Factoring $(16, 6, 2)$ Hadamard difference sets

Chirashree Bhattacharya

Department of Mathematics
Randolph-Macon College
Ashland, VA 23005
cbhattacharya@rmc.edu

Ken W. Smith

Department of Mathematics & Statistics
Sam Houston State University
Huntsville, TX 77340
kenwsmith@shsu.edu

Submitted: Dec 11, 2007; Accepted: Aug 26, 2008; Published: Aug 31, 2008
Mathematics Subject Classification: 05B10

Abstract

We describe a "factoring" method which constructs all twenty-seven Hadamard $(16, 6, 2)$ difference sets. The method involves identifying perfect ternary arrays of energy 4 (PTA(4)) in homomorphic images of a group G, studying the image of difference sets under such homomorphisms and using the preimages of the PTA(4)s to find the "factors" of difference sets in G.

This "factoring" technique generalizes to other parameters, offering a general mechanism for creating Hadamard difference sets.

1 Introduction

Let G be a group of order v and $X = \sum_{g \in G} x_g g$ an element of the integral group ring $\mathbb{Z}[G]$. By $X^{(-1)}$ we will mean the integral group ring element $X^{(-1)} = \sum_{g \in G} x_g g^{-1}$. We also identify G with the group ring element $\sum_{g \in G} g$. We say that X is a *difference set* with parameters (v, k, λ) if X has coefficients $x_g \in \{0, 1\}$ and

$$XX^{(-1)} = (k - \lambda)1_G + \lambda G.$$

A difference set D with parameters $(4m^2, 2m^2 - m, m^2 - m)$ (m a positive integer) is called a *Hadamard difference set.* An element $T = \sum_{g \in G} t_g g$ of the integral group ring $\mathbb{Z}[G]$ is a *perfect ternary array* of energy ν (PTA(ν)) if T has coefficients $t_g \in \{-1, 0, 1\}$ and

$$TT^{(-1)} = \nu 1_G.$$

A good introduction to perfect ternary arrays is the article [1] by Arasu and Dillon. The beauty of Hadamard difference sets (especially in abelian groups) is nicely displayed in the article by Dillon [3]. That paper includes a general product construction for Hadamard difference sets; that product construction is generalized further by this paper. For the general theory of symmetric designs and difference sets, see Lander's monograph, [8]. The $(16, 6, 2)$ designs in detail are described in [2].

Kibler found, by computer in 1978, all $(16, 6, 2)$ difference sets. There are 27 inequivalent difference sets in 12 groups of order 16. These are listed in Kibler's survey [6].

The article by Marcel Wild ([9]) provides a nice discussion of the groups of order 16. These groups are also easily analyzed using the public domain software package *GAP*, [5].

We will discuss in detail in sections 2 and 3 how PTA's, especially products of PTA(4)s are related to finding the Hadamard difference sets we seek in groups of order 16. All $(16, 6, 2)$ difference sets are constructed in this manner; in section 4 we provide the factoring for each of the 27 $(16, 6, 2)$ difference sets.

The techniques in this paper generalize to other parameters of Hadamard difference sets. Of the 259 groups of order 64 possessing a $(64, 28, 12)$ difference set, a product construction using PTAs will construct difference sets in 212 of these groups ([4].) Of the 132 groups of order 144 conjectured to have a $(144, 66, 30)$ difference set, a PTA product construction will provide difference sets in *all* but one of these groups (see [7].)

2 Perfect Ternary Arrays

The following lemma easily follows from the definitions in section 1.

Lemma 1 *D is a Hadamard difference set in a group G of order $4m^2$ if and only if $\hat{D} := G - 2D$ is a $PTA(4m^2)$ in G.*

Furthermore, it can be easily verified that if T is a PTA(ν) in a group G, then for any $g \in G$, $-T, gT$, and Tg are also perfect ternary arrays. Furthermore, if ϕ is an automorphism of G, then $\phi(T)$ is also a PTA(ν). We say that two PTAs T_1, T_2 are **equivalent** if there exists a group element $g \in G$ and an automorphism ϕ of G such that $T_2 = \pm g\phi(T_1)$.

We explore PTA(4)s in detail. The results which follow, leading to Lemma 2, were first observed by John Dillon and communicated to the second author during the author's sabbatical visit to the National Security Agency in 1990. We are not aware of any place these computations have appeared in print.

Suppose T is a PTA(4). Since $TT^{(-1)} = 4$, then under the trivial representation of the group, T must be sent to ± 2. Replacing T by $-T$ if necessary, we may assume that T involves a single element g with coefficient $+1$ and three elements with coefficients -1. Premultiplying by g^{-1}, we may assume that $T = 1 - a - b - c$ where a, b, c are distinct nonidentity elements of G. Writing out the definition of PTA(4), we have that $T = 1 - a - b - c$ satisfies the equation

$$TT^{(-1)} = (1 - a - b - c)(1 - a^{-1} - b^{-1} - c^{-1}) = 4.$$

Formally multiplying out $(1 - a - b - c)(1 - a^{-1} - b^{-1} - c^{-1})$ we have

$$4 - (a + b + c + a^{-1} + b^{-1} + c^{-1}) + (ab^{-1} + ac^{-1} + ba^{-1} + bc^{-1} + ca^{-1} + cb^{-1}).$$

If this is equal, in the group ring, to the element $4 \cdot 1_G$ then the (multi)sets $\{a, b, c, a^{-1}, b^{-1}, c^{-1}\}$ and $\{ab^{-1}, ac^{-1}, ba^{-1}, bc^{-1}, ca^{-1}, cb^{-1}\}$ must be equal. We walk through the various cases forced by this requirement.

The element a cannot be equal to ab^{-1} or ac^{-1}, for then, contrary to our assumption, b or c is the identity. We may, therefore, assume without loss of generality, that $a = cb^{-1}$ or $a = ba^{-1}$. (The assumptions $a = bc^{-1}$ or $a = ca^{-1}$ are equivalent to these two cases, after a relabelling of variables.)

Case 1. We assume $a = cb^{-1}$ and therefore $c = ab$. We examine the set equation $\{b, ab, b^{-1}, b^{-1}a^{-1}\} = \{ab^{-1}, ab^{-1}a^{-1}, ba^{-1}, aba^{-1}\}$.

1. Suppose $b = ab^{-1}$. Then $a = b^2$.

   This forces the set equation $\{ab, b^{-1}a^{-1}\} = \{ab^{-1}a^{-1}, aba^{-1}\}$. We may choose

   (a) $ab = ab^{-1}a^{-1} = ab^{-3} \implies b^4 = 1$. Therefore $T = 1 - b - b^2 - b^3$ and $b^4 = 1$.

   (b) $ab = aba^{-1} \implies a = 1$, which is not allowed.

2. Suppose $b = ab^{-1}a^{-1}$.

   This forces the set equation $\{ab, b^{-1}a^{-1}\} = \{ab^{-1}, ba^{-1}\}$. We may choose

   (a) $ab = ab^{-1} \implies b^2 = 1$. This and the earlier condition ($b = ab^{-1}a^{-1}$) force a and b to commute. Thus $T = 1 - a - b - ab$ where b is an involution commuting with a. (We call this solution the "commuting involution" solution.)

   (b) $ab = ba^{-1}$. This forces $ab = a^2b^{-1}a^{-1} = ba^{-1} \implies a^2 = b^2$. Thus $T = 1 - a - b - ab$ where a, b obey the "quaternion-like" conditions $bab^{-1} = a^{-1}, a^2 = b^2$.

3. Suppose $b = aba^{-1}$.

   This forces the multiset equality $\{ab, b^{-1}a^{-1}\} = \{ab^{-1}, ba^{-1}\}$. We may choose either

   (a) $ab = ba^{-1} \implies b^2 = 1$, that is, we have a commuting involution solution.

   (b) $ab = ba^{-1} \implies a^2 = 1$, equivalent to the previous solution.

Thus far we have two types of solutions:

1. the "commuting involution" solution, where $c = ab$, $ab = ba$, and at least one of a, b has order 2.

2. the "quaternion" solution, where $c = ab, a^2 = b^2, bab^{-1} = a^{-1}$.

Case 2. Suppose $a = ba^{-1}$ and therefore $b = a^2$. Furthermore, the sets $\{a^2, c, a^{-2}, c^{-1}\}$ and $\{ac^{-1}, a^2c^{-1}, ca^{-1}, ca^{-2}\}$ are equal. If $a^2 = ac^{-1}$ then $c = a^{-1}$, so $a = bc$ and we have a solution equivalent (after a relabeling of variables) to Case 1. Similarly, if $a^2 = ca^{-1}$ then $c = a^3$ and $c = ab$. However, if $a^2 = ca^{-2}$ then $c = a^4$ and we are forced to conclude that $a^{-3} = a^4$ and so $a^7 = 1$. Thus the set $\{a, b, c\}$ is the $(7, 3, 1)$ difference set $\{a, a^2, a^4\}$ in the cyclic subgroup generated by a and if we write $D := a + a^2 + a^4$ then $T = 1 - D$. This is the "Fano plane solution," the only solution occurring in a group of odd order.

Lemma 2 *In summary, $TT^{(-1)} = 4$ allows three types of solutions. There is the sporadic "Fano plane" solution, $T = 1 - a - a^2 - a^4$ where $a^7 = 1$ and two others. The two other solutions are the "commuting involution" solution $T = 1 - a - b - ab$ where a (or b) is an involution and a and b commute and the "quaternion" solution $T = 1 - a - b - ab$ where $bab^{-1} = a^{-1}$ and $a^2 = b^2$.*

(Note: If a, b generate the Klein 4-group then both conditions above are satified, that is, a, b satisfy both the "commuting involution" and the "quaternion" conditions. Otherwise, $bab^{-1} = a^{-1}, a^2 = b^2$ implies that $\langle a, b\rangle$ is the quaternion group Q_8.)

From here on, for group elements a, b, we will use the notation $T^+_{a,b} := 1+a+b+ab$ and $T^-_{a,b} := 1 - a - b - ab$ when necessary. If $T = \sum_{g\in G} t_g g$ is an element of the integral group ring $\mathbb{Z}[G]$ where $t_g \in \{-1, 0, 1\}$, we define the **support** of T to be the set of elements $g \in G$ such that t_g is not zero.

Lemma 3 *Suppose there exist $\epsilon_i \in \{-1, 1\}$ such that $T = \epsilon_0 1 + \epsilon_1 a + \epsilon_2 b + \epsilon_3 ab$ is a PTA(4). Then T is equivalent to the PTA(4) $T^-_{x,y} = 1 - x - y - xy$ where x is either a or a^{-1} and y is either b or b^{-1}.*

Proof Since $TT^{(-1)} = 4$, the trivial representation forces exactly three of the ϵ_i to agree in sign. Multiplying by -1 if necessary, we assume that three of the ϵ_i are negative. There are four cases, depending on the choice of the single positive ϵ_i. If $\epsilon_0 = 1$ then $T = T^-_{a,b}$. Otherwise:

1. $-1 + a - b - ab = a(T^-_{a^{-1},b})$,

2. $-1 - a + b - ab = (T^-_{a,b^{-1}})b$,

3. $-1 - a - b + ab = a(T^-_{a^{-1},b^{-1}})b$.

Corollary 1 *If $T = \epsilon_0 1 + \epsilon_1 a + \epsilon_2 b + \epsilon_3 ab$ is a PTA(4) of commuting involution type where a is a commuting involution then T is equivalent to either $T^-_{a,b}$ or $T^-_{a,b^{-1}}$.*

We conclude this section with a brief example. Suppose $G \cong C_2 \times C_4 = \langle w, y : w^2 = y^4 = [w, y] = 1\rangle$. Each of the group ring elements

1. $T^-_{w,y} = 1 - w - y - wy$,
2. $T^-_{w,y^2} = 1 - w - y^2 - wy^2$,
3. $T^-_{y^2,y} = 1 - y^2 - y - y^3$,

are perfect ternary arrays with energy 4. The automorphism group of G is isomorphic to the dihedral group of order 8. There is an automorphism which fixes w but maps y^2 to wy^2. Given a fixed element g of order four, there is a unique automorphism which fixes both w and y^2 yet map y to g. The automorphisms just described generate the full automorphism group of G and so the three PTAs listed above are mutually inequivalent and any PTA is G is equivalent to one of these. Therefore, up to equivalence, the three PTAs listed above are all the PTA(4)s in $C_2 \times C_4$.

3 Perfect Ternary Arrays and Hadamard difference sets

In this section we explain how PTA(4)s can be used to find (16, 6, 2) Hadamard difference sets. The following theorem provides some crucial observations.

Theorem 1 *Let G be a group of order $4m^2$ and z a central involution in G. Use the bar convention for homomorphic images modulo $\langle z\rangle$. Let D be a $(4m^2, 2m^2 - m, m^2 - m)$ - difference set. Then:*

1. $\overline{DD}^{(-1)} = m^2 + 2(m^2 - m)\ \overline{G}$ *and* $\overline{T} = \overline{D} - \overline{G}$ *is a PTA of energy* m^2.
2. *Let H be a transversal of G modulo $\langle z\rangle$. Then $\overline{T}_{\overline{h}} = |D \cap \{h, hz\}| - 1$ for $h \in H$. Define $T \in \mathbb{Z}[H]$ by $T_h = \overline{T}_{\overline{h}}$, and $F \in \mathbb{Z}[H]$ by $F_h = 0$ if $|D \cap \{h, hz\}| = 0$ or 2, $F_h = 1$ (or -1) if $D \cap \{h, hz\} = \{h\}$ (or $= \{hz\}$). Then*
$$D = (T + H)(\frac{1+z}{2}) + F(\frac{1-z}{2}) \tag{1}$$
and
$$FF^{(-1)}(1 - z) = m^2(1 - z). \tag{2}$$

Proof 1. By definition,
$$DD^{(-1)} = m^2 + (m^2 - m)G.$$

Passing to images in $\overline{G}$,
$$\overline{DD}^{(-1)} = m^2 + 2(m^2 - m)\overline{G}.$$

Also,

$$\begin{aligned}\overline{T}\overline{T}^{(-1)} &= (\overline{D}-\overline{G})(\overline{D}^{(-1)}-\overline{G}^{(-1)}) = \overline{D}\overline{D}^{(-1)} - \overline{G}\overline{D}^{(-1)} - \overline{D}\overline{G}^{(-1)} + \overline{G}\overline{G}^{(-1)} \\ &= m^2 + 2(m^2-m)\overline{G} - (2m^2-m)\overline{G} - (2m^2-m)\overline{G} + (2m^2)\overline{G} \\ &= m^2.\end{aligned}$$

$\overline{T}$ is thus a PTA of energy m^2.

2. The image of D may be written as

$$\overline{D} = \sum_{h\in H} a_h \overline{h}$$

where $a_h \in \{0,1,2\}$. Note that $a_h = |D \cap \{h, hz\}|$ for $h \in H$. Since

$$\sum_{h\in H} a_h = 2m^2 - m$$

and

$$\sum_{h\in H} a_h^2 = m^2 + 2(m^2-m) = 3m^2 - 2m,$$

and $|H| = 2m^2$, the multiset $\{a_h : h \in H\}$ must consist of $\frac{m^2-m}{2}$ twos, m^2 ones, and $\frac{m^2+m}{2}$ zeroes.

Now, $\overline{T} = \overline{D} - \overline{G} = \sum_{h\in H} a_h\overline{h} - \sum_{h\in H}\overline{h} = \sum_{h\in H}(a_h - 1)\overline{h} = \sum_{h\in H}(|D\cap\{h,hz\}|-1)\overline{h}$.

Then

$$T = \sum_{h\in H}(|D\cap\{h,hz\}|-1)h$$

and

$$T + H = \sum_{h\in H}(|D\cap\{h,hz\}|)h = 2\sum_{|D\cap\{h,hz\}|=2} h + \sum_{D\cap\{h,hz\}=h} h + \sum_{D\cap\{h,hz\}=hz} h.$$

Combining with $F \in \mathbb{Z}[H]$ as defined,

$$\begin{aligned}(T+H)\frac{(1+z)}{2} + F\frac{(1-z)}{2} & \\ &= \sum_{|D\cap\{h,hz\}|=2}(h+hz) + \sum_{D\cap\{h,hz\}=h}\frac{(h+hz)}{2} + \sum_{D\cap\{h,hz\}=hz}\frac{(h+hz)}{2} \\ &\quad + \sum_{D\cap\{h,hz\}=h}\frac{(h-hz)}{2} + \sum_{D\cap\{h,hz\}=hz}\frac{(hz-h)}{2} \\ &= D\end{aligned}$$

proving Equation (1). We may further write

$$\hat{D} := G - 2D = -(T(1+z) + F(1-z)). \tag{3}$$

Since $\overline{T}$, the image of T in $G/\langle z\rangle$, is a PTA(m^2), we have that

$$TT^{(-1)} = m^2 + Y(1-z)$$

where Y is some element in $\mathbb{Z}[G]$. According to Lemma 1, for D to be a difference set in a group of order $4m^2$, $\hat{D}$ must be a PTA($4m^2$) which yields

$$4m^2 = \hat{D}\hat{D}^{(-1)} = 2TT^{(-1)}(1+z) + 2FF^{(-1)}(1-z).$$

This implies that

$$FF^{(-1)}(1-z) = m^2(1-z).$$

This suggests a two step search algorithm for Hadamard difference sets in groups of order $4m^2$ possessing a commuting involution z. First, we find, up to equivalence all PTA's $\overline{T}$ in $\overline{G}$. This defines $T \subseteq \mathbb{Z}[H]$. Given T, the set $H - Supp(T)$ is the support of F. We then choose coefficients ± 1 for the elements of F so that F satisfies Equation (2). In theory, both of these steps could be computationally difficult. (Indeed, if m is not a power of 2, the element z might not exist.) But for the $(16, 6, 2)$ case, this process is efficient and provides all 27 difference sets.

We assume hereafter that $m = 2$ and so G has order 16. Thus, $\overline{G}$ has order 8 and $\overline{T}$ is a PTA(4) that is either of the "commuting involution" or "quaternion" type.

If $\overline{T}$ is equivalent to $\overline{1}-\overline{a}-\overline{b}-\overline{ab}$ where $\overline{a}$ is a commuting involution, then $\{\overline{1}, \overline{a}\}, \{\overline{b}, \overline{ab}\}$ are cosets of $\langle\overline{a}\rangle$ in $\overline{G}$ and there exists an element $\overline{g} \in \overline{G}$ such that $\{\overline{1}, \overline{b}, \overline{g}, \overline{bg}\}$ is a transversal of $\langle\overline{a}\rangle$ in $\overline{G}$. We have $\overline{G} = \{\overline{1}, \overline{a}, \overline{b}, \overline{ab}\} \cup \{\overline{g}, \overline{ag}, \overline{bg}, \overline{abg}\}$. Choosing the transversal $H = \{1, a, b, ab, g, ag, bg, abg\}$ such that a, b, g are preimages in G of $\overline{a}, \overline{b}, \overline{g}$ respectively, allows for $T \in \mathbb{Z}[H]$ to be $1 - a - b - ab$. Then $Supp(F) = \{g, ag, bg, abg\}$ is a translate of $Supp(T)$.

If $\overline{T}$ is equivalent to $\overline{1} - \overline{a} - \overline{b} - \overline{ab}$ of the "quaternion" type, that is, $\langle\overline{a}, \overline{b}\rangle = \overline{G} \cong Q_8$ then $\overline{G} = \{\overline{1}, \overline{a}, \overline{b}, \overline{ab}\} \cup \{\overline{g}, \overline{ag}, \overline{bg}, \overline{abg}\}$ where $\overline{g} = \overline{a^2}$. As before, choosing the transversal $H = \{1, a, b, ab, g, ag, bg, abg\}$ such that a, b, g are preimages in G of $\overline{a}, \overline{b}, \overline{g}$ respectively, allows for $T \in \mathbb{Z}[H]$ to be $1 - a - b - ab$. Then $Supp(F) = \{g, ag, bg, abg\}$ is a translate of $Supp(T)$.

We may substitute $F = Xg$ in equation (2) where $Supp(X) = \{1, a, b, ab\} = Supp(T)$. Since $FF^{(-1)} = (Xg)(Xg)^{(-1)} = XX^{(-1)}$, it is enough to find all X that satisfy the equation:

$$XX^{(-1)}(1-z) = 4(1-z)$$

which may be rewritten as

$$(XX^{(-1)} - 4)(1-z) = 0. \tag{4}$$

If X satisfies equation (4), then so does $-X$, hence we may work with X of the form $1 \pm a \pm b \pm ab$. Theorem 2 describes all X satisfying equation (4), but first we prove Lemma 4 for special cases.

Lemma 4 *If*

$$(XX^{(-1)} - 4) = A(1 - z)$$

where $A \in \mathbb{C}[G]$ *then*

$$(XX^{(-1)} - 4)(1 - z) = 0 \Longrightarrow X \textit{ is a } PTA(4).$$

Proof As

$$0 = (XX^{(-1)} - 4)(1 - z) = A(1 - z)^2 = 2A(1 - z)$$

we obtain $A(1 - z) = 0$ and then $XX^{(-1)} = 4$.

What does the image $\overline{T}$ of an element T say about the element F? The answer to this question is subtle.

Theorem 2 *Suppose* $X = 1 + \epsilon_1 a + \epsilon_2 b + \epsilon_3 ab$, *where* $\epsilon_i \in \{-1, 1\}$, $i \in \{1, 2, 3\}$ *and* $\overline{T} = \overline{1} - \overline{a} - \overline{b} - \overline{ab}$ *is PTA(4) in* $G/\langle z\rangle$ *of the "commuting involution" type. If*

$$(XX^{(-1)} - 4)(1 - z) = 0$$

then either

1. *X is itself a PTA(4) in G (if* $a^2 = 1, ab = ba$ *and X has an odd number of minus signs) or,*

2. *X is of the "quaternion type", i.e.,* $\langle a, b\rangle = Q_8$ *(if* $a^2 = b^2 = z, ab = baz$*).*

Proof A straightforward computation shows that

$$XX^{(-1)} - 4 =$$

$$(\epsilon_1+\epsilon_2\epsilon_3)(a+a^{-1})+\epsilon_2(b+b^{-1})+\epsilon_1\epsilon_3(aba^{-1}+ab^{-1}a^{-1})+\epsilon_3(ab+b^{-1}a^{-1})+\epsilon_1\epsilon_2(ab^{-1}+ba^{-1}) \tag{5}$$

If X has an odd number of minus signs, then $\epsilon_i = -\epsilon_j\epsilon_k$ for distinct i, j, k. If X has an even number of (or possibly 0) minus signs, then $\epsilon_i + \epsilon_j\epsilon_k = \pm 2$ for distinct i, j, k. There are four cases depending on the choice of a and b in G.

Case 1. $a^2 = 1, ab = ba$
Using the above relations in equation (5), we get

$$XX^{(-1)} - 4 = 2(\epsilon_1 + \epsilon_2\epsilon_3)(a) + (\epsilon_2 + \epsilon_1\epsilon_3)(b + b^{-1}) + (\epsilon_3 + \epsilon_1\epsilon_2)a(b + b^{-1}).$$

If X has an odd number of negative signs, then setting $(\epsilon_1 + \epsilon_2\epsilon_3) = (\epsilon_2 + \epsilon_1\epsilon_3) = (\epsilon_3 + \epsilon_1\epsilon_2) = 0$,

$$(XX^{(-1)} - 4) = 0.$$

If X has an even number of negative signs, then

$$(XX^{(-1)} - 4)(1 - z) = (\pm 4a \pm 2(b + b^{-1}) \pm 2a(b + b^{-1}))(1 - z) = 0$$

$$\Longrightarrow \pm 2a \pm (b+b^{-1}) \pm a(b+b^{-1}) = \pm 2az \pm (b+b^{-1})z \pm a(b+b^{-1})z.$$

Then a must be equal to an element x in the set $\{az, bz, b^{-1}z, abz, ab^{-1}z\}$. But as $\bar{x} = \bar{a}$ and $a \neq az$, we obtain a contradiction.

Case 2. $a^2 = 1, ab = baz$
Using these relations in equation (5) we get

$$XX^{(-1)} - 4 = 2(\epsilon_1 + \epsilon_2\epsilon_3)(a) + (\epsilon_2 + \epsilon_1\epsilon_3 z)(b+b^{-1}) + (\epsilon_3 + \epsilon_1\epsilon_2 z)(ab + b^{-1}a)$$

If X has an odd number of negative signs,

$$(XX^{(-1)} - 4) = \pm(1-z)(b+b^{-1}) \pm (1-z)(ab+b^{-1}a)$$

By Lemma 4,

$$(XX^{(-1)} - 4)(1-z) = 0 \Longrightarrow (XX^{(-1)} - 4) = 0.$$

However, if X is PTA(4), X would have to be of the "commuting involution" or "quaternion" type. Since it is neither, this case is impossible. If X has an even number of negative signs, then

$$\begin{aligned}(XX^{(-1)} - 4)(1-z) &= (\pm 4a \pm (1+z)(b+b^{-1}) \pm (1+z)(ab+b^{-1}a))(1-z)\\ &= \pm 4a(1-z).\end{aligned}$$

Then

$$(XX^{(-1)} - 4)(1-z) = 0 \Longrightarrow \pm 4a(1-z) = 0 \Longrightarrow a = az.$$

But that is impossible.

Case 3. $a^2 = z, ab = ba$
We may assume without any loss of generality that $b^2 \neq 1$ and $(ab)^2 \neq 1$, otherwise we may relabel and get to Case 1. Using the above relations in equation (5) we get

$$XX^{(-1)} - 4 = (\epsilon_1 + \epsilon_2\epsilon_3)(a+a^{-1}) + (\epsilon_2 + \epsilon_1\epsilon_3)(b+b^{-1}) + (\epsilon_3 + \epsilon_1\epsilon_2 z)(ab + ab^{-1}z).$$

If X has an odd number of negative signs, then

$$XX^{(-1)} - 4 = \pm a(1-z)(b+b^{-1}z)$$

By Lemma 4,

$$(XX^{(-1)} - 4)(1-z) = 0 \Longrightarrow (XX^{(-1)} - 4) = 0.$$

However, if X is PTA(4), X would have to be of the "commuting involution" or "quaternion" type. Since it is neither, this case is impossible. If X has an even number of negative signs, then

$$\begin{aligned}(XX^{(-1)} - 4)(1-z) &= (\pm 2a(1+z) \pm 2(b+b^{-1}) \pm a(1+z)(b+b^{-1}z))(1-z)\\ &= \pm 2(b+b^{-1})(1-z).\end{aligned}$$

Then

$$(XX^{(-1)} - 4)(1 - z) = 0$$

implies that b is equal to one of b^{-1}, bz or $b^{-1}z$. The first two choices yield $z = 1$ which is impossible hence the only remaining possibility is that $b = b^{-1}z$ which implies that $b^2 = z$. But if $a^2 = b^2 = z$, then $(ab)^2 = 1$, a possibility we already dismissed.

Case 4. $a^2 = z, ab = baz$

Using the above relations in equation (5) we get

$$XX^{(-1)} - 4 = (\epsilon_1 + \epsilon_2\epsilon_3)a(1 + z) + (\epsilon_2 + \epsilon_1\epsilon_3 z)(b + b^{-1}) + (\epsilon_3 + \epsilon_1\epsilon_2)(ab + ab^{-1}).$$

If X has an odd number of negative signs, then

$$XX^{(-1)} - 4 = \pm(1 - z)(b + b^{-1}).$$

By Lemma 4,

$$(XX^{(-1)} - 4)(1 - z) = 0 \Longrightarrow (XX^{(-1)} - 4) = 0.$$

However, if X is PTA(4), X would have to be of the "commuting involution" or "quaternion" type. In this case X is of the quaternion type if $b^2 = z$ as well. If X has an even number of negative signs, then

$$\begin{aligned}(XX^{(-1)} - 4)(1 - z) &= (\pm 2a(1 + z) \pm (1 + z)(b + b^{-1}) \pm 2(ab + ab^{-1}))(1 - z)\\ &= \pm 2(1 - z)(ab + ab^{-1})\end{aligned}$$

In that case,

$$(XX^{(-1)} - 4)(1 - z) = 0$$

implies that $ab = ab^{-1}z$ which leads to $b = b^{-1}z$ or $b^2 = z$. This gives us that $(ab)^2 = abab = bazab = z$. Again X is of the "quaternion" type.

Recall from the discussion in Section 2 that X being a PTA(4) implies that X must have an odd number of minus signs and be either of the "sporadic" (Fano plane) type, the "commuting involution" type or the "quaternion" type. For 2-groups, Lagrange's theorem rules out the "sporadic" case and so a PTA(4) is either of "commuting involution" type or "quaternion" type. Our experience in groups of order 16 and 64 indicates that the "commuting involution" PTA(4) is extremely common in the construction of difference sets; the "quaternion" type is rare but does occur.

Most groups of order 64 which possess a $(64, 28, 12)$ difference set possess at least one difference set which is the product of three PTA(4)s. A computer search reveals that of the 259 groups with a difference set, 212 groups allow such a product construction. However, the abelian group $C_8 \times C_8$ contains many difference sets but, as this abelian group only has three involutions, none of these difference sets may be constructed using a product of three PTA(4)s. Some other construction is necessary to explain the difference sets in the group $C_8 \times C_8$.

The groups of order sixteen are small enough that *all* 27 difference sets in these groups have a simple description as a product of two PTA(4)s. This is the result of our next theorem. The last section then explicitly gives the PTA(4)s used to construct each of these $(16, 6, 2)$ difference sets.

Theorem 3 *Up to equivalence, all* $(16, 6, 2)$ *difference sets may be written in the form* $\hat{D} = T^{-}_{a_1,b_1}T^{-}_{a_2,b_2}$ *for some collection of group elements* a_1, b_1, a_2, b_2.

Proof By equation (3) we have $\hat{D} = G - 2D = -(T(1+z) + F(1-z)) = -(T^{-}_{a,b}(1+z) + F(1-z))$. We will write out this expression for each choice of $T^{-}_{a,b}$ and $F = Xg$.

Case (a): $a^2 = 1, ab = ba$

1. $X = 1 - a - b - ab$. $\hat{D} = -((1 - a - b - ab)(1 + z) + (1 - a - b - ab)g(1 - z)) = (T^{-}_{a,bz})(T^{-}_{z,(ag)^{-1}})ag$.

2. $X = -1 + a - b - ab$. $\hat{D} = -((1 - a - b - ab)(1 + z) + (-1 + a - b - ab)g(1 - z)) = (T^{-}_{a,b})(T^{-}_{z,(ag)^{-1}})agz$.

3. $X = -1 - a + b - ab$. $\hat{D} = -((1 - a - b - ab)(1 + z) + (-1 - a + b - ab)g(1 - z)) = (T^{-}_{az,bz})(T^{-}_{z,(ag)^{-1}})ag$.

4. $X = -1 - a - b + ab$. $\hat{D} = -((1 - a - b - ab)(1 + z) + (-1 - a - b + ab)g(1 - z)) = (T^{-}_{az,b})(T^{-}_{z,(ag)^{-1}})ag$.

Notice that each $T^{-}_{*,*}$ in the factorization of $\hat{D}$ is a PTA(4) of the commuting involution type.

Case (b): $a^2 = 1, ab = baz$ and

Case (c): $a^2 = z, ab = ba$ do not yield difference sets as a result of Theorems 1 and 2.

Case (d): $a^2 = z, ab = baz$

1. $X = 1 - a - b - ab$. $\hat{D} = -((1 - a - b - ab)(1 + z) + (1 - a - b - ab)g(1 - z)) = (T^{-}_{az,b})(T^{-}_{z,(ag)^{-1}})ag$.

2. $X = -1 + a - b - ab$. $\hat{D} = -((1 - a - b - ab)(1 + z) + (-1 + a - b - ab)g(1 - z)) = (T^{-}_{az,bz})(T^{-}_{z,(ag)^{-1}})agz$.

3. $X = -1 - a + b - ab$. $\hat{D} = -((1 - a - b - ab)(1 + z) + (-1 - a + b - ab)g(1 - z)) = (T^{-}_{a,b})(T^{-}_{z,(ag)^{-1}})ag$.

4. $X = -1 - a - b + ab$. $\hat{D} = -((1 - a - b - ab)(1 + z) + (-1 - a - b + ab)g(1 - z)) = (T^{-}_{a,bz})(T^{-}_{z,(ag)^{-1}})ag$.

5. $X = -1 - a + b + ab$. $\hat{D} = -((1 - a - b - ab)(1 + z) + (-1 - a + b + ab)g(1 - z)) = (T^{-}_{bz,a})(T^{-}_{z,(ag)^{-1}})ag$.

6. $X = -1 + a - b + ab$. $\hat{D} = -((1 - a - b - ab)(1 + z) + (-1 + a - b + ab)g(1 - z)) = (T^{-}_{b,az})(T^{-}_{z,(ag)^{-1}})agz$.

7. $X = -1 + a + b - ab$. $\hat{D} = -((1 - a - b - ab)(1 + z) + (-1 + a + b - ab)g(1 - z)) = (T^{-}_{bz,az})(T^{-}_{z,(ag)^{-1}})agz$.

8. $X = 1 + a + b + ab$. $\hat{D} = -((1 - a - b - ab)(1 + z) + (1 + a + b + ab)g(1 - z)) = (T^{-}_{b,a})(T^{-}_{z,(ag)^{-1}})agz$.

   Notice that in each case $\hat{D}$ has the form $\hat{D} = T_{a_1,b_1}T_{a_2,b_2}g'$ where g' is some element of G. By considering $\hat{D}g'^{-1} = (G - 2D)g'^{-1} = G - 2D'$ we get an equivalent difference set of the form $T_{a_1,b_1}T_{a_2,b_2}$. We also notice that if $F = Xg$ corresponds to $\hat{D} = T_1T_2g'$ then $-Xg$ corresponds to $\hat{D} = T_1T_2g'z$ both of which are translation equivalent to T_1T_2. Therefore we have not listed them above.

The strategy for finding difference sets in groups of order 16 will be as follows.

1. For each group G we identify a special commuting involution z in G.

2. We find, up to equivalence in $G/\langle z\rangle$, all perfect ternary arrays $\overline{T}$ in $G/\langle z\rangle$.

3. Each $\overline{T}$ is the image of an element T in G. We verify that every automorphism of $G/\langle z\rangle$ extends to an automorphism of G and so we have, up to equivalence in G, all possible T that might occur in the equation $\hat{D} = -(T(1 + z) + F(1 - z))$.

4. For each such T, we identify all F such that $\hat{D} = -(T(1 + z) + F(1 - z))$ gives a difference set. The support of F is a translate of the support of T; we apply Theorem 2 in our search for F. of $T_{a,bz}$. Theorem 3 leads to a comprehensive list of the possibilities of F.

5. Once our list is complete, we weed out equivalent solutions using our knowledge of the automorphisms of G.

The cyclic group C_{16} does not have a difference set; this is “Turyn's bound” (see, for example, [8], Theorem 4.30, p. 161 or [3], p. 14) It then follows that the dihedral group D_8 does not have a $(16, 6, 2)$ difference set ([3], p. 16.) The remaining 12 groups of order 16 do have difference sets. The elementary abelian group C_2^4 has a single difference set $D = 1 + a + b + c + d + abcd$ where $\{a, b, c, d\}$ is a generating set for the group. (This exercise is left for the reader; it is straightforward to write $\hat{D}$ as a product of two PTAs. For example, if $D = 1 + a + b + c + d + abcd$ then $\hat{D} = abT^{-}_{a,b}T^{-}_{cd,cab}$.)

The remaining eleven groups will be handled as follows. In the remaining three abelian groups, we choose z so that $G/\langle z\rangle$ is isomorphic to $C_4 \times C_2$. (In *GAP*'s library, these are $[16, 2] \cong C_4 \times C_4$, $[16, 5] \cong C_8 \times C_2$ and $[16, 10] \cong C_4 \times C_2 \times C_2$.)

There are two groups in which the derived subgroup G' has order two and G/G' is isomorphic to $C_4 \times C_2$. Since G' is a characteristic subgroup, every automorphism of G fixes z and so our choice of z is unique. (In *GAP*'s SmallGroup library, these groups are [16,3], [16,4], [16,6].)

There are two groups in which the center of G is of order two and $G/Z(G)$ is isomorphic to the dihedral group D_4. (In *GAP*'s library, these are [16,8], [16,9].)

There are three groups in which the derived subgroup G' has order two and G/G' is isomorphic to C_2^3. (In *GAP*'s library, these are [16,11], [16,12], [16,13].)

From Theorem 2, we will require that F be a PTA in G unless, given $T_{a,b}$, it happens that $z = [a,b] = a^2 = b^2$ and $\langle a, b\rangle$ generate a quaternion subgroup. Only four groups of order 16 have a subgroup isomorphic to Q_8. There are, in *GAP*'s library, the groups [16,8], [16,9], [16,12], [16,13]. So, in most cases, we may assume F is a PTA(4).

Example 1

Let $G = C_4 \times C_4 = \langle x, y : x^4 = y^4 = 1\rangle$. There are several choices for a commuting involution z in G. The automorphism group of G is transitive on involutions of G so we may assume, without loss of generality, that $z = x^2$. Then $G/\langle z\rangle \simeq C_2 \times C_4$. We first look for possible $\overline{T}$ which are PTA(4) in $G/\langle z\rangle$. Next we choose F so that the union of the support of F and T forms a transversal H of $\langle z\rangle$ in G as well as gives rise to a difference set according to equation (1).

There are three possibilities for T up to equivalence in $G/\langle z\rangle$.

1. $\overline{T} = T_{\overline{x},\overline{y}}$, $T_{x,y} = 1 - x - y - xy$ and $Supp(F) = y^2 Supp(T^-_{x,y})$,
2. $\overline{T} = T_{\overline{y^2},\overline{y}}$, $T_{y^2,y} = 1 - y - y^2 - y^3$ and $Supp(F) = xSupp(T^-_{y,y^2})$,
3. $\overline{T} = T_{\overline{y^2},\overline{x}}$, $T_{y^2,x} = 1 - x - y^2 - xy^2$ and $Supp(F) = ySupp(T^-_{x,y^2})$,

Since the group G is abelian, the element F must be a perfect ternary array in G and so its translate is also. We are essentially into Case (a) of Theorem 3 (with $a := y^2, b := x, z := x^2$) and there are four cases. Any Hadamard difference set $\hat{D}$ is equivalent to one of the following four:

1. $T^-_{y^2,x} T^-_{x^2,y}$
2. $T^-_{y^2,x^3} T^-_{x^2,y}$
3. $T^-_{y^2,y} T^-_{x^2,x}$
4. $T^-_{y^2,x^2y} T^-_{x^2,x}$

Since there is an automorphism of $C_4 \times C_4$ which fixes y and transposes x and x^3, the first two solutions, above, are equivalent. But the remainder are mutually inequivalent and so there are three inequivalent $(16, 6, 2)$ difference sets in $C_4 \times C_4$.

Example 2 Let's examine the group $[16, 3]$ in *GAP*'s SmallGroup library. In this case $G \cong (C_4 \times C_2) \rtimes C_2 = \langle x, y, z : x^4 = y^2 = z^2 = [x, y] = [y, z] = 1, zxz = xy\rangle$, a semidirect product of $C_4 \times C_2$ with an element of order 2. This group has a unique nonidentity element y in the derived subgroup and $G/\langle y\rangle$ is isomorphic to $C_4 \times C_2$. There is no subgroup of G isomorphic to the quaternions and so we are in Case (a) of Theorem 3. In this case all four solutions given there are inequivalent.

In a similar manner, we can work through the remaining groups of order 16. Each of the 27 difference sets discovered by Kibler can be rediscovered in this manner. The results are listed below.

4 All (16,6,2) Difference sets

We list all twenty-seven $(16, 6, 2)$ difference sets obtained by our methods in the previous sections. The groups are ordered according to *GAP*'s SmallGroups library of groups of order 16.

1. $C_{16} = \langle x : x^{16} = 1\rangle$.
   There are no difference sets in C_{16}.
2. $G = C_4 \times C_4 = \langle x, y : x^4 = y^4 = 1\rangle$.
   (a) $T^-_{y^2,x}T^-_{x^2,y}$
   (b) $T^-_{y^2,x}T^-_{x^2y^2,y}$
   (c) $T^-_{y^2,x}T^-_{x^2y^2,xy}$
3. $(C_4 \times C_2) \rtimes C_2 = \langle x, y, z : x^4 = y^2 = z^2 = [x, y] = [y, z] = 1, zxz = xy\rangle$.
   (a) $T^-_{y,x}T^-_{x^2,z}$
   (b) $T^-_{y,x}T^-_{x^2y,z}$
   (c) $T^-_{y,x}T^-_{x^2,xz}$
   (d) $T^-_{y,x}T^-_{x^2y,xz}$
4. $C_4 \rtimes_{-1} C_4 = \langle x, y : x^4 = y^4 = 1, yxy^{-1} = x^{-1}\rangle$.
   (a) $T^-_{y^2,x}T^-_{x^2y^2,y}$
   (b) $T^-_{y^2,x}T^-_{x^2,xy}$
   (c) $T^-_{y^2,x}T^-_{x^2y^2,xy}$
5. $C_8 \times C_2 = \langle x, y : x^8 = y^2 = [x, y] = 1\rangle$.
   (a) $T^-_{y,x^2}T^-_{x^4,x}$
   (b) $T^-_{y,x^2}T^-_{x^4y,x}$
6. The modular group, $M_{16} = \langle x, y : x^8 = y^2 = 1, yxy^{-1} = x^5\rangle$.
   (a) $T^-_{x^4,x}T^-_{y,x^2}$

(b) $T^{-}_{x^4,x}T^{-}_{y,x^6}$

7. The dihedral group, $D_8 = \langle x, y : x^8 = y^2 = 1, yxy = x^{-1}\rangle$.
There are no difference sets in D_8.

8. The semi-dihedral group, $SD_{16} = \langle x, y : x^8 = y^2 = 1, yxy = x^3\rangle$.

   (a) $T^{-}_{xy,x^2}T^{-}_{y,x^4}$

   (b) $T^{-}_{xy,x^2}T^{-}_{x^4,x}$

9. The generalized quaternion group, $Q_{16} = \langle x, y : x^8 = y^4 = 1, yxy^{-1} = x^{-1}, x^4 = y^2\rangle$.

   (a) $T^{-}_{x^5y,x^6}T^{-}_{x^6,x^7y}$

   (b) $T^{-}_{x^5y,x^6}T^{-}_{x^7y,xy}$

10. $C_4 \times C_2 \times C_2 = \langle x, y, z, x^4 = y^2 = z^2 = [x, y] = [x, z] = [y, z] = 1\rangle$.

    (a) $T^{-}_{x,y}T^{-}_{x^2,xyz}$

    (b) $T^{-}_{x,y}T^{-}_{x^2y,xz}$

11. $D_4 \times C_2 = \langle x, y, z : x^4 = y^2 = z^2 = 1 = [x, z] = [y, z]; yxy = x^3\rangle$.

    (a) $T^{-}_{y,z}T^{-}_{x^2,x^3y}$.

    (b) $T^{-}_{y,z}T^{-}_{x^2z,x^3y}$.

12. $Q_8 \times C_2 = \langle z, y, z : x^4 = y^4 = z^2 = x^2y^2 = yxy^{-1}x = [x, z] = [y, z] = 1\rangle$.

    (a) $T^{-}_{x^2,x}T^{-}_{z,y}$

    (b) $T^{-}_{x^2,x}T^{-}_{y,xz}$

13. $(C_4 \times C_2) \rtimes C_2 = \langle x, y, z : x^4 = y^2 = z^2 = [x, y] = [x, z] = 1, zyz = x^2y\rangle$.

    (a) $T^{-}_{y,x^2}T^{-}_{z,x^3z}$

    (b) $T^{-}_{y,x^2}T^{-}_{x^2y,x}$

14. $C_2 \times C_2 \times C_2 \times C_2 = \langle x, y, z, w : x^2 = y^2 = z^2 = w^2 = 1\rangle$.

    (a) $\hat{D} = (T^{-}_{x,y})(T^{-}_{w,z})$

Acknowledgements The second author's enthusiasm for Hadamard difference sets and perfect ternary arrays is due to long conversations with John F. Dillon (Mathematics Research Group, National Security Agency.) He is grateful for John Dillon's ideas and mentoring. (It is possible that *all* of the results in this paper are known to Dillon but have not appeared in print.)

The authors of this paper began collaborating on difference sets while the second author was on sabbatical from Central Michigan University and visiting James A. Davis, University of Richmond. The support of Central Michigan University and the hospitality of Jim Davis and the University of Richmond are greatly appreciated. The first author wishes to acknowledge a Walter Williams Craigie grant from Randolph-Macon College for providing partial support. The authors also wish to thank an anonymous referee for many helpful suggestions improving the exposition of this paper.

References

[1] Arasu, K. T.; Dillon, J. F. Perfect ternary arrays. Difference sets, sequences and their correlation properties (Bad Windsheim, 1998), 1–15, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 542, Kluwer Acad. Publ., Dordrecht, 1999.

[2] E.F. Assmus, Jr., C.J. Salwach, The (16,6,2) designs, Internat. J. Math. & Math. Sci., v. 2, no. 2 (1979), 261-281.

[3] J.F. Dillon, Variations on a scheme of McFarland for noncyclic difference sets,. Combin. Theory. (A), Vol. 40, (1985) pp. 9-21.

[4] Unpublished work of John Dillon and Ken Smith, 1990.

[5] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.10; 2007. (http://www.gap-system.org)

[6] Kibler, Robert E., A summary of noncyclic difference sets, $k < 20$, J. Combinatorial Theory Ser. A 25 (1978), no. 1, 62–67.

[7] Kroeger, Miller, Mooney, Shepard, Determining Existence of Hadamard Difference Sets in Groups of Order 144, Undergraduate Research Report, 2007, Central Michigan University. (available at http://www.shsu.edu/ kws006/REU2007/KroegerMillerMooneyShepard.pdf.)

[8] E. S. Lander, Symmetric designs: an algebraic approach, Cambridge University Press, 1983.

[9] Wild, Marcel, The groups of order 16 made easy, MAA Monthly, January 2005, 20-31.