Received: 17 July 2023 | Accepted: 26 December 2023 | Published Online: 30 December 2023
Recoletos Multidisciplinary Research Journal Vol. 11 no. 2 (December 2023)
DOI: https://doi.org/10.32871/rmrj2311.02.06

On Some New Almost Difference Sets Constructed from Cyclotomic Classes of Order 12

Benedict M. Estrella
Mathematics Department, College of Science, Bulacan State University, Bulacan, Philippines
Email correspondence: benedict.estrella@bulsu.edu.ph

Abstract

Almost Difference Sets have extensive applications in coding theory and cryptography. In this study, we introduce new constructions of Almost Difference Sets derived from cyclotomic classes of order 12 in the finite field $GF(q)$, where q is a prime satisfying the form $q = 12n + 1$ for positive integers $n \geq 1$ and $q < 1000$. We show that a single cyclotomic class of order 12 (with and without zero) can form an almost difference set. Additionally, we successfully construct almost difference sets using unions of cyclotomic classes of order 12, both for even and odd values of n. To accomplish this, an exhaustive computer search employing Python was conducted. The method involved computing unions of two cyclotomic classes up to eleven classes and assessing the presence of almost difference sets. Finally, we classify the resulting almost difference sets with the same parameters up to equivalence and complementation.

Keywords: almost difference set, cyclotomic class, cyclotomy, union

1.0 Introduction

Almost Difference Sets (ADSs) have significant implications in various mathematical areas, including coding theory and cryptography. Within coding theory, ADSs have been utilized by Heng (2023) to build projective linear codes capable of error correction through their dual codes. ADSs also play a role in constructing cyclic codes and codebooks. Ding and Feng (2008) have investigated a general approach to constructing codebooks using ADSs, achieving classes of codebooks that come close to meeting the Welch bound. In cryptography, ADSs have the potential to create functions with optimal nonlinearity, as referenced in Nowak (2014).

Consider an abelian group $(G, +)$ of order q. We define a k-subset D of G as a (q, k, λ, t) almost difference set of G if, when considering all nonzero elements x of G, the difference function $\text{diff}_D(x)$ takes on a value of λ exactly t times, and a value of λ + 1 exactly $q - 1 - t$ times. The difference function $\text{diff}_D(x)$ is given by $\text{diff}_D(x) = |D \cap (D + x)|$. This definition is derived from Ding et al. (2001), which presents a generalization and unification of two previously introduced definitions of almost difference sets by Davis (1992) and Ding (1994). It is worth noting that almost difference sets are just generalizations of difference sets when $t = 0$ or $t = q - 1$. Throughout this paper, the researcher focuses exclusively on almost difference sets where t is not equal to 0 and not equal to $q - 1$.

An almost difference set D is categorized as abelian or cyclic (nonabelian or noncyclic) based on whether the group G is abelian or cyclic (nonabelian or noncyclic). Two almost difference sets D_1 and D_2 are considered equivalent if there exists an automorphism σ of G and an element $b \in G$ such that $\sigma(D_1) = D_2 + b$. Specifically, in the case of G being cyclic, D_1 and D_2 are equivalent if there exists an integer a with $\gcd(a, q) = 1$, such that $aD_1 = D_2 + b$ for some $b \in G$ (Ding et al., 2014).

If D is a (q, k, λ, t) almost difference set in an abelian group $(G, +)$, then $k(k-1) = t\lambda + (q-1-t)(\lambda+1)$. Moreover, its complement, $D^C = G \setminus D$ is also an almost difference set in $(G, +)$ with parameters $(q, q-k, q-2k+\lambda, t)$ (Ding, 2014).

Cyclotomic classes of finite fields are very useful building blocks for constructing almost difference sets. Let $q = nN + 1$ be a power of a prime and let α be a fixed primitive element of the Galois field $GF(q)$. Define $C_i^{(N,q)} := \alpha^i \langle \alpha^N \rangle$, where $\langle \alpha^N \rangle$ denotes the multiplicative group generated by α^N. The cosets $C_i^{(N,q)}$ are called the cyclotomic classes of order N in $GF(q)$.

Extensive research has been conducted on the construction of almost difference sets using cyclotomic classes. Nowak's work in 2014 provides insight into the utilization of cyclotomic classes of orders 2, 3, and 4 for generating almost difference sets. Ding (as cited in Ding, 2014) established the creation of almost difference sets from a single cyclotomic class of order 8, while Ding et al. (2014) presented the union of cyclotomic classes of the same order. Recently, Estrella (2023) devised almost difference sets from unions of cyclotomic classes of order 10. Moreover, Nowak et al. (2013) and Qi et al. (2016) constructed infinite families of almost difference sets by employing unions of cyclotomic classes of order 12 modulo a prime, specifically when $q = 12n + 1$ and n is odd. Additionally, Nowak et al. (2013) demonstrated that neither the multiplicative cyclic subgroup C of index twelve nor $C \cup \{0\}$ forms an almost difference set for specific finite fields. Despite these developments, the problem of constructing almost difference sets when n is even remains unresolved.

This paper revisits the construction of almost difference sets from cyclotomic classes of order 12 in the finite field $GF(q)$, where q is a prime less than 1000 and follows the form $q = 12n + 1$, with n being an integer greater than or equal to 1 (both even and odd). The researcher utilizes an exhaustive computer search to investigate this construction. Additionally, the author demonstrates that a single cyclotomic class of order 12, whether it includes zero or not, can generate almost difference sets. Furthermore, the paper examines the equivalence of the resulting almost difference sets up to complementation.

2.0 Methods

Building upon the research approach utilized by Balmaceda and Estrella (2021) as well as Estrella (2022) in their investigation of cyclotomic difference sets, this study explores the existence of almost difference sets through the implementation of cyclotomy with an order of 12. The computational methodology employed in this paper is based on Estrella's work in 2023. By taking a prime number q as input, the search method generates almost difference sets by combining two cyclotomic classes or up to eleven classes of $GF(q)$ with or without the residue zero. The search is conducted for all prime numbers $q < 1000$, where q follows the form $q = 12n + 1$. Additionally, the study determines whether the obtained almost difference sets, which share the same parameters, are equivalent up to complementation.

Python computer programs were implemented to execute the following steps, given an input prime number q:

1. Choose a primitive element α of the field $GF(q)$.
2. Compute the cyclotomic classes $C_i^{(12,q)}$ using the chosen primitive element.
3. Take the union of $C_0^{(12,q)}$ with a second cyclotomic class and test if the obtained set forms an almost difference set.
4. If no almost difference set is found, repeat steps 1–3 using a different primitive element until an almost difference set is obtained or until the primitive elements of $GF(q)$ are exhausted.
5. Repeat steps 1–4 using the union of $C_0^{(12,q)}$ with another cyclotomic class, until all unions of $C_0^{(12,q)}$ with a second cyclotomic class are exhausted.

6. Repeat steps 1–5, this time using ${C_0}^{(12,q)}$ with two other cyclotomic classes, then ${C_0}^{(12,q)}$ with three other cyclotomic classes, and so on up to ${C_0}^{(12,q)}$ with ten other cyclotomic classes.
7. For each almost difference set obtained, check its equivalence with other generated sets with the same parameters.

The same steps will be applied but include zero in the unions to search for other possible cyclotomic almost difference sets.

3.0 Results and Discussion

Let $q < 1000$ be a prime of the form $q = 12n + 1$ for any integer $n \geq 1$. Table 1 summarizes the parameters (q, k, λ, t), the unions of cyclotomic classes ${C_i}^{(12,q)}$ (with and without the residue zero) which form an almost difference set (up to equivalence) in the additive group $GF(q)$ for a properly chosen primitive element of $GF(q)$ employed to define the cyclotomic classes of order 12, and the class indicator that shows the family to which it belongs. These are:

P – Paley partial difference set (Theorem 5.4 (1) in Ding (2014))
P0 – Paley partial difference set together with zero
D – Theorem 5.4 (2) in Ding (2014)
D0 – Theorem 5.4 (3) in Ding (2014)
D1 – Theorem 5.4 (4) in Ding (2014)
D2 – Theorem 5.4 (5) in Ding (2014)
D3 – Theorem 5.5 in Ding (2014)
Q1 – Theorem 3.1 in Qi et al. (2016)
Q2 – Theorem 3.4 in Qi et al. (2016)
Q3 – Theorem 3.6 in Qi et al. (2016)
N – Theorem 9 in Nowak et al. (2013) or Theorem 3.3 in Qi et al. (2016)
New – Not equivalent to one of the above

Table 1. *Almost Difference Sets from Cyclotomic Classes of Order* 12 *(up to equivalence)*

	(q, k, λ, t)	**Almost Difference Sets**	**Class**
1	$(13, 2, 0, 10)$	${C_0}^{(12,q)} \cup {C_i}^{(12,q)}$ for any $1 \leq i \leq 11$ or ${C_0}^{(12,q)} \cup \{0\}$	New
2	$(13, 3, 0, 6)$	${C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_2}^{(12,q)}$ or ${C_0}^{(12,q)} \cup {C_i}^{(12,q)} \cup \{0\}$ for any $i \in \{1, 3, 4, 5, 7, 8, 9, 11\}$	New
3	$(13, 3, 0, 6)$	${C_0}^{(12,q)} \cup {C_4}^{(12,q)} \cup {C_8}^{(12,q)}$ or ${C_0}^{(12,q)} \cup {C_i}^{(12,q)} \cup \{0\}$ for any $i \in \{2, 10\}$	Q1 or D
4	$(13, 5, 1, 4)$	${C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_2}^{(12,q)} \cup {C_3}^{(12,q)} \cup {C_4}^{(12,q)}$ or ${C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_2}^{(12,q)} \cup {C_3}^{(12,q)} \cup \{0\}$	New
5	$(13, 5, 1, 4)$	${C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_2}^{(12,q)} \cup {C_3}^{(12,q)} \cup {C_6}^{(12,q)}$ or ${C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_4}^{(12,q)} \cup {C_5}^{(12,q)} \cup \{0\}$	New
6	$(13, 5, 1, 4)$	${C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_2}^{(12,q)} \cup {C_4}^{(12,q)} \cup {C_5}^{(12,q)}$ or ${C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_2}^{(12,q)} \cup {C_4}^{(12,q)} \cup \{0\}$	New
7	$(13, 6, 2, 6)$	${C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_2}^{(12,q)} \cup {C_3}^{(12,q)} \cup {C_4}^{(12,q)} \cup {C_6}^{(12,q)}$ or ${C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_2}^{(12,q)} \cup {C_3}^{(12,q)} \cup {C_6}^{(12,q)} \cup \{0\}$	New
8	$(13, 6, 2, 6)$	${C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_4}^{(12,q)} \cup {C_5}^{(12,q)} \cup {C_8}^{(12,q)} \cup {C_9}^{(12,q)}$ or ${C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_2}^{(12,q)} \cup {C_3}^{(12,q)} \cup {C_9}^{(12,q)} \cup \{0\}$	N or D2
9	$(13, 6, 2, 6)$	${C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_2}^{(12,q)} \cup {C_3}^{(12,q)} \cup {C_5}^{(12,q)} \cup {C_6}^{(12,q)}$ or ${C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_2}^{(12,q)} \cup {C_3}^{(12,q)} \cup {C_4}^{(12,q)} \cup \{0\}$	New
10	$(13, 6, 2, 6)$	${C_0}^{(12,q)} \cup {C_2}^{(12,q)} \cup {C_4}^{(12,q)} \cup {C_6}^{(12,q)} \cup {C_8}^{(12,q)} \cup {C_{10}}^{(12,q)}$ or ${C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_3}^{(12,q)} \cup {C_8}^{(12,q)} \cup {C_9}^{(12,q)} \cup \{0\}$	P
11	$(13, 7, 3, 6)$	${C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_2}^{(12,q)} \cup {C_3}^{(12,q)} \cup {C_4}^{(12,q)} \cup {C_5}^{(12,q)} \cup {C_6}^{(12,q)}$ or ${C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_2}^{(12,q)} \cup {C_3}^{(12,q)} \cup {C_4}^{(12,q)} \cup {C_7}^{(12,q)} \cup \{0\}$	New

Table 1. *Almost Difference Sets from Cyclotomic Classes of Order 12 (up to equivalence) cont.*

	(q, k, λ, t)	**Almost Difference Sets**	**Class**
12	$(13, 7, 3, 6)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)}$ or $C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)} \cup \{0\}$	Q3
13	$(13, 7, 3, 6)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_7^{(12,q)} \cup C_8^{(12,q)}$ or $C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup \{0\}$	New
14	$(13, 7, 3, 6)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_5^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)}$ or $C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_5^{(12,q)} \cup C_8^{(12,q)} \cup \{0\}$	New
15	$(13, 8, 4, 4)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)}$ or $C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup \{0\}$	New
16	$(13, 8, 4, 4)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)}$ or $C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_8^{(12,q)} \cup \{0\}$	New
17	$(13, 8, 4, 4)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)}$ or $C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)} \cup \{0\}$	New
18	$(13, 10, 7, 6)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)}$ or $C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)} \cup C_8^{(12,q)} \cup \{0\}$	New
19	$(13, 10, 7, 6)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)} \cup C_8^{(12,q)} \cup C_{10}^{(12,q)}$ or $C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)} \cup C_{10}^{(12,q)} \cup \{0\}$	New
20	$(13, 11, 9, 10)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)} \cup C_{10}^{(12,q)}$ or $C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)} \cup \{0\}$	New
21	$(37, 3, 0, 30)$	$C_0^{(12,q)} = \{1, 10, 26\}$	New
22	$(37, 4, 0, 24)$	$C_0^{(12,q)} \cup \{0\} = \{0, 1, 10, 26\}$	New
23	$(37, 6, 0, 6)$	$C_0^{(12,q)} \cup C_i^{(12,q)}$ for any $i \in \{2, 10\}$	New
24	$(37, 6, 0, 6)$	$C_0^{(12,q)} \cup C_i^{(12,q)}$ for any $i \in \{4, 8\}$	New
25	$(37, 7, 1, 30)$	$C_0^{(12,q)} \cup C_i^{(12,q)} \cup \{0\}$ for any $i \in \{3, 9\}$	New
26	$(37, 10, 2, 18)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup \{0\}$	New
27	$(37, 10, 2, 18)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_3^{(12,q)} \cup \{0\}$	New
28	$(37, 10, 2, 18)$	$C_0^{(12,q)} \cup C_4^{(12,q)} \cup C_8^{(12,q)} \cup \{0\}$	Q2 or D0
29	$(37, 12, 3, 12)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_4^{(12,q)} \cup C_7^{(12,q)}$	New
30	$(37, 12, 3, 12)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_4^{(12,q)} \cup C_9^{(12,q)}$	New
31	$(37, 13, 4, 24)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_4^{(12,q)} \cup C_7^{(12,q)} \cup \{0\}$	New
32	$(37, 13, 4, 24)$	$C_0^{(12,q)} \cup C_3^{(12,q)} \cup C_6^{(12,q)} \cup C_9^{(12,q)} \cup \{0\}$	New
33	$(37, 15, 5, 6)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_7^{(12,q)}$	New
34	$(37, 16, 6, 12)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_7^{(12,q)} \cup \{0\}$	New

Table 1. *Almost Difference Sets from Cyclotomic Classes of Order 12 (up to equivalence) cont.*

	(q, k, λ, t)	**Almost Difference Sets**	**Class**
35	(37, 16, 6, 12)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup \{0\}$	New
36	(37, 16, 6, 12)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup \{0\}$	New
37	(37, 18, 8, 18)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_9^{(12,q)}$	New
38	(37, 18, 8, 18)	$C_0^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_{10}^{(12,q)}$	P
39	(37, 19, 9, 18)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_9^{(12,q)} \cup \{0\}$	New
40	(37, 19, 9, 18)	$C_0^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_{10}^{(12,q)} \cup \{0\}$	P0
41	(37, 21, 11, 12)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_9^{(12,q)}$	New
42	(37, 21, 11, 12)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_7^{(12,q)} \cup C_8^{(12,q)}$	New
43	(37, 21, 11, 12)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)}$	New
44	(37, 22, 12, 6)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_9^{(12,q)} \cup \{0\}$	New
45	(37, 24, 15, 24)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)}$	New
46	(37, 24, 15, 24)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)} \cup C_9^{(12,q)} \cup C_{10}^{(12,q)}$	New
47	(37, 25, 16, 12)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)} \cup \{0\}$	New
48	(37, 25, 16, 12)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_9^{(12,q)} \cup C_{10}^{(12,q)} \cup \{0\}$	New
49	(37, 27, 19, 18)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)} \cup C_8^{(12,q)}$	New
50	(37, 27, 19, 18)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)} \cup C_9^{(12,q)}$	New
51	(37, 27, 19, 18)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)} \cup C_{10}^{(12,q)}$	New
52	(37, 30, 24, 30)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)} \cup C_9^{(12,q)} \cup C_{10}^{(12,q)}$	New
53	(37, 31, 25, 6)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)} \cup C_8^{(12,q)} \cup C_{10}^{(12,q)} \cup \{0\}$	New
54	(37, 31, 25, 6)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)} \cup C_{10}^{(12,q)} \cup \{0\}$	New
55	(37, 33, 29, 24)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)} \cup C_{10}^{(12,q)}$	New
56	(37, 34, 31, 30)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)} \cup C_{10}^{(12,q)} \cup \{0\}$	New
57	(61, 5, 0, 40)	$C_0^{(12,q)} = \{1, 9, 20, 34, 58\}$	New
58	(61, 6, 0, 30)	$C_0^{(12,q)} \cup \{0\} = \{0, 1, 9, 20, 34, 58\}$	New
59	(61, 10, 1, 30)	$C_0^{(12,q)} \cup C_i^{(12,q)}$ for any $i \in \{1, 5, 7, 11\}$	New
60	(61, 15, 3, 30)	$C_0^{(12,q)} \cup C_4^{(12,q)} \cup C_8^{(12,q)}$	Q1 or D
61	(61, 15, 3, 30)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_3^{(12,q)}$	New
62	(61, 30, 14, 30)	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_7^{(12,q)} \cup C_8^{(12,q)}$	New

Table 1. *Almost Difference Sets from Cyclotomic Classes of Order 12 (up to equivalence) cont.*

	(q, k, λ, t)	**Almost Difference Sets**	**Class**
63	$(61, 30, 14, 30)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_9^{(12,q)}$	New
64	$(61, 30, 14, 30)$	$C_0^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_{10}^{(12,q)}$	P
65	$(61, 31, 15, 30)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_7^{(12,q)} \cup C_8^{(12,q)} \cup \{0\}$	New
66	$(61, 31, 15, 30)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_9^{(12,q)} \cup \{0\}$	New
67	$(61, 31, 15, 30)$	$C_0^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_{10}^{(12,q)} \cup \{0\}$	P0
68	$(61, 46, 34, 30)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)} \cup C_9^{(12,q)} \cup \{0\}$	New
69	$(61, 46, 34, 30)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)} \cup C_{10}^{(12,q)} \cup \{0\}$	New
70	$(61, 51, 42, 30)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)} \cup \{0\}$	New
71	$(61, 55, 49, 30)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)} \cup C_{10}^{(12,q)}$	New
72	$(61, 56, 51, 40)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)} \cup C_{10}^{(12,q)} \cup \{0\}$	New
73	$(109, 27, 6, 54)$	$C_0^{(12,q)} \cup C_4^{(12,q)} \cup C_8^{(12,q)}$	Q1 or D
74	$(109, 45, 18, 72)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)}$	New
75	$(109, 64, 37, 72)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_7^{(12,q)} \cup C_8^{(12,q)} \cup \{0\}$	New
76	$(109, 82, 61, 54)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)} \cup C_{10}^{(12,q)} \cup \{0\}$	New
77	$(229, 38, 6, 190)$	$C_0^{(12,q)} \cup C_i^{(12,q)}$ for any $i \in \{4, 8\}$	New
78	$(229, 39, 6, 114)$	$C_0^{(12,q)} \cup C_i^{(12,q)} \cup \{0\}$ for any $i \in \{4, 8\}$	New
79	$(229, 114, 56, 114)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)}$	N or D2
80	$(229, 114, 56, 114)$	$C_0^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_{10}^{(12,q)}$	P
81	$(229, 115, 57, 114)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)} \cup \{0\}$	Q6
82	$(229, 115, 57, 114)$	$C_0^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_{10}^{(12,q)} \cup \{0\}$	P0
83	$(229, 190, 157, 114)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)} \cup C_{10}^{(12,q)}$	New
84	$(229, 191, 159, 190)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)} \cup C_{10}^{(12,q)} \cup \{0\}$	New
85	$(349, 87, 21, 174)$	$C_0^{(12,q)} \cup C_4^{(12,q)} \cup C_8^{(12,q)}$	Q1 or D
86	$(349, 262, 196, 174)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)} \cup C_{10}^{(12,q)} \cup \{0\}$	New
87	$(373, 94, 23, 186)$	$C_0^{(12,q)} \cup C_4^{(12,q)} \cup C_8^{(12,q)} \cup \{0\}$	Q2 or D0
88	$(373, 279, 208, 186)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)} \cup C_{10}^{(12,q)}$	New
89	$(733, 366, 182, 366)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)}$	N or D2
90	$(733, 366, 182, 366)$	$C_0^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_{10}^{(12,q)}$	P

Table 1. *Almost Difference Sets from Cyclotomic Classes of Order 12 (up to equivalence) cont.*

	(q, k, λ, t)	**Almost Difference Sets**	**Class**
91	$(733, 367, 183, 366)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)} \cup \{0\}$	Q3
92	$(733, 367, 183, 366)$	$C_0^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_{10}^{(12,q)} \cup \{0\}$	P0
93	$(877, 146, 24, 730)$	$C_0^{(12,q)} \cup C_i^{(12,q)}$ for any $i \in \{3, 9\}$	New
94	$(877, 147, 24, 438)$	$C_0^{(12,q)} \cup C_i^{(12,q)} \cup \{0\}$ for any $i \in \{3, 9\}$	New
95	$(877, 730, 607, 438)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)} \cup C_9^{(12,q)} \cup C_{10}^{(12,q)}$	New
96	$(877, 731, 609, 730)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup C_7^{(12,q)} \cup C_9^{(12,q)} \cup C_{10}^{(12,q)} \cup \{0\}$	New

Based on the findings, a single cyclotomic class $C_0^{(12,q)}$ can produce almost difference sets if $q = 37, 61$. On the other hand, a single cyclotomic class together with zero, $C_0^{(12,q)} \cup \{0\}$, can form almost difference sets if $q = 13, 37, 61$. There exist three new inequivalent $(13, 5, 1, 4)$ almost difference sets generated from unions of five cyclotomic classes, two new inequivalent $(13, 6, 2, 6)$ almost difference sets generated from six cyclotomic classes, two new inequivalent $(37, 6, 0, 6)$ almost difference sets generated from two cyclotomic classes, two new inequivalent $(37, 10, 2, 18)$ almost difference sets generated from three cyclotomic classes together with zero, two new inequivalent $(37, 12, 3, 12)$ almost difference sets generated from four cyclotomic classes, two new inequivalent $(37, 13, 4, 24)$ almost difference sets generated from four cyclotomic classes together with zero, three new $(37, 16, 6, 24)$ almost difference sets generated from five cyclotomic classes together with zero, and two new inequivalent $(61, 30, 14, 30)$ almost difference sets generated from six cyclotomic classes. There are also new constructions for $q = 109, 229, 877$.

If we restrict our attention to almost difference set D with $|D| \leq q/2$, the results are summarized in Table 2 up to complementation.

Table 2. *Almost Difference Sets from Cyclotomic Classes of Order* 12 *(up to complementation)*

	(q, k, λ, t)	**Almost Difference Sets**	**Class**
1	$(13, 2, 0, 10)$	$C_0^{(12,q)} \cup C_i^{(12,q)}$ for any $1 \leq i \leq 11$ or $C_0^{(12,q)} \cup \{0\}$	New
2	$(13, 3, 0, 6)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)}$ or $C_0^{(12,q)} \cup C_i^{(12,q)} \cup \{0\}$ for any $i \in \{1, 3, 4, 5, 7, 8, 9, 11\}$	New
3	$(13, 3, 0, 6)$	$C_0^{(12,q)} \cup C_4^{(12,q)} \cup C_8^{(12,q)}$ or $C_0^{(12,q)} \cup C_i^{(12,q)} \cup \{0\}$ for any $i \in \{2, 10\}$	Q1 or D
4	$(13, 5, 1, 4)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)}$ or $C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup \{0\}$	New
5	$(13, 5, 1, 4)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_6^{(12,q)}$ or $C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup \{0\}$	New
6	$(13, 5, 1, 4)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)}$ or $C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup \{0\}$	New
7	$(13, 6, 2, 6)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)}$ or $C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_6^{(12,q)} \cup \{0\}$	New
8	$(13, 6, 2, 6)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)}$ or $C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_9^{(12,q)} \cup \{0\}$	N or D2
9	$(13, 6, 2, 6)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)}$ or $C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup \{0\}$	New

Table 2. *Almost Difference Sets from Cyclotomic Classes of Order 12 (up to complementation) cont.*

	(q, k, λ, t)	**Almost Difference Sets**	**Class**
10	$(13, 6, 2, 6)$	$C_0^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_{10}^{(12,q)}$ or $C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_3^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)} \cup \{0\}$	P
11	$(37, 3, 0, 30)$	$C_0^{(12,q)} = \{1, 10, 26\}$	New
12	$(37, 4, 0, 24)$	$C_0^{(12,q)} \cup \{0\} = \{0, 1, 10, 26\}$	New
13	$(37, 6, 0, 6)$	$C_0^{(12,q)} \cup C_i^{(12,q)}$ for any $i \in \{2, 10\}$	New
14	$(37, 6, 0, 6)$	$C_0^{(12,q)} \cup C_i^{(12,q)}$ for any $i \in \{4, 8\}$	New
15	$(37, 7, 1, 30)$	$C_0^{(12,q)} \cup C_i^{(12,q)} \cup \{0\}$ for any $i \in \{3, 9\}$	New
16	$(37, 10, 2, 18)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup \{0\}$	New
17	$(37, 10, 2, 18)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_3^{(12,q)} \cup \{0\}$	New
18	$(37, 10, 2, 18)$	$C_0^{(12,q)} \cup C_4^{(12,q)} \cup C_8^{(12,q)} \cup \{0\}$	Q2 or D0
19	$(37, 12, 3, 12)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_4^{(12,q)} \cup C_7^{(12,q)}$	New
20	$(37, 12, 3, 12)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_4^{(12,q)} \cup C_9^{(12,q)}$	New
21	$(37, 13, 4, 24)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_4^{(12,q)} \cup C_7^{(12,q)} \cup \{0\}$	New
22	$(37, 13, 4, 24)$	$C_0^{(12,q)} \cup C_3^{(12,q)} \cup C_6^{(12,q)} \cup C_9^{(12,q)} \cup \{0\}$	New
23	$(37, 15, 5, 6)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_7^{(12,q)}$	New
24	$(37, 16, 6, 12)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_7^{(12,q)} \cup \{0\}$	New
25	$(37, 16, 6, 12)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)} \cup \{0\}$	New
26	$(37, 16, 6, 12)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup \{0\}$	New
27	$(37, 18, 8, 18)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_9^{(12,q)}$	New
28	$(37, 18, 8, 18)$	$C_0^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_{10}^{(12,q)}$	P
29	$(61, 5, 0, 40)$	$C_0^{(12,q)} = \{1, 9, 20, 34, 58\}$	New
30	$(61, 6, 0, 30)$	$C_0^{(12,q)} \cup \{0\} = \{0, 1, 9, 20, 34, 58\}$	New
31	$(61, 10, 1, 30)$	$C_0^{(12,q)} \cup C_i^{(12,q)}$ for any $i \in \{1, 5, 7, 11\}$	New
32	$(61, 15, 3, 30)$	$C_0^{(12,q)} \cup C_4^{(12,q)} \cup C_8^{(12,q)}$	Q1 or D
33	$(61, 15, 3, 30)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_3^{(12,q)}$	New
34	$(61, 30, 14, 30)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_7^{(12,q)} \cup C_8^{(12,q)}$	New
35	$(61, 30, 14, 30)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_9^{(12,q)}$	New
36	$(61, 30, 14, 30)$	$C_0^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_{10}^{(12,q)}$	P
37	$(109, 27, 6, 54)$	$C_0^{(12,q)} \cup C_4^{(12,q)} \cup C_8^{(12,q)}$	Q1 or D
38	$(109, 45, 18, 72)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)}$	New
39	$(229, 38, 6, 190)$	$C_0^{(12,q)} \cup C_i^{(12,q)}$ for any $i \in \{4, 8\}$	New
40	$(229, 39, 6, 114)$	$C_0^{(12,q)} \cup C_i^{(12,q)} \cup \{0\}$ for any $i \in \{4, 8\}$	New

Table 2. *Almost Difference Sets from Cyclotomic Classes of Order 12 (up to complementation) cont.*

	(q, k, λ, t)	**Almost Difference Sets**	**Class**
41	$(229, 114, 56, 114)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)}$	N or D2
42	$(229, 114, 56, 114)$	$C_0^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_{10}^{(12,q)}$	P
43	$(349, 87, 21, 174)$	$C_0^{(12,q)} \cup C_4^{(12,q)} \cup C_8^{(12,q)}$	Q1 or D
44	$(373, 94, 23, 186)$	$C_0^{(12,q)} \cup C_4^{(12,q)} \cup C_8^{(12,q)} \cup \{0\}$	Q2 or D0
45	$(733, 366, 182, 366)$	$C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_4^{(12,q)} \cup C_5^{(12,q)} \cup C_8^{(12,q)} \cup C_9^{(12,q)}$	N or D2
46	$(733, 366, 182, 366)$	$C_0^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_{10}^{(12,q)}$	P
47	$(877, 146, 24, 730)$	$C_0^{(12,q)} \cup C_i^{(12,q)}$ for any $i \in \{3, 9\}$	New
48	$(877, 147, 24, 438)$	$C_0^{(12,q)} \cup C_i^{(12,q)} \cup \{0\}$ for any $i \in \{3, 9\}$	New

In addition, the set $D = C_0^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_{10}^{(12,q)}$ is an almost difference set in $(GF(q), +)$ with parameters $(q, (q-1)/2, (q-5)/4, (q-1)/2)$ where $q \equiv 1 \ (mod\ 4)$. This set is equivalent to Paley partial difference set. Similarly, the set $D = C_0^{(12,q)} \cup C_2^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)} \cup C_8^{(12,q)} \cup C_{10}^{(12,q)} \cup \{0\}$ is also an almost difference set in $(GF(q), +)$ with parameters $(q, (q+1)/2, (q-1)/4, (q-1)/2)$ where $q \equiv 1 \ (mod\ 4)$ which is equivalent to Paley partial difference set with the residue zero. These constructions can generate infinitely many almost difference sets with such parameters in $(GF(q), +)$, for example, $q = 13, 37, 61, 73, 97, 109, 157, 181, 193, 229, 241, 277, 313, 337, 349, 373, 397, 409, 421, 433, 457, 541, 577, 601, 613, 661, 673, 709, 733, 757, 769, 829, 853, 877, 937, 997, \ldots$. Furthermore, these constructions showed that almost difference sets can be constructed from the cyclotomic classes of order twelve modulo a prime $q = 12n + 1$ with an even n, for example, $q = 73, 97, 193, 241, 313, 337, 409, 433, 457, 577, 601, 673, 769,$ and 937.

The following are some examples of almost difference sets generated from unions of cyclotomic classes of order 12.

Example 3.1 Let $q = 13$, and let the primitive element $\alpha = 6$. Then

$$D = C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)}$$
$$= \{1, 6, 8, 9, 10\}$$

is a $(13, 5, 1, 4)$ almost difference set in $(GF(13), +)$.

Example 3.2 Let $q = 13$, and let the primitive element $\alpha = 2$. Then

$$D = C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_4^{(12,q)} \cup C_6^{(12,q)}$$
$$= \{1, 2, 3, 4, 8, 12\}$$

is a $(13, 6, 2, 6)$ almost difference set in $(GF(13), +)$. This set is not a Paley partial difference set.

Example 3.3 Let $q = 13$, and let the primitive element $\alpha = 7$. Then

$$D = C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup C_3^{(12,q)} \cup C_5^{(12,q)} \cup C_6^{(12,q)}$$
$$= \{1, 5, 7, 10, 11, 12\}$$

is a $(13, 6, 2, 6)$ almost difference set in $(GF(13), +)$. This set is not a Paley partial difference set.

Example 3.4 Let $q = 37$, and let the primitive element $\alpha = 17$. Then

$$D = C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_2^{(12,q)} \cup \{0\}$$
$$= \{0, 1, 3, 4, 10, 17, 22, 26, 30, 35\}$$

is a $(37, 10, 2, 18)$ almost difference set in $(GF(37), +)$.

Example 3.5 Let $q = 37$, and let the primitive element $\alpha = 2$. Then

$$D = C_0^{(12,q)} \cup C_1^{(12,q)} \cup C_3^{(12,q)} \cup \{0\}$$

$= \{0, 1, 2, 6, 8, 10, 15, 20, 23, 26\}$

is a $(37, 10, 2, 18)$ almost difference set in $(GF(37), +)$.

Example 3.6 Let $q = 37$, and let the primitive element $\alpha = 2$. Then

$D = {C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_4}^{(12,q)} \cup {C_7}^{(12,q)}$

$= \{1, 2, 9, 10, 12, 15, 16, 17, 20, 22, 26, 35\}$

is a $(37, 12, 3, 12)$ almost difference set in $(GF(37), +)$.

Example 3.7 Let $q = 37$, and let the primitive element $\alpha = 2$. Then

$D = {C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_3}^{(12,q)} \cup {C_4}^{(12,q)} \cup {C_6}^{(12,q)} \cup {C_9}^{(12,q)}$

$= \{1, 2, 6, 8, 9, 10, 11, 12, 14, 15, 16, 20, 23, 26, 27, 29, 31, 36\}$

is a $(37, 18, 8, 18)$ almost difference set in $(GF(37), +)$. This set is not a Paley partial difference set.

Example 3.8 Let $q = 61$, and let the primitive element $\alpha = 2$. Then

$D = {C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_2}^{(12,q)} \cup {C_3}^{(12,q)} \cup {C_7}^{(12,q)} \cup {C_8}^{(12,q)}$

$= \{1, 2, 4, 6, 7, 8, 9, 11, 12, 14, 18, 19, 20, 21, 25, 28, 34, 36, 37, 38, 40, 42, 43, 47, 49,$
$54, 55, 57, 58, 59\}$

is a $(61, 30, 14, 30)$ almost difference set in $(GF(61), +)$. This set is not a Paley partial difference set.

Example 3.9 Let $q = 61$, and let the primitive element $\alpha = 10$. Then

$D = {C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_3}^{(12,q)} \cup {C_4}^{(12,q)} \cup {C_6}^{(12,q)} \cup {C_9}^{(12,q)}$

$= \{1, 3, 8, 9, 10, 11, 12, 17, 20, 23, 24, 25, 27, 28, 29, 31, 33, 34, 35, 37, 38, 41, 42, 47,$
$50, 52, 53, 57, 58, 60\}$

is a $(61, 30, 14, 30)$ almost difference set in $(GF(61), +)$. This set is not a Paley partial difference set.

Example 3.10 Let $q = 37$, and let the primitive element $\alpha = 2$. Then

$D = {C_0}^{(12,q)} \cup {C_2}^{(12,q)} \cup {C_4}^{(12,q)} \cup {C_6}^{(12,q)} \cup {C_8}^{(12,q)} \cup {C_{10}}^{(12,q)}$

$= \{1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36\}$

is a $(37, 18, 8, 18)$ almost difference set in $(GF(37), +)$. This set is a Paley partial difference set.

4.0 Conclusion

This paper presented a new construction of almost difference sets via cyclotomy of order 12. Moreover, the equivalence of the obtained almost difference sets having the same parameters was determined up to complementation.

Based on the findings, we have constructed a $(q, (q-1)/2, (q-5)/4, (q-1)/2)$ almost difference set in $GF(q)$ from the union of six cyclotomic classes of order 12, where $q \equiv 1\ (mod\ 4)$. This set is equivalent to Paley partial difference set and can generate sequences of period $q \equiv 1\ (\mathrm{mod}\ 4)$, where $k = \frac{q-1}{2}$. Similarly, the same union of six cyclotomic classes together with zero forms an almost difference set with parameters $(q, (q+1)/2\,, (q-1)/4,\ (q-1)/2)$ where $q \equiv 1\ (mod\ 4)$.

In addition, we also have found three inequivalent $(q, (q-3)/2, (q-9)/4, (q-5)/2)$ almost difference sets in $GF(q)$ from unions of five cyclotomic classes of order 12, where $q = 13$. The obtained $(13, 5, 1, 4)$ almost difference sets can generate sequences of period $q \equiv 1\ (\mathrm{mod}\ 4)$ with optimal autocorrelation values -1 and 3, where $k = 5$.

Furthermore, there exist two new inequivalent $(13, 6, 2, 6)$ almost difference sets which are not partial difference sets, two new inequivalent $(37, 6, 0, 6)$ almost difference sets, two new inequivalent $(37, 10, 2, 18)$ almost difference sets, two new inequivalent $(37, 12, 3, 12)$ almost difference sets, two new inequivalent $(37, 13, 4, 24)$ almost difference sets, three new $(37, 16, 6, 24)$ almost difference sets, and two new inequivalent $(61, 30, 14, 30)$ almost difference sets which are not partial difference sets, all generated from

unions of suitable cyclotomic classes of order 12. Other new almost difference sets are also constructed for $q = 109, 229, 877$.

The question of whether the set $D = {C_0}^{(12,q)} \cup {C_1}^{(12,q)} \cup {C_3}^{(12,q)} \cup {C_4}^{(12,q)} \cup {C_6}^{(12,q)} \cup {C_9}^{(12,q)}$ belongs to an infinite family of almost difference sets that are different from the Paley partial difference set remains unresolved. However, it has been established that this set can be considered an almost difference set when q is equal to either 37 or 61. It is intriguing to explore the conditions under which q satisfies this property and to extend its parameters in a general context.

It is still an open problem to generalize and prove that the set $D = {C_0}^{(12,q)} \cup {C_2}^{(12,q)} \cup {C_4}^{(12,q)} \cup {C_6}^{(12,q)} \cup {C_8}^{(12,q)} \cup {C_{10}}^{(12,q)}$ is an almost difference set in $(GF(q), +)$ with parameters $(q, (q-1)/2, (q-5)/4, (q-1)/2)$ for all $q \equiv 1\ (mod\ 4)$ 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. https://doi.org/10.56899/150.6B.16

Davis, J. A. (1992). Almost difference sets and reversible difference sets. *Archiv Der Mathematik. 59*(6), 595–602. https://doi.org/10.1007/BF01194853

Ding, C. (1994). The differential cryptanalysis and design of the natural stream ciphers. In *R. Anderson Fast software encryption: Cambridge security workshop, Cambridge, U.K., December 9-11, 1993 proceedings,* (pp. 101–115). https://doi.org/10.1007/3-540-58108-1

Ding, C. (2014). *Codes from difference sets.* World Scientific. https://doi.org/10.1142/9283

Ding, C., & Feng, T. (2008). Codebooks from almost difference sets. *Designs, Codes and Cryptography, 46,* 113-126. https://doi.org/10.1007/s10623-007-9140-z

Ding, C., Helleseth, T. & Martinsen, H. M. (2001). New families of binary sequences with optimal three-level autocorrelation. *IEEE Trans. Information Theory, 47*(1), 428–433. https://doi.org/10.1109/18.904555

Ding, C., Pott, A. & Wang, Q. (2014). Constructions of almost difference sets from finite fields. *Designs, Codes and Cryptography, 72,* 581-592. https://doi.org/10.1007/s10623-012-9789-9

Estrella, B. M. (2022). Construction of difference sets from unions of cyclotomic classes of order N=14. R*ecoletos Multidisciplinary Research Journal, 10*(1), 67-76. https://doi.org/10.32871/rmrj2210.01.04

Estrella, B. M. (2023). Construction of almost difference sets from unions of cyclotomic classes of order 10. In E.P. Sheehan & M. Kohler (Eds.), Book of abstracts: The *9th International Conference on Education 2023 (ICEDU 2023)* (p. 42). The International Institute of Knowledge Management. https://www.researchgate.net/publication/370231464_Book_of_Abstracts_of_The_9th_International_Conference_on_Education_ICEDU_2023

Heng, Z. (2023). Projective linear codes from some almost difference sets. *IEEE Transactions on Information Theory, 69*(2), 978-994. https://doi.org/10.1109/TIT.2022.3203380

Nowak, K. (2014, August 30). *A survey on almost difference sets*. arXiv. https://doi.org/10.48550/arXiv.1409.0114

Nowak, K., Olmez, O., & Song, S. Y. (2013, October 4). *Almost difference sets, normally regular digraphs and cyclotomic schemes fom cyclotomy of order twelve*. arXiv. https://doi.org/10.48550/arXiv.1310.1164

Qi, M., Xiong, S., Yuan, J., Rao, W., & Zhong, L. (2016). On some new families of almost difference sets constructed from cyclotomic classes of order 12. *IEEE Communications Letters, 20*(1), 61-64. https://doi.org/10.1109/LCOMM.2015.2503279