IEICE TRANSACTIONS

on Fundamentals of Electronics, Communications and Computer Sciences

DOI:10.1587/transfun.2024EAL2044

Publicized:2024/07/12

A PUBLICATION OF THE ENGINEERING SCIENCES SOCIETY

The Institute of Electronics, Information and Communication Engineers

Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3 chome, Minato-ku, TOKYO, 105-0011 JAPAN

LETTER

Difference Unit Groups in $\mathbb{Z}_n$*

Zongxiang YI[†a)], ***Member and*** **Qiuxia XU**[†b)], ***Nonmember***

SUMMARY In 2004, Ryoh Fuji-Hara *et al.* (IEEE Trans. Inf. Theory. 50(10):2408-2420, 2004) proposed an open problem of finding a maximum multiplicative subgroup G in $\mathbb{Z}_n$ satisfying two conditions: (1) the sum of any two distinct elements in G is nonzero; (2) any difference from G is still a unit in $\mathbb{Z}_n$. The subgroups satisfying Condition (2) is called difference unit group. Difference unit group is related to difference packing, zero-difference balanced function and partitioned difference family, and thus have many applications in coding and communication.

Suppose the canonical factorization of n is $\prod_{i=1}^{k} p_i^{e_i}$. In this letter, we mainly answer the open problem with the result that the maximum cardinality of such a subgroup G is $\frac{d}{2^m}$, where $d = \gcd(p_1 - 1, p_2 - 1, \cdots, p_k - 1)$ and $m = \nu_2(d)$. Also an explicit construction of such a subgroup is introduced.

key words: *Frequency Hopping Sequence, Difference Unit Group, Difference Packing*

1. Introduction

In 2004, Fuji-Hara et al. established a connection between optimal frequency hopping sequences (FHS) and partition type difference packings (DP) from a combinatorial approach [1]. For a full account of difference packings, please refer to [2]. In this letter, we concern on a special class of subgroups on $\mathbb{Z}_n$, which was implicitly introduced by Fuji-Hara et al.[1] and explicitly defined by Chung et al.[3].

Definition 1. *[1, 3] Let R be a ring and $R^\times$ be the set of all units. A subset S of $R^\times$ is called a difference unit set (DUS) if $s_1 - s_2 \in R^\times$ for any two distinct elements $s_1 \in S$ and $s_2 \in S$. S is called a difference unit group (DUG) if S is a DUS and a subgroup of $R^\times$. For a ring R, a DUG G is called a maximal DUG if $\#S \le \#G$ for any DUG S.*

This concept was generalized to a generic ring R by Cao et al.[4, Page 182] and the idea of this concept was connected to Ferrero pair by Buratti[5, Lemma 3.2]. There are many topics related to difference unit set(group), such as difference packing[1], frequency hopping sequence[3, 4], zero-difference balanced function[6, 7], external difference family[8] and difference family[5].

In this letter, we solve an open problem[1, Problem 5.5] about difference unit group on $\mathbb{Z}_v$, proposed by Fuji-Hara et al. in 2004:

Problem 2. *Find a maximum multiplicative subgroup G of $\mathbb{Z}_v^\times$ such that $\theta + \theta' \not\equiv 0 \pmod v$ for any $\theta \neq \theta'$, $\theta, \theta' \in G$, and that any difference from G is still a unit in $\mathbb{Z}_v$. Here the term "maxinum" means that the subgroup is the maximum cardinality among all subgroups satisfying the above conditions.*

Our work is quit different from the previous studies. On one hand, Reference [8] studies the cyclic DUG over rings, such as Z_n but the DUG can be non-cyclic over other rings (See Reference [7] for examples). On the other hand, Reference [7, 12] concerns the fact that, if $n \ge 3$ and G is a DUG in $\mathbb{Z}_n$, then $-1 \in G$ if and only if $2 \mid \#G$ (It is not true if G is not a DUG). Moreover, they concern the feasible sizes of DUGs while the maximum size of a DUG is concerned in this letter.

Our solution to this problem consists of two steps:

1. Proof that the DUG must be cyclic in $\mathbb{Z}_n$;
2. Obtain the maximum DUG in $\mathbb{Z}_n$ and hence solve Problem 2.

Moreover, we give a method to construct the maximum subgroup in Problem 2.

The rest of this letter is organized as follows: Section 2 introduces some notations used in this letter. Then the solution to the open problem is proposed in Section 3. Finally we conclude in Section 4

2. Notations

Here are some notations which will be used in this letter.

- $R^\times$: the set of all units in ring R;
- $\mathrm{char}(R)$: the characteristic of ring R;
- $\nu_p(n)$: p-adic order of n, i.e., the integer e such that $p^e \mid n$ and $p^{e+1} \nmid n$;
- $R_1 \cong R_2$: R_1 is isomorphic to R_2 and there is an isomorphism from R_1 to R_2.
- $\mathbb{Z}_n$: the residual class ring over integers $\mathbb{Z}$;

[†]The author is with the School of Mathematics and Systems Science, Guangdong Polytechnic Normal University, Guangzhou 510665, China, and the Guangdong Provincial Key Laboratory of Information Security Technology, Guangzhou University, Guangzhou 510006, China.

[*]The research of Zongxiang Yi was supported by the Talent Special Project of Research Project of Guangdong Polytechnic Normal University [Grant No. 2021SDKYA051], Scientific Research Capacity Improvement Project of the Doctoral Program Construction Unit of Guangdong Polytechnic Normal University [Grant No. 22GPNUZDJS31]. The research of Qiuxia Xu was supported by the National Natural Science Foundation of China [Grant No. 12201133], Special Research Basic and Applied Research Foundation of Guangzhou [Grant No. 2023A04J0365] and Special Fund for Scientific Research Talents of GPNU [Grant No. 2021SDKYA029].

a) E-mail: tpu01yzx@gmail.com
b) E-mail: xia_mi0622@126.com

- $\mathbb{F}_q$: the finite field with q elements;
- $\#G$: the cardinality of the set G;
- $H \leq G$: group H is a subgroup of group G;
- $\langle g \rangle$: the group generated by element g, i.e., $G = \{g^i \mid i \in \mathbb{Z}\}$.

3. Solution to An Open Problem on Difference Unit Group

In this section, we consider the difference unit groups over $\mathbb{Z}_n$. It is easy to see that if n is even, then $a - b$ can not be a unit for all $a, b \in \mathbb{Z}_n^\times$. So when n is even, the maximum difference unit group is the only one group $G_0 = \{1\}$. So in the following, assume that n is odd and $n \geq 3$.

3.1 Step 1: The Maximum Difference Unit Group

Firstly we introduce a lemma for $\mathbb{Z}_n$.

Lemma 3. *[9, Page 36, Page 44] Let $n = p_1^{e_1} \cdots p_r^{e_r}$ be the canonical prime factorization of n. Then*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{e_r}}$$

and

$$\mathbb{Z}_n^\times \cong \mathbb{Z}_{p_1^{e_1}}^\times \times \mathbb{Z}_{p_2^{e_2}}^\times \times \cdots \times \mathbb{Z}_{p_r^{e_r}}^\times.$$

Moreover, $\mathbb{Z}_{p_i^{e_i}}^\times$ is cyclic for all $i = 1, 2, \ldots, r$

Denote $d = \gcd(p_1 - 1, \cdots, p_r - 1)$. Since $\mathbb{Z}_{p_i^{e_i}}$ is a Galois ring[10, Page 309], we can obtain a DUG G_i over $\mathbb{Z}_{p_i^{e_i}}$ from the following lemma by letting $R = \mathbb{Z}_{p_i^{e_i}}$, $v = p_i^{e_i}$, $I = (p_i)$, $n = r_i$, $q = p_i$ and $k = d$.

Lemma 4. *[8, Lemma 10] Let R be a ring of order v. I is a nilpotent ideal of R such that $I^n = \{0\}$ for some positive integer n. Denote $R_i = R/I^i$. If $R/I \cong \mathbb{F}_q$, then for any positive integer k such that $k \mid q - 1$, there exist a DUG G_i of order k over R_i for $1 \leq i \leq n$.*

Remark 1. *To see the explicit construction of G_i, please refer to [8, Lemma 9]. The form of G_i is also shown in the following lemma, i.e., Lemma 5.*

Together with Lemma 3, we can obtain a DUG G of order d over $\mathbb{Z}_n$ from Lemma 5 by letting $k_i = d$ for all $1 \leq i \leq r$, $R = \mathbb{Z}_n$ and $R_i = \mathbb{Z}_{p_i^{e_i}}$.

Lemma 5. *[8, Lemma 11] If a multiplicative group $G_i = \langle g_i \rangle$ is a DUG of order k_i over a ring R_i $(i = 1, 2, \cdots, n)$, then the multiplicative group $G = \langle (g_1^{\frac{k_1}{k}}, g_2^{\frac{k_2}{k}}, \ldots, g_n^{\frac{k_n}{k}}) \rangle$ is a DUG of order k over the ring $R = R_1 \oplus R_2 \oplus \cdots \oplus R_n$ where $k = \gcd(k_1, k_2, \ldots, k_n)$.*

Obviously the DUG G is cyclic. It follows from Lemma 6 that G is the maximum cyclic DUG over $\mathbb{Z}_n$.

Lemma 6. *[11, Lemma 2] Let $n = p_1^{e_1} \cdots p_r^{e_r}$ be the canonical prime factorization of n. Assume $b^s \equiv 1 \pmod{n}$ and $\gcd(\prod_{j=1}^{s-1}(b^j - 1), n) = 1$. Then*

- *For all $1 \leq i \leq r$, s is a factor of $p_i - 1$;*
- $\gcd(p_1 - 1, \cdots, p_r - 1) > 1$.

Remark 2. *From [3, Lemma 12], the size of the maximum DUS over $\mathbb{Z}_n$ is $p_k - 1$ where $p_k = \max_{1 \leq i \leq r} p_i$. However, what we concern is DUG.*

In general, a DUG H may be generated by finite elements, i.e., $H = \langle h_1, h_2, \ldots, h_m \rangle$. However, for all $1 \leq j \leq m$, we have $\langle h_j \rangle \leq G_i$ over $\mathbb{Z}_{p_i^{e_i}}$, because $\#\langle h_j \rangle \mid \#G_i$ and $\mathbb{Z}_{p_i^{e_i}}^\times$ is cyclic. As a result $\langle h_j \rangle \leq G$ over $\mathbb{Z}_n$ for all $1 \leq j \leq m$. Consequently, $H \leq G$. Finally, we conclude that

Proposition 7. *Let $n = p_1^{e_1} \cdots p_r^{e_r}$ be the canonical prime factorization of n. Then the maximum difference unit group over $\mathbb{Z}_n$ is cyclic and is of order $d = \gcd(p_1 - 1, \cdots, p_r - 1)$.*

3.2 Step 2: The difference unit group with odd order

In this subsection, assume that G is the maximum cyclic DUG. We have the following lemmas.

Lemma 8. *[12, Lemma 10] Let $(R, +, \times)$ be a ring and G be a DUG of order $d \geq 2$. Then $-1 \in G$ if and only if $2 \mid d$ or $\mathrm{char}(R) = 2$.*

Lemma 9. *Let $(R, +, \times)$ be a ring and G be a DUG of order $d \geq 2$. Then the following three statements are equivalent.*

(1) $-1 \in G$;
(2) $2 \mid d$ or $\mathrm{char}(R) = 2$;
(3) There exist two distinct elements $\theta \neq \theta'$, $\theta, \theta' \in G$, such that $\theta + \theta' = 0$.

Proof. It follows from Lemma 8 that Statement (1) and Statement (2) are equivalent. It is sufficient to show that Statement (1) and Statement (3) are equivalent.

On one hand, if $-1 \in G$, then put $\theta = 1$ and $\theta' = -1$. It has $\theta + \theta' = 1 + (-1) = 0$. On the other hand, if there exists $\theta, \theta' \in G$ such that $\theta + \theta' = 0$, then we have $\theta' = -\theta$. As a result, $-1 = \theta'\theta^{-1} \in G$.

According to Lemma 9, it is clear that if G is a DUG and satisfies the condition "$\theta + \theta' \not\equiv 0 \pmod{v}$ for any $\theta \neq \theta'$, $\theta, \theta' \in G$", then the order of G must be odd, i.e., $2 \nmid \#G$, since $\mathrm{char}(\mathbb{Z}_n) = n \geq 3$.

3.3 Solution: Odd Difference Unit Group

A DUG is called an odd DUG if its size is an odd number. Gathering the results (mainly Proposition 7 and Lemma 9) in Subsection 3.1 and Subsection 3.2, we can say that the special class of subgroups in Problem 2 is indeed odd DUG. Then we can answer Problem 2 with the following theorem.

Theorem 1. *Let $n = p_1^{e_1} \cdots p_r^{e_r}$ be the canonical prime factorization of n. Denote $d = \gcd(p_1 - 1, \cdots, p_r - 1)$ and $m = \nu_2(d)$.Then the order of maximum odd difference unit group is $\frac{d}{2^m}$.*

Furthermore, to construct the maximum odd DUG G, follow the steps below:

(a) For $1 \leq i \leq r$, find an element b_i of order $\frac{d}{2^m}$ in $\mathbb{Z}_{p_i} = \mathbb{F}_{p_i}$;
(b) For $1 \leq i \leq r$, lift the element b_i in $\mathbb{Z}_{p_i}$ to element g_i in $\mathbb{Z}_{p_i^{r_i}}$ (refer to [11, Lemma 3] and [8, Lemma 9] for more details);
(c) Obtain the generator g by the isomorphism φ in Lemma 3 with $(g_1, g_2, \ldots, g_r)$, i.e., $g = \varphi(g_1, g_2, \ldots, g_r)$;
(d) Get the maximum odd DUG $G = \langle g \rangle$.

4. Conclude

In this letter, we answer an open problem proposed by Fuji-Hara et al. in 2004. It is a problem about odd difference unit group. This problem is solved by involving the concept of difference unit group. Difference unit group was proposed some years ago but did not receive much attention, while the idea of difference unit group appears in many fields. So far as we know, difference unit group over $\mathbb{Z}_n$ is clear but not over the matrix ring. In the future, we would investigate the difference unit group over all kinds of rings.

References

[1] R. Fuji-Hara, Y. Miao, and M. Mishima, "Optimal frequency hopping sequences: a combinatorial approach," IEEE Transactions on Information Theory, vol.50, no.10, pp.2408–2420, 2004.

[2] C. Colbourne and J. Dinitz, Handbook of combinatorial designs, CRC press Boca Raton, FL, 2007.

[3] J.H. Chung, Y.K. Han, and K. Yang, "New classes of optimal frequency-hopping sequences by interleaving techniques," IEEE Transactions on Information Theory, vol.55, no.12, pp.5783–5791, 2009.

[4] Z. Cao, G. Ge, and Y. Miao, "Combinatorial characterizations of one-coincidence frequency-hopping sequences," Designs, Codes and Cryptography, vol.41, no.2, pp.177–184, 2006.

[5] M. Buratti, "On disjoint $(v, k, k-1)$ difference families," Designs, Codes and Cryptography, vol.87, no.4, pp.745–755, 2019.

[6] Z. Yi, Z. Lin, and L. Ke, "A generic method to construct zero-difference balanced functions," Cryptography and Communications, vol.10, no.4, pp.591–609, 2018.

[7] Z. Yi, Y. Yu, C. Tang, and Y. Zheng, "A note on two constructions of zero-difference balanced functions," IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, vol.102, no.4, pp.680–684, 2019.

[8] C. Xiang, Z. Yi, F. Fu, and W. Yin, "New constructions of near-complete external difference families over galois rings," IEEE Communications Letters, vol.24, no.5, pp.995 – 999, 2020.

[9] K. Ireland and M.I. Rosen, A Classical Introduction to Modern Number Theory, Springer Science & Business Media, 1990.

[10] Z.X. Wan, Lectures on finite fields and Galois rings, World Scientific Publishing Company, 2003.

[11] Z. Zha and L. Hu, "Cyclotomic constructions of zero-difference balanced functions with applications," IEEE Transactions on Information Theory, vol.61, no.3, pp.1491–1495, 2015.

[12] Z. Yi, D. Pei, and C. Tang, "The Zero-Difference Properties of Functions and Their Applications," arXiv e-prints, p.arXiv:1811.08132, Nov 2018.