Philippine Journal of Science
150 (6B): 1803-1810, December 2021
ISSN 0031 - 7683
Date Received: 21 Jun 2021

Difference Sets from Unions of Cyclotomic Classes of Orders 12, 20, and 24

Jose Maria P. Balmaceda[1] and **Benedict M. Estrella**[2]*

[1]Institute of Mathematics, College of Science,
University of the Philippines Diliman Quezon City, National Capital Region 1101 Philippines
[2]Mathematics Department, College of Science, Bulacan State University
Central Luzon Region 3000 Philippines

Let q be a prime of the form $q = nN + 1$ for integers $n \geq 1$ and $N > 1$. For $q < 10^5$, we show that difference sets in the additive group of the field $\mathrm{GF}(q)$ are obtained from unions of cyclotomic classes of orders $N = 12, 20,$ and 24 and determine all such unions using a computer search. We then determine if the difference sets are equivalent to known cyclotomic or modified cyclotomic quadratic, quartic, sextic, or octic difference sets or their complements. This fills the gaps in the literature on the existence of difference sets from unions of cyclotomic classes for the specified orders. In addition, we extend Baumert and Fredricksen's 1967 work on the construction of all inequivalent $(127, 63, 31)$-difference sets from unions of 18^{th}-cyclotomic classes of $GF(127)$ by constructing six inequivalent $(127, 64, 32)$-difference sets with zero added from unions of cyclotomic classes of order $N = 18$.

Keywords: difference set, cyclotomic class, cyclotomic number, unions

INTRODUCTION

Let G be a finite group of order v, D be a non-empty proper subset of G of cardinality k, and λ be any integer. Then D is a (v, k, λ)-difference set if each non-identity element of G can be written as a product $d_1 {d_2}^{-1}$ of elements of D in exactly λ ways. The difference set is cyclic, abelian, or non-abelian if the group G has the corresponding property. If G is an abelian group written additively, the defining condition is that every nonzero element of the group can be expressed as a difference $d_1 - d_2$ of elements of D in exactly λ ways.

Difference sets are closely related to finite geometries, designs, codes, and periodic sequences with favorable correlation properties. They are used for optical alignment, interpreting signals in the presence of noise, imaging astronomical events, constructing error-correcting codes, and facilitating processes in quantum informatics.

A powerful method for constructing difference sets in the additive groups of finite fields is cyclotomic construction. This idea of using cyclotomic classes of finite fields to produce difference sets goes back to Paley (1933) and was pursued vigorously in the succeeding decades as seen in works such as Dickson (1935), Chowla (1944), Lehmer (1953), Hall (1956), and Whiteman (1960), among others.

*Corresponding Author: benedict.estrella@bulsu.edu.ph

Let $n \geq 1$ and $N > 1$ be integers. Let q be a prime power of the form $q = nN + 1$. Let $(GF(q), +)$ denote the additive group of the finite field $GF(q)$ consisting of all field elements under addition. Let $GF(q)^*$ denote the cyclic group of all nonzero field elements under multiplication. Let α be a fixed primitive element of $GF(q)$, *i.e.* α is a generator of $GF(q)^*$. For a fixed N, the N subsets of $GF(q)$ given by ${C_i}^{(N,q)} = \left\{\alpha^{jN+i} : 0 \leq j \leq \frac{q-1}{N} - 1\right\}$ for $0 \leq i \leq N-1$ are called the N^{th}-cyclotomic classes of $GF(q)$, *i.e.* ${C_0}^{(N,q)}$ is the subgroup of $GF(q)^*$ consisting of all N^{th} powers in $GF(q)$ and ${C_i}^{(N,q)} = \alpha^i {C_0}^{(N,q)}$ for $1 \leq i \leq N-1$. If q is a prime we call the elements of ${C_0}^{(N,q)}$ the N^{th}-power residues; in the cases $N = 2, 3, 4, 5, 6, 8$, these residues are called quadratic, cubic, quartic (or biquadratic), quintic, sextic, and octic residues, respectively. The numbers $(i,j)^{(N,q)} = \left|\left({C_i}^{(N,q)} + 1\right) \cap {C_j}^{(N,q)}\right|$ for $0 \leq i,j \leq N-1$ are called cyclotomic numbers.

Let $q = nN + 1$ as before. If the N^{th}-power residues form a $(q, n, \frac{n-1}{N})$-difference set in $(GF(q), +)$, then it is called an N^{th}-cyclotomic difference set or N^{th}-power residue difference set. If the N^{th}-power residues together with zero is a $(q, n+1, \frac{n+1}{N})$-difference set in $(GF(q), +)$, then it is called a modified N^{th}-cyclotomic difference set or modified N^{th}-power residue difference set. It is known in the literature that for $N \leq 24$, the cyclotomic class ${C_0}^{(N,q)}$ forms a difference set in $(GF(q), +)$ if and only if $N = 2, 4$, or 8, and q satisfies certain conditions. Details are presented in the next section. Results when $N > 24$ are sparse likely due to the difficulty of computing cyclotomic numbers, as noted by Beth *et al.* (1999) and Momihara *et al.* (2018).

Instead of using just a single cyclotomic class, Hall (1956) was able to construct a difference set from a union of three cyclotomic classes consisting of sextic residues. This result led researchers to the problem of finding difference sets from unions of two or more cyclotomic classes. A $(31, 6, 1)$-difference set from a union of two cyclotomic classes was found by Hayashi (1965) in the case where $N = 10$. According to the survey by Momihara *et al.* (2018), for many years, most researchers thought that no new difference sets could further be found by taking unions of cyclotomic classes and that it was a great surprise when Feng and Xiang (2012) discovered new infinite families of difference sets by taking unions of cyclotomic classes of order $N = 2p^m$, where p ≡ 7 (mod 8) is a prime. Momihara (2013) then gave a generalization for the same order N and prime p ≡ 3 (mod 4). Feng *et al.* (2015) further generalized the construction to the case $N = 2p^m$, where $p \equiv 3 \pmod 8$ is a prime. We see from the survey of results that no constructions of difference sets from unions of cyclotomic classes are known when $N = 12, 20$ or 24.

In this work, we obtained cyclotomic difference sets from unions of suitable cyclotomic classes of orders $N = 12, 20, 24$ (with and without zero) of the field $GF(q)$, where q is a prime of the form $q = nN + 1$, $n \geq 1$, and $q < 10^5$ using a computer search. The obtained difference sets were then classified based on their equivalence to the known cyclotomic and modified cyclotomic quadratic, quartic, sextic, and octic difference sets. The constructions in this paper also produced two difference sets equivalent to the complement of a quartic difference set and three difference sets equivalent to the complements of modified quartic, octic, and modified octic cyclotomic difference sets, respectively. In addition, for $N = 18$, we extended the work of Baumert and Fredricksen (1967) to construct six new modified 18^{th}-cyclotomic difference sets with parameters $(127, 64, 32)$.

The reader may consult Moore and Pollatsek (2013) and Ding (2015) for basic properties of difference sets and their applications. The book (Ireland and Rosen 1982) is a standard reference for number theory and finite fields.

PRELIMINARIES

The following theorem gives a necessary condition for parameters of a difference set.

Theorem 2.1: If D is a (v, k, λ)-difference set, then $k(k-1) = \lambda(v-1)$.

In generating difference sets, we use the concept of difference function. The difference function $\text{diff}_D(x)$ of a subset D of $(G, +)$ is defined as $\text{diff}_D(x) = |D \cap (D + x)|, x \in G$, where $D + x = \{y + x : y \in D\}$. As a consequence of the definition, a subset D of size k in an abelian group $(G, +)$ with order v is called a (v, k, λ)-difference set in $(G, +)$ if the difference function $\text{diff}_D(x) = \lambda$ for every nonzero $x \in G$ (Ding 2015).

The following gives a way to use one difference set to construct another (Wallis 1988).

Theorem 2.2: If D is a (v, k, λ)-difference set in $(G, +)$, its complement, $D^C = G\backslash D$ is also a difference set in $(G, +)$ with parameters $(v, v-k, v-2k+\lambda)$. The set D^C is called the complementary difference set of D.

From now on, we consider (v, k, λ)-difference sets in the additive group $(GF(q), +)$. Given the difference set $D = \{d_1, \ldots, d_k\}$, then for any integer s, the set $D + s = \{d_1 + s, \ldots, d_k + s\}$ taken modulo v is also a difference set called a shift of the set D. For any integer t, with $gcd(t, v) = 1$, the set $tD = \{td_1, \ldots, td_k\}$ taken modulo v is a difference set with the same parameters v, k, λ. If $D_1 = tD_2 + s$ for some t, s, with $gcd(t, v) = 1$, then the two difference sets D_1, D_2 are called equivalent. If $gcd(t, v) = 1$ and $tD = D + s$ for some s, then t is called a multiplier of the difference set D.

The following elementary result will be used to efficiently calculate all the primitive elements of a finite field.

Lemma 2.3: Let q be a prime power. Let α and q be relatively prime positive integers. The element α is a primitive element of $GF(q)$ if and only if $\alpha^{(q-1)/p} \neq 1$ for each prime factor p of $q-1$.

The following lemma shows that it is sufficient to just consider even values of N (Beth *et al.* 1999).

Lemma 2.4: Let $q = nN + 1$ be an odd prime power. If a union of cyclotomic classes of order N forms a difference set, then n is odd and N is even.

Cyclotomic Difference Sets from a Single Cyclotomic Class

We first discuss the case when a cyclotomic class $C_i^{(N,q)}$, for some integer i with $0 \leq i \leq N-1$, is a difference set in $(GF(q), +)$. Since $C_i^{(N,q)} = \alpha^i C_0^{(N,q)}$, it is enough to consider the cyclotomic class $C_0^{(N,q)}$ – possibly together with zero – to check if a single cyclotomic class forms a difference set. Paley (1933) proved and completed the case when $N = 2$, and Chowla (1944) settled the problem in the case when q is prime and $N = 4$. Lehmer (1953) established the following necessary and sufficient conditions for $C_0^{(N,q)}$ to be a difference set in terms of cyclotomic numbers. The version below is taken from Ding (2015).

Theorem 2.5 (**Lehmer**)**:** Let q be a prime power. Then $C_0^{(N,q)}$ is a difference set in $(GF(q), +)$ with parameters $(q, n, (n-1)/N)$ if and only if $(i, 0)^{(N,q)} = (n-1)/N$ for all $i \in \{0, 1, \ldots, N-1\}$.

Similarly, $C_0^{(N,q)} \cup \{0\}$ is a difference set in $(GF(q), +)$ with parameters $(q, n+1, (n+1)/N)$ if and only if $1 + (0,0)^{(N,q)} = (i, 0)^{(N,q)} = (n+1)/N$ for all $i \in \{1, \ldots, N-1\}$.

In either case, the only multipliers of the difference set are the elements of $C_0^{(N,q)}$.

The following collected results based on Theorem 2.5 when $N = 2, 4, 6,$ and 8 can be found in the works of Lehmer (1953), Momihara *et al.* (2018), and Ding (2015) and will be referred to when we determine the equivalence types of difference sets in our constructions.

Theorem 2.6: Let $GF(q)$ be the finite field of order q, where q is a power of an odd prime p. Let $N \geq 2$ be an even divisor of $q-1$, and $C_0^{(N,q)}$ be the subgroup of $GF(q)^*$ of index N.

1) When $N = 2$, $C_0^{(2,q)}$ is a quadratic cyclotomic difference set in $(GF(q), +)$ with parameters $(q, (q-1)/2, (q-3)/4)$ if and only if $q \equiv 3 \pmod 4$.
2) When $N = 2$, $C_0^{(2,q)} \cup \{0\}$ is a modified quadratic cyclotomic difference set in $(GF(q), +)$ with parameters $(q, (q+1)/2, (q+1)/4)$ if and only if $q \equiv 3 \pmod 4$.
3) When $N = 4$, $C_0^{(4,q)}$is a quartic cyclotomic difference set in $(GF(q), +)$ with parameters $(q, (q-1)/4, (q-5)/16)$ if and only if $q = 4t^2 + 1$ and t is odd.
4) When $N = 4$, $C_0^{(4,q)} \cup \{0\}$ is a modified quartic cyclotomic difference set in $(GF(q), +)$ with parameters $(q, (q+3)/4, (q+3)/16)$ if and only if $q = 4t^2 + 9$ and t is odd.
5) When $N = 6$, $C_0^{(6,q)}$is never a difference set in $(GF(q), +)$.
6) When $N = 8$, $C_0^{(8,q)}$is an octic cyclotomic difference set in $(GF(q), +)$ with parameters $(q, (q-1)/8, (q-9)/64)$ if and only if $q = 8t^2 + 1 = 64u^2 + 9$ for odd t and odd u.

7) When $N = 8$, ${C_0}^{(8,q)} \cup \{0\}$ is a modified octic cyclotomic difference set in $(GF(q), +)$ with parameters $(q, (q + 7)/8, (q + 7)/64)$ if and only if $q = 8t^2 + 49 = 64u^2 + 441$ for odd t and even u.

It is not known whether any of the cases in Theorem 2.6, with the exception of the quadratic cyclotomic difference set (also called Paley type difference set), yield infinite families. We now present other known results for cyclotomic difference sets from single cyclotomic classes for orders $N \leq 24$.

Theorem 2.7 (Xia 2018): Let $GF(q)$ be the finite field of order q, where $q = p^f$ is an odd prime power. Let $N \geq 2$ be an even divisor of $q - 1$, and ${C_0}^{(N,q)}$ be the subgroup of $GF(q)^*$ of index N. If $N \leq 22$ and $N \neq 2, 4$ or 8, then ${C_0}^{(N,q)}$ is never a difference set in $(GF(q), +)$.

Evans and van Veen (2017) proved the nonexistence of cyclotomic difference sets from single cyclotomic classes in $(GF(q), +)$ for the case $N = 24$ and prime q by computing cyclotomic numbers with the help of a Mathematica program.

Cyclotomic Difference Sets from Unions of Cyclotomic Classes

The first construction using unions is due to Hall (1956).

Theorem 2.8 (Hall): Let q be an odd prime power of the form $q = 4x^2 + 27$ for some integer x. Then ${C_0}^{(6,q)} \cup {C_1}^{(6,q)} \cup {C_3}^{(6,q)}$ is a $(q, (q - 1)/2, (q - 3)/4)$ difference set in $(GF(q), +)$.

The difference sets arising from the above theorem are called Hall sextic residue difference sets (or Hall type). The proof of this theorem included an exhaustive search on the SWAC computer, utilizing a method based on formulas of Dickson (1935) for cyclotomic numbers of order $N = 6$.

Hayashi (1965) made a similar difference set search on the Control Data Corporation 1604A computer for primes of the form $q = 10n + 1$, utilizing the formulas of Whiteman (1960) for cyclotomic numbers of order $N = 10$.

Theorem 2.9 (Hayashi): Let *D* be a cyclic difference set in $(GF(q), +)$, where q is a prime congruent to 1 *modulo* 10, which admits the 10th-powers as multipliers. Then we have (up to equivalence) one of the following two cases:

i) $q \equiv 3$ (mod 4) and *D* consists of the quadratic residues, or

ii) $q = 31$ and $D = {C_0}^{(10,q)} \cup {C_1}^{(10,q)}$.

In proving the above theorem, Hayashi showed that when constructing difference sets from unions of cyclotomic classes, it is sufficient to consider only unions containing the cyclotomic class ${C_0}^{(N,q)}$.

When $N = 18$, Baumert and Fredricksen (1967) found six inequivalent $(127, 63, 31)$ cyclic difference sets which all arise as unions of cyclotomic classes for $N = 18$. The case when zero is added to the sets to construct modified $(127, 64, 32)$-difference sets was not covered in their work.

From Lemma 2.4, the cases $N = 12, 20$, and 24 are the only orders ≤ 24 not covered by the preceding theorems that may yield difference sets.

SEARCH METHOD AND COMPUTATIONAL PROCEDURE

We discuss our search method that determines whether difference sets are obtained from unions of cyclotomic classes in the field $GF(q)$, where q is a prime of the form $nN + 1$. The method is applied to the orders $N = 12, 20$, and 24. Given an input prime q, the method finds all difference sets from unions of two or more cyclotomic classes of $GF(q)$ with or without zero. As per Hayashi (1965), it is sufficient to consider only unions containing the class ${C_0}^{(N,q)}$. The search is performed for all primes $q < 10^5$ of the stated form. We then determine whether the obtained difference sets, if any, are equivalent to known cyclotomic difference sets, as described in Theorems 2.6 and 2.8, or equivalent to their complements.

To prepare for the search, for each of the orders $N = 12, 20$, and 24, we first determine all primes $q < 10^5$ of the form $nN + 1$. By Lemma 2.4, it is enough to consider only odd values of n. For each such prime, we determine all primitive elements of $GF(q)$ using Lemma 2.3. As noted by Ding (2015), the primitive element employed to define the cyclotomic classes may have to be chosen properly.

We have written a program using Python 3.7 that performs the following steps for given inputs N and q:

1) Choose a primitive element α of $GF(q)$.
2) Compute the cyclotomic classes ${C_i}^{(N,q)}$ using the chosen primitive element.
3) Take the union of ${C_0}^{(N,q)}$ with a second cyclotomic class and test if the obtained set forms a difference set.
4) If no difference set is found, repeat steps 1–3 using a different primitive element until a difference set is obtained or until the primitive elements of $GF(q)$ are exhausted.
5) Repeat steps 1–4 using the union of ${C_0}^{(N,q)}$ with another cyclotomic class, until all unions of ${C_0}^{(N,q)}$ with a second cyclotomic class are exhausted.
6) Repeat steps 1–5, this time using ${C_0}^{(N,q)}$ with two other cyclotomic classes, then ${C_0}^{(N,q)}$ with three other cyclotomic classes, and so on up to ${C_0}^{(N,q)}$ with $N - 1$ other cyclotomic classes.
7) For each difference set obtained, check its equivalence with the known cyclotomic difference sets.

To search for modified difference sets, we perform the same steps but include zero in the unions. The codes to perform the search and test for equivalence, as well as codes used to compute primes and find primitive elements, can be found in a supplementary file that may be publicly accessed. The reader may adopt the codes for bigger values of N and higher bounds for q.

RESULTS AND CONCLUSION

We obtained the following theorems which give constructions of difference sets from unions of cyclotomic classes of order $N = 12, 20$, and 24 (with and without zero).

Theorem 4.1: Let $q < 10^5$ be a prime of the form $q = 12n + 1$ for $n \geq 1$ and odd. Then:

i) The set $D = {C_0}^{(12,q)} \cup {C_4}^{(12,q)} \cup {C_8}^{(12,q)}$ is a difference set in $(GF(q), +)$ with parameters $(q, (q-1)/4, (q-5)/16)$, where $q = 4t^2 + 1$ and t is odd, which contains quartic residues.

Similarly, the set $D = {C_0}^{(12,q)} \cup {C_4}^{(12,q)} \cup {C_8}^{(12,q)} \cup \{0\}$ is a difference set in $(GF(q), +)$ with parameters $(q, (q+3)/4, (q+3)/16)$, where $q = 4t^2 + 9$ and t is odd, which contains quartic residues together with zero.

ii) The set $D = {C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_2}^{(12,q)} \cup {C_4}^{(12,q)} \cup {C_5}^{(12,q)} \cup {C_6}^{(12,q)} \cup {C_8}^{(12,q)} \cup {C_9}^{(12,q)} \cup {C_{10}}^{(12,q)}$ is a difference set in $(GF(q), +)$ with parameters $(q, (3q-3)/4, (9q-21)/16)$, where $q = 4t^2 + 9$ and t is odd. This difference set is equivalent to the complement of modified quartic cyclotomic difference set.

Similarly, the set $D = {C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_2}^{(12,q)} \cup {C_4}^{(12,q)} \cup {C_5}^{(12,q)} \cup {C_6}^{(12,q)} \cup {C_8}^{(12,q)} \cup {C_9}^{(12,q)} \cup {C_{10}}^{(12,q)} \cup \{0\}$ is a difference set in $(GF(q), +)$ with parameters $(q, (3q+1)/4, (9q+3)/16)$, where $q = 4t^2 + 1$ and t is odd. This difference set is equivalent to the complement of quartic cyclotomic difference set.

Theorem 4.2: Let $q < 10^5$ be a prime of the form $q = 20n + 1$ for $n > 1$ and odd. Then:

i) The set $D = {C_0}^{(20,q)} \cup {C_4}^{(20,q)} \cup {C_8}^{(20,q)} \cup {C_{12}}^{(20,q)} \cup {C_{16}}^{(20,q)}$ is a difference set in $(GF(q), +)$ with parameters $(q, (q-1)/4, (q-5)/16)$, where $q = 4t^2 + 1$ and t is odd, which contains quartic residues.

With zero included, there is no union of cyclotomic classes that forms a difference set.

ii) The set $D = C_0{}^{(20,q)} \cup C_1{}^{(20,q)} \cup C_2{}^{(20,q)} \cup C_4{}^{(20,q)} \cup C_5{}^{(20,q)} \cup C_6{}^{(20,q)} \cup C_8{}^{(20,q)} \cup C_9{}^{(20,q)} \cup C_{10}{}^{(20,q)} \cup C_{12}{}^{(20,q)} \cup C_{13}{}^{(20,q)} \cup C_{14}{}^{(20,q)} \cup C_{16}{}^{(20,q)} \cup C_{17}{}^{(20,q)} \cup C_{18}{}^{(20,q)} \cup \{0\}$ is a difference set in $(GF(q),+)$ with parameters $(q,(3q+1)/4\,,(9q+3)/16)$, where $q = 4t^2+1$ and t is odd. This difference set is equivalent to the complement of the quartic cyclotomic difference set.

Theorem 4.3: Let $q < 10^5$ be a prime of the form $q = 24n+1$ *for* $n > 1$ and odd. Then:

i) The set $D = C_0{}^{(24,q)} \cup C_8{}^{(24,q)} \cup C_{16}{}^{(24,q)}$ is a difference set in $(GF(q),+)$ with parameters $(q,(q-1)/8\,,(q-9)/64)$, where $q = 8t^2+1 = 64u^2+9$ for odd t and odd u, which contains octic residues.

Similarly, the set $D = C_0{}^{(24,q)} \cup C_8{}^{(24,q)} \cup C_{16}{}^{(24,q)} \cup \{0\}$ is a difference set in $(GF(q),+)$ with parameters $(q,(q+7)/8\,,(q+7)/64)$, where $q = 8t^2+49 = 64u^2+441$ for odd t and even u, which contains octic residues together with zero.

ii) The set $D = C_0{}^{(24,q)} \cup C_1{}^{(24,q)} \cup C_2{}^{(24,q)} \cup C_3{}^{(24,q)} \cup C_4{}^{(24,q)} \cup C_5{}^{(24,q)} \cup C_6{}^{(24,q)} \cup C_8{}^{(24,q)} \cup C_9{}^{(24,q)} \cup C_{10}{}^{(24,q)} \cup C_{11}{}^{(24,q)} \cup C_{12}{}^{(24,q)} \cup C_{13}{}^{(24,q)} \cup C_{14}{}^{(24,q)} \cup C_{16}{}^{(24,q)} \cup C_{17}{}^{(24,q)} \cup C_{18}{}^{(24,q)} \cup C_{19}{}^{(24,q)} \cup C_{20}{}^{(24,q)} \cup C_{21}{}^{(24,q)} \cup C_{22}{}^{(24,q)}$ is a difference set in $(GF(q),+)$ with parameters $(q,(7q-7)/8\,,(49q-105)/64)$, where $q = 8t^2+49 = 64u^2+441$ for odd t and even u. This difference set is equivalent to the complement of the modified octic cyclotomic difference set.

Similarly, the set $D = C_0{}^{(24,q)} \cup C_1{}^{(24,q)} \cup C_2{}^{(24,q)} \cup C_3{}^{(24,q)} \cup C_4{}^{(24,q)} \cup C_5{}^{(24,q)} \cup C_6{}^{(24,q)} \cup C_8{}^{(24,q)} \cup C_9{}^{(24,q)} \cup C_{10}{}^{(24,q)} \cup C_{11}{}^{(24,q)} \cup C_{12}{}^{(24,q)} \cup C_{13}{}^{(24,q)} \cup C_{14}{}^{(24,q)} \cup C_{16}{}^{(24,q)} \cup C_{17}{}^{(24,q)} \cup C_{18}{}^{(24,q)} \cup C_{19}{}^{(24,q)} \cup C_{20}{}^{(24,q)} \cup C_{21}{}^{(24,q)} \cup C_{22}{}^{(24,q)} \cup \{0\}$ is a difference set in $(GF(q),+)$ with parameters $(q,(7q+1)/8\,,(49q+7)/64)$, where $q = 8t^2+1 = 64u^2+9$ for odd t and odd u. This difference set is equivalent to the complement of the octic cyclotomic difference set.

Although examples of difference sets from unions of 18^{th}-cyclotomic classes can be computed from the results of Momihara (2013), we performed our method for the case $N = 18$ to obtain the explicit decompositions. In particular, the search also yielded six modified $(127, 64, 32)$-difference sets. This extends the result in Baumert and Fredricksen (1967) that produced six $(127, 63, 31)$-difference sets without zero.

Theorem 4.4: Let $q < 10^5$ be a prime of the form $q = 18n+1$ for $n \geq 1$ and odd. Then,

i) The set $D = C_0{}^{(18,q)} \cup C_2{}^{(18,q)} \cup C_4{}^{(18,q)} \cup C_6{}^{(18,q)} \cup C_8{}^{(18,q)} \cup C_{10}{}^{(18,q)} \cup C_{12}{}^{(18,q)} \cup C_{14}{}^{(18,q)} \cup C_{16}{}^{(18,q)}$ is a difference set in $(GF(q),+)$ with parameters $(q,(q-1)/2\,,(q-3)/4)$, where $q \equiv 3\ (mod\ 4)$, which contains quadratic residues.

Similarly, the set $D = C_0{}^{(18,q)} \cup C_2{}^{(18,q)} \cup C_4{}^{(18,q)} \cup C_6{}^{(18,q)} \cup C_8{}^{(18,q)} \cup C_{10}{}^{(18,q)} \cup C_{12}{}^{(18,q)} \cup C_{14}{}^{(18,q)} \cup C_{16}{}^{(18,q)} \cup \{0\}$ is a difference set in $(GF(q),+)$ with parameters $(q,(q+1)/2\,,(q+1)/4)$, where $q \equiv 3\ (mod\ 4)$, which contains quadratic residues together with the residue zero.

ii) The set $D = C_0{}^{(18,q)} \cup C_1{}^{(18,q)} \cup C_3{}^{(18,q)} \cup C_6{}^{(18,q)} \cup C_7{}^{(18,q)} \cup C_9{}^{(18,q)} \cup C_{12}{}^{(18,q)} \cup C_{13}{}^{(18,q)} \cup C_{15}{}^{(18,q)}$ is a difference set in $(GF(q),+)$ equivalent to Hall sextic residue difference set with parameters $(q,(q-1)/2\,,(q-3)/4)$ for $q \equiv 1\ (mod\ 6)$, where $q = 4t^2+27$ and $gcd(3,t) = 1$. The primitive element of $GF(q)$ employed to define the cyclotomic classes must be properly chosen for the construction to work.

Similarly, the set $D = C_0{}^{(18,q)} \cup C_1{}^{(18,q)} \cup C_3{}^{(18,q)} \cup C_6{}^{(18,q)} \cup C_7{}^{(18,q)} \cup C_9{}^{(18,q)} \cup C_{12}{}^{(18,q)} \cup C_{13}{}^{(18,q)} \cup C_{15}{}^{(18,q)} \cup \{0\}$ is a difference set in $(GF(q),+)$ equivalent to modified Hall sextic residue difference set with parameters $(q,(q+1)/2\,,(q+1)/4)$ for $q \equiv 1\ (mod\ 6), q < 10^5$, where $q = 4t^2 + 27$ and $gcd(3, t) = 1$. The primitive element of $GF(q)$ employed to define the cyclotomic classes must be properly chosen for the construction to work.

iii) The sets

a) $D_1 = C_0{}^{(18,q)} \cup C_1{}^{(18,q)} \cup C_2{}^{(18,q)} \cup C_3{}^{(18,q)} \cup C_4{}^{(18,q)} \cup C_6{}^{(18,q)} \cup C_7{}^{(18,q)} \cup C_{11}{}^{(18,q)} \cup C_{16}{}^{(18,q)} \cup \{0\}$

b) $D_2 = C_0{}^{(18,q)} \cup C_1{}^{(18,q)} \cup C_2{}^{(18,q)} \cup C_3{}^{(18,q)} \cup C_4{}^{(18,q)} \cup C_6{}^{(18,q)} \cup C_8{}^{(18,q)} \cup C_9{}^{(18,q)} \cup C_{12}{}^{(18,q)} \cup \{0\}$

c) $D_3 = C_0{}^{(18,q)} \cup C_1{}^{(18,q)} \cup C_2{}^{(18,q)} \cup C_3{}^{(18,q)} \cup C_4{}^{(18,q)} \cup C_6{}^{(18,q)} \cup C_{11}{}^{(18,q)} \cup C_{14}{}^{(18,q)} \cup C_{15}{}^{(18,q)} \cup \{0\}$

d) $D_4 = C_0{}^{(18,q)} \cup C_1{}^{(18,q)} \cup C_3{}^{(18,q)} \cup C_5{}^{(18,q)} \cup C_8{}^{(18,q)} \cup C_9{}^{(18,q)} \cup C_{12}{}^{(18,q)} \cup C_{14}{}^{(18,q)} \cup C_{15}{}^{(18,q)} \cup \{0\}$

e) $D_5 = C_0{}^{(18,q)} \cup C_1{}^{(18,q)} \cup C_3{}^{(18,q)} \cup C_6{}^{(18,q)} \cup C_7{}^{(18,q)} \cup C_9{}^{(18,q)} \cup C_{12}{}^{(18,q)} \cup C_{13}{}^{(18,q)} \cup C_{15}{}^{(18,q)} \cup \{0\}$

f) $D_6 = C_0{}^{(18,q)} \cup C_2{}^{(18,q)} \cup C_4{}^{(18,q)} \cup C_6{}^{(18,q)} \cup C_8{}^{(18,q)} \cup C_{10}{}^{(18,q)} \cup C_{12}{}^{(18,q)} \cup C_{14}{}^{(18,q)} \cup C_{16}{}^{(18,q)} \cup \{0\}$

form 6 inequivalent $(127,64,32)$-difference sets. The set D_5 is equivalent to modified Hall sextic residue difference set, while D_6 is equivalent to a modified quadratic cyclotomic difference set.

REMARKS

The theory of cyclotomic difference sets in $(GF(q), +)$ covers not only primes but also prime powers $q = p^m$, where $m > 1$. Information on certain prime powers implies the non-existence of cyclotomic difference sets obtained from unions of cyclotomic classes. For the orders $N = 12, 18, 20$, and 24 considered in this paper, we note the following. The term prime power in the succeeding will mean an integer $q = p^m$, where p is a prime and $m > 1$.

i) Cohn (1993) showed that there is no prime power q satisfying the condition $q = 4t^2 + 1$ or $q = 4t^2 + 9$, where t is odd. Therefore, when q is a prime power, there is no difference set generated from unions of cyclotomic classes of order $N = 12$.

ii) Liqun (2008) proved that the equation $x^2 + 3^{2m+1} = y^n, (x, y) = 1, n > 2, m \geq 1$ has only one positive integer solution $(x, y, m, n) = (10, 7, 2, 3)$. Thus, there is no Hall sextic residue difference set, where q is a prime power generated from unions of cyclotomic classes of order $N = 18$.

iii) From a result of Lebesgue (1850), it is known that there is no prime power q satisfying the condition $q = 4t^2 + 1$, where t is odd. Thus, there is no difference set where q is a prime power from unions of cyclotomic classes of order $N = 20$.

iv) In Cohn (1993), it is also shown that there is no prime power q satisfying the condition $64u^2 + 9$. Thus, there is no difference set where q is a prime power generated from unions of cyclotomic classes of order $N = 24$.

We have obtained difference sets from unions of cyclotomic classes for the cases $N = 12, 20, 24$. This fills the gaps in the literature on their existence. It will be desirable to generalize these constructions along the lines of the previously mentioned results of Feng and Xiang (2012), Momihara (2013), and Feng *et al.* (2015).

SUPPLEMENTARY FILE

The codes used in this paper and examples of difference sets generated from the search can be found online at: https://drive.google.com/file/d/1GJqy7sdaP7bEoSnckI1mw8bJ8h5mbZFD/view?usp=sharing

REFERENCES

BAUMERT LD, FREDRICKSEN H. 1967. The cyclotomic numbers of order eighteen with applications to difference sets, Math Comput (21): 204–219.

BETH T, JUNGNICKEL D, LENZ H. 1999. Design theory, Vol. 1, 2nd ed. Cambridge: Cambridge Univ Press. 705p.

CHOWLA S. 1944. A property of biquadratic residues. Proc Nat Acad Sci India 14(A): 45–46.

COHN JHE. 1993. The diophantine equation $x^2 + C = y^n$. Acta Arith (65): 367–381.

DICKSON LE. 1935. Cyclotomy, higher congruences, and Waring's problem. Amer J Math 57(3): 391–424.

DING C. 2015. Codes from difference sets, Singapore: World Scientific. 354p.

EVANS R, VAN VEEN M. 2017. Nonexistence of twenty-fourth power residue addition sets. Finite Fields Appl 46: 139–146.

FENG T, MOMIHARA K, XIANG Q. 2015. Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes. Combinatorica 35: 413–434.

FENG T, XIANG Q. 2012. Cyclotomic constructions of skew Hadamard difference sets. J Combin Th 119(A): 245–256.

HALL M. 1956. A survey of difference sets. Proc Amer Math Soc 7: 975–986.

HAYASHI HS. 1965. Computer investigation of difference sets. Math Comp 19: 73–78.

IRELAND K, ROSEN M. 1982. A classical introduction to modern number theory, New York-Heidelberg-Berlin: Springer-Verlag. 341p.

LEBESGUE VA. 1850. Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 +1$. Nouvelles Annales des Mathématiques 9(1): 178–181.

LEHMER E. 1953. On residue difference sets. Canad J Math 5: 425–432.

LIQUN T. 2008. On the Diophantine equation $x^2 + 3^m = y^n$. Integers: Electron J Combin Number Th 8: A55.

MOMIHARA K, WANG Q, XIANG Q. 2018. Cyclotomy, difference sets, sequences with low correlation, strongly regular graphs, and related geometric substructures. arXiv:1809.03007 [math.CO]. p. 1–29.

MOMIHARA K. 2013. Inequivalence of skew Hadamard difference sets and triple intersection numbers modulo a prime. Electron J Combin 20(4): 19.

MOORE EH, POLLATSEK HS. 2013. Difference sets: connecting algebra, combinatorics, and geometry. American Math Soc, Providence, RI. 315p.

PALEY REAC. 1933. On orthogonal matrices. Studies in Appl Math 12: 311–320.

WALLIS WD. 1988. Combinatorial designs. New York and Basel: Marcel Dekker.

WHITEMAN AL. 1960. The cyclotomic numbers of order ten. Proc Sympos Appl Math: 95–111.

XIA B. 2018. Cyclotomic difference sets in finite fields. Math Comput 87: 2461–2482.