Journal of Algebraic Combinatorics, 22, 181–187, 2005
© 2005 Springer Science + Business Media, Inc. Manufactured in The Netherlands.

A Ring Theoretic Construction of Hadamard Difference Sets in $\mathbb{Z}_8^n \times \mathbb{Z}_2^n$

XIANG-DONG HOU xhou@tarski.math.usf.edu
Department of Mathematics and Statistics, Wright State University, Dayton, Ohio 45435

Received August 22, 2002; Revised January 26, 2005; Accepted February 11, 2005

Abstract. Let $S = \mathrm{GR}(2^3, n)$ be the Galois ring of characteristic 2^3 and rank n and let $R = S[X]/(X^2,\ 2X - 4)$. We give an explicit construction of Hadamard difference sets in $(R, +) \cong \mathbb{Z}_8^n \times \mathbb{Z}_2^n$.

Keywords: bent function, finite Frobenius local ring, Galois ring, hadamard difference set

1. Introduction

Let G be a finite group of order v. A subset $D \subset G$ is called a difference set in G with parameters (v, k, λ) if $|D| = k$ and $d_1 d_2^{-1}$ $(d_1, d_2 \in D,\ d_1 \neq d_2)$ represents each element in $G \setminus \{e\}$ exactly λ times. A difference set with parameters $(v, k, \lambda) = (4N^2, 2N^2 - N, N^2 - N)$ is called a Hadamard difference set. Initially studied by Menon [8], Hadamard difference sets have received much attention ever since. A lot is known about Hadamard difference sets: For example, in finite 2-groups, every nontrivial difference set is either a Hadamard difference set or a complement of a Hadamard difference set [8]. A finite abelian 2-group G of order 2^{2d+2} has a Hadamard difference if and only if $\exp(G) \leq d + 2$ [10, 6]. For a survey on Hadamard difference sets, the reader is referred to [2] by Davis and Jedwab.

The existence of Hadamard difference sets in abelian 2-groups with $|G| = 2^{2d+2}$ and $\exp(G) \leq d + 2$ was proved by Kraemer [6]. The construction in [6] is algorithmic. There are still interests in more explicit constructions of Hadamard difference sets in abelian 2-groups, as stated in one of the open problems in [2]. It seems that suitable ring structures on the groups are the key to explicit constructions. (The reader may see [3] and [4] for ring theoretic constructions of other types of difference sets.) In this note, we consider a finite ring $R = S[X]/(X^2,\ 2X - 4)$ where $S = \mathrm{GR}(2^3, n)$ is the Galois ring of characteristic 2^3 and rank n [7]. We give a simple and explicit construction of Hadamard difference sets in $(R, +) \cong \mathbb{Z}_8^n \times \mathbb{Z}_2^n$.

Research supported by NSA grant MDA 904-02-1-0080.
Present address. Department of Mathematics, University of South Florida, Tampa, FL 33620.

2. The construction

Let $S = \mathrm{GR}(2^3, n)$ and

$$R = S[X]/(X^2,\ 2X - 4).$$

Denote the image of X in R by x. R is a local ring with maximal ideal $2R + xR$. Note that $2R + xR$ is not a principal ideal, hence R is not a chain ring [7]. However, R has a unique minimal ideal $4R$, hence R is a finite Frobenius local ring [4]. In fact, the complete ideal lattice of R is as follows:

$$\begin{tikzcd}[arrows=-]
 & R \arrow[d] & \\
 & 2R + xR \arrow[dl] \arrow[dr] & \\
2R \arrow[dr] & & xR \arrow[dl] \\
 & 4R \arrow[d] & \\
 & \{0\} &
\end{tikzcd}$$

It is easy to see that $(R, +) \cong \mathbb{Z}_8^n \times \mathbb{Z}_2^n$ and that as an abelian group,

$$(2R + xR)/4R \cong \mathbb{Z}_2^{2n}.$$

Let $\mathrm{Tr} : S \to \mathbb{Z}_8$ be the trace map of S. Define

$$\begin{array}{rccc} \lambda : & S[X] & \to & \mathbb{Z}_8 \\ & a_0 + a_1X + \cdots & \mapsto & \mathrm{Tr}(a_0 + 2a_1) \end{array} \tag{2.1}$$

Then $(X^2,\ 2X - 4) \subset \ker\lambda$, hence λ induces a $\mathbb{Z}_8$-linear map $\bar{\lambda} : R \to \mathbb{Z}_8$. Let $\xi = e^{2\pi i/8}$. Then $\chi(\ ) = \xi^{\bar{\lambda}(\ )}$ is a character of $(R, +)$. Note that the minimal ideal $4R \not\subset \ker\chi$. Hence χ is a generating character of $(R, +)$, i.e., every character of $(R, +)$ is of the form $\chi_a(\ ) = \chi(a\,\cdot)$ for some $a \in R$ [4]. Let

$$V = \{v \in 4S : \mathrm{Tr}(v) = 0\}. \tag{2.2}$$

V is an $(n-1)$-dimensional vector space over $\mathbb{Z}_2$. Note that

$$\begin{array}{l} (S/2S) \times 4S \to 4\mathbb{Z}_8 \cong \mathbb{Z}_2 \\ (a + 2S,\ v) \mapsto \mathrm{Tr}(av), \qquad a \in S \end{array}$$

is a nondegenerate $\mathbb{Z}_2$-bilinear form. Thus

$$\{a + 2S \in S/2S : \mathrm{Tr}(av) = 0 \text{ for all } v \in V\}$$

is a 1-dimensional $\mathbb{Z}_2$-subspace of $S/2S$. Therefore, for $a \in S$,

$$\mathrm{Tr}(av) = 0 \text{ for all } v \in V \quad \text{iff } a \equiv 0 \text{ or } 1 \pmod{2S}. \tag{2.3}$$

Let T be the Teichmüller set of S and put $T^* = T\backslash\{0\}$. Define

$$D = T^*(1 + xT + 2T + V) \subset R\backslash(2R + xR).$$

Clearly, $|D| = (2^n - 1)2^{3n-1}$. For any subgroup $H \subset (R, +)$, we use $H^\perp$ to denote the group of characters of $(R, +)$ which are principal on H. The following lemma gives the interesting character value distribution of D.

Lemma 2.1 *Let ψ be a nonprincipal character of $(R, +)$. We have*

$$\begin{cases} |\psi(D)| = 2^{2n-1}, & \text{if } \psi \notin (4R)^\perp, \\ \psi(D) = 0, & \text{if } \psi \in (4R)^\perp\backslash(2R + xR)^\perp, \\ \psi(D) = -2^{3n-1}, & \text{if } \psi \in (2R + xR)^\perp \setminus R^\perp. \end{cases} \tag{2.4}$$

Proof:
Case 1. $\psi \notin (4R)^\perp$. In this case, $\psi = \chi_a$ for some $a \in R^\times$, where $R^\times$ is the multiplicative group of R and $R^\times = T^*(1 + xT + 2T + 4T)$. We may assume that $a = 1 + xb + 2c + 4d$ $(b, c, d \in T)$. Thus

$$\begin{aligned} \chi_a(D) &= \sum_{\substack{\epsilon\in T^*, v\in V \\ w,z\in T}} \chi(\epsilon(1 + xw + 2z + v)(1 + xb + 2c + 4d)) \\ &= \sum_{\substack{\epsilon\in T^* \\ w,z\in T}} \chi(\epsilon(1 + xw + 2z)(1 + xb + 2c + 4d)) \sum_{v\in V} \chi(\epsilon v). \end{aligned}$$

It follows from (2.3) that

$$\sum_{v\in V} \chi(\epsilon v) = \begin{cases} |V|, & \text{if } \epsilon = 1, \\ 0, & \text{otherwise.} \end{cases}$$

Hence

$$\begin{aligned}\chi_a(D) &= |V|\sum_{w,z\in T}\chi((1+xw+2z)(1+xb+2c+4d))\\ &= |V|\sum_{w,z\in T}\chi(1+xb+2c+4d+xw+2xwc+2z+2xzb+4zc)\\ &= |V|\sum_{w,z\in T}\chi(1+2b+2c+4d+2w+4wc+2z+4zb+4zc) \quad \text{(by (2.1))}.\end{aligned}$$

Therefore,

$$|\chi_a(D)| = |V|\left|\sum_{w\in T}\chi(2w+4wc)\right|\left|\sum_{z\in T}\chi(2z+4(b+c)z)\right|.$$

In the above,

$$\begin{aligned}\left|\sum_{w\in T}\chi(2w+4wc)\right| &= \left|\sum_{w\in T}\chi(2w^2+4wc)\right|\\ &= \left|\sum_{w\in T}\chi(2(w+c)^2)\right|\\ &= \left|\sum_{w\in T}\chi(2w)\right|\\ &= 2^{\frac{n}{2}},\end{aligned}$$

where the last step follows from the well known result about the exponential sum over the Teichmüller set of GR(4, n) [1, 11]. Of course, we also have $|\sum_{z\in T}\chi(2z+4(b+c)z)| = 2^{n/2}$. Therefore,

$$|\chi_a(D)| = |V|2^n = 2^{2n-1}.$$

Case 2. $\psi \in (4R)^\perp\backslash(2R+xR)^\perp$. In this case we may write $\psi = \chi_a$ where $a = xb+2c+4d$ ($b, c, d \in T$, b and c not both 0). We then have

$$\begin{aligned}\chi_a(D) &= \sum_{\substack{\epsilon\in T^*, v\in V\\ w,z\in T}}\chi(\epsilon(1+xw+2z+v)(xb+2c+4d))\\ &= |V|\sum_{\substack{\epsilon\in T^*\\ w,z\in T}}\chi(\epsilon(xb+2c+4d+2xwc+2xzb+4zc))\\ &= |V|\left[\sum_{\epsilon\in T^*}\chi(\epsilon(2b+2c+4d))\right]\left[\sum_{w\in T}\chi(4wc)\right]\left[\sum_{z\in T}\chi(4z(b+c))\right].\end{aligned}$$

At least one of c and $b + c$ is nonzero. Thus

$$\left[\sum_{w \in T} \chi(4wc)\right]\left[\sum_{z \in T} \chi(4z(b+c))\right] = 0.$$

Case 3. $\psi \in (2R + xR)^{\perp} \backslash R^{\perp}$. We can assume that $\psi = \chi_4$. Clearly,

$$\chi_4(D) = |T|^2|V| \sum_{\epsilon \in T^*} \chi(4\epsilon) = -|T|^2|V| = -2^{3n-1}.$$

□

Theorem 2.2 *Let* $E \subset (2R + xR)/4R \cong \mathbb{Z}_2^{2n}$ *be any Hadamard difference set. Let* $\bar{E} \subset 2R + xR$ *be the preimage of* E. *Then* $D \cup \bar{E}$ *is a Hadamard difference set in* $(R, +)$.

Proof: First we have

$$|D \cup \bar{E}| = |D| + |4R||E| = (2^n - 1)2^{3n-1} + 2^n(2^{2n-1} - 2^{n-1}) = 2^{4n-1} - 2^{2n-1}.$$

Let ψ be any nonprincipal character of $(R, +)$. By the well known characterization of difference sets in abelian groups in terms of character values [10], we only have to show that $|\psi(D \cup \bar{E})| = 2^{2n-1}$. We have

$$\psi(\bar{E}) = \begin{cases} 0, & \text{if } \psi \notin (4R)^{\perp}, \\ \pm 2^n 2^{n-1}, & \text{if } \psi \in (4R)^{\perp} \backslash (2R + xR)^{\perp}, \\ 2^n(2^{2n-1} - 2^{n-1}), & \text{if } \psi \in (2R + xR)^{\perp} \backslash R^{\perp}. \end{cases} \tag{2.5}$$

Combining (2.4) and (2.5), we always have $|\psi(D \cup \bar{E})| = 2^{2n-1}$. □

In the above construction, there are two independent pieces: a shell D in $R \backslash (2R + xR)$ and a core $\bar{E}$ in $2R + xR$. We mention that this kind of shell-nesting method is common in constructions of Latin square type partial difference sets [5].

We compare the above construction with known constructions of Hadamard difference sets in finite abelian 2-groups. First, if the group is of the form $H \times H$, there is a very general construction of Hadamard difference sets using finite local rings [4]. However, when n is odd, $\mathbb{Z}_8^n \times \mathbb{Z}_2^n$ is not of the form $H \times H$. Next, we consider the Menon construction [8]: Let G_1 and G_2 be finite groups and $D_1 \subset G_1$, $D_2 \subset G_2$. Then

$$(D_1 \times (G_2 \backslash D_2)) \cup ((G_1 \backslash D_1) \times D_2) \tag{2.6}$$

is a Hadamard difference set in $G_1 \times G_2$ if and only if D_i is a Hadamard difference set in G_i for $i = 1, 2$. When $G_1 \neq 0$ and $G_2 \neq 0$, we call a subset in $G_1 \times G_2$ of the type (2.6) decomposable.

Proposition 2.3 *In Theorem* 2.2, *if* $D \cup \bar{E}$ *is decomposable in* $(R, +)$, *then* E *is decomposable in* $(2R + xR)/4R \cong \mathbb{Z}_2^{2n}$.

Proof: Assume that $R = G_1 \times G_2$, $(G_i \neq 0,\ i = 1, 2)$, $D_i \subset G_i$ $(i = 1, 2)$ and

$$D \cup \bar{E} = (D_1 \times (G_2 \backslash D_2)) \cup ((G_1 \backslash D_1) \times D_2).$$

Note that all elements in D have order 8 and all elements in $\bar{E}$ have order ≤ 4. Let $H_i = \{g \in G_i : 4g = 0\}$ and put $F_i = D_i \cap H_i$ $(i = 1, 2)$. Then $2R + xR = H_1 \times H_2$ and

$$\bar{E} = (F_1 \times (H_2 \backslash F_2)) \cup ((H_1 \backslash F_1) \times F_2). \tag{2.7}$$

We have

$$\mathbb{Z}_2^{2n} \cong \frac{2R + xR}{4R} = \frac{H_1}{4G_1} \times \frac{H_2}{4G_2},$$

where $H_i/4G_i \neq 0$ $(i = 1, 2)$. (Otherwise we would have $\operatorname{rank}(\frac{H_1}{4G_1} \times \frac{H_2}{4G_2}) < 2n$.) We claim that F_i is a union of cosets of $4G_i$ in H_i $(i = 1, 2)$. If $F_i = \emptyset$ or H_i for some $i = 1$ or 2, the claim is obviously true. So assume that $F_i \neq H_i$ $(i = 1, 2)$. Choose a nonprincipal character ψ_2 of H_2 such that $\psi_2(F_2) \neq 0$. Let ψ_1 be any character of H_1 which is not principal on $4G_1$. Then $\psi_1 \times \psi_2$ is a character of $H_1 \times H_2 = 2R + xR$ which is nonprincipal on $4G_1 \times 4G_2 = 4R$. Thus

$$0 = (\psi_1 \times \psi_2)(\bar{E}) = \psi_1(F_1)\psi_2(H_2 \backslash F_2) + \psi_1(H_1 \backslash F_1)\psi_2(F_2) = -2\psi_1(F_1)\psi_2(F_2).$$

It follows that $\psi_1(F_1) = 0$ for all $\psi_1 \notin (4G_1)^{\perp}$. Therefore F_1 is a union of cosets of $4G_1$ in H_1. In the same way, F_2 is a union of cosets of $4G_2$ in H_2. Mapping both sides of (2.7) to $\frac{2R+xR}{4R} = \frac{H_1}{4G_1} \times \frac{H_2}{4G_2}$, we have

$$E = \left[\tilde{F}_1 \times \left(\frac{H_2}{4G_2} \Big\backslash \tilde{F}_2\right)\right] \cup \left[\left(\frac{H_1}{4G_1} \Big\backslash \tilde{F}_1\right) \times \tilde{F}_2\right]$$

where $\tilde{F}_i$ is the image of F_i in $H_i/4G_i$. Thus E is decomposable. □

Hadamard difference sets in $\mathbb{Z}_2^{2n}$ are precisely supports of bent functions on $\mathbb{Z}_2^{2n}$ [9]. There are many indecomposable bent functions. For example, any bent function on $\mathbb{Z}_2^{2n}$ of degree n is indecomposable [9]. Choose any indecomposable bent function on $\mathbb{Z}_2^{2n}$ and let E be the corresponding indecomposable Hadamard difference set in $\mathbb{Z}_2^{2n}$. Then by Proposition 2.3, the Hadamard difference set $D \cup \bar{E}$ in Theorem 2.2 is indecomposable hence can not be obtained from the Menon construction.

The construction in [6] works for all abelian groups G with $|G| = 2^{2d+2}$ and $\exp(G) \leq d + 2$. However, we find it difficult to compare the constructions in this note and in [6] because of the algorithmic nature of the latter.

References

1. S. Boztaş, R. Hammons, and P.V. Kumar "4-phase sequences with near-optimum correlation properties," *IEEE Trans. Inform. Theory* **38** (1992), 1101–1113.
2. J.A. Davis and J. Jedwab, "A survey of Hadamard difference sets," in *Groups, Difference Sets, and the Monster*, K. T. Arasu et al. (Eds.), de Gruyter, New York, 1996, pp. 145–156.
3. X. Hou, "Bent functions, partial difference sets and quasi-Frobenius local rings," *Des. Codes Cryptogr.* **20** (2000), 251–268.
4. X. Hou, "Rings and constructions of partial difference sets," *Discrete Math.* **270** (2003), 149–176.
5. X. Hou and A. Nechaev, A construction of finite Frobenius rings and its applications to partial difference sets, preprint.
6. R.G. Kraemer, "Proof of a conjecture on Hadamard 2-groups," *J. Combin. Theory A* **63** (1993), 1–10.
7. B.R. McDonald, *Finite Rings with Identity*, Marcel Dekker, New York, 1974.
8. P.K. Menon, "On difference sets whose parameters satisfy a certain relation," *Proc. Amer. Math. Soc.* **13** (1962), 739–745.
9. O.S. Rothaus, "On "bent" functions," *J. Combin. Theory A* **20** (1976), 300–305.
10. R.J. Turyn, "Character sums and difference sets," *Pacific J. Math.* **15** (1965), 319–346.
11. K. Yang, T. Helleseth, and P.V. Kumar, "On the weight hierarchy of Kerdock codes over $\mathbb{Z}_4$," *IEEE Trans. Inform. Theory* **42** (1996), 1587–1593.