

BALANCED HOWELL ROTATIONS OF THE TWIN PRIME POWER TYPE

BY

DING-ZHU DU AND F. K. HWANG

ABSTRACT. We prove by construction that a balanced Howell rotation for n players always exists if $n = p^r q^s$ where p and $q \neq 3$ are primes and $q^s = p^r + 2$. This generalizes a much weaker previous result. The construction uses properties of a Galois domain which is a direct sum of two Galois fields.

1. Introduction. A balanced Howell rotation for $n = 2k$ players, denoted by $\text{BHR}(n)$, consists of a set of n players (denoted by $\infty, 0, 1, \dots, n-2$) and a set of $n-1$ boards (denoted by $0, 1, \dots, n-2$). For each board i the n players are divided into k ordered pairs $(a_{ij}, b_{ij}), j = 1, \dots, k$, where a_{ij} and b_{ij} are said to *oppose* each other on board i , and a_{ij} and each of $a_{ij'}, j' \neq j$, are said to *compete* with each other on board i . The partitions on the $n-1$ boards together must also satisfy the following two conditions.

- (i) Each player opposes every other player exactly once.
- (ii) Each player competes with every other player exactly $k-1$ times.

A $\text{BHR}(n)$ can also be represented by an $(n-1) \times n$ array $A = (a_{ij})$ where the rows are boards and the columns are players. Define $a_{ij} = k$ if (j, k) is an opposing pair for board i and define $a_{ij} = -k$ if (k, j) is such a pair. Let A^* be obtained from A by adding a row ∞ such that $a_{\infty j} = j$. Then the signs in A^* constitute a Hadamard matrix, and the numbers in A^* constitute a latin square $L = (l_{ij})$ with the property $l_{ij} = k \Rightarrow l_{ik} = j$ (called a *tournament latin square*). Of course, superimposing a Hadamard matrix on a tournament latin square does not automatically generate a $\text{BHR}(n)$ unless for each row $i \neq \infty$, the signs of $a_{ij} = k$ and $a_{ik} = j$ are different for all j .

Direct constructions for $\text{BHR}(n)$'s have been given mostly when n is related to a prime power, for example,

1. $n = P + 1$ where $P = 4k + 3$ is a prime power, $k \geq 1$ [1, 5].
2. $n = 2(P + 1)$ where $P = 2^m k + 1$ is a prime power, $m \geq 1, k \geq 1$ and k is odd [2, 4, 6].

In [3], an attempt was made to construct $\text{BHR}(n)$'s when n is related to a product of two prime powers differing by 2 (called *twin prime powers*). More specifically, it was proved (where $\text{GF}^*(P)$ is the multiplicative group of $\text{GF}(P)$) that

Received by the editors January 23, 1981.

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

THEOREM 1 [3]. *A BHR(n) exists if*

- (i) $n - 1 = PQ$ where P and Q are twin prime powers, and
- (ii) there exist generators x of $\text{GF}^*(P)$ and y of $\text{GF}^*(Q)$ with $x^a \equiv 2 \pmod{P}$, $P - 2 \geq a \geq 0$, $y^b \equiv 2 \pmod{Q}$, $Q - 2 \geq b \geq 0$, such that one of the following three cases holds: $b = a + 1$, $(P - 1)/2 \geq b = a \geq 0$, and $P - 2 \geq b - 2 \geq (P + 1)/2$.

In this paper we look again into the twin prime power case and prove a much stronger result.

THEOREM 2. *A BHR(n) exists if $n - 1 = PQ = p^r q^s$ where P and Q are twin prime powers, $P < Q$ and $q \neq 3$.*

2. Some preliminary results. Let x and y generate $\text{GF}^*(p^r)$ and $\text{GF}^*(q^s)$, respectively. Let G be the Galois domain (see [7]) $G = \text{GF}(p^r) \oplus \text{GF}(q^s)$ (direct sum), and let $U = \{(u, 0) : u \in \text{GF}(p^r)\}$, $V = \{(0, v) : v \in \text{GF}(q^s)\}$. Define $d = (P - 1)(Q - 1)/2$. The two cyclotomic classes in G are

$$C_0 = \{(x^i, y^i), i = 0, 1, \dots, d - 1\} = \{(x^i, y^j), i = j \pmod{2}\},$$

$$C_1 = \{(-x^i, -y^i), i = 0, 1, \dots, d - 1\} = \{(x^i, y^j), i \neq j \pmod{2}\}.$$

It is well known [7] that $C_0 + U$ forms a difference set. Therefore $C_1 + V - \{0\}$ is also a difference set.

Let the n players be denoted by the elements in $G \cup \{\infty\}$. Suppose we can partition the n players into $n/2$ pairs a_i vs. b_i , $i = 1, 2, \dots, n/2$, which meet the following two requirements.

(R1) $\pm(a_i - a_j)$ over all i , except the pair involving ∞ , runs through the set of nonzero elements of G .

(R2) $\pm(a_i - a_j)$, $\pm(b_i - b_j)$ over all a_i, a_j, b_i, b_j , except ∞ , covers each nonzero element of G an equal number of times.

Then a cyclic development of this set of $n/2$ pairs (which defines a board) yields a BHR(n), with requirement (R1) guaranteeing condition (i) and requirement (R2) guaranteeing condition (ii), since the cyclic development preserves differences.

By letting $\{a_1, a_2, \dots, a_{n/2}\} = C_0 + U + \{\infty\}$, $\{b_1, b_2, \dots, b_{n/2}\} = C_1 + V - \{0\}$, requirement (R2) is automatically satisfied. It suffices to produce a pairing between $\{a_i\}$ and $\{b_j\}$ which satisfies requirement (R1). We first prove some lemmas.

LEMMA 1. *Suppose that j, k, l, m satisfy the conditions*

$$x^{2k} + x^j = x^m, \quad 0 \leq m - j \leq P - 2, \quad -2y^{j+2l} = 1.$$

Furthermore, suppose that (i) when $0 \leq m - j \leq (P - 1)/2$, then $2j + 2l - m - (P + 1)/2$ is either 0 or 1, (ii) when $(P - 1)/2 \leq m - j \leq P - 2$, then $2j + 2l - m - (P + 1)/2$ is either 1 or 2. Then there exists a pairing satisfying requirements (R1) and (R2).

PROOF. We demonstrate pairings between elements in $C_0 + U + \{\infty\}$ and elements in $C_1 + V - \{0\}$ satisfying requirement (R1) for both case (i) and case (ii).

Case (i). The pairing is:

- (1) (x^{i+2k}, y^i) vs. $(-x^{i+j}, -y^{i+j+2l})$, $(P-1)/2 \leq i \leq d-1$,
- (2) (x^{i+2k}, y^i) vs. $(0, y^i)$, $0 \leq i \leq (P-3)/2$,
- (3) $(-x^{i+j}, 0)$ vs. $(-x^{i+j}, -y^{i+j+2l})$, $0 \leq i \leq (P-3)/2$,
- (4) $(-x^{i+j}, 0)$ vs. $(0, y^{i+2j+2l-m-(P+1)/2})$,
 $(P-1)/2 \leq i \leq m + (P-3)/2 - j$,
 $(-x^{i+j}, 0)$ vs. $(0, y^{i+2j+2l-m-(P+1)/2+1})$,
- (5) $m + (P-1)/2 - j \leq i \leq P-2$,
- (6) $(0, 0)$ vs. $(0, y^{j+2l-1})$,
- (7) ∞ vs. $(0, y^P)$, if $2j + 2l - m - (P+1)/2 = 0$,
 ∞ vs. $(0, y^{(P-1)/2})$, if $2j + 2l - m - (P+1)/2 = 1$.

The symmetric differences are:

- (1) $\pm (x^{i+m}, -y^{i+j+2l})$, $(P-1)/2 \leq i \leq d-1$,
- (2) $\pm (x^{i+2k}, 0)$, $0 \leq i \leq (P-3)/2$,
- (3) $\pm (0, y^{i+j+2l})$, $0 \leq i \leq (P-3)/2$,
- (4) $\pm (x^{i+j}, y^{i+2j+2l-m-(P+1)/2})$, $(P-1)/2 \leq i \leq m + (P-3)/2 - j$,
 $= \pm (x^{i+m}, y^{i+j+2l-(P+1)/2})$, $(P-1)/2 - m + j \leq i \leq (P-3)/2$,
 $= \pm (x^{i+m}, -y^{i+j+2l})$, $(P-1)/2 - m + j \leq i \leq (P-3)/2$,
- (5) $\pm (x^{i+j}, y^{i+2j+2l-m-(P+1)/2+1})$, $m + (P-1)/2 - j \leq i \leq P-2$,
 $= \pm (x^{i+m-(P-1)/2}, y^{i+j+2l})$, $0 \leq i \leq (P-3)/2 - m + j$,
 $= \pm (x^{i+m}, -y^{i+j+2l})$, $0 \leq i \leq (P-3)/2 - m + j$,
- (6) $\pm (0, y^{j+2l-1}) = (0, -y^{(P-1)/2+j+2l}) = \pm (0, y^{(P-1)/2+j+2l})$.

Case (ii). The pairing is:

- (1) (x^{i+2k}, y^i) vs. $(-x^{i+j}, y^{i+j+2l})$, $(P-1)/2 \leq i \leq d$,
- (2) (x^{i+2k}, y^i) vs. $(0, y^i)$, $0 \leq i \leq (P-3)/2$,
- (3) $(-x^{i+j}, 0)$ vs. $(-x^{i+j}, y^{i+j+2l})$, $0 \leq i \leq (P-3)/2$,
- (4) $(-x^{i+j}, 0)$ vs. $(0, y^{i+2j+2l-m-(P+1)/2-1})$, $(P-1)/2 \leq i \leq m-j-1$,
- (5) $(-x^{i+j}, 0)$ vs. $(0, y^{i+2j+2l-m-(P+1)/2})$, $m-j \leq i \leq P-2$,
- (6) $(0, 0)$ vs. $(0, y^{j+2l-(P+3)/2})$,
- (7) ∞ vs. $(0, y^P)$, if $2j + 2l - m - (P+1)/2 = 1$,
 ∞ vs. $(0, y^{(P-1)/2})$ if $2j + 2l - m - (P+1)/2 = 2$.

The symmetric differences are:

- (1) $\pm (x^{i+m}, y^{i+j+2l}), \quad (P-1)/2 \leq i \leq d-1,$
- (2) $\pm (x^{i+2k}, 0), \quad 0 \leq i \leq (P-3)/2,$
- (3) $\pm (0, y^{i+j+2l}), \quad 0 \leq i \leq (P-3)/2,$
 $\pm (x^{i+j}, y^{i+2j+2l-m-(P+1)/2-1}), \quad (P-1)/2 \leq i \leq m-j-1,$
 $= \pm (x^{i+j}, y^{i+2j+2l-m+(P+1)/2-1}), \quad (P-1)/2 \leq i \leq m-j-1,$
- (4) $= \pm (x^{i+m-(P-1)/2}, y^{i+j+2l}), \quad P-1-m+j \leq i \leq (P-3)/2,$
 $= \pm (x^{i+m}, -y^{i+j+2l}), \quad P-1-m+j \leq i \leq (P-3)/2,$
 $\pm (x^{i+j}, y^{i+2j+2l-m-(P+1)/2}), \quad m-j \leq i \leq P-2,$
- (5) $= \pm (x^{i+m}, y^{i+j+2l-(P+1)/2}), \quad 0 \leq i \leq P-2-m+j,$
 $= \pm (x^{i+m}, -y^{i+j+2l}), \quad 0 \leq i \leq P-2-m+j,$
- (6) $\pm (0, y^{j+2l-(P+3)/2}) = \pm (0, y^{(P-1)/2+j+2l}).$

In both cases, it is straightforward to verify that the pairings and the symmetric differences are indeed what we want. Note that if $m-j = (P-1)/2$, then subcases (i)(5) and (ii)(4) do not occur.

LEMMA 2. Suppose that k, m, z satisfy the following conditions:

$$x^{2k} + 1 = x^m, \quad 0 \leq m \leq P-2, \quad 2 = y^z.$$

Furthermore, suppose that (i) when $0 \leq m \leq (P-1)/2$, then $z-m$ is either 0 or 1, (ii) when $(P-1)/2 \leq m \leq P-2$, then $z-m$ is either 1 or 2. Then there exists a pairing satisfying requirements (R1) and (R2).

PROOF. Case (i). The pairing is:

- (1) (x^{i+2k}, y^i) vs. $(-x^i, -y^i), \quad (P-1)/2 \leq i \leq d-1,$
- (2) (x^{i+2k}, y^i) vs. $(0, y^i), \quad 0 \leq i \leq (P-3)/2,$
- (3) $(-x^i, 0)$ vs. $(-x^i, -y^i), \quad 0 \leq i \leq (P-3)/2,$
- (4) $(-x^i, 0)$ vs. $(0, y^{i+z-m}), \quad (P-1)/2 \leq i \leq (P-3)/2 + m,$
- (5) $(-x^i, 0)$ vs. $(0, y^{i+z-m+1}), \quad (P-1)/2 + m \leq i \leq P-2,$
- (6) $(0, 0)$ vs. $(0, y^P), \quad \text{if } z-m = 0,$
 $(0, 0)$ vs. $(0, y^{(P-1)/2}), \quad \text{if } z-m = 1,$
- (7) ∞ vs. $(0, y^{z+(P-1)/2}).$

The symmetric differences are:

- (1) $\pm (x^{i+m}, y^{i+z}), \quad (P-1)/2 \leq i \leq d-1,$
- (2) $\pm (x^{i+2k}, 0), \quad 0 \leq i \leq (P-3)/2,$
- (3) $\pm (0, y^i), \quad 0 \leq i \leq (P-3)/2,$

$$\begin{aligned}
 (4) \quad & \pm (x^i, y^{i+z-m}), \quad (P-1)/2 \leq i \leq (P-3)/2 + m, \\
 & = \pm (x^{i+m}, y^{i+z}), \quad (P-1)/2 - m \leq i \leq (P-3)/2, \\
 & \pm (x^i, y^{i+z-m+1}), \quad (P-1)/2 + m \leq i \leq P-2, \\
 (5) \quad & = \pm (x^{i+m}, y^{i+z+1}), \quad (P-1)/2 \leq i \leq P-2-m, \\
 & = \pm (x^{i+m}, y^{i+z}), \quad 0 \leq i \leq (P-3)/2 - m, \\
 (6) \quad & \pm (0, y^P) \pm (0, y^P) = \pm (0, y^{(P-1)/2}), \quad \text{if } z-m=0, \\
 & \pm (0, y^{(P-1)/2}), \quad \text{if } z-m=1.
 \end{aligned}$$

Case (ii). The pairing is:

$$\begin{aligned}
 (1) \quad & (x^{i+2k}, y^i) \text{ vs. } (-x^i, -y^i), \quad (P-1)/2 \leq i \leq d-1, \\
 (2) \quad & (x^{i+2k}, y^i) \text{ vs. } (0, y^i), \quad 0 \leq i \leq (P-3)/2, \\
 (3) \quad & (-x^i, 0) \text{ vs. } (-x^i, -y^i), \quad 0 \leq i \leq (P-3)/2, \\
 (4) \quad & (-x^i, 0) \text{ vs. } (0, y^{i+z-m-1}), \quad (P-1)/2 \leq i \leq m-1, \\
 (5) \quad & (-x^i, 0) \text{ vs. } (0, y^{i+z-m}), \quad m \leq i \leq P-2, \\
 (6) \quad & (0, 0) \text{ vs. } (0, y^P), \quad \text{if } z-m=1, \\
 & (0, 0) \text{ vs. } (0, y^{(P-1)/2}), \quad \text{if } z-m=2, \\
 (7) \quad & \infty \text{ vs. } (0, y^{z-1}).
 \end{aligned}$$

The symmetric differences are:

$$\begin{aligned}
 (1) \quad & \pm (x^{i+m}, y^{i+z}), \quad (P-1)/2 \leq i \leq d-1, \\
 (2) \quad & \pm (x^{i+2k}, 0), \quad 0 \leq i \leq (P-3)/2, \\
 (3) \quad & \pm (0, y^i), \quad 0 \leq i \leq (P-3)/2, \\
 & \pm (x^i, y^{i+z-m-1}), \quad (P-1)/2 \leq i \leq m-1, \\
 (4) \quad & = \pm (x^i, y^{i+z-m+P}), \quad (P-1)/2 \leq i \leq m-1, \\
 & = \pm (x^{i+m-(P-1)/2}, y^{i+z-(P+1)/2}), \quad P-1-m \leq i \leq (P-3)/2, \\
 & = \pm (x^{i+m}, y^{i+z}), \quad P-1-m \leq i \leq (P-3)/2, \\
 (5) \quad & \pm (x^i, y^{i+z-m}), \quad m \leq i \leq P-2, \\
 & = \pm (x^{i+m}, y^{i+z}), \quad 0 \leq i \leq P-2-m, \\
 (6) \quad & \pm (0, y^P) = (0, y^{(P-1)/2}), \quad \text{if } z-m=1, \\
 & \pm (0, y^{(P-1)/2}), \quad \text{if } z-m=2.
 \end{aligned}$$

Note that when $m = (P-1)/2$, then subcases (i)(5) and (ii)(4) do not occur.

3. Proof of Theorem 2. Let x be a generator of $GF^*(P)$. For $u \in GF^*(P)$, define $\log_x u = i$ if $u = x^i, 0 \leq i \leq P-2$. Similarly, we can define $\log_y v$ for $v \in GF^*(Q)$. Let $\log_y 2 = z$. Then $z \neq (P+1)/2$ since $2 = y^z = y^{(P+1)/2} = -1$ implies $q = 3$, a contradiction to our assumption. We consider four other possible cases.

Case (i). $1 \leq z \leq (P-1)/2$, $\log_x(x^z - 1) \equiv 1 \pmod{2}$.

Set $j = 0$ or 1 where $j \equiv (P+1)/2 - z \pmod{2}$,

$$2l = 3(P+1)/2 - z - j, \quad 2k = 2j + 2l - 3 + \log_x(x^z - 1),$$

$$m = 2j + 2l - (P+1)/2 - 2.$$

We now verify that the conditions in Lemma 1(ii) are satisfied.

First of all it is easily seen that both $2l$ and $2k$ are even. So k and l are well defined. Furthermore

$$\begin{aligned} x^{2k} + x^j &= x^{2j+2l-3+\log_x(x^z-1)} + x^j \\ &= x^{m+(P-1)/2}(x^z - 1) + x^j = -x^m(x^{3(P+1)/2-j-2l} - 1) + x^j \\ &= -x^m(x^{(P+1)/2-j-2l+2} - 1) + x^j = -x^j + x^m + x^j = x^m, \\ -2y^{j+2l} &= -2y^{3(P+1)/2-z} = -2(-1)^{\frac{1}{2}} = 1. \end{aligned}$$

Finally,

$$2j + 2l - m - (P+1)/2 = 2,$$

and

$$m - j = j + 2l - (P+1)/2 - 2 = P + 1 - z - 2 = P - 1 - z$$

imply $(P-1)/2 \leq m - j \leq P - 2$. Thus Theorem 2 follows from Lemma 1(ii).

Case (ii). $1 \leq z \leq (P-1)/2$, $\log_x(x^z - 1) \equiv 0 \pmod{2}$.

Set $m = z$, $2k = \log_x(x^z - 1)$. We now verify that the conditions in Lemma 2(i) are satisfied. Clearly, $2k$ is even. Furthermore

$$x^{2k} + 1 = x^z - 1 + 1 = x^m.$$

Finally, by our assumptions,

$$y^z = 2, \quad 0 \leq m \leq (P-1)/2,$$

and $z - m = 0$.

Case (iii). $(P+3)/2 \leq z \leq P$, $\log_x(x^{z-2} - 1) \equiv 1 \pmod{2}$.

Set $j = 0$ or 1 where $j \equiv (P+1)/2 - z \pmod{2}$,

$$2l = 3(P+1)/2 - z - j, \quad 2k = 2j + 2l - 1 + \log_x(x^{z-2} - 1),$$

$$m = 2j + 2l - (P+1)/2.$$

The verification that the conditions in Lemma 1(i) are satisfied is similar to case (i).

Case (iv). $(P+3)/2 \leq z \leq P$, $\log_x(x^{z-2} - 1) \equiv 0 \pmod{2}$.

Set $m = z - 2$, $2k = \log_x(x^{z-2} - 1)$.

The verification that the conditions in Lemma 2(ii) are satisfied is similar to case (ii). The proof is complete.

4. Examples.

EXAMPLE 1. $n = 16$, $P = 3$, $Q = 5$, $d = 4$.

$x = 2$ and $y = 2$ are generators of $\text{GF}^*(3)$ and $\text{GF}^*(5)$, respectively. Since $z = \log_y 2 = 1$ and $\log_x(x^3 - 1) \equiv 0 \pmod{2}$, we set

$$m = z = 1, \quad 2k = \log_x(x^z - 1) = 2,$$

and use the pairing of Lemma 2(i), i.e.,

- (1) (2, 2) vs. (1, 3),
(1, 4) vs. (2, 1),
(2, 3) vs. (1, 2),
- (2) (1, 1) vs. (0, 1),
- (3) (2, 0) vs. (2, 4),
- (4) (1, 0) vs. (0, 2),
- (6) (0, 0) vs. (0, 3),
- (7) ∞ vs. (0, 4).

EXAMPLE 2. $n = 36, P = 5, Q = 7, d = 12$.

$x = 2$ and $y = 3$ are generators of $GF^*(5)$ and $GF^*(7)$, respectively. Since $z = \log_y 2 = 2$ and $\log_x(x^z - 1) \equiv 1 \pmod{2}$, we set

$$j = 1 \equiv (P + 1)/2 - z \pmod{2}, \quad 2l = 3(P + 1)/2 - z - j = 6,$$

$$2k = 2j + 2l - 3 + \log_x(x^z - 1) = 8, \quad m = 2j + 2l - (P + 1)/2 - 2 = 3,$$

and use the pairing of Lemma 1(ii), i.e.,

- (1) (4, 2) vs. (2, 1), (3, 6) vs. (4, 3), (1, 4) vs. (3, 2),
(2, 5) vs. (1, 6), (4, 1) vs. (2, 4), (3, 3) vs. (4, 5),
(1, 2) vs. (3, 1), (2, 6) vs. (1, 3),
(4, 4) vs. (2, 2), (3, 5) vs. (4, 6),
- (2) (1, 1) vs. (0, 1), (2, 3) vs. (0, 3),
- (3) (3, 0) vs. (3, 4), (1, 0) vs. (1, 5),
- (5) (2, 0) vs. (0, 4), (4, 0) vs. (0, 5),
- (6) (0, 0) vs. (0, 6),
- (7) ∞ vs. (0, 2).

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. D.-Z. Du and F. K. Hwang, *Symmetrical skew balanced starters and complete balanced Howell rotations*, Trans. Amer. Math. Soc. **271** (1982), 409–413.
3. F. K. Hwang, *New constructions for balanced Howell rotations*, J. Combin. Theory Ser. A **21** (1976), 44–51.
4. F. K. Hwang, Q. D. Kang and J. E. Yu, *Complete balanced Howell rotations for $16k + 12$ teams* (to appear).
5. E. T. Parker and A. N. Mood, *Some balanced Howell rotations for duplicate bridge sessions*, Amer. Math. Monthly **62** (1955), 714–716.
6. P. J. Schellenberg, *Constructions for (balanced) Room squares*, Aequationes Math. **9** (1973), 75–90.
7. T. Storer, *Cyclotomy and difference sets*, Markham, Chicago, Ill., 1967.

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

BELL LABORATORIES, MURRAY HILL, NEW JERSEY 07974