広島大学学位請求論文

Point arrangements on some combinatorial objects

(いくつかの組合せ論的対象上の点配置について)

２０２２年

広島大学大学院理学研究科

数学専攻

梶浦　大起

目　次

主論文

Point arrangements on some combinatorial objects

Hiroki Kajiura

Organization of this thesis

The subject of this thesis is to study and give characterizations of the existence and non-existence of "good point arrangements" for sets with mathematical structures. In Chapter 1, we study 3-dimensional digital nets (in base 2), which are point arrangements on a cube $[0,1)^3$. In Chapter 2, we study pre-difference sets, which are point arrangements on a finite group.

We give an abstract for each chapter below:

Chapter 1. We study 3-dimensional digital nets over $\mathbb{F}_2$ generated by matrices (I, B, B^2) where I is the identity matrix and B is a square matrix. We give a characterization of B for which the t-value of the digital net is 0. As a corollary, we prove that such B satisfies $B^3 = I$.

Chapter 2. We gave a construction of a pre-difference set in $G = NA$ with A an abelian subgroup and N a subgroup satisfying $N \cap A = \{e\}$, from a difference set in $N \times A$. This gives a $(16, 6, 2)$ pre-difference set in D_{16} and a $(27, 13, 6)$ pre-difference set in $UT(3, 3)$, where no non-trivial difference sets exist. We also give a product construction of pre-difference sets similar to Kesava Menon construction, which provides infinite series of pre-difference sets that are not difference sets. We show some necessary conditions for the existence of a pre-difference set in a group with index 2 subgroup. For the proofs, we use a rather simple framework "relation partitions", which is obtained by dropping an axiom from association schemes. Most results are proved in that frame work.

Contents

Chapter 1

Characterization of matrices B such that (I, B, B^2) generates a digital net with t-value zero

1.1 Introduction and main result

Let $\mathbb{F}_2 = \{0, 1\}$ be the field of two elements, $m \geq 1$ be a positive integer, and $\mathbb{F}_2^{m\times m}$ be the set of $m \times m$ matrices over $\mathbb{F}_2$. For $C_1, \ldots, C_s \in \mathbb{F}_2^{m\times m}$, the digital net generated by $(C_1, \ldots, C_s)$ is a point set in $[0, 1)^s$ defined as follows. For $0 \leq l < 2^m$, we denote the 2-adic expansion of l by $l = \iota_0 + \iota_1 2 + \cdots + \iota_{m-1}2^{m-1}$ with $\iota_0, \ldots, \iota_{m-1} \in \mathbb{F}_2$. We define $\boldsymbol{y}_{l,j} \in \mathbb{F}_2^m$ for $1 \leq j \leq s$ as

$$\boldsymbol{y}_{l,j} := C_j(\iota_0, \ldots, \iota_{m-1})^\top \in \mathbb{F}_2^m.$$

Then we obtain the l-th point

$$\boldsymbol{x}_l := (\phi(\boldsymbol{y}_{l,1}), \ldots, \phi(\boldsymbol{y}_{l,s})) \tag{1.1}$$

where $\phi\colon \mathbb{F}_2^m \to [0, 1)$ is defined as

$$\phi((y_1, \ldots, y_m)^\top) := \frac{y_1}{2} + \frac{y_2}{2^2} + \cdots + \frac{y_m}{2^m}.$$

The digital net generated by $(C_1, \ldots, C_s)$ is the point set $\{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{2^m-1}\} \subset [0, 1)^s$. Digital nets are introduced by Niederreiter and have been widely used to generate point sets in Quasi-Monte Carlo (QMC) theory, see [16] for details.

A popular criterion of the uniformity of digital nets is the t-value. Let $m \geq 1$, $0 \leq t \leq m$, and $s \geq 1$ be integers. A point set $P = \{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{2^m-1}\} \subset [0,1)^s$ is called a (t, m, s)-net over $\mathbb{F}_2$ if, for all nonnegative integers $d_1, \ldots, d_s$ with $d_1 + \cdots + d_s = m - t$, the elementary intervals $\prod_{i=1}^{s} \left[a_i/2^{d_i}, (a_i+1)/2^{d_i}\right)$ contain exactly 2^t points for all choices of $0 \leq a_i < 2^{d_i}$ with $a_i \in \mathbb{Z}$ for $1 \leq i \leq s$. In this paper we study t-values of specific 3-dimensional digital nets over $\mathbb{F}_2$. Small value of t is preferable for QMC integration [16].

To state our main result, we introduce our notation. Let I_m be the $m \times m$ identity matrix. Let J_m be the $m \times m$ anti-diagonal matrix whose anti-diagonal entries are all 1, and P_m be the $m \times m$ upper-triangular Pascal matrix, i.e.,

$$J_m = \begin{pmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{pmatrix}, \qquad P_m = \left(\binom{j-1}{i-1}\right)_{i,j=1}^{m} = \begin{pmatrix} \binom{0}{0} & \binom{1}{0} & \cdots & \binom{m-1}{0} \\ & \binom{1}{1} & & \vdots \\ & & \ddots & \vdots \\ & & & \binom{m-1}{m-1} \end{pmatrix},$$

which are considered in modulo 2. If there is no confusion, we omit the subscripts and simply write as I, J, and P. Let $\mathcal{L}_m$ (resp. $\mathcal{U}_m$) be the set of $m \times m$ lower- (resp. upper-) triangular matrices over $\mathbb{F}_2$. Note that $\mathcal{L}_m \cap \mathcal{U}_m = \{I\}$ holds. For matrices $C_1, \ldots, C_s \in \mathbb{F}_2^{m \times m}$, $t(C_1, \ldots, C_s)$ denotes the t-value of the digital net generated by $(C_1, \ldots, C_s)$.

Now we are ready to state our main result.

Theorem 1.1.1. *Let $m \geq 1$ be an integer and $B \in \mathbb{F}_2^{m \times m}$. Then the following are equivalent.*

(i) $t(I, B, B^2) = 0$.

(ii) *There exists $L \in \mathcal{L}_m$ such that $B = LPJL^{-1}$.*

Moreover, if one of the above holds, then we have $B^3 = I$.

Note that for digital nets over $\mathbb{F}_2$, $t(C_1, \ldots, C_s) = 0$ is achievable if and only if $s \leq 3$ (see [16, Corollary 4.21] or [8]). Thus, the above theorem shows that this extreme $s = 3$ can be realized in the special form $t(I, B, B^2)$.

Background. Our original motivation is to find a periodic sequence for Markov Chain Quasi-Monte Carlo (MCQMC) method. Let us recall the rough idea. Let $x_1, x_2, \dots$ be a sequence of points in $[0,1)$. For an integer $s \geq 1$, we define

$$\bar{\boldsymbol{x}}_i^{(s)} = (x_i, x_{i+1}, \dots x_{i+s-1}) \in [0,1)^s, \tag{1.2}$$

where they are made up of overlapping consecutive s-tuples from the sequence. The sequence is said to be completely uniformly distributed (CUD) if $\bar{\boldsymbol{x}}_1^{(s)}, \bar{\boldsymbol{x}}_2^{(s)}, \dots$ is uniformly distributed in $[0,1)^s$ for all $s \geq 1$.

We do not explain on MCQMC method, but it is shown that CUD sequence can be used instead of uniformly i.i.d. uniform random numbers in $[0,1)$. Markov Chain Monte Carlo (MCMC) with the driving sequence being CUD is consistent to the original MCMC, see [2].

Constructions for CUD points given in [15] are not convenient to implement. Instead, it was suggested by Tribble [18] to use multiple congruential generators and linear feedback shift registers. Chen et. al. [3] considered a periodic sequence $x_1, x_2, \dots$ with period p, the s-dimensional point set

$$S_s := \{\bar{\boldsymbol{x}}_i^{(s)} = (x_i, x_{i+1}, \dots x_{i+s-1}) \in [0,1)^s \mid i = 1, \dots, p\} \tag{1.3}$$

whose cardinality is p as a multi set. It is expected to work well for MCQMC if S_s is hyperuniform for every s. Assume that $S_s \cup \{0\}$ is a $\mathbb{F}_2$-sub vector space (this condition is necessary to compute t-value in a practical time) of, say, dimension m. Here, each x_i is assumed to be identified with an element in $\mathbb{F}_2^m$ through ϕ. Let V be this vector space $S_s \cup \{0\}$. We further require that S_1 is a $(0, m, 1)$-net. Then, the projection to the first component $\mathrm{pr}_1 \colon V \to \mathbb{F}_2^m$ is linearly isomorphic. This implies that the second projection $\mathrm{pr}_2 \colon V \to \mathbb{F}_2^m$ is also isomorphic since the images of them are the same. Thus $\mathrm{pr}_2 \circ \mathrm{pr}_1^{-1}$ is also isomorphic. This means that there is a fixed $B \in \mathbb{F}_2^{m \times m}$ such that

$$x_{i+1} = Bx_i$$

holds for $i = 1, 2, \dots$. Moreover, since we have assumed that $S_s \cup \{0\}$ is a m-dimensional vector space, x_i must take all non zero values once for $1 \leq i \leq p-1$. This is equivalent that B is primitive (i.e., the multiplicative order of B is $2^m - 1$ and $p = 2^m - 1$). This type of pseudorandom number generator is well studied, such as combined Tausworthe generators, see L'Ecuyer et. al. [14]. Under our assumptions, we observe that the set

$$\{\bar{\boldsymbol{x}}_i^{(s)} \mid 0 \leq i < 2^m - 1\} \cup \{\mathbf{0}\}$$

is the digital net generated by $(I, B, B^2, \ldots, B^{s-1})$, as a set.

Our original interest is to obtain such a maximal periodic B with small t-value for wide s, to generate a pseudo-CUD sequence. For example, $t = 0$ might be possible for $s = 2$, which is the theoretical bound stated above (below Theorem 1.1.1). However, an exhaustive search for matrices B with $t(I, B, B^2) = 0$ for $m \leq 5$ resulted non-primitive B. Actually, we obtained a negative result Theorem 1.1.1: For $s = 3$ and $m \geq 3$, the digital net generated by (I, B, B^2) is a $(0, m, 3)$-net only if $B^3 = I$. Thus there is no $B \in \mathbb{F}_2^{m\times m}$ satisfying our assumptions for $m \geq 3$. Hence we conclude that our construction of $\mathbb{F}_2$-linear generator with maximal period is not optimal with respect to the t-value for $s = 3$. We need to consider some looser condition, such as considered in [3].

1.2 Preliminaries

We first recall results for t-value of digital nets. It is known that t-value of digital nets is related to the linear independence of column vectors of generating matrices.

Lemma 1.2.1 ([6, Theorem 4.52])**.** *Let $C_1, \ldots, C_s \in \mathbb{F}_2^{m\times m}$ and denote by $\boldsymbol{c}_i^j$ the j-th row of C_i. Assume that, for all choices of nonnegative integers $d_1, \ldots, d_s$ with $d_1 + \cdots + d_s = m - t$, $m - t$ vectors $\{\boldsymbol{c}_i^j \mid 1 \leq j \leq d_i\}$ are linear independent. Then the digital net generated by $(C_1, \ldots, C_s)$ is a (t, m, s)-net over $\mathbb{F}_2$.*

Lemma 1.2.2. *Let $C_1, \ldots, C_s \in \mathbb{F}_2^{m\times m}$ and $L_1, \ldots, L_s \in \mathcal{L}_m$. Let $G \in \mathbb{F}_2^{m\times m}$ be non-singular. Then we have $t(C_1, \cdots, C_s) = t(L_1C_1G, \cdots, L_sC_sG)$.*

Proof. Since G is non-singular, $(L_1C_1, \cdots, L_sC_s)$ and $(L_1C_1G, \cdots, L_sC_sG)$ generate the same digital net (as set) and hence we have $t(L_1C_1, \cdots, L_sC_s) = t(L_1C_1G, \cdots, L_sC_sG)$. Further, since $L_1, \ldots, L_s \in \mathcal{L}_m$, multiplying them from left does not change the linear independence appearing in Lemma 1.2.1. Thus it does not change the t-value, i.e., $t(C_1, \cdots, C_s) = t(L_1C_1, \cdots, L_sC_s)$. □

In the rest of this section, we give explicit B where the digital net generated by (I, B, B^2) is a $(0, m, 3)$-net over $\mathbb{F}_2$. To this end, we introduce the notion of (t, s)-sequence.

Definition 1.2.3. *Let $t \geq 0$ and $s \geq 1$ be integers. A sequence $\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots$ of points in $[0,1)^s$ is said to be a (t,s)-sequence over $\mathbb{F}_2$ if, for all integers $k \geq 0$ and $m > t$, the point set $\{\boldsymbol{x}_n \mid k2^m \leq n < (k+1)2^m\}$ forms a (t,m,s)-net over $\mathbb{F}_2$.*

There are many known explicit constructions of digital nets with low t-value. Among them we introduce the Faure sequence [8]. The Faure sequence over $\mathbb{F}_2$ is a $(0,2)$-sequence where the l-th point $\boldsymbol{x}_l \in [0,1)^2$ is generated as in (1.1) by matrices (I_m, P_m) (note that it gives the same $\boldsymbol{x}_l$ even if m is different), see, for example, [6, Section 8.1].

From (t,s)-sequence, we can generate $(t,m,s+1)$-net [16, Lemma 4.22].

Lemma 1.2.4. *Let $\{\boldsymbol{x}_i\}_{i\geq 0}$ be (t,s)-sequence over $\mathbb{F}_2$. Then $\{(\boldsymbol{x}_i, i2^{-m})\}_{i=0}^{2^m-1}$ is a $(t,m,s+1)$-net over $\mathbb{F}_2$.*

When $\{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{2^m-1}\}$ is the first 2^m points of the Faure sequence over $\mathbb{F}_2$, which is the digital net generated by (I_m, P_m), the 3-dimensional point set $\{(\boldsymbol{x}_i, i2^{-m})\}_{i=0}^{2^m-1}$ is found to be a digital net generated by (I_m, P_m, J_m). Thus it follows from Lemma 1.2.4 that

$$t(I_m, P_m, J_m) = 0. \tag{1.4}$$

We move on to the property of the matrix PJ.

Lemma 1.2.5. *For any positive integer m, we have*

$$P^2 = J^2 = (PJ)^3 = I \quad \text{in } \mathbb{F}_2^{m\times m}.$$

Proof. It is clear to check $J^2 = I$. We now prove $P^2 = I$ in $\mathbb{F}_2^{m\times m}$. Let k be a field and $k(x)$ a field of rational functions. Define two ring endmorphisms:

$$\mathcal{P}\colon k(x) \to k(x); \quad x \mapsto (1-x), \qquad \mathcal{K}\colon k(x) \to k(x); \quad x \mapsto x^{-1}.$$

Define also a k-linear map

$$\mathcal{J}\colon k(x) \to k(x); \quad f(x) \mapsto x^{m-1} \cdot \mathcal{K}(f(x)).$$

Let $V_m := \langle 1, x, \ldots, x^{m-1}\rangle$ be a k-linear subspace of $k(x)$. Then the restriction of $\mathcal{P}$ and $\mathcal{J}$ on V_m are k-linear endomorphisms. We find that the representation matrix of $\mathcal{P}$ restricted to V_m has coefficients of P'_m defined as

$$P' = P'_m := \left((-1)^{i-1}\binom{j-1}{i-1}\right)_{i,j=1}^{m}$$

Note that $P = P'$ in modulo 2. It is clear that the representation matrix of $\mathcal{J}$ restricted to V_m is J_m. We will show equalities between matrices via showing corresponding equalities between k-linear endomorphisms on $k(x)$.

For two k-ring endomorphisms $\mathcal{F}_1, \mathcal{F}_2 \colon k(x) \to k(x)$, $\mathcal{F}_1 = \mathcal{F}_2$ holds if and only if $\mathcal{F}_1(x) = \mathcal{F}_2(x)$ holds, since $k(x)$ is generated by x as a ring (to be precise we need to consider x^{-1} as well, but the inverse element is preserved by a ring homomorphism). From this property we have

$$\mathcal{P}^2 = \mathcal{K}^2 = \mathcal{P}\mathcal{K}\mathcal{P}\mathcal{K}\mathcal{P}\mathcal{K} = \mathrm{id}_{k(x)}, \tag{1.5}$$

since all of them map x to itself. Thus, by restricting $\mathcal{P}^2 = \mathrm{id}_{k(x)}$ on V_m, we have $P'^2 = I$. Hence $P^2 = I$ in $\mathbb{F}_2^{m\times m}$.

We now show $(PJ)^3 = I$ in $\mathbb{F}_2^{m\times m}$. For $a \in k(x)$, we define the multiplication map

$$(a\times) \colon k(x) \to k(x), \qquad f(x) \mapsto af(x).$$

Then

$$\mathcal{P} \circ (a\times) = \mathcal{P}(a) \cdot \mathcal{P} \quad \textit{and} \quad \mathcal{K} \circ (a\times) = \mathcal{K}(a) \cdot \mathcal{K}$$

hold. Using this property and (1.5), we have

$$\begin{aligned}\mathcal{P}\mathcal{J}\mathcal{P}\mathcal{J}\mathcal{P}\mathcal{J} &= \mathcal{P} \circ (x^{m-1}\times) \circ \mathcal{K}\mathcal{P} \circ (x^{m-1}\times) \circ \mathcal{K}\mathcal{P} \circ (x^{m-1}\times) \circ \mathcal{K} \\ &= \mathcal{P}(x^{m-1}) \cdot \mathcal{P}\mathcal{K}\mathcal{P}(x^{m-1}) \cdot \mathcal{P}\mathcal{K}\mathcal{P}\mathcal{K}\mathcal{P}(x^{m-1}) \cdot \mathcal{P}\mathcal{K}\mathcal{P}\mathcal{K}\mathcal{P}\mathcal{K} \\ &= (-1)^{m-1}\mathrm{id}_{k(x)}.\end{aligned}$$

By restricting above to V_m, whenever k has characteristic 2 we have

$$(PJ)^3 = I,$$

as we wanted. □

We now show that the matrix PJ is what we want.

Lemma 1.2.6. *For any positive integer m, we have*

$$t(I_m, P_mJ_m, (P_mJ_m)^2) = 0.$$

Proof. Lemma 1.2.5 implies $(PJP)^{-1} = JPJ$. Further $JPJ \in \mathcal{L}_m$ holds. Hence by Lemma 1.2.2 with $(L_1, L_2, L_3) = (J, I, JPJ)$ and $G = J$ we have

$$t(I, PJ, (PJ)^2) = t(J, P, I) = 0,$$

where the last equality follows from (1.4). □

1.3 Proof of Theorem 1.1.1

To prove Theorem 1.1.1, we need the following lemmas which will be shown in Section 1.4.

Lemma 1.3.1. *Let $B \in \mathbb{F}_2^{m\times m}$. Then the following are equivalent.*

(i) $t(I, B) = 0$.

(ii) *There exist $L_1, L_2 \in \mathcal{L}_m$ such that $B = L_1 J L_2$.*

Lemma 1.3.2. *Let $A, B, C, C' \in \mathbb{F}_2^{m\times m}$. Suppose that $t(A, B, C) = t(A, B, C') = 0$. Then there exists $L \in \mathcal{L}_m$ such that $LC = C'$.*

Assuming the above lemmas, we show the main theorem.

Proof of Theorem 1.1.1. First we assume (ii). By Lemma 1.2.2 with $(L_1, L_2, L_3) = (L^{-1}, L^{-1}, L^{-1})$ and $G = L$ we have

$$\begin{aligned} t(I, B, B^2) &= t(I, LPJL^{-1}, LPJPJL^{-1}) \\ &= t(I, PJ, PJPJ) = 0. \end{aligned}$$

Here the last equality follows from Lemma 1.2.6. Hence (i) follows.

We now assume (i). By Lemma 1.3.1, there exists $L_1, L_2 \in \mathcal{L}_m$ such that $B = L_1 J L_2$. Then by Lemma 1.2.2 with $(L_1, L_2, L_3) = (L_2^{-1}, L_1, L_1)$ and $G = L_2$ we have

$$t(I, J, JL_2L_1J) = t(I, L_1JL_2, (L_1JL_2)^2) = t(I, B, B^2) = 0.$$

On the other hand, from (1.4) we have $t(I, J, P) = 0$. Hence it follows from Lemma 1.3.2 that there exists $L_3 \in \mathcal{L}_m$ such that $L_3JL_2L_1J = P$ and thus $L_3 = P(JL_2L_1J)^{-1}$. Since $L_3 \in \mathcal{L}_m$ and $P(JL_2L_1J)^{-1} \in \mathcal{U}_m$ hold, both are equal to I. Thus $L_3 = I$ and $JL_2L_1J = P$ hold, and the latter implies $L_2 = JPJL_1^{-1}$. Hence $B = L_1JL_2 = L_1PJL_1^{-1}$, which shows (ii).

We now assume that one of them holds (and thus (ii) holds). Then there exist $L \in \mathcal{L}_m$ such that $B = LPJL^{-1}$. Hence we have

$$B^3 = (LPJL^{-1})^3 = L(PJ)^3L^{-1} = LL^{-1} = I,$$

where the the third equality follows from Lemma 1.2.5. □

1.4 Proofs of lemmas

1.4.1 Proof of Lemma 1.3.1

Proof of Lemma 1.3.1. First we assume (ii). By Lemma 1.2.2 with $(L_1, L_2) = (L_2^{-1}, L_1^{-1})$ and $G = L_2^{-1}$ we have

$$t(I, B) = t(I, L_1 J L_2) = t(I, J) = 0.$$

and thus (i) follows.

We now assume (i). From this we have $t(J, BJ) = t(I, B) = 0$. From $t(J, BJ) = 0$, we can show that all of the leading principal minor matrices of BJ are non-singular. Hence there exist $L \in \mathcal{L}_m$ and $U \in \mathcal{U}_m$ such that $LBJU = I$. Thus we have

$$B = L^{-1}U^{-1}J = L^{-1}J^2U^{-1}J = L^{-1}J(JU^{-1}J).$$

This shows (i) since $JU^{-1}J \in \mathcal{L}_m$. □

1.4.2 Proof of Lemma 1.3.2

Here we prove two lemmas to show Lemma 1.3.2.

Let us denote

$$A = \begin{pmatrix} \boldsymbol{a}_1 \\ \boldsymbol{a}_2 \\ \vdots \\ \boldsymbol{a}_m \end{pmatrix}, \qquad B = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \\ \vdots \\ \boldsymbol{b}_m \end{pmatrix}, \qquad C = \begin{pmatrix} \boldsymbol{c}_1 \\ \boldsymbol{c}_2 \\ \vdots \\ \boldsymbol{c}_m \end{pmatrix}, \qquad C' = \begin{pmatrix} \boldsymbol{c}'_1 \\ \boldsymbol{c}'_2 \\ \vdots \\ \boldsymbol{c}'_m \end{pmatrix}.$$

Lemma 1.4.1. *Let $A, B, C \in \mathbb{F}_2^{m\times m}$ and assume that $t(A, B, C) = 0$. For $i, j \in \mathbb{N}$ with $i + j \leq m - 1$, we define a subspace $V_{i,j}$ of $\mathbb{F}_2^{1\times m}$ as*

$$V_{i,j} := \langle \boldsymbol{a}_1, \ldots, \boldsymbol{a}_i, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{m-i-j-1}, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_j \rangle.$$

Let $1 \leq k \leq m - j$ and $0 \leq i_1 < \cdots < i_k \leq m - 1 - j$ be integers. Then the following holds true.

$$\dim \bigcap_{l=1}^{k} V_{i_l,j} = m - k, \tag{1.6}$$

$$\left| \bigcap_{0\leq i\leq m-j-1} V_{i,j}^c \right| = 2^j. \tag{1.7}$$

Proof. First we show (1.6) by induction on k. The assumption that $t(A,B,C) = 0$ implies that $\dim V_{i,j} = m-1$ for all i and j. This shows the lemma for $k=1$. We now assume the lemma for $k-1$ and show for k. Fix $0 \le i_1 < \cdots < i_k \le m-1-j$ and let $U := \bigcap_{l=2}^{k} V_{i_l,j}$. It follows from $t(A,B,C) = 0$ that $\boldsymbol{a}_{i_1+1} \notin V_{i_1,j}$. Combining this with $\boldsymbol{a}_{i_1+1} \in U$, we have

$$m = 1 + \dim V_{i_1,j} \le \dim(U + V_{i_1,j}) \le m,$$

which shows $\dim(U + V_{i_1,j}) = m$. Further we have $\dim U = m-k+1$ by induction assumption. Thus we have

$$\begin{aligned}\dim(U \cap V_{i_1,j}) &= \dim U + \dim V_{i_1,j} - \dim(U + V_{i_1,j}) \\ &= (m-k+1) + (m-1) - m \\ &= m-k.\end{aligned}$$

This shows the lemma for k.

Now we show (1.7). By (1.6) and the inclusion-exclusion principle, we have

$$\begin{aligned}\left|\bigcap_{0\le i\le m-j-1} V_{i,j}^c\right| &= \left|\mathbb{F}_2^{1\times m}\right| - \sum_{\emptyset\ne S\subset\{0,1,\dots,m-j-1\}} (-1)^{|S|} \left|\bigcap_{i\in S} V_{i,j}\right| \\ &= 2^m - \sum_{\emptyset\ne S\subset\{0,1,\dots,m-j-1\}} (-1)^{|S|} 2^{m-|S|} \\ &= 2^m - \sum_{k=1}^{m-j} (-1)^k 2^{m-k} \sum_{\emptyset\ne S\subset\{0,\dots,m-j-1\},|S|=k} 1 \\ &= 2^m - \sum_{k=1}^{m-j} (-1)^k 2^{m-k} \binom{m-j}{k} \\ &= 2^j \sum_{k=0}^{m-j} (-1)^k 2^{m-j-k} \binom{m-j}{k} \\ &= 2^j (2-1)^{m-j} \\ &= 2^j.\end{aligned}$$

This shows (1.7). □

Lemma 1.4.2. *Under the assumption and notation of Lemma 1.4.1, we further assume that* $C' \in \mathbb{F}_2^{m\times m}$ *and* $t(A,B,C') = 0$. *For* $i,j \in \mathbb{N}$ *with* $i+j \le m-1$ *we define a subspace* $W_{i,j}$ *of* $\mathbb{F}_2^{1\times m}$ *as*

$$W_{i,j} := \langle \boldsymbol{a}_1, \dots, \boldsymbol{a}_i, \boldsymbol{b}_1, \dots, \boldsymbol{b}_{m-i-j-1}, \boldsymbol{c}'_1, \dots, \boldsymbol{c}'_j \rangle.$$

Then the following holds true.

(i) $\boldsymbol{c}'_j \in \boldsymbol{c}_j + \langle \boldsymbol{c}_1, \dots, \boldsymbol{c}_{j-1} \rangle$ *for* $j \ge 1$,

(ii) $\langle \boldsymbol{c}_1, \dots, \boldsymbol{c}_j \rangle = \langle \boldsymbol{c}'_1, \dots, \boldsymbol{c}'_j \rangle$ *for* $j \ge 1$

(iii) $V_{i,j} = W_{i,j}$ *for all* i *and* j,

Proof. We show the lemma by induction on j. When $j = 0$, trivially $V_{i,0} = W_{i,0}$. We now assume the claim for j and show for $j+1$. It follows from $t(A,B,C) = 0$ that $\boldsymbol{c}_{j+1} \notin V_{i,j}$ for all i. Further we have $\langle \boldsymbol{c}_1, \dots, \boldsymbol{c}_j \rangle \subset V_{i,j}$ for all i. Hence

$$\boldsymbol{c}_{j+1} + \langle \boldsymbol{c}_1, \dots, \boldsymbol{c}_j \rangle \subset \bigcap_{0\le i\le m-j-1} V_{i,j}^c. \tag{1.8}$$

The cardinality of the left hand side is 2^j, and that of the right hand side is also 2^j from Lemma 1.4.1. Thus we have

$$\boldsymbol{c}_{j+1} + \langle \boldsymbol{c}_1, \dots, \boldsymbol{c}_j \rangle = \bigcap_{0\le i\le m-j-1} V_{i,j}^c.$$

In the same way, it holds that

$$\boldsymbol{c}'_{j+1} + \langle \boldsymbol{c}'_1, \dots, \boldsymbol{c}'_j \rangle = \bigcap_{0\le i\le m-j-1} W_{i,j}^c = \bigcap_{0\le i\le m-j-1} V_{i,j}^c.$$

where the last equality follows from induction assumption. Hence we have

$$\boldsymbol{c}_{j+1} + \langle \boldsymbol{c}_1, \dots, \boldsymbol{c}_j \rangle = \boldsymbol{c}'_{j+1} + \langle \boldsymbol{c}'_1, \dots, \boldsymbol{c}'_j \rangle.$$

In particular, using the induction assumption of (ii), we have

$$\langle \boldsymbol{c}_1, \dots, \boldsymbol{c}_{j+1} \rangle = \langle \boldsymbol{c}'_1, \dots, \boldsymbol{c}'_{j+1} \rangle \qquad \text{and} \qquad \boldsymbol{c}'_{j+1} \in \boldsymbol{c}_{j+1} + \langle \boldsymbol{c}_1, \dots, \boldsymbol{c}_j \rangle.$$

This shows (i) and (ii) for $j+1$. This implies

$$\begin{aligned} V_{i,j+1} &= \langle \boldsymbol{a}_1, \dots, \boldsymbol{a}_i, \boldsymbol{b}_1, \dots, \boldsymbol{b}_{m-i-j-2}, \boldsymbol{c}_1, \dots, \boldsymbol{c}_{j+1} \rangle \\ &= \langle \boldsymbol{a}_1, \dots, \boldsymbol{a}_i, \boldsymbol{b}_1, \dots, \boldsymbol{b}_{m-i-j-2}, \boldsymbol{c}'_1, \dots, \boldsymbol{c}'_{j+1} \rangle = W_{i,j+1}, \end{aligned}$$

which shows (iii) for $j+1$. □

Now Lemma 1.3.2 is easy to show: Lemma 1.4.2 (i) directly implies that there exists $L \in \mathcal{L}_m$ such that $LC = C'$.

Chapter 2

Non-existence and construction of pre-difference sets, and equi-distributed subsets in association schemes

2.1 Pre-difference sets

Let G be a finite group, e its unit, and $\mathbb{Z}[G]$ its group ring. For $D \subset G$, we denote by the same symbol D an element of $\mathbb{Z}[G]$ defined by $\sum_{g \in D} g$, and $D^{-1} := \sum_{g \in D} g^{-1}$. Let v be the order of G, and k the cardinality of D. If the equality

$$D^{-1}D = \lambda G + (k - \lambda)e$$

holds for an integer λ, D is called a (v, k, λ)-difference set. This is equivalent to that the cardinality of the set $\{(x, y) \in D \times D \mid x^{-1}y = g\}$ is λ for every $g \in G$ if $g \neq e$. The parameters satisfy $\lambda(v - 1) = k(k - 1)$. The difference sets are well-studied, see for example [10]. In a previous paper [11], the authors introduced the notion of pre-difference set.

Definition 2.1.1. *Let G be a finite group of order v, and D its subset with cardinality k. For $g \in G$, $[g]$ denotes the conjugacy class of g. If the value*

$$\#\{(x, y) \in D \times D \mid x^{-1}y \in [g]\}/\#[g]$$

is $\lambda \in \mathbb{Q}$ for any $g \in G - \{e\}$, then D is called a pre-difference set with

parameter (v, k, λ). *If* k *is one of* $0, 1, v, v-1$, *then* D *is a pre-difference set, called trivial.*

We showed the following [11]:

1. If G is abelian, the notion of difference sets and that of pre-difference sets coincide.

2. A difference set is a pre-difference set.

3. If a pre-difference set exists, λ is an integer satisfying $\lambda(v-1) = k(k-1)$,

4. The dihedral group D_{16} has a (non-trivial) $(16, 6, 2)$ pre-difference sets, whereas D_{16} has no non-trivial difference sets. (Note that it is an open conjecture that dihedral groups have only trivial difference sets [7].)

5. Classification of all the pre-difference sets in the non-abelian groups of order 16.

We introduced this notion of the pre-difference sets in the following representation-theoretic context. It is well-known that the function space $\mathbb{C}^G$ is decomposed as $\oplus_\rho V_\rho$ for ρ runs over the equivalent classes of irreducible representations of G, and for $f \in \mathbb{C}^G$ let $f^\rho \in V_\rho \subset \mathbb{C}^G$ denote the V_ρ components. Let $\delta_D : G \to \mathbb{C}$ be the characteristic function of $D \subset G$. Then, D is a pre-difference set if and only if $||\delta_D^\rho||/\dim(\rho)$ is independent of ρ if ρ is a non-trivial character ([11, Theorem 3 and §2], where the notation $\partial_\rho(D)$ there means $||\frac{1}{\#D}\delta_D^\rho||$, and the norm comes from the standard Hermittian inner product). There, the notion of pre-difference set is proved to be equivalent to a solution of a certain optimization problem. A natural generalization to association schemes is given in §5 there.

In this paper, in §2 we give a general frame work as a preliminary: the notion of "unital relation-partition" (which contains association schemes) and the notion of "equi-distributed subset in a unital relation-partition." The notion of equi-distributed subsets is equivalent to the notion of difference sets if the relation-partition is a thin-group association scheme, and to the pre-difference sets if the relation-partition is a group association scheme. The complement of an equi-distributed subset of a unital regular relation-partition is proved to be an equi-distributed subset, which implies the similar statements for difference sets (well-known) and for the pre-difference sets.

In §2.3, we show a construction method of a pre-difference set which in particular yields a $(16, 6, 2)$ pre-difference sets in the dihedral group D_{16} (where no non-trivial difference sets exist, as mentioned above) and a $(27, 13, 6)$ pre-difference set in the upper triangle group $UT(3, 3)$ which has no non-trivial difference sets.

In §2.4, we discuss on the product of equi-distributed subsets, when those have parameters satisfying $v = 4k - 4\lambda$, generalizing the results for difference sets [13]. This yields some infinite families of groups having a pre-difference set which is not a difference set.

In §2.5, we show some necessary conditions for existence of pre-difference sets. For example, it is shown that every group G of order $2p^m$ for p odd primes have only trivial pre-difference sets, generalizing [17].

2.2 Relation partition, equi-distribution and difference set

We introduce rather primitive mathematical objects and properties, which should have names but we could not find in the literatures, so we named "relation-partition" and "equi-distribution."

Definition 2.2.1. *Let X, I be sets, and $R : X \times X \to I$ a surjection. We call (X, R, I) a relation-partition. For each $i \in I$, $R^{-1}(i)$ gives a relation on X named R_i. This gives a partition of $X \times X$. Let A_i be the incidence matrix of R_i with the rows and columns are indexed by elements of X.*

A morphism from (X_1, R_1, I_1) to (X_2, R_2, I_2) is a pair of functions $f : X_1 \to X_2$ and $g : I_1 \to I_2$ such that the following diagram commutes:

$$\begin{array}{rcl} X_1 \times X_1 & \to & I_1 \\ f \times f \downarrow & \circlearrowleft & \downarrow g \\ X_2 \times X_2 & \to & I_2. \end{array}$$

This gives a category of relation-partitions. The two objects are isomorphic if and only if f and g are bijective.

Definition 2.2.2. *A relation-partition is regular, if for every i the number of ones in every column of A_i is constant, and the same holds for every row. Let k_i denote this positive integer, named the i-th valency of the regular relation-partition. This regularity is equivalent to the regularity of the directed graph induced from R_i, and k_i is the valency of the graph.*

A relation-partition is unital if there is $i_0 \in I$ with R_{i_0} being the identity relation, and i_0 is called the unit of (X, R, I). Clearly, X and I are non-empty. A morphism of unital relation-partition is a morphism between two relation-partitions that are both unital. Then $g : I_1 \to I_2$ maps the unit to the unit.

From now on through this paper, we assume that X in a relation-partitions is a finite set.

Definition 2.2.3. *(Equi-distribution.) Let (X, R, I) be a relation-partition. Let $D \subset X$. Then, we define $\lambda_i(D) := \#((D \times D) \cap R_i)$ and the ratio $r_i(D)$ of D in R_i by $\lambda_i(D)/\#(R_i)$. If the relation-partition is unital, we say D is equi-distributed if $r_i(D)$ is independent of the choice of $i \in I - \{i_0\}$. In this case, $r_i(D)$ is called the ratio of D and denoted by r. We define $\lambda := r\#X$, $v := \#X$ and $k := \#D$. We call D an equi-distributed subset in (X, R, I) with parameter (v, k, λ).*

If the relation-partition is regular, then the equi-distribution property is equivalent to that $\lambda_i(D)/k_i$ $(= r_i(D)v)$ is independent of the choice of $i \neq i_0$. Then we have $\lambda_i(D)/k_i = \lambda$.

We point out that the i-th inner distribution a_i in Delsarte theory [4, §3] is defined by $a_i = \lambda_i(D)/\#D$. We remark that association schemes (cf.[1]) are regular unital relation-partitions, so the notion of the equi-distributed subsets is defined for the association schemes (see [11, §5], where this notion is studied using Delsarte theory). Thus, all the results in this paper proved for regular unital relation-partitions hold for association schemes. Since the notion of relation-partitions is far weaker than association schemes, it might seem to be an abstract-nonsense, but it turns out to be somewhat useful. One may think that the denominator in the ratio is artificial, but it seems to be natural because of the following lemma.

Lemma 2.2.4. *Let (X, R, I) be a relation-partition, and $h : I \to J$ a surjection. Then, we have a relation partition (X, R', J) defined by $R' = h \circ R$.*

1. *Suppose that (X, R, I) is unital. If $h^{-1}(h(i_0)) = \{i_0\}$ holds, then (X, R', J) is unital. If $D \subset X$ is equi-distributed in (X, R, I) with ratio r, then D is equi-distributed in (X, R', J) with the same ratio r. Thus, if D has parameter (v, k, λ) in the former, D has the same parameter in the latter.*

2. *If (X, R, I) is regular, so is (X, R', J). The valency k'_j for the latter is $\sum_{i \in h^{-1}(j)} k_i$.*

Proof. Note that $R'^{-1}(j) = R^{-1}(h^{-1}(j))$ is the disjoint union of $R^{-1}(i)$ with $i \in h^{-1}(j)$. The condition $h^{-1}(h(i_0)) = \{i_0\}$ implies that (X, R', J) has unit $h(i_0) \in J$. The ratio $r'_j(D)$ for (X, R', J) is

$$\frac{\sum_{i \in h^{-1}(j)} \lambda_i(D)}{\sum_{i \in h^{-1}(j)} \#R^{-1}(i)},$$

but the equi-distribution property in (X, R, I) implies that

$$\frac{\lambda_i(D)}{\#R^{-1}(i)} = r$$

for any $i \neq i_0$, which implies the equi-distribution property in (X, R', J) with ratio r. The inheritance of regularity follows similarly. □

Corollary 2.2.5. *Let (X, R, I) be a unital relation-partition, and D an equi-distributed subset. Then $r = \frac{k(k-1)}{v(v-1)}$ and $\lambda(v-1) = k(k-1)$ holds. In particular, this equality holds for difference sets and pre-difference sets (see Lemma 2.2.7 below).*

Proof. We consider a surjection $h : I \to J = \{i_0, i'_0\}$ defined by $h(i_0) = i_0$ and $h(i) = i'_0$ for $i \neq i_0$. If D is equi-distributed with ratio r in (X, R, I), then the above lemma implies that D is equi-distributed with the same ratio in $(X, h \circ R, J)$. Since $(h \circ R)^{-1}(i'_0)$ is the complement of the identity relation $(h \circ R)^{-1}(i_0)$, its cardinality is $v^2 - v$. Also, we have $\lambda_{i'_0}(D) = k^2 - k$ and $r = r_{i'_0}(D) = (k^2 - k)/(v^2 - v)$. Since $\lambda = rv$, $\lambda(v-1) = k(k-1)$ follows. □

Lemma 2.2.6. *(Probabilistic view point.) Let (X, R, I) be a relation-partition. Take $(x, y) \in X \times X$ uniformly randomly. The ratio $r_i(D)$ is the conditional probability that under the condition $(x, y) \in R_i$, the event $(x, y) \in D \times D$ occurs. This is because the probability for $(x, y) \in R_i$ is $\#(R_i)/\#(X \times X)$, and the probability for $(x, y) \in (D \times D) \cap R_i$ is $\#((D \times D) \cap R_i)/\#(X \times X)$. The equi-distribution property is saying that this conditional probability is independent of the choice of i if $i \neq i_0$.*

The inheritance of equi-distribution and ratio in Lemma 2.2.4 is natural: R'_j $(j \neq h(i_0))$ is a disjoint union of R_i with $i \in h^{-1}(j)$ (and by the assumption

we have $i_0 \notin h^{-1}(j)$), and the conditional probability $r_j(D)$ that "under the condition $(x,y) \in R'_j$ $(x,y) \in D \times D$ occurs" is r, since if $(x,y) \in R'_j$ then $(x,y) \in R_i$ for some $i \neq i_0$ and the probability for $(x,y) \in D \times D$ is $r_i(D) = r$ independent of i.

The following lemma relates the equi-distribution property with difference sets.

Lemma 2.2.7. *1. Let G be a finite group. Then $R : G \times G \to G$ given by $(x,y) \mapsto x^{-1}y$ is a unital regular relation-partition, called the thin-association scheme of G. A subset $D \subset G$ is a difference set if and only if D is equi-distributed in the (G,R,G).*

2. Let $C(G)$ be the set of conjugacy classes of G, and $\pi : G \to C(G)$ the mapping $g \mapsto [g]$. Then $R' : G \times G \to C(G)$ obtained by the composition $R' := \pi \circ R$ is a unital regular relation-partition, called the group association scheme of G. A subset $D \subset G$ is a pre-difference set if and only if D is equi-disributed in $(G,R',C(G))$.

3. If D is a difference set with parameter (v,k,λ), then D is a pre-difference set with the same parameter.

Proof. (1). The unit is $e \in G$, and the regularity follows since $k_g = 1$ for every $g \in G$. Thus $\#R_g = \#G$, and the ratio $r_g(D)$ is $\#\{(x,y) \in D \times D \mid x^{-1}y = g\}/\#G$. Thus, D is equi-distributed if and only if D is a difference set.

(2). The unit is $[e]$, and the regularity follows from (1) and Lemma 2.2.4(2) with $k_{[g]} = \#\pi^{-1}(g) = \#[g]$. Then $\#R_{[g]} = k_{[g]}\#X = \#[g]\#G$ holds, and the ratio $r_{[g]}(D)$ is $\#\{(x,y) \in D \times D \mid [x^{-1}y] = [g]\}/(\#[g]\#G)$. Thus, by definition, the pre-difference set property is equivalent to the equi-distribution property.

(3). This follows from Lemma 2.2.4 (1). □

Lemma 2.2.8. *(Complement) If D is a (v,k,λ) equi-distributed subset in a unital regular relation-partition (X,R,I), then D^c is a $(v, v-k, v-2k+\lambda)$ equi-distributed subset. We write $\overline{\lambda} := v - 2k + \lambda$. The value $r_i(D^c)$ $(i \neq i_0)$ is $1 - 2k/v + r$, which is denoted by $\overline{r}$.*

Proof. The counting argument in the proof in Proposition 5.17 in [11] will do. Here instead, we give a proof by Lemma 2.2.6. Take $(x,y) \in X \times X$ uniformly randomly. Assume that $(x,y) \in R_i$. We consider two cases: (A) $(x,y) \in D \times X$ and (B) $(x,y) \in X \times D$. Let p_A be the probability (A) occurs,

and p_B for (B). Then "(A) and (B)" is $(x, y) \in D \times D$, and the probability is $r_i(D) = r$ for $i \neq i_0$. The complement of "(A) or (B)" is $(x, y) \in D^c \times D^c$, and its probability is $r_i(D^c)$, which is $1 - p_A - p_B + r$. Now, $p_A = p_B = k/v$ follows from the regularity: $\#R_i = vk_i$ and $\#((D \times X) \cap R_i) = kk_i$ (since for each $x \in D$ we have $k_i = \#\{y \in X \mid (x, y) \in R_i\}$) and thus $p_A = (kk_i)/(vk_i) = k/v$ holds. The same argument gives $p_B = k/v$. We obtained $r_i(D^c) = 1 - 2k/v + r$, independent of the choice of $i \neq i_0$, which shows that D^c is equi-distributed with ratio $\overline{r} = 1 - 2k/v + r$. By multiplying v, we have $\overline{\lambda} = v - 2k + \lambda$. □

2.3 Construction of pre-difference sets from difference sets

Theorem 2.3.1. *Let G be a finite group, A its abelian subgroup, and N its subgroup. Assume that the map $\varphi : N \times A \to G$ defined by $(n, a) \mapsto na$ is bijective (i.e. $N \cap A = \{e\}$ and φ is surjective). If the direct product group $N \times A$ has a difference set D, then its image $\varphi(D)$ in G is a pre-difference set of G with the same parameter as D.*

Proof. Consider the thin-association scheme $(N \times A, R, N \times A)$, $R((n_1, a_1), (n_2, a_2)) = (n_1^{-1}n_2, a_1^{-1}a_2)$. Then D is equi-distributed there. There is a surjection $h : N \times A \to C(G)$, given by $(n, a) \mapsto [na]$. Then by Lemma 2.2.4, D is equi-distributed in $(N \times A, h \circ R, C(G))$ with the same ratio. We claim that the diagram

$$\begin{array}{ccc} (N \times A) \times (N \times A) & \stackrel{R}{\to} & N \times A \\ \varphi \times \varphi \downarrow & \circlearrowleft & \downarrow h \\ G \times G & \stackrel{R'}{\to} & C(G) \end{array}$$

commutes, and then since $(N \times A, h \circ R, C(G))$ is isomorphic to $(G, R', C(G))$, $\varphi(D)$ is equi-distributed there with the same ratio, that is, $\varphi(D)$ is a pre-difference set in G with the same parameter. To show the claim, we take $(n_1, a_1), (n_2, a_2)$ at the left top corner. Its image to the right top is $(n_1^{-1}n_2, a_1^{-1}a_2)$, and its image by h is $[n_1^{-1}n_2a_1^{-1}a_2]$. A diagram chase via the left bottom corner gives $[(n_1a_1)^{-1}(n_2a_2)]$. Since A is abelian, $n_1^{-1}n_2a_1^{-1}a_2 = n_1^{-1}n_2a_2a_1^{-1}$ and it is conjugate to $a_1^{-1}n_1^{-1}n_2a_2 = (n_1a_1)^{-1}(n_2a_2)$, which proves the commutativity of the diagram. □

Corollary 2.3.2. *The dihedral group D_{16} has a pre-difference set with parameter $(16, 6, 2)$, and the group $UT(3, 3)$ of the upper half triangle matrices with diagonal being 1 in $\mathrm{GL}_3(\mathbb{F}_3)$ has a pre-difference set with parameter $(27, 13, 6)$.*

Note that the non-existence of non-trivial difference sets in these groups is well-known (e.g. [12]).

Proof. The group D_{16} is a semi-direct product of C_8 and C_2. It is known that $C_8 \times C_2$ has a difference set with parameter $(16, 6, 2)$ (which goes back to [19]). Theorem 2.3.1 for $N = C_8$ and $A = C_2$ in D_{16} shows the existence of a pre-difference set.

The group $UT(3, 3)$ has a presentation

$$\left\langle a, b, c \mid a^3 = b^3 = c^3 = 1, ac = ca, bc = ca, ba = abc \right\rangle,$$

and it is a semi-direct product of $N := \langle a, c\rangle$ and $A := \langle b\rangle$, where the former is $C_3 \times C_3$ and the latter is C_3. Paley's construction ([20, Theorem 27.5]) gives a $(27, 13, 6)$ difference sets in $C_3^3 = N \times A$, and Theorem 2.3.1 shows the existence of a pre-difference set with the same parameter in $UT(3, 3)$. □

Remark 2.3.3. *By using GAP[9], we checked that D_{36} has no non-trivial pre-difference set (though there are nine groups having $(36, 15, 6)$ difference sets [12]).*

Remark 2.3.4. *If we use the notion of fusions of association schemes (cf. [21, P.28]), we see that the proof of Theorem 2.3.1 shows that the group association scheme $(NA, R', C(NA))$ is a fusion of a thin association scheme $(N \times A, R, N \times A)$. This group association scheme is also a fusion of a thin association scheme (NA, R, NA), and gives an example that a group association scheme is a fusion of two non-isomorphic thin association schemes, if NA is not isomorphic to $N \times A$.*

2.4 Product for the case $v = 4k - 4\lambda$

Definition 2.4.1. *The product of two relation-partitions (X_1, R_1, I_1) and (X_2, R_2, I_2) is defined as $(X_1 \times X_2, R_1 \times R_2, I_1 \times I_2)$. If both are unital (or regular), then so is the product. If both are association schemes, then so is the product. If both are group association schemes, so is the product. If both are thin-group association schemes, so is the product.*

The following is a direct generalization of a result in [13] on the difference sets in groups.

Theorem 2.4.2. *Let D_1 be a (v_1, k_1, λ_1) equi-distributed subset in a unital regular relation-partition (X_1, R_1, I_1) with $D_1 \neq \emptyset, X_1$, and D_2 be a (v_2, k_2, λ_2) equi-distributed subset in a unital regular relation-partition (X_2, R_2, I_2) with $D_2 \neq \emptyset, X_2$. Then, $D := (D_1 \times D_2) \coprod (D_1^c \times D_2^c)$ is an equi-distributed subset in the product relation-partition if and only if $v_i = 4(k_i - \lambda_i)$ holds for $i = 1, 2$. In this case, D has the parameter (v, k, λ) satisfying $v = 4(k - \lambda)$. If D_1 or D_2 is not equi-distributed, then D is not equi-distributed.*

Proof. Let $i_1 \in I_1$ and $i_2 \in I_2$. For $P \subset (X_1 \times X_2)^2 = X_1^2 \times X_2^2$, we define

$$\Gamma_{i_1,i_2}(P) := P \cap (R_{i_1} \times R_{i_2}).$$

Note that the cardinality of $\Gamma_{i_1,i_2}(D \times D)$ is $\lambda_{i_1,i_2}(D)$. We have

$$\begin{aligned}\Gamma_{i_1,i_2}(D \times D) &= \Gamma_{i_1,i_2}((D_1 \times D_2) \times (D_1 \times D_2)) + \Gamma_{i_1,i_2}((D_1 \times D_2) \times (D_1^c \times D_2^c)) \\ &\quad + \Gamma_{i_1,i_2}((D_1^c \times D_2^c) \times (D_1 \times D_2)) + \Gamma_{i_1,i_2}((D_1^c \times D_2^c) \times (D_1^c \times D_2^c)).\end{aligned}$$

Computing the cardinality, we have

$$\begin{aligned}\lambda_{i_1,i_2}(D) &= \lambda_{i_1}(D_1)\lambda_{i_2}(D_2) + \langle A_{i_1}\delta_{D_1}, \delta_{X_1} - \delta_{D_1}\rangle \langle A_{i_2}\delta_{D_2}, \delta_{X_2} - \delta_{D_2}\rangle \\ &\quad + \langle A_{i_1}(\delta_{X_1} - \delta_{D_1}), \delta_{D_1}\rangle \langle A_{i_2}(\delta_{X_2} - \delta_{D_2}), \delta_{D_2}\rangle \\ &\quad + \lambda_{i_1}(D_1^c)\lambda_{i_2}(D_2^c) \\ &= \lambda_{i_1}(D_1)\lambda_{i_2}(D_2) + 2(k_{i_1}k_1 - \lambda_{i_1}(D_1))(k_{i_2}k_2 - \lambda_{i_2}(D_2)) \\ &\quad + \lambda_{i_1}(D_1^c)\lambda_{i_2}(D_2^c).\end{aligned}$$

We divide this by $k_{i_1}k_{i_2}$ to obtain

$$\begin{aligned}\lambda_{i_1,i_2}(D)/(k_{i_1}k_{i_2}) &= \frac{\lambda_{i_1}(D_1)}{k_{i_1}}\frac{\lambda_{i_2}(D_2)}{k_{i_2}} + 2\left(k_1 - \frac{\lambda_{i_1}(D_1)}{k_{i_1}}\right)\left(k_2 - \frac{\lambda_{i_2}(D_2)}{k_{i_2}}\right) \\ &\quad + \frac{\lambda_{i_1}(D_1^c)}{k_{i_1}}\frac{\lambda_{i_2}(D_2^c)}{k_{i_2}}. \qquad (2.1)\end{aligned}$$

If $i_1 \neq i_0$ and $i_2 \neq i_0$, (2.1) becomes

$$\lambda_1\lambda_2 + 2(k_1 - \lambda_1)(k_2 - \lambda_2) + \bar{\lambda_1}\bar{\lambda_2}, \qquad (2.2)$$

where $\bar{\lambda_1}$, $\bar{\lambda_2}$ is the λ-parameter for D_1^c, D_2^c, respectively. If $i_1 = i_0$ and $i_2 \neq i_0$, since $k_{i_0} = 1$, (2.1) becomes

$$k_1\lambda_2 + 2(k_1 - k_1)(k_2 - \lambda_2) + (v_1 - k_1)\bar{\lambda_2} = k_1\lambda_2 + (v_1 - k_1)\bar{\lambda_2}. \qquad (2.3)$$

Computing (2.2) minus (2.3), we have

$$\begin{aligned} & (\lambda_1 - k_1)\lambda_2 + 2(k_1 - \lambda_1)(k_2 - \lambda_2) + (\bar{\lambda_1} - v_1 + k_1)\bar{\lambda_2} \\ = \; & (\lambda_1 - k_1)\lambda_2 + 2(k_1 - \lambda_1)(k_2 - \lambda_2) + (\lambda_1 - k_1)\bar{\lambda_2} \\ = \; & (\lambda_1 - k_1)(\lambda_2 - 2k_2 + 2\lambda_2 + \bar{\lambda_2}) \\ = \; & (\lambda_1 - k_1)(\lambda_2 - 2k_2 + 2\lambda_2 + v_2 - 2k_2 + \lambda_2) \\ = \; & (\lambda_1 - k_1)(v_2 - 4k_2 + 4\lambda_2), \end{aligned}$$

since $\bar{\lambda_i} = v_i - 2k_i + \lambda_i$. If $k_1 = \lambda_1$, then $\lambda_1(v_1 - 1) = k_1(k_1 - 1)$ impies $k_1 = 0$ or v. Then $D_1 = \emptyset$ or X_1, contradicting the assumption. For the case $i_1 \neq i_0$ and $i_2 = i_0$, the difference is $(\lambda_2 - k_2)(v_1 - 4k_1 - 4\lambda_1)$. Thus, D is equi-distributed if and only if $v_i - 4k_i - \lambda_i = 0$ holds for $i = 1, 2$.

Let (v, k, λ) be the parameter of D. Then, $v = v_1v_2$, $k = k_1k_2 + (v_1 - k_1)(v_2 - k_2)$, and λ is given by (2.2). Then

$$\begin{aligned} k - \lambda &= k_1k_2 + (v_1 - k_1)(v_2 - k_2) - \lambda_1\lambda_2 - 2(k_1 - \lambda_1)(k_2 - \lambda_2) - \bar{\lambda_1}\bar{\lambda_2} \\ &= 4(k_1 - \lambda_1)(k_2 - \lambda_2) \end{aligned}$$

holds (through a long computation), and hence

$$v = v_1v_2 = 4(k_1 - \lambda_1) \cdot 4(k_2 - \lambda_2) = 4(k - \lambda)$$

follows.

Suppose that D_2 is not equi-distributed. Then, for the case $i_1 = i_0$ and $i_2 \neq i_0$, the computation of (2.3) gives

$$\lambda_{i_1,i_2}(D)/(k_{i_1}k_{i_2}) = k_1\frac{\lambda_{i_2}(D_2)}{k_{i_2}} + (v_1 - k_1)\frac{\lambda_{i_2}(D_2^c)}{k_{i_2}}$$

Using

$$\lambda_{i_2}(D_2^c) = \langle A_{i_1}(\delta_{X_2} - \delta_{D_2}), (\delta_{X_2} - \delta_{D_2})\rangle = k_{i_2}v_2 - 2k_{i_2}k_2 + \lambda_{i_2}(D_2),$$

we have

$$\begin{aligned}\lambda_{i_1,i_2}(D)/(k_{i_1}k_{i_2}) &= k_1\frac{\lambda_{i_2}(D_2)}{k_{i_2}} + (v_1-k_1)\frac{k_{i_2}v_2 - 2k_{i_2}k_2 + \lambda_{i_2}(D_2)}{k_{i_2}} \\ &= v_1\frac{\lambda_{i_2}(D_2)}{k_{i_2}} + (v_1-k_1)(v_2-k_2).\end{aligned}$$

Since $v_1 \neq 0$, we notice that this value varies if $\frac{\lambda_{i_2}(D_2)}{k_{i_2}}$ varies. Since D_2 is not equi-distributed, this value varies if i_2 varies among $i_2 \neq i_0$. Thus, D is not equi-distributed. □

Corollary 2.4.3. *Let D be a pre-difference set in a finite group G with parameter (v,k,λ), $v = 4(k-\lambda)$, which is not a difference set in G. Let $D' \subset G'$ be a pre-difference set in G' with $v' = 4(k'-\lambda')$. Then, the direct product construction in the product $G \times G'$ yields a pre-difference set which is not a difference set. This gives infinitely many examples of groups with a pre-difference set which is not a difference set. For example, G^n has a pre-difference set which is not a difference set for any positive integer n. We may use a pre-difference set in $G = D_{16}$ which is not a difference set (shown in Corollary 2.3.2).*

2.5 Non-existence of pre-difference sets in some groups

As a necessary condition on the parameter for the existence of a difference set, the following Bruck-Ryser-Chowla condition (cf. [20, Theorem 19.11]) is known:

Theorem 2.5.1. *Suppose that a (v,k,λ) difference set exists. If v is even, $k-\lambda$ is a square. If v is odd, then the equation*

$$(k-\lambda)X^2 + (-1)^{(v-1)/2}\lambda Y^2 = Z^2$$

has a nontrivial integer solution.

At present, we don't know the answer to the following question.

Question 2.5.2. *Is the Bruck-Ryser-Chowla condition a necessary condition for the existence of a pre-difference set with parameter (v,k,λ)?*

On the other hand, we show that a necessary condition proved in [17] for the existence of difference sets is a necessary condition for the existence of pre-difference sets.

Theorem 2.5.3. *Let $N \subset G$ be a normal subgroup of a finite group G with index 2. Let $D \subset G$ be a pre-difference set. Put $m := \#N = v/2$, $D_1 := D \cap N$, $D_2 := D \setminus N$, $k_1 := \#D_1$, and $k_2 := \#D_2$. (Hence $k = k_1 + k_2$.) Then, the following hold.*

A1 $\lambda(m-1) = k_1(k_1-1) + k_2(k_2-1)$.

A2 $\lambda m = 2k_1k_2$.

As a consequence, $k - \lambda = (k_1 - k_2)^2$ follows, and hence Bruck-Ryser-Chowla condition holds in this case. If D is not trivial, then $k_1 < m$ and $k_2 < m$ hold.

Remark 2.5.4.

1. *The above two conditions are given in [17, (2.3), (2.4)].*
2. *Summation of the above two implies*

$$\lambda(v-1) = k(k-1),$$

   hence any two of the three equalities imply the other.

3. *Let $b \in N^c$. Then $G = N \coprod Nb$. If D is a pre-difference set as above, $Db = D_2b \cup D_1b$ is a pre-difference set with $D_1' := D_2b \subset N$ and $D_2' = D_1b \subset N^c$, and thus a pre-difference set with $\#D_1' = k_2$ and $\#D_2' = k_1$ exists.*

Proof. Let $f : X \to Y$ be a map between finite sets, $C \subset Y$ be a non-empty subset. Then we define the density of f on C by $\#f^{-1}(C)/\#(C)$. Let $D \subset G$ be a subset of a finite group G. It is easy to see that D is a pre-difference set if and only if

$$R_{|D} : D \times D \to G, \quad (x, y) \mapsto x^{-1}y$$

have the density λ on every conjugacy class $C \subset G$ except $C = [e]$.

Because N is normal, N is a union of conjugacy classes, and N^c is a union of conjugacy classes. Thus, any conjugacy class C of G is contained one of N or N^c.

It is easy to see that

$$R : G \times G \to G, \quad (x, y) \mapsto x^{-1}y$$

is the direct sum of the two maps:

$$R_1 : (N \times N) \coprod (N^c \times N^c) \to N, \quad R_2 : (N \times N^c) \coprod (N \times N^c) \to N^c.$$

This implies that the restrictions of each map to $D \times D$ gives

$$R_1' : (D_1 \times D_1) \coprod (D_2 \times D_2) \to N, \quad R_2' : (D_1 \times D_2) \coprod (D_2 \times D_1) \to N^c,$$

and the density of R_1' on every conjugacy class $C \subset N$ (except $C = [e]$) is λ. Thus, the density of R_1' on $N - \{e\}$ is λ. Since the inverse image of e by R_1' is the union of the diagonal sets in $D_1 \times D_1$ and $D_2 \times D_2$, the inverse image of $N - \{e\}$ by R_1' has cardinality $(k_1^2 - k_1) + (k_2^2 - k_2)$, which is equal to $\lambda(\#(N) - 1) = \lambda(m - 1)$, hence A1 holds. Since the density of R_2' on every conjugacy class $C \subset N^c$ is λ, we have $k_1k_2 + k_2k_1 = \lambda m$, hence A2 holds. A1 minus A2 gives

$$-\lambda = (k_1 - k_2)^2 - (k_1 + k_2).$$

Since $k = k_1 + k_2$, $k - \lambda = (k_1 - k_2)^2$ follows.

Clearly $k_1 \leq m$ holds. Suppose that the equality holds. Then $\lambda k_1 = 2k_1k_2$, and hence $\lambda = 2k_2$. Thus

$$2k_2(k_1 - 1) = k_1(k_1 - 1) + k_2(k_2 - 1).$$

This is equivalent to

$$(k_1 - k_2)(k_1 - k_2 - 1) = 0.$$

Since $k_1 = m$, this implies that $k_2 = m$ or $k_2 = m - 1$. In either cases, D is trivial. If $k_2 = m$, then $k_1 = m$ or $m - 1$, and again D is trivia l. □

Corollary 2.5.5. *Let G be a group of order $2p^\alpha$ for an odd prime p and integer α. Then, G has only trivial pre-difference sets.*

Proof. The proof is the same as [17, Corollary 2.4]. There it is proved that G has a subgroup of index 2, and then show that A1 and A2 have no integer solution. □

Corollary 2.5.6. *Let G be a group of order $4p^\alpha$ with p prime and α odd. Assume that G has an index 2 subgroup. Then there is no non-trivial pre-difference set in G.*

Proof. It is proved that A1, A2 have no nontrivial integer solutions in [5, Proposition 2.2]. □

Suppose that $v = 4(k - \lambda)$. If Bruck-Ryser-Chowla condition holds, then $k - \lambda = u^2$, and it is easy to show that $(v, k, \lambda) = (4u^2, 2u^2 - u, u^2 - u)$ if $k \leq v/2$. This parameter is called Hadamard-type. For a pre-difference set, it is open whether $k - \lambda$ is a square or not for even v. Nevertheless, it is interesting to consider the Hadamard-type parameters for a group with index 2 subgroups, because they have a (unique) solution to A1 and A2, $\{k_1, k_2\} = \{u^2, u^2 - u\}$.

Question 2.5.7. *Are there interesting examples of pre-difference sets with Hadamard-type parameter, in a group G having index 2 subgroup? For $u = 2$ in D_{16}, yes. For $u = 3$ in D_{36}, there is no non-trivial pre-difference set (checked by a computer program).*

We have a straight forward generalization of Theorem 2.5.3 to relation-partitions.

Lemma 2.5.8. *Let (X, R, I) be a relation-partition. Let $\mathbb{F}_2$ denote the corresponding association scheme $(\mathbb{F}_2, R', \mathbb{F}_2)$ defined by $R'(x, y) = x - y$. Assume that there is a morphism $(f, g) : (X, R, I) \to \mathbb{F}_2$ with f being surjective. Let $X^+ \subset X$ ($X^- \subset X$) be the inverse image of 0 (1, respectively) by $f : X \to \mathbb{F}_2$. Then*

$$(gR)^{-1}(0) = (X^+ \times X^+) \coprod (X^- \times X^-), (gR)^{-1}(1) = (X^+ \times X^-) \coprod (X^- \times X^+)$$

hold. If (X, R, I) is regular, then $\#X^+ = \#X^- = \#X/2$. hold.

Proof. Since f is surjective, g is surjective, too. The definition of morphism (Definition 2.2.1) implies that $gR(x, y) = f(x) - f(y)$ with gR, and $gR(x, y) = 0$ holds if and only if $x, y \in X^+$ or $x, y \in X^-$, and $gR(x, y) = 1$ holds if and only if $(x, y) \in (X^+ \times X^-) \coprod (X^- \times X^+)$.

Assume the regularity. The relation-partition $(X, gR, \mathbb{F}_2)$ is regular by Lemma 2.2.4(2). For $x \in X^+$, the valency of x in the relation $(gR)^{-1}(0)$ is $\#X^+$, and that in $(gR)^{-1}(1)$ is $\#X^-$. By regularity, they are equal. Since $\#X = \#X^+ + \#X^-$, the claim follows. □

Theorem 2.5.9. *Assume that a regular unital (X, R, I) satisfies the condition of Lemma 2.5.8. Let D be an equi-distributed subset in X with parameter (v, k, λ). Let $m := \#X/2$, $k_1 := \#(X^+ \cap D)$, $k_2 := \#(X^- \cap D)$. Then, the conditions A1, A2 and the statements below them in Theorem 2.5.3 hold.*

Proof. Let us define $h : I \to \{i_0, +, -\} =: J$ by $h(i_0) = i_0$, $h(i) = +$ if $i \neq i_0$ and $g(i) = 0$, $h(i) = -$ if $g(i) = 1$. By Lemma 2.2.4, (X, hR, J) is a regular unital relation-partition, and D is equi-distributed there with the same parameter. The cardinality $\#hR^{-1}(j)$ is if $j = +$

$$\#((X^+ \times X^+) - \Delta_{X^+}) \coprod ((X^- \times X^-) - \Delta_{X^-}) = 2m(m-1)$$

where Δ_{X^+} means the diagonal subset, and if $j = -$

$$\#((X^+ \times X^-) \coprod (X^- \times X^+)) = 2m^2.$$

The $\lambda_j(D)$ is if $j = +$

$$\#((D^+ \times D^+) - \Delta_{D^+}) \coprod ((D^- \times D^-) - \Delta_{D^-}) = k_1(k_1-1) + k_2(k_2-1)$$

and if $j = -$

$$\#((D^+ \times D^-) \coprod (D^- \times D^+)) = 2k_1k_2.$$

Computing the ratio, we have

$$(k_1(k_1-1) + k_2(k_2-1))/(2m(m-1)) = \lambda/v = 2k_1k_2/(2m^2).$$

By $v = 2m$, we have A1 and A2. The rest of the proof is the same as that of Theorem 2.5.3. □

As a corollary, if (X, R, I) satisfies the conditions in Lemma 2.5.8 and $\#X = 2p^\alpha$ (p odd prime and α integer) or $\#X = 4p^\alpha$ (p prime and α odd integer) as in Corollaries 2.5.5 and 2.5.6, then there is no non-trivial equi-distributed subset. Note that this theorem implies Theorem 2.5.3 since there is a surjective morphism $(G, R', C(G)) \to \mathbb{F}_2$ defined by $f : G \to G/N \cong \mathbb{F}_2$ which factors through $g : C(G) \to \mathbb{F}_2$. The necessary commutativity is that $R'(x, y) = [x^{-1}y] \mapsto x^{-1}yN \in G/N$ equals to $f(x) - f(y) \in \mathbb{F}_2$ through the identification $G/N \cong \mathbb{F}_2$, which is easy to check.

Bibliography

[1] Eiichi Bannai, Tatsuro Ito. *Algebraic Combinatorics I: Association Schemes*. Benjamin/Cummings, Calfornia, 1984.

[2] S. Chen, J. Dick, and A. B. Owen. Consistency of Markov chain quasi-Monte Carlo on continuous state spaces. *Ann. Statist.*, 39(2):673–701, 2011.

[3] Su Chen, Makoto Matsumoto, Takuji Nishimura, and Art B. Owen. New inputs and methods for Markov chain quasi-Monte Carlo. In *Monte Carlo and quasi-Monte Carlo methods 2010*, volume 23 of *Springer Proc. Math. Stat.*, pages 313–327. Springer, Heidelberg, 2012.

[4] P. Delsarte. *An algebraic approach to the association schemes of coding theory. Philips Res. Rep. Suppl. 10*, i–vi, 1–97, 1973.

[5] Y. Deng. *A note on difference sets in dihedral groups. Arch. Math.*, (Basel) 82, 4–7, 2004.

[6] Josef Dick and Friedrich Pillichshammer. *Digital Nets and Sequences: Discrepancy Theory and Quasi-Monte Carlo Integration*. Cambridge University Press, Cambridge, 2010.

[7] C.T. Fan, M.K. Siu, S.L. Ma. *Difference sets in dihedral groups and interlocking difference sets. Ars Combin*, 20.A, 99–107, 1985.

[8] Henri Faure. Discrépance de suites associées à un système de numération (en dimension s). *Acta Arith.*, 41(4):337–351, 1982.

[9] GAP. NTL. *GAP—groups, algorithms, programming—a system for computational discrete algebra*. `https://www.gap-system.org/`, Accessed 20 July 2020.

[10] D. Jungnickel, B. Schmidt. *Difference Sets: an Update*. London Mathematical Society Lecture Note Series, pp. 89–112. Cambridge University Press, Cambridge, 1997.

[11] Hiroki Kajiura, Makoto Matsumoto, Takayuki Okuda. *Approximation of integration over finite groups, difference sets and association schemes*. arXiv:1903.00697.

[12] R. Kibler. *A summary of noncyclic difference sets, $k < 20$. J. Combin. Theory Ser*, A 25, 62–67, 1978.

[13] P.K. Menon. *On difference sets whose parameters satisfy a certain relation. Proc. AMS.*, 13, 739–745, 1962.

[14] Piere L'Ecuyer and Christiane Lemieux. Quasi-monte carlo via linear shift-register sequences. In *Proceedings of the 31st Conference on Winter Simulation: Simulation—a Bridge to the Future - Volume 1*, WSC '99, pages 632–639, New York, NY, USA, 1999. ACM.

[15] Mordechay B. Levin. Discrepancy estimates of completely uniformly distributed and pseudorandom number sequences. *Internat. Math. Res. Notices*, (22):1231–1251, 1999.

[16] Harald Niederreiter. *Random number generation and quasi-Monte Carlo methods*, volume 63 of *CBMS-NSF Regional Conference Series in Applied Mathematics*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1992.

[17] W. Shiu. *Difference sets in groups containing subgroups of index 2*. Ars Combin., 42, 199–205, 1996.

[18] Seth D. Tribble. *Markov chain Monte Carlo algorithms using completely uniformly distributed driving sequences*. PhD thesis, 2007. Stanford University.

[19] R.J. Turyn. *Character sums and difference sets. Pac. J. Math.*, 15, 319–346, 1965.

[20] J.H. van Lint, R.M. Wilson. *A Course in Combinatorics, 2nd edn.* Cambridge University Press, Cambridge, 2001.

[21] P.H. Zieschang. *An Algebraic Approach to Association Schemes*. Lecture Notes in Mathematics, vol. 1628. Springer, Berlin, 1996.