Partitionable starters for twin prime power type

Ding-Zhu Du

Mathematics Department, Massachusetts Institute of Technology, Cambridge, MA 02139, USA

D. Frank Hsu

Department of Computer Science, Fordham University, Bronx, NY 10458-5198, USA

Received 8 April 1987
Revised 18 October 1988

Abstract

Du, D.-Z. and D.F. Hsu, Partitionable starters for twin prime power type, Discrete Mathematics 87 (1991) 23–28.

Skew starters, balanced starters, partitionable starters are used in the construction of various combinatorial designs and configurations such as Room squares, Howell designs and Howell rotations. In this paper, we construct partitionable starters of order n when n is a product of two prime powers differing by 2. These partitionable starters are shown to be skew for $n \geqslant 143$. The results imply the existence of certain balanced Howell rotations. Moreover, we show the existence of partionable balanced starters of order $n = 2^m - 1$.

1. Introduction

Let G be an additive Abelian group of odd order n and G^* the set of its nonzero elements. A subset A of G is called a *difference set* if every nonzero element of G appears in the differences $x - y$, x, $y \in A$, equally often. k disjoint subsets $A_1, A_2, \ldots, A_k$ of G are called *supplementary difference sets* if every nonzero element of G appears in the differences $x - y$, x, $y \in A_i$ for $i = 1, \ldots, k$ equally often. A *starter* of G is a collection of $(n-1)/2$ disjoint pairs (x_i, y_i), $i = 1, \ldots, (n-1)/2$, which are supplementary difference sets, that is, $\{\pm(x_i - y_i): i = 1, \ldots, (n-1)/2\} = G^*$. This starter is called *strong* if $x_i + y_i$, $i = 1, \ldots, (n-1)/2$ are different elements of G^*, is called *balanced* if $\{x_i: i = 1, \ldots, (n-1)/2\}$ and $\{y_i: i = 1, 2, \ldots, (n-1)/2\}$ are supplemetary difference sets, is called *skew* if $\{\pm(x_i + y_i): i = 1, \ldots, (n-1)/2\} = G^*$, and is called *partitionable* if it can be divided into two halves S_1 and S_2 such that

(a) if $n = 4k + 3$, then $|S_2| = |S_1| + 1$ and $\{0\} \cup \{x: x$ is in a pair of $S_1\}$ and $\{x: x$ is in a pair of $S_2\}$ are supplementary difference sets,

0012-365X/91/$03.50 © 1991 — Elsevier Science Publishers B.V. (North-Holland)

(b) if $n = 4k + 1$, then $|S_1| = |S_2|$ and $\{x : x$ is in a pair of $S_1\}$ and $\{x : x$ is in a pair of $S_2\}$ are supplementary difference sets.

Strong starter, skew starters, balanced starters and partitionable starters have been used in the construction of various combinatorial designs and configurations such as Room squares, Howell designs and Howell rotation [3–4, 6, 8]. Although the problem on the existence of strong starters has been well studied, it is not known if there exists a construction for skew starters of order $5k$ [6].

The concept of a partitionable starter was introduced in [4] and its construction is known only for the following n: (i) $n = 4k + 1$ a prime power [6], and (ii) $n = 4k + 3$ a prime and -2 a generator of $\mathrm{GF}(n)$ [4]. In this paper, we give a construction of partitionable starters for $n = PQ$ where P and Q are twin prime powers, i.e., they are prime powers satisfying $P + 2 = Q$. These partitionable starters are skew for $n \geqslant 143$. In addition, we also show that partitionable balanced starters for order $2^m - 1$ exist. Using a multiplication theorem of Du and Hwang [4], partitionable starters constructed in this paper imply the existence of certain balanced Howell rotations.

2. Main results

Let p and q be distinct odd primes and α and β natural numbers. The Galois domain $\mathrm{GD}(p^\alpha q^\beta)$ is a direct sum of Galois fields $\mathrm{GF}(p^\alpha)$ and $\mathrm{GF}(q^\beta)$, which means that $\mathrm{GD}(p^\alpha q^\beta) = \{(a, b) : a \in \mathrm{GF}(p^\alpha),\ b \in \mathrm{GF}(q^\beta)\}$ with operations $(a, b) + (c, d) = (a + c, b + d)$ and $(a, b)(c, d) = (ac, bd)$. Let x and y be generators of $\mathrm{GF}^*(p^\alpha)$ and $\mathrm{GF}^*(q^\beta)$, respectively. Let $e = \gcd(p^\alpha - 1, q^\beta - 1)$ and $d = (p^\alpha - 1)(q^\beta - 1)/e$. The cyclotomic classes in $\mathrm{GD}(p^\alpha q^\beta)$ are $C_s = \{(x^i, y^{i+s}) : i = 0, 1, \ldots, d - 1\}$, $s = 0, 1, \ldots, e - 1$. Let $U = \{(u, 0) : u \in \mathrm{GF}(p^\alpha)\}$ and $V = \{(0, v) : v \in \mathrm{GF}(q^\beta)\}$. It is well known that if $C_0 \cup U$ is a difference set, so is its complement. It was shown in [9] that $C_0 \cup U$ is a difference set if and only if $p^\alpha + 2 = q^\beta$. In this case, its complement is $C_1 \cup V \backslash \{(0, 0)\}$ since $e = 2$. Therefore, we have the following lemma.

Lemma 1. *If $p^a + 2 = q^b$, then $C_0 \cup U$ and $C_1 \cup V \backslash \{(0, 0)\}$ both are difference sets.*

From now on, we denote $P = p^\alpha$, $Q = q^\beta$ and assume that $P + 2 = Q$. Skew starters of the additive group of $\mathrm{GF}(n)$ for a prime power n except 3, 5 and 9 have been constructed before ([3, 8]). Since U and V are isomorphic to $\mathrm{GF}(P)$ and $\mathrm{GF}(Q)$, respectively, we can divide $U \backslash \{(0, 0)\}$ and $V \backslash \{(0, 0)\}$ into pairs which form skew starter for U and V, respectively, that is,

Lemma 2. *If $PQ \geqslant 143$, then $U \backslash \{(0, 0)\}$ can be divided into $(P - 1)/2$ pairs $(a_i, 0)$ vs. $(b_i, 0)$, $i = 1, 2, \ldots, (P - 1)/2$ such that $\{\pm(a_i - b_i, 0) :\ i = 1, \ldots,$*

$(P-1)/2\} = \{\pm(a_1+b_1): i=1,\ldots,(P-1)/2\} = U\backslash\{(0,0)\}$, and $V\backslash\{(0,0)\}$ can be divided into $(Q-1)/2$ pairs $(0, c_i)$ vs. $(0, d_i)$, $i=1,\ldots,(Q-1)/2$ such that $\{\pm(0, c_i-d_i)$: $i=1,\ldots,(Q-1)/2\} = \{(0, c_i+d_i)$: $i=1,\ldots,(Q-1)/2\} = V\backslash\{(0,0)\}$.

Now, we prove our main result.

Theorem 1. *Skew partitionable starters of order n exist for $n = PQ \geqslant 143$ where P and Q are twin prime powers.*

Proof. Consider two cases.

Case 1: $P \equiv 3 \pmod 4$.

We divide C_0 and C_1 into the following pairs:

$$(x^{2i}, y^{2i}) \text{ vs. } (x^{2i+1}, y^{2i+1}), \quad i=0,1,\ldots,(d/2)-1,$$
$$(x^{2i}, y^{2i+1}) \text{ vs. } (x^{2i+1}, y^{2i+2}), \quad i=0,1,\ldots,(d/2)-1$$

The symmetric differences are as follows:

$$\pm(x^{2i}(x-1), y^{2i}(y-1)), \quad i=0,1,\ldots,(d/2)-1. \tag{1}$$
$$\pm(x^{2i}(x-1), y^{2i+1}(y-1)), \quad i=0,1,\ldots,(d/2)-1. \tag{2}$$

Since $Q > P > 2$, $x-1 \neq 0$ and $y-1 \neq 0$. Hence, the above differences are all in $C_0 \cup C_1$. To see that every element of $C_0 \cup C_1$ appears in those differences exactly once, it suffices to show that no two differences in (1) and (2) are equal. This fact is obviously true if they both belong to (1) or if they both belong to (2). Therefore, we only need to show the case that one difference is in (1) and the other is in (2). Suppose on the contrary that

$$(x^{2i}(x-1), y^{2i}(y-1)) = (x^{2j}(x-1), y^{2j+1}(y-1))$$

or

$$(x^{2i}(x-1), y^{2i}(y-1)) = (-x^{2j}(x-1), -y^{2j+1}(y-1))$$

for some $i, j \in \{0, 1, \ldots, (d/2)-1\}$. Then, we have

$$2i \equiv 2j+1 \pmod{Q-1}, \tag{3}$$

or

$$2i \equiv 2j+1+(Q-1)/2 \pmod{Q-1}. \tag{4}$$

Since $Q-1$ is even, (3) cannot occur. Moreover, $P \equiv 3 \pmod 4$ implies that $Q \equiv 1 \pmod 4$. Hence, $(Q-1)/2$ is even. Thus, (4) cannot occur, a contradiction.

By the similar argument, we can show that the following sums and their opposite numbers contain every element of $C_0 \cup C_1$ exactly once.

$$\pm(x^{2i}(x+1), y^{2i}(y+1)), \quad i=0,1,\ldots,(d/2)-1,$$
$$\pm(x^{2i}(x+1), y^{2i+1}(y+1)), \quad i=0,1,\ldots,(d/2)-1.$$

Here, we note that $n > 15$ guarantees $P > Q > 3$ which implies $x + 1 \neq 0$ and $y + 1 \neq 0$.

Case 2: $P \equiv 1 \pmod 4$.

We divide C_0 and C_1 into the following pairs:

$$(x^{2i}, y^{2i}) \text{ vs. } (x^{2i+1}, y^{2i+1}), \quad i = 0, 1, \ldots, (d/2) - 1,$$
$$(x^{2i+1}, y^{2i+2}) \text{ vs. } (x^{2i+2}, y^{2i+3}), \quad i = 0, 1, \ldots, (d/2) - 1.$$

The symmetric differences are as follows:

$$\pm(x^{2i}(x-1), y^{2i}(y-1)), \quad i = 0, 1, \ldots, (d/2) - 1, \tag{5}$$
$$\pm(x^{2i+1}(x-1), y^{2i+2}(y-1)), \quad i = 0, 1, \ldots, (d/2) - 1. \tag{6}$$

To see that every element of $C_0 \cup C_1$ appears exactly once in (5) and (6), by the reason as in Case 1, it suffices to prove that no one in (5) is equal to others in (6). Suppose on the contrary that

$$(x^{2i}(x-1), y^{2i}(y-1)) = (x^{2j+1}(x-1), y^{2j+2}(y-1))$$

or

$$(x^{2i}(x-1), y^{2i}(y-1)) = (-x^{2j+1}(x-1), -y^{2j+2}(y-1)),$$

for some $i, j \in \{0, 1, \ldots, (d/2) - 1\}$. Then, we have

$$2i \equiv 2j + 1 \pmod{P-1}, \tag{7}$$

or

$$2i \equiv 2j + 1 + (P-1)/2 \pmod{P-1}. \tag{8}$$

However, $P \equiv 1 \pmod 4$ implies that $P - 1$ and $(P-1)/2$ both are even. Therefore, neither (7) nor (8) can occur. Similarly, we can show that every element of $C_0 \cup C_1$ appears exactly once in the following:

$$\pm(x^{2i}(x+1), y^{2i}(y+1)), \quad i = 0, 1, \ldots, (d/2) - 1,$$
$$\pm(x^{2i+1}(x+1), y^{2i+2}(y+1)), \quad i = 0, 1, \ldots, (d/2) - 1.$$

Finally, the proof is completed by using Lemma 1 and Lemma 2. □

The construction in the above proof cannot give skew partitionable starters of orders 15, 35, 63, or 99. However, it gives partitionable starters of such orders since a starter always exists for group V or group U. Thus, we have the following corollary.

Corollary 1. *A partitionable starter for order n, a product of twin prime powers always exists.*

Suppose that a tournament consists of $n = 2k$ teams and $n - 1$ boards. On each board i, the n teams are divided into k ordered pairs (a_{ij}, b_{ij}), $j = 1, 2, \ldots, k$ where a_{ij} and b_{ij} are said to *oppose* each other on board i and any two teams of the set $\{a_{i1}, a_{i2}, \ldots, a_{ik}\}$ are said to *compete* with one another on board i, as are any two teams of $\{b_{i1}, b_{i2}, \ldots, b_{ik}\}$. A balanced Howell rotation of n teams, denoted by BHR(n), is such a tournament satisfying the following conditions.

(a) Each team opposes every other team exactly once.

(b) Each team competes with every other team exactly $k - 1$ times.

A multiplication theorem for balanced Howell rotations was given by Du and Hwang [4], which states that if BHR(m) and BHR(n) exist and a partitionable starter of order $m - 1$ exists, then BHR(mn) exists, Du and Hwang also proved in [5] that BHR($PQ + 1$) exists if Q is not a power of 3. Hence, we have the following corollary.

Corollary 3. *Let P and Q be twin prime powers. Assume that Q is not a power of* 3. *If* BHR(n) *exists then* BHR(n (PQ + 1)) *exist.*

3. Final remarks

Skew partitionable starters for twin prime power type have been constructed in this paper. The construction is simpler than that of balanced starters for twin prime power. On the other hand, skew balanced starters for prime powers $n = 4k + 3$ can be easily found. However, the construction for partitionable starters of prime power $n = 4k + 3$ is still unknown except when -2 is a generator of GF(n). It seems difficult to construct starters which are both balanced and partitionable. Here we show that partitionable balanced starters of order $n = 2^m - 1$ exist.

Consider the $(m - 1)$-dimensional projective space PG($m - 1, 2$) represented by the nonzero elements of GF(2^m). Let x be a generator of GF(2^m). Each line in PG($m - 1, 2$) contains exactly three elements; those three elements x^a, x^b, x^c satisfy $x^a + x^b + x^c = 0$. Now, consider all lines l through the point 1 and take a hyperplane H not through the point 1. Then, every line l through the point 1 intersects H at exactly one point, denoted by $x^{i(l)}$. Anderson [1] proved that $S = \{(i(l), j(l)): x^{i(l)} + x^{j(l)} = 1\}$ is a balanced starter. Furthermore, S is strong if m is odd. His proof used the following result of Baumert [2]: For $n = 2^{m-1} - 1$, if $H = \{x^{a_1}, x^{a_2}, \ldots, x^{a_n}\}$ is the set point of a hyperplane then $\{a_1, a_2, \ldots, a_n\}$ and its complementary set are both difference sets of the cyclic group Z_{2n+1}. Now if we choose another hyperplane H^* through the point 1, and divide S into two parts according to whether the line $x^{i(l)} + y^{i(l)} = 1$ is on H^* or not, then S can be shown to be a partitionable balanced starter.

The partitionable starter for prime power $n = 4k + 1$ in [6] is not skew. However, the skew starter for prime power $n = 2^m t + 1$ for some odd $t \neq 1$, in [8], is indeed partitionable. Does a skew partitionable starter exist for the order of a Fermat prime? It is an open question. Nonexistence of a strong balanced starter of order n which is a Fermat prime has been conjected by Hwang [6]. We feel that the same thing could happen for the skew partitionable starter.

References

[1] B.A. Anderson, Hyperplanes and balanced Howell rotations, Ars Combin. 13 (1983) 163–168.

[2] L.D. Baumert, Cyclic Difference Sets, Lecture Notes in Mathematics No. 182 (Springer, Berlin, 1971).

[3] B.C. Chong and K.M. Chan, On the existence of normalized Room squares, Nata Math. 7 (1971) 8–17.

[4] D.-Z. Du and F.K. Hwang, A multiplication theorem for balanced Howell rotations, J. Combin. Theory 37 (1984) 121–126.

[5] D.-Z. Du and F.K. Hwang, Balanced Howell rotations for the twin prime power type, Trans. Amer. Math. Soc. 271 (1982) 396–400.

[6] F.K. Hwang, Strong starters, balanced starters and partitionable starters, Bull. Inst. Math. (1983) 561–572.

[7] S. Lins and P.J. Schellenberg, The existence of skew strong starters in Z_{16k^2+1}: a simple proof, Ars Combin. II (1981) 123–129.

[8] R.C. Mullin and E. Nemeth, An existence theorem for Room squares, Canad. Math. Bull. 12 (1969) 493–497.

[9] T. Storer, Cyclotomy and Difference Sets (Markham, Chicago, 1967).