received June 12, 1996; revised May 16, 1997

We improve the constructions of S. Bagchi and B. Bagchi for Steiner 2-designs which are point-regular over the additive group of a Galois ring. As a consequence, we get new cyclotomic conditions leading to point-regular Steiner 2-designs with block size $k \in \{7, 9, 11, 13, 17\}$. © 1997 Academic Press

INTRODUCTION

Sometimes, the validity of elementary cyclotomic conditions in a finite field is sufficient to guarantee the existence of some Steiner 2-designs with a nice group of automorphisms. For instance, Bose [3] proved that if $q = 12t + 1$ (resp. $q = 20t + 1$) is a prime power such that -3 (resp. 5) is not a fourth power in GF(q), then there exists a point-regular S(2, 4, q) (resp. S(2, 5, q)). We also recall that cyclotomic conditions weaker than those of Bose may be found in [4].

In the present work, we obtain new cyclotomic conditions starting from a paper by Bagchi and Bagchi [1], where they give constructions for Steiner 2-designs generated by a relative difference family $\mathcal{D}$ over the additive group of a Galois ring.

We point out that the constructions of Bagchi and Bagchi were previously considered by Mathon [11, Theorem 3], but, unlike them, he did not give explicit cyclotomic conditions which are a consequence of the constructions in object.

We also point out that similar constructions for relative difference families were recently given by Greig [9]. The method of Greig is very successful

1071-5797/97 $25.00

but needs the aid of a computer and yields difference families that have multipliers of orders smaller than those of our difference families.

The results below are the main consequences of our constructions:

(i) Let $q = 6t + 1$ be a prime power and let 3^e be the largest power of 3 dividing t. Then, if 3 is a 3^eth power but not a 3^{e+1}th power in GF(q), there exists a point-regular S(2, 7, 7q).

(ii) Let $q = 8t + 1$ be a prime power and let 2^e be the largest power of 2 dividing t. Then, if 2 is a 2^{e+2}th power while $1 + \sqrt{2}$ is a 2^eth power but not a 2^{e+1}th power in GF(q), there exists a point-regular S(2, 9, 9q).

(iii) Let $q = 10t + 1$ be a prime power and let 5^e be the largest power of 5 dividing t. Then, if w is a primitive fifth root of unity in GF(q) such that both $w^2(w - 1)$ and $w^4(w + 1)$ are 5^{e+1}th powers in GF(q), there exists a point-regular S(2, 11, 11q).

(iv) Let $q = 12t + 1$ be a prime power and let 3^e be the largest power of 3 dividing t. Then, if 3 and $2 + \sqrt{3}$ are 3^eth powers but not 3^{e+1}th powers in GF(q) and if 6 is not a 3^{e+1}th power, there exists a point-regular S(2, 13, 13q).

Results (i), (ii), (iii) improve the results by Bagchi and Bagchi (corresponding to the cases where $e = 0$) while (iv) is completely new.

A less nice condition leading to point-regular S(2, 17, 17q) is also reported.

1. PRELIMINARIES

An S(2, k, v) (Steiner 2-design of order v and block-size k) is a pair (V, $\mathfrak{B}$), where V is a v-set of elements called points and $\mathfrak{B}$ is a family of k-subsets of V (blocks) such that each 2-subset of V is contained in exactly one block.

An automorphism of a Steiner 2-design (V, $\mathfrak{B}$) is a bijection on V whose induced mapping from $\mathfrak{B}$ to $\mathfrak{B}$ is a bijection too.

Let G be an automorphism group of a Steiner 2-design (V, $\mathfrak{B}$). Then (V, $\mathfrak{B}$) is said to be point-regular over G when G acts sharply transitively on V. Many point-regular Steiner 2-designs are realizable starting from a difference family.

Let N be a subgroup of an additive group G. A (G, N, k, 1) difference family (over G and relative to N) is a family $\mathfrak{D}$ of k-subsets of G (base blocks) such that the equation $x - y = g$ has exactly one solution pair $(x, y) \in \bigcup_{D \in \mathfrak{D}} D \times D$ for any fixed $g \in G - N$ and no solution pair $(x, y) \in \bigcup_{D \in \mathfrak{D}} D \times D$ for any fixed $g \in N - \{0\}$ (cf. [6]).

A multiplier of a $(G, N, k, 1)$-DF is an automorphism of the group G turning each base block of the family into the translate of itself of some other base block.

The following theorem is an useful tool for obtaining Steiner 2-designs starting from a difference family.

THEOREM 1.1. *Let G be an additive group of order v and let $\mathfrak{D}$ be a $(G, N, k, 1)$-DF, where N is a subgroup of G of order k. Then the pair $(G, \mathfrak{B} := (D + g \mid D \in \mathfrak{D}, g \in G) \cup (\text{right cosets of } N))$ is an $S(2, k, v)$ admitting G as a point-regular automorphism group with exactly one short block-orbit.*

In the case where G is cyclic, $(G, \mathfrak{B})$ is a cyclic design (cf. [7]).

Let $\mathrm{EA}(q)$ denote the elementary abelian group of order q. Our aim is to construct $(\mathrm{EA}(p) \oplus \mathrm{EA}(q), \mathrm{EA}(p) \times \{0\}, p, 1)$-DF's ($p$ and q prime powers). In order to simplify the notation, such a difference family will be denoted by $(pq, p, 1)$-DF. In view of Theorem 1.1 it generates a point-regular Steiner 2-design. Note that such a Steiner 2-design is cyclic in the case where p and q are distinct primes.

Notation 1.2. Given a finite field $\mathrm{GF}(q)$, by $\mathrm{GF}(q)^*$ and $\mathrm{GF}(q)^{\square}$ we respectively denote the set of nonzero elements and the set of nonzero squares in $\mathrm{GF}(q)$. Also, for a fixed primitive element ω, ind is the map from $\mathrm{GF}(q)^*$ to $\mathbb{Z}_{q-1}$ defined by $\mathrm{ind}(\omega^i) = i$.

For realizing our constructions, we need the following concept.

DEFINITION 1.3. Let $\mathrm{GF}(q)$ be the finite field of order q and let A be a subset of $\mathrm{GF}(q)^*$. Following [8], we say that *A splits $GF(q)$* if there exists a subset S of $\mathrm{GF}(q)^*$ such that the list $AS := (as \mid (a, s) \in A \times S)$ contains each element of $\mathrm{GF}(q)^*$ exactly once. (If this is the case we say that A splits $GF(q)$ with the splitting set S).

Of course, in order that two sets A and B split $\mathrm{GF}(q)$ with the same splitting set S, it is necessary that they have the same cardinality.

Without treating in detail the problem of how to establish if a given set $A \subset \mathrm{GF}(q)^*$ splits $\mathrm{GF}(q)$ (or equivalently (cf. [5]) whether the development of $\mathrm{ind}(A)$ possesses a perfect packing), we only give the following elementary results.

THEOREM 1.4. *Let $q = mnt + 1$ be a prime power, let d be a divisor of t and let $A = BC$ be an mn-subset of $GF(q)^*$, where B is a coset of the mth roots of unity in $GF(q)^*$. Then, if* $\mathrm{ind}(C) = \{0, d, 2d, \ldots, (n-1)d\} \pmod{nd}$, *we have that A splits $GF(q)$ with the splitting set $S := \{\omega^{ndi+j} \mid 0 \le i < t/d; 0 \le j < d\}$.*

Proof. We can set $C = \{c_0, c_1, \ldots, c_{n-1}\}$ assuming that $\mathrm{ind}(c_h) \equiv hd \pmod{nd}$, $h = 0, 1, \ldots, n-1$. Now, let x be an arbitrary residue (mod

nt) and consider the triple $(h, i, j) \in \{0, 1, \ldots, n-1\} \times \{0, 1, \ldots, t/d - 1\} \times \{0, 1, \ldots, d-1\}$ defined as

$$j \equiv x \pmod{d}; \qquad h \equiv \frac{x-j}{d} \pmod{n}; \qquad i \equiv \frac{x - j - \mathrm{ind}(c_h)}{nd} \left(\mathrm{mod}\, \frac{t}{d} \right).$$

Note that $x - j/d$ is an integer by definition of j and that $(x - j - \mathrm{ind}(c_h))/nd$ is also an integer by definition of h.

It is easily seen that with this choice of (h, i, j), we have that $\mathrm{ind}(c_h) + ndi + j \equiv x \pmod{nt}$. This means that $c_h \omega^{ndi+j}$, which belongs to the list CS, has index equivalent to $x \pmod{nt}$. So, since x is arbitrary and CS has exactly nt elements, we have that $\mathrm{ind}(CS) = \{0, 1, \ldots, nt - 1\} \pmod{nt}$. In other words, CS is a complete system of representatives for the cosets of the mth roots of unity in $\mathrm{GF}(q)$. So we have $AS = B(CS) = \mathrm{GF}(q)^*$. ■

THEOREM 1.5. *If A splits $GF(q)$ with the splitting set S, then A splits $GF(q^\alpha)$ with the splitting set ST, being T any complete system of representatives for the cosets of $GF(q)^*$ in $GF(q^\alpha)^*$.*

Proof. It is a consequence of the identities $AS = \mathrm{GF}(q)^*$ and $\mathrm{GF}(q)^* T = \mathrm{GF}(q^\alpha)^*$. ■

2. SOME GENERAL CONSTRUCTIONS

In this section we give two theorems that improve a construction by Bagchi and Bagchi [1] and that lead to $(pq, p, 1)$-DF's, where every base block is a coset of a subgroup of the units of $\mathrm{GF}(p) \oplus \mathrm{GF}(q)$ and zero.

THEOREM 2.1. *Let $p \equiv 3 \pmod 4$ and $q \equiv 1 \pmod{p-1}$ be prime powers. Let δ be a generator of $GF(p)^\square$ and let ε be a primitive $(p-1)$th root of unity in $GF(q)$. Denote by $\langle \varepsilon \rangle$ the subgroup generated by ε in the multiplicative group of $GF(q)$ and denote by $\langle (\delta, \varepsilon) \rangle$ the subgroup generated by (δ, ε) in the group of the units of $GF(p) \oplus GF(q)$. Then set*

$$I := \{(i, j) \mid \delta^i - \delta^j = 1\}, \qquad A = \{\pm \varepsilon^i \pm \varepsilon^j \mid (i, j) \in I\} \cup \{\pm 1\}.$$

Assume that $\langle \varepsilon \rangle$ and A split $GF(q)$ with the same splitting set S. Then, setting $D := \langle (\delta, \varepsilon) \rangle \cup \{(0, 0)\}$, we have that the family

$$\mathfrak{D} := (D \cdot (1, s) \mid s \in S)$$

is a $(pq, p, 1)$-DF.

Proof. We have

$$D = \{(0,0), (1, \pm 1), (\delta, \pm\varepsilon), (\delta^2, \pm\varepsilon^2), \ldots, (\delta^{(p-3)/2}, \pm\varepsilon^{(p-3)/2})\}.$$

Let ΔD be the list of differences $\neq (0,0)$ from D. It is easy to see that

$$\Delta D = \{0\} \times (2\langle\varepsilon\rangle) \cup \bigcup_{h=0}^{(p-3)/2} \{\delta^h\} \times (\varepsilon^h A) \cup \bigcup_{h=0}^{(p-3)/2} \{-\delta^h\} \times (\varepsilon^h A).$$

So, by definition of $\mathfrak{D}$, the list $\Delta\mathfrak{D}$ of differences $\neq (0,0)$ from $\mathfrak{D}$ is given by

$$\Delta\mathfrak{D} = \{0\} \times (2\langle\varepsilon\rangle S) \cup \bigcup_{h=0}^{(p-3)/2} \{\delta^h\} \times (\varepsilon^h AS) \cup \bigcup_{h=0}^{(p-3)/2} \{-\delta^h\} \times (\varepsilon^h AS).$$

On the other hand, we have by assumption $\langle\varepsilon\rangle S = AS = \mathrm{GF}(q)^*$ so that

$$\begin{aligned}\Delta\mathfrak{D} &= \{0\} \times \mathrm{GF}(q)^* \cup \bigcup_{h=0}^{(p-3)/2} \{\delta^h\} \times \mathrm{GF}(q)^* \cup \bigcup_{h=0}^{(p-3)/2} \{-\delta^h\} \times \mathrm{GF}(q)^* \\ &= \left(\{0\} \cup \bigcup_{h=0}^{(p-3)/2} \{\delta^h\} \cup \bigcup_{h=0}^{(p-3)/2} \{-\delta^h\}\right) \times \mathrm{GF}(q)^* = \mathrm{GF}(p) \times \mathrm{GF}(q)^*.\end{aligned}$$

This proves the theorem. ∎

Using the same notation as in the above theorem, note that $\langle\varepsilon\rangle$ and A may actually split $\mathrm{GF}(q)$ with the same splitting set S because they have the same cardinality. In fact we have $|\langle\varepsilon\rangle| = p - 1$ by definition of ε; further we have $|I| = (p-3)/4$ since $\mathrm{GF}(p)^\square$ is a $(p, (p-1)/2, (p-3)/4)$ difference set and, hence, $|A| = 4|I| + 2 = p - 1$.

THEOREM 2.2. *Let $p \equiv 1 \pmod 4$ and $q \equiv 1 \pmod{p-1}$ be prime powers. Let δ be a generator of $GF(p)^\square$ and let ε be a primitive $(p-1)$th root of unity in $GF(q)$. Set*

$$I := \{(i,j) \mid \delta^i - \delta^j = 1\}, \qquad I' := \{(i,j) \mid \delta^i - \delta^j = \alpha\},$$

where α is a fixed nonsquare in $GF(p)$. Now set $A := \{\pm\varepsilon^i \pm \varepsilon^j \mid (i,j) \in I\} \cup \{\pm 1, \pm\varepsilon^{(p-1)/4}\}$ and $A' := \{\pm\varepsilon^i \pm \varepsilon^j \mid (i,j) \in I'\}$. Assume that $\langle\varepsilon\rangle$, A and A' split $GF(q)$ with the same splitting set S. Then, setting $D := \langle(\delta, \varepsilon)\rangle \cup \{(0,0)\}$, we have that the family

$$\mathfrak{D}: = (D \cdot (1, s) \mid s \in S)$$

is a $(pq, p, 1)$*-DF.*

Proof. Here, we have

$$\Delta D = \{0\} \times (2\langle\varepsilon\rangle) \cup \bigcup_{h=0}^{(p-3)/2} \{\delta^h\} \times (\varepsilon^h A) \cup \bigcup_{h=0}^{(p-3)/2} \{\alpha\delta^h\} \times (\varepsilon^h A').$$

So, $\Delta\mathfrak{D} = \{0\} \times (2\langle\varepsilon\rangle) \cup \bigcup_{h=0}^{(p-3)/2} \{\delta^h\} \times (\varepsilon^h AS) \cup \bigcup_{h=0}^{(p-3)/2} \{\alpha\delta^h\} \times (\varepsilon^h A'S)$. Then, since $\langle\varepsilon\rangle S = AS = A'S = \mathrm{GF}(q)^*$, we have

$$\Delta\mathfrak{D} = \{0\} \times \mathrm{GF}(q)^* \cup \bigcup_{h=0}^{(p-3)/2} \{\delta^h\} \times \mathrm{GF}(q)^* \cup \bigcup_{h=0}^{(p-3)/2} \{\alpha\delta^h\} \times \mathrm{GF}(q)^*$$

$$= \left(\{0\} \cup \bigcup_{h=0}^{(p-3)/2} \{\delta^h\} \cup \bigcup_{h=0}^{(p-3)/2} \{\alpha\delta^h\}\right) \times \mathrm{GF}(q)^* = \mathrm{GF}(p) \times \mathrm{GF}(q)^*. \quad \blacksquare$$

Also here, it is easy to see that $\langle\varepsilon\rangle$, A and A' may possibly split $\mathrm{GF}(q)$ with the same splitting set S. This is essentially due to the fact that $\mathrm{GF}(p)^{\square}$ is a $(p, (p-1)/2, (p-5)/4, (p-1)/4)$ partial difference set (cf. [10]).

Remark 2.3. Note that the difference families constructed above, admit $\langle(\delta, \varepsilon)\rangle$ as a group of multipliers fixing each base block.

Applying the previous constructions with the smallest values of p (i.e., with $p = 3$ and $p = 5$), one may refind the following well-known results (cf. also [2, Chap. VII, Construction 4.1, Theorem 7.2]).

THEOREM 2.4 [13]. *There exists a* $(3q, 3, 1)$*-DF for any odd prime power* q*.*

THEOREM 2.5 [3]. *There exists a* $(5q, 5, 1)$*-DF for any prime power* $q \equiv 1 \pmod 4$.

It is easy to see that our constructions, like those of Bagchi and Bagchi, always work with pairs of prime powers (p, q), where q is a power of p. We point out that the result below—easily obtainable using our constructions and Theorem 1.5—is not deducible from the constructions of Bagchi and Bagchi.

THEOREM 2.6. *If Theorem* 2.1 *(or* 2.2*) yields a* $(pq, p, 1)$*-DF, then the same theorem yields a* $(pq^\alpha, p, 1)$*-DF for any positive integer* α*.*

In the next section we will obtain new results applying Theorems 2.1, 2.2 with $p = 7, 9, 11, 13, 17$.

3. SOME EXPLICIT CONDITIONS

In this section we finally prove the results summarized in the introduction. We warn the reader that in each of the theorems and lemmas, ω will denote a primitive element of the field GF(q).

THEOREM 3.1. *Let $q = 6t + 1$ be a prime power and let 3^e be the largest power of 3 dividing t. Then, if 3 is a 3^eth power but not a 3^{e+1}th power in GF(q), there exists a $(7q, 7, 1)$-DF.*

Proof. Apply Theorem 2.1 with $p = 7$, $\delta = 2$, and $\varepsilon \in \{\omega^t, \omega^{-t}\}$ such that 3ε is not a 3^{e+1}th power in GF(q). Note that such an ε surely exists because if both $3\omega^t$ and $3\omega^{-t}$ are 3^{e+1}th powers in GF(q), then ω^{2t} ($= 3\omega^t/3\omega^{-t}$) would be also such, contradicting the hypothesis that 3^e is the largest power of 3 dividing t.

We have $1 = \delta^i - \delta^j$ only for $(i, j) = (1, 0)$ and, hence, $I = \{(1, 0)\}$ and $A = \pm\{\varepsilon - 1, \varepsilon + 1, 1\}$.

Since ε is a sixth primitive root of unity we have $0 = (\varepsilon^3 + 1)/(\varepsilon + 1) = \varepsilon^2 - \varepsilon + 1$ so that $(\varepsilon + 1)^2 = 3\varepsilon$ and $(\varepsilon - 1)^2 = -\varepsilon$. So, since 3 and 3ε are not 3^{e+1}th powers, we easily deduce that $\mathrm{ind}(\{1, (\varepsilon - 1)^2, (\varepsilon + 1)^2\}) \equiv \{0, 3^e, 3^e 2\} \pmod{3^{e+1}}$. It follows that $\mathrm{ind}(\{1, \varepsilon - 1, \varepsilon + 1\}) \equiv \{0, 3^e, 3^e 2\} \pmod{3^{e+1}}$. Of course, we have also $\mathrm{ind}(\{1, \varepsilon, \varepsilon^2\}) \equiv \{0, 3^e, 3^e 2\} \pmod{3^{e+1}}$ so that using Theorem 1.4 with $m = 2$, $n = 3$, and $d = 3^e$ we have that $\langle\varepsilon\rangle$ and A split GF(q) with the splitting set $S := \{\omega^{3^{e+1}i+j} \mid 0 \le i < t/3^e; 0 \le j < 3^e\}$. It follows that the family

$$\mathfrak{D} = \left(\{(0, 0), (1, \pm 1), (2, \pm\varepsilon), (4, \pm\varepsilon^2)\} \cdot (1, \omega^{3^{e+1}i+j}) \mid 0 \le i < \frac{t}{3^e}; 0 \le j < 3^e\right)$$

is a $(7q, 7, 1)$-DF. ∎

Restating the previous theorem in the case where $e = 0$, we refind the following weaker result of Bagchi and Bagchi.

THEOREM 3.2. *Let $q \equiv 7, 13 \pmod{18}$ be a prime power. Then, if 3 is not a cube in GF(q), we have that the family*

$$\mathfrak{D} = (\{(0, 0), (1, \pm 1), (2, \pm\varepsilon), (4, \pm\varepsilon^2)\} \cdot (1, \omega^{3i}) \mid 0 \le i < t)$$

is a $(7q, 7, 1)$-DF for a suitable cube root of unity ε in GF(q).

COROLLARY 3.3. *There exists a cyclic* $S(2, 7, 7p)$ *for any prime* $p \equiv 7, 13 \pmod{18}$ *but* $p \neq 7$, *provided that* 3 *is not a cube* $\pmod{p}$.

The primes $q < 1.000$ for which Theorem 3.1 succeeds are 7, 13, 31, 43, 73, 79, 97, 139, 157, 211, 223, 229, 241, 271, 277, 283, 313, 331, 337, 349, 373, 409, 421, 457, 463, 571, 577, 601, 607, 613, 673, 691, 709, 733, 751, 769, 823, 859, 877, 907, 991.

Among these primes, those having $e \neq 0$ are $q = 73, 577, 613, 991$ (having $e = 1$) and $q = 271$ (having $e = 2$). The first prime for which Theorem 3.1 works with $e = 3$ is 2,269; the first one with $e = 4$ is 32,563; the first one with $e = 5$ is 176,419.

LEMMA 3.4. *Let* $q = 8t + 1$ *be a prime power, let* 2^e *be the largest power of* 2 *dividing* t *and let* $\varepsilon = \omega^t$. *Then we have:*

(i) $(\varepsilon^2 - 1)$ *is a* 2^e*th power but not a* 2^{e+1}*th power in* $GF(q)$ *if and only if* 2 *is a* 2^{e+2}*th power in* $GF(q)$.

(ii) $(\varepsilon + 1)/(\varepsilon - 1)$ *is a* 2^e*th power but not a* 2^{e+1}*th power in* $GF(q)$ *if and only if* $1 + \sqrt{2}$ *is a* 2^e*th power but not a* 2^{e+1}*th power in* $GF(q)$. (*Note that this statement is not ambiguous; in fact, if the condition "*$1 + \sqrt{2}$ *is a* 2^f*th* ($f \leq e + 1$) *power in* $GF(q)$*" holds for one square root of* 2, *it also holds for the other. This is because* $(1 + \sqrt{2})(1 - \sqrt{2}) = -1$).

(iii) *If* $e = 0$ *and* 2 *is a fourth power in* $GF(q)$, *then* $1 + \sqrt{2}$ *is a nonsquare in* $GF(q)$.

Proof. (i) Of course, $(\varepsilon^2 - 1)$ is a 2^eth power but not a 2^{e+1}th power in $\mathrm{GF}(q)$ if and only if $(\varepsilon^2 - 1)^2$ is a 2^{e+1}th power but not a 2^{e+2}th power in $\mathrm{GF}(q)$, that is if and only if $\mathrm{ind}((\varepsilon^2 - 1)^2) \equiv 2^{e+1} \pmod{2^{e+2}}$. On the other hand, being ε a primitive eighth root of unity in $\mathrm{GF}(q)$, we have $(\varepsilon^2 - 1)2 = -2\varepsilon^2$ so that

$$\mathrm{ind}((\varepsilon^2 - 1)^2) = \mathrm{ind}(-1) + \mathrm{ind}(2) + \mathrm{ind}(\varepsilon^2) =$$
$$= 4t + \mathrm{ind}(2) + 2t \equiv \mathrm{ind}(2) + 2^{e+1} \pmod{2^{e+2}}.$$

Hence we have $\mathrm{ind}(\varepsilon^2 - 1)^2 \equiv 2^{e+1} \pmod{2^{e+2}}$ if and only if $\mathrm{ind}(2) \equiv 0 \pmod{2^{e+2}}$, that is, if and only if 2 is a 2^{e+2}th power in $\mathrm{GF}(q)$.

(ii) Note that $(\varepsilon^2(\varepsilon + 1)/(\varepsilon - 1) - 1)^2 = 2$. In fact we have

$$\left(\frac{\varepsilon^2(\varepsilon + 1)}{\varepsilon - 1} - 1\right)^2 = \frac{(\varepsilon^3 + \varepsilon^2 - \varepsilon + 1)^2}{(\varepsilon - 1)^2} = \frac{\varepsilon^6 + 2\varepsilon^5 - \varepsilon^4 + 3\varepsilon^2 - 2\varepsilon + 1}{(\varepsilon - 1)^2}$$
$$= (\text{since } \varepsilon^4 = -1)\, \frac{2\varepsilon^2 - 4\varepsilon + 2}{(\varepsilon - 1)^2} = 2.$$

It follows that $(\varepsilon + 1)/(\varepsilon - 1) = \varepsilon^6(1 + \sqrt{2})$ and, hence, that $\mathrm{ind}((\varepsilon + 1)/(\varepsilon - 1)) = 6t + \mathrm{ind}(1 + \sqrt{2})$. The assertion easily follows.

(iii) Under the hypothesis that $e = 0$ and that 2 is a fourth power in GF(q), we have, by (i), that $\varepsilon^2 - 1$ ($= (\varepsilon + 1)(\varepsilon - 1)$) is a nonsquare in GF($q$) so that $(\varepsilon + 1)/(\varepsilon - 1)$ is also a nonsquare. Then the assertion follows from (ii). ■

THEOREM 3.5. *Let $q = 8t + 1$ be a prime power and let 2^e be the largest power of 2 dividing t. Then, if 2 is a 2^{e+2}th power and if $1 + \sqrt{2}$ is a 2^eth power but not a 2^{e+1}th power in GF(q), there exists a $(9q, 9, 1)$-DF.*

Proof. Let us apply Theorem 2.2 with $p = 9$, $\delta = \sqrt{2}$, $\alpha = \sqrt{2} + 2$, and $\varepsilon = \omega^t$. Of course, $\sqrt{2}$ here represents a square root of 2 in GF(9) while in the statement of the theorem it represents a square root of 2 in GF(q).

We have $1 = \delta^i - \delta^j$ only for $(i, j) = (2, 0)$ and, hence, $A = \pm\{\varepsilon^2 - 1, \varepsilon^2 + 1, 1, \varepsilon^2\}$. Also, we have that $\sqrt{2} + 2 = \delta^i - \delta^j$ for $(i, j) \in \{(1, 0), (2, 3)\}$. Hence, we have $A' = \pm\{\varepsilon - 1, \varepsilon + 1, \varepsilon^3 - \varepsilon^2, \varepsilon^3 + \varepsilon^2\}$.

It is easy to check that

$$\langle\varepsilon\rangle = \{\pm 1, \pm\varepsilon^2\} \cdot \{1, \varepsilon\};$$

$$A = \{\pm 1, \pm\varepsilon^2\} \cdot \{1, \varepsilon^2 - 1\};$$

$$A' = (\varepsilon - 1) \cdot \{\pm 1, \pm\varepsilon^2\} \cdot \left\{1, \frac{\varepsilon + 1}{\varepsilon - 1}\right\}.$$

By (i) and (ii) of Lemma 3.4, $\varepsilon^2 - 1$ and $(\varepsilon + 1)/(\varepsilon - 1)$ are 2^eth powers but not 2^{e+1}th powers in GF(q) so that

$$\mathrm{ind}(\{1, \varepsilon\}) = \mathrm{ind}(\{1, \varepsilon^2 - 1\} = \mathrm{ind}\left(\left\{1, \frac{\varepsilon + 1}{\varepsilon - 1}\right\}\right) = \{0, 2^e\} \,(\mathrm{mod}\, 2^{e+1}).$$

So, using Theorem 1.4 with $m = 4$, $n = 2$, and $d = 2^e$ we have that $\langle\varepsilon\rangle$, A, and A' split GF(q) with the splitting set S: $= \{\omega^{2^{e+1}i+j} \mid 0 \le i < t/2^e;\ 0 \le j < 2^e\}$.

It follows that the family

$$\mathfrak{D} = (\{(0, 0), (1, \pm 1), (\sqrt{2}, \pm\varepsilon), (2, \pm\varepsilon^2), (2\sqrt{2}, \pm\varepsilon^3)\}(1, \omega^{2^{e+1}i+j}) \mid$$
$$0 \le i < t/2^e; 0 \le j < 2^e)$$

is a $(9q, 9, 1)$-DF. ■

The previous theorem succeeds quite rarely with $e \neq 0$. Taking into account Lemma 3.4(iii), the statement of Theorem 3.5 in the case $e = 0$ sounds as follows.

THEOREM 3.6. *Let $q \equiv 9 \pmod{16}$ be a prime power and let ε be a primitive eighth root of unity in GF(q). Then, if 2 is a fourth power in GF(q), we have that the family*

$$\mathfrak{D} = (\{(0,0), (1, \pm 1), (\sqrt{2}, \pm\varepsilon), (2, \pm\varepsilon^2), (2\sqrt{2}, \pm\varepsilon^3)\} \cdot (1, \omega^{2i}) \mid 0 \leq i < t)$$

is a $(9q, 9, 1)$-DF.

Bagchi and Bagchi obtained the previous theorem with the superfluous hypothesis that $1 + \sqrt{2}$ is not a square in GF(q), although they themselves conjectured its uselessness. This conjecture, which we have proved to be true in Lemma 3.4(iii), has been proved also in [12].

Note that 2 is a fourth power in GF($q^{2\alpha}$) for any prime $q \equiv 3 \pmod 8$ and any positive integer α. So we have:

COROLLARY 3.7. *There exists a point-regular $S(2, 9, 9q^{2\alpha})$ for any prime $q \equiv 3 \pmod 8$ and any positive integer α.*

Using the previous results, we succeed in finding a point-regular $S(2, 9, 9q)$ for each of the following prime powers $q < 5.000$: 9, 73, 89, 121, 233, 281, 337, 361, 601, 617, 881, 937, 1,033, 1,049, 1,097, 1,193, 1,289, 1,433, 1,481, 1,553, 1,609, 1,721, 1,753, 1,801, 1,849, 1,913, 2,281, 2,393, 2,441, 2,473, 2,809, 2,857, 2,969, 3,049, 3,257, 3,449, 3,481, 3,529, 3,673, 3,833, 4,049, 4,153, 4,201, 4,217, 4,273, 4,297, 4,409, 4,457, 4,489, 4,937.

The only primes of this list having $e \neq 0$ are 881, 1,553, 4,049, 4,273 ($e = 1$). The first prime q for which Theorem 3.10 works with $e = 2$ is 10,657.

THEOREM 3.8. *Let $q = 10t + 1$ be a prime power and let 5^e be the largest power of 5 dividing t. Then, if there exists a primitive fifth root of unity w in GF(q) such that both $w^2(w - 1)$ and $w^4(w + 1)$ are 5^{e+1}th powers in GF(q), there exists an $(11q, 11, 1)$-DF.*

Proof. Apply Theorem 2.1 with $p = 11$, $\delta = 3$, and $\varepsilon = -w$. We have $1 = \delta^i - \delta^j$ for $(i, j) \in \{(4, 1), (3, 4)\}$ and, hence,

$$A = \pm\{w^4 - w, w^4 + w, w^3 - w^4, w^3 + w^4, 1\}.$$

Taking into account that w is a fifth primitive root of unity, it is easy to see that

$$A = \pm w^3 \cdot \left\{w - 1, w + 1, w(w-1)(w+1), \frac{1}{w+1}, w^2\right\}.$$

We have $\mathrm{ind}(w) = 5^e h$ for some $h \in \{1, 2, 3, 4\}$. Then, since $w^2(w-1)$ and $w^4(w+1)$ are 5^{e+1}th powers, we have $\mathrm{ind}(w-1) \equiv 5^e 3h \pmod{5^{e+1}}$ and $\mathrm{ind}(w+1) \equiv 5^e h \pmod{5^{e+1}}$. It easily follows that

$$\mathrm{ind}\left(\left\{w-1, w+1, w(w-1)(w+1), \frac{1}{w+1}, w^2\right\}\right)$$
$$= \{0, 5^e, 5^e 2, 5^e 3, 5^e 4\} \pmod{5^{e+1}}.$$

So, using Theorem 1.4 with $m = 2$, $n = 5$, and $d = 5^e$ we have that $\langle \varepsilon \rangle$ and A split $\mathrm{GF}(q)$ with the splitting set $S := \{\omega^{5^{e+1}i+j} \mid 0 \le i < t/5^e; 0 \le j < 5^e\}$. It follows that the family

$$\mathfrak{D} = (\{(0,0), (1, \pm 1), (3, \pm w), (9, \pm w^2), (5, \pm w^3), (4, \pm w^4)\}(1, \omega^{5^{e+1}i+j}) \mid$$
$$0 \le i < t/5^e; 0 \le j < 5^e)$$

is an $(11q, 11, 1)$-DF. ■

In the case where $e = 0$, we can restate Theorem 3.8 in the following way equivalent to [1, Theorem 2(e)].

THEOREM 3.9. *Let q be a prime power such that $q \equiv 1 \pmod{10}$ and $q \not\equiv 1 \pmod{50}$. Then, if w is a primitive fifth root of unity in $GF(q)$ such that both $w^2(w-1)$ and $w^4(w+1)$ are fifth powers in $GF(q)$, we have that the family*

$$\mathfrak{D} = (\{(0,0), (1, \pm 1), (3, \pm w), (9, \pm w^2), (5, \pm w^3), (4, \pm w^4)\}(1, \omega^{5i}) \mid 0 \le i < t)$$

is an $(11q, 11, 1)$-DF.

Applying Theorem 3.8 we find a cyclic $S(2, 11, 11q)$ for each of the following primes $q < 5.000$: 331, 541, 571, 911, 941, 1.231, 1,481, 1,621, 1,721, 1,741, 2,161, 2,281, 2,371, 3,011, 3,361, 3,391, 3,821, 4,231, 4,931.

In the previous list there is no prime having $e \neq 0$ and in fact it is the same list as given by Bagchi and Bagchi. We have found no prime $q < 10^6$ for which Theorem 3.8 works with $e \neq 0$. Anyway, Theorem 3.8 surely yields some DF's which are not obtainable by Theorem 3.9. For instance, all the $(11q^{5\alpha}, 11, 1)$-DF's, where q is a prime satisfying Theorem 3.9 itself and α is a positive integer (cf. Theorem 2.6).

LEMMA 3.10. *Let $q = 12t + 1$ be a prime power and let 3^e be the largest power of 3 dividing t. If both 3 and $2 + \sqrt{3}$ are 3^eth powers but not 3^{e+1}th powers in $GF(q)$ and if 6 is not a 3^{e+1}th power in $GF(q)$, we have that:*

(i) $\varepsilon(\varepsilon + 1)$ *is a* 3^e*th power but not a* 3^{e+1}*th power in GF*(q) *for each* $\varepsilon \in \{\pm\omega^t, \pm\omega^{-t}\}$.

(ii) $\mathrm{ind}(\{\varepsilon, \varepsilon^2 + 1, \varepsilon^3 + 1\}) = \{0, 3^e, 3^e 2\} \pmod{3^{e+1}}$ *for an appropriate choice of* $\varepsilon \in \{\omega^t, \omega^{-t}\}$.

Proof. Before proving the lemma, we observe that the condition "$2 + \sqrt{3}$ is a 3^fth ($f \le e + 1$) power in GF(q)" does not depend on the choice of the square root of 3. This is because $(2 + \sqrt{3})(2 - \sqrt{3}) = 1$.

(i) Assume that $\varepsilon \in \{\pm\omega^t, \pm\omega^{-t}\}$, namely that ε is a primitive 12th root of unity in GF(q). Then ε is an element of the set $\{\pm(\sqrt{3} + \sqrt{-1})/2, \pm(\sqrt{3} - \sqrt{-1})/2\}$. In fact, a trivial calculation shows that each element of this set has order 12 in the multiplicative group of GF(q). We only consider the case where $\varepsilon = (\sqrt{3} + \sqrt{-1})/2$ since the other cases are very similar. In this case we have $\varepsilon(\varepsilon + 1) = (1 + \sqrt{-1})(1 + \sqrt{3})/2$. It follows that $[\varepsilon(\varepsilon + 1)]^2 = \sqrt{-1}(2 + \sqrt{3})$. So, being $\sqrt{-1}$ a 3^{e+1}th power and being $2 + \sqrt{3}$ a 3^eth power but not a 3^{e+1}th power, we have the assertion.

(ii) Since the three cube roots of -1 (i.e., -1, ε^2, $-\varepsilon^4$) sum to zero, we have $(\varepsilon^2 + 1)^2 = 3\varepsilon^2$; in addition, $(\varepsilon^3 + 1)^2 = 2\varepsilon^3$. So we have $\mathrm{ind}(\{\varepsilon^2, (\varepsilon^2 + 1)^2, (\varepsilon^3 + 1)^2\}) = \mathrm{ind}(\varepsilon^2\{1, 3, 2\varepsilon\}) \pmod{3^{e+1}}$. It follows that also $\mathrm{ind}(\{\varepsilon, \varepsilon^2 + 1, \varepsilon^3 + 1\}) = \mathrm{ind}(\varepsilon^2\{1, 3, 2\varepsilon\}) \pmod{3^{e+1}}$. Finally, 3 being a 3^eth power but not a 3^{e+1}th power in GF(q), it is easy to see that $\mathrm{ind}(\varepsilon^2\{1, 3, 2\varepsilon\}) = \{0, 3^e, 3^e 2\} \pmod{3^{e+1}}$, provided that 6ε is a 3^{e+1}th power. So, we only have to check that 6ε is a 3^{e+1}th power for an appropriate choice of $\varepsilon \in \{\omega^t, \omega^{-t}\}$. First note that $\mathrm{ind}(6\omega^t) \neq \mathrm{ind}(6\omega^{-t}) \pmod{3^{e+1}}$, since otherwise ω^{2t} $(= 6\omega^t/6\omega^{-t})$ would be a 3^{e+1}th power contradicting the hypothesis that 3^e is the highest power of 3 dividing t. Then, if 6ε is not a 3^{e+1}th power for both $\varepsilon = \omega^t$ and $\varepsilon = \omega^{-t}$, we would have that $\mathrm{ind}(\{6\omega^t, 6\omega^{-t}\}) = \{3^e, 3^e 2\} \pmod{3^{e+1}}$. It would follow that $(6\omega^t)(6\omega^{-t})$, that is 6^2, is a 3^{e+1}th power in GF(q) contradicting the assumption that 6 is not a 3^{e+1}th power. ∎

THEOREM 3.11. *Let* $q = 12t + 1$ *be a prime power and let* 3^e *be the largest power of* 3 *dividing* t. *If both* 3 *and* $2 + \sqrt{3}$ *are* 3^e*th powers but not* 3^{e+1}*th powers in GF*(q) *and if* 6 *is not a* 3^{e+1}*th power in GF*(q), *then there exists a* $(13q, 13, 1)$*-DF.*

Proof. Let us apply Theorem 2.2 with $p = 13$, $\delta = 4$, $\alpha = 2$, and $\varepsilon \in \{\omega^t, \omega^{-t}\}$ satisfying $\mathrm{ind}(\{\varepsilon, \varepsilon^2 + 1, \varepsilon^3 + 1\}) = \{0, 3^e, 3^e 2\} \pmod{3^{e+1}}$ (Lemma 3.13(ii) assures the existence of such an ε).

We have $1 = \delta^i - \delta^j$ for $(i, j) \in \{(1, 2), (5, 4)\}$. So we have

$$A = \pm\{\varepsilon^2 - \varepsilon, \varepsilon^2 + \varepsilon, \varepsilon^5 - \varepsilon^4, \varepsilon^5 + \varepsilon^4, 1, \varepsilon^3\}.$$

Also, we have that $2 = \delta^i - \delta^j$ for $(i, j) \in \{(2, 0), (0, 3), (3, 5)\}$. Hence, we have

$$A' = \pm\{\varepsilon^2 - 1, \varepsilon^2 + 1, \varepsilon^3 - 1, \varepsilon^3 + 1, \varepsilon^5 - \varepsilon^3, \varepsilon^5 + \varepsilon^3\}.$$

Now, it is easy to check that:

$$\langle \varepsilon \rangle = \{\pm 1, \pm \varepsilon^3\} \cdot \{1, \varepsilon, \varepsilon^2\};$$

$$A = \{\pm 1, \pm \varepsilon^3\} \cdot \left\{1, \varepsilon(\varepsilon + 1), \frac{1}{\varepsilon(\varepsilon + 1)}\right\};$$

$$A' = \{\pm 1, \pm \varepsilon^3\} \cdot \{\varepsilon, \varepsilon^2 + 1, \varepsilon^3 + 1\}.$$

In view of Lemma 3.10 we have

$$\operatorname{ind}(\{1, \varepsilon, \varepsilon^2\}) = \operatorname{ind}\left(\left\{1, \varepsilon(\varepsilon + 1), \frac{1}{\varepsilon(\varepsilon + 1)}\right)\right\} = \operatorname{ind}(\{\varepsilon, \varepsilon^2 + 1, \varepsilon^3 + 1\})$$
$$= \{0, 3^e, 3^e 2\} \pmod{3^{e+1}}.$$

So, using Theorem 1.4 with $m = 4$, $n = 3$, and $d = 3^e$ we have that $\langle \varepsilon \rangle$, A and A' split GF(q) with the splitting set S: $= \{\omega^{3^{e+1}i+j} \mid 0 \le i < t/3^e; 0 \le j < 3^e\}$. It follows that the family

$$\mathfrak{D} = (\{(0, 0), (1, \pm 1), (4, \pm \varepsilon), (3, \pm \varepsilon^2), (12, \pm \varepsilon^3), (9, \pm \varepsilon^4), (10, \pm \varepsilon^5)\}$$
$$\cdot (1, \omega^{3^{e+1}i+j}) \mid 0 \le i < t/3^e; 0 \le j < 3^e\})$$

is a $(13q, 13, 1)$-DF. ■

Once again, it is convenient to restate the previous theorem in the case where $e = 0$.

THEOREM 3.12. *Let* $q \equiv 13, 25 \pmod{36}$ *be a prime power such that both* 3, 6, *and* $2 + \sqrt{3}$ *are noncubes in GF*(q). *Then the family*

$$\mathfrak{D} = (\{(0, 0), (1, \pm 1), (4, \pm \varepsilon), (3, \pm \varepsilon^2), (12, \pm \varepsilon^3), (9, \pm \varepsilon^4), (10, \pm \varepsilon^5)\}(1, \omega^{3i}) \mid$$
$$0 \le i < t)$$

is a $(13q, 13, 1)$*-DF.*

COROLLARY 3.13. *There exists a cyclic* $S(2, 13, 13q)$ *for any prime* $q \equiv 13, 25 \pmod{36}$ *but* $q \neq 13$, *provided that* 3, 6, *and* $2 + \sqrt{3}$ *are noncubes* (mod q).

Applying Theorem 3.11 we find a cyclic $S(2, 13, 13q)$ for each of the following primes $q < 5.000$: 157, 229, 457, 601, 613, 673, 709, 769, 1,069, 1,201, 1,381, 1,429, 1,489, 1,549, 1,777, 1,789, 1,993, 2,113, 2,293, 2,437, 2,689,

2,749, 2,797, 2,833, 3,121, 3,301, 3,769, 3,793, 4,129, 4,153, 4,273, 4,621, 4,657, 4,909.

In the above list the only primes having $e \neq 0$ are 613 and 1,549 ($e = 1$).

We finally report without proof the consequences of Theorem 2.2 in the case where $p = 17$.

THEOREM 3.14. *Let $q = 16t + 1$ be a prime power and let 2^e be the highest power of 2 dividing t. Then, if w is a primitive 16th root of unity in $GF(q)$ such that both the sets $\{1, w^2, w - 1, w + 1\}$ and $\{w^2, w^3, w^3 - 1, w^3 + 1\}$ are systems of representatives for the cosets of the 2^{e+2}th powers in the group of the 2^eth powers in $GF(q)$, there exists a $(17q, 17, 1)$-DF.*

The only primes $q < 10.000$ for which Theorem 3.14 leads to a cyclic $S(2, 17, 17q)$ are 2,801, 3,793, 6,833, 6,961 and 8,017.

ACKNOWLEDGMENT

The author wishes to thank the referees for their valuable and helpful comments.

REFERENCES

1. S. Bagchi and B. Bagchi, Designs from pairs of finite fields I. A cyclic Unital U(6) and other regular Steiner 2-designs, *J. Combin. Theory Ser. A* **52** (1989), 51–61.
2. T. Beth, D. Jungnickel, and H. Lenz, "Design Theory," Cambridge Univ. Press, Cambridge, 1993.
3. R. C. Bose, On the construction of balanced incomplete block designs, *Ann. Eugenics* **9** (1939), 353–399.
4. M. Buratti, Improving two theorems of Bose on difference families, *J. Combin. Designs* **3** (1995), 15–24.
5. M. Buratti, A packing problem and its application to Bose's families, *J. Combin. Designs* **4** (1996), 457–472.
6. M. Buratti, Recursive constructions for difference matrices and relative difference families, *J. Combin. Designs,* to appear.
7. M. J. Colbourn and R. Mathon, On cyclic Steiner 2-designs, *Ann. Discrete Math.* **7** (1980), 215–253.
8. S. Galovich and S. Stein, Splittings of Abelian groups by integers, *Aequationes Math.* **22** (1981), 249–267.
9. M. Greig, Some group divisible design constructions, *J. Combin. Math. Combin. Comput.,* to appear.
10. S. L. Ma, A survey on partial difference sets, *Designs Codes Cryptogr.* **4** (1994), 221–261.
11. R. Mathon, Constructions for cyclic Steiner 2-designs, *Ann. Discrete Math.* **34** (1987), 353–362.
12. B. Schmidt, Note on a question by S. Bagchi and B. Bagchi, *Designs Codes Cryptogr.* **2** (1992), 395.
13. T. Skolem, Note 16, *in* "Kombinatorik" (E. Netto, Ed.), 2nd ed., Teubner, Leipzig, 1927.