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 \( n = p'q' \) where \( p \) and \( q \neq 3 \) are primes and \( q' = p' + 2 \). 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 \( \infty, 0, 1, \ldots , n - 2 \)) and a set of \( n - 1 \) boards (denoted by \( 0, 1, \ldots , n - 2 \)). For each board \( i \) the \( n \) players are divided into \( k \) ordered pairs \( (a_{ij}, b_{ij}), j = 1, \ldots , k \), 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 \( \infty \) 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 GF*(P) is the multiplicative group of GF(P)) that

Received by the editors January 23, 1981.

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

©1982 American Mathematical Society
0002-9947/82/0000-1053/03.00

415

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
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 \( GF^*(P) \) and \( y \) of \( GF^*(Q) \) with \( x^a \equiv 2 \pmod{P}, P - 2 - a \geq 0, y^b \equiv 2 \pmod{Q}, Q - 2 - b \geq 0, \) 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 \( n - 1 = PQ = p^aq^r \) where \( P \) and \( Q \) are twin prime powers, \( P < Q \) and \( q \neq 3. \)

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

\[
C_0 = \{(x^i, y^i), i = 0, 1, \ldots, d - 1\} = \{(x^i, y^i), i \equiv j \pmod{2}\},
\]

\[
C_1 = \{(-x^i, -y^i), i = 0, 1, \ldots, d - 1\} = \{(x^i, y^i), i \not\equiv j \pmod{2}\}.
\]

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. \( b_i \), \( i = 1, 2, \ldots, n/2, \) which meet the following two requirements.

(R1) \( \pm(a_i - a_j) \) over all \( i, \) except the pair involving \( \infty, \) 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 \( \infty, \) 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 \( \{a_1, a_2, \ldots, a_{n/2}\} = C_0 + U + \{\infty\}, \{b_1, b_2, \ldots, b_{n/2}\} = C_1 + V - \{0\}, \) 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. \((0, y^{i+2j}+2l-m-(P+1)/2)\),
   \((P-1)/2 \leq i \leq m + (P-3)/2 - j\),
5. \((-x^{i+j}, 0)\) vs. \((0, y^{i+2j}+2l-m-(P+1)/2+1)\),
6. \((0, 0)\) vs. \((0, y^{i+2j-1})\),
7. \((0, 0)\) vs. \((0, y^{(P-1)/2})\), if \(2j + 2l - m - (P + 1)/2 = 0\),
8. \((0, 0)\) 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. \(\pm (x^{i+m}, y^{i+j}+2l-(P+1)/2)\), \((P-1)/2 \leq i \leq m + (P-3)/2 - j\),
5. \(\pm (x^{i+m}, y^{i+j}+2l-(P+1)/2+1)\), \(m + (P-1)/2 - j \leq i \leq P-2\),
6. \(\pm (0, y^{i+j+2l}) = (0, -y^{(P-1)/2+j+2l}) = \pm (0, y^{(P-1)/2+j+2l})\).

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. \((0, y^{i+2l-(P+3)/2})\),
7. \(\infty\) vs. \((0, y^p)\), if \(2j + 2l - m - (P + 1)/2 = 1\),
8. \(\infty\) 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. \( \pm (0, y^{i+j+2l}), \quad 0 \leq i \leq (P - 3)/2, \)
4. \( \pm (x^{i+j}, y^{i+2j+2l-m-(P+1)/2-1}), \quad (P - 1)/2 \leq i \leq m - j - 1, \)
5. \( \pm (x^{i+m}, y^{i+j+2l}), \quad P - 1 - m + j \leq i \leq (P - 3)/2, \)
6. \( \pm (x^{i+j}, y^{i+2l-(P+1)/2}), \quad 0 \leq i \leq P - 2 - m + j, \)
7. \( \pm (0, y^{j+2l-(P+3)/2}) = \pm (0, y^{(P-1)/2+j+2l}). \)

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:

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

Furthermore, suppose that (i) when \( 0 < m < (P - 1)/2, \) 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. \( (0, y^P), \quad \text{if } z - m = 0, \)
7. \( (0, 0) \) vs. \( (0, y^{(P-1)/2}), \quad \text{if } z - m = 1, \)
8. \( \infty \) 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. \( \pm (0, y^i), \quad 0 \leq i \leq (P - 3)/2, \)
\[ \pm (x^i, y^{i+z-m}), \quad (P - 1)/2 \leq i \leq (P - 3)/2 + m, \]
\[ = \pm (x^{i+m}, y^{i+z}), \quad (P - 1)/2 - m \leq i \leq (P - 3)/2, \]
\[ \pm (x^i, y^{i+z-m+1}), \quad (P - 1)/2 + m \leq i \leq P - 2, \]
\[ \pm (x^{i+m}, y^{i+z+1}), \quad (P - 1)/2 \leq i \leq P - 2 - m, \]
\[ = \pm (x^{i+m}, y^{i+z}), \quad 0 \leq i \leq (P - 3)/2 - m, \]
\[ \pm (0, y^P) \pm (0, y^P) = \pm (0, y^{(P-1)/2}), \quad \text{if } z - m = 0, \]
\[ \pm (0, y^{(P-1)/2}), \quad \text{if } z - m = 1. \]

**Case (ii).** 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. \((-x^i, 0) vs. (0, y^{i+z-m-1}), \quad (P - 1)/2 \leq i \leq m - 1,\)
5. \((-x^i, 0) vs. (0, y^{i+z}), \quad m \leq i \leq P - 2,\)
6. \((0, 0) vs. (0, y^{(P-1)/2}), \quad \text{if } z - m = 1,\)
7. \((0, 0) vs. (0, y^{(P-1)/2}), \quad \text{if } z - m = 2,\)
8. \(\infty vs. (0, y^{-1}).\)

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. \(\pm (0, y^i), \quad 0 \leq i \leq (P - 3)/2,\)
4. \(\pm (x^i, y^{i+z-m-1}), \quad (P - 1)/2 \leq i \leq m - 1,\)
5. \(= \pm (x^i, y^{i+z-m+p}), \quad (P - 1)/2 \leq i \leq m - 1,\)
6. \(= \pm (x^{i+m-(P-1)/2}, y^{i+z-(P+1)/2}), \quad P - 1 - m \leq i \leq (P - 3)/2,\)
7. \(= \pm (x^{i+m}, y^{i+z}), \quad P - 1 - m \leq i \leq (P - 3)/2,\)
8. \(\pm (x^i, y^{i+z-m}), \quad m \leq i \leq P - 2,\)
9. \(\pm (0, y^P) = (0, y^{(P-1)/2}), \quad \text{if } z - m = 1,\)
10. \(\pm (0, y^{(P-1)/2}), \quad \text{if } z - m = 2.\)

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 \(\log_2 z = 2.\) Then \(z \neq (P + 1)/2\) since \(2 = y^2 = y^{(P+1)/2} = -1\) 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 $j \equiv (P + 1)/2 - z \pmod{2}$,

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

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,

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

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,

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

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 $j \equiv (P + 1)/2 - z \pmod{2}$,

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

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

$$m = z = 1, \quad 2k = \log_x(x^3 - 1) = 2.$$
and use the pairing of Lemma 2(i), i.e.,

\[(2, 2) \text{ vs. } (1, 3),\]
\[(1, 4) \text{ vs. } (2, 1),\]
\[(2, 3) \text{ vs. } (1, 2),\]
\[(1, 1) \text{ vs. } (0, 1),\]
\[(2, 0) \text{ vs. } (2, 4),\]
\[(1, 0) \text{ vs. } (0, 2),\]
\[(0, 0) \text{ vs. } (0, 3),\]
\[\infty \text{ vs. } (0, 4).\]

**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 \(z = \log_x 2 = 2\) 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.,

\[(4, 2) \text{ vs. } (2, 1),\]
\[(2, 5) \text{ vs. } (1, 6),\]
\[(1, 2) \text{ vs. } (3, 1),\]
\[(4, 4) \text{ vs. } (2, 2),\]
\[(1, 0) \text{ vs. } (0, 1),\]
\[(3, 0) \text{ vs. } (3, 4),\]
\[(2, 0) \text{ vs. } (0, 4),\]
\[(0, 0) \text{ vs. } (0, 6),\]
\[\infty \text{ vs. } (0, 2).\]

**References**


**Institute of Applied Mathematics, Academy of Science, Beijing, China**

**Bell Laboratories, Murray Hill, New Jersey 07974**