TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 271, Number 2, June 1982

SYMMETRIC SKEW BALANCED STARTERS AND COMPLETE BALANCED HOWELL ROTATIONS

BY

DING-ZHU DU AND F. K. HWANG

ABSTRACT. Symmetric skew balanced starters on n elements have been previously constructed for $n = 4k + 3$ a prime power and $8k + 5$ a prime power. In this paper we give an approach for the general case $n = 2^m k + 1$ a prime power with k odd. In particular we show how this approach works for $m = 2$ and 3. Furthermore, we prove that for n of the general form and $k > 9 \cdot 2^{3m}$, then a symmetric skew balanced starter always exists. It is known that a symmetric skew balanced starter on n elements, n odd, can be used to construct complete balanced Howell rotations (balanced Room squares) for n players and $2(n + 1)$ players, and in the case that n is congruent to 3 modulo 4, also for $n + 1$ players.

1. Introduction. Let $S_1, S_2, \ldots, S_m$ be a family of subsets of the elements in $\mathrm{GF}(n)$ where n is an odd prime power. Let $D_i = \{x - x' \text{ for all } x \text{ and } x' \text{ in } S_i,\ x \neq x'\}$ denote the set of symmetric differences generated by S_i. Then $S_1, S_2, \ldots, S_m$ are called *supplementary difference sets* (mod n) if $D_1, D_2, \ldots, D_m$ together contain each nonzero element of $\mathrm{GF}(n)$ an equal number of times.

A set of $m = (n - 1)/2$ pairs $(x_1, y_1), (x_2, y_2), \ldots, (x_m, y_m)$ is called a *starter* if

(i) the m pairs contain each nonzero element of $\mathrm{GF}(n)$ exactly once and

(ii) the m pairs are supplementary difference sets (mod n).

A starter is *strong* if

(iii) $x_1 + y_1, x_2 + y_2, \ldots, x_m + y_m$ are all distinct elements of $\mathrm{GF}(n)$.

It is *skew* if in addition

(iv) $\pm(x_1 + y_1), \pm(x_2 + y_2), \ldots, \pm(x_m + y_m)$ are all distinct.

A starter is *balanced* if

(v) the two sets $\{x_1, x_2, \ldots, x_m\}$ and $\{y_1, y_2, \ldots, y_m\}$ are supplementary difference sets (mod n).

A starter is *symmetric* if

(vi) $\{x_1, x_2, \ldots, x_m\} = \{-x_1, -x_2, \ldots, -x_m\}$.

It is well known [7] that a Room square of side n can be constructed from a strong starter modulo n by assigning the pair $(x_i + j, y_i + j)$ to cell $(j, x_i + y_i + j)$ for $j = 0, 1, \ldots, n - 1$, and the pair (∞, j) to cell (j, j) for $j = 0, 1, \ldots, n - 1$. If the starter is balanced or skew, then the constructed Room square is also balanced or skew. It is also known [4] that a strong balanced starter modulo n can be used to construct a complete balanced Howell rotation for n players and, if $n \equiv 3 \bmod 4$, then also a complete balanced Howell rotation for $n + 1$ players [1] (which is

Received by the editors January 23, 1981.

1980 *Mathematics Subject Classification*. Primary 05B15; Secondary 05B10, 12C20.

equivalent to a balanced Room square of side n). Finally, it has been shown [**5, 7**] that a balanced Room square (or a complete balanced Howell rotation) for $2(n+1)$ players can be constructed from a symmetric skew balanced starter modulo n.

Symmetric skew balanced starters have been constructed for the case $n = 4k + 3 > 3$ a prime power [**1**], and for the case $n = 8k + 5 > 5$ a prime power [**4, 5**]. In this paper we give an approach for the general case $n = 2^m k + 1$ a prime power with k odd (the two previous cases correspond to $m = 1$ and $m = 2$). In particular we give a construction for the case $m = 3$ and prove an asymptotic result for the general case.

2. The general approach. Let $\mathrm{GF}^*(n)$ denote the multiplicative group of $\mathrm{GF}(n)$. We quote a result of Bose [**2**].

BOSE LEMMA. *Let $n = 4k + 1$ be a prime power and let x be a generator of* $\mathrm{GF}^*(n)$. *Then the two sets $\{x^2, x^4, \ldots, x^{4k}\}$ and $\{x, x^3, \ldots, x^{4k-1}\}$ are supplementary difference sets* (mod n).

From now on we will always assume that n is a prime power of the form $2^m k + 1$ where k is odd and $m \geqslant 2$. Let x be a generator of $\mathrm{GF}^*(n)$ and for any element $y \in \mathrm{GF}^*(n)$, we write $T(y) = z$ if $y = x^z$.

THEOREM 1. *Suppose that there exists an element $y \in \mathrm{GF}^*(n)$ satisfying*
(i) $T(y) \equiv -1 \pmod{2^m}$,
(ii) $T(y-1) \equiv T(x-1) \pmod 2$,
(iii) $T(y+1) \equiv T(x+1) \pmod 2$.
Then the set of $(n-1)/2$ pairs

$$\left(x^{2^m i + 2j+1}, x^{2^m i + 2j+2}\right), \qquad i = 0, 1, \ldots, k-1, j = 0, 1, \ldots, 2^{m-2}-1,$$

$$\left(x^{2^m i + 2^{m-1} + 2j+2} y, x^{2^m i + 2^{m-1} + 2j+2}\right), \qquad i = 0, 1, \ldots, k-1, j = 0, 1, \ldots, 2^{m-2}-1,$$

is a symmetric skew balanced starter.

PROOF. That the $n - 1$ elements in the $(n-1)/2$ pairs are all distinct powers of x follows from condition (i). That the $(n-1)/2$ pairs are supplementary difference sets follows from condition (ii). Therefore the set of $(n-1)/2$ pairs is a starter. The "skew" property comes from condition (iii). The "symmetric" and the "balanced" properties come from the fact that y is an odd power of x and the Bose Lemma. $\square$

The next task is to prove the existence of an element y satisfying the three conditions of Theorem 1. Let Y denote the set of elements satisfying conditions (i), (ii), (iii). Let Y' denote the set of elements y satisfying conditions (i), (ii′), (iii′) where
(ii′) $T(y-1) \equiv T(x-1) + 1 \bmod 2$,
(iii′) $T(y+1) \equiv T(x+1) + 1 \bmod 2$.
Then clearly, $Y \cap Y' = \varnothing$. Finally, let Z denote the set of elements z satisfying conditions (iv), (v) where
(iv) $T(z) \equiv -2 \pmod{2^m}$,
(v) $T(z-1) \equiv T(x^2-1) \pmod 2$.
Since there exists a 1-1 mapping between z satisfying condition (iv) and y satisfying condition (i), while condition (v) implies that y must satisfy either conditions (ii) and (iii) or conditions (ii′) and (iii′), we have $|Z| = |Y| + |Y'|$.

Let U denote the set of elements satisfying conditions (i) and (ii). Let V denote the set of elements satisfying conditions (i) and (iii'). Then $Y = U \setminus V$ and $Y' = V \setminus U$. Suppose $Y = \varnothing$, i.e., $U \subseteq V$. Then $|Y'| = |V| - |U|$. Therefore if we can show $|Z| > |V| - |U|$, then $Y \neq \varnothing$.

3. The cases $m = 2$ and $m = 3$. The existence of a symmetric skew balanced starter for the $m = 2$, i.e., $n = 8k + 5$, case has been shown in **[5]** for $n > 5$. Here we use the approach given in §2 for a different proof. By using the cyclotomic matrix and equations (see pp. 28 and 48 of **[8]**, for example) with $n = 4k + 1$, k odd, we obtain

$$\begin{aligned} |U| &= B + E && \text{if } T(x-1) \text{ is odd,} \\ &= D + E && \text{if even,} \\ |V| &= D + E && \text{if } T(x+1) \text{ is even,} \\ &= B + E && \text{if odd,} \\ |Z| &= B + D && \text{if } T(X^2 - 1) \text{ is odd,} \\ &= A + C && \text{if even,} \end{aligned}$$

with

$$16B = n + 1 + 2s - 8t, \quad 16D = n + 1 + 2s + 8t, \quad 8(A + C) = n - 3 - 2s,$$

where $n = s^2 + 4t^2$ with $s \equiv 1 \bmod 4$. As the parity of $T(x^2 - 1)$ is determined by the parities of $T(x - 1)$ and $T(x + 1)$, therefore there are only four choices for $|U|$, $|V|$ and $|Z|$. The possible value of $|Z| - |V| + |U|$ in these four possible choices are $2B$, $2D$, and $A + C$. Therefore it suffices to prove

$$\min\{n + 1 + 2s + 8|t|, n - 3 - 2s\} > 0.$$

Note that $n + 1 + 2s - 8|t| = (s + 1)^2 + 4(|t| - 1)^2 - 4$ and $n - 3 + 2s = (s + 1)^2 + 4t^2 - 4$. Using the property that $s \equiv 1 \pmod 4$, the minimum of the two equations can be $\leqslant 0$ only for the following set of pairs: $s = 1$, $|t| \leqslant 1$; $s = -3$, $|t| \leqslant 1$. The values of n corresponding to these pairs are 1, 5, 9, 13, of which only 13 is of the form $n = 8k + 5 > 5$. But 2 is a generator of GF(13) and it is straightforward to check that $y = 2^5$ satisfies conditions (i)–(iii) of Theorem 1. Therefore the $m = 2$ case is settled. Next we deal with the case $m = 3$.

THEOREM 2. *There exists a symmetric skew balanced starter* (mod $n = 16k + 9$) *for every* $k \geqslant 1$.

PROOF. Using the cyclotomic matrix and equations (see pp. 29 and 79 of **[8]**) with $n = 8k + 1$, k odd, we obtain

$|U|$ is either $H + K + J + 0 = \frac{1}{16}(n - 1 - 4y + 4b)$ if $T(x - 1)$ is even, or $M + B + 0 + I = \frac{1}{16}(n - 1 + 4y - 4b)$ if $T(x - 1)$ is odd,

$|V|$ is either $J + L + D + M = \frac{1}{16}(n - 1 - 4y - 4b)$ if $T(x + 1)$ is odd, or $K + F + L + I = \frac{1}{16}(n - 1 + 4y + 4b)$ if $T(x - 1)$ is even,

$|Z|$ is either $G + C + N + N = \frac{1}{16}(n - 3 + 2x)$ if $T(x^2 - 1)$ is even, or $L + K + 0 + M = \frac{1}{16}(n + 1 - 2x)$ if $T(x - 1)$ is odd, (even though the values of the upper case variables depend on whether 2 is a fourth power of GF(n), the above sums remain unchanged,) with

(i) $n = x^2 + 4y^2$, $x \equiv 1 \pmod 4$ is the unique proper representation of $n = p^\alpha$ if $p \equiv 1 \pmod 4$; otherwise, $x = \pm p^{\alpha/2}$, $y = 0$.

(ii) $n = a^2 + 2b^2$, $a \equiv 1 \pmod 4$ is the unique proper representation of $n = p^\alpha$ if $p \equiv 1$ or $3 \pmod 8$; otherwise, $a = \pm p^{\alpha/2}$, $b = 0$.

Consider the four possible choices of $|U|$, $|V|$ and $|Z|$ in $|Z| - |V| + |U|$. It suffices to prove

$$n - 3 > 2|x| + 8|y|, \qquad n + 1 > 2|x| + 8|b|.$$

The first inequality is of the same type as we encountered in the $m = 2$ case. The only values of n not satisfying the inequalities are $n = 1, 5, 9, 13, 17$ of which none is of the form $n = 16k + 9$, $k \geqslant 1$. To prove the second inequality, note that $x \leqslant \sqrt{n}$ and $b \leqslant \sqrt{n/2}$. Therefore it suffices to prove $n + 1 > (2 + 4\sqrt{2})\sqrt{n}$ which is equivalent to requiring that

$$\sqrt{n} > \frac{2 + 4\sqrt{2} + \left(\left(2 + 4\sqrt{2}\right)^2 - 4\right)^{1/2}}{2} = 1 + 2\sqrt{2} + 2\left(2 + \sqrt{2}\right)^{1/2}.$$

It is easily seen that if $n \geqslant 64$, the above inequality is satisfied. There are two values of n, $9 < n < 64$, of the form $n = 16k + 9$ (n a prime power), i.e., $n = 25$, 41. We deal with these two cases separately.

$n = 25$. Then $x = -3$, $y = \pm 2$, $a = 5$, $b = 0$.

$$n - 3 = 22 > 2|-3| + 8|0| = 6.$$

$n = 41$. Then $x = 5$, $y = \pm 2$, $a = (-3)$, $b = \pm 4$.

$$n - 3 = 38 \not> 2|5| + 8|4| = 42.$$

But $x = 13$ is a generator of GF(41) while $y = 13^{15} = 14$ satisfies conditions (i)–(iii) of Theorem 1.

COROLLARY 1. *There exists a complete balanced Howell rotation for* $n = 16k + 9$ *players*, $k \geqslant 1$.

COROLLARY 2. *There exists a complete balanced Howell rotation, and also a balanced Room square, for* $n = 32k + 20$ *players for every* $k \geqslant 0$ (*since such a rotation exists for* $n = 20$ *using the method of* [**1**], *no exception is needed*).

The complete balanced Howell rotations constructed by using Corollaries 1 and 2 are all new, except for those n for which $n - 1 \equiv 3 \bmod 4$ and $n - 1$ is a prime power.

4. An asymptotic result. The cyclotomic numbers for the $m = 4$ case are known [**3, 9**]. However, there are too many equations and parameters which determine the cyclotomic numbers to go through and there are too many cases of $|Z| + |U| - |V|$ to check. Therefore we change direction from proving complete results for a single m to proving asymptotic results for all m.

THEOREM 3. *For each fixed m, let $n = 2^m k + 1$ be a prime power where k is odd. Then a symmetric skew balanced starter, hence complete balanced Howell rotations for n and $2n$ players, always exists for $k > 9 \cdot 2^{3m}$.*

PROOF. Let $q = ef + 1$ be a prime power. Then it is well known **[8]** that any cyclotomic number (i, j) with order e satisfies

$$(i, j)_e = \frac{1}{e^2} \sum_{u=0}^{e-1} \sum_{v=0}^{e-1} (-1)^{uf} \beta^{-iu-jv} J(\chi^u, \chi^v),$$

where $\beta = \exp(2\pi i/e)$ and $J(\chi^u, \chi^v)$ is the Jacobi sum

$$\sum_{\substack{\alpha \in \mathrm{GF}(q) \\ \alpha \neq 0,1}} \chi^u(\alpha)\chi^v(1-\alpha) = J(\chi^u, \chi^v)$$

for a character χ on $\mathrm{GF}(q)$ of order e. Furthermore, it is well known (see Chapter 8.3 of **[6]**, Theorem 1 and Corollary) that $J(\chi^0, \chi^0) = q - 2$ and all other $J(\chi^u, \chi^v)$ have absolute value $\sqrt{q}$ or 1. Thus for i, j, e fixed,

$$|(i, j)_e - q/e^2| < \sqrt{q}\,.$$

To prove Theorem 3, let $q = n$ and $e = 2^m$. Then each of Z, U and V is a sum over 2^{m-1} cyclotomic numbers. Therefore

$$|Y| = |Z| + |U| - |V| > n/2^{m+1} - 3 \cdot 2^{m-1}\sqrt{n} > 0$$

if $\sqrt{n} > 3 \cdot 2^{2m}$, or equivalently, if $k > 9 \cdot 2^{3m}$. Theorem 3 is now an immediate consequence of Theorem 1.

ACKNOWLEDGMENT. The authors wish to thank R. Evans, R. L. Graham and A. M. Odlyzko for providing helpful information.

REFERENCES

1. E. R. Berlekamp and F. K. Hwang, *Constructions for balanced Howell rotations for bridge tournaments*, J. Combin. Theory Ser. A **12** (1972), 159–166.

2. R. C. Bose, *On a resolvable series of balanced incomplete block designs*, Sankhyā **8** (1947), 249–256.

3. R. J. Evans and J. R. Hill, *The cyclotomic numbers of order sixteen*, Math. Comp. **33** (1979), 827–835.

4. F. K. Hwang, *Complete balanced Howell rotations for 8k + 5 players*, Discrete Math. (to appear).

5. F. K. Hwang, Q. D. Kang and J. E. Yu, *Complete balanced Howell rotations for 16k + 12 players* (to appear).

6. K. Ireland and M. I. Rosen, *Elements of number theory*, Bogden and Quigley, New York, 1972.

7. P. J. Schellenberg, *On balanced Room squares and complete balanced Howell rotations*, Aequationes Math. **9** (1973), 75–90.

8. T. Storer, *Cyclotomy and difference sets*, Markham, Chicago, Ill., 1967.

9. A. L. Whiteman, *The cyclotomic numbers of order sixteen*, Trans. Amer. Math. Soc. **86** (1957), 401–413.

INSTITUTE OF APPLIED MATHEMATICS, ACADEMY OF SCIENCE, BEIJING, CHINA

BELL LABORATORIES, MURRAY HILL, NEW JERSEY 07974