Construction of Difference Sets from Unions of Cyclotomic Classes of Order N=14

Benedict M. Estrella

Bulacan State University, Bulacan, Philippines
https://orcid.org/0000-0002-3159-293X
Email Correspondence: benedict.estrella@bulsu.edu.ph

Abstract

Let G be an additive group of order v, D be a non-empty proper k-subset of G, and λ be any integer. Then D is a (v, k, λ) - difference set if every nonzero element of the group can be expressed as a difference d_1 - d_2 of elements of D in exactly λ ways. Let q be a prime of the form q = nN + 1 for integers n>1 and N>1. For q<1000, this study shows the construction of difference sets in the additive group of the field GF(q) from unions of cyclotomic classes of order N = 14 using a computer search. The construction consisted of computer programs derived from the definitions and theorems on difference sets using Python. The results revealed that only the union of seven cyclotomic classes such as $C_0^{(14, q)} \cup C_2^{(14, q)} \cup C_4^{(14, q)} \cup C_6^{(14, q)} \cup C_8^{(14, q)} \cup C_{10}^{(14, q)} \cup C_{12}^{(14, q)}$ forms a quadratic cyclotomic difference set. Similarly, this union together with zero forms a difference set equivalent to the modified quadratic cyclotomic difference sets.

Keywords: difference set, cyclotomic class, union, computer search

1.0 Introduction

The study of difference sets are of intrinsic interest because they have several applications to real-world problems. It is found that difference sets can be used to construct complex codebooks which have important applications in communication systems. In engineering and science contexts, difference sets 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.

Difference sets connect other areas of mathematics such as Algebra, Combinatorics, and Geometry. It also uses tools from group theory, number theory, representation theory, and other areas. For instance, in Combinatorics, it is closely related to design theory which was originally studied for its connection to statistics and the design of experiments. In geometry, one can create a specific geometric structure like the Fano plane (Moore & Pollatsek, 2013).

A powerful and classical method for constructing difference sets in the additive groups of finite fields is cyclotomic construction. This construction uses cyclotomic classes of finite fields to produce difference sets. To define cyclotomic classes, let q be a prime power of the form $q = nN + 1$ for two positive integers $n,N > 1$, and let α be a fixed primitive element of $GF(q)$. The N^{th} cyclotomic classes $C_{\mathrm{i}}^{(\mathrm{N,q})}$ of $GF(q)$ is defined by $C_i^{(N,q)} = \left\{\alpha^{jN+i} : 0 \leq j \leq \frac{q-1}{N} - 1\right\}$, where $0 \leq i \leq N\text{-}1$.

That is, $C_0^{(N,q)}$ is the subgroup of $GF(q)^*$ consisting of all nonzero 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, the elements of $C_0^{(N,q)}$ are called 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.

If the nonzero N^{th} -power residues is 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.

Lehmer (as cited in Momihara et al. (2019)) proved that a single 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. On the other hand, there have been very few results on the existence of difference sets using unions of cyclotomic classes. Details are presented in the next section.

In this work, the researcher shows the construction of cyclotomic difference sets from unions of suitable cyclotomic classes of order N=14 (with and without the residue zero) of the finite field $GF(q)$, where q is a prime of the form $q = 14n+1$ for integer $n>1$ using an exhaustive computer search. Also, the obtained difference sets are classified based on their equivalence to the known cyclotomic and modified cyclotomic difference sets.

2.0 Methodology

Preliminaries

In order to determine valid parameters for the existence of a difference set, the following theorem was used in the construction. The proof can be found in Moore and Pollatsek (2013).

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

The concept of difference function was also utilized in verifying the resulting difference sets. 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 $D+x = \{y+x : y \in D\}$. In terms of the difference function, 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).

Now, what it means for two difference sets to be equivalent? Given the difference set $D = \{d_1, ..., d_k\}$ then for any integer s, the set $D+s = \{d_1 + s, ..., d_k + s\}$ 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 $tD = \{td_1, ..., td_k\}$ taken modulo v is also 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 (Baumert & Fredricksen, 1967).

Definition 2.2: A primitive element α of a finite field $GF(q)$ is a generator of the multiplicative group $GF(q)^*$ of nonzero elements of $GF(q)$.

The following theorem was applied to efficiently calculate all the primitive elements of a finite field. The reader is referred to Estrella (2019) for the proof.

Theorem 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 for the theory of cyclic difference sets to 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

Consider first the problem when a cyclotomic class $C_{\mathrm{i}}^{(\mathrm{N,q})}$, where i is some integer such that $0 \leq \mathrm{i} \leq \mathrm{N}-1$, is a difference set in $(GF(q),+)$. Since $\mathrm{C}_{\mathrm{i}}^{(\mathrm{N,q})} = \alpha^{\mathrm{i}}\, C_0^{(\mathrm{N,q})}$, it is enough to consider the cyclotomic class $C_0^{(\mathrm{N,q})}$ to check if a single cyclotomic class forms a difference set. According to the survey by Momihara et al. (2019), Paley proved and completed the case when $N= 2$ and Chowla settled the problem in the case when q is prime and $N= 4$.

The following collected results when $N= 2$, 4, 6, and 8 can be found in Momihara et al. (2019), Xia (2018), and Ding (2015) and will be referred to when determining the equivalence types of difference sets in the construction.

Theorem 2.5: 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 $C_0^{(\mathrm{N,q})}$ be the subgroup of $GF(q)^*$ of index N.

1. When $N= 2$, $C_0^{(2,\mathrm{q})}$ 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 $N= 2$, $\mathrm{C}_0^{(2,\mathrm{q})} \cup \{0\}$ 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 $N=4$, $C_0^{(4,\mathrm{q})}$ 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 $N= 4$, $C_0^{(4,\mathrm{q})} \cup \{0\}$ 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 $N= 6$, $C_0^{(6,\mathrm{q})}$ is never a difference set in $(GF(q),+)$.
6. When $N= 8$, $C_0^{(8,\mathrm{q})}$ 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 $N= 8$, $C_0^{(8,\mathrm{q})} \cup \{0\}$ 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.

The first construction of difference sets using unions of cyclotomic classes is due to Hall (1956). The difference sets arising from the theorem below are usually called the Hall sextic residue difference sets.

Theorem 2.6 (Hall): Let q be an odd prime power of the form $q = 4x^2+27$ for some integer x. Then $C_0^{(6,\mathrm{q})} \cup C_1^{(6,\mathrm{q})} \cup C_3^{(6,\mathrm{q})}$ is a $(q,\ (q-1)/2,\ (q-3)/4)$ difference set in $(GF(q),+)$.

In 1965, Hayashi made a similar difference set search using cyclotomic classes of order N=10. His results were summarized in the theorem below.

Theorem 2.7 (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. $q \equiv 3 \pmod 4$ and D consists of the quadratic residues, or

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

In 1967, Baumert and Fredricksen found that there are six inequivalent $(127,63,31)$-difference sets which all arise as unions of cyclotomic classes for N=18. In 2012, Feng and Xiang discovered new infinite families of Hadamard difference sets in $(GF(q),+)$ by using a union of cyclotomic classes of order $N = 2p_1^{m}$, where $p_1 \equiv 7 \pmod 8$ is a prime. Then Momihara (2013) gave a generalization of Feng-Xiang skew Hadamard difference sets. In 2015, Feng et al. generalized the construction of skew Hadamard difference sets to the case $N = 2p_1^{m}$, where $p_1 \equiv 3 \pmod 8$ is a prime.

Recently, Balmaceda and Estrella (2021) constructed difference sets from unions of cyclotomic classes of orders N = 12, 20, and 24. Moreover, their search also yielded six modified $(127, 64, 32)$-difference sets from unions of cyclotomic classes of order $N = 18$.

Computational Procedure

For the computational procedure, the search method was adopted from the algorithms of (Balmaceda & Estrella, 2021). 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. The search is performed for all primes $q < 1000$ of the form $q = 14n + 1$. Lastly, it is determined whether the obtained difference sets, if any, are equivalent to known cyclotomic difference sets, as described in Theorems 2.5.

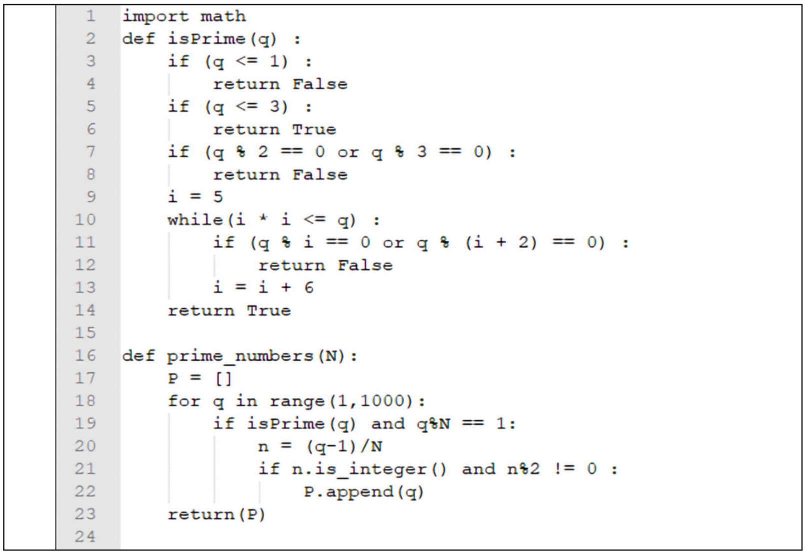
Computer programs were written using Python that performs the following steps for given inputs $N = 14$ and q.

1. Choose a primitive element α of $GF(q)$.
2. Compute the cyclotomic classes $C_i^{(14,q)}$ using the chosen primitive element.
3. Take the union of $C_0^{(14,q)}$ 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 $C_0^{(14,q)}$ with another cyclotomic class, until all unions of $C_0^{(14,q)}$ with a second cyclotomic class are exhausted.
6. Repeat steps 1–5, this time using $C_0^{(14,q)}$ with two other cyclotomic classes, then $C_0^{(14,q)}$ with three other cyclotomic classes, and so on up to $C_0^{(14,q)}$ with thirteen other cyclotomic classes.
7. For each difference set obtained, check its equivalence with the known cyclotomic difference sets.

To search for modified cyclotomic difference sets, the same steps will be applied but include zero in the unions.

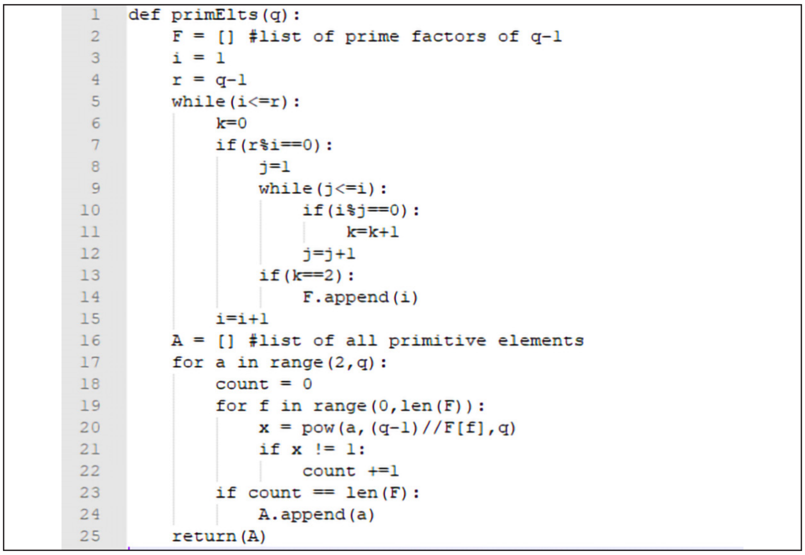
First determine all primes $q < 1000$ of the form $14n+1$. By Lemma 2.4, it is enough to consider only odd values of n. The function *prime_numbers* (N) is created to list all the primes less than 1000 and congruent to 1 modulo 14. The code is given in Figure 1. This function will be called in the main program at the latter part of this section. Lines 2-14 is a function which checks if the number q is prime or not. Lines 16-23 will return all prime numbers less than 1000 satisfying the desired form.

Next, create the function *primElts(q)* to find all the primitive elements of $GF(q)$ for each prime q using Theorem 2.3. As noted by Ding (2015), the primitive element employed to define the cyclotomic classes may have to be chosen properly. See Figure 2 below for the sample code.



```
 1  import math
 2  def isPrime(q) :
 3      if (q <= 1) :
 4          return False
 5      if (q <= 3) :
 6          return True
 7      if (q % 2 == 0 or q % 3 == 0) :
 8          return False
 9      i = 5
10      while(i * i <= q) :
11          if (q % i == 0 or q % (i + 2) == 0) :
12              return False
13          i = i + 6
14      return True
15
16  def prime_numbers(N):
17      P = []
18      for q in range(1,1000):
19          if isPrime(q) and q%N == 1:
20              n = (q-1)/N
21              if n.is_integer() and n%2 != 0 :
22                  P.append(q)
23      return(P)
24
```

Figure 1. *Prime Numbers of the Form 14n + 1*



```
def primElts(q):
    F = [] #list of prime factors of q-1
    i = 1
    r = q-1
    while(i<=r):
        k=0
        if(r%i==0):
            j=1
            while(j<=i):
                if(i%j==0):
                    k=k+1
                j=j+1
            if(k==2):
                F.append(i)
        i=i+1
    A = [] #list of all primitive elements
    for a in range(2,q):
        count = 0
        for f in range(0,len(F)):
            x = pow(a,(q-1)//F[f],q)
            if x != 1:
                count +=1
        if count == len(F):
            A.append(a)
    return(A)
```

Figure 2. *Primitive Elements*

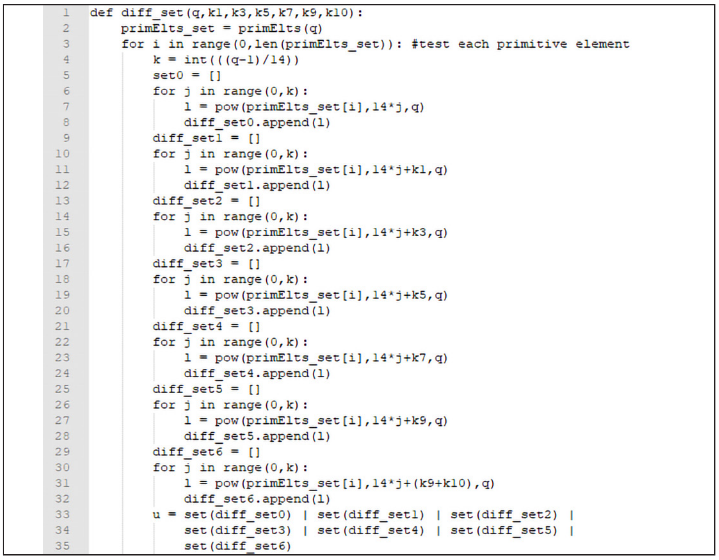
For steps 1 to 4, write another function *diff_set(parameters)* to compute the 14th-cyclotomic classes $C_i^{(14,q)}$ using a primitive element, take their unions and test the existence of difference sets. Start with combination of two classes and continue up to unions of 13 classes. To illustrate this, the case of seven classes of order 14 will be discussed. The classes can be represented by $C_0^{(14,q)} \cup C_{i_1}^{(14,q)} \cup C_{i_2}^{(14,q)} \cup C_{i_3}^{(14,q)} \cup C_{i_4}^{(14,q)} \cup C_{i_5}^{(14,q)} \cup C_{i_6}^{(14,q)}$, where $0 < i_1 < i_2 < i_3 < i_4 < i_5 < i_6 \leq 13$. The source codes of the function are given in Figure 3 and Figure 4.

From Figure 3, the function *primElts(q)* in line 2 was called to list all the primitive elements. In line 3, the program will choose the first primitive element in the list (Step 1). The cyclotomic classes will be computed in lines 4-32 (Step 2). For step 3, the first combination of cyclotomic classes will be computed in line 33. The obtained union will be tested using the codes in lines 37-59 of Figure 4 if it will form a difference set. For step 4, if no difference set is found, the program will choose the next primitive element. Using the second primitive element, the cyclotomic classes will again be computed. Then, the same union will be considered and will be tested for the existence of difference set. Steps 1 to 4 will be repeated until the primitive elements of $GF(q)$ are all exhausted. After that, the next set of unions will be tested using the code in the main program. The same procedure will be executed until the possible unions of seven classes are all exhausted.

If there exists a difference set, the function *diff_set(parameters)* will return the obtained difference set. Then, the next set of union will be considered until all the possible unions of seven classes are exhausted.

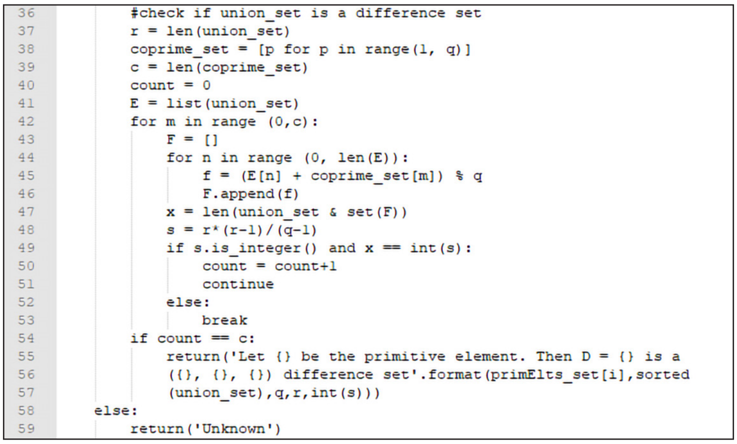
Finally, the main program in Figure 5 is needed to execute all the possible unions of seven cyclotomic classes and test each prime $q < 1000$. In line 3, the function *prime_numbers(N)* was called to list all primes q of the form $q = 14n + 1$ for some odd integer $n > 1$. In line 14, the function *diff_set(parameters)* was called to form the union and test the existence of difference sets.

If there exist difference sets, create another code to test the equivalence of two or more difference sets. For illustration, the following code in Figure 6 determines if the difference sets $D1$, $D2$, ..., Dn are equivalent to the known difference sets *D,* as described in Theorem 2.5.



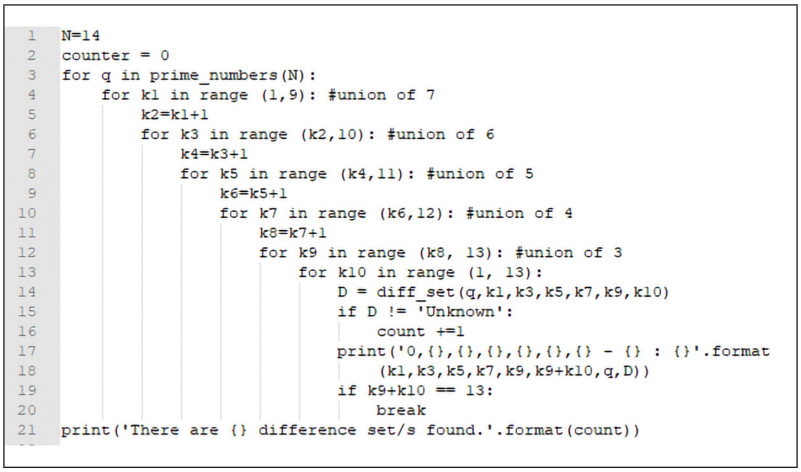
```
1   def diff_set(q,k1,k3,k5,k7,k9,k10):
2       primElts_set = primElts(q)
3       for i in range(0,len(primElts_set)): #test each primitive element
4           k = int(((q-1)/14))
5           set0 = []
6           for j in range(0,k):
7               l = pow(primElts_set[i],14*j,q)
8               diff_set0.append(l)
9           diff_set1 = []
10          for j in range(0,k):
11              l = pow(primElts_set[i],14*j+k1,q)
12              diff_set1.append(l)
13          diff_set2 = []
14          for j in range(0,k):
15              l = pow(primElts_set[i],14*j+k3,q)
16              diff_set2.append(l)
17          diff_set3 = []
18          for j in range(0,k):
19              l = pow(primElts_set[i],14*j+k5,q)
20              diff_set3.append(l)
21          diff_set4 = []
22          for j in range(0,k):
23              l = pow(primElts_set[i],14*j+k7,q)
24              diff_set4.append(l)
25          diff_set5 = []
26          for j in range(0,k):
27              l = pow(primElts_set[i],14*j+k9,q)
28              diff_set5.append(l)
29          diff_set6 = []
30          for j in range(0,k):
31              l = pow(primElts_set[i],14*j+(k9+k10),q)
32              diff_set6.append(l)
33          u = set(diff_set0) | set(diff_set1) | set(diff_set2) |
34              set(diff_set3) | set(diff_set4) | set(diff_set5) |
35              set(diff_set6)
```

Figure 3. *Union of seven cyclotomic classes*



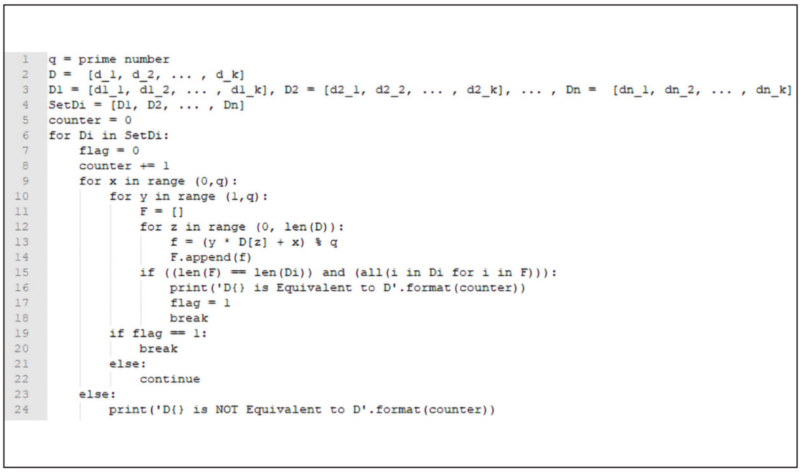
```
        #check if union_set is a difference set
        r = len(union_set)
        coprime_set = [p for p in range(1, q)]
        c = len(coprime_set)
        count = 0
        E = list(union_set)
        for m in range (0,c):
            F = []
            for n in range (0, len(E)):
                f = (E[n] + coprime_set[m]) % q
                F.append(f)
            x = len(union_set & set(F))
            s = r*(r-1)/(q-1)
            if s.is_integer() and x == int(s):
                count = count+1
                continue
            else:
                break
        if count == c:
            return('Let {} be the primitive element. Then D = {} is a
            ({}, {}, {}) difference set'.format(primElts_set[i],sorted
            (union_set),q,r,int(s)))
    else:
        return('Unknown')
```

Figure 4. *Test for the existence of difference sets*



```
N=14
counter = 0
for q in prime_numbers(N):
    for k1 in range (1,9): #union of 7
        k2=k1+1
        for k3 in range (k2,10): #union of 6
            k4=k3+1
            for k5 in range (k4,11): #union of 5
                k6=k5+1
                for k7 in range (k6,12): #union of 4
                    k8=k7+1
                    for k9 in range (k8, 13): #union of 3
                        for k10 in range (1, 13):
                            D = diff_set(q,k1,k3,k5,k7,k9,k10)
                            if D != 'Unknown':
                                count +=1
                            print('0,{},{},{},{},{},{} - {} : {}'.format
                                (k1,k3,k5,k7,k9,k9+k10,q,D))
                            if k9+k10 == 13:
                                break
print('There are {} difference set/s found.'.format(count))
```

Figure 5. *Main Program*



```
q = prime number
D =  [d_1, d_2, ... , d_k]
D1 = [d1_1, d1_2, ... , d1_k], D2 = [d2_1, d2_2, ... , d2_k], ... , Dn =  [dn_1, dn_2, ... , dn_k]
SetDi = [D1, D2, ... , Dn]
counter = 0
for Di in SetDi:
    flag = 0
    counter += 1
    for x in range (0,q):
        for y in range (1,q):
            F = []
            for z in range (0, len(D)):
                f = (y * D[z] + x) % q
                F.append(f)
            if ((len(F) == len(Di)) and (all(i in Di for i in F))):
                print('D{} is Equivalent to D'.format(counter))
                flag = 1
                break
        if flag == 1:
            break
        else:
            continue
    else:
        print('D{} is NOT Equivalent to D'.format(counter))
```

Figure 6. *Test for Equivalence*

3.0 Results and Discussion

Let $q < 1000$ be a prime of the form $q = 14n + 1$ for $n > 1$ and odd. Table 1 summarizes the parameters v, k, λ, the index set I, and the conditions for q in which the set $D = \cup_{i \in I} C_i^{(14,q)}$ forms a difference set in the additive group $GF(q)$. The class that indicates the family to which the difference set belongs is also included in the table.

Table 1. *Difference Sets from Unions of Cyclotomic Classes of Order N = 14*

(v, k, λ)	Index Set I	Conditions for q	Class
$(q, (q-1)/2, (q-3))/4)$	$\mathrm{I} = \{0,2,4,6,8,10,12\}$	$q \equiv 3 \pmod 4$	Paley Type
$(q, (q+1)/2, (q+1)/4)$	$\mathrm{I} = \{0,2,4,6,8,10,12\}$ with 0	$q \equiv 3 \pmod 4$	Modified Paley Type

When the index set I contains 0, 2, 4, 6, 8, 10, and 12 the union of $C_i^{(14,q)}$ forms a $(q, (q-1))/2, (q-3)/4)$ -difference set if $q \equiv 3 \pmod 4$. This difference set is equivalent to quadratic cyclotomic difference sets which are often called Paley type. Similarly, when 0 is added to the same union, it also forms a difference set with parameters $(q, (q+1)/2, (q+1)/4)$ satisfying the same condition for q. The obtained difference set belongs to the modified quadratic cyclotomic difference sets or modified Paley type. These results are summarized in the following theorem.

Theorem 3.1 Let $q < 1000$ be a prime of the form $q = 14n + 1$ for $n > 1$ and odd. Then,

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

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

The following are some examples of difference sets generated from unions of cyclotomic classes of order $N = 14$. The elements of the set, parameters and equivalence type are also provided.

Example 3.2 Let $q = 43$, and let the primitive element $\alpha = 3$. Then

$$D = C_0^{(14,q)} \cup C_2^{(14,q)} \cup C_4^{(14,q)} \cup C_6^{(14,q)} \cup C_8^{(14,q)} \cup C_{10}^{(14,q)} \cup C_{12}^{(14,q)}$$
$$= \{1,4,6,9,10,11,13,14,15,16,17,21,23,24,25,31,35,36,38,40,41\}$$

is a (43, 21, 10)-difference set in $(GF(43),+)$. This difference set is the same as the quadratic cyclotomic difference set $C_0^{(2,43)}$.

Example 3.3 Let $q = 71$, and let the primitive element $\alpha = 7$. Then

$$D = C_0^{(14,q)} \cup C_2^{(14,q)} \cup C_4^{(14,q)} \cup C_6^{(14,q)} \cup C_8^{(14,q)} \cup C_{10}^{(14,q)} \cup C_{12}^{(14,q)}$$
$$= \{1,2,3,4,5,6,8,9,10,12,15,16,18,19,20,24,25,27,29,30,32,36,37,38,40,43,45,48,49,50,54,57,58,60,64\}$$

is a (71, 35, 17)-difference set in $(GF(71),+)$. This difference set is the same as the quadratic cyclotomic difference set $C_0^{(2,71)}$.

Example 3.4 Let $q = 43$, and let the primitive element $\alpha = 3$. Then

$$D = C_0^{(14,q)} \cup C_2^{(14,q)} \cup C_4^{(14,q)} \cup C_6^{(14,q)} \cup C_8^{(14,q)} \cup C_{10}^{(14,q)} \cup C_{12}^{(14,q)} \cup \{0\}$$
$$= \{0,1,4,6,9,10,11,13,14,15,16,17,21,23,24, 25,31,35,36,38,40,41\}$$

is a $(43, 22, 11)$-difference set in $(GF(43),+)$. This difference set is the same as the modified quadratic cyclotomic difference set $C_0^{(2,43)} \cup \{0\}$.

Example 3.5 Let q = 71, and let the primitive element α = 7. Then

$$D = C_0^{(14,q)} \cup C_2^{(14,q)} \cup C_4^{(14,q)} \cup C_6^{(14,q)} \cup C_8^{(14,q)} \cup C_{10}^{(14,q)} \cup C_{12}^{(14,q)} \cup \{0\}$$
$$= \{0,1,2,3,4,5,6,8,9,10,12,15,16,18,19,20, 24, 25,27,29,30,32,36,37,38,40,43,45,48,49, 50,54,57,58,60,64\}$$

is a $(71, 36, 18)$-difference set in $(GF(71),+)$. This difference set is the same as the modified quadratic cyclotomic difference set $C_0^{(2,71)} \cup \{0\}$.

4.0 Conclusion

Based from the findings, if q a prime congruent to 3 modulo 4 and of the form $q = 14n + 1$ for $n > 1$ and odd, a $(q, (q–1)/2, (q–3)/4)$- difference sets in $(GF(q), +)$ can be constructed by taking the union of cyclotomic classes $C_0^{(14,q)} \cup C_2^{(14,q)} \cup C_4^{(14,q)} \cup C_6^{(14,q)} \cup C_8^{(14,q)} \cup C_{10}^{(14,q)} \cup C_{12}^{(14,q)}$ which is equivalent to quadratic cyclotomic difference sets. Similarly, a $(q, (q+1)/2, (q+1)/4)$-difference sets in $(GF(q),+)$ can be constructed by taking the union of cyclotomic classes $C_0^{(14,q)} \cup C_2^{(14,q)} \cup C_4^{(14,q)} \cup C_6^{(14,q)} \cup C_8^{(14,q)} \cup C_{10}^{(14,q)} \cup C_{12}^{(14,q)} \cup \{0\}$ which is equivalent to modified quadratic cyclotomic difference sets. The same results were obtained from the constructions of Feng and Xiang (2012), and Momihara (2013).

More so, the study only focused on the detailed construction of cyclotomic difference sets using unions of cyclotomic classes of order 14 for the stated values of $q < 1000$ using an exhaustive computer search. The reader may adopt the codes for higher bounds for q. It is desirable to generalize the results for all primes and prime powers q of the form $q = nN + 1$ for $N = 14$ using other theoretical methods without computer search.

References

Balmaceda, J. M. P., & Estrella, B. M. (2021). Difference sets from unions of cyclotomic classes of orders 12, 20, and 24. *Philippine Journal of Science, 150* (6B), 1803–1810.

Baumert, L.D., & Fredricksen, H. (1967). The cyclotomic numbers of order eighteen with applications to difference sets. *Mathematics of Computation, 21*(98), 204-219. https://www.ams.org/mcom/1967-21-098/S0025-5718-1967-0223322-5/S0025-5718-1967-0223322-5.pdf

Beth, T., Jungnickel, D., & Lenz, H. (1999). *Design theory* (2nd ed., Vol. 1). Cambridge University Press.

Ding, C. (2015). *Codes from difference sets*. World Scientific.

Estrella, B. M. (2019). *Generating difference sets from Unions of Cyclotomic classes* [Unpublished master's thesis]. University of the Philippines Diliman.

Feng, T., Momihara, K., & Xiang, Q. (2015). Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes. *Combinatorica, 35*(4), 413–434.

Feng, T., & Xiang, Q. (2012). Cyclotomic constructions of Skew Hadamard difference sets. *Journal of Combinatorial Theory, Series A, 119*(1), 245–256. https://doi.org/10.1016/j.jcta.2011.08.007

Hall, M. (1956). A survey of difference sets. *Proceedings of the American Mathematical Society*, *7*(6), 975-986.

Hayashi, H. S. (1965). Computer investigation of difference sets. *Mathematics of Computation, 19*(89), 73–78. https://doi.org/10.1090/s0025-5718-1965-0171368-6

Momihara, K. (2013). Inequivalence of Skew Hadamard difference sets and triple intersection numbers modulo a prime. *The Electronic Journal of Combinatorics, 20*(4). https://doi.org/10.37236/3762

Momihara, K., Wang, Q., & Xiang, Q. (2019). 9. Cyclotomy, difference sets, sequences with low correlation, strongly regular graphs and related geometric substructures. In K.-U. Schmidt & A. Winterhof (Eds.), *Combinatorics and finite fields: Difference sets, polynomials, pseudorandomness and applications* (pp. 173–198). De Gruyter.

Moore, E. H., & Pollatsek, H. S. (2013). *Difference sets: Connecting algebra, combinatorics, and geometry* (Vol. 67). American Mathematical Society.

Xia, B. (2018). Cyclotomic difference sets in finite fields. *Mathematics of Computation, 87*(313), 2461–2482. https://doi.org/10.1090/mcom/3311