Advances in Applied Mathematics 46 (2011) 94–108

Contents lists available at ScienceDirect

Advances in Applied Mathematics

www.elsevier.com/locate/yaama

Lam's power residue addition sets

Kevin Byard [a], Ron Evans [b,*], Mark Van Veen [c]

[a] Institute of Information and Mathematical Sciences, Massey University, Albany, North Shore, Auckland, New Zealand
[b] Department of Mathematics 0112, University of California at San Diego, La Jolla, CA 92093-0112, United States
[c] Varasco LLC, 2138 Edinburg Avenue, Cardiff by the Sea, CA 92007, United States

ARTICLE INFO

Article history:
Available online 8 October 2010

MSC:
primary 05B10
secondary 11A15, 11T22, 11T24

Keywords:
Qualified residue difference sets
Power residue difference sets
Cyclic difference sets
Power residue addition sets
Cross-correlation function
Cyclotomic numbers
Gauss sums
Jacobi sums

ABSTRACT

Classical n-th power residue difference sets modulo p are known to exist for $n = 2, 4, 8$. During the period 1953–1999, their nonexistence has been proved for all odd n and for $n = 6, 10, 12, 14, 16, 18, 20$. In 1976, Lam showed that *qualified* n-th power residue difference sets modulo p exist for $n = 2, 4, 6$, and he proved their nonexistence for all odd n and for $n = 8, 10, 12$. We further prove their nonexistence for $n = 14, 16, 18, 20$.

1. Introduction

For an integer $n > 1$, let p be a prime of the form $p = nf + 1$. Let H_n denote the set of (nonzero) n-th power residues in $\mathbb{F}_p^*$, where $\mathbb{F}_p$ is the field of p elements. For $\epsilon \in \{0, 1\}$, define $H_{n,\epsilon} = H_n \cup \{1 - \epsilon\}$. Note that $|H_{n,\epsilon}| = f + \epsilon$.

Fix $m \in \mathbb{F}_p^*$. In 1975, Lam [18] introduced *addition sets*, which generalize cyclic difference sets. He called $H_{n,\epsilon}$ an n-th power residue addition set modulo p if there exists an integer $\lambda > 0$ such that the list of differences $s - mt \in \mathbb{F}_p^*$ with $s, t \in H_{n,\epsilon}$ hits each element of $\mathbb{F}_p^*$ exactly λ times. If $m \in H_n$, such an addition set is a *classical* power residue difference set modulo p; see [3, p. 174]. If $m \notin H_n$,

* Corresponding author.
E-mail addresses: k.byard@massey.ac.nz (K. Byard), revans@ucsd.edu (R. Evans), mvanveen@ucsd.edu (M. Van Veen).

0196-8858/$ – see front matter
doi:10.1016/j.aam.2010.09.008

we call such an addition set a *qualified* power residue difference set modulo p with qualifier m; cf. [14,15].

The classical n-th power residue difference sets $H_{n,\epsilon}$ for $n \leqslant 8$ are the following [3, pp. 177–179]:

$$H_{2,\epsilon}, \quad \text{if } p > 3, \quad p \equiv 3 \pmod 4, \tag{1.1}$$

$$H_{4,\epsilon}, \quad \text{if } p > 5, \quad p = (1+8\epsilon) + 4y^2 \text{ for some odd } y, \tag{1.2}$$

$$H_{8,\epsilon}, \quad \text{if } p = (1+48\epsilon) + 8u^2 = (9+432\epsilon) + 64v^2, \text{ with integers } u, v. \tag{1.3}$$

It is known that $H_{n,\epsilon}$ is never a classical power residue difference set when n is odd [3, p. 177], $n = 6$ [3, p. 178], $n = 10$ [26], $n = 12$ [3, p. 179], $n = 14$ [21], $n = 16$ [9,25], $n = 18$ [1,2], and $n = 20$ [10,22]. These nonexistence results were obtained sporadically during the period 1953–1999. The cases with even $n > 20$ are open (see [3, p. 497]), but we conjecture that the list (1.1)–(1.3) is complete.

As was noted above, complete information on the existence of classical n-th power residue difference sets is known for all $n \leqslant 20$. The primary goal of this paper is to similarly obtain complete information on the existence of qualified n-th power residue difference sets for all $n \leqslant 20$.

The qualified n-th power residue difference sets for $n \leqslant 6$ with qualifier m are the following, due to Lam [18,19]:

$$H_{2,\epsilon}, \quad \text{if } p \equiv 1 \pmod 4, \ m \in \mathbb{F}_p^*, \ m \notin H_2, \tag{1.4}$$

$$H_{4,\epsilon}, \quad \text{if } p = (1+8\epsilon) + 16x^2 \text{ for some integer } x, \ m \in H_2, \ m \notin H_4, \tag{1.5}$$

$$H_{6,\epsilon}, \quad \text{if } p = (1+24\epsilon) + 108w^2 \text{ for some integer } w, \ m \in H_3, \ m \notin H_6. \tag{1.6}$$

It is shown in [19] that $H_{n,\epsilon}$ is never a qualified residue difference set when n is odd and when $n = 8$, $n = 10$, and $n = 12$. Lam's results for $n = 2, 4, 6, 8, 10, 12$ have also been obtained in the papers [14,15,4–6], whose authors were at the time unaware of Lam's work. For related addition sets formed by taking unions of index classes for p, see [20, Theorems 3.2–3.5].

In this paper, we accomplish our goal by showing that $H_{n,\epsilon}$ is never a qualified residue difference set when $n = 14, 16, 18, 20$. We also give a new proof of Lam's nonexistence result for odd n, in Section 2. Those looking to find new qualified residue difference sets may thus limit their search to the cases with even $n > 20$. However, we conjecture that the list (1.4)–(1.6) is complete.

It is well known that cyclic difference sets have applications in astronomy [7,12,13,17]. The first author was led to rediscover qualified residue difference sets while working on coded aperture imaging for the European Space Agency's International Gamma-Ray Astrophysical Laboratory (INTEGRAL) [8,27]. Difference sets have also been used in medical imaging [16,24].

Consider a qualified residue difference set $H = H_{n,0}$ modulo $p = nf + 1$ with qualifier m. For integer $t \pmod p$, define a binary array $A(t)$ by setting $A(t) = 1$ if $t \in H$, and $A(t) = 0$ otherwise. Define a post processing array $G(t)$ by setting $G(t) = 1 - n$ if $t \in mH$, and $G(t) = 1$ otherwise. The corresponding cross-correlation function F on the integers is given by

$$F(u) = \sum_{t=0}^{p-1} A(t)G(t+u).$$

Because H is a qualified residue difference set, $F(u) = f$ if $u \equiv 0 \pmod p$, and $F(u) = 0$ otherwise. Periodic two-valued cross-correlation functions such as $F(u)$ are potentially useful in signal processing, aperture synthesis, and image formation techniques.