Pacific Journal of Mathematics

SEQUENCINGS AND HOWELL DESIGNS

BRUCE ALLEM ANDERSON AND PHILIP A. LEONARD

Vol. 92, No. 2

February 1981

SEQUENCINGS AND HOWELL DESIGNS

B. A. ANDERSON AND P. A. LEONARD

We show that if p is a prime, $p \ge 5$, the cyclic group Z_{2p} has a strong symmetric sequencing. It follows that if p is any prime, there is a Howell design of type $H^*(2p, 2p+2)$.

1. Introduction. Suppose X is a set such that |X| = 2n. A *Howell design* on X of type H(s, 2n) consists of a square array of side s such that (1) each cell is either empty or contains an unordered pair of elements taken from X, (2) each element of X appears exactly once in each row and each column of the array and (3) every unordered pair appears at most once in a cell of the array. It is easy to see that existence requires $n \leq s \leq 2n - 1$. If $Y \subset X$ such that |Y| = 2n - s and no pair of elements of Y occupy a cell of the design of type H(s, 2n), we will denote this fact notationally by writing $H^*(s, 2n)$.

For information concerning the existence of Howell designs, see [2, 3, 4, 5, 6, 9]. Howell designs of type $H^*(2n - 1, 2n)$ are often called *Room Squares*. Room Squares are now known to exist for all *n* except n = 2, 3 [10]. In this paper we deal with the existence question for designs of type $H^*(2n - 2, 2n)$, or equivalently, of type $H^*(2m, 2m + 2)$.

It is not difficult [9] to show that there is no design of type $H^*(2, 4)$. However, it now seems certain that this is the only case in which a design of type $H^*(2m, 2m + 2)$ fails to exist. Indeed, in [4] the existence question for these types of designs is reduced to the following.

(A) Are there designs of type $H^*(2p, 2p + 2)$, p prime?

(B) Are there designs of type $H^*(6p, 6p + 2)$, p prime?

(C) Are there designs of type $H^*(24, 26)$, $H^*(48, 50)$ and $H^*(54, 56)$?

In this paper, we give an affirmative answer to (A).

Our argument for settling (A) depends upon the following ideas. Suppose G is a finite group of order n with identity e. A sequencing of G is an ordering e, a_2, \dots, a_n of all the elements of G such that the partial products $e, ea_2, ea_2a_3, \dots, ea_2 \dots a_n$ are distinct and hence comprise all of G. Gordon [8] characterized sequenceable Abelian groups as those Abelian groups with a unique element of order 2.

DEFINITION 1. Suppose G is a group of order 2n with identity e and unique element g^* of order 2. A sequencing e, a_{2n}, \dots, a_{2n}

will be called a symmetric sequencing iff $a_{n+1} = g^*$ and for $1 \le i \le n-1$, $a_{n+1+i} = (a_{n+1-i})^{-1}$.

If g^* is the unique element of order 2 in G, then g^* is in the center of G. Thus, symmetric sequencings

S: e,
$$a_2$$
, ..., a_n , g^* , a_n^{-1} , ..., a_3^{-1} , a_2^{-1}

have the associated partial product sequence

$$P: e, b_2, \cdots, b_n, b_n g^*, b_{n-1} g^*, \cdots, b_2 g^*, g^*.$$

There is a natural way [1] to use P to partition G into 2-element sets. The element that is paired with e in this partition is denoted m; m is b_n if n is even and b_{n+1} otherwise. Since we will consider the cyclic groups Z_{2p} , $p \ge 3$, p prime, m will always denote b_{p+1} in this paper. The remaining partition elements coming from P form what is called a (left) even starter and m is the nonidentity element of G "missing" from the pairs of the starter.

DEFINITION 2. Suppose G is an Abelian group of order 2n and S is a symmetric sequencing of G. S is strong iff in the associated partial product sequence P

(i) $1 \leq i < j \leq n-1$ implies $b_i b_{i+1} \neq b_j b_{j+1}$ and

(ii) $1 \leq i \leq n-1$ implies $b_i b_{i+1} \notin \{e, m^2\}$.

The sequencings of Gordon are symmetric but not strong [1]. It is known [1] that a strong symmetric sequencing on an Abelian group of order 2n will induce a Howell Design of type $H^*(2n, 2n+2)$. Thus, since [3, 9] give designs of type $H^*(4, 6)$ and $H^*(6, 8)$, in order to show that designs of all types $H^*(2p, 2p+2)$ exist (pprime), it will suffice to show that when $p \ge 5$, p prime, Z_{2p} has a strong symmetric sequencing. This will be done in the next section. We note in passing that apparently the only other known family of strong symmetric sequencings occurs on the cyclic groups Z_{p-1} , when p > 3 is prime and p = 5 or $p \equiv \pm 3$, $\pm 13 \pmod{40}$ [3].

2. The construction. Suppose $p \ge 3$ is a prime, Z_{2p} is the additive cyclic group of order 2p and $x = 2y \in Z_{2p}$. Note that since x is even, the subgroup $\langle x \rangle$ generated by x has p elements. Our candidate for a strong symmetric sequencing of Z_{2p} is defined as follows.

$$S: \; a_i = egin{cases} (i-1)x({
m mod}\;\; 2p);\; 1 \leq i \leq (p+1)/2 \;, \ 2(i-1)-p;\; (p+3)/2 \leq i \leq (3p+1)/2 \;, \ (i-1)x({
m mod}\;\; 2p);\; (3p+3)/2 \leq i \leq 2p \;. \end{cases}$$

With this definition it is easy to compute the corresponding partial

sum sequence (note again that things are written additively in this section). The notation β_x will be used for $b_{(p+1)/2} = [(p^2 - 1)/8]x$ and, as mentioned previously, since p is odd, $m_x = b_{p+1}$.

$$P: \ b_i = \begin{cases} \left[\frac{i(i-1)}{2}\right] x (\text{mod } 2p); & 1 \leq i \leq (p+1)/2 \text{ ,} \\ (\beta_x + [i-(p+1)/2]^2) (\text{mod } 2p); & (p+3)/2 \leq i \leq (3p+1)/2 \text{ ,} \\ (\left[\frac{i(i-1)}{2}\right] x + p) (\text{mod } 2p); & (3p+3)/2 \leq i \leq 2p \text{ .} \end{cases}$$

Although S is not always a strong symmetric sequencing, it is not difficult to show that S and P do always have many of the properties required. Before delineating these properties, we give two examples to facilitate understanding. In each case S is the sequence of a_i 's and P is the sequence of b_i 's. The elements β_x and m_x are starred in each case, C contains the set mentioned in Definition 2(i) and the underlining will be explained shortly.

EXAMPLE 1. p = 11, x = 6, arithmetic mod 22.

S: 0, 6, 12, 18, 2, 8, 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 14, 20, 4, 10, 16 P: $\underline{0}, \underline{6}, \underline{18}, \underline{14}, \underline{16}, \underline{2^*}, 3, \underline{6}, \underline{11}, \underline{18}, 5, \underline{16^*}, 7, \underline{0}, \underline{17}, \underline{14}, \underline{13}, 5, 3, 7, \underline{17}, \underline{11} = p$. C: 6 2 10 8 18 5 9 17 7 1 21

EXAMPLE 2. p = 13, x = 4, arithmetic mod 26.

S: 0, 4, 8, 12, 16, 20, 24, 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 2, 6, 10, 14, 18, 22 P: 0, 4, 12, 24, 14, 8, 6*, 7, 10, 15, 22, 5, 16, 3*, 18, 9, 2, 23, 20, 19, 21, 1, 11, 25, 17, 13 = p. C: 4 16 10 12 22 14 13 17 25 11 1 21 19

THEOREM 1. Suppose $p \ge 3$ is a prime, $x = 2y \in Z_{2p}$ and S and P are as defined above. Then

(i)
$$\{a_i: 1 \leq i \leq 2p\} = Z_{2p}$$
 (we will write this as $S = Z_{2p}$);

(ii) $a_1 = b_1 = 0, a_{p+1} = b_{2p} = p;$

(iii) $1 \leq k \leq p-1$ implies $a_{p+1+k} = -(a_{p+1-k});$

(iv) $1 \leq j \leq 2p$ implies $b_j + p = b_{2p-(j-1)}$;

 $(v) \quad 2 \leq i < j \leq p+1 \ implies \ b_{i-1} + b_i \not\equiv b_{j-1} + b_j \ ({
m mod} \ 2p);$

(vi) $2 \leq i \leq p+1$ implies $b_{i-1} + b_i \not\equiv 0 \pmod{2p}$.

Proof. The verification of statements (i) through (iv) is straightforward. Note that (v) and (vi) are slightly stronger statements than appear in Definition 2, although one part of that definition is not covered by these statements. We proceed with the proof of (v). For $2 \leq i \leq p$, let

$$egin{aligned} c_i &= b_{i-1} + b_i \ &= egin{cases} &(i-1)^2 x (ext{mod} \ 2p); & 2 \leq i \leq (p+1)/2 \ , \ &2eta_x + [(i-(p+3)/2)^2 + (i-(p+1)/2)^2]; \ (p+3)/2 \leq i \leq p+1 \ . \end{aligned}$$

It is easy to see that if $2 \leq i \leq (p+1)/2$, then c_i is even while the remaining c_i 's are odd. Thus it will suffice to show that there is no duplication in either half above.

Suppose $2 \leq i < j \leq (p+1)/2$. Then

$$(i-1)^2 x \equiv (j-1)^2 x \pmod{2p}$$

iff $[(i-1)^2 - (j-1)^2] y \equiv 0 \pmod{p}$
iff either $i \equiv j \pmod{p}$ or $i+j \equiv 2 \pmod{p}$.

Since neither of these conditions is possible, the even c_i 's are distinct.

Similarly, the other half reduces to showing that if $0 \leq i < j \leq (p-1)/2$, then

$$i^2 + (i + 1)^2 \not\equiv [j^2 + (j + 1)^2] \pmod{2p}$$
.

If we assume the contrary, then there are i and j within the specified limits such that

$$i^2 + (i+1)^2 \equiv [j^2 + (j+1)^2] \pmod{2p}$$

iff $i(i+1) \equiv j(j+1) \pmod{p}$.

Let j = i + k and the above reduces to

either
$$k \equiv 0 \pmod{p}$$
 or $2i + k + 1 \equiv 0 \pmod{p}$.

But since $k \leq (p-1)/2 - i$ it follows that $2i + k + 1 \leq p - 1$ and (v) is verified.

Finally, in order to show (vi), it suffices to show that $2 \leq i \leq (p+1)/2$ implies $c_i \neq 0 \pmod{2p}$ since the other c_i 's in the given range are odd numbers. But if $2 \leq i \leq (p+1)/2$,

$$c_i \equiv (i-1)^2 x (\mathrm{mod}\ 2p)$$
 .

Thus

$$egin{aligned} c_i &\equiv 0 ({
m mod} \ 2p) \ & ext{iff} \ (i-1)^2 y &\equiv 0 ({
m mod} \ p) \ & ext{iff} \ (i-1)^2 &\equiv 0 ({
m mod} \ p) \ , \end{aligned}$$

and this is clearly false.

Note that in the two given examples, the rows labelled C show the c_i 's in each case.

Now, it is clear from Theorem 1 that if S is a sequencing, it

is symmetric and that it has several of the properties of strong symmetric sequencings. Thus, we would like to answer two questions. First, when is it the case that S is a sequencing? Clearly S will be a sequencing precisely when $\{b_i: 1 \leq i \leq 2p\} = Z_{2p}$; that is, when $P = Z_{2p}$. The next result will show exactly when this happens. Second, when is it true that $2m \neq c_i \pmod{2p}$, $2 \leq i \leq p+1$? We are also able to settle this point. Certainly if we can choose x so that $P = Z_{2p}$ and 2m misses all the c_i 's, we will have a strong symmetric sequencing.

Let $N = \{1, 2, \dots, 2p\}$, let $Q = \{\{j, 2p - (j - 1)\}: 1 \leq j \leq p\}$ and suppose V is a set with exactly p elements such that every member of Q has exactly one element in V. If $x = 2y \in Z_{2p}$ is given such that $\{b_r: r \in V\} = \langle x \rangle$, then by Theorem 1 (iv) $\{b_t: t \in N \setminus V\} = \langle x \rangle + p$, and in such a case, $P = Z_{2p}$.

DEFINITION 3. Suppose $D = \{1, 2, \dots, (p+1)/2\}$ and $E = \{(p+1)/2 + 2k: 1 \leq k \leq (p-1)/2\}$. Then let $V = D \cup E$.

It is easy to see that V contains exactly one element of each member of Q. In Examples 1 and 2, the underlined elements in P are $\{b_r: r \in V\}$.

DEFINITION 4. Suppose $x = 2y \in Z_{2p}$ and S and P are constructed as usual. Then

$$\sum_x = \{(0+1+\cdots+i)x (ext{mod } 2p): 0 \leq i \leq (p-1)/2\}$$

and

$$W_x = \{ [eta_x + (2k)^2] (ext{mod } 2p) \colon 1 \leq k \leq (p-1)/2 \} \; .$$

Note that $\sum_x \cup W_x = \{b_r : r \in V\}$ and $\sum_x \cup W_x \subset \langle x \rangle$.

THEOREM 2. If $x = 2y \in Z_{2p}$, then $|\sum_x| = (p+1)/2$ and $|W_x| = (p-1)/2$.

Proof. An argument very much like that used in the second half of Theorem 1(v) shows that $|\sum_x| = (p+1)/2$ and it is straightforward to see that $|W_x| = (p-1)/2$.

Thus, $P = Z_{2p}$ exactly when $\sum_x \cap W_x = \phi$. In the following result we use the Legendre symbol $(a \mid p)$.

THEOREM 3. Suppose $p \ge 3$ is a prime, $x = 2y \in Z_{zp}$ and S and P are defined as usual. Then

(1) (y | p) = -1 iff $\sum_x \cup W_x = \langle x \rangle$ iff S is a symmetric sequencing,

(2) (y | p) = 1 iff $\sum_{x} \{\beta_x\} = W_x$.

Proof. Notice first that $\sum_x \cap W_x \neq \phi$ is equivalent to saying that there exist $i, 0 \leq i \leq (p-1)/2$ and $k, 1 \leq k \leq (p-1)/2$ such that

$$[(p^2-1)/8]2y + 4k^2 \equiv [i(i+1)/2]2y ({
m mod}\ 2p)$$
 .

This is equivalent to

(*) $16k^2 \equiv (2i + 1)^2 y \pmod{p}$.

In this form it is clear that since $16 k^2 \not\equiv 0 \pmod{p}$ for any k in the allowed range, $i \neq (p-1)/2$.

It is now very easy to prove (1). If (y|p) = -1 then (*) fails to hold so that $\sum_x \cap W_x = \phi$ and hence $\sum_x \cup W_x = \langle x \rangle$. Conversely, if $\sum_x \cup W_x = \langle x \rangle$, then the cardinalities force $\sum_x \cap W_x = \phi$. If (y|p) = 1, then any permissible choice of *i* would allow the solution of (*) for a permissible *k*. Thus (y|p) = -1. It is apparent that $\sum_x \cup W_x = \langle x \rangle$ is equivalent to *S* being a symmetric sequencing.

Now suppose (y | p) = 1. As above, given a permissible *i*, there is a unique permissible *k* such that (*) holds. Since different values of *i* lead to different values of *k*, one solution to (*) implies (p - 1)/2 solutions. Since i = (p - 1)/2 has been eliminated from consideration, it follows that $\sum_x \{\beta_x\} = W_x$. Conversely, if $W_x = \sum_x \{\beta_x\}$, then $\sum_x \cap W_x \neq \phi$ so that by (*) and the properties of the Legendre symbol, (y | p) = 1.

It is clear from Theorem 3 that if $p \ge 3$ is a prime, we can choose x = 2y such that S is a symmetric sequencing. In fact, it is not much harder to insure that S is a strong symmetric sequencing. In what follows, let

$$C=\{b_{i-1}+b_i\colon 2\leq i\leq p+1\}=\{c_i\colon 2\leq i\leq p+1\}$$
 ,

THEOREM 4. Suppose $p \ge 3$ is a prime, $x = 2y \in Z_{2p}$ and S and P are constructed as usual. The following statements holds.

(1) If $p \equiv 1 \pmod{4}$, then $2m \notin C$ iff $(y \mid p) \neq (y - 1 \mid p)$.

(2) If $p \equiv 3 \pmod{4}$, then $2m \notin C$ iff $(y \mid p) = (y - 1 \mid p)$.

Proof. Certainly 2m is even so that we need only concern ourselves with $\{c_i: 2 \leq i \leq (p+1)/2\}$. Thus $2m \in C$ iff there is an $i, 2 \leq i \leq (p+1)/2$ such that

$$(i-1)^2 x \equiv ([(p^2-1)/4]x + [(p+1)^2]/2) (\mathrm{mod}\ 2p)$$
.

This is equivalent to each of the congruences

$$(i-1)^2 y \equiv ([(p^2-1)/4]y + [(p+1)^2]/4) \pmod{p}$$

and

$$4(i-1)^2 y \equiv (-1)(y-1) \pmod{p}$$
.

Since the limits on *i* allow $(i-1)^2$ and hence $4(i-1)^2$ to be any quadratic residue, $2m \in C$ iff (y|p) = (-1|p)(y-1|p) and the result follows immediately.

THEOREM 5. Suppose $p \ge 3$ is a prime, $x = 2y \in Z_{2p}$ and S and P are constructed as usual. The following statements hold.

(1) If $p \equiv 1 \pmod{4}$, then S is a strong symmetric sequencing iff $(y \mid p) = -1$ and $(y - 1 \mid p) = 1$.

(2) If $p \equiv 3 \pmod{4}$, then S is a strong symmetric sequencing iff $(y \mid p) = -1$ and $(y - 1 \mid p) = -1$.

Proof. This is clear from Theorems 3 and 4.

THEOREM 6. If $p \ge 5$ is a prime, then Z_{2p} has a strong symmetric sequencing.

Proof. This follows immediately from Theorem 5 and facts about consecutive quadratic residues (e.g., see [7, p. 132]).

If p = 3, then our process gives a symmetric sequencing of Z_6 but it fails to be strong.

We conclude by applying the methods of this paper to the construction of a Howell Design of type $H^*(14, 16)$. Let p = 7 and 2y = x = 12. Then $p \equiv 3 \pmod{4}$ and (y - 1|p) = (y|p) = -1. Thus S is a strong symmetric sequencing.

Now the results of [1] tell us that

 $E = \{\{12, 8\}, \{2, 3\}, \{6, 11\}, \{13, 10\}, \{9, 1\}, \{5, 7\}\}$

is a "strong even starter" on Z_{14} and that if α and β are ideal elements added to Z_{14} ,

 α , 0 — — 6, 11 — 2, 3 12, 8 — β , 4 13, 10 9, 1 — 5, 7 —

is the first row of a starter-adder defined $H^*(14, 16)$.

Added in proof. P. J. Schellenberg and S. A. Vanstone have shown, in a paper to appear in the Proc. Eleventh S.E. Conf. on Combinatorics, Graph Theory and Computing, that the design types mentioned in (B) and (C) exist.

References

1. B. A. Anderson, Sequencings and starters, Pacific J. Math., 64 (1976), 17-24.

2. _____, Starters, digraphs and Howell Designs, Utilitas Math., 14 (1978), 219-248.

3. _____, Howell designs of type H(P-1, P+1), J. Combinatorial Theory Ser A, 24 (1978), 131-140.

4. ____, Hyperovals and Howell designs, Ars. Combinatorica, to appear.

5. B. A. Anderson and K. B. Gross, *A partial starter construction*, Proc. of the Ninth Southeastern Conf. on Comb., Graph Theory and Computing, (1978), 57-64.

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

7. G.E. Andrews, Number Theory, Saunders, 1971.

8. B. Gordon, Sequences in groups with distinct partial products, Pacific J. Math., 11 (1961), 1309-1313.

9. S.H.Y. Hung and N.S. Mendelsohn, On Howell designs, J. Combinatorial Theory Ser A, 16 (1974), 174-198.

10. R.C. Mullin and W.D. Wallis, *The existence of Room squares*, Aequationes Math., **13** (1975), 1-7.

Received April 17, 1979.

Arizona State University Tempe, AZ 85281

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

DONALD BABBITT (Managing Editor) University of California Los Angeles, CA 90024 HUGO ROSSI University of Utah Salt Lake City, UT 84112 C. C. MOORE and ANDREW OGG

University of California Berkeley, CA 94720 J. DUGUNDJI Department of Mathematics University of Southern California Los Angeles, CA 90007 R. FINN and J. MILGRAM Stanford University Stanford, CA 94305

ASSOCIATE EDITORS

R. ARENS E. F. BECKENBACH B. H. NEUMANN F. WOLF K. YOSHIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF ARIZONA	UNIVERSITY OF OREGON
UNIVERSITY OF BRITISH COLUMBIA	UNIVERSITY OF SOUTHERN CALIFORNIA
CALIFORNIA INSTITUTE OF TECHNOLOGY	STANFORD UNIVERSITY
UNIVERSITY OF CALIFORNIA	UNIVERSITY OF HAWAII
MONTANA STATE UNIVERSITY	UNIVERSITY OF TOKYO
UNIVERSITY OF NEVADA, RENO	UNIVERSITY OF UTAH
NEW MEXICO STATE UNIVERSITY	WASHINGTON STATE UNIVERSITY
OREGON STATE UNIVERSITY	UNIVERSITY OF WASHINGTON

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Mathematical papers intended for publication in the Pacific Journal of Mathematics should be in typed form or offset-reproduced, (not dittoed), double spaced with large margins. Please do not use built up fractions in the text of the manuscript. However, you may use them in the displayed equations. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. Please propose a heading for the odd numbered pages of less than 35 characters. Manuscripts, in triplicate, may be sent to any one of the editors. Please classify according to the scheme of Math. Reviews, Index to Vol. **39**. Supply name and address of author to whom proofs should be sent. All other communications should be addressed to the managing editor, or Elaine Barth, University of California, Los Angeles, California, 90024.

50 reprints to each author are provided free for each article, only if page charges have been substantially paid. Additional copies may be obtained at cost in multiples of 50.

The Pacific Journal of Mathematics is issued monthly as of January 1966. Regular subscription rate: \$102.00 a year (6 Vols., 12 issues). Special rate: \$51.00 a year to individual members of supporting institutions.

Subscriptions, orders for numbers issued in the last three calendar years, and changes of address shoud be sent to Pacific Journal of Mathematics, P.O. Box 969, Carmel Valley, CA 93924, U.S.A Old back numbers obtainable from Kraus Periodicals Co., Route 100, Millwood, NY 10546.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.).

8-8, 3-chome, Takadanobaba, Shinjuku-ku, Tokyo 160, Japan.

Copyright © 1981 by Pacific Jounal of Mathematics Manufactured and first issued in Japan

Pacific Journal of Mathematics

Vol. 92, No. 2 February, 1981