Mutually Disjoint 5-designs from Pless Symmetry Codes

Masayuki Angata
Denso Corporation
Kariya, Aichi 448-8661, Japan
MASAYUKI_ANGATA@denso.co.jp

and

Keisuke Shiromoto
Department of Mathematics and Engineering
Kumamoto University
2-39-1, Kurokami, Kumamoto 860-8555, Japan
keisuke@kumamoto-u.ac.jp

Abstract

Pless (1972) defines symmetry codes over the field of three elements, called the Pless symmetry codes, and shows that some of these codes yield 5-designs. In this paper, we generalize the construction of mutually disjoint Steiner systems studied in Jimbo and Shiromoto (2009) to 5-designs related to a certain class of Pless symmetry codes. As a consequence, we derive new simple 5-designs from the construction.

AMS Subject Classification: 05B05 and 94B05

Keywords: Pless symmetry code, simple 5-design, self-dual code

1 Introduction

One of the main problems in combinatorial design theory is to construct designs with given parameters. Many designs have been constructed from the supports of codewords of certain weight in linear codes (cf. Colbourn and Dinitz (2007, Chapter VII.1), and Huffman and Pless (2003)). The problem of finding the codes which construct t-designs have been studied. Pless (1972) defined a kind of ternary symmetry codes and proved that these codes are self-dual and many 5-designs are constructed from them.

Let V be a set of v elements and let t, k be integers with $0 < t < k < v$. For a collection $\mathcal{B}$ of k element subsets (called, *blocks*) of V, $(V, \mathcal{B})$ is called a t-(v, k, λ) *design* if $|\{B \in \mathcal{B} \,:\, T \subset B\}| = \lambda$ for all t element subsets T of V. In particular, a t-$(v, k, 1)$ design is called a *Steiner system* $S(t, k, v)$. If a t-(v, k, λ) design has no repeated blocks, then the design is said to be *simple*. All designs studied in this paper are simple.

Two t-(v, k, λ) designs $(V, \mathcal{B}^{(i)})$ and $(V, \mathcal{B}^{(j)})$ are said to be *disjoint* if they have no blocks in common. The t-(v, k, λ) designs $(V, \mathcal{B}^{(1)}), \ldots, (V, \mathcal{B}^{(m)})$ are *mutually disjoint* if any two distinct designs are disjoint. It was shown in Beth, et al. (2003) that mutually disjoint t-designs can construct t-spontaneous emission error designs (SEEDs) related to quantum jump codes. Also mutually disjoint t-designs can construct simple t-designs by taking the union of block sets (cf. Jimbo and Shiromoto (2009)).

In Kramer and Magliveras (1974) and Araya (2003), the authors gave a computational construction of mutually disjoint Steiner systems $S(5, 8, 24)$ by finding permutations on 24 points such that all images of a Steiner system $S(5, 8, 24)$ under these permutations are mutually disjoint. A theoretical construction of mutually disjoint Steiner systems $S(5, 8, 24)$ and 5-$(48, 12, 8)$ designs related to binary self-dual codes were presented in Jimbo and Shiromoto (2009).

The main purpose of this paper is to show the following results by generalizing the construction methods in Jimbo and Shiromoto (2009) to 5-designs related to the Pless symmetry codes.

Theorem 1.1 *There exist at least*

(1) 34 *mutually disjoint* 5-$(36, k, \lambda)$ *designs, for each* $(k, \lambda) = (12, 45), (15, 5577)$, *and*

(2) 58 *mutually disjoint* 5-$(60, k, \lambda)$ *designs, for each* $(k, \lambda) = (18, 3060), (21, 449820), (24, 34337160), (27, 1271766600)$.

Theorem 1.2 *There exist at least*

(1) 11 *mutually disjoint* 5-$(24, 9, 6)$ *designs, and*

(2) 23 *mutually disjoint* 5-$(48, k, \lambda)$ *designs, for each* $(k, \lambda) = (15, 364), (18, 50456), (21, 2957388)$.

In Section 2, we shall define some terminology and state some known results for later use. In Section 3, we study coordinate permutations on the codewords for Pless symmetry codes and the intersections among their images of the codes under these permutations (Propositions 3.1–3.3). We apply them to some of Pless symmetry codes which form 5-designs and demonstrate the above theorems in Section 4. The obtained simple 5-designs from the previous results are summarized in Table 4.1.

2 Preliminaries

Let $\mathbb{F}_3$ be the finite field of 3 elements. An (linear) $[n, r]$ code C is an r-dimensional subspace of the vector space $\mathbb{F}_3^n$. For any vector $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_3^n$, we define the *support* and (Hamming) *weight* of $\boldsymbol{x}$ as follows:

$$\begin{aligned} \mathrm{supp}(\boldsymbol{x}) &= \{i \ : \ x_i \neq 0\}, \\ \mathrm{wt}(\boldsymbol{x}) &= |\mathrm{supp}(\boldsymbol{x})| = |\{i \ : \ x_i \neq 0\}| \end{aligned}$$

The *minimum* (Hamming) *weight* of a linear code C is defined by

$$d = \min\{\mathrm{wt}(\boldsymbol{x}) \ : \ \boldsymbol{0} \neq \boldsymbol{x} \in C\}.$$

For any vectors $\boldsymbol{x} = (x_1, \ldots, x_n), \boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{F}_3^n$, the *inner product* between $\boldsymbol{x}$ and $\boldsymbol{y}$ is defined by $(\boldsymbol{x}, \boldsymbol{y}) = x_1y_1 + \cdots + x_ny_n$. The *dual code* of a linear code C is the linear code defined by $C^\perp = \{\boldsymbol{y} \in \mathbb{F}_3^n \ : \ (\boldsymbol{x}, \boldsymbol{y}) = 0, \text{ for all } \boldsymbol{x} \in C\}$. A linear code is said to be *self-dual* if $C = C^\perp$. A *generator matrix* G of a linear code C is a matrix whose rows are a basis for C. And a *parity-check matrix* H of C is a generator matrix of $C^\perp$. If C is a self-dual code, then G is also a parity-check matrix of C and so $G\boldsymbol{x}^T = \boldsymbol{0}$ for any codeword $\boldsymbol{x} \in C$.

Throughout the remaining part of this paper, let p be an odd prime such that $p \equiv 2 \pmod 3$. We define $Q = (q_{ij})$, $i, j = 0, 1, \ldots, p-1$, to be the $p \times p$ matrix such that $q_{ij} = \chi(j - i)$, where $\chi(0) = 0$, $\chi(\text{a square modulo } p) = 1$ and $\chi(\text{a non-square modulo } p) = -1$. Note that Q is a circulant matrix over $\mathbb{F}_3$. The following facts are shown in Hall (1967).

Lemma 2.1 *Let* Q *be the matrix over* $\mathbb{F}_3$ *defined above. Then*

(a) Q *is symmetric if* $p \equiv 1 \pmod 4$ *and is skew-symmetric if* $p \equiv 3 \pmod 4$, *and*

(b) $QQ^T = pI_p - J_p$, *where* I_p *is the* $p \times p$ *identity matrix and* J_p *is the* $p \times p$ *all-one matrix.*

Let $C(p)$ be the $[2p + 2, p + 1]$ code over $\mathbb{F}_3$ having generator matrix

$$H_p = \begin{pmatrix} & 0 & 1 & \ldots & 1 \\ & \chi(-1) & & & \\ & \vdots & & & \\ I_{p+1} & \vdots & & Q & \\ & \vdots & & & \\ & \chi(-1) & & & \end{pmatrix}.$$

The code $C(p)$ is introduced by Pless (1972), and is called the *Pless symmetry code*. Since $C(p)$ is a self-dual code, H_p is also a parity-check matrix of $C(p)$. In Pless (1972), it is shown that, for each $p = 5, 11, 17, 23, 29$, the supports of codewords of certain weight w in $C(p)$ form simple 5-$(2p+2, w, \lambda)$ designs as indicated in Table 4.1.

3 General results

Throughout this paper, permutations on a set $\{1, 2, \ldots, n\}$ are considered as coordinate permutations which act on a vector space $\mathbb{F}_3^n$. Let $\sigma = (p+3, p+4, \ldots, 2p+2)$ and $\tau = (2, p+3)(3, p+4)\cdots(p+1, 2p+2)$ be the permutations on a set $\{1, 2, \ldots, 2p+2\}$. We denote by P the permutation matrix corresponding to the cyclic permutation $(1, 2, \ldots, p)$ on a set $\{1, 2, \ldots, p\}$. We shall study the intersection between the images of $C(p)$ under all permutations of the form $\tau^i\sigma^j$.

We examine the following three cases individually.

Proposition 3.1 *For any $i, j \in \{0, 1, \ldots, p-1\}$, $i \neq j$, the dimension of $C(p)^{\sigma^i} \cap C(p)^{\sigma^j}$ is 2 if and only if the rank of the matrix $\begin{pmatrix} 2QP^i + QP^j \\ 1 \cdots 1 \end{pmatrix}$ is p*

Proof. $C(p)$ is a self-dual code whose parity-check matrix is H_p. Then $C(p)^{\sigma^i}$ is also a self-dual code with parity-check matrix $H_p^{\sigma^i}$. Therefore,

$$\dim(C(p)^{\sigma^i})^\perp \cap (C(p)^{\sigma^j})^\perp = \dim C(p)^{\sigma^i} \cap C(p)^{\sigma^j} = 2$$

if and only if the rank of the $(2p+2) \times (2p+2)$ matrix

$$\begin{pmatrix} H_p^{\sigma^i} \\ H_p^{\sigma^j} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 & 1 & \ldots & 1 \\ 0 & & & & \chi(-1) & & & \\ \vdots & & I_p & & \vdots & & QP^i & \\ 0 & & & & \chi(-1) & & & \\ 1 & 0 & \ldots & 0 & 0 & 1 & \ldots & 1 \\ 0 & & & & \chi(-1) & & & \\ \vdots & & I_p & & \vdots & & QP^j & \\ 0 & & & & \chi(-1) & & & \end{pmatrix} \tag{3.1}$$

is $2p$.

Permuting in rows and columns of the matrix (3.1) yields the following matrix:

$$\begin{pmatrix} & I_p & & & QP^i & & 0 & \chi(-1) \\ & & & & & & \vdots & \vdots \\ & I_p & & & QP^j & & 0 & \chi(-1) \\ 0 & \cdots & 0 & 1 & \cdots & 1 & 1 & 0 \\ 0 & \cdots & 0 & 1 & \cdots & 1 & 1 & 0 \end{pmatrix}. \tag{3.2}$$

Then the matrix (3.3) is obtained from (3.2) by subtracting the $(2p+1)$-st row from the $(2p+2)$-nd, adding $2\chi(-1)$ times the first, second, …, pth columns to the $(2p+2)$-nd column, and adding the $(p+1)$-st, …, $2p$th columns to the $(2p+1)$-st column, since $\sum_{i=0}^{p-1} \chi(i) = 0$ (cf. Hall (1967, p. 209)) and $p+1 \equiv 0 \pmod 3$:

$$\begin{pmatrix} & I_p & & & QP^i & & 0 & 0 \\ & & & & & & \vdots & \vdots \\ & I_p & & & QP^j & & 0 & 0 \\ 0 & \cdots & 0 & 1 & \cdots & 1 & 0 & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}. \tag{3.3}$$

For each l $(1 \le l \le p)$, adding 2 times both of the lth and the $(2p+1)$-st rows to the $(l+p)$-th row gives the matrix (3.4):

$$\begin{pmatrix} & I_p & & & QP^i & & 0 & 0 \\ & & & & & & \vdots & \vdots \\ & O & & & 2QP^i + QP^j + J_p & & 0 & 0 \\ 0 & \cdots & 0 & 1 & \cdots & 1 & 0 & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}. \tag{3.4}$$

Thus it holds that

$$\operatorname{rank} \begin{pmatrix} H_p^{\sigma^i} \\ H_p^{\sigma^j} \end{pmatrix} = \operatorname{rank} \begin{pmatrix} I_p & QP^i \\ O & 2QP^i + QP^j + J_p \end{pmatrix} = 2p$$

if and only if

$$\operatorname{rank} \begin{pmatrix} 2QP^i + QP^j \\ 1 \cdots 1 \end{pmatrix} = p.$$

□

Proposition 3.2 *For any $i, j \in \{0, 1, \ldots, p-1\}$, $i \neq j$, the dimension of $C(p)^{\tau\sigma^i} \cap C(p)^{\tau\sigma^j}$ is equal to that of $C(p)^{\sigma^{-i}} \cap C(p)^{\sigma^{-j}}$.*

Proof. We easily have the following after some row permutations to the matrix $H_p^{\tau\sigma^l}$:

$$\begin{pmatrix} 1 & 1 & \ldots & 1 & 0 & 0 & \ldots & 0 \\ 0 & & & & \chi(-1) & & & \\ \vdots & & QP^{-l} & & \vdots & & I_p & \\ 0 & & & & \chi(-1) & & & \end{pmatrix},$$

because P commutes with Q so that $P^{-l}Q = QP^{-l}$. This implies $C(p)^{\tau\sigma^l} = C(p)^{\sigma^{-l}\tau}$, and hence

$$\begin{aligned} C(p)^{\tau\sigma^i} \cap C(p)^{\tau\sigma^j} &= C(p)^{\sigma^{-i}\tau} \cap C(p)^{\sigma^{-j}\tau} \\ &= (C(p)^{\sigma^{-i}} \cap C(p)^{\sigma^{-j}})^{\tau} \end{aligned}$$

□

Proposition 3.3 *For any $i, j \in \{0, 1, \ldots, p-1\}$, the dimension of $C(p)^{\sigma^i} \cap C(p)^{\tau\sigma^j}$ is 1 if and only if the rank of the matrix $I_p P^{j-i} - Q^2$ is p.*

Proof. It is sufficient to prove the rank of the matrix

$$\begin{pmatrix} H_p^{\sigma^i} \\ H_p^{\tau\sigma^j} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 & 1 & \ldots & 1 \\ 0 & & & & \chi(-1) & & & \\ \vdots & & I_p & & \vdots & & QP^i & \\ 0 & & & & \chi(-1) & & & \\ 1 & 1 & \ldots & 1 & 0 & 0 & \ldots & 0 \\ 0 & & & & \chi(-1) & & & \\ \vdots & & Q & & \vdots & & I_p P^j & \\ 0 & & & & \chi(-1) & & & \end{pmatrix}$$

is equal to that of the matrix of $\begin{pmatrix} I_p & Q \\ Q & I_p P^{j-i} \end{pmatrix}$.

Applying the permutation σ^{-i} on the above matrix and the row and column cyclic-sifts, one obtains

$$\begin{pmatrix} & I_p & & & Q & & 0 & \chi(-1) \\ & & & & & & \vdots & \vdots \\ & Q & & & I_pP^{j-i} & & 0 & \chi(-1) \\ 0 & \cdots & 0 & 1 & \cdots & 1 & 1 & 0 \\ 1 & \cdots & 1 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}. \tag{3.5}$$

We add 2 times the first, ..., $(2p+1)$-st rows to the $(2p+2)$-nd row and add $2\chi(-1)$ times the first, ..., $(2p+1)$-st columns to the $(2p+2)$-nd column in the matrix (3.5). Then we have

$$\begin{pmatrix} & I_p & & & Q & & 0 & 0 \\ & & & & & & \vdots & \vdots \\ & Q & & & I_pP^{j-i} & & 0 & 0 \\ 0 & \cdots & 0 & 1 & \cdots & 1 & 1 & 0 \\ 0 & \cdots & 0 & 1 & \cdots & 1 & 0 & 0 \end{pmatrix},$$

because of $\overbrace{2\chi(-1)+\cdots+2\chi(-1)}^{2p} \equiv 2\chi(-1) \pmod 3$ and $\overbrace{2\chi(-1)+\cdots+2\chi(-1)}^{p+1} \equiv 0 \pmod 3$.

Adding the $(p+1)$-st, ..., $2p$th rows to the $(2p+2)$-nd row gives the following matrix:

$$\begin{pmatrix} & I_p & & & Q & & 0 & 0 \\ & & & & & & \vdots & \vdots \\ & Q & & & I_pP^{j-i} & & 0 & 0 \\ 0 & \cdots & 0 & 1 & \cdots & 1 & 1 & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}.$$

□

4 Special cases

In this section, we prove Theorems 1.1 and 1.2 by using previous results. The following lemma is well known and is essential (see, for instance, MacWilliams and Sloane (1978, Chapter 16)).

Lemma 4.1 *Let X be a circulant matrix with the first row $(c_0, c_1, \ldots, c_{n-1})$ over a finite field. X is invertible if and only if $c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ is relatively prime to $x^n - 1$.*

Set $f_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$.

4.1 Proof of Theorem 1.1

Proposition 4.2 *If p is a odd prime such that $p \equiv 1 \pmod 4$ and 3 is a primitive root of 1 modulo p, then*

(1) *the intersection of $C(p)^{\sigma^i}$ and $C(p)^{\sigma^j}$ is generated by $\mathbf{1}_2$ and $\boldsymbol{x}$, for any $i, j \in \{0, 1, \ldots, p-1\}$, $i \neq j$,*

(2) *the intersection of $C(p)^{\tau\sigma^i}$ and $C(p)^{\tau\sigma^j}$ is generated by $\mathbf{1}_2$ and $\boldsymbol{y}$, for any $i, j \in \{0, 1, \ldots, p-1\}$, $i \neq j$, and*

(3) *the intersection of $C(p)^{\sigma^i}$ and $C(p)^{\tau\sigma^j}$ is generated by $\mathbf{1}_2$, for any $i, j \in \{0, 1, \ldots, p-1\}$,*

where $\mathbf{1}_2 = (1, \ldots, 1, \overset{p+2}{2}, 1, \ldots, 1)$, $\boldsymbol{x}$ is the vector $(1, 0, \ldots, 0, 1, \ldots, 1)$ of weight $p+1$, and $\boldsymbol{y}$ is the vector $(1, 1, \ldots, 1, 0, \ldots, 0)$ of weight $p+1$.

Proof. (1) We easily find that $\mathbf{1}_2^{\sigma^i} = \mathbf{1}_2^{\sigma^j} = \mathbf{1}_2$, $\boldsymbol{x}^{\sigma^i} = \boldsymbol{x}^{\sigma^j} = \boldsymbol{x}$, and so $\alpha\mathbf{1}_2 + \beta\boldsymbol{x} \in C(p)^{\sigma^i} \cap C(p)^{\sigma^j}$, for any $\alpha, \beta \in \mathbb{F}_3$. Therefore, from Proposition 3.1, it remains to show that the matrix $2QP^i + QP^j + J_p$ is invertible.

Without loss of generality, we assume that $i < j$. Let $g(x)$ be the polynomial corresponding to the first row of $2QP^i + QP^j + J_p$. Then the coefficients of x^i and x^j in $g(x)$ are as follows, respectively:

$$\chi(p-j+i)+1 = \chi(-j+i)+1 = \chi(-1)\chi(j-i)+1$$

and

$$2\chi(p-i+j)+1 = 2\chi(-i+j)+1 = 2\chi(j-i)+1.$$

Both of them are always different with each other, since $p \equiv 1 \pmod 4$ and so $\chi(-1) = 1$. As 3 is a primitive root of 1 modulo p so that $f_p(x)$ is irreducible, $g(x)$ is relatively prime to $f_p(x)$. And we have that $g(1) = p \equiv 2 \pmod 3 \neq 0$. Therefore the matrix $2QP^i + QP^j + J_p$ is invertible from Lemma 4.1.

(2) From Proposition 3.2 and part (1), $C(p)^{\tau\sigma^i} \cap C(p)^{\tau\sigma^j}$ is generated by $\mathbf{1}_2^\tau = \mathbf{1}_2$ and $\boldsymbol{x}^\tau = \boldsymbol{y}$.

(3) Since $p \equiv 2 \pmod 3$ and $p \equiv 1 \pmod 4$, it follows that $I_pP^{j-i} - Q^2 = I_pP^{j-i} - QQ^T \equiv I_pP^{j-i} - 2I_p + J_p \pmod 3$ from Lemma 2.1. Let $h(x)$ be the polynomial corresponding to the first row of $I_pP^{j-i} - Q^2$. Then

$$\begin{aligned} h(x) &= 2 + x + \cdots + x^{j-i-1} + 2x^{j-i} + x^{j-i+1} + \cdots + x^{p-1} \quad \text{if } i < j, \\ h(x) &= 2 + x + \cdots + x^{p+j-i-1} + 2x^{p+j-i} + x^{p+j-i+1} + \cdots + x^{p-1} \quad \text{if } i > j, \end{aligned}$$

and $h(x) = x + x^2 + \cdots + x^{p-1}$ if $i = j$. Therefore $h(x)$ is always relatively prime to $f_p(x)$, since $f_p(x)$ is irreducible and $f_p(x) \neq h(x)$. Part (3) follows from Lemma 4.1 and Proposition 3.3. □

By summarizing the previous results, we have the following:

Theorem 4.3 *Let p be a odd prime such that $p \equiv 2 \pmod 3$. Let $\sigma = (p+3, p+4, \ldots, 2p+2)$ and $\tau = (2, p+3)(3, p+4)\cdots(p+1, 2p+2)$ be the coordinate permutations on $\mathbb{F}_3^{2p+2}$ and let G_p be the set of all permutations of the form $\tau^i\sigma^j$ in the symmetric group S_{2p+2}. If $p \equiv 1 \pmod 4$ and 3 is a primitive root of 1 modulo p, then the minimum weight of $C(p)^a \cap C(p)^b$ is at least $p+1$ for any $a, b \in G_p$, $a \neq b$.*

Let $\mathcal{B}_p(w)$ be the set of supports of all codewords of Hamming weight w in $C(p)$.

Proof of Theorem 1.1: For $p = 17$ and 29, 3 is a primitive root of 1 modulo p, for instance, from Magma calculations in Cannon and Bosma (2008). From Theorem 4.3, there exists no codeword of Hamming weight less than $p+1$ in the intersection of $C(p)^a$ and $C(p)^b$, for any $a, b \in G_p$, $a \neq b$, and for each $p = 17, 29$. Therefore $\{\mathcal{B}_{17}(w)^g : g \in G_{17}\}$ forms a set of 34 mutually disjoint 5-$(36, w, \lambda)$ designs, for each $(w, \lambda) = (12, 45), (15, 5577)$ and $\{\mathcal{B}_{29}(w)^g : g \in G_{29}\}$ forms a set of 58 mutually disjoint 5-$(60, w, \lambda)$ designs, for each $(w, \lambda) = (18, 3060), (21, 449820), (24, 34337160), (27, 1271766600)$, where the values of λ when $p = 29$ are given in Colbourn and Dinitz (2007, p. 683). □

Remark 4.4 For $p = 5$, 3 is a primitive root of 1 modulo 5. However, both of the vectors $\boldsymbol{x} = (1,0,0,0,0,0,0,1,1,1,1,1)$ and $\boldsymbol{y} = (1,1,1,1,1,1,0,0,0,0,0,0)$ defined in Proposition 4.2 are codewords of minimum weight in $C(5)$, and so

$$\mathcal{B}_5(6)^a \cap \mathcal{B}_5(6)^b \neq \emptyset,$$

for any $a, b \in \{\sigma^i : i \in \mathbb{Z}\}$ or $a, b \in \{\tau\sigma^i : i \in \mathbb{Z}\}$. On the other hand, Proposition 4.2(3) maintains that

$$\mathcal{B}_5(6)^{\sigma^i} \cap \mathcal{B}_5(6)^{\tau\sigma^j} = \emptyset,$$

for any i, j, $i \neq j$. Therefore there exist at least two mutually disjoint 5-$(12, 6, 1)$ designs. A similar argument proves that there exist at least two mutually disjoint 5-$(36, w, \lambda)$ designs, for each $(w, \lambda) = (18, 209685), (21, 2438973)$, and 5-$(60, w, \lambda)$ designs, for each $(w, \lambda) = (30, 24140500956), (33, 239329029060)$.

For mutually disjoint t-(v, k, λ) designs $(V, \mathcal{B}^{(1)}), \ldots, (V, \mathcal{B}^{(l)})$ and a subset $K \subseteq \{1, \ldots, l\}$, the collection $\bigcup_{i \in K} \mathcal{B}^{(i)}$ can be viewed as a set of blocks in a simple t-$(v, k, \lambda|K|)$ design. Therefore the following results are straightforward from Theorem 1.1 and Remark 4.4.

Corollary 4.5 *There exist simple* 5-$(36, w, \lambda m)$ *designs, for all* $m = 1, 2, \ldots, 34$, *and simple* 5-$(60, w, \lambda m)$ *designs, for all* $m = 1, 2, \ldots, 58$, *where each* (w, λ) *is indicated in Table* 4.1.

Corollary 4.6 *There exist simple* 5-$(12, 6, m)$ *designs,* 5-$(36, w, \lambda m)$ *designs, and* 5-$(60, w, \lambda m)$ *designs, for all* $m = 1, 2$, *where each* (w, λ) *is indicated in Table* 4.1.

4.2 Proof of Theorem 1.2

We first prove the following result on the codes $C(p)$ for $p = 11$ and 23.

Proposition 4.7 *If* $p = 11$ *or* 23, *then the intersection of* $C(p)^{\sigma^i}$ *and* $C(p)^{\sigma^j}$ *is generated by* $\mathbf{1}_2$ *and* $\boldsymbol{x}$, *and the intersection of* $C(p)^{\sigma^i}$ *and* $C(p)^{\tau\sigma^j}$ *is generated by* $\mathbf{1}_2$, *for any* $i, j \in \{0, 1, \ldots, p-1\}$, $i \neq j$, *where* $\mathbf{1}_2$ *and* $\boldsymbol{x}$ *are the vectors defined in Proposition* 4.2.

Proof. By Lemma 2.1, $I_pP^{j-i} - Q^2 = I_pP^{j-i} + QQ^T \equiv I_pP^{j-i} + 2I_p - J_p \pmod 3$. We denote the polynomial corresponding to the first row of Q by $a_0(x)$. From the proofs of Proposition 4.2(1) and (3), it is sufficient to prove that both of the polynomials corresponding to the first rows of $2QP^i + QP^j$ and $I_pP^{j-i} + 2I_p$, for all i, j, $i < j$, are not divisible by all the factors of $f_p(x)$ for each $p = 11, 23$.
Case 1: $p = 11$. $f_{11}(x)$ has the irreducible factors $g(x) = x^5+2x^3+x^2+2x+2$ and $h(x) = x^5+x^4+2x^3+x^2+2$ over $\mathbb{F}_3$, for instance, from Magma calculations in Cannon and Bosma (2008). The polynomial $a_0(x)$ has the irreducible factorization $a_0(x) = x(x+1)^6(x+2)(x^2+1)$. Since the polynomials corresponding to the first rows of QP^i+QP^j and $I_pP^{j-i}+2I_p$ are $x^i(x^{j-i}+2)a_0(x) (\mathrm{mod} x^{11}-1)$ and $x^{j-i}+2$ respectively, we shall check that the polynomials $x^l + 2$, $l = 5, 6, \ldots, 10$ are not divisible by $g(x)$ or $h(x)$. Among all these polynomials, the polynomial which has irreducible factors of degree at least 5 is $x^7 + 2 = (x+2)(x^6 + x^5 + \cdots + 1)$. Thus Case 1 is complete.
Case 2: $p = 23$. $f_{23}(x)$ has the irreducible factors $g(x) = x^{11} + 2x^8 + 2x^6 + x^4 + x^3 + 2x^2 + 2x + 2$ and $h(x) = x^{11}+x^{10}+x^9+2x^8+2x^7+x^5+x^3+2$ over $\mathbb{F}_3$, for instance, from Magma calculations in Cannon and Bosma (2008). The polynomial $a_0(x)$ has no irreducible factor of degree at least 11. So we shall check that the polynomials $x^l + 2$, $l = 11, 12, \ldots, 22$ are not divisible by $g(x)$ or $h(x)$. Among all these polynomials, the polynomials which have irreducible factors of degree at least 11 are $x^{17}+2 = (x+2)(x^{16}+x^{15}+\cdots+1)$ and $x^{19} + 2 = (x + 2)(x^{18} + x^{17} + \cdots + 1)$. Thus Case 2 is complete. □

Theorem 1.2 immediately follows from the above proposition.

Corollary 4.8 *There exist simple* 5-$(24, 9, 6m)$ *designs, for all* $m = 1, 2, \ldots, 11$, *and simple* 5-$(48, w, \lambda m)$ *designs, for all* $m = 1, 2, \ldots, 23$, *where each* (w, λ) *is indicated in Table* 4.1.

Corollary 4.9 *There exist simple* 5-$(24, w, \lambda m)$ *designs and simple* 5-$(48, w, \lambda m)$ *designs, for all* $m = 1, 2$, *where each* (w, λ) *is indicated in Table* 4.1.

4.3 Summary

We summarize in Table 4.1 the obtained simple 5-designs from the sets of mutually disjoint 5-designs. According to Colbourn and Dinitz (2007, Table 4.46), 5-$(24, 9, 6m)$ $(m = 3, 4, 5)$, 5-$(36, 12, 45m)$, $(m = 2, 3, \ldots, 34)$, 5-$(36, 15, 5577m)$ $(m = 2, 3, \ldots, 34)$, 5-$(36, 18, 419370)$ designs are the first 5-designs with these parameters.

Acknowledgments

We gratefully thank Masakazu Jimbo for his helpful comments and suggestions. We would like to thank the anonymous referees for their good corrections and comments. This work was partially supported by KAKENHI (20740063 and 20654012) from MEXT.

Table 4.1: The obtained simple 5-designs

simple 5-$(2p+2, w, \lambda m)$ designs	m
$(12, 6, m)$	$m = 1, 2$
$(24, 9, 6m)$	$m = 1, 2, \ldots, 11$
$(24, 12, 576m)$	$m = 1, 2$
$(24, 15, 8580m)$	$m = 1, 2$
$(36, 12, 45m)$	$m = 1, 2, \ldots, 34$
$(36, 15, 5577m)$	$m = 1, 2, \ldots, 34$
$(36, 18, 209685m)$	$m = 1, 2$
$(36, 21, 2438973m)$	$m = 1, 2$
$(48, 15, 364m)$	$m = 1, 2, \ldots, 23$
$(48, 18, 50456m)$	$m = 1, 2, \ldots, 23$
$(48, 21, 2957388m)$	$m = 1, 2, \ldots, 23$
$(48, 24, 71307600m)$	$m = 1, 2$
$(48, 27, 749999640m)$	$m = 1, 2$
$(60, 18, 3060m)$	$m = 1, 2, \ldots, 58$
$(60, 21, 449820m)$	$m = 1, 2, \ldots, 58$
$(60, 24, 34337160m)$	$m = 1, 2, \ldots, 58$
$(60, 27, 1271766600m)$	$m = 1, 2, \ldots, 58$
$(60, 30, 24140500956m)$	$m = 1, 2$
$(60, 33, 239329029060m)$	$m = 1, 2$

References

Araya, M., 2003. More mutually disjoint Steiner systems $S(5, 8, 24)$, *Journal of Combinatorial Theory, Series A*, 102, 201–203.

Beth, T., Charnes, C., Grassl, M., Alber, G., Delgado, A., Mussinger, M., 2003. A new class of designs which protect against quantum jumps, *Designs, Codes and Cryptography*, 29, 51–70.

Colbourn, C.J., Dinitz, J.H., 2007. *Handbook of Combinatorial Designs*, Second Edition, CRC Press, Boca Raton.

Hall, M., 1967. *Combinatorial Theory*, Blaisdell, Waltham, Mass.

Huffman, W., Pless, V., 2003. *Fundamentals of Error-Correcting Codes*, Cambridge.

Jimbo, M., Shiromoto, K., 2009. A construction of mutually disjoint Steiner systems from isomorphic Golay codes, *Journal of Combinatorial Theory, Series A*, 116, 1245–1251.

Kramer, E.S., Magliveras, S.S., 1974. Some mutually disjoint Steiner systems, *Journal of Combinatorial Theory, Series A*, 17, 39–43.

MacWilliams, F.J., Sloane, N.J.A., 1978. *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, Amsterdam.

Cannon, J., Bosma, W. (Eds.), 2008. *Handbook of Magma Functions*, Version 2.15, University of Sydney.

Pless, V., 1972. Symmetry codes over $GF(3)$ and new five-designs, *Journal of Combinatorial Theory, Series A*, 12, 119–142.