Azam, S., Tomie, M. and Yoshii, Y.
Osaka J. Math.
58 (2021), 563–589

CLASSIFICATION OF POINTED REFLECTION SPACES

Saeid AZAM, Masaya TOMIE and Yoji YOSHII

(Received September 10, 2018, revised March 18, 2020)

Abstract

We classify isomorphism and similarity classes of pointed reflection spaces of residue ≤ 2. This leads to the classification of reduced extended affine root systems whose involved pointed reflection spaces have residue ≤ 2.

1. Introduction

It is well known that root systems provide a powerful tool for the classification as well as for questions arising in the structure and representation theory of Lie algebras. In the last few decades, some extensions of affine root systems such as (locally) extended affine root systems and affine reflection systems have been considered. These are root systems of (locally) extended affine Lie algebras and invariant affine reflection algebras, respectively, which have been intensively investigated in recent years, see for example [1], [11], [12] and [13], and references therein.

For the description and classification of such root systems the concept of a *pointed reflection space* (PRS for short) arises naturally. It turns out that the classification of PRS up to similarity is the key point in the classification of the root systems under consideration. More precisely, the classification of (locally) extended affine root systems of reduced types reduces to the classification of similarity classes of pairs of PRSs which interact in some prescribed way, and this in turn reduces to the classification of similarity classes of PRSs (see Section 2 for details).

For non-reduced types, the classification reduces to the classification of similarity classes of triples of (pointed) reflection spaces which interact again in a prescribed way, see [1, Chapter II]. However, in this case, the problem is more subtle, in the sense that it does not reduce merely to the classification of similarity classes of PRSs. Anyhow, the classification of extended affine root systems is known when the dimension of radical of the form is ≤ 3.

By definition, a PRS of rank n is a spanning subset, containing zero, of a vector space of dimension n over field $\mathbb{F}_2$ of two elements. Two PRS S and S' in the same vector space are called *similar* if there exists a linear isomorphism φ of the ground vector space with $\varphi(S) = S' + \sigma'$ for some $\sigma' \in S'$.

In general, from theoretical point of view, the classification of similarity classes of PRS is not an easy task. Nevertheless, the answer for small rank, say ≤ 3, is easy and can be achieved by a simple direct observation. For a PRS S of rank n, we define the *residue* of S by

2010 Mathematics Subject Classification. 17B67, 17B65, 05B35.

The first author would like to thank IPM-Isfahan Branch where this research was partially carried out there.

$$\operatorname{res} S := |S \setminus \{0\}| - n.$$

In this work similarity classes of PRSs with residue ≤ 2 are classified.

In Section 3, the basic definitions and some preliminary lemmas are presented. In Section 4, the similarity classes of PRS of residue 1 are classified. Precisely, there are $[n/2]$ similarity classes of PRS of residue 1, and all are constructed from certain given circuits. In Section 5, isomorphism classes of PRS with residue 2 are classified. Each class is associated to either a pair or a triple of circuits, accordingly the classification is partitioned in 2 types. The total number of isomorphism classes is equal to $|N| + |M|$, where

$$N := \{(p, q) \mid 2 \leq p \leq q \text{ and } p + q \leq n\}$$

and

$$M := \{(s, p, q) \mid 1 \leq s \leq p + 1 \leq q + 1 \quad \text{and} \quad p + s + q \leq n\}.$$

Finally in Section 6, the similarity classes of PRS of residue 2 are classified. Using new notations $\{t, u\}_n$ and $\{s, t, u\}_n$ (see Definition 6.5), we determine a complete representative system of PRSs of residue 2 in $\mathbb{F}_2^n$ for even n and odd n separately (see Theorem 6.33 and Theorem 6.34). Moreover, we give a formula for counting the number of similarity classes in Theorem 6.44. This in particular gives a new sequence,

$$1, 2, 4, 6, 9, 12, 17, 21, 27, 33, 41, 48, \ldots,$$

which is not in the site OEIS. Although the next target would be residue ≥ 3, but from our methods it looks extremely complicated.

As it was explained in the preceding paragraph, the concept of a "circuit" plays an essential role in the description and classification of PRSs. This concept is borrowed from "binary matroid theory", see [14], which is the matroid theory for a vector space over the field $\mathbb{F}_2$. As we saw, our motivation comes from Lie theory, where we classify root systems and PRSs through isomorphisms and similarities. The concept of "similarity" seems to be new in the binary matroid theory.

To conclude, we should mention that in addition to their importance in classification of (extended affine) root systems and algebras, PRSs play a very important role in related objects such as Weyl groups and their presentations. A more recent attention to PRSs is appeared in a characterization of reflectable bases which has been studied in [7] and [6]. For more details about the classification of root systems under consideration, we refer the interested reader to [15], [1], [2], [3], [4], [5], [9], [10], [16] and [17].

2. From root systems to pointed reflection spaces

In this section we sketch briefly how the classification of extended affine root systems of reduced types reduces to the classification of similarity classes of pointed reflection spaces.

Let R be a reduced extend affine root system. By definition R is a spanning subset of a real vector space $\mathcal{V}$ equipped with a positive semidefinite bilinear form satisfying axioms (R1)-(R8) of [1, Definition II.2.1]. Let $\mathcal{V}^0$ be the radical of the form. It turns out that R contains an irreducible finite root system $\dot{R}$ and two subsets S and L of $\mathcal{V}^0$ such that

$$R = R(\dot{R}, S, L) = (S + S) \cup (\dot{R}_{sh} + S) \cup (\dot{R}_{lg} + L), \tag{2.1}$$

where $\dot{R}_{sh}$ and $\dot{R}_{lg}$ are the sets of short and long roots of $\dot{R}$ (if $\dot{R}$ is simply laced, then by convention we assume that $\dot{R}_{lg}$ and L are empty sets). Moreover if F is one of S or L then F satisfies

- F is a discrete subsets of $\mathcal{V}^0$,
- F spans $\mathcal{V}^0$,
- $0 \in F$ and $F \pm 2F \subseteq F$.

Finally, if $\dot{R}_{lg}$ is not empty, then the pair (S, L) satisfies

- $S + L \subseteq S$ and $kS + L \subseteq L$ where $k = 3$ if $\dot{R}$ is of type G_2 and $k = 2$ if $\dot{R}$ is of type B, C, or F_4.

We recall from [1] that the rank and the type of R refers to the rank and type of $\dot{R}$ respectively. The nullity of R is by definition the dimension of $\mathcal{V}^0$.

In [1], the authors use the term a semilattice in $\mathcal{V}^0$ for a subset F satisfying the above conditions. It is known that the rank, type and nullity are isomorphism invariants of extended affine root systems. Moreover, two extended affine root systems $R(\dot{R}, S, L)$ and $R' = (\dot{R}, S', L')$ of the form (2.1) are isomorphic if and only if the pairs (S, L) and (S', L') are similar in the following sense. Two semilattices F and F' in $\mathcal{V}^0$ are called *similar*, denoted $F \sim F'$, if there exists a linear automorphism φ of $\mathcal{V}^0$ such that $\varphi(F) = F' + \sigma'$ for some $\sigma' \in F'$. Then two pairs (S, L) and (S', L') are called *similar* if they are simultaneously similar, namely there exists a linear isomorphism φ of $\mathcal{V}^0$ such that $\varphi(S) = S' + \sigma'$ for some $\sigma' \in S'$ and $\varphi(L) = L' + \lambda'$ for some $\lambda' \in L'$. In this case we write $(S, L) \sim (S', L')$. Therefore the classification of isomorphism classes of extended affine root systems of reduced types reduces to the classification of similarity classes of pairs of the above form.

We now explain that in practice the classification of extended affine root systems of reduced types reduces to the classification of semilattices, up to similarity. In fact, one can show that the pairs (S, L) and (S', L') of the above forms can be decomposed as $S = S_1 \oplus \Lambda_2$, $S' = S'_1 \oplus \Lambda_2$, $L = 2\Lambda_1 + S_2$ and $L' = 2\Lambda_1 + S'_2$, where Λ_1 and Λ_2 are lattices and S_1, S'_1, S_2 and S'_2 are semilattices in some subspaces of $\mathcal{V}^0$ characterized by an isomorphism invariant of the root system called the *twist number*. Now the main achievement ([1, Proposition II.4.17]) is that

$$(S, L) \sim (S', L') \Longleftrightarrow S_1 \sim S'_1 \text{ and } S_2 \sim S'_2.$$

This concludes the classification reduction from root systems to semilattices.

Finally, we explain how one reduces the similarity of semilattices to the similarity of pointed reflection spaces over field $\mathbb{F}_2$. Let F be a semilattice in $\mathcal{V}^0$ and Λ be its $\mathbb{Z}$-span. Λ is a lattice in $\mathcal{V}^0$. Let $\tilde{\Lambda} := \Lambda/2\Lambda$, considered as a vector space over $\mathbb{F}_2$. Let $\tilde{}: \Lambda \to \tilde{\Lambda}$ be the canonical map. Then $\tilde{F}$, the image of F under $\tilde{}$, is a large set in $\tilde{\Lambda}$ in the sense that it is a spanning subset of the vector space $\tilde{\Lambda}$ which contains zero. Conversely, the preimage of any large subset of $\tilde{\Lambda}$ is a semilattice in $\mathcal{V}^0$ whose $\mathbb{Z}$-span is Λ. Two large sets $\tilde{F}$ and $\tilde{F}'$ in $\tilde{\Lambda}$ are called similar if $\varphi(\tilde{F}) = \tilde{F}' + \sigma'$ for some $\sigma' \in \tilde{F}'$. Now, as there exists a one to one correspondence between similarity classes of semilattices in $\mathcal{V}^0$ with $\mathbb{Z}$-span Λ and the similarity classes of large subsets of $\tilde{\Lambda}$, the classification of extended affine root systems of reduces types, reduces to the classification of similarity classification of large sets in $\tilde{\Lambda}$.

We emphasize here that the concept of a large set coincides with the concept of a pointed reflection space over field $\mathbb{F}_2$. In this work, we use the term a *pointed reflection space* instead of a large set, as it was originally defined under this name, in the study of symmetric spaces [8].

3. Basic concepts

We explained in Section 1 that the classification of extended affine root systems reduces to the classification of pointed reflection spaces. We begin with some basic definitions and concepts.

Definition 3.1. Let $\mathbb{F}_2 = \{0, 1\}$ be the field of order 2 and V a vector space of dimension n over $\mathbb{F}_2$. A subset $S = (S, V)$ of V is called a *pointed reflection space (PRS) of rank n* if $0 \in S$ and $\langle S \rangle = V$. We use the notation $S^\times := S \setminus \{0\}$, and $|S^\times|$ is called the *index* of S, denoted $\mathrm{ind} S$, and $|S^\times| - n$ is called the *residue* of S, denoted $\mathrm{res} S$. Note that $0 \leq \mathrm{res} S < 2^n - n$.

Two PRS (S, V) and (S', V') are called *isomorphic*, denoted $S \cong S'$, if there exists a linear isomorphism $f : V \longrightarrow V'$ such that $f(S) = S'$, and *similar*, denoted $S \sim S'$, if there exists some $s \in S$ such that $s + S \cong S'$.

Remark 3.2. If S is a PRS, then $s + S$ $(s \in S)$ and $S + S$ are also PRS. Also, if $S \sim S'$, then $S + S \cong S' + S'$.

If $\mathrm{res} S = 0$, there is only one isomorphism class. In fact, let $B = \{\epsilon_1, \ldots, \epsilon_n\}$ be a basis of V. Then $S = \{0, \epsilon_1, \ldots, \epsilon_n\}$ is a representative.

The concept of a "circuit" from matroid theory plays a very important role in the sequel. We record here its formal definition of vector space version from [14].

Definition 3.3. In general, a non-empty subset $C \neq \{0\}$ of a vector space is called a *circuit* if C is linearly dependent and $C \setminus \{c\}$ is linearly independent for any $c \in C$. We call $|C|$ the *length* of C. Note that $|C| \geq 2$.

For example,

$$C_i := \{\epsilon_1, \ldots, \epsilon_i, \ \epsilon_1 + \cdots + \epsilon_i\} \tag{3.1}$$

is a circuit of V of length $i + 1$.

Lemma 3.4. *Let $W = \{v_1, \ldots, v_k\}$ be a subset of V. Then, W is linearly independent if and only if $v_{i_1} + \cdots + v_{i_r} \neq 0$ for any non-empty subset $\{v_{i_1}, \ldots, v_{i_r}\}$ of W. (We are assuming that all v_{i_j} are different!)*

Proof. Clear. □

Lemma 3.5. *Let $C = \{v_1, \ldots, v_k\}$ $(k \geq 2)$ be a subset of V. Then, C is a circuit if and only if $v_1 + \cdots + v_k = 0$ and $v_{i_1} + \cdots + v_{i_r} \neq 0$ for any proper non-empty subset $\{v_{i_1}, \ldots, v_{i_r}\}$ of C.*

Proof. Clear from Lemma 3.4. □

Lemma 3.6. *Let D be a subset of V such that $0 \notin D$ and the total sum of the elements of D is zero. Then, D is a union of some circuits.*

Proof. Let $v_1 \in D$. Then there is a sequence $v_1, v_2, \ldots, v_r$ in D such that $v_1 + \cdots + v_i \neq 0$ for $i < r$ and $v_1 + \cdots + v_r = 0$. Then $C = \{v_1, \ldots, v_r\}$ is a circuit, by Lemma 3.5. If $C \neq D$, then use induction on $|D|$. □

We shall clarify the isomorphism classes and the similarity classes of PRS of residue 1 and 2.

4. The case of res$S = 1$

Theorem 4.1. *Let S be a PRS of V of* res$S = 1$. *Then S is isomorphic to*

$$S_i := \{0\} \cup C_i \cup \{\epsilon_{i+1}, \ldots, \epsilon_n\}$$

for some $2 \leq i \leq n$, where C_i is the circuit defined in (3.1).

Moreover, the set of isomorphism classes is $\{S_2, \ldots, S_n\}$.

Proof. We may assume that $S^\times$ contains B since S contains a basis of V. Then one can make the matrix whose columns are the coordinates of $S^\times$ relative to B. Namely, we identify $S^\times$ with the $n \times (n+1)$ matrix (I_n, v), where I_n is the identity matrix of size $n \times n$ and some $v \in \mathbb{F}_2^n$. Elementary row operations and interchanging columns are allowed to get an isomorphic PRS. Thus, at first, interchanging rows (if necessary), we get $(I_n, v) \to (J_n, w)$, where J_n is some permutation matrix and ${}^t w = (1, \ldots, 1, 0, \ldots, 0)$. Then, interchanging columns (if necessary), we obtain $(J_n, w) \to (I_n, w)$, and hence $S \cong S_i$.

$$(I_n, v) = \begin{pmatrix} 1 & 0 & \cdots & & 0 & \\ 0 & 1 & & \vdots & \vdots & \\ \vdots & & \ddots & & 0 & v \\ & & & & & \\ 0 & & \cdots & 0 & 1 & \end{pmatrix} \to (J_n, w) \to \begin{pmatrix} 1 & 0 & \cdots & & 0 & 1 \\ 0 & 1 & & \vdots & \vdots & \vdots \\ \vdots & & \ddots & & 0 & 1 \\ & & & & & 0 \\ & & & & & \vdots \\ 0 & & \cdots & 0 & 1 & 0 \end{pmatrix} = (I_n, w).$$

Moreover, each S_i contains only one circuit C_i of length $i + 1$. Thus, $S_i \not\cong S_j$ if $i \neq j$. □

Corollary 4.2. *Let S be a PRS of V, and* res$S = 1$. *Then $s + S$ $(s \in S)$ contains only one circuit.*

Proof. Since $s + S$ is a PRS of residue 1, we have $s + S \cong S_i$ for some i, by Theorem 4.1. Hence $s + S$ contains only one circuit. □

Lemma 4.3. *Let $C = \{v_1, \ldots, v_k\}$ $(k \geq 2)$ be a subset of V. Then, C is a circuit $\iff$ $v_1 + \cdots + v_k = 0$ and $v_{i_1} + \cdots + v_{i_r} \neq 0$ for any subset $\{v_{i_1}, \ldots, v_{i_r}\}$ of $\{v_1, \ldots, v_{k-1}\}$.*

Proof. ($\Longrightarrow$) Clear from Lemma 3.5.

($\Longleftarrow$) From the first condition, C is linearly dependent. Thus, it is enough to show that $v_{j_1} + \cdots + v_{j_s} \neq 0$ for any proper subset $\{v_{j_1}, \ldots, v_{j_s}\}$ of C. From the second condition, we only need to consider a subset $\{v_{j_1}, \ldots, v_{j_t}, v_k\}$ for $1 \leq t < k-1$. If $v_{j_1} + \cdots + v_{j_t} + v_k = 0$, then we get $v_{j_1} + \cdots + v_{j_t} + v_1 + \cdots + v_{k-1} = 0$ (from $v_1 + \cdots + v_k = 0$). Since $t < k-1$, the left hand side is the sum of subsets of $\{v_1, \ldots, v_{k-1}\}$. This contradicts to the second condition. Hence,

$v_{j_1} + \cdots + v_{j_t} + v_k \neq 0$, and we finish the proof. □

Lemma 4.4.

(i) *When i is odd, we have* $\epsilon_1 + \cdots + \epsilon_i + S_i \cong S_{i-1}$ *and* $\begin{cases} \epsilon_j + S_i \cong S_{i-1} & \textit{for } j \leq i, \\ \epsilon_j + S_i \cong S_i & \textit{for } j > i. \end{cases}$

(ii) *When i is even, we have* $\epsilon_1 + \cdots + \epsilon_i + S_i \cong S_i$ *and* $\begin{cases} \epsilon_j + S_i \cong S_i & \textit{for } j \leq i, \\ \epsilon_j + S_i \cong S_{i+1} & \textit{for } j > i. \end{cases}$

Proof. Let $\epsilon := \epsilon_1 + \cdots + \epsilon_i$.

(i) We have $S := \epsilon + S_i = \{\epsilon,\ \epsilon + \epsilon_1,\ \ldots,\ \epsilon + \epsilon_n, 0\}$, and $C := \{\epsilon + \epsilon_1,\ \epsilon + \epsilon_2,\ \ldots,\ \epsilon + \epsilon_i\}$ is a subset of S with $|C| = i$ satisfying $\sum_{x \in C} x = 0$ since each ϵ_k is added even times (since i is odd). Moreover, any partial sum of C is never 0. In fact, if $A := \{\epsilon + \epsilon_{j_1}, \ldots, \epsilon + \epsilon_{j_r}\}$ is a proper subset of C. Then

$$\sum_{x \in A} x = \begin{cases} \epsilon_{j_1} + \cdots + \epsilon_{j_r} & \text{if } r \text{ is even,} \\ \epsilon + \epsilon_{j_1} + \cdots \epsilon_{j_r} = \sum_{\{1,\ldots,i\} \setminus \{j_1,\ldots,j_r\}} \epsilon_i & \text{if } i \text{ is odd,} \end{cases}$$

which shows that in both cases the sum is nonzero. Thus by Lemma 3.4, C is a circuit of length i. Then, by Theorem 4.1, we obtain $\epsilon + S_i \cong S_{i-1}$.

Suppose that $j \leq i$, and then

$$\epsilon_j + S_i = \{\epsilon_j,\ \epsilon_1 + \epsilon_j,\ \ldots, \epsilon_{j-1} + \epsilon_j,\ 0,\ \epsilon_{j+1} + \epsilon_j,\ \ldots,\ \epsilon_i + \epsilon_j,\ \ldots,\ \epsilon_n + \epsilon_j,\ \epsilon + \epsilon_j\}$$

(note $\epsilon_i + \epsilon_j = 0$ if $j = i$). Consider the subset

$$C := \{\epsilon_1 + \epsilon_j,\ \ldots, \epsilon_{j-1} + \epsilon_j,\ \epsilon_{j+1} + \epsilon_j,\ \ldots,\ \epsilon_i + \epsilon_j,\ \epsilon + \epsilon_j\}$$

of $\epsilon_j + S_i$ with $|C| = i$. If $1 \leq k \neq j \leq i$, then in the set C, ϵ_k appears twice, and ϵ_j appears $i - 1$ times (which is even times). Hence, $\sum_{x \in C} x = 0$. Also, any partial sum of the subset $C \setminus \{\epsilon + \epsilon_j\}$ is never 0 since ϵ_ℓ for $1 \leq \ell < i$ appears only once in the sum. Hence, by Lemma 4.3, C is a circuit, and so by Theorem 4.1, we get $\epsilon_j + S_i \cong S_{i-1}$.

Suppose that $j > i$, and then

$$\epsilon_j + S_i = \{\epsilon_j,\ \epsilon_1 + \epsilon_j,\ \ldots, \epsilon_i + \epsilon_j,\ \ldots, \epsilon_{j-1} + \epsilon_j,\ 0,\ \epsilon_{j+1} + \epsilon_j,\ \ldots,\ \epsilon_n + \epsilon_j,\ \epsilon + \epsilon_j\}$$

(note $\epsilon_n + \epsilon_j = 0$ if $j = n$). Consider the subset

$$C := \{\epsilon_1 + \epsilon_j,\ \ldots, \epsilon_i + \epsilon_j,\ \epsilon + \epsilon_j\}$$

of $\epsilon_j + S_i$ with $|C| = i + 1$. If $k \neq j$, then ϵ_k appears twice, and ϵ_j appears $i + 1$ times (which is even times). Hence, $\sum_{x \in C} x = 0$. Also, note that the sum of any subset of $C \setminus \{\epsilon + \epsilon_j\}$ is never 0. Thus C is a circuit by Lemma 4.3. Then, by Theorem 4.1, we obtain $\epsilon_j + S_i \cong S_i$.

(ii) We have $S := \epsilon + S_i = \{\epsilon,\ \epsilon + \epsilon_1,\ \ldots,\ \epsilon + \epsilon_n, 0\}$, and $C := \{\epsilon, \epsilon + \epsilon_1,\ \epsilon + \epsilon_2,\ \ldots,\ \epsilon + \epsilon_i\}$ is a subset of S with $|C| = i + 1$ satisfying $\sum_{x \in C} x = 0$. We show that C is a circuit. Let $A := \{p_{j_1}, \ldots, p_{j_r}\}$ be a proper subset of $C \setminus \{\epsilon\}$. Then, since $r < i$, there exists $1 \leq k \leq i$ such that ϵ_k appears in all the terms $p_{j_1}, \ldots, p_{j_r}$. Hence, if $p_{j_1} + \cdots + p_{j_r} = 0$, then $r\epsilon_k = 0$, and so r is even. But then, we have $0 = p_{j_1} + \cdots + p_{j_r} = r\epsilon + \epsilon_{j_1} + \cdots + \epsilon_{j_r} = \epsilon_{j_1} + \cdots + \epsilon_{j_r}$, which is a contradiction since $\epsilon_{j_1} + \cdots + \epsilon_{j_r}$ is linearly independent. Therefore, $p_{j_1} + \cdots + p_{j_r} \neq 0$, and thus C is a circuit of length $i + 1$, by Lemma 4.3. Then, by Theorem 4.1, we obtain

$\epsilon + S_i \cong S_i$.

Suppose that $j \leq i$, and Consider the subset

$$C := \{\epsilon_j,\ \epsilon_1 + \epsilon_j,\ \ldots, \epsilon_{j-1} + \epsilon_j,\ \epsilon_{j+1} + \epsilon_j,\ \ldots,\ \epsilon_i + \epsilon_j,\ \epsilon + \epsilon_j\}$$

of $\epsilon_j + S_i$ with $|C| = i + 1$. If $k \neq j$, then ϵ_k appears twice, and ϵ_j appears i times (which is even times). Hence, $\sum_{x \in C} x = 0$. Also, any partial sum of the subset $C \setminus \{\epsilon + \epsilon_j\}$ is never 0 since ϵ_j appears i times and ϵ_ℓ for $1 \leq \ell \leq i$ with $\ell \neq j$ appears only once in the sum. Hence, by Lemma 4.3, C is a circuit, and so by Corollary 4.2, we get $\epsilon_j + S_i \cong S_i$.

Suppose that $j > i$, and consider the subset

$$C := \{\epsilon_j,\ \epsilon_1 + \epsilon_j,\ \ldots, \epsilon_i + \epsilon_j,\ \epsilon + \epsilon_j\}$$

of $\epsilon_j + S_i$ with $|C| = i + 2$. If $k \neq j$, then ϵ_k appears twice, and ϵ_j appears $i + 2$ times (which is even times). Hence, $\sum_{x \in C} x = 0$. Also, note that the sum of any subset of $C \setminus \{\epsilon + \epsilon_j\}$ is never 0. Thus C is a circuit by Lemma 4.3. Then, by Theorem 4.1, we obtain $\epsilon_j + S_i \cong S_{i+1}$. □

Theorem 4.5. *If* res$S = 1$*, then the similarity class of PRS consists of* $(n-1)/2$ *elements, i.e.,* $S_2, S_4, \ldots, S_{n-1}$ *when n is odd, and* $n/2$ *elements, i.e.,* $S_2, S_4, \ldots, S_n$ *when n is even.*

Proof. It follows from Theorem 4.1 and Lemma 4.4. □

Let $\mathcal{I}_i(n)$ and $\mathcal{S}_i(n)$ be the number of isomorphism classes and similarity classes of rank n and residue i, respectively. Then we have $\mathcal{I}_1(n) = n - 1$ and $\mathcal{S}_1(n) = [n/2]$.

n	2	3	4	5	6	7	8	9	10	11	12	13	$\cdots$
$\mathcal{I}_1(n)$	1	2	3	4	5	6	7	8	9	10	11	12	$\cdots$
$\mathcal{S}_1(n)$	1	1	2	2	3	3	4	4	5	5	6	6	$\cdots$

5. Isomorphism classes of case res$S$ = 2

Lemma 5.1. *Let* C_1 *and* C_2 *be circuits of S with* $C_1 \cap C_2 \neq \emptyset$ *and let*

$$C_1 \vartriangle C_2 := (C_1 \cup C_2) \setminus (C_1 \cap C_2) = (C_1 \setminus C_2) \cup (C_1 \setminus C_2)$$

be the symmetric difference. Then the total sum of the elements of $C_1 \vartriangle C_2$ *is zero.*

Proof. Let $C_1 = \{v_1, \ldots, v_i,\ w_1, \ldots, w_j\}$ and $C_2 = \{v_1, \ldots, v_i,\ x_1, \ldots, x_k\}$, i.e., $C_1 \cap C_2 = \{v_1, \ldots, v_i\}$. Then we have $v_1 + \cdots + v_i + w_1 + \cdots + w_j = 0$ and $v_1 + \cdots + v_i + x_1 + \cdots + x_k = 0$. Thus we obain $w_1 + \cdots + w_j + x_1 + \cdots + x_k = 0$. □

Remark 5.2. In general, $C_1 \vartriangle C_2$ is not necessarily a circuit. For example, $C_1 = \{\epsilon_1, \epsilon_1 + \epsilon_4, \epsilon_2 + \epsilon_4, \epsilon_2 + \epsilon_5, \epsilon_5\}$ and $C_2 = \{\epsilon_1, \epsilon_1 + \epsilon_3, \epsilon_2 + \epsilon_3, \epsilon_5 + \epsilon_6, \epsilon_6\}$ are both circuits. But

$$\begin{aligned} C_1 \vartriangle C_2 &= \{\epsilon_1 + \epsilon_4, \epsilon_2 + \epsilon_4, \epsilon_5, \epsilon_1 + \epsilon_3, \epsilon_2 + \epsilon_3, \epsilon_5 + \epsilon_6, \epsilon_6\} \\ &= \{\epsilon_1 + \epsilon_4, \epsilon_2 + \epsilon_4, \epsilon_1 + \epsilon_3, \epsilon_2 + \epsilon_3\} \sqcup \{\epsilon_5, \epsilon_5 + \epsilon_6, \epsilon_6\} \end{aligned}$$

is a union of two circuits. In this case, $S := \{0\} \cup C_1 \cup C_2$ is a PRS of $\mathbb{F}_2^6$ with res$S = 3$. We will show in Theorem 5.4 that if res$S = 2$, then $C_1 \vartriangle C_2$ is always a circuit.

Lemma 5.3. *Let A and B be some finite sets with intersection. Let $\mathcal{X} = \{A, B, A \triangle B\}$. Then $\mathcal{X} = \{C, D, C \triangle D\}$ with $|C \cap D| \leq |C \setminus D| \leq |D \setminus C|$.*

Proof. Without loss of generality, one can assume that $|A| \leq |B|$, and so we have $|A \setminus B| \leq |B \setminus A|$. Also, we note that $A \triangle (A \triangle B) = B$ and $B \triangle (A \triangle B) = A$, and so $\mathcal{X} = \{C, D, C \triangle D\}$ for any choice of C and D from $\{A, B, A \triangle B\}$. If $|A \cap B| \leq |A \setminus B| \leq |B \setminus A|$, then put $C := A$ and $D := B$. Suppose that $|A \setminus B| \leq |A \cap B| \leq |B \setminus A|$. Then putting $C := A$ and $D := A \triangle B$, we have

$$|C \cap D| = |A \cap (A \triangle B)| = |A \setminus B| \leq |A \cap B| = |C \setminus D| \leq |B \setminus A| = |(A \triangle B) \setminus A| = |D \setminus C|.$$

Finally suppose that $|A \setminus B| \leq |B \setminus A| \leq |A \cap B|$. Then putting $C := A \triangle B$ and $D := A$, we have

$$|C \cap D| = |(A \triangle B) \cap A| = |A \setminus B| \leq |B \setminus A| = |(A \triangle B) \setminus A| = |C \setminus D| \leq |A \cap B| = |D \setminus C|.$$

Thus we finish the proof. □

Theorem 5.4. *If $\operatorname{res} S = 2$, then S is isomorphic to*

$$S_{pq} := \{0, \epsilon_1, \dots, \epsilon_n, v_1, v_2\} \quad \textit{or} \quad S_{spq} := \{0, \epsilon_1, \dots, \epsilon_n, w_1, w_2\},$$

where

$$\begin{aligned} v_1 &:= \epsilon_1 + \cdots + \epsilon_p, \\ v_2 &:= \epsilon_{p+1} + \cdots + \epsilon_{p+q}, \\ w_1 &:= \epsilon_1 + \cdots + \epsilon_p + \epsilon_{p+1} + \cdots + \epsilon_{p+s}, \\ w_2 &:= \epsilon_{p+1} + \cdots + \epsilon_{p+s} + \epsilon_{p+s+1} \cdots + \epsilon_{p+s+q} \end{aligned}$$

for $p, s, q \in \mathbb{N}$ satisfying

$$\begin{aligned} &2 \leq p \leq q \quad \textit{and} \quad p + q \leq n \quad \textit{for } S_{pq} \\ &1 \leq s \leq p + 1 \leq q + 1 \quad \textit{and} \quad p + s + q \leq n \quad \textit{for } S_{spq}. \end{aligned}$$

In particular, S_{pq} contains two disjoint circuits

$$C_1 = \{\epsilon_1, \dots, \epsilon_p, v_1\} \quad \textit{and} \quad C_2 = \{\epsilon_{p+1}, \dots, \epsilon_{p+q}, v_2\}$$

of length $p + 1$ and $q + 1$, respectively, and each element of

$$N := \{(p, q) \mid 2 \leq p \leq q \textit{ and } p + q \leq n\} \subset \mathbb{N}^2$$

determines a different S_{pq}. Also, S_{spq} contains three circuits

$$\begin{aligned} C_1 = \{\epsilon_1, \dots, \epsilon_{p+s}, w_1\}, \;\; C_2 &= \{\epsilon_{p+1}, \dots, \epsilon_{p+s+q}, w_2\} \quad \textit{and} \\ C_1 \triangle C_2 &= \{\epsilon_1, \dots, \epsilon_p, \epsilon_{p+s+1}, \dots, \epsilon_{p+s+q}, w_1, w_2\} \end{aligned}$$

of length $s + p + 1$, $s + q + 1$ and $p + q + 2$, respectively, and each element of

$$M := \{(s, p, q) \mid 1 \leq s \leq p + 1 \leq q + 1 \quad \textit{and} \quad p + s + q \leq n\} \subset \mathbb{N}^3.$$

determines a different S_{spq}.

Hence, the number of isomorphism classes when $\operatorname{res} S = 2$ is equal to $|N| + |M|$.

Proof. We can assume that S contains the basis $B = \{\epsilon_1, \dots, \epsilon_n\}$. For the matrix of S relative to B, using elementary row operations and interchanging columns, we get

$$S \cong S_{ijk} = \{0, \epsilon_1, \dots, \epsilon_n,\ \epsilon_1 + \cdots + \epsilon_i,\ \epsilon_j + \epsilon_{j+1} + \cdots + \epsilon_{j+k}\}$$

for some $i \geq 2$ and $1 \leq j, k < n$, that is,

$$S^{\times}_{ijk} = \left(\begin{array}{ccc} & 1 & 0 \\ & \vdots & \vdots \\ & 1 & 0 \\ & 0 & 0 \\ & \vdots & \vdots \\ & 0 & 0 \\ I & 0 & 1 \\ & \vdots & \vdots \\ & 0 & 1 \\ & 0 & 0 \\ & \vdots & \vdots \\ & 0 & 0 \end{array}\right) \quad \text{or} \quad \left(\begin{array}{ccc} & 1 & 0 \\ & \vdots & \vdots \\ & & 0 \\ & \vdots & \\ & & 1 \\ & & \vdots \\ & 1 & \\ I & 0 & \\ & \vdots & \vdots \\ & & 1 \\ & & 0 \\ & \vdots & \vdots \\ & 0 & 0 \end{array}\right).$$

For the first case, i.e., if $i < j$, then interchanging rows and columns, we get $S_{ijk} \cong S_{pq} = \{0, \epsilon_1, \dots, \epsilon_n, v_1, v_2\}$, which only contains the disjoint circuits $C_1 = \{\epsilon_1, \dots, \epsilon_p, v_1\}$ of length $p + 1$ and $C_2 = \{\epsilon_{p+1}, \dots, \epsilon_{p+q}, v_2\}$ of length $q + 1$. Also, interchanging rows and columns if necessary, we can assume that $p \leq q$. Thus it is clear that the set N determines the isomorphism classes since the number and lengths of circuits are isomorphic invariants.

We investigate the second case, i.e., $i > j$. Clearly there are two circuits $C_1 = \{\epsilon_1, \dots, \epsilon_i, \epsilon_1 + \cdots + \epsilon_i\}$ and $C_2 = \{\epsilon_j, \dots, \epsilon_{j+k},\ \epsilon_j + \cdots + \epsilon_{j+k}\}$. Hence, by Lemma 5.1, the total sum of the elements of $C_3 := C_1 \vartriangle C_2$ is zero. Moreover, one can see that the subset of C_3 obtained by excluding any element is linearly independent, and so C_3 is a circuit. Also, it is easily checked that these are the only circuits, and they have intersections. Thus, by Lemma 5.3, we can also assume that S contains three circuits A, B and C such that for $s := |A \cap B| \geq 1$, $t := |A| - s$ and $u := |B| - s$,

$$1 \leq s \leq t \leq u \quad \text{and} \quad m := s + t + u \leq n + 2.$$

Note that $|A| = s + t \leq |B| = s + u \leq |A \vartriangle B| = t + u$. Also, if $t = 1$, then $s = 1$ and so $|A| = 2$. But a circuit cannot have length 2, and so $t \neq 1$.

Now we show that S is isomorphic to S_{spq}, as $p = t - 1$ and $q = u - 1$. Let $A = \{z_1, \dots, z_s, x_1, \dots, x_t\}$, $B = \{z_1, \dots, z_s, y_1, \dots, y_u\}$ and $C := A \vartriangle B = \{x_1, \dots, x_t, y_1, \dots, y_u\}$. Then, we claim that

$$D = \{z_1, \dots, z_s, x_1, \dots, x_{t-1}, y_1, \dots, y_{u-1}\}$$

is linearly independent. In fact, suppose that $\sum_{i=1}^{s} a_i z_i + \sum_{i=1}^{t-1} b_i x_i + \sum_{i=1}^{u-1} c_i y_i = 0$. If there are nonzero coefficients among a_i, b_i, c_i, then there are some $a_j \neq 0$, $b_k \neq 0$ and $c_\ell \neq 0$ since $A \setminus \{x_t\}$, $B \setminus \{y_u\}$ and $C \setminus \{x_t, y_u\}$ are all linearly independent. But then, by Lemma 3.6, $\{z_i \mid a_i \neq 0\} \cup \{x_i \mid b_i \neq 0\} \cup \{y_i \mid c_i \neq 0\}$ is a union of some circuits, which are different from A, B or C. This is a contradiction since S has only three circuits. Hence D is linearly independent.

Note that $\operatorname{span}(D \cup \{x_t, y_u\}) = \operatorname{span} D$, and so $S^{\times} \setminus \{x_t, y_u\}$ is a basis of V. Thus, if $m = n+2$, then D is a basis, and otherwise, let

$$S^{\times} \setminus \{x_t, y_u\} = D \sqcup \{g_1, \dots, g_{n+2-m}\}$$

be a basis of V. Let f be the linear automorphism of V determined by

$$\begin{aligned} f(x_i) &= \epsilon_i \quad (1 \le i \le t-1),\\ f(z_i) &= \epsilon_i \quad (1 \le i \le s),\\ f(y_i) &= \epsilon_i \quad (1 \le i \le u-1),\\ f(g_i) &= \epsilon_i \quad (1 \le i \le n+2-m). \end{aligned}$$

Then we have $f(S) = S_{s,t-1,u-1}$. In fact, it is enough to show that $f(x_t) = \epsilon_1 + \cdots + \epsilon_{s+t-1}$ and $f(y_u) = \epsilon_{t+1} + \cdots + \epsilon_{m-1}$. But since $x_t = \sum_{i=1}^{s} z_i + \sum_{i=1}^{t-1} x_i$ and $y_u = \sum_{i=1}^{s} z_i + \sum_{i=1}^{u-1} y_i$, we get $f(x_t) = \sum_{i=1}^{s} f(z_i) + \sum_{i=1}^{t-1} f(x_i) = \epsilon_1 + \cdots + \epsilon_{s+t-1}$ and $f(y_u) = \sum_{i=1}^{s} f(z_i) + \sum_{i=1}^{u-1} f(y_i) = \epsilon_{t+1} + \cdots + \epsilon_{m-1}$. Therefore, we obtain $S \cong S_{spq}$ with $p = t-1$ and $q = u-1$.

As the case of S_{pq} above, it is clear that the set M determines the isomorphism classes since the number and lengths of circuits are isomorphic invariants. □

Remark 5.5. From the proof of Theorem 5.4, we see that there are only two patterns, i.e., S contains two circuits or three circuits. More precisely, if S contains two circuits of length t and u with $3 \le t \le u$ and $t + u \le n + 2$, then $S \cong S_{t-1,u-1}$. If S contains three circuits, then there exist s, t, u such that the lengths of the circuits are $s + t$, $s + u$ and $t + u$ with $1 \le s \le t \le u \le n + 2$ and $t \ne 1$, and $S \cong S_{s,t-1,u-1}$. In any case, a PRS is determined only by the lengths of circuits. Thus we define the type of a PRS in terms of the lengths of circuits, as the following definition.

Definition 5.6. If S contains two circuits of length t and u with $3 \le t \le u$ and $t+u \le n+2$, then the *type* of S is (t, u). If S contains three circuits of lengths $s + t$, $s + u$ and $t + u$ with $1 \le s \le t \le u \le n + 2$ and $t \ne 1$, then the *type* of S is (s, t, u).

Note that S_{pq} has the type $(p + 1, q + 1)$, and S_{spq} has the type $(s, p + 1, q + 1)$.

$$S^{\times}_{pq} = \left(\begin{array}{cc} & p\left\{\begin{matrix}1 & 0\\ \vdots & \vdots\\ 1 & 0\end{matrix}\right. \\ I & q\left\{\begin{matrix}0 & 1\\ \vdots & \vdots\\ 0 & 1\end{matrix}\right. \\ & \begin{matrix}0 & 0\\ \vdots & \vdots\\ 0 & 0\end{matrix} \end{array}\right) \quad \text{and} \quad S^{\times}_{spq} = \left(\begin{array}{cc} & p\left\{\begin{matrix}1 & 0\\ \vdots & \vdots\\ 1 & 0\end{matrix}\right. \\ & s\left\{\begin{matrix}1 & 1\\ \vdots & \vdots\\ 1 & 1\end{matrix}\right. \\ I & q\left\{\begin{matrix}0 & 1\\ \vdots & \vdots\\ 0 & 1\end{matrix}\right. \\ & \begin{matrix}0 & 0\\ \vdots & \vdots\\ 0 & 0\end{matrix} \end{array}\right)$$

From now on, we will not use the notation S_{pq} or S_{spq}, and use the types (t, u) and (s, t, u) for the convenience of the following section.

Example 5.7. Note that if $n = 2$, then $|\mathbb{F}_2^2| = 4$ and $\mathrm{res} S \leq 1$. We now set $n \geq 3$ and $\mathrm{res} S = 2$. We count the number of isomorphism classes from $n = 3$ to $n = 8$.

(1) For $n = 3$, there is only one, i.e., $(s, t, u) = (1, 2, 2)$.

(2) For $n = 4$, besides (1), there are $(t, u) = (3, 3)$ and $(s, t, u) = (1, 2, 3)$, $(2, 2, 2)$. Thus the total is 4.

(3) For $n = 5$, besides (2), there are $(3, 4)$, $(1, 2, 4)$, $(1, 3, 3)$ and $(2, 2, 3)$. Thus the total is 8.

(4) For $n = 6$, besides (3), there are $(3, 5)$, $(4, 4)$, $(1, 2, 5)$, $(1, 3, 4)$, $(2, 2, 4)$ and $(2, 3, 3)$. The total is 14.

(5) For $n = 7$, besides (4), there are $(3, 6)$, $(4, 5)$, $(1, 2, 6)$, $(1, 3, 5)$, $(1, 4, 4)$, $(2, 2, 5)$, $(2, 3, 4)$ and $(3, 3, 3)$. The total is 22.

(6) For $n = 8$, besides (5), there are $(3, 7)$, $(4, 6)$, $(5, 5)$, $(1, 2, 7)$, $(1, 3, 6)$, $(1, 4, 5)$, $(2, 2, 6)$, $(2, 3, 5)$, $(2, 4, 4)$ and $(3, 3, 4)$. The total is 32.

Similarly, let $f(n)$ be the number of isomorphism classes of type (t, u) satisfying $t + u = n + 2$. Then we get the following.

n	3	4	5	6	7	8	9	10	11	12	13	14	15	$\cdots$
$f(n)$	0	1	1	2	2	3	3	4	4	5	5	6	6	$\cdots$

In general, one can see that

$$f(n) = [n/2] - 1.$$

Next, let $g(n)$ be the number of isomorphism classes of type (s, t, u) satisfying $s + t + u = n + 2$. Then we get the following.

n	3	4	5	6	7	8	9	10	11	12	13	14	15	$\cdots$
$g(n)$	1	2	3	4	6	7	9	11	13	15	18	20	23	$\cdots$

If we denote by $p(n, 3)$, the number of partitions of n by three positive integers, then $g(n)$ is equal to $p(n + 2, 3)$, excluding the case $(1, 1, n)$. Thus we have

$$g(n) = p(n + 2, 3) - 1.$$

Therefore, we obtain

$$\mathcal{I}_2(n) = \sum_{i=3}^{n} (f(i) + g(i)) = \sum_{i=3}^{n} ([i/2] + p(i + 2, 3) - 2).$$

n	3	4	5	6	7	8	9	10	11	12	13	14	$\cdots$
$\mathcal{I}_2(n)$	1	4	8	14	22	32	44	59	76	96	119	144	$\cdots$

6. Similarity classes of the case res$S$ = 2

6.1. In this subsection, we determine a complete representative of the similarity classes of $\mathbb{F}_2^n$ of residue 2. Note that n has to be bigger than 2.

For convenience, we define the following.

Definition 6.1. (1) For a subset $C \subset \mathbb{F}_2^n$, we set $\tilde{C} := C \cup \{0\}$.

(2) A subset $D \subset \mathbb{F}_2^n$ is called a *zero-sum-set* if $\sum_{v \in D} v = 0$ (Thus a circuit is a zero-sum-

set).

At first, as a corollary of Lemma 4.4, we have the following.

Corollary 6.2. *Let C be a zero-sum-set of length i.*

(i) *Suppose that i is odd. If $v \in C$, then $(v + \tilde{C}) \setminus \{0\}$ is a zero-sum-set of length i. If $v \notin C$, then $v + \tilde{C}$ is a zero-sum-set of length $i + 1$.*

(ii) *Suppose that i is even. If $v \in C$, then $(v + \tilde{C}) \setminus \{0, v\}$ is a zero-sum-set of length $i - 1$. If $v \notin C$, then $v + \tilde{C} \setminus \{v\}$ is a zero-sum-set of length i.*

Proof. Through isomorphisms, we can assume that $C = \{\epsilon_1, \dots, \epsilon_{i-1}, \epsilon_1 + \cdots + \epsilon_{i-1}\}$. Then the assertions follow from Lemma 4.4 and its proof. □

Remark 6.3. From Theorem 5.4 (see also Remark 5.5 and Definition 5.6), a PRS of type (t, u) is isomorphic to any PRS containing exactly two circuits of lengths t and u, and a PRS of type (s, t, u) is isomorphic to any PRS containing exactly three circuits of lengths $s + t$, $s + u$ and $t + u$. In other words, the lengths of two or three circuits determine an isomorphism class. Thus, to investigate similarity relations for a PRS S, we only need to consider the type of $v + S$ for $v \in S$ contained in a circuit in S or outside a circuit in S, using Corollary 6.2.

Example 6.4. To simplify the notation, we use the index i, instead of ϵ_i. For example, 2 for ϵ_2, 123 for $\epsilon_1 + \epsilon_2 + \epsilon_3$, etc., and 0 is a zero vector .

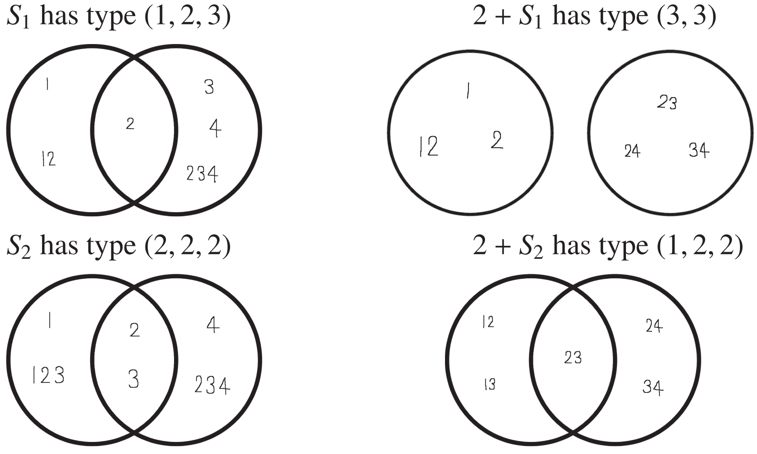
(1) From Example 5.7, if $n = 4$, then the types of isomorphism classes are $(3, 3)$, $(1, 2, 2)$, $(1, 2, 3)$ and $(2, 2, 2)$. Let $S_1 = \{0, 1, 2, 3, 4, 12, 234\}$ be a representative of type $(1, 2, 3)$ and $S_2 = \{0, 1, 2, 3, 4, 123, 234\}$ a representative of type $(2, 2, 2)$ in $\mathbb{F}_2^4$. Then we have

$$2 + S_1 = \{2, 12, 0, 23, 24, 1, 34\} = \{0\} \sqcup \{1, 2, 12\} \sqcup \{23, 24, 34\},$$

which has type $(3, 3)$. Also, we have

$$2 + S_2 = \{2, 12, 0, 23, 24, 13, 34\} = \{0\} \sqcup \{12, 23, 13\} \cup \{23, 24, 34\} \sqcup \{2\},$$

which has type $(1, 2, 2)$.


S_1 has type $(1, 2, 3)$

$2 + S_1$ has type $(3, 3)$

S_2 has type $(2, 2, 2)$

$2 + S_2$ has type $(1, 2, 2)$

Each circle forms a circuit.

Hence, the similarity classes are at most the types $(3,3)$ and $(1,2,2)$. But by Corollary 6.2(i), the type $(3,3)$ can only be similar to $(1,2,3)$ (which has circuits of length 3, 4 and 5), and never similar to $(1,2,2)$ (which has circuits of length 3, 3 and 4). Therefore, for $n = 4$, we have

① $(1,2,3) \sim (3,3)$

② $(2,2,2) \sim (1,2,2)$

and so the total number of similarity classes is just 2.

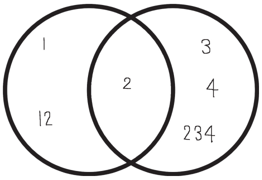
(2) From Example 5.7, if $n = 5$, then the types of isomorphism classes are $(3,3)$, $(3,4)$, $(1,2,2)$, $(1,2,3)$, $(1,2,4)$, $(1,3,3)$, $(2,2,2)$ and $(2,2,3)$. By the observation in (1), we only need to consider the old ones $(1,2,3)$ and $(2,2,2)$, and the new ones, $(3,4)$, $(1,2,4)$, $(1,3,3)$ and $(2,2,3)$.

For the old ones, let $S_1 = \{0,1,2,3,4,5,12,234\}$ be a representative of type $(1,2,3)$ in $\mathbb{F}_2^5$. Since 5 is outside of the three circuits of S_1, we should check $5 + S_1$:

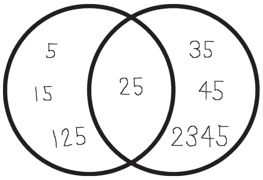
$$5 + S_1 = \{0,5,15,25,35,45,125,2345\} = \{0\} \sqcup \{5,15,25,125\} \cup \{25,35,45,2345\},$$

which has type $(1,3,3)$. Hence, $(1,2,3)$ and $(2,2,2)$ are still not similar in $\mathbb{F}_2^5$.

S_1 has type $(1,2,3)$



$5 + S_1$ has type $(1,3,3)$

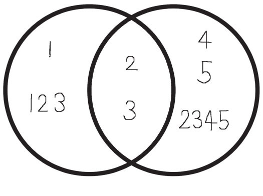


Thus it is enough to consider the types, $(3,4)$, $(1,2,4)$, and $(2,2,3)$. First, by Corollary 6.2(i), type $(3,4)$ is not similar to anyone. Let $S_3 = \{0,1,2,3,4,5,123,2345\}$ be a representative of type $(2,2,3)$. Then we have

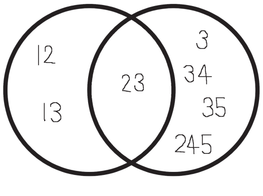
$$3 + S_3 = \{3,13,23,0,34,35,12,245\} = \{0\} \sqcup \{12,13,23\} \cup \{34,35,245,3,23\},$$

which is similar to type $(1,2,4)$.

S_3 has type $(2,2,3)$



$3 + S_1$ has type $(1,2,4)$



Finally, by Corollary 6.2(i), type $(1,2,4)$ is not similar to any of $(3,3)$, $(3,4)$ and $(1,2,2)$. Therefore, for $n = 5$, we have

① $(1,2,2) \sim (2,2,2)$

② $(3,3) \sim (1,2,3) \sim (1,3,3)$

③ $(3,4)$

$$④ \quad (2,2,3) \sim (1,2,4)$$

and so the total number of similarity classes is 4.

As we observed in the examples above, the lengths of circuits are not unique for a similarity class. To classify similarity classes, we define new notations for convenience.

DEFINITION 6.5. (1) A PRS of $\mathbb{F}_2^n$ containing exactly two circuits of length t and u is denoted by $\{t,u\}_n$, where $t,u \geq 3$ and $t+u \leq n+2$. Thus we have $\{t,u\}_n \cong \{u,t\}_n$, and if $t \leq u$, then $\{t,u\}_n$ has type (t,u) (the type defined in Definition 5.6).

(2) A PRS of $\mathbb{F}_2^n$ containing exactly three circuits of lengths $s+t$, $s+u$ and $t+u$ is denoted $\{s,t,u\}_n$, where $s,t,u \geq 1$, $s+t+u \leq n+2$, and two of s, t, u cannot be 1 (since the length of a circuit is more than 2). Thus we have $\{s,t,u\}_n = \{s,u,t\}_n = \cdots = \{u,t,s\}_n$ (any permutation of s, t, u), and if $s \leq t \leq u$, then $\{s,t,u\}_n$ has type (s,t,u) (the type defined in Definition 5.6). Also, if a PRS S has three circuits of length x,y and z, then S is isomorphic to $\{\frac{x+y-z}{2}, \frac{x-y+z}{2}, \frac{-x+y+z}{2}\}_n$.

REMARK 6.6. (1) $\{t,u\}_n$ is isomorphic to the PRS

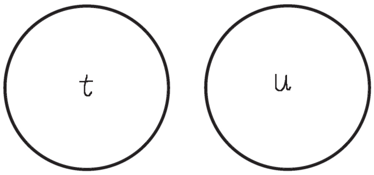
$$\left\{\epsilon_1, \epsilon_2, \ldots, \epsilon_n, \sum_{1\leq i\leq t-1} \epsilon_i, \sum_{t\leq j\leq t+u-2} \epsilon_j\right\},$$

containing two disjoint circuits

$$C_1 = \left\{\epsilon_1, \epsilon_2, \ldots, \epsilon_{t-1}, \sum_{1\leq i\leq t-1} \epsilon_i\right\},$$

$$C_2 = \left\{\epsilon_t, \epsilon_{t+1}, \ldots, \epsilon_{t+u-2}, \sum_{t\leq j\leq t+u-2} \epsilon_j\right\}.$$

We denote the Venn diagram of circuits for $\{t,u\}_n$ by the following picture:



(2) $\{s,t,u\}_n$ is isomorphic to the PRS

$$\left\{\epsilon_1, \epsilon_2, \ldots, \epsilon_n, \sum_{1\leq i\leq s+t-1} \epsilon_i, \sum_{s\leq j\leq s+t+u-2} \epsilon_j\right\},$$

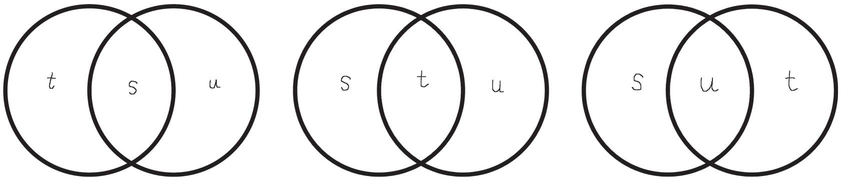
containing three circuits

$$C_1 = \left\{\epsilon_1, \epsilon_2, \ldots, \epsilon_{s+t-1}, \sum_{1\leq i\leq s+t-1} \epsilon_i\right\},$$

$$C_2 = \left\{\epsilon_s, \epsilon_{s+1}, \ldots, \epsilon_{s+t+u-2}, \sum_{s\leq j\leq s+t+u-2} \epsilon_j\right\},$$

$$C_3 = \left\{\epsilon_1, \ldots, \epsilon_{s-1}, \epsilon_{s+t}, \ldots, \epsilon_{s+t+u-2}, \sum_{1\le i\le s+t-1} \epsilon_i, \sum_{s\le j\le s+t+u-2} \epsilon_j\right\}.$$

Note that $C_1 = C_2 \vartriangle C_3$, $C_2 = C_3 \vartriangle C_1$ and $C_3 = C_1 \vartriangle C_2$, and the Venn diagram of circuits for $\{s, t, u\}_n$ can be any of the following pictures:



Definition 6.7. If one of s, t, u is zero, then $\{s, t, u\}_n$ can be considered as the case having disjoint circuits. Thus, we set $\{0, s, t\}_n := \{s, t\}_n$.

We will use the following lemma which is now clear.

Lemma 6.8. *Let S be a PRS of $\mathbb{F}_2^n$ of residue* 2*. Then, S has exactly three zero-sum-sets, say C_1, C_2 and C_3. Moreover:*

(1) *If S has two disjoint zero-sum-sets, say $C_1 \cap C_2 = \phi$, then S is isomorphic to $\{|C_1|, |C_2|\}_n$, and $C_3 = C_1 \cup C_2$.*

(2) *If any two of the zero-sum-sets are not disjoint, then S is isomorphic to*

$$\left\{\frac{|C_1| + |C_2| - |C_3|}{2}, \frac{|C_1| - |C_2| + |C_3|}{2}, \frac{-|C_1| + |C_2| + |C_3|}{2}\right\}_n.$$

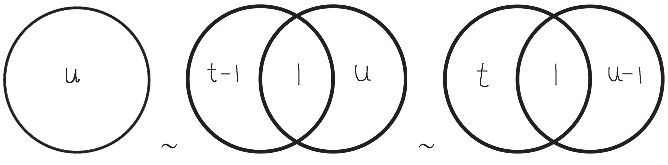
We also define the following term.

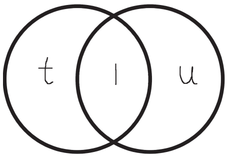
Definition 6.9. A PRS $\{t, u\}_n$ (resp. $\{s, t, u\}_n$) is called *full* if it satisfies $t + u = n + 2$ (resp. $s + t + u = n + 2$).

We can now show many similarity relations.

Lemma 6.10. *Let t and u be odd. If $\{t, u\}_n$ is full, then $\{t, u\}_n \sim \{1, t-1, u\}_n \sim \{1, t, u-1\}_n$, and if $\{t, u\}_n$ is not full, then we have an extra relation $\{t, u\}_n \sim \{1, t, u\}_n$. Moreover, no more similarity relation exists in this case.*

For odd t and odd u,



and similar to 

if it is full.

Proof. Let $S = \{t, u\}_n$ having only two circuits C_1 and C_2 with $C_1 \cap C_2 = \emptyset$, $|C_1| = t$ and $|C_2| = u$. If S is full, it is enough to check the type of the PRS $v + S$, where $v \in C_1$ or $v \in C_2$. If $v \in C_1$, then $v + S$ contains zero-sum-sets $(v + \tilde{C}_1) \setminus \{0\}$ of length t and $(v + \tilde{C}_2)$ of length $u + 1$ with intersection $\{v\}$ from Corollary 6.2, and hence by Lemma 6.8, $S \cong \{1, t - 1, u\}_n$. Similarly, by taking $v \in C_2$, we get that $v + S \cong \{1, t, u - 1\}_n$.

If S is not full, we can take $v \in (C_1 \cup C_2)^c$ (the complement of $C_1 \cup C_2$) and $v + S$ has two zero-sum-sets, i.e., $(v + \tilde{C}_1)$ of length $t + 1$ and $(v + \tilde{C}_2)$ of length $u + 1$ with intersection $\{v\}$ by Corollary 6.2, and hence by Lemma 6.8, $S \cong \{1, t, u\}_n$.

Finally, the last statement is clear since we have checked all possibilities of similarity relations. □

Lemma 6.11. *Let t be odd and u even. If $\{t, u\}_n$ is full, then $\{t, u\}_n \sim \{t + 1, u - 1\}_n$, and if $\{t, u\}_n$ is not full, then we have an extra relation $\{t, u\}_n \sim \{t + 1, u\}_n$. Moreover, no more similarity relation exists in this case.*

Proof. We can show this in the same way as in Lemma 6.10. This time each of the two cases, $v \in C_2$ and $v \in (C_1 \cup C_2)^c$, gives us a new relation, but the case, $v \in C_1$, does not. □

Lemma 6.12. *Let t and u be even. Then $\{t, u\}_n \sim \{t - 1, u\}_n \sim \{t, u - 1\}_n$. Moreover, no more similarity relation exists in this case.*

Proof. Again, we can show this in the same way as in Lemma 6.10. This time each of the two cases, $v \in C_1$ and $v \in C_2$, gives us a new relation, but the case, $v \in (C_1 \cup C_2)^c$, does not. □

Lemma 6.13. *Let $s+t$ and $s+u$ be odd. If $\{s, t, u\}_n$ is full, then $\{s, t, u\}_n \sim \{s+1, t-1, u\}_n \sim \{s+1, t, u-1\}_n$, and if $\{s, t, u\}_n$ is not full, then we have an extra relation $\{s, t, u\}_n \sim \{s+1, t, u\}_n$. Moreover, no more similarity relation exists in this case.*

Proof. Let $S = \{s, t, u\}_n$ having three circuits C_1, C_2 and C_3 such that $|C_1| = s + t$ and $|C_2| = s + u$ are odd. Note that $|C_3| = t + u$ is even since $2s + t + u$ is even.

If S is full, then it is enough to check the type of $v + S$ for $v \in C_1 \cap C_2$, $v \in C_1 \setminus C_2$ or $v \in C_2 \setminus C_1$. First, if $v \in C_1 \cap C_2$, then $v + S$ has the zero-sum-sets, $(v + \tilde{C}_1) \setminus \{0\}$ of length $s + t$, $(v + \tilde{C}_2) \setminus \{0\}$ of length $s + u$ and $(v + \tilde{C}_3) \setminus \{v\}$ of length $t + u$ by Corollary 6.2. Moreover, we have

$$[(v + \tilde{C}_1) \setminus \{0\}] \cap [(v + \tilde{C}_2) \setminus \{0\}] = v + \widetilde{C_1 \cap C_2} \setminus \{0\},$$
$$[(v + \tilde{C}_1) \setminus \{0\}] \cap [(v + \tilde{C}_3) \setminus \{v\}] = v + \widetilde{C_1 \cap C_3} \setminus \{v\},$$
$$[(v + \tilde{C}_2) \setminus \{0\}] \cap [(v + \tilde{C}_3) \setminus \{v\}] = v + \widetilde{C_1 \cap C_3} \setminus \{v\},$$

and they are all nonempty. Hence, by Lemma 6.8, these three zero-sum-sets are all circuits, and S has type $\{s, t, u\}_n$.

Next, let $v \in C_1 \setminus C_2$. Suppose that $t = 1$, i.e., $C_1 \setminus C_2 = C_1 \cap C_3 = \{v\}$. Then, $v + S$ has the zero-sum-sets $(v + \tilde{C}_1) \setminus \{0\}$ of length $s + 1$, $(v + \tilde{C}_2)$ of length $s + u + 1$ and $(v + \tilde{C}_3) \setminus \{0, v\}$ of length u, by Corollary 6.2. Moreover, we have $[(v + \tilde{C}_1) \setminus \{0\}] \cap [(v + \tilde{C}_3) \setminus \{0, v\}] = \emptyset$, and by Lemma 6.8, $S \cong \{s + 1, u\}_n = \{s + 1, 0, u\}_n = \{s + 1, t - 1, u\}_n$ (see Definition 6.7). Note that $v + \tilde{C}_2$ is the disjoint union of $(v + \tilde{C}_1) \setminus \{0\}$ and $(v + \tilde{C}_3) \setminus \{0, v\}$.

Suppose that $t \geq 2$. Then $v + S$ has the zero-sum-sets, $(v + \tilde{C}_1) \setminus \{0\}$ of length $s + t$, $v + \tilde{C}_2$ of length $s + u + 1$ and $(v + \tilde{C}_3) \setminus \{0, v\}$ of length $t + u - 1$, by Corollary 6.2. Moreover, we have

$$[(v + \tilde{C}_1) \setminus \{0\}] \cap [v + \tilde{C}_2] = (v + \widetilde{C_1 \cap C_2}),$$

$$[(v + \tilde{C}_1) \setminus \{0\}] \cap [(v + \tilde{C}_3) \setminus \{0, v\} = (v + \widetilde{C_1 \cap C_3}) \setminus \{0, v\},$$

$$[v + \tilde{C}_2] \cap [(v + \tilde{C}_3) \setminus \{0, v\}] = (v + \widetilde{C_2 \cap C_3}) \setminus \{v\},$$

and they are all nonempty. Hence, by Lemma 6.8, these three zero-sum-sets are all circuits, and $S \cong \{s + 1, t - 1, u\}_n$.

Let $v \in C_2 \setminus C_1$. As above, suppose $u = 1$, and so $C_2 \setminus C_1 = C_2 \cap C_3 = \{v\}$. Then, $v + \{s, t, 1\}_n$ has the zero-sum-sets, $v + \tilde{C}_1$ of length $s + t + 1$, $(v + \tilde{C}_2) \setminus \{0\}$ of length $s + 1$ and $(v + \tilde{C}_3) \setminus \{0, v\}$ of length t, by Corollary 6.2. Moreover, we have $[(v + \tilde{C}_2) \setminus \{0\}] \cap [(v + \tilde{C}_3) \setminus \{0, v\}] = \emptyset$, and so by Lemma 6.8, $S \cong \{s + 1, t\}_n = \{s + 1, t, 0\}_n = \{s + 1, t, u - 1\}_n$ (see Definition 6.7). Note that $v + \tilde{C}_1$ is the disjoint union of $(v + \tilde{C}_2) \setminus \{0\}$ and $(v + \tilde{C}_3) \setminus \{0, v\}$.

Suppose that $u \geq 2$, then $v + \{s, t, u\}_n$ has the zero-sum-sets, $v + \tilde{C}_1$ of length $s + t + 1$, $(v + \tilde{C}_2) \setminus \{0\}$ of length $s + u$ and $(v + \tilde{C}_3) \setminus \{0, v\}$ of length $t + u - 1$, by Corollary 6.2. Moreover, we have

$$(v + \tilde{C}_1) \cap [(v + \tilde{C}_2) \setminus \{0\}] = (v + \widetilde{C_1 \cap C_2}),$$

$$(v + \tilde{C}_1) \cap [(v + \tilde{C}_3) \setminus \{0, v\} = (v + \widetilde{C_1 \cap C_3}) \setminus \{v\},$$

$$[(v + \tilde{C}_2) \setminus \{0\}] \cap [(v + \tilde{C}_3) \setminus \{0, v\}] = (v + \widetilde{C_2 \cap C_3}) \setminus \{0, v\},$$

and they are all nonempty. Hence, by Lemma 6.8, these three zero-sum-sets are all circuits, and $S \cong \{s + 1, t, u - 1\}_n$.

If S is not full, we can take $v \in (C_1 \cup C_2)^c$. Then, $v + \{s, t, u\}_n$ has the zero-sum-sets, $v + \tilde{C}_1$ of length $s + t + 1$, $v + \tilde{C}_2$ of length $s + u + 1$ and $(v + \tilde{C}_3) \setminus \{v\}$ of length $t + u$, by Corollary 6.2. Moreover, we have

$$[v + \tilde{C}_1] \cap [v + \tilde{C}_2] = v + \widetilde{C_1 \cap C_2},$$

$$[v + \tilde{C}_1] \cap [(v + \tilde{C}_3) \setminus \{v\}] = v + \widetilde{C_1 \cap C_3} \setminus \{v\},$$

$$[v + \tilde{C}_2] \cap [(v + \tilde{C}_3) \setminus \{v\}] = v + \widetilde{C_1 \cap C_3} \setminus \{v\},$$

and they are all nonempty. Hence, by Lemma 6.8, these three zero-sum-sets are all circuits, and $S \cong \{s + 1, t, u\}_n$. Thus the proof is complete. □

Lemma 6.14. *Let $s + t$ be even and $s + u$ odd. If $\{s, t, u\}_n$ is full, then $\{s, t, u\}_n \sim \{s - 1, t, u + 1\}_n \sim \{s, t - 1, u + 1\}_n$, and if $\{s, t, u\}_n$ is not full, then we have an extra relation $\{s, t, u\}_n \sim \{s, t, u + 1\}_n$. Moreover, no other similarity relation exists in this case.*

Proof. We can show this in the same way as in Lemma 6.13. This time each of the three cases, $v \in C_1 \cap C_2$, $v \in C_1 \setminus C_2$ and $v \in (C_1 \cup C_2)^c$, gives us a new relation, but the case, $v \in C_2 \setminus C_1$, does not. □

Lemma 6.15. *Let $s + t$ and $s + u$ be even. Then, $\{s, t, u\} \sim \{s - 1, t, u\}_n \sim \{s, t - 1, u\}_n \sim \{s, t, u - 1\}_n$. Moreover, no other similarity relation exists in this case.*

Proof. Again we can show this in the same way as in Lemma 6.13. This time each of the three cases, $v \in C_1 \cap C_2$, $v \in C_1 \setminus C_2$ and $v \in C_2 \setminus C_1$, gives us a new relation, but the case, $v \in (C_1 \cup C_2)^c$, does not. □

The following proposition summarizes all the similarity relations in the previous lemmas.

Proposition 6.16. *We list all similarity relations as follows.*

(1) $\{2k+1, 2l+1\}_n \sim \{1, 2k, 2l+1\}_n \sim \{1, 2k+1, 2l\}_n$ *for full type, and* $\sim \{1, 2k+1, 2l+1\}_n$ *for non-full type.*
(2) $\{2k+1, 2l\}_n \sim \{2k+2, 2l-1\}_n$ *for full type, and* $\sim \{2k+2, 2l\}_n$ *for non-full type.*
(3) $\{2k, 2l\}_n \sim \{2k-1, 2l\}_n \sim \{2k, 2l-1\}_n$.
(4) $\{s, t, u\}_n \sim \{s+1, t-1, u\}_n \sim \{s+1, t, u-1\}_n$ *for full type, where* $s+t$ *and* $s+u$ *are odd, and* $\sim \{s+1, t, u\}_n$ *for non-full type.*
(5) $\{s, t, u\}_n \sim \{s-1, t, u+1\}_n \sim \{s, t-1, u+1\}_n$ *for full type, where* $s+t$ *is even and* $s+u$ *is odd, and* $\sim \{s, t, u+1\}_n$ *for non-full type.*
(6) $\{s, t, u\}_n \sim \{s-1, t, u\}_n \sim \{s, t-1, u\}_n \sim \{s, t, u-1\}_n$, *where* $s+t$ *and* $s+u$ *are even.*

6.2. Toward classification.

Definition 6.17. A PRS S is called of *type A* if $S \cong \{t, u\}_n$, and of *type B* if $S \cong \{s, t, u\}_n$.

Lemma 6.18. *For* $a, b, c \in \mathbb{N}$, $\{a, b, c\}_n$ *has type A if and only if* $a = 1$ *and* $(b, c) \equiv (0,1), (1,0), (1,1) \bmod 2$.

Proof. For "if" part, by Proposition 6.16 (1), (2) and (3), for $p, q \geq 1$ with $1 + (2p+1) + (2q+1) \leq n+2$, we see $\{1, 2p+1, 2q+1\}_n \sim \{2p+1, 2q+1\}_n$ and for $r, s \geq 1$ with $1 + (2r+1) + 2s \leq n+2$, we have $\{1, 2r+1, 2s\}_n \sim \{2r+1, 2s+1\}_n$.

For "only if" part, if $\{a, b, c\}_n \sim \{x, y, z\}_n$, then, without loss of generality, we can assume that $x \in \{a, a \pm 1\}$, $y \in \{b, b \pm 1\}$ and $z \in \{c, c \pm 1\}$. Hence, if $x, y, z \geq 2$, then $\{x, y, z\}_n$ is not similar to a PRS of type A. Also, $\{1, 2t, 2u\}_n$ cannot have type A from Proposition 6.16 (1), (2) and (3). This completes the proof. □

Thus the similarity classes decompose into three parts.

Lemma 6.19. *The similarity classes in* $\mathbb{F}_2^n$ *are the disjoint union of similarity classes of* $\{x, y\}_n$, *similarity classes of* $\{1, 2x, 2y\}_n$ *and similarity classes of* $\{s, t, u\}_n$ *for* $s, t, u \geq 2$.

Proof. By Lemma 6.18, $\{1, 2x+1, 2y\}_n$ and $\{1, 2x+1, 2y+1\}_n$ are similar to a PRS of type A, and moreover, $\{s, t, u\}_n$ for $s, t, u \geq 2$ is never similar to a PRS of type A. Hence the assertion is shown. □

6.3. Classification of type A. In this subsection we determine the similarity classes of $\{t, u\}_n$. Note that $n \geq 4$ and $t, u \geq 3$.

Let

$$U = \{\{2p+1, 2q+1\}_n \mid p, q \geq 1,\ 2p+2q+2 \leq n+2\},$$
$$V = \{\{2p, 2q+1\}_n \mid p \geq 2,\ q \geq 1,\ 2p+2q+1 \leq n+2\}.$$

Then we have the following:

Lemma 6.20. *The similarity classes of $\{t,u\}_n$ are the disjoint union of similarity classes containing U and similarity classes containing V.*

Proof. From Proposition 6.16 (3), we see $\{2k,2l\}_n \sim \{2k-1,2l\}_n$. From Proposition 6.16 (1), $\{2p+1,2q+1\}_n$ is not similar to $\{2x,2y+1\}_n$, and hence the proof is finished. □

Lemma 6.21. *The set U is a complete representative system of the similarity classes containing U.*

Proof. By Proposition 6.16 (1), $\{2p+1,2q+1\}_n$ is the only similarity class of type A, and so the assertion is shown. □

Let

$$\begin{aligned}
V_1 &= \{\{4p,4q+1\}_n \mid p,q \geq 1,\ 4p+4q+1 \leq n+2\},\\
V_2 &= \{\{4p,4q+3\}_n \mid p \geq 1,\ q \geq 0,\ 4p+4q+3 \leq n+2\},\\
V_3 &= \{\{4p+2,4q+1\}_n \mid p,q \geq 1,\ 4p+4q+3 \leq n+2\},\\
V_4 &= \{\{4p+2,4q+3\}_n \mid p \geq 1,\ q \geq 0,\ 4p+4q+5 \leq n+2\}.
\end{aligned}$$

Then we have the following:

Lemma 6.22. *The similarity classes of V are the disjoint union of similarity classes containing V_1, similarity classes containing V_2 and similarity classes containing V_3.*

Proof. The similarity classes of V are the union of similarity classes of V_1, V_2, V_3 and V_4. But V_4 can be eliminated because, for any $x \in V_4$, there exists $y \in V_1$ such that $x \sim y$ by Proposition 6.16 (2). Moreover, any two elements in V_1, V_2, and V_3 are not similar to each other by Proposition 6.16 (2). Hence we obtain the assertion. □

Let

$$\begin{aligned}
V_2' &= \{\{4p,4q+3\}_n \in V_2 \mid p \leq q+1\} \subset V_2,\\
V_3' &= \{\{4p+2,4q+1\}_n \in V_3 \mid p \leq q\} \subset V_3.
\end{aligned}$$

Then we have the following:

Lemma 6.23. (i) *The set V_1 is a complete representative system of the similarity classes containing V_1.*

(ii) *The subset V_2' of V_2 is a complete representative system of the similarity classes containing V_2.*

(iii) *The subset V_3' of V_3 is a complete representative system of the similarity classes containing V_3.*

Proof. All statements follow from Proposition 6.16 (2). In fact, we only have the relation $\{2k+1,2l\}_n \sim \{2k+2,2l-1\}_n$ for these cases.

For (i), we have $\{4p,4q+1\}_n \sim \{4p-1,4q+2\}_n$, and we have already eliminated the similarity classes of $\{4p-1,4q+2\}_n$ in Lemma 6.22.

For (ii), we have the relation $\{4p,4q+3\}_n \sim \{4p-1,4q+4\}_n$. Now, if $p > q+1$, then letting $x := q+1$ and $y := p-1$ for convenience, we have $\{4p,4q+3\}_n \sim \{4x,4y+3\}_n$ with

$x < y+1$. Thus the similarity classes of V_2 consist of the similarity classes of V_2'. Next if $\{4p, 4q+3\}_n \sim \{4x, 4y+3\}_n$ for $p \leq q+1$ and $x \leq y+1$, then ① $p = x$ and $q = y$, or ② $4q+4 = 4x$ and $4p-1 = 4y+3$, i.e., $x = q$ and $p = y+1$. We are done if ② cannot happen.

Now, ② implies $q \leq p$ since $q = x \leq y+1 = p$. Moreover, since $p \leq q+1$, we have $p = q$ or $p = q+1$. If $p = q$, then we have $x = p$ (and $y = p-1$), and so $\{4p, 4p+3\}_n \sim \{4p, 4(p-1)+3\}_n = \{4p, 4p-1\}_n$, which is impossible by Propositon 6.16 (2). If $p = q+1$, then we have $x = p-1$ (and $y = p-1$), and so $\{4p, 4p+3\}_n \sim \{4(p-1), 4(p-1)+3\}_n = \{4p-4, 4p-1\}_n$, which is impossible by Proposition 6.16 (2). Thus we have shown that ② cannot happen.

For (iii), we have the relation $\{4p+2, 4q+1\}_n \sim \{4p+1, 4q+2\}_n$. Now, if $p > q$, then letting $x := q$ and $y := p$ for convenience, we have $\{4p+2, 4q+1\}_n \sim \{4x+2, 4y+1\}_n$ with $x < y$. Thus the similarity classes of V_3 consist of the similarity classes of V_3'. Next if $\{4p+2, 4q+1\}_n \sim \{4x+2, 4y+1\}_n$ for $p \leq q$ and $x \leq y$, then ① $p = x$ and $q = y$, or ② $4q+2 = 4x+2$ and $4p+1 = 4y+1$, i.e., $x = q$ and $p = y$. But ② implies $q \leq p$ since $q = x \leq y = p$. Moreover, since $p \leq q$, we have $p = q$. Thus ② implies ①. So we are done. □

The following proposition summarizes the above results.

Proposition 6.24. *A complete representative system of the similarity classes of type* $\{t, u\}_n$ *is the disjoint union of* U, V_1, V_2' *and* V_3'.

6.4. Classification of type B. Let $\mathfrak{S} = \mathfrak{S}_1 \sqcup \mathfrak{S}_2$, where

$$\mathfrak{S}_1 = \{\{1, 2x, 2y\}_n |\ x, y \geq 1,\ 1+2x+2y \leq n+2\} \quad (n \geq 3),$$
$$\mathfrak{S}_2 = \{\{s, t, u\}_n |\ s, t, u \geq 2,\ s+t+u \leq n+2\}.$$

We need to determine a complete representative system of $\mathfrak{S}$ (see Lemma 6.19).

Lemma 6.25. *Suppose that* $\{s, t, u\}_n$ *and* $\{s', t', u'\}_n$ *satisfy* $|(s+t+u) - (s'+t'+u')| \geq 2$. *Then* $\{s, t, u\}_n$ *is not similar to* $\{s', t', u'\}_n$.

Proof. It follows from Proposition 6.16. □

Lemma 6.26. *For* $\{s, t, u\}_n$, *there exists a PRS* $\{x, y, z\}_n$ *with* $x+y+z \equiv n \mod 2$ *such that* $\{s, t, u\}_n \sim \{x, y, z\}_n$.

Proof. Suppose that $n \in 2\mathbb{Z}$. If $s+t+u \in 2\mathbb{Z}$, then we can set $\{x, y, z\}_n = \{s, t, u\}_n$. If $s+t+u \in 2\mathbb{Z}+1$, then $\{s, t, u\}$ is not of full type. Thus we can proceed to show this on a case by case basis for the parities of s, t and u.

Let $(s, t, u) \equiv (1, 0, 0), (0, 1, 0), (0, 0, 1) \mod 2$. Then from Proposition 6.16, we have $\{s, t, u\} \sim \{s+1, t, u\}_n$ when $(s, t, u) \equiv (1, 0, 0) \mod 2$, $\{s, t, u\} \sim \{s, t+1, u\}$ when $(s, t, u) \equiv (0, 1, 0) \mod 2$, and $\{s, t, u\} \sim \{s, t, u+1\}_n$ when $(s, t, u) \equiv (0, 0, 1) \mod 2$, and therefore we can set $\{x, y, z\}_n = \{s+1, t, u\}_n, \{s, t+1, u\}_n$ and $\{s, t, u+1\}_n$ respectively. If $(s, t, u) \equiv (1, 1, 1) \mod 2$, then $\{s, t, u\}_n \sim \{s-1, t, u\}_n$ from Proposition 6.16, and we can set $\{x, y, z\}_n = \{s-1, t, u\}_n$.

Suppose that $n \in 2\mathbb{Z}+1$. If $s+t+u \in 2\mathbb{Z}+1$, then we can set $\{x, y, z\}_n = \{s, t, u\}_n$. If $s+t+u \in 2\mathbb{Z}$, then $\{s, t, u\}$ is not full. Thus we show this on a case by case basis. Let

$(s,t,u) \equiv (1,1,0),(1,0,1),(0,1,1) \mod 2$. Then from Proposition 6.16, we have $\{s,t,u\} \sim \{s,t,u+1\}_n$ when $(s,t,u) \equiv (1,1,0) \mod 2$, $\{s,t,u\} \sim \{s,t+1,u\}$ when $(s,t,u) \equiv (1,0,1) \mod 2$, and $\{s,t,u\} \sim \{s+1,t,u\}_n$ when $(s,t,u) \equiv (0,1,1) \mod 2$, and therefore we can set $\{x,y,z\}_n = \{s,t,u+1\}_n, \{s,t+1,u\}_n$ and $\{s+1,t,u\}_n$ respectively. If $(s,t,u) \equiv (0,0,0) \mod 2$, then $\{s,t,u\}_n \sim \{s-1,t,u\}_n$ from Proposition 6.16, and we can set $\{x,y,z\}_n = \{s-1,t,u\}_n$. This completes the proof. □

6.4.1. The case of $n \in 2\mathbb{Z}+1$**.** In this subsection we determine a complete representative system of $\mathfrak{S}$ for $n \in 2\mathbb{Z}+1$. From Lemma 6.26, any PRS in $\mathfrak{S}$ with $n \in 2\mathbb{Z}+1$ is similar to a PRS in $\mathfrak{T} = \mathfrak{T}_1 \sqcup \mathfrak{T}_2$, where

$$\begin{aligned}\mathfrak{T}_1 &= \{\{2p,2q,2r-1\}_n \mid p,q,r \geq 1\},\\ \mathfrak{T}_2 &= \{\{2p+1,2q+1,2r+1\}_n \mid p,q,r \geq 1\}.\end{aligned}$$

Note that $\mathfrak{T}_1$ contains $\{\{1,2x,2y\}_n \mid x,y \geq 1\}$.

Let

$$\mathfrak{T}_1' = \{\{2x,2x,2z-1\}_n \in \mathfrak{T}_1 \mid 2x,2y > 2r-1\} \subset \mathfrak{T}_1.$$

Lemma 6.27. *The set* $\mathfrak{T}_1'$ *is a complete representative system of the similarity classes containing* $\mathfrak{T}_1$*.*

Proof. From Proposition 6.16 (5), we see $\{2p,2q,2r-1\}_n \sim \{2p,2q-1,2r\}_n \sim \{2p-1,2q,2r\}_n$ for $p,q,r \geq 1$ with $2p+2q+2r-1 \leq n+2$. So we can take the odd part as a minimum entry.

Suppose $\{2a,2b,2c-1\}_n \sim \{2x,2y,2z-1\}$ with $2a,2b > 2c-1$ and $2x,2y > 2z-1$. We see $2a+2b+(2c-1) = 2x+2y+(2z-1)$ from Lemma 6.25. Then, Proposition 6.16 (5) yields that $\{2a,2b,2c-1\} = \{2x,2y,2z-1\}$ as sets, and hence $\{2a,2b,2c-1\}_n = \{2x,2y,2z-1\}_n$. □

Lemma 6.28. *The set* $\mathfrak{T}_2$ *is a complete representative system of the similarity classes containing* $\mathfrak{T}_2$*.*

Proof. From Lemma 6.25, Proposition 6.16 (6) and a similar argument as in the proof of Lemma 6.27, we obtain the assertion. □

We summarize the above lemmas as a proposition.

Proposition 6.29. *A complete representative system of the similarity classes containing* $\mathfrak{T}$ *is the disjoint union of the sets* $\mathfrak{T}_1'$ *and* $\mathfrak{T}_2$*.*

6.4.2. The case of $n \in 2\mathbb{Z}$**.** In this subsection we determine a complete representative system of $\mathfrak{S}$ for $n \in 2\mathbb{Z}$. From Lemma 6.26, any PRS in $\mathfrak{S}$ with $n \in 2\mathbb{Z}$ is similar to a PRS in $\mathfrak{U} = \mathfrak{U}_1 \sqcup \mathfrak{U}_2$, where

$$\begin{aligned}\mathfrak{U}_1 &= \{\{2x,2y,2z\}_n \mid x,y,z \geq 1\},\\ \mathfrak{U}_2 &= \{\{2p+1,2q+1,2r\}_n \mid p,q,r \geq 1\}.\end{aligned}$$

Let

$$\mathfrak{U}'_1 = \{\{2p+1, 2q+1, 2r\}_n \in \mathfrak{U}_1 \mid 2p+1, 2q+1 > 2r\} \subset \mathfrak{U}_1.$$

Lemma 6.30. *The set $\mathfrak{U}'_1$ is a complete representative system of the similarity classes containing $\mathfrak{U}_1$.*

Proof. From Proposition 6.16 (5), we see $\{2p+1, 2q+1, 2r\}_n \sim \{2p+1, 2q, 2r+1\}_n \sim \{2p, 2q+1, 2r+1\}_n$ for $p, q, r \geq 1$ with $(2p+1) + (2q+1) + 2r \leq n+2$. So we can set the even part as a minimum entry.

Suppose $\{2a+1, 2b+1, 2c\}_n \sim \{2x+1, 2y+1, 2z\}$ with $2a+1, 2b+1 > 2c$ and $2x+1, 2y+1 > 2z$ with $a, b, c, x, y, z \geq 1$. From Lemma 6.25, we see $(2a+1)+(2b+1)+2c = (2x+1)+(2y+1)+2z$. From Proposition 6.16 (5), we can conclude that $\{2a+1, 2b+1, 2c\} = \{2x+1, 2y+1, 2z\}$ as sets, and hence $\{2a+1, 2b+1, 2c\}_n = \{2x+1, 2y+1, 2z\}_n$. Hence we obtain the assertion. □

Lemma 6.31. *The set $\mathfrak{U}_2$ is a complete representative system of the similarity classes containing $\mathfrak{U}_2$.*

Proof. From Lemma 6.25, Proposition 6.16 (6) and a similar argument as in the proof of Lemma 6.30, we obtain the assertion. □

The following proposition summarizes lemmas above.

Proposition 6.32. *A complete representative system of the similarity classes containing $\mathfrak{U}$ is the disjoint union of the sets $\mathfrak{U}'_1$ and $\mathfrak{U}_2$.*

6.4.3. A complete representative system. We summarize the results from Lemma 6.19, Proposition 6.24, Proposition 6.29 and Proposition 6.32 in the following two theorems.

Theorem 6.33. *Let $n \in 2\mathbb{Z}$ with $n \geq 4$. The following sets form a complete representative system of the similarity classes of residue 2 in $\mathbb{F}_2^n$.*

(1) $\{\{2p+1, 2q+1\}_n \mid 2p+2q+2 \leq n+2\}$;
(2) $\{\{4p, 4q+1\}_n \mid 4p+4q+1 \leq n+2\}$;
(3) $\{\{4p, 4q+3\}_n| \mid p \leq q+1$ *and* $4p+4q+3 \leq n+2\}$;
(4) $\{\{4p+2, 4q+1\}_n \mid p \leq q$ *and* $4p+4q+3 \leq n+2\}$;
(5) $\{\{2p+1, 2q+1, 2r\}_n \mid 2r < 2p+1, 2q+1$ *and* $2p+2q+2r+2 \leq n+2\}$;
(6) $\{\{2p, 2q, 2r\}_n \mid 2p+2q+2r \leq n+2\}$, *where* $p, q, r \in \mathbb{N}$.

Theorem 6.34. *Let $n \in 2\mathbb{Z}+1$ with $n \geq 3$. The following sets form a complete representative system of the similarity classes of residue 2 in $\mathbb{F}_2^n$.*

(1) $\{2p+1, 2q+1\}_n \mid 2p+2q+2 \leq n+2\}$;
(2) $\{\{4p, 4q+1\}_n \mid 4p+4q+1 \leq n+2\}$;
(3) $\{\{4p, 4q+3\}_n \mid p \leq q+1$ *and* $4p+4q+3 \leq n+2\}$;
(4) $\{\{4p+2, 4q+1\}_n \mid p \leq q$ *and* $4p+4q+3 \leq n+2\}$;
(5) $\{\{2p, 2q, 2r-1\}_n \mid 2z-1 < 2x, 2y$ *and* $2x+2y+2z-1 \leq n+2\}$;
(6) $\{\{2p+1, 2q+1, 2r+1\}_n \mid 2p+2q+2r+3 \leq n+2\}$, *where* $p, q, r \in \mathbb{N}$.

Example 6.35. (1) In Example 6.4(1), the total number of similarity classes in $\mathbb{F}_2^4$ is 2, and we box a complete representative system following Theorem 6.34:

① $(1,2,3) \sim \boxed{(3,3)}$ ② $\boxed{(2,2,2)} \sim (1,2,2)$

(2) In Example 6.4(2), the total number of similarity classes in $\mathbb{F}_2^5$ is 4, and we box a complete representative system following Theorem 6.33:

① $\boxed{(1,2,2)} \sim (2,2,2)$ ② $\boxed{(3,3)} \sim (1,2,3) \sim (1,3,3)$
③ $\boxed{(3,4)}$ ④ $(2,2,3) \sim \boxed{(1,2,4)}$

(3) We did the same observation for $n = 6$:

① $(1,2,2) \sim \boxed{(2,2,2)}$ ② $\boxed{(3,3)} \sim (1,2,3) \sim (1,3,3)$ ③ $\boxed{(3,4)} \sim (4,4)$
④ $(1,2,4) \sim (2,2,3) \sim \boxed{(2,2,4)}$ ⑤ $\boxed{(3,5)} \sim (1,2,5) \sim (1,3,4)$
⑥ $\boxed{(2,3,3)}$

and the total number of similarity classes in $\mathbb{F}_2^6$ is 6.

(4) We did the same observation for $n = 7$:

① $\boxed{(1,2,2)} \sim (2,2,2)$ ② $\boxed{(3,3)} \sim (1,2,3) \sim (1,3,3)$ ③ $\boxed{(3,4)} \sim (4,4)$
④ $\boxed{(1,2,4)} \sim (2,2,3) \sim (2,2,4)$ ⑤ $\boxed{(3,5)} \sim (1,2,5) \sim (1,3,4) \sim (1,3,5)$
⑥ $(2,3,3) \sim \boxed{(3,3,3)}$ ⑦ $\boxed{(4,5)} \sim (3,6)$ ⑧ $\boxed{(1,2,6)} \sim (2,2,5)$
⑨ $\boxed{(1,4,4)} \sim (2,3,4)$

and the total number of similarity classes in $\mathbb{F}_2^7$ is 9.

6.5. Enumeration for the similarity classes.

In this subsection, we give some enumerative results for the similarity classes of residue 2 in $\mathbb{F}_2^n$.

For $n \geq 3$, let α_n be the number of similarity classes listed in Theorem 6.33 (1), (2), (3) and (4) for $n \in 2\mathbb{Z}$ and Theorem 6.34 (1), (2), (3) and (4) for $n \in 2\mathbb{Z}+1$. Also, for $n \geq 3$, let β_n be the number of similarity classes listed in Theorem 6.33 (5) and (6) for $n \in 2\mathbb{Z}$ and Theorem 6.34 (5) and (6) for $n \in 2\mathbb{Z}+1$. Thus $\mathcal{S}_2(n) = \alpha_n + \beta_n$ for $n \geq 3$ is the number of the similarity classes of residue 2 in $\mathbb{F}_2^n$. We can easily see that $\alpha_3 = 0$, $\alpha_4 = 1$, $\alpha_5 = 2$, $\alpha_6 = 3$, $\alpha_7 = 4$, $\alpha_8 = 6$, $\alpha_9 = 8$, $\alpha_{10} = 10, \ldots$, and $\beta_3 = 1$, $\beta_4 = 1$, $\beta_5 = 2$, $\beta_6 = 3$, $\beta_7 = 5$, $\beta_8 = 6$, $\beta_9 = 9$, $\beta_{10} = 11, \ldots$, and hence $\{\mathcal{S}_2(n)\}_{n\geq 3} = 1, 2, 4, 6, 9, 12, 17, 21, \ldots$.

6.5.1. The formula for α_n.

Lemma 6.36. *We have*
(1) $\alpha_{8k} - \alpha_{8k-1} = 2k$ *for* $k \geq 1$;
(2) $\alpha_{8k+1} - \alpha_{8k} = 2k$ *for* $k \geq 1$;
(3) $\alpha_{8k+2} - \alpha_{8k+1} = 2k$ *for* $k \geq 1$;
(4) $\alpha_{8k+3} - \alpha_{8k+2} = 2k$ *for* $k \geq 1$;
(5) $\alpha_{8k+4} - \alpha_{8k+3} = 2k+1$ *for* $k \geq 0$;
(6) $\alpha_{8k+5} - \alpha_{8k+4} = 2k+1$ *for* $k \geq 0$;
(7) $\alpha_{8k+6} - \alpha_{8k+5} = 2k+1$ *for* $k \geq 0$;
(8) $\alpha_{8k+7} - \alpha_{8k+6} = 2k+1$ *for* $k \geq 0$.

Proof. We only prove (1), and the other cases can be proved similarly. From (1), (2), (3) and (4) of Theorem 6.33, we have $\alpha_{8k} - \alpha_{8k-1}$
$= \sharp\{\{2p+1, 2q+1\}_n \mid 2p+2q+2 = 8k+2\}$
$+\sharp\{\{4p, 4q+1\}_n \mid 4p+4q+1 = 8k+2\}$
$+\sharp\{\{4p, 4q+3\}_n \mid p \leq q+1,\ 4p+4q+3 = 8k+2\}$
$+\sharp\{\{4p+2, 4q+1\}_n \mid p \leq q, 4p+4q+3 = 8k+2\}$, but the last three terms are zero. Thus we get

$$\begin{aligned}\alpha_{8k} - \alpha_{8k-1} &= \sharp\{\{2p+1, 2q+1\}_n \mid 2p+2q = 8k\}\\ &= \sharp\{\{3, 8k-1\}_n, \{5, 8k-3\}_n, \ldots, \{4k-1, 4k+3\}_n, \{4k+1, 4k+1\}_n\}\\ &= 2k.\end{aligned}$$

□

Lemma 6.37. *We have*
(a) $\alpha_{4k} - \alpha_{4k-1} = k$ *for* $k \geq 1$;
(b) $\alpha_{4k+1} - \alpha_{4k} = k$ *for* $k \geq 1$;
(c) $\alpha_{4k+2} - \alpha_{4k+1} = k$ *for* $k \geq 1$;
(d) $\alpha_{4k+3} - \alpha_{4k+2} = k$ *for* $k \geq 1$.

Proof. (a) follows from (1) and (5) in Lemma 6.36, (b) follows from (2) and (6) in Lemma 6.36, (c) follows from (3) and (7) in Lemma 6.36, and (d) follows from (4) and (8) in Lemma 6.36. □

Lemma 6.38. *We have*
(i) $\alpha_{4k} = k(2k-1)$ *for* $k \geq 1$;
(ii) $\alpha_{4k+1} = 2k^2$ *for* $k \geq 1$;
(iii) $\alpha_{4k+2} = k(2k+1)$ *for* $k \geq 1$;
(iv) $\alpha_{4k+3} = 2k(k+1)$ *for* $k \geq 0$.

Proof. We show (iv) by induction on k. It is true for $k = 0$ since we know $\alpha_3 = 0$. Assume that $\alpha_{4k-1} = 2k(k-1)$. By Lemma 6.37(a), we have $\alpha_{4k} = k + \alpha_{4k-1} = k(2k-1)$, which is (i). Then, by Lemma 6.37(b), we have $\alpha_{4k+1} = k + \alpha_{4k} = 2k^2$, which is (ii). Then, by Lemma 6.37(c), we have $\alpha_{4k+2} = k + \alpha_{4k+1} = k(2k+1)$, which is (iii). Finally, by Lemma 6.37(d), we have $\alpha_{4k+3} = k + \alpha_{4k+2} = 2k(k+1)$, and hence (iv) is true by induction. Thus (i), (ii) and (iii) also hold, by Lemma 6.37. □

Using Lemma 6.38, we get the following formulas.

Proposition 6.39. *We have:*
(1) $\alpha_{2n+1} = 2\lfloor \frac{n}{2} \rfloor \lfloor \frac{n+1}{2} \rfloor$ *for* $n \geq 1$;
(2) $\alpha_{2n} = \frac{n(n-1)}{2}$ *for* $n \geq 2$.

Proof. For (1), we have $\alpha_{2(2k-2)+1} = \alpha_{4k-3} = 2(k-1)^2$ by Lemma 6.38(ii), and $2\lfloor \frac{2k-2}{2} \rfloor \lfloor \frac{2k-2+1}{2} \rfloor = 2(k-1)^2$. Also, we have $\alpha_{2(2k-1)+1} = \alpha_{4k-1} = 2k(k-1)$ by Lemma 6.38(iv), and $2\lfloor \frac{2k-1}{2} \rfloor \lfloor \frac{2k-1+1}{2} \rfloor = 2k(k-1)$.

For (2), we have $\alpha_{2\cdot 2k} = \alpha_{4k} = k(2k-1)$ by Lemma 6.38(i), and $\frac{2k(2k-1)}{2} = k(2k-1)$. Also, we have $\alpha_{2(2k+1)} = \alpha_{4k+2} = k(2k+1)$ by Lemma 6.38(iii), and $\frac{(2k+1)(2k+1-1)}{2} = k(2k+1)$. □

6.5.2. The formula for β_{2n}. We set

$$X_{2n} = \{\{2p+1, 2q+1, 2r\}_{2n} \mid 2r < 2p+1, 2q+1,\ p+q+r = n\},$$
$$Y_{2n} = \{\{2p, 2q, 2r\}_{2n} \mid p+q+r = n+1\},$$

where $p, q, r \in \mathbb{N}$. Then we have $\beta_{2n} - \beta_{2n-2} = \sharp X_{2n} + \sharp Y_{2n}$. We recall that $p(n, 3)$ denotes the number of partitions of n by three positive integers.

Lemma 6.40. *We have $\sharp X_{2n} = p(n, 3)$ and $\sharp Y_{2n} = p(n+1, 3)$.*

Proof. Let $X' = \{\{a, b, c\} \mid a, b, c \geq 1,\ a+b+c = n\}$ be the set of partitions of n by three positive integers. We define a map $\Phi : X_{2n} \longrightarrow X'$ as follows. For $\{x, y, z\}_{2n} \in X_{2n}$ with $z = \min\{x, y, z\}$, we define $\Phi(\{x, y, z\}_{2n}) = \{\frac{x-1}{2}, \frac{y-1}{2}, \frac{z}{2}\}$. Also, we define a map $\Psi : X' \longrightarrow X_{2n}$ as follows. For $\{a, b, c\} \in X'$ with $a, b \geq c$, we define $\Psi(\{a, b, c\}) = \{2a+1, 2b+1, 2c\}_{2n}$. Then Ψ is the inverse of Φ. Hence we get $\sharp X_{2n} = p(n, 3)$.

Let $Y' = \{\{a, b, c\} \mid a, b, c \geq 1,\ a+b+c = n+1\}$ be the set of partitions of $n+1$ by three positive integers. We define a map $f : Y_{2n} \longrightarrow Y'$ by $f(\{2x, 2y, 2z\}_{2n}) = \{x, y, z\}$. Also, we define a map $g : Y' \longrightarrow Y_{2n}$ by $g(\{a, b, c\}) = \{2a, 2b, 2c\}_{2n}$. Then g is the inverse of f. Hence we get $\sharp Y_{2n} = p(n+1, 3)$. □

Proposition 6.41. *We have $\beta_{2n} = 2\sum_{3\leq k\leq n} p(k, 3) + p(n+1, 3)$.*

Proof. We have

$$\begin{aligned}
\beta_4 &= 1 = p(3,3); \\
\beta_6 - \beta_4 &= p(3,3) + p(4,3), \\
\beta_8 - \beta_6 &= p(4,3) + p(5,3), \\
&\vdots \\
\beta_{2n} - \beta_{2n-2} &= p(n,3) + p(n+1,3),
\end{aligned}$$

and hence we see $\beta_{2n} = 2\sum_{3\leq k\leq n} p(k, 3) + p(n+1, 3)$. □

6.5.3. The formula for β_{2n+1}. We set

$$Z_{2n+1} = \{\{2p, 2q, 2r-1\}_{2n+1} \mid 2r-1 < 2p, 2q,\ p+q+r = n+2\},$$
$$W_{2n+1} = \{\{2p+1, 2q+1, 2r+1\}_{2n+1} \mid p+q+r = n\},$$

where $p, q, r \in \mathbb{N}$. Then we have $\beta_{2n+1} - \beta_{2n-1} = \sharp Z_{2n+1} + \sharp W_{2n+1}$, and similar methods as in Lemma 6.40 yield the following.

Lemma 6.42. *We have $\sharp Z_{2n+1} = p(n+2, 3)$ and $\sharp W_{2n+1} = p(n, 3)$.*

Moreover:

Proposition 6.43. *We have $\beta_{2n+1} = 2\sum_{3\leq k\leq n} p(n, 3) + p(n+1, 3) + p(n+2, 3)$.*

Proof. We have

$$\begin{aligned}
\beta_3 &= 1 = p(3,3); \\
\beta_5 - \beta_3 &= p(4,3) + p(2,3) = p(4,3),
\end{aligned}$$

$$\begin{aligned}\beta_7 - \beta_5 &= p(5,3) + p(3,3),\\ \beta_9 - \beta_7 &= p(6,3) + p(4,3)\\ &\vdots\\ \beta_{2n+1} - \beta_{2n-1} &= p(n+2,3) + p(n+1,3),\end{aligned}$$

and hence we obtain the result. □

6.5.4. Enumeration for the similarity classes. Combining Proposition 6.39, Proposition 6.41 and Proposition 6.43, we obtain the following results.

Theorem 6.44. (1) *For $n \geq 2$, the number of similarity classes of residue* 2 *in* $\mathbb{F}_2^{2n}$ *is*

$$\mathcal{S}_2(2n) = \frac{n(n-1)}{2} + 2\sum_{3 \leq k \leq n} p(k,3) + p(n+1,3).$$

(2) *For $n \geq 1$, the number of similarity classes of residue* 2 *in* $\mathbb{F}_2^{2n+1}$ *is*

$$\mathcal{S}_2(2n+1) = 2\lfloor\frac{n}{2}\rfloor\lfloor\frac{n+1}{2}\rfloor + 2\sum_{3 \leq k \leq n} p(k,3) + p(n+1,3) + p(n+2,3).$$

Thus we have the sequence $\mathcal{S}_2(n)$ by this Theorem:

n	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	$\cdots$
$\mathcal{S}_2(n)$	1	2	4	6	9	12	17	21	27	33	41	48	58	67	79	90	$\cdots$

We note that this sequence is not in the site OEIS.

[Open Problem] Classify isomorphism classes and similarity classes of residue ≥ 3 in $\mathbb{F}_2^n$, and find the numbers $\mathcal{I}_i(n)$ and $\mathcal{S}_i(n)$ for $i \geq 3$.

Remark 6.45. As it was explained in Section 2, our results concerning the classification of PRS up to similarity, leads to the classification of extended affine root systems of reduced types whose involved pointed reflection spaces (semilattices) have residue ≤ 2, plus some subclasses of non-reduced types. This includes a large class of extended affine root systems of nullity n. The results also provide important invariants for extended affine Lie algebras whose root systems are of the types mentioned above.

References

[1] B. Allison, S. Azam, S. Berman, Y. Gao and A. Pianzola: *Extended affine Lie algebras and their root systems*, Mem. Amer. Math. Soc. **126** (1997), no. 603.

[2] S. Azam: *Extended affine root systems*. J. Lie Theory **12** (2002), 515–527.

[3] S. Azam: *Nonreduced extended affine root systems of nullity* 3, Comm. Algebra **25** (1997), 3617–3654.

[4] S. Azam, Y. Khalili and M. Yousofzadeh: *Extended affine root systems of type BC*, J. Lie Theory **15** (2005), 145–181.

[5] S. Azam and V. Shahsanaei: *Extended affine Weyl groups of type A_1*, J. Algebraic Combin. **28** (2008), 481–493.

[6] S. Azam, M.B. Soltani, M. Tomie and Y. Yoshii: *A graph-theoretical classification for reflectable bases*, Publ. Res. Inst. Math. Sci. **55** (2019), 689–736.

[7] S. Azam, H. Yamane and M. Yousofzadeh: *Reflectable bases for affine reflection systems*, J. Algebra **371** (2012), 63–93.

[8] O. Loos: Symmetric spaces, I: General theory, Benjamin Inc. New York, 1969.

[9] O. Loos and E. Neher: *Locally finite root systems*, Mem. Amer. Math. Soc. **171** (2004), no. 811.

[10] O. Loos and E. Neher: *Reflections systems and partial root systems*, Forum Math **23** (2011), 349–411.

[11] J. Morita and Y. Yoshii: *Locally extended affine Lie algebras*, J. Algebra **301** (2006), 59–81.

[12] J. Morita and Y. Yoshii: *Locally loop algebras and locally affine Lie algebras*, J. Algebra **440** (2015), 379–442.

[13] E. Neher: *Extended affine Lie algebras and other generalizations of affine Lie algebras- a survey*; in Developments and Trends in Infinite-Dimensional Lie Theory, Prog. Math. **288**, Birkhäuser Boston, Inc., Boston, MA, 2011, 53–126.

[14] J. Oxley: Matroid Theory, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1992.

[15] S. Saito: *Extended affine root systems I (Coxeter transformations)*, Publ. Rre Inst. Math. Sci. **21** (1985), 75–179.

[16] Y. Yoshii: *Locally extended affine root systems*; in Quantum Affine Algebras, Extended Affine Lie Algebras and Applications, Contemp. Math. **506** (2010), 285–302.

[17] Y. Yoshii: *New Lie tori from Naoi tori*, Toyama Math. J. **37** (2015), 155–187.

Saeid Azam
Department of Mathematics, University of Isfahan
Isfahan, Iran, P.O.Box: 81745–163
and
School of Mathematics
Institute for Research in Fundamental Sciences
P.O.Box: 19395–5746, Tehran
Iran
e-mail: azam@ipm.ir

Masaya Tomie
Morioka University
Takizawa, Iwate, 020–0694
Japan
e-mail: tomie@morioka-u.ac.jp

Yoji Yoshii
Faculty of Education, Iwate University
3–18–33 Ueda
Morioka, Iwate, 020–8550
Japan
e-mail: yoshii@iwate-u.ac.jp