ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 25, Number 4, Fall 1995

BIQUADRATIC RESIDUES AND SELF-ORTHOGONAL 2-SEQUENCINGS

STEPHEN D. COHEN AND PHILIP A. LEONARD

1. Introduction. Let $2K_n$ denote the complete multigraph on n vertices in which each edge has multiplicity two. If $2K_n$ can be partitioned into Hamiltonian paths such that any two distinct paths have exactly one edge in common, write $2K_n \to P_n$. The object of this paper is to examine a particular class of such partitions introduced in [**2**], to which the reader is referred for wider discussion of this and related graph decomposition problems. In particular, attention is paid to constructions of these partitions that are based on self-orthogonal 2-sequencings of the additive groups of finite fields.

Definition 1. Suppose H is a finite group of order n with identity element e. A 2-*sequencing* (or *terrace*) of H is an ordering $e, c_2, \dots, c_n$ of elements of H (not necessarily distinct) such that

(i) the partial products $e, ec_2, ec_2c_3, \dots, ec_2\cdots e_n = e, d_2, \dots, d_n$ are distinct (and hence all of H),

(ii) if $h \neq h^{-1}$, then $|\{i : 2 \leq i \leq n \text{ and } (c_i = h \text{ or } c_i = h^{-1})\}| = 2$,

(iii) if $h = h^{-1}$, then $|\{i : 1 \leq i \leq n \text{ and } c_i = h\}| = 1$.

As all groups considered in this paper are abelian, additive notation is used. An example taken from [**2**] on $\mathbf{Z}_{19}$ is useful as an illustration.

Consider, on $\mathbf{Z}_{19}$, the 2-sequencing S, and associated partial sum sequence P, as follows:

$$\begin{aligned} S:&\quad 0,2,5,6,4,1,7,-3,-2,9,6,-8,1,5,-3,4,9,7,-8\\ P:&\quad 0,2,7,13,17,18,6,3,1,10,16,8,9,14,11,15,5,12,4 \end{aligned}$$

The sequence P can be thought of as a Hamiltonian path through the vertices of K_{19}, the complete graph with vertices labelled by elements

Received by the editors on September 8, 1993.
Sabbatical support for the second author provided by the Departments of Mathematics at Arizona State University and at the University of Glasgow is gratefully acknowledged.

of $\mathbf{Z}_{19}$. In the sequel, the same notation P will be used to represent both a partial sum sequence associated with a 2-sequencing of the additive group of a finite field $\mathbf{F}_q$ and the corresponding Hamiltonian path through K_q. (In most places only the partial sum sequence P, and not the underlying 2-sequencing S, appears in our discussion).

Let S be a 2-sequencing of H, taken henceforth to be an additive abelian group of odd order, with h representing an element different from the identity element of H.

The edge $\{d_{i-1}, d_i\}$ in P is associated with the element c_i in S by $d_{i-1} + c_i = d_i$, $2 \leq i \leq n$. Each 2-set $\{h, -h\}$ will be represented *twice* among the c_i, the differences of edge pairs from P. If these two pairs are $\{d_{i-1}, d_i\}$ and $\{d_{j-1}, d_j\}$, these pairs are said to *have the same length.* There is then an element z_h such that $z_h + \{d_{i-1}, d_i\} = \{d_{j-1}, d_j\}$ (and thus $-z_h + \{d_{j-1}, d_j\} = \{d_{i-1}, d_i\}$); a representative of $\{z_h, -z_h\}$ is called a *distance*, and a selection of one distance for each h provides a *set of distances* for the 2-sequencing S.

In the illustration, the pairs $\{7, 13\}$ and $\{10, 16\}$ have length 6, and the distance can be taken as $z_6 = 3$.

Definition 2. Let S be a 2-sequencing of the abelian group H of odd order.

(i) S is said to be *self-orthogonal* if and only if every set of distances of S is a transversal for $\{\{h, -h\} : h \neq 0\}$.

(ii) If S is self-orthogonal, then S is said to *admit a 2-coloring* if and only if, whenever two edges in P have the same length, they are separated by an odd number of edges of P.

The importance of the first of these concepts is due to a result implicit in [**7**], a proof of which is outlined in [**8**], namely,

Theorem 1. *If H is a finite Abelian group of order n with self-orthogonal 2-sequencing S, then $2K_n \to P_n$.*

In fact, the collection $\{P + h : h \in H\}$ consists of n Hamiltonian paths, any two of which have exactly one edge in common.

The importance of the second concept in Definition 2 is that a product theorem in [**8**] requires partitions that admit a 2-coloring. The example in $\mathbf{Z}_{19}$ is self-orthogonal; however, it does not admit a 2-coloring.

In [**2**], constructions of self-orthogonal 2-sequencings related to finite fields were employed to give many new values of n with $2K_n \to P_n$. The constructions were shown to be successful for infinitely many values of n. In some cases the solutions admit 2-colorings. The methods employed involve *starters* and other tools developed in the study of Room squares and Howell designs. The reader unfamiliar with these may consult references [**6, 12**]; additional terms appearing in the statements of the results mentioned below are defined in [**2**]. The principal results (Theorems 17 and 19) obtained there are as follows:

Theorem 2. *Suppose m and r are positive integers, r odd, such that $(m,r) \notin \{(1,1),(2,1)\}$. There is a positive integer $B_1(m,r)$ such that if $p \geq 5$ is a prime, $q = p^n = 2^m rs + 1 > B_1(m,r)$ and*

(i) $(r,s) = 1$,

(ii) 2 *and* 3 *are not* $(2^m r)$*-th power residues in* $\mathbf{F}_q$,

(iii) *at most one of* $2,3$ *is a* $(2^{m-1}r)$*-th power residue in* $\mathbf{F}_q$,

then the additive group of $\mathbf{F}_q$ has a self-orthogonal 2-sequencing.

Theorem 3. *Suppose $m \geq 2$ and r (odd) are positive integers. There is a positive integer $B_2(m,r)$ such that if $p \geq 5$ is a prime, $q = p^n = 2^m rs + 1 > B_2(m,r)$, $(r,s) = 1$ and $1,2,3,4$ are in different cosets of the subgroup of $(2^m r)$-th power residues in $\mathbf{F}_q^*$, then the additive group of $\mathbf{F}_q$ has a self-orthogonal 2-sequencing that admits a 2-coloring.*

The case $(m,r) = (2,1)$, excluded from Theorem 2, was studied independently. Results valid for sufficiently large $p^n \equiv 5 \pmod 8$, were combined with computations for primes $p \equiv 5 \pmod 8$ not exceeding 300. It was evident that the methods of construction were much better than the theoretical bounds obtained. The present paper is devoted to this "4-coset" case. We prove the following result

Theorem 4. *Let p be a prime, and suppose $q = p^n \equiv 5 \pmod 8$.*

If 3 *is not a fourth power in* $\mathbf{F}_q$*, then the additive group of* $\mathbf{F}_q$ *has a self-orthogonal* 2*-sequencing.*

Theorem 4 provides a complement to [**2**], and a tribute to the effectiveness of constructions developed by Bruce Anderson, to whose memory this paper is dedicated.

2. The case of four cosets. Suppose p is prime and $q = p^n = 4s+1$ with s odd, so that $p \equiv 5 \pmod 8$ and n is odd. For a primitive element x of the finite field $\mathbf{F}_q$, let

$$C(i) = \{x^{4t+i} : 0 \le t < s\}, \qquad 0 \le i \le 3,$$

so that $C(i)$ are the cosets of the subgroup $C(0)$ of $\mathbf{F}_q^*$.

As 2 is a nonsquare in $\mathbf{F}_q$ under the conditions imposed, it is possible, interchanging x^{-1} for x if necessary, to choose a primitive element x for which $2 \in C(1)$. This will be assumed in the sequel. The 1-2-3-4 construction of [**2**] does not apply if $3 \in C(0)$. In what follows we treat the three remaining possibilities completely. The exposition will be particular to the 4-coset case, but expansive enough to suit readers not familiar with the general construction.

It will be helpful to have a numerical example in mind. When $q = 37$, $x = 2$ is a primitive element, and $2^{26} \equiv 3 \pmod{37}$ so that $3 \in C(2)$. Consider the following array, in which indications of the construction are superimposed on a Hamiltonian cycle through a graph labelled so that $[i]$ represents the coset $C(i)$.

$$\begin{tikzcd}
 & xb \in C(3) & x \in C(1) & 3 \in C(2) & 1 \in C(0) \\
{[0]} \arrow[r, "a"] & {[3]} \arrow[r, "b^{-1}"] & {[1]} \arrow[r, "2"] & {[2]} \arrow[r, "3^{-1}"] & {[0]} \\
1 \in C(0) & a \in C(3) & 2 \in C(1) & 4 \in C(2) &
\end{tikzcd}$$

The construction relies on finding a and b such that the cosets of a and b are specified according to the Hamiltonian cycle, the cosets of $a-1$ and $b-1$ satisfy conditions needed for lengths (or “differences”) in the eventual path, and the cosets of $a-b$ and $1-ab$ satisfy conditions needed for “distances” in the eventual path. (The precise conditions are in Case 2 below). For this example, $a = 5$ and $b = 30$ yield “base pairs” for two starters U, with base pairs $\{1,3\}$ and $\{x, xb\} = \{2, 23\}$, and V, with base pairs $\{2,4\}$ and $\{1,a\} = \{1,5\}$, the 18 pairs in each starter being $\{ur, vr\}$ where $\{u, v\}$ is a base pair and $r \in C(0)$. This choice of a and b gives a Hamiltonian cycle because $\rho = a \cdot b^{-1} \cdot 2 \cdot 3^{-1}$ has order $9 = (37-1)/4$ in $\mathbf{F}_{37}^*$. The two starters U and V give a Hamiltonian cycle through $\mathbf{F}_{37}^*$, with $-$ representing an edge arising from a pair in U and $=$ representing an edge arising from a pair in V, namely,

$$\begin{array}{rcrcrcrcrcrcrcrcrcr}
1 & = & 5 & - & 31 & = & 25 & - & 33 & = & 17 & - & 24 & = & 11 & - & 16 & = & 6 \\
 & - & 15 & = & 30 & - & 10 & = & 13 & - & 14 & = & 28 & - & 34 & = & 22 & - & 18 \\
 & = & 36 & - & 12 & = & 23 & - & 2 & = & 4 & - & 26 & = & 19 & - & 29 & = & 21 \\
 & - & 7 & = & 35 & - & 32 & = & 27 & - & 9 & = & 8 & - & 20 & = & 3 & - & 1
\end{array}$$

(Passage from any element in $C(0)$ to the next-occurring one is effected by multiplication by $\rho = a \cdot b^{-1} \cdot 2 \cdot 3^{-1}$.) The pair $\{2, 4\}$ is replaced by $\{0, 2\}$ to make a path through $\mathbf{F}_{37}$; the *length*, and the *distance* from the pair $\{1, 3\}$ are unaltered by this replacement. This path, arising from a self-orthogonal 2-sequencing, gives a solution for $2K_{37} \to P_{37}$. This solution does not admit a 2-coloring, as two edges with the same length are always separated by an *even* number of edges. (This situation arises whenever the base pairs give starters; in case $3 \in C(3)$ the base pairs yield "supplementary half-starters," and the resulting solution to $2K_q \to P_q$ does admit a 2-coloring. See Case 3 below.)

Remark. It can be noted (see Table 2 in [**2**]) that for $q = 37$ exactly six pairs a, b meet the conditions needed to make starters appropriate for the construction, but that in three of these cases the associated element $\rho \in C(0)$ has order 3. Thus, in place of the Hamiltonian cycle shown above, the procedures of the 1-2-3-4 construction produce a decomposition of $\mathbf{F}_{37}^*$ into three disjoint 12-cycles.

The existence of solutions to $2K_q \to P_q$ (including those that admit 2-colorings) can be guaranteed by proving the feasibility of the following project from [**2**].

Case 1. If $3 \in C(1)$, the Hamiltonian cycle is $[0] - [1] - [2] - [3] - [0]$

i) Pick $a \in C(3)$ so that $a - 1 \in C(0) \cup C(2)$.

ii) Pick $b \in C(1)$ so that $b - 1 \in C(0) \cup C(2)$.

iii) This builds starters $U : \{1, 3\}, \{x^2, x^2 b\}$ and $V : \{2, 4\}, \{1, a\}$.

iv) Then pick the pairs (a,b) so that $a-b$, $1-ab \in C(1) \cup C(3)$.

v) Ensure that $\rho = 3 \cdot 2 \cdot b \cdot a^{-1} = 6ba^{-1}$ is a generator of $C(0)$.

Case 2. If $3 \in C(2)$, the Hamiltonian cycle is $[0]-[3]-[1]-[2]-[0]$.

i) Pick $a \in C(3)$ so that $a-1 \in C(0) \cup C(2)$.

ii) Pick $b \in C(2)$ so that $b-1 \in C(1) \cup C(3)$.

iii) This builds starters $U: \{1,3\}$, $\{x, xb\}$ and $V: \{2,4\}, \{1,a\}$.

iv) Then pick pairs (a,b) so that $a-b, 1-ab \in C(0) \cup C(2)$.

v) Ensure that $\rho = ab^{-1} \cdot 2 \cdot 3^{-1}$ is a generator of $C(0)$.

Case 3. If $3 \in C(3)$, the Hamiltonian cycle is $[0]-[3]-[1]-[2]-[0]$.

i) Pick $a \in C(2)$ so that $a-1 \in C(0) \cup C(2)$.

ii) Pick $b \in C(2)$ so that $b-1 \in C(1) \cup C(3)$.

iii) This builds half-starters $U: \{1,3\}, \{2,4\}$ and $V: \{1,a\}, \{x, xb\}$.

iv) Then pick pairs (a,b) so that $a-b, 1-ab \in C(0) \cup C(2)$.

v) Ensure that $\rho = 3b^{-1}2a^{-1} = 6b^{-1}a^{-1}$ is a generator of $C(0)$.

Examples for the three cases (all for primes p with primitive root $x=2$) are as follows:

Case 1.	$p = 317$;	$a = 78$,	$b = 2$,	$\rho = 244$
Case 2.	$p = 349$;	$a = 105$,	$b = 3$,	$\rho = 256$
	$p = 373$;	$a = 8$,	$b = 3$,	$\rho = 209$
	$p = 613$;	$a = 8$,	$b = 3$,	$\rho = 138$
Case 3.	$p = 389$;	$a = 46$,	$b = 4$,	$\rho = 55$

The proof of Theorem 4 depends on a detailed analysis of the character sums in the original paper. This is preceded by a careful balancing of coset membership conditions with order conditions, and depends on special features of the 4-coset case. The argument occupies the next three sections.

3. Guarantee of a generator of $C(0)$. Rather than first choosing a and b to meet specified coset conditions and then asking if the resulting

ρ is a generator of $C(0)$, we first seek an appropriate generator of the set $C(0)$ of biquadratic residues, stipulating as well that one condition on a and b also be satisfied. This balances conditions between the two parts of the argument and leads to more useful estimates.

The shape of ρ in the three cases suggests how to proceed. In cases 1 and 2 let $c = ab^{-1}$, and in case 3 let $c = ab$. The requirement that $\rho \in C(0)$, and coset membership conditions on a and b, lead to a coset membership condition on c in each case. The quadratic condition on $b-1$ leads to a quadratic condition on $a-c$. The conditions on $a-b$, $1-ab$ lead to a quadratic condition on a^2-c and to a quadratic condition on $c-1$. This last condition, and the requirement that ρ be a generator of $C(0)$, are treated together in the present section. In the next section, c is regarded as already selected, and the argument shows that a may be chosen so that all remaining conditions are satisfied. Explicit conditions for the three cases are not introduced until they are needed for the next section.

It is required, then, to choose an element c of $\mathbf{F}_q$ so that, for appropriate fixed elements e, δ_1, δ_2, it is the case that $\delta_1 ec$ lies in $C(0)$ and has (odd) order s, and $\delta_2(c-1) \in Q = C(0) \cup C(2)$. Let M denote the number of c's satisfying those conditions. Then, with η denoting a fixed fourth-power character, (specified, say, by $\eta(x) = i$), and λ the quadratic character, on $\mathbf{F}_q$, it follows (as in [**3**], for example) that

$$(3.1)\quad M = \frac{1}{2}\bigg[\frac{1}{4}\frac{\phi(s)}{s}q + \frac{1}{4}\frac{\phi(s)}{s}\sum_{c}\sum_{d|s}\frac{\mu(d)}{\phi(d)}\sum_{\chi}\chi(ec) \cdot \{1+\eta(\delta_1 ec)+\eta^2(\delta_1 ec)+\eta^3(\delta_1 ec)\}\cdot\{1+\lambda(\delta_2(c-1))\}\bigg].$$

Here the sum on χ is over all characters of order d, that on d over all divisors of s, and that on c over all elements of $\mathbf{F}_q$; μ and ϕ are the arithmetical functions of Möbius and Euler, respectively. Note that

$$1+\eta(w)+\eta^2(w)+\eta^3(w) = (1+\eta(w))(1+\lambda(w)) \quad \text{for all } w \text{ in } \mathbf{F}_q.$$

The principal term comes from taking $d = 1$. For $d > 1$, observe that the terms coming from choosing "1" in $\{1+\lambda(\sigma_2(c-1))\}$ are zero as (with $c' = \delta_1 ec$ summed over $\mathbf{F}_q$)

$$\sum_{c'}\chi(c')\eta^j(c') = 0 \quad \text{in all cases.}$$

Let $\omega(s)$ denote the number of distinct (odd) primes dividing s. In what remains there are two character sums of magnitude 1, namely, $\sum_c \chi_0(ec)\lambda(\delta_2(c-1))$ and $\sum_c \chi_0(ec)\lambda(\delta_1 e\delta_2 c(c-1))$, and $4\cdot 2^{\omega(s)}-2$ character sums that are essentially Jacobi sums, each of magnitude $\leq \sqrt{q}$. Therefore $M>0$ provided

$$q-1 > (4\cdot 2^{\omega(s)}-2)\sqrt{q}+2. \tag{3.2}$$

This last surely holds when $q>[4(2^{\omega(s)}-1/2)]^2$. If $\omega(s)\geq 4$, then $M>0$ whenever $q>3844$; on the other hand, $\omega(s)\geq 4$ implies $s=(q-1)/4\geq 3\cdot 5\cdot 7\cdot 11$, or $q\geq 4621$. Therefore $M>0$ whenever $\omega(s)\geq 4$. When $\omega(s)=1$ or $\omega(s)=2$, then the same argument gives $M>0$ whenever $q>36$ or $q>196$, respectively. Cases below these bounds are covered by the computations in [**2**]. It remains to consider cases in which $\omega(s)=3$. The inequality (3.2) is valid for $q>904$. The prime power values $q\equiv 5 \pmod 8$, $q\leq 904$, $\omega(s)=3$ are handled one by one.

The only integral values of q with odd $s=(q-1)/4$, $\omega(s)=3$, and $q\leq 904$ are $q=421$, 661 and 781. Of these $781=11\cdot 71$ is not prime, and $421=9\cdot 5^2+4\cdot 7^2$ so that $3\in C(0)$ and the value is not covered by the 4-coset case [**2**]. It remains to check $q=661$.

The value $q=661$ requires a simple sieve [**4**]. (For a more extensive treatment of the sieving process and its many applications, see [**5**].) For a divisor r of $s=(661-1)/4=3\cdot 5\cdot 11$, let $S(r)$ denote the set of c in $\mathbf{F}_q$ such that ec has order divisible by r, $\delta_1 ec\in C(0)$ and $\delta_2(c-1)\in Q$, and let $N(r)$ denote the cardinality of $S(r)$. In analogy with (3.1) we have

$$\begin{aligned} 8N(r) = \frac{\phi(r)}{r}q-1) + \frac{\phi(r)}{r}\sum_{d|u}\frac{\mu(d)}{\phi(d)}\sum_{\substack{\chi\\ \operatorname{ord}\chi=d}}\sum_{c\in\mathbf{F}_q}\chi(ec)\\ \cdot(1+\eta(\delta_1 ec))(1+\lambda(\delta_1 ec))\lambda(\sigma_2(c-1)). \end{aligned}\tag{3.3}$$

From $S((u,v))\supseteq S(u)\cup S(v)$ it follows that, for any u and v dividing s, $N([u,v])\geq N(u)+N(v)-N((u,v))$, where $[u,v]$ and (u,v) denote the least common multiple and greatest common divisor, respectively, of u and v. This inequality is useful with $u=15$, $v=11$. All four character sums (two with magnitude 1, as above, and two with magnitude $\sqrt{q}$) for $r=1=(15,11)$ also occur in $N(15)$, $N(11)$ and $N(1)$ with coefficients

8/15, 10/11 and 1, respectively. The remaining character sums all have magnitude $\sqrt{q}$. The sieve inequality thus implies

$$8N(165) \geq \left[\left(\frac{8}{15}+\frac{10}{11}-1\right)(q-1-2\sqrt{q}-2)\right]-\left[4\cdot\frac{8}{15}\cdot 3+4\cdot\frac{10}{11}\cdot 1\right]$$

so that (taking $q = 661$) $8N(165) \geq 10.3316\ldots$, implying $N(165) \geq 1$ as required. This completes the proof that a suitable generator of $C(0)$ may always be found.

4. The coset conditions on a. Suppose c has been chosen to satisfy the conditions of Section 3. In order to complete the construction of a self-orthogonal 2-sequencing it is necessary to choose a, with the coset of a and the quadratic character of $a-1$, $a-c$ and a^2-c assigned in advance. With δ, σ_1 and σ_2 to be specified according to the three cases under consideration, let N_1 denote the number of elements a of $\mathbf{F}_q$ satisfying

$$\begin{aligned}
\delta a &\in C(0), && \text{i.e., } \frac{1}{4}\{1+\eta(\delta a)+\eta^2(\delta a)+\eta^3(\delta a)\}=1,\\
\lambda(a-c) &= \sigma_1, && \text{i.e., } \frac{1}{2}\{1+\sigma_1\lambda(a-c)\}=1,\\
\lambda(a^2-c) &= \sigma_2, && \text{i.e., } \frac{1}{2}\{1+\sigma_2\lambda(a^2-c)\}=1,\\
\lambda(a-1) &= 1, && \text{i.e., } \frac{1}{2}\{1+\lambda(a-1)\}=1.
\end{aligned} \tag{4.1}$$

For each $a \in \mathbf{F}_q$, let ε_a denote the error from using the product of the four "character quantities" above to count a precisely when it satisfies the required conditions. In this way, N_1 is represented in a standard manner by

$$N_1 = \frac{1}{32}\sum_{a\in\mathbf{F}_q}\{(\text{character quantity})+\varepsilon_1(a)\}, \tag{4.2}$$

that is, (ignoring the $\varepsilon_1(a)$ for the moment) as a sum of 32 character sums. In order to show the construction can be completed, it is enough to show that $N_1 > 0$. This will be done by estimating the character sums that appear in the expansion of N_1.

The number of cases to be settled by direct calculation can be made quite small if the interplay between a and c/a is taken into account by way of the following:

$$\begin{aligned} \eta(c/a) &= \eta(c)\eta^3(a), \\ \lambda(c/a-1) &= \lambda(a)\lambda(a-c), \\ \lambda(c/a-c) &= \lambda(ac)\lambda(a-1), \\ \lambda((c/a)^2-c) &= \lambda(c)\lambda(a^2-c). \end{aligned} \tag{4.3}$$

As a runs through the nonzero elements of $\mathbf{F}_q$, so does c/a. The conditions on a give rise to corresponding conditions on c/a. With ν, τ_1 and τ_2 to be specified later, let N_2 denote the number of elements x $(= c/a)$ of $\mathbf{F}_q$ satisfying

$$\begin{aligned} \nu x \in C(0), \qquad \lambda(x-c) = \tau_1, \\ \lambda(x^2-c) = \tau_2, \qquad \lambda(x-1) = -1, \end{aligned} \tag{4.4}$$

the last because $\lambda(a)\lambda(a-c) = -1$ in each of the three cases under consideration. Incorporating these conditions and counting x $(= c/a)$ instead of a, a second way of counting solutions is realized, namely,

$$N_2 = \frac{1}{32}\sum_{x\in\mathbf{F}_q}\{(\text{character quantity}) + \varepsilon_2(x)\}. \tag{4.5}$$

Of course $N_2 = N_1$, and we distinguish between them only to note connections between character sums that occur in the two expansions.

It is easy to verify that the quantities introduced in (1) and (3) above are as indicated in the following table:

TABLE 1.

	δ	ν	σ_1	σ_2	τ_1	τ_2
Case 1	2	2	$+1$	-1	-1	-1
Case 2	2	4	$+1$	$+1$	$+1$	-1
Case 3	4	4	-1	$+1$	$+1$	$+1$

Now also using x in place of a in N_1, form the expression for $(N_1+N_2)/2$. This contains 32 character sums; in the following table we give for each sum the general term, an estimate and/or description of the sum, and the coefficient in each of the three cases. Note that values of the quartic and quadratic characters of δ and ν are incorporated into the coefficients.

TABLE 2.

						Estimate/	Coefficient (by Case)		
Sum	i_1	i_2	i_3	i_4	Term	Descr.	1	2	3
1	0	0	0	0	1	q princ.	1	1	1
2	0	0	0	1	$\lambda(x^2-c)$	triv.	-1	0	1
3	0	0	1	0	$\lambda(x-c)$	triv.	0	1	0
4	0	0	1	1	$\lambda((x-c)(x^2-c))$	$2\sqrt{q}$	0	0	0
5	0	1	0	0	$\lambda(x-1)$	triv.	0	0	0
6	0	1	0	1	$\lambda((x-1)(x^2-c))$	$2\sqrt{q}$	0	1	0
7	0	1	1	0	$\lambda((x-1)(x-c))$	triv.	1	0	-1
8	0	1	1	1	$\lambda((x-1)(x-c)(x^2-c))$	$2\sqrt{q}$ J_2	-1	1	-1
9	1	0	0	0	$\eta(x)$	triv.	i	$(-1+i)/2$	-1
10	1	0	0	1	$\eta(x)\lambda(x^2-c)$	$2\sqrt{q}$	$-i$	$(1+i)/2$	-1
11	1	0	1	0	$\eta(x)\lambda(x-c)$	$\sqrt{q}$ J_1	0	$(-1+i)/2$	0
12	1	0	1	1	$\eta(x)\lambda((x-c)(x^2-c))$	$3\sqrt{q}$	0	$(1+i)/2$	0
13	1	1	0	0	$\eta(x)\lambda(x-1)$	$\sqrt{q}$ J_1	0	$(1+i)/2$	0
14	1	1	0	1	$\eta(x)\lambda((x-1)(x^2-c))$	$3\sqrt{q}$	0	$(-1+i)/2$	0
15	1	1	1	0	$\eta(x)\lambda((x-1)(x-c))$	$2\sqrt{q}$	i	$(1+i)/2$	1
16	1	1	1	1	$\eta(x)\lambda((x-1)(x-c)(x^2-c))$	$4\sqrt{q}$	$-i$	$(-1+i)/2$	1
17	2	0	0	0	$\lambda(x)$	triv.	-1	0	1
18	2	0	0	1	$\lambda(x(x^2-c))$	$2\sqrt{q}$ J_2	1	-1	1
19	2	0	1	0	$\lambda(x(x-c))$	triv.	0	0	0
20	2	0	1	1	$\lambda(x(x-c)(x^2-c))$	$2\sqrt{q}$	0	-1	0
21	2	1	0	0	$\lambda(x(x-1))$	triv.	0	-1	0
22	2	1	0	1	$\lambda(x(x-1)(x^2-c))$	$2\sqrt{q}$	0	0	0
23	2	1	1	0	$\lambda(x(x-1)(x-c))$	$2\sqrt{q}$	-1	-1	-1
24	2	1	1	1	$\lambda(x(x-1)(x-c)(x^2-c))$	$4\sqrt{q}$	1	0	-1

Remark 1. Entries 25-32 are omitted; these are the same as 9-16, with η^3 replacing η in each case. For each of 25-32, the general term (respectively, the coefficient in each of the three cases) is the complex conjugate of the corresponding table entry from 9-16.

Remark 2. Trivial sums are of two types, those involving λ, η or η^3 summed over all elements of $\mathbf{F}_q$ and those involving λ and a general term that is a quadratic in x. Estimates of the form $k\sqrt{q}$ follow from the work of A. Weil, applied as in [**1**], for example.

Remark 3. A special circumstance occurs for entry 10 and its companion entry 26. Instead of pairing the occurrence of each in N_1 with its occurrence in N_2, we pair the terms in N_1 (and, separately, in N_2) for entries 10 and 26. This results in cancellation. To see this, let Σ denote the sum of terms from entries 10 and 26 in the sum N_1. Then

$$\begin{aligned}\Sigma &= \sum_{a\in\mathbf{F}_q}\{\eta(\delta a)+\eta^3(\delta a)\}\lambda(a^2-c)\\ &= \sum_a \eta(\delta a)\{1+\lambda(\delta a))\lambda(a^2-c)\}\\ &= \sum_a \eta(-\delta a)\{1+\lambda(-\delta a)\}\lambda(a^2-c)\end{aligned}$$

(summing over $-a$ in place of a)

$$= \eta(-1)\cdot\sum_a \eta(\delta a)\{1+\lambda(\delta a)\}\lambda(a^2-c) = \eta(-1)S = -\Sigma,$$

as $p \equiv 5 \pmod 8$, and it follows that $\Sigma = 0$. The details for the corresponding terms from N_2 are similar.

Let $\Lambda = (N_1+N_2)/2$, the number of interest for completing the construction. Then

$$|32\Lambda - q| \leq W\sqrt{q} + L,$$

where W is the "Weil constant" resulting from accumulating the estimates of the form $k\sqrt{q}$, and L is the result of accumulating both counting errors and terms having trivial estimates.

Somewhat remarkably, counting errors do not occur, that is, the terms $\varepsilon_1(a)$ and $\varepsilon_2(x)$ noted above are all zero. Partial details will suffice to indicate the nature of the argument.

The four expressions in (4.1), and their counterparts in (4.4), provide the "character quantity" terms in (4.2) and (4.5). Counting errors $\varepsilon_1(a)$ would occur for $a=0$, $a=c$, $a=\pm\sqrt{c}$ or $a=1$ if the four bracketed expressions had a product other than zero. We consider only $a=\pm\sqrt{c}$.

In Case 1, $c \in C(2)$ so this possibility does arise, and without loss of generality we may suppose $\sqrt{c} \in C(1)$, $-\sqrt{c} \in C(3)$. As $\sigma = 2$, the expression governing $\sqrt{a} \in C(0)$ is zero when $a = \sqrt{c}$. As $\sigma_1 = 1$ and $\lambda(\sqrt{c}) = -1$, the conditions $\lambda(a - c) = \sigma_1$ and $\lambda(a - 1) = 1$ cannot both hold when $a = -\sqrt{c}$ and so one of the corresponding expressions is zero. In Case 2, $c \in C(1)$ so that $a = \pm\sqrt{c}$ does not arise. In Case 3 an argument similar to that for Case 1 again shows that $\varepsilon_1(a) = 0$ whenever $a = \pm\sqrt{c}$. The remaining possibilities, both for $\varepsilon_1(a)$ and for $\varepsilon_2(x)$, can be argued in a similar fashion.

Among terms with trivial estimates, sums 3, 5, 9 (and 25) and 17 are zero, as each is of the form $\sum_x \psi(x)$ for a nontrivial character ψ. Sums 2, 7 and 17 are of the form $\sum_x \lambda(f(x))$ for a monic quadratic with distinct roots. Therefore, each has value -1 by ([**11**, Theorem 5.48]). Taking coefficients into account, we find that $L = 0$ in Cases 1 and 3, while we may take $L = 1$ in Case 2.

As the estimates from the table give $W = 22$ in Cases 1 and 3, and $W = 10 + 14\sqrt{2} \approx 29.8$ in Case 2, we conclude that the construction can be realized in Cases 1 and 3 when $q > 484$, and in Case 2 when $q > 900$.

5. Computations, comment and conclusion. In [**2**, pages 177–178], the existence of solutions from the construction studied here was tabulated for all $q = p$ (prime), $p \equiv 5 \pmod 8$, $29 \le p < 300$. In general, when $3 \notin C(0)$ there are many choices of a and b that provide solutions. There are two small primes omitted from the table of values. When $p = 13$, $2^4 \equiv 3 \in C(0)$ and the methods under discussion do not apply. When $p = 5$ it is not possible to realize the coset conditions on a and $a - 1$ called for by these methods; on the other hand, the sequence $P : 0, 2, 1, 3, 4$ and its translates $P + a$ provide a solution to $2K_5 \to P_5$.

Prime powers $q = p^k \equiv 5 \pmod 8$ must have $p \equiv 5 \pmod 8$ and k odd. The only case with $k > 1$ that falls in the range determined in the previous section is $q = 5^3 = 125$. In order to show that the construction provides solutions for all $q \equiv 5 \pmod 8$ with $3 \notin C(0)$, it suffices to consider $q = 125$ and those primes $p \equiv 5 \pmod 8$ below the bounds described earlier.

The following results from [**2**] allow primes to be classified into the three cases followed in the construction.

Proposition. *Suppose* $q = p^n \equiv 5 \pmod 8$ *and* x *is a primitive element of* $\mathbf{F}_q$ *chosen so that* $2 \in C(1)$.

(i) $3 \in C(0)$ *if and only if* $q \equiv 13 \pmod{24}$ *and* $p = 9u^2 + 4v^2$ *for integers* u *and* v,

(ii) $3 \in C(1)$ *if and only if* $q \equiv 5 \pmod{24}$ *and* $p = 2x^2 + 3y^2$ *for positive integers* x *and* y *with* $\lambda(xy) = -1$,

(iii) $3 \in C(2)$ *if and only if* $q \equiv 13 \pmod{24}$ *and* $p = u^2 + 36v^2$ *for integers* u *and* v,

(iv) $3 \in C(3)$ *if and only if* $q \equiv 5 \pmod{24}$ *and* $p = 2x^2 + 3y^2$ *for positive integers* x *and* y *with* $\lambda(xy) = 1$.

Cases (ii), (iii) and (iv) in this Proposition correspond to Cases 1, 2 and 3, respectively, of the construction under consideration here.

The next table lists all primes $p \equiv 5 \pmod 8$, $300 < p < 900$, and the data needed to determine $\cos 3$, the number of the coset to which 3 belongs.

TABLE 3.

p	$p \pmod{24}$	Representation	$\cos 3$
317	5	$2 \cdot 11^2 + 3 \cdot 5^2$	1
349	13	$5^2 + 36 \cdot 3^2$	2
373	13	$7^2 + 36 \cdot 3^2$	2
389	5	$2 \cdot 11^2 + 3 \cdot 7^2$	3
421	13	$9 \cdot 5^2 + 4 \cdot 7^2$	0
461	5	$2 \cdot 7^2 + 3 \cdot 11^2$	3
509	5	$2 \cdot 1^2 + 3 \cdot 13^2$	1
541	13	$4 \cdot 7^2 + 4 \cdot 5^2$	0
557	5	$2 \cdot 5^2 + 3 \cdot 13^2$	3
613	13	$17^2 + 36 \cdot 3^2$	2
653	5	$2 \cdot 17^2 + 3 \cdot 5^2$	3
661	13	$25^2 + 36 \cdot 1^2$	2
677	5	$2 \cdot 1^2 + 3 \cdot 15^2$	3

TABLE 3. continued

p	$p \pmod{24}$	Representation	$\cos 3$
701	5	$2\cdot 13^2+3\cdot 11^2$	1
709	13	$9\cdot 5^2+4\cdot 11^2$	0
733	13	$9\cdot 9^2+4\cdot 1^2$	0
757	13	$9\cdot 3^2+4\cdot 13^2$	0
773	5	$2\cdot 7^2+3\cdot 15^2$	1
797	5	$2\cdot 19^2+3\cdot 5^2$	3
821	5	$2\cdot 17^2+3\cdot 9^2$	1
829	13	$9\cdot 9^2+4\cdot 5^2$	0
853	13	$23^2+36\cdot 3^2$	2
877	13	$29^2+36\cdot 1^2$	2

In view of the remark that concludes Section 4, the following primes must be checked, as well as $q=125$, for which $3\in C(3)$ as $5=2\cdot 1^2+3\cdot 1^2$:

Case 1. $p=317, 509$
Case 2. $p=349, 373, 613, 661, 853, 877$
Case 3. $p=389, 557$

For $q=5^3$ a primitive element x such that $x^3-x+2=0$ gives $2\in C(1)$. In this case $\rho=6b^{-1}a^{-1}=(ab)^{-1}$ as $6=2\cdot 3=1$ in this field. It can be verified easily that, with $b=4$, the conditions required for the construction are satisfied for five values of a, namely, $2x+2$, $3x+4$, $4x^2+3x+3$, x^2+4x and $4x^2+x+1$. Hence, comfortably, $2K_{125}\to P_{125}$.

We reduce the number of cases requiring computation by considering special character sums involved in the argument. Let g be a primitive root of the prime $p=A^2+B^2$, where A and B are uniquely determined by $A\equiv 1 \pmod 4$ and $B\equiv Ag^{(p-1)/4} \pmod p$. Let i be a fixed primitive complex fourth root of unity, and let η be the character of order four with $\eta(g)=i$. Explicit evaluations have been given by

Emma Lehmer for Jacobi sums [**10**] and Jacobsthal sums [**9**] as follows:

(5.1)
$$J(\eta,\lambda)=\sum_{x \pmod p}\eta(x)\lambda(x-1)=A+Bi,$$

(5.2)
$$\phi_2(a)=\sum_{x \pmod p}\lambda(x)\lambda(x^2+a)=\begin{cases}-2A & \text{if } a\in C(0),\\ -2B & \text{if } a\in C(1),\\ 2A & \text{if } a\in C(2),\\ 2B & \text{if } a\in C(3).\end{cases}$$

Jacobi sums occur, and are described by J_1, as sums 11, 13 (and their conjugates as 27, 29) in Table 2. In particular, sum 13 is exactly $J(\eta,\lambda)$, while sum 11 is $\eta(c)\lambda(-c)J(\eta,\lambda)$ (see Lemma 4 of [**1**]). These sums have zero coefficients except in Case 2. As $c\in C(1)$ in Case 2, Sum 11 is $(-i)J(\eta,\lambda)$. The evaluation provided by (5.1) above, together with the coefficients from Table 2, give the contribution of the four Jacobi sums occurring in Case 2 as $2(A-B)$.

Jacobsthal sums occur, and are described by J_2, as sums 8 and 18; in particular, $S_{18}=\phi_2(-c)$, while replacing x by $(x-c)/(x-1)$ in sum 8 gives $S_8=\lambda(1-c)\{\phi_2(-c)-1\}$. The coefficients from Table 2 and the fact that $\lambda(1-c)=1$ in cases 1 and 3, gives $S_8+S_{18}=1$ in these cases. In case 2, where $\lambda(1-c)=-1$ and $-c\in C(3)$, formula (5.2) above gives $S_8+S_{18}=1-2\cdot 2B=1-4B$.

In Cases 1 and 3, the result of considering the special sums is to replace two sums, each estimated by $2\sqrt{q}$, by the exact value 1. This reduces the Weil constant from 22 to 18. The values $p=509$ (Case 1) as well as $p=389$ and 557 (Case 3) are comfortably completed. In Case 2, four Jacobi sums and two Jacobsthal sums have explicit evaluations combining to $2A-6B+1$. The substitution of this exact value for estimates of the sums in question can result in significant gain only if one is fortunate. (The estimates contribute $4+2\sqrt{2}\cong 6.8284$ to the "Weil constant." The absolute value of $(2A-6B)/\sqrt{q}$ can only be bounded by 6.3248, so the gain is not great in general.) The details for the primes that remain in Case 2 are instructive.

Beginning from $32\Lambda=q+$(remaining terms), and letting J denote the contribution from Jacobi and Jacobsthal sums, $|32\Lambda-q-J|\leq 23\sqrt{q}+L$

in Case 2. Thus

$$32\Lambda > q - 23\sqrt{q} + J - L.$$

For the values q to be considered, the following data are needed:

TABLE 4.

q	$q - 23\sqrt{q}$	A	B	$J = 2A - 6B + 1$
349	−80.68	5	18	−97
373	−71.20	−7	18	−121
613	43.55	17	18	−73
661	69.67	25	−6	87
853	181.26	−23	18	−153
877	195.87	29	−6	95

For $q = 661$, 853 and 877, analysis of character sums thus leads to the desired conclusion ($\Lambda > 0$) as L is quite small. For $q = 317$ (from Case 1) and the three remaining values from Case 2, examples showing $2K_q \to P_q$ were provided in Section 1.

REFERENCES

1. B.A. Anderson, K.B. Gross and P.A. Leonard, *Some Howell designs of prime side*, Discrete Math. **28** (1979), 113–134.

2. B.A. Anderson and P.A. Leonard, *A class of self-orthogonal 2-sequencings*, Des., Codes Cryptogr. **1** (1991), 149–181.

3. L. Carlitz, *Distribution of primitive roots in a finite field*, Quart. J. Math. **4** (1953), 4–10.

4. S.D. Cohen, *Consecutive primitive roots in a finite field*, Proc. Amer. Math. Soc. **93** (1985), 189–197.

5. ———, *Primitive elements and polynomials: existence results.* In *Finite fields, coding theory and advances in communication and computing*, Lecture Notes in Pure and Appl. Math. **141** (1992), 43–55.

6. J.H. Dinitz and D.R. Stinson, *Room squares and related designs.* In *Contemporary design theory: a collection of surveys*, J. H. Dinitz and D. R. Stinson (eds.), John Wiley and Sons, Inc., New York, 1993, 137–204.

7. K. Heinrich and G. Nonay, *Path and cycle decompositions of complete multigraphs*, Ann. Discrete Math. **27** (1985), 275–286.

8. J.D. Horton and G. Nonay, *Self-orthogonal Hamilton path decompositions*, Discrete Math. **97** (1991), 251–264.

9. E. Lehmer, *On the number of solutions of* $u^k + D \equiv w^2 \pmod p$, Pacific J. Math. **5** (1955), 103–118.

10. ———, *On Jacobi functions*, Pacific J. Math. **10** (1960), 887–893.

11. R. Lidl and H. Niederreiter, *Finite fields. encyclopedia of mathematics and its applications*, vol. 20, Addison-Wesley, Reading, Mass., 1983.

12. W.D. Wallis, *Room squares*. In *Combinatorics*: *room squares, sum-free sets, Hadamard matrices*, Lecture Notes in Math. **239** (1972), 29–121.

Department of Mathematics, University of Glasgow, Glasgow G12 8QW, Scotland, U.K.

Department of Mathematics, Arizona State University, Tempe, AZ 85287-1804, USA