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.

In 2004, Ryoh Fuji-Hara et al. established a connection between zero-difference balanced function and partitioned difference family[8] and difference family[5].

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

**Problem 2.** Find a maximum multiplicative subgroup $G$ of $\mathbb{Z}_n^*$ such that $\theta \neq \theta' \pmod{\phi}$ for any $\theta \neq \theta'$, $\theta', \theta' \in G$, and that any difference from $G$ is still a unit in $\mathbb{Z}_n$. Here the term "maximum" means that the subgroup is the maximum cardinality among all subgroups satisfying the above conditions.

Our work is quite different from the previous studies. On one hand, Reference [8] studies the cyclic DUG over rings, such as $\mathbb{Z}_n$ 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 $n \geq 3$ 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 $R$;
- $\text{char}(R)$: 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 $\mathbb{Z}$. 

Copyright © 200x The Institute of Electronics, Information and Communication Engineers
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 \( a, b \in \mathbb{Z}_n^* \). 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

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

Moreover, \( \mathbb{Z}_{p_i^{e_i}}^{*} \) is cyclic for all \( i = 1, 2, \ldots, r \).

Denote \( d = \gcd(p_1 - 1, \ldots, p_r - 1) \). 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 \( R = \mathbb{Z}_{p_i^{e_i}}^{*}, v = p_i^{e_i}, I = (p_i), n = r, q = p_i \) 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 \( I^r = \{0\} \) for some positive integer \( n \). Denote \( R_I = R/I^r \). If \( R/I \cong \mathbb{Z}_n \), then for any positive integer \( k \) such that \( k \mid n - 1 \), there exist a DUG \( G_i \) of order \( k \) over \( R_I \) for \( 1 \leq i \leq r \).

**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 \( 1 \leq i \leq r \) and \( R = \mathbb{Z}_n \) 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 \( R_i \) (\( i = 1, 2, \ldots, n \)), then the multiplicative group \( G = \langle (g_1^{e_1}, g_2^{e_2}, \ldots, g_n^{e_n}) \rangle \) 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 \( b^s \equiv 1 \) (mod \( n \)) and \( \gcd(b^s - 1, n) = 1 \). Then

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

**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 \( \langle h_j \rangle \leq G \) over \( \mathbb{Z}_{p_k^{e_k}}^{*} \), because \( \#(h_j) \mid \#G \) and \( \mathbb{Z}_{p_k^{e_k}}^{*} \) 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 \( d = \gcd(p_1 - 1, \ldots, p_r - 1) \).

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 \( \text{char}(R) = 2 \).

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

1. \( -1 \in G \);
2. \( 2 \mid d \) or \( \text{char}(R) = 2 \);
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, \( -1 = \theta' - \theta = 0 \in G \).

According to Lemma 9, it is clear that if \( G \) is a DUG and satisfies the condition “\( \theta + \theta' \neq 0 \) (mod \( v \)) for any \( \theta \neq \theta' \), \( \theta, \theta' \in G \)”, then the order of \( G \) must be odd, i.e., \( 2 \nmid \#G \), since \( \text{char}(\mathbb{Z}_n) = n \geq 3 \).

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 \( d = \gcd(p_1 - 1, \ldots, p_r - 1) \) and \( m = v_2(d) \). Then the order of maximum odd difference unit group is \( d/m \).
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 $\frac{d}{m}$ in $\mathbb{Z}_{P_i}^\times = \mathbb{F}_{P_i}$;

(b) For $1 \leq i \leq r$, lift the element $b_i$ in $\mathbb{Z}_{P_i}$ to element $g_i$ in $\mathbb{Z}_{P_i}^\times$ (refer to [11, Lemma 3] and [8, Lemma 9] for more details);

(c) Obtain the generator $g$ by the isomorphism $\varphi$ 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


