Designs from Pairs of Finite Fields. I. A Cyclic Unital $U(6)$ and Other Regular Steiner 2-Designs

SUNANDA BAGCHI AND BHASKAR BAGCHI

Computer Science Unit, Stat-Math. Division,
Indian Statistical Institute, 203 Barrackpore Trunk Road,
Calcutta 700 035, India

Communicated by the Managing Editors

Received January 15, 1988

A general construction for Steiner 2-designs with prime power block size (and with a point-regular automorphism group) is presented. Its success depends on number-theoretic restrictions on the parameters--these are completely analysed in case of block sizes $k \leqslant 11$. The new designs constructed include infinitely many cyclic Steiner 2-designs with block size 7. Among them is a cyclic unital $U(6)$, that is, an $S(2, 6+1, 6^3+1)$. It is the first example of a unital with non-prime power parameter and the second example of a cyclic unital.

1. INTRODUCTION

Recall that a Steiner t-design with parameters v and k, denoted by $S(t, k, v)$, is a pair (X, B), where X is a v-set (its elements are called points) and B is a set of k-subsets of X (its elements are called blocks) such that each t-subset of X is contained in a unique block. The design is called *regular* if it admits an automorphism group of order v which acts transitively on the points. If, further, this group is cyclic then the design is called *cyclic*.

Barring the (desarguesian) projective spaces $S(2, s+1, (s^n-1)/(s-1))$, $n \geqslant 3$ and s a prime power (which are cyclic by Singer's argument in [14]), the only general constructions of cyclic $S(2, k, v)$'s available so far were for $k \leqslant 5$ (see [3, 5, 11]).

In the following, $E(s)$ will denote the cyclic group of order s if s is a prime, and, more generally, we put $E(s) = E(s_1) \times E(s_2) \times \cdots \times E(s_n)$ if $s = s_1 s_2 \cdots s_n$ with s_i's primes. Thus, if s is squarefree then $E(s)$ is cyclic.

Let p and q be two odd prime powers such that $p-1$ divides $q-1$. In Section 2 below we use the finite fields of order p and q to present a construction of a regular $S(2, p, pq)$ admitting $E(pq)$ as a point-regular automorphism group—provided p and q satisfies certain complicated number-theoretic conditions (see Theorem 1). Note that the divisibility condition on p, q is necessary for the existence of $S(2, p, pq)$. In case p and q are distinct primes, the design obtained is cyclic.

The conditions involved have defied complete analysis so far. A complete analysis appears to be feasible for each fixed value of p, but it is of increasing complexity with increase in p. In this paper the analysis has been carried through for $p \leqslant 11$. The results are presented in Theorem 2 in Section 3. As a corollary it is shown that for each p in this range there are infinitely many q with $(p, q) = 1$ for which the construction works. We conjecture that for each prime p there are infinitely many primes q for which the construction works, yielding cyclic $S(2, p, pq)$. We prove this for $p \leqslant 7$.

It is briefly pointed out in Section 2 that when the construction succeeds, the full automorphism group of the design obtained is larger than $E(v)$; indeed, it is nonabelian. Determination of the group appears to be a difficult problem.

A notable success of our construction is the case $(p, q) = (7, 31)$, yielding a cyclic unital $U(6)$. Recall that a unital with parameter s, denotes here by $U(s)$, is an $S(2, s+1, s^3+1)$. As pointed out by Hughes and Piper in [8] and by Piper in [12], unitals $U(s)$ were hitherto known only for prime powers s. The case $(p, q) = (5, 13)$ of our construction yields a cyclic unital $U(4)$. This one is implicitly contained in [5]. Apparently, other than the $U(4)$ and $U(6)$ thus constructed, no cyclic unitals are known.

In Section 3, we also present a list of the "small" values of q corresponding to $p = 7, 9, 11$ for which the construction succeeds. Theorem 2 itself is proved in Section 4. Section 5 contains a number of concluding remarks.

The only facts about finite fields used in this paper are (i) cyclicity of their multiplicative groups and (ii) the quadratic reciprocity law; see [13], for instance. The higher reciprocity laws [9] have been used to facilitate the computation of explicit examples, but they are not necessary for the proofs. Results from algebraic number theory [1] are used only in the proof of Corollary 1 to Theorem 2.

2. Construction

Standing Notations. For any prime power s, F_s will denote the field with s elements, and F_s^* will be its multiplicative group. For positive integers m dividing $s-1$, $G_s(m)$ will denote the unique (cyclic) subgroup of F_s^* of order m. We also put $\overline{G_s}(m) = \{0\} \cup G_s(m)$.

Let p and q be *odd prime powers* such that $p-1$ *divides* $q-1$. Let

$f: G_q(p-1) \to G_p((p-1)/2)$ be an epimorphism (=onto group homomorphism). Our construction will depend on appropriate choice of f (when possible). Let t denote the largest divisor of $p-1$ which is relatively prime to $(q-1)/(p-1)$. Let us fix a generator γ of $G_q((q-1)/t)$.

Let us set $X = F_p \times F_q$, regarded as a ring with component-wise operations. For any subset A of X and for any x in X, $x+A$ (resp. xA) will denote the additive (resp. multiplicative) translate of A by x. Thus,

$$x+A=\{x+a: a\in A\},\quad xA=\{xa: a\in A\}.$$

By setting $f(0)=0$, we extend f to a function $f:\overline{G_q}(p-1)\to \bar{G}_p((p-1)/2)$. Let $A_0=\{(f(x),x): x\in \overline{G_q}(p-1)\}\subseteq X$ and put $A_j=(1,\gamma^j)A_0$, $0\leqslant j<(q-1)/(p-1)$. Finally let **B** consist of all the additive translates of the sets A_j, $0\leqslant j<(q-1)/(p-1)$, and of the set $A_\infty = F_p\times\{0\}$. Thus $(X,\mathbf{B})$ is a 1-design admitting the additive group $E(pq)$ of X as a point-regular automorphism group. It has $v=pq$ points and block size p, having a total of $pq(q-1)/(p-1)+q=v(v-1)/p(p-1)$ blocks. So, in order to conclude that $(X,\mathbf{B})$ is a regular $S(2,p,pq)$, it is enough to check that any two distinct points occur in at most one block. This will follow if the within-set differences of the "generating blocks" A_∞ and A_j, $0\leqslant j<(q-1)/(p-1)$, are all distinct. Trivially, the within-set differences of A_∞ are distinct among themselves and also distinct from those of the other A_j's.

For $y\in F_p$, let us put:

$$D_y=\{x_1-x_2: x_1,x_2\in G_q(p-1),\ x_1\neq x_2,\ f(x_1)-f(x_2)=y\}. \qquad (2.1)$$

Thus D_y consists of the second co-ordinates of those within-set differences of A_0 which have y in the first co-ordinate. In view of the above discussion, the system $(X,\mathbf{B})$ is a regular $S(2,p,pq)$ provided for each $y\in F_p$ the $p-1$ elements of D_y are distinct and the sets $\gamma^j D_y$, $0\leqslant j<(q-1)/(p-1)$, are pairwise disjoint.

Since the Kernel of f is $G_q(2)=\{1,-1\}$, we have $D_0=2G_q(p-1)$, so that the elements of D_0 are all distinct. Also, if for some j_1, j_2, $0\leqslant j_1$, $j_2<(q-1)/(p-1)$, $\gamma^{j_1}D_0$ and $\gamma^{j_2}D_0$ intersect then $\gamma^{j_1-j_2}\in G_q(p-1)\cap G_q((q-1)/t)=G_q((p-1)/t)$ (since by the choice of t, the greatest common divisor of $p-1$ and $(q-1)/t$ is $(p-1)/t$) and hence (as the order of γ is $(q-1)/t$) $j_1=j_2\ (\mathrm{mod}(q-1)/(p-1))$ and, hence, $j_1=j_2$.

So the requirements on D_y are always fulfilled for $y=0$. Next let y be in F_p^*. If for some $x_1, x_2\in D_y$ we have $\gamma^{j_1}x_1=\gamma^{j_2}x_2$, with $0\leqslant j_1$, $j_2<(q-1)/(p-1)$, then x_1, x_2 belong to the same coset of $G_q((q-1)/t)$. In order to conclude as before that $j_1=j_2$, we require x_1 and x_2 to belong to the same coset of $G_q((p-1)/t)$.

Let $y_1, y_2\in F_p^*$ belong to the same coset of $G_p((p-1)/2)$, say $y_2=yy_1$ with $y\in G_p((p-1)/2)$. Choose $x\in G_q(p-1)$ such that $y=f(x)$. Then

$A_0=(y,x)A_0$, and hence $D_{y_2}=xD_{y_1}$. Hence if D_{y_1} satisfies our requirements then so does D_{y_2}. So it suffices to check the requirements on D_y for exactly two values of y representing the two cosets of $G_p((p-1)/2)$ in F_p^*, that is, for one nonzero square and one nonsquare. If further $p\equiv 3 \pmod 4$ then, for any y in F_p^*, y and $-y$ represent these two cosets. Since clearly $D_{-y}=-D_y$, in this case it suffices to check the conditions for a single value of y.

Thus we have proved:

THEOREM 1. *Let p and q be odd prime powers such that $p-1$ divides $q-1$. In case $p\equiv 1 \pmod 4$ fix a non-square y_0 in F_p. Suppose there is an epimorphism $f\colon G_q(p-1)\to G_p((p-1)/2)$ for which D_y (as defined in (2.1)) satisfies the following two conditions for $y=1$ when $p\equiv 3 \pmod 4$ and for $y=1$, y_0 when $p\equiv 1 \pmod 4$:*

(a) *There are $p-1$ distinct elements in D_y, and*

(b) *whenever two elements of D_y belong to the same coset of $G_q((q-1)/t)$, they actually belong to the same coset of $G_q((p-1)/t)$.*

Then the above construction yields an $S(2, p, pq)$ on which $E(pq)$ acts as a point-regular automorphism group. In particular, if p, q are distinct primes, then the design is cyclic.

(Recall that here t is the largest divisor of $p-1$ which is relatively prime to $(q-1)/(p-1)$.)

Remarks. (1) Isomorphism. Clearly the success of the construction does not depend on the choice of y. If $t=p-1$ or $=(p-1)/2$, then different choices of y (with the same f) yield isomorphic designs. We know of no instance where the construction yields non-isomorphism designs with the same parameter.

(2) Automorphism. It is clear from the construction that as x ranges over $G_q(p-1)$, multiplications by $(f(x),x)$ constitute a cyclic automorphism group of order $p-1$ of the design. This group does not commute with the point-regular automorphism group $E(pq)$. Thus the full automorphism groups of the designs obtained are always nonabelian. If further $t=p-1$ or $t=(p-1)/2$, multiplication by $(1,y)$ generates a cyclic automorphism group of order $(q-1)/t$.

3. EXPLICIT CONDITIONS FOR $p\leqslant 11$

Our main result is:

THEOREM 2. *Let p and q be odd prime powers with $p\leqslant 11$. Then an $S(2, p, pq)$ admitting $E(pq)$ as a point-regular automorphism group exists in the following cases:*

(a) $p=3$ *and* $q\equiv 1 \pmod 2$,

(b) $p=5$ *and* $q\equiv 1 \pmod 4$,

(c) $p=7$, $q\equiv 7$ *or* $13 \pmod{18}$ *and* 3 *is not a cube in* F_q,

(d) $p=9$, $q\equiv 9 \pmod{16}$, *and* $\sqrt{2}$ *is a square but* $\sqrt{2}+1$ *is a nonsquare in* F_q, *and*

(e) $p=11$, $q\equiv 1 \pmod{10}$, $q\not\equiv 1 \pmod{50}$, *and there is a primitive fifth root of unity, say* w, *in* F_q *such that* w^2+w *and* w^4+w+3 *are both fifth powers in* F_q.

Remarks. Note that in (d) above, since $q\equiv 1 \pmod 8$, 2 is a square in F_q; $\sqrt{2}$ denotes either of the two square roots of 2. Clearly the validity of the hypothesis does not depend on the choice of this square root. In (a) above, since $q\equiv 1 \pmod 5$, there are four primitive fifth roots of unity in F_q; it can be shown that at most one of them satisfies the hypothesis.

Examples. The smallest pairs (p, q) (excepting $q=p^e$, in which case the construction always works, see (7) of Section 5), with $p=7, 9, 11$ for which Theorem 2 yields regular $S(2, p, pq)$, are the following:

(a) When $p=7$, $q=13$, 31, 43, 79, 97, 139, 157, 169, 211, 223, 229, 241, 277.

(b) When $p=9$, $q=73$, 89, 121, 233, 281, 361, 601, 617, 937, 1033, 1049, 1097, 1193.

(c) When $p=11$, $q=331$, 541, 571, 911, 941, 1231, 1481, 1621, 1721, 1741, 2161, 2281, 2371, 3011, 3361, 3391, 3821, 4231, 4931.

The corresponding values of the primitive fifth root w in F_q (satisfying the hypothesis of Theorem 2(e)) are:

$w=124$, 124, 481, 361, 349, 771, 1383, 231, 869, 195, 1618, 633, 1554, 817, 200, 3131, 3542, 136, 3375.

In Section 4 we shall prove Theorem 2 as a consequence of Theorem 1. Indeed, when $p\leqslant 11$ and $q\neq p^e$ for $e\geqslant 1$, the conditions of Theorem 2 are necessary as well as sufficient for Theorem 1 to apply. (For $q=p^e$, see (7) of the concluding section.) For now, we prove two corollaries of Theorem 2.

Corollary 1. *For each* $p=3, 5, 7$, *there are infinitely many primes* q *for which a cyclic* $S(2, p, pq)$ *exists.*

Proof. For $p=3$ or 5, this is immediate from Dirichlet's theorem on primes in arithmetic progressions (see [9]) and Theorem 2 (a), (b) (also see [3, 5, 11]). For $p=7$, it is immediate from Theorem 2 (c) and the following:

LEMMA. *There are infinitely many primes p such that $p \equiv 7$ or 13 (mod 18) and 3 is not a cube modulo p.*

Proof. Let K be the extension field of rationals by the three cube roots of 3. Suppose the lemma is false. Then, arguing as in the proof of Lemma 4 in [1], we see that for all sufficiently large primes $p \equiv 7$ or 13 (mod 18), there are exactly m prime ideals P in K with norm p, where m is the degree of this extension. Hence,

$$\sum N(P)^{-s} \geqslant m \cdot \sum p^{-s} \tag{3.1}$$

when the left-hand sum is over all prime ideals P of K. $N(P)$ denoting the norm over rationals of P, and the right-hand sum is over all sufficiently large rational primes $p \equiv 7$ or 13 (mod 18), $s > 1$. Now, as $s \to 1+$, the left-hand side of (3.1) is asymptotically $-\log(s-1)$ while the right-hand side is $-2m/\varphi(18)\log(s-1) = -m/3\log(s-1)$. Hence $m \leqslant 3$. But this is absurd, since clearly $m = 6$.

COROLLARY 2. *For each odd prime power $p \leqslant 11$ there are infinitely many prime powers q with $(p, q) = 1$ for which regular $S(2, p, pq)$ exist.*

Proof. Here, as usual, $(\cdot, \cdot)$ denotes greatest common divisor. Note that, since the desarguesian euclidean spaces $S(2, p, p^e)$ are regular, the corollary would be trivial without the restriction $(p, q) = 1$. For $p = 3, 5, 7$ the result is contained in Corollary 1. So we have to prove it for $p = 9, 11$. When $p = 11$, if $q = q_0$ is prime to 11 and satisfies the hypothesis of Theorem 2(e), then so does $q = q_0^e$ for $e \geqslant 1$ and $e \not\equiv 0$ (mod 5). Finally, if r is a prime power such that $(r, 9) = 1$ and $r \equiv 3$ (mod 8) then $q = r^2$ satisfies the hypotheses of Theorem 2(d). (In this case the elements of F_q may be uniquely written as $a + b\sqrt{2}$ with a, b in F_r. It can be shown that $a + b\sqrt{2}$ is a square in F_q if and only if $a^2 - 2b^2$ is a square in F_r. Hence the claim.)

4. PROOF OF THEOREM 2

We prove Theorem 2 by showing that under its hypotheses, there is a choice of the epimorphism f satisfying the hypotheses of Theorem 1. We continue to use the notation of Section 2. Also we put $n = (q-1)/(p-1)$.

Proof of Theorem 2(c). Choose the epimorphism $f\colon G_q(6) \to G_7(3)$ given by $f(-w) = 2$, where w is the primitive cube root of unity in F_q determined as follows. Since 3 is not a cube in F_q, nor is -3. Hence $(-3)^{\pm n}$ is a primitive cube root of unity in F_q (since $q \equiv 1$ (mod 3), -3 is a square in

F_q. Hence $(-3)^{\pm 3n} = (-3)^{(q-1)/2} = 1$. But $(-3)^{\pm n} \neq 1$, since -3 is not a cube). Of these two primitive cube roots of unity, determine w by:

$$w = (-3)^n \qquad \text{if} \quad n \equiv 1 \pmod 3$$

and

$$w = (-3)^{-n} \qquad \text{if} \quad n \equiv 2 \pmod 3).$$

(By our hypothesis on q, $n \not\equiv 0 \pmod 3$).)

With f thus chosen, we have $D_1 = \{\pm 1, \pm 1 \pm w\}$. Clearly D_1 satisfies condition (a) of Theorem 1 provided $w \neq \pm 2$. But -2 is not a cube root of unity in F_q since $q \not\equiv 0 \pmod 3$. Also, 2 is a cube root of unity only if $q = 7^e$, $e \geqslant 1$, but in this case our choice of w simplifies to $w = -3 \neq 2$.

Note that in the present case $t = 3$ or 6. In either case, D_1 satisfies condition (b) of Theorem 1 provided $(1 \pm w)^{2n} \neq 1$ and $(1 + w)^{2n} \neq (1 - w)^{2n}$. Using $w^2 + w + 1 = 0$, we have $1 + w = -w^2$ and $(1 - w)^2 = -3w$. Thus $(1 + w)^{2n} \neq 1$ since $n \not\equiv 0 \pmod 3$ and $(1 - w)^{2n} \neq 1$ since $w^n \neq (-3)^{-n}$ by our choice of w. Finally, the requirement $(1 + w)^{2n} \neq (1 - w)^{2n}$ simplifies to $(-3)^n \neq 1$ which we have, since 3 is not a cube in F_q. Since $p = 7 \equiv 3 \pmod 4$, this completes the proof.

Proof of Theorem 2(d). Here $p = 9$. We claim that under our hypothesis on q, any epimorphism $f: G_q(8) \to G_9(4)$ satisfies the requirements. Let β be any primitive eighth root of unity in F_q and put $\alpha = f(\beta)$. Thus α is a primitive fourth root of unity in F_9. Then $1 + \alpha$ is a nonsquare in F_9, and we have

$$D_1 = \{\pm 1, \pm \beta^2, \pm 1 \pm \beta^2\}, \qquad D_{1+\alpha} = \{\pm \beta \pm \beta^2, \pm 1 \pm \beta^3\}.$$

It suffices to show that both D_1 and $D_{1+\alpha}$ satisfy conditions (a) and (b) of Theorem 1.

Clearly $D_{1+\alpha}$ satisfies condition (a). Also D_1 fails to satisfy condition (a) only if one of ± 2, $\pm \frac{1}{2}$ is a primitive fourth root of unity in F_q, which happens only if q is a power of 5. But if $q \equiv 9 \pmod{16}$ and q is a power of 5 then $q = 5^{2e}$ with e odd. But $\sqrt{2}$ is a nonsquare in F_{25} and hence also in the field of order 5^{2e} for all odd e. Thus under our hypotheses on q, q cannot be a power of 5. So D_1 satisfies condition (a).

Since $q \equiv 9 \pmod{16}$, we have $t = 8$. Hence D_x satisfies condition (b) provided the nth powers of distinct elements of D_x are distinct. Using $\beta^3 = -\beta^{-1}$ and $\beta^2 + 1 = \sqrt{2}\,\beta$ we find that D_1 and $D_{1+\alpha}$ satisfy condition (b) provided $(\sqrt{2})^{(q-1)/2} \neq -1$ and $(\sqrt{2} + 1)^{(q-1)/2} \neq +1$, respectively. But these hold since $\sqrt{2}$ is a square and $\sqrt{2} + 1$ is a nonsquare in F_q.

Proof of Theorem 2(e). Here $p = 11$. Choose the epimorphism $f: G_q(10) \to G_{11}(5)$ given by $f(-w) = -2$, where w is the (unique) primitive fifth root of unity in F_q satisfying the hypothesis of the theorem. In this case,

$$D_1 = \{\pm 1, \pm w^2 \pm w^3, \pm w^2 \pm w^4\}.$$

Any two elements of D_1 are of the form $p_1(w)$, $p_2(w)$, where p_1, p_2 are polynomials with integer coefficients. Let $p(x) = \sum_{k=0}^{4} x^k$ be the minimal polynomial of w. We use the euclidean algorithm to compute the greatest common divisor p_0 of p and $p_1 - p_2$ (regarded as polynomials over the ring of rational integers). In order to prove that $p_1(w) \neq p_2(w)$, it suffices to check that $p_0(w) \neq 0$. This can be done for each pair of distinct elements of D_1, proving that D_1 satisfies condition (a) of Theorem 1, provided (i) if q is a power of 11 then $w = 3$ and (ii) if q is a power of 31 then $w \neq 2$. But (i) and (ii) hold because of the choice of w.

Because of the congruence conditions on q, we have $t = 5$ or 10. Thus, to prove that D_1 satisfies condition (b), we have to verify that the $(2n)$th powers of distinct elements of D_1 are distinct, except when these two elements are negatives of each other.

Dividing the identity $\sum_{k=0}^{4} w^k = 0$ by w^2, we see that there is a square root $\sqrt{5}$ of 5 in F_q such that

$$w + w^{-1} = (\sqrt{5} - 1)/2. \tag{4.1}$$

Let us put $u = (\sqrt{5} + 1)/2$. By our assumption $u\sqrt{5} = w^4 + w + 3$ (and hence also $-u\sqrt{5}$) is a fifth power. Also, $-u\sqrt{5} = (2w - u^{-1})^2$. Hence $-u\sqrt{5}$ is a tenth power, so that $(-u\sqrt{5})^n = 1$. That is,

$$(\sqrt{5})^n = (-u)^{9n}. \tag{4.2}$$

Since $uw^{-1} = w(1 + w)$ is a fifth power, so is $u^6 w^{-1}$. Also w is a square (since $q \equiv 1 \pmod{10}$). Hence $u^6 w^{-1}$ is a tenth power, so that $(u^6 w^{-1})^n = 1$. That is,

$$w^n = u^{6n}. \tag{4.3}$$

Using (4.1), (4.2), (4.3), the $(2n)$th powers of the ratios of elements of D_1 can be written as powers of w. Since $n \not\equiv 0 \pmod 5$, it can hence be seen that D_1 satisfies condition (b). Since $p = 11 \equiv 3 \pmod 4$, this completes the proof.

When $p = 3$, 5 and $p - 1$ divides $q - 1$, there is a unique epimorphism f from $G_q(p-1)$ to $G_p(p - 1/2)$. We omit the trivial verification that this satisfies the conditions.

5. Concluding Remarks

(1) Use was made of the Royal Society Math Table 9 [16] to compute the examples in Section 3. Further, a computer was resorted to in order to obtain the examples with $p = 11$. Note that whenever $p \neq q$ are both primes the construction yields cyclic designs. Thus the examples include several (apparently new) cyclic designs with block size 7 and 11.

(2) During computation of the examples it was noticed that within the range of our calculations, whenever $q \equiv 9 \pmod{16}$ is a prime power such that 2 is a fourth power in F_q, we also have that $\sqrt{2}+1$ is a nonsquare. Thus the last condition in Theorem 2(d) appears to be superfluous, but we are unable to prove it.

(3) In [11] it was shown that cyclic Steiner 2-design with block size 3 exists for all $v \equiv 1$ or $3 \pmod 6$ except for $v = 9$. In Theorem 2.2 of [5] a construction of cyclic $S(2, 5, 5q)$ is presented whenever $q \equiv 1 \pmod 4$ is a prime satisfying certain conditions. The congruence condition on the primitive root of F_q imposed in this Theorem is vacuously fulfilled for $q \neq 5$ in view of the Chinese Remainder Theorem (see [9]). Also, the second requirement in this theorem may be rephrased as asking for a nonsquare x in F_q such that $(x+1)(x-1)^{-1}$ is also a nonsquare. Since the map $x \to (x+1)(x-1)^{-1}$ is a bijection of $F_q \backslash 1$ onto itself taking the two squares 0 and -1 into squares, it is clear that it must take some nonsquare into a nonsquare. Thus Theorem 2.2 in [5] yields cyclic $S(2, 5, 5q)$ for each prime $q \equiv 1 \pmod 4$, $q \neq 5$. Thus there is little that is new in parts (a) and (b) of our Theorem 2.

(4) As noted in the Introduction, the most notable success of our construction is the unital $U(6)$. It may be recalled that there are two classical series of unitals. The one due to Bose [4] exists for all prime-power parameters s and admits the unitary group $U_3(s)$ as an automorphism group acting doubly transitively on points. The other series due to Luneburg [10] exists for $s = 3^e$, e odd, and admits the Ree group as a doubly transitive automorphism group. Curiously, none of these classical unitals are cyclic. So, in a sense, the unital $U(6)$ (and the $U(4)$ arising from $(p, q) = (5, 13)$ which is also implicit in [5]) is better than the classical ones! Other constructions of unitals (all with prime-power parameters) arise from variations of Bose's construction (see [12] and the references there), but none of these appear to yield cyclic unitals.

(5) Recall that an inversive plane of order s is an $S(3, s+1, s^2+1)$. It is instructive to compare unitals with inversive planes. There are also two classical series of inversive planes, admitting doubly transitive automorphism groups. The first exists for all prime-power orders s, while the second for $s = 2^e$, e odd. The first arises from an orthogonal polarity in projective 3-space (exactly as the first series of unitals arises from a unitary

polarity in projective 2-spaces), while the second series arises from the internal structure of the twisted Lie-type simple group of Suzuki or equivalently from polarities of certain classical generalized 4-gons (while the second series of unitals comes from the internal structure of the twisted Lie-type groups of Ree or, equivalently, from polarities of certain classical generalized 6-gons).

Now in [6] Dembowski proved that if an inversive plane has even order s then s must be a power of two. In [2] it was shown that an even order inversive plane having a point-transitive automorphism group is necessarily classical. The cyclic unital $U(6)$ shows that the natural analogues of both these results are false for unitals.

(6) Another interesting series of Steiner 2-designs is with $v = k(2k-1)$ (For the significance of this series see [15]). Designs in this series are known for $k = 2^e$, $e \geqslant 1$, and $k = 3, 5, 7$. The cases $(p, q) = (3, 5)$, $(5, 9)$, and $(7, 13)$ yield examples with $k = 3, 5, 7$. Indeed, the designs thus obtained are isomorphic to the corresponding ones in Hall's table [7]. All the same, it is perhaps interesting to find that all these sporadic examples can be obtained by a common construction. A computer search is under way to see if the construction yields further examples in this series.

(7) When $q = p^\alpha$, $\alpha \geqslant 1$, and p is a prime power—so that $F_p \subseteq F_q$—the function $f\colon G_q(p-1) \to G_p((p-1)/2)$ given by $f(x) = x^2$ always satisfies the requirements of Theorem 1. The design obtained has the same parameters as (and at least in small cases is isomorphic to) the point-line design of $EG(\alpha+1, p)$. If, further, $p = 3^{2e+1}$, $e \geqslant 1$, then $f(x) = x^4$ also satisfies these requirements. We do not know if the designs obtained are new. In particular, these include (when $p = q = 3^{2e+1}$) affine planes of order 3^{2e+1}, $e \geqslant 1$, which may be new.

Post-script. While this paper was in preparation, we learned, by courtesy of R. C. Mullin, that R. A. Mathon has in a forthcoming paper used a similar difference family construction to obtain a number of cyclic Steiner 2-designs with block sizes 7, 11, and 13. While some of the results in this paper are thus anticipated by Mathon, it should still be of interest because of its theoretical results, in general, and for its proof of infinitude of cyclic designs with block size seven, in particular.

References

1. N. C. Ankeny and C. A. Rogers, A conjecture of Chowla, *Ann. Math.* **53** (1951), 541–550.
2. B. Bagchi and N. S. N. Sastry, Even order inversive planes, generalised quadrangles and codes, *Geom. Dedicata* **22** (1987), 137–147.
3. R. C. Bose, On the construction of balanced incomplete block designs, *Ann. Eugenics* **9** (1939), 353–399.

4. R. C. Bose, On the application of finite projective geometry for deriving a certain series of Kirkman arrangements, *Bull. Calcutta Math. Soc.*, The Golden Jubilee volume (1963), 341–354.
5. M. J. Colbourn and R. A. Mathon, On cyclic Steiner 2-designs, *in* "Topics on Steiner Systems" (C. C. Lindner and A. Rosa, Eds.), Annals of Discrete Math. Vol. 7, North-Holland, Amsterdam/New York/Oxford, 1980.
6. P. Dembowski, Mobiusebenen gerader ordnung, *Math. Ann.* **157** (1964), 179–205.
7. M. Hall, Jr., "Combinatorial Theory," Wiley, New York/London/Sydney/Toronto, 1967.
8. D. R. Hughes and F. C. Piper, "Design Theory," Cambridge Univ. Press, Cambridge, 1985.
9. K. Ireland and M. Rosen, "A Classical Introduction to Modern Number Theory," Graduate Texts in Math. Vol. 84, Springer-Verlag, Berlin/Heidelberg/New York, 1982.
10. H. Luneburg, Some remarks concerning the Ree group of type (G_2), *J. Algebra* **3** (1966), 256–259.
11. R. Peltesohn, Eine Losung der beiden Heffterschen Differenzeprobleme, *Compositio Math.* **6** (1939), 251–257.
12. F. Piper, Unitary block designs, *in* "Graph Theory and Combinatorics" (R. J. Wilson, Ed.), Pitman, San Francisco/London/Melbourne, 1979.
13. J. P. Serre, "A course in Arithmetic," Graduate Texts in Math. Vol. 7, Springer-Verlag, Berlin/Heidelberg/New York, 1973.
14. J. Singer, A theorem in finite projective geometry and some application to number theory, *Trans. Amer. Math. Soc.* **43** (1938), 377–385.
15. W. D. Wallis, My favourite family of block designs, *in* "Congressus Numerantium Vol. 8," pp. 91–107, Utilitas Math., Winipeg, 1973.
16. A. E. Western and J. C. P. Miller, "Indices and Primitive Roots," Royal Society Math. Tables Vol. 9, Cambridge Univ. Press, Cambridge, 1968.