Constructions and Bounds for Splitting and Separating Systems

Li, Xiangyang [1,2*]
[2]Dept. of Scientific Research, Shanghai Customs College.
Shanghai, 201204, P.R.C.;
[1]School of Finance, Shanghai University of Fin. and Econ.
Shanghai, 200433, P.R.C.;

Shen, Hao[3]
[3]Department of Mathematics, Shanghai Jiaotong University
Shanghai, 200240, P.R.C.

Abstract

Suppose m and t are integers such that $0 < t \leq m$, an (m,t)-splitting system is a pair $(X,\mathcal{B})$ that satisfies for every $Y \subseteq X$ with $|Y| = t$, there is a subset B of X in $\mathcal{B}$, such that $|B \cap Y| = \lfloor \frac{t}{2} \rfloor$ or $|(X \backslash B) \cap Y| = \lfloor \frac{t}{2} \rfloor$. Suppose m, t_1 and t_2 are integers such that $t_1 + t_2 \leq m$, an (m,t_1,t_2)-separating system is a pair $(X,\mathcal{B})$ which satisfies for every $P \subseteq X$, $Q \subseteq X$ with $|P| = t_1$, $|Q| = t_2$ and $P \cap Q = \emptyset$, there exists a block $B \in \mathcal{B}$ for which either $P \subseteq B$, $Q \cap B = \emptyset$ or $Q \subseteq B$, $P \cap B = \emptyset$. We will give some results on splitting systems and separating systems for $t = 5$ and $t = 6$.

Keywords: splitting system, separating system, block, construction, bound

1 Introduction

Recently, splitting systems were used by Stinson in [1] and were further defined and discussed in [2] by Alan C.H. Ling et al. who present us many interesting and new results on splitting systems and separating systems which are mainly concentrated on the case $t = 2$ and 4. D.Deng et al. studied the case for $t = 3$ in [3]. In this paper we study the case for $t = 5, 6$ and we also give a generalization to Theorem 2.17 in [2] and some new

*Correspondent author; Email:ahnulxy@163.com; Thanks for the financial support from SUFE PHD Innovative Fund No.CXJJ-2011-385.

results on the general case. First we define splitting system and separating system.

2 Definitions

Definition 2.1 (Splitting System). *Suppose m and t are integers such that $0 < t \leq m$, an (m,t)-splitting system is a pair $(X,\mathcal{B})$ that satisfies the following two properties:*

(1) $|X| = m < \infty$, i.e. X is a set with m elements,

(2) for every $Y \subseteq X$ with $|Y| = t$, there is a subset B of X in $\mathcal{B}$ such that

$|Y \cap B| = \lfloor \frac{t}{2} \rfloor$ *or* $|(X \backslash B) \cap Y| = \lfloor \frac{t}{2} \rfloor$.

In Definition 1, we call block B splits Y if B satisfies *(2)*. We will also say that $(X,\mathcal{B})$ is a t-splitting system and use the notation $(N;m,t)$-*SS* to denote an (m,t)-splitting system having N blocks, i.e. if $(X,\mathcal{B})$ is an $(N;m,t)$-*SS*, then $|X| = m$, $|\mathcal{B}| = N$.

Definition 2.2 (Uniform Splitting System). *Suppose m and t are integers such that $0 < t \leq m$, an uniform (m,t)-splitting system is an (m,t)-splitting system in which every block has cardinality $\lfloor \frac{m}{2} \rfloor$.*

We use notation $(N;m,t)$-*USS* to denote an uniform (m,t)-splitting system having N blocks.

Next we will introduce another important definition: separating system used by Friedman et al. [4] and further defined in [2]. Here we give the definition of separating system with slightly differences with the one in [2]. First we do not restricting m to be an even integer. Second we do not specify each block size to be uniform, i.e. the same size. Actually, what those called separating systems in [2] are now be called uniform separating systems. We now define it.

Definition 2.3 (Separating System). *Suppose m, t_1 and t_2 are integers such that $t_1 + t_2 \leq m$, an (m,t_1,t_2)-separating system is a pair $(X,\mathcal{B})$ which satisfies the following two properties:*

(1) $|X| = m < \infty$,

(2) for every $P \subseteq X$, $Q \subseteq X$ with $|P| = t_1, |Q| = t_2$ and $P \bigcap Q = \emptyset$, there exists a block $B \in \mathcal{B}$ for which either $P \subseteq B, Q \bigcap B = \emptyset$ or $Q \subseteq B, P \bigcap B = \emptyset$.

We will use the notation (m,t_1,t_2)-*SEPS* to denote an (m,t_1,t_2) - separating system. We also say that $(X,\mathcal{B})$ is an (t_1,t_2)-separating system.

Definition 2.4 (Uniform Separating System). *An uniform (m,t_1,t_2)-separating system is an (m,t_1,t_2)-separating system in which every block has cardinality $\lfloor \frac{m}{2} \rfloor$.*

We will use the notation (m, t_1, t_2)-*USEPS* to denote an uniform (m, t_1, t_2)-separating system.

Most constructions of splitting systems are conveniently described by using incidence matrix which will be defined below.

Definition 2.5 (Incidence Matrix). *Let $(X, \mathcal{B})$ be an $(N; m, t)$-SS where $X = \{x_i : 1 \le i \le m\}$ and $\mathcal{B} = \{B_j : 1 \le j \le N\}$, the incidence matrix of $(X, \mathcal{B})$ is the $m \times N$ matrix $\mathbf{A} = (a_{i,j})$ where*

$$a_{i,j} = \begin{cases} 1 & \text{if } x_i \in B_j, \\ 0 & \text{otherwise.} \end{cases} \tag{1}$$

Obviously, $\mathbf{A}$ is an (0,1)-matrix. A column in $\mathbf{A}$ represents a block in $\mathcal{B}$, so we always call a column in $\mathbf{A}$ a block of $(X, \mathcal{B})$.

Example 2.1. *For any set X and integer t with $0 < t < |X| < \infty$, then $(X, 2^X)$ is $(|X|, t)$-SS where 2^X is the power set of X.*

Example 2.2. *Let $X = \{1, 2, 3, 4\}$, $\mathcal{B} = \{\{1, 2\}, \{2, 3\}, \{3, 4\}\}$, then $(X, \mathcal{B})$ is an $(3; 4, 2)$-USS. The incidence matrix is an 4×3 matrix as follows:*

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Example 2.3. *Let $X = \{1, 2, 3, \cdots, m+1\}$, $m \in \mathbb{Z}^+$, $\mathcal{B} = \{\{1, 2, \cdots, \lfloor \frac{m}{2} \rfloor\}, \{\lfloor \frac{m}{2} \rfloor + 1, \cdots, m\}\}$. It is easy to check that $(X, \mathcal{B})$ is an $(2; m+1, m)$-SS. The incidence matrix is an $(m+1) \times 2$ matrix as follows:*

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \\ \cdots & \cdots \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ \cdots & \cdots \\ 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

In fact, if we take any two disjoint $\lfloor \frac{m}{2} \rfloor$-subsets of X, we actually get an $(2; m+1, m)$-USS.

3 Constructions With Separating System

In this section, we want to use separating system constructions used by Ling et al. in [2] and by Friedman in [5]. This paper is mostly interested in systems that are both (2,2) separating and 5-splitting and both (2,3) separating and 6-splitting. We suppose that all t_i, $i = 1, 2, 3$ and t, m, i, j, k, l, n used in the rest of the paper are positive integers.
First we give some basic results about separating systems which will be useful in the constructions of splitting systems later in the paper. The proof will be omitted if it is obvious. Lemma 3.1 is a restatement of Lemma 2.3 in [2].

Lemma 3.1. *If $(X, \mathcal{B})$ is an (m, t_1, t_2)-USEPS and $0 < t_3 \leq t_2$, then it is an (m, t_1, t_3)-USEPS.*

Lemma 3.2. *If $(X, \mathcal{B})$ is an (m, t_1, t_2)-USEPS and $|t_1 - t_2| \leq 1$, then it is an $(m, t_1 + t_2)$-USS.*

Proof. We need to check for any $Y \subseteq X$ with $|Y| = t_1 + t_2$, there is a block $B \in \mathcal{B}$, such that $|Y \cap B| = \lfloor \frac{t_1+t_2}{2} \rfloor$ or $|(X \backslash B) \cap Y| = \lfloor \frac{t_1+t_2}{2} \rfloor$. Without loss of generality, let $t_1 \geq t_2$, thus we have $t_1 = t_2$ or $t_1 = t_2 + 1$. In other hand, since $(X, \mathcal{B})$ is an (m, t_1, t_2)-USEPS, so if we let $Y = P \cup Q$ where $P \cap Q = \emptyset, P, Q \subseteq X$ and $|P| = t_1, |Q| = t_2$, then there exists a block $B \in \mathcal{B}$ such that $P \subseteq B$, $Q \cap B = \emptyset$ or $Q \subseteq B$, $P \cap B = \emptyset$. So we get $|Y \cap B| = |Q| = t_2 = \lfloor \frac{t_1+t_2}{2} \rfloor$ or $|(X \backslash B) \cap Y| = |Q| = t_2 = \lfloor \frac{t_1+t_2}{2} \rfloor$. □

Remark 3.1. In Lemma 3.2, if $t_1 = t_2$, we have the following corollary.

Corollary 3.1. *If there exists an (m, t, t)-USEPS, then there is an $(m, 2t)$-USS.*

Lemma 3.3. *If there exists an $(m, 2, 3)$-USEPS on b blocks, then there is an $(b - 9; m, 5)$-USS.*

Proof. Consider the subset $\{i, j, k, l, n\}$. The pairs of the sets :

$$(\{i,j\},\{k,l,n\}),\ (\{i,k\},\{j,l,n\}),\ (\{i,l\},\{j,k,n\}),\ (\{i,n\},\{k,l,j\}),$$
$$(\{j,k\},\{i,l,n\}),\ (\{j,l\},\{i,k,n\}),\ (\{j,n\},\{i,k,l\}),\ (\{k,l\},\{i,j,n\}),$$
$$(\{k,n\},\{i,j,l\}),\ (\{l,n\},\{i,j,k\})$$

must be separated in the separating system in ten distinct blocks. Then if only nine blocks are deleted, the system must still splits $\{i, j, k, l, n\}$. □

Lemma 3.4 is a generalization of Lemma 3.3.

Lemma 3.4. *If there exists an (m, t_1, t_2)-USEPS having $|t_1 - t_2| \leq 1$ on b blocks, then there is an $(m, t_1 + t_2)$-USS on $b - \binom{t_1 + t_2}{\lfloor \frac{t_1+t_2}{2} \rfloor} + 1$ blocks.*

Proof. Let $\alpha = \lfloor \frac{t_1+t_2}{2} \rfloor, \beta = t_1 + t_2$. Consider the subset $\{i_1, \cdots, i_\beta\}$. The pairs of the sets of the form $(\{j_1, \cdots, j_\alpha\}, \{j_{\alpha+1}, \cdots, j_\beta\})$ which was chosen from the subset must be separated in the separating system in $\binom{\beta}{\alpha}$ distinct blocks since the total number of the pairs is $\binom{\beta}{\alpha}$. Then if only $\binom{\beta}{\alpha}$-1 blocks are deleted, the system must still splits $\{i_1, \cdots, i_\beta\}$. □

Lemma 3.5. *If there exists an $(m, 2, 3)$-USEPS on b blocks with $m > 4$, then there is an $(m, 2, 2)$-USEPS on $b - 1$ blocks.*

We now prove a general case from Lemma 3.5 as follows.

Lemma 3.6. *If there exists an (m, t_1, t_2)-USEPS on b blocks with $t_1 + t_2 \leq m$, there exists an $(m, t_1 - 1, t_2)$-USEPS and $(m, t_1, t_2 - 1)$-USEPS on $b - 1$ blocks.*

Proof. Delete one block from the (m, t_1, t_2)-*USEPS*. Consider an $(t_1 + t_2 - 1)$-subset $\{i_1, \cdots, i_{t_1+t_2-1}\}$. If $i_1, \cdots, i_{t_1-1}$ are in the deleted block and $i_{t_1}, \cdots, i_{t_1+t_2-1}$ are not, i.e. in the complement of the deleted block, then $\{i_1, \cdots, i_{t_1+t_2-1}\}$ may no longer separated by the new system. However, let n be another element in the block containing $i_1, \cdots, i_{t_1-1}$, then the previous system must separate $\{i_1, \cdots, i_{t_1-1}; i_{t_1}, \cdots, i_{t_1+t_2-1}, n\}$ in some other block other than the deleted block. In this block $\{i_1, \cdots, i_{t_1+t_2-1}\}$ is separated by the new system. □

Lemma 3.7 ([2] Lemma2.6). *Suppose $m > 4$, if $(X, \mathcal{B})$ is $(m, 2, 2)$-USEPS on b blocks, then there exists an $(m, 2, 1)$-USEPS on $b - 1$ blocks.*

From Lemma 3.7 and Lemma 3.5, we get the following one lemma.

Lemma 3.8. *Suppose $m > 4$, if $(X, \mathcal{B})$ is an $(m, 2, 3)$-USEPS on b blocks, there exists an $(m, 2, 1)$-USEPS on $b - 2$ blocks.*

From Lemma 3.2 and Lemma 3.5, we get the following one lemma.

Lemma 3.9. *Suppose $m > 4$, if $(X, \mathcal{B})$ is an $(m, 2, 3)$-USEPS on b blocks, then there exists an $(m, 2, 2)$-USEPS on $b-1$ blocks which is also an $(m, 5)$-USS.*

From Lemma 3.2 and Lemma 3.6, we get the following one lemma.

Lemma 3.10. *Suppose $m > 4$, if $(X, \mathcal{B})$ is an (m, t_1, t_2)-USEPS on b blocks and $t_1 + t_2 \leq m$, $|t_1 - t_2| \leq 1$, then there exists an $(m, t_1 - 1, t_2)$-USEPS and $(m, t_1, t_2 - 1)$-USEPS on $b-1$ blocks which is also an $(m, t_1 + t_2)$-USS.*

Lemma 3.11 give a lower boundary to the number of blocks contains in a separating system.

Lemma 3.11. *Suppose $m > 4$, if $(X, \mathcal{B})$ is an (m, t, t)-USEPS where $\lfloor \frac{m}{2} \rfloor \geq t$, then*

$$|\mathcal{B}| \geq \left\lceil \left(\binom{m}{t} \right) \Big/ \binom{\lfloor m/2 \rfloor}{t} \right\rceil.$$

Proof. If there exists subsets $\{i_1, \cdots, i_t\}$ and $\{j_1, \cdots, j_t\}$ such that $\{i_1, \cdots, i_t\} \cap \{j_1, \cdots, j_t\} = \emptyset$, but there not exists a block $B \in \mathcal{B}$ such that

$$\{i_1, \cdots, i_t\} \subseteq B, \quad \{j_1, \cdots, j_t\} \cap B = \emptyset$$

and

$$\{j_1, \cdots, j_t\} \subseteq B, \quad \{i_1, \cdots, i_t\} \cap B = \emptyset,$$

then $(X, \mathcal{B})$ is not a separating system. So if $(X, \mathcal{B})$ is a separating system, then the times of distinct t-subset of X occurs in $\mathcal{B}$ must not less than $\binom{m}{t}$. While the occurrence of the t-subset in each block is $\binom{\lfloor m/2 \rfloor}{t}$, thus we have the conclusion. □

For the special case $t = 2$ in Lemma 3.11, we get the following lemma.

Lemma 3.12. *Suppose $m > 4$, if $(X, \mathcal{B})$ is an $(m, 2, 2)$-USEPS, then*

$$|\mathcal{B}| \geq \left\lceil \left(\binom{m}{2} \right) \Big/ \binom{\lfloor m/2 \rfloor}{2} \right\rceil.$$

Theorem 3.1 is an extension of Lemma 1.2 in [2]. Here m is an integer not necessary to be an even integer which was required in [2]. This theorem gives us a direct construction of a certain type of splitting system.

Theorem 3.1. *For all integer $m > 4$ and even integer t with $0 < t \leq m-2$, there exists an $(\lfloor \frac{m+1}{2} \rfloor; m, t)$-USS.*

Proof. We only consider the case m is odd. The case that m is even was proved in Lemma 1.2 [2]. Let

$$X = \{1, 2, 3, \cdots, m\}, \tag{2}$$

$$B_i = \{i, i+1, \cdots, i + \frac{m-1}{2}\}, \ i = 1, 2, \cdots, \frac{m+1}{2}, \tag{3}$$

$$\mathcal{B} = \{B_i : 1 \leq i \leq \frac{m+1}{2}\}. \tag{4}$$

It is easy to check that

$$|B_i| = \frac{m+1}{2}, 1 \leq i \leq m; \ |\mathcal{B}| = \frac{m+1}{2}.$$

We now prove $(X, \mathcal{B})$ is an $(\frac{m+1}{2}; m, t)$-*USS*. We need show for any subset $Y \subseteq X$ with $|Y| = t$, there exists a block $B \in \mathcal{B}$ that splits Y.

Let

$$Y = \{y_1, y_2, y_3, \cdots, y_{t-1}, y_t\},\ y_i < y_j,\ 1 \le i < j \le t. \tag{5}$$

Obviously, we have

$$1 \le y_1 < y_t \le m.$$

First, we assert that there must be a integer $i : \frac{t}{2} \le i \le t$ such that

$$y_i - y_{i-\frac{t}{2}+1} \le \frac{m-3}{2}. \tag{6}$$

Otherwise, if for all $i : \frac{t}{2} \le i \le t$,

$$y_i - y_{i-\frac{t}{2}+1} > \frac{m-3}{2},$$

i.e.

$$y_{i-\frac{t}{2}+1} \le y_i - \frac{m-3}{2} - 1 = y_i - \frac{m-1}{2}.$$

Let $i = t$ and $\frac{t}{2}$, we get

$$y_{\frac{t}{2}+1} \le y_t - \frac{m-1}{2} \le \frac{m+1}{2}, \tag{7}$$

$$y_1 \le y_{\frac{t}{2}} - \frac{m-1}{2} < y_{\frac{t}{2}+1} - \frac{m-1}{2} \le 1, \tag{8}$$

i.e. $y_1 < 1$, this is a contradiction.

Second, let

$$\alpha = max\{i : \frac{t}{2} \le i \le t,\ y_i - y_{i-\frac{t}{2}+1} \le \frac{m-3}{2}\}, \tag{9}$$

$$\beta = min\{i : \frac{t}{2} \le i \le t,\ y_i - y_{i-\frac{t}{2}+1} \le \frac{m-3}{2}\}. \tag{10}$$

Now we construct the block B which will splits Y. There are few cases:

(1) If $y_{\alpha-\frac{t}{2}+1} \le \frac{m+1}{2}$, we choose a block $B \in \mathcal{B}$ that contains $y_{\alpha-\frac{t}{2}+1}$ as its smallest elements, then

$$\{y_{\alpha-\frac{t}{2}+1}, \cdots, y_\alpha\} \subseteq B \text{ and } \{y_{\alpha+1}, \cdots, y_t\} \cap B = \emptyset,$$

thus B splits Y.

(2) If $y_{\alpha-\frac{t}{2}+1} > \frac{m+1}{2}$, then $y_{\frac{t}{2}+1} > \frac{m+1}{2}$ since $\frac{t}{2} \le \alpha \le t$. We need to check y_β.

(a) If $y_\beta \geq \frac{m-1}{2}$, it also easy to check that there is a block $B \in \mathcal{B}$ that contains y_β as its largest elements, then

$$\{y_{\beta-\frac{t}{2}+1}, \cdots, y_\beta\} \subseteq B \text{ and } \{y_{\beta+1}, \cdots, y_t\} \cap B = \emptyset,$$

thus B splits Y.

(b) If $y_\beta < \frac{m-1}{2}$, i.e. $y_\beta \leq \frac{m-3}{2}$, because $\frac{t}{2} \leq \beta < t$ and $y_{\frac{t}{2}+1} > \frac{m+1}{2}$, thus $\beta = \frac{t}{2}$. Since $y_{\frac{t}{2}} - y_1 \leq \frac{m-3}{2}$, we can choose a block B that contains y_1 as its smallest element, then

$$\{y_1, \cdots, y_{\frac{t}{2}}\} \subseteq B \text{ and } \{y_{\frac{t}{2}+1}, \cdots, y_t\} \cap B = \emptyset,$$

then B splits Y. □

Here is one example based on Theorem 3.1.

Example 3.1. *Let* $X = \{1, 2, \cdots, 10\}$, $B_1 = \{1, 2, 3, 4, 5\}$,$B_2 = \{2, 3, 4, 5, 6\}$, $B_3 = \{3, 4, 5, 6, 7\}$, $B_4 = \{4, 5, 6, 7, 8\}$, $B_5 = \{5, 6, 7, 8, 9\}$, $\mathcal{B} = \{B_i : 1 \leq i \leq 5\}$, *then* $(X, \mathcal{B})$ *is an* $(5; 10, t)$*-USS where* $t \in \{2, 4, 6, 8\}$.

Theorem 3.2 gives a quasi doubling construction for 5-splitting system which is similar to the well-known doubling construction used for Hadamard Matrix.

Theorem 3.2. *If there exists an* $(m, 2, 2)$*-USEPS on* b *blocks and which is also an* $(m, 5)$*-USS, then there exists an* $(2m, 5)$*-USS on* b *blocks and an* $(2m, 5)$*-USS that is also an* $(2m, 2, 2)$*-USEPS on* $2b + 1$ *blocks.*

Proof. Let $\mathbf{T}$ be the incidence matrix of the $(m, 5)$*-USS* which is also an $(m, 2, 2)$*-USEPS* on b blocks. Let $\mathbf{T}^c$ be the complement matrix of $\mathbf{T}$, in which 0's and 1's have been interchanged. Then we claim that the following matrix $\mathbf{R}$ is the incidence matrix of an $(2m, 5)$*-USS* that is also an $(2m, 2, 2)$*-USEPS* on $2b + 1$ blocks, and the leftmost b columns of R is incidence matrix of an $(2m, 5)$*-USS*.

$$\mathbf{R} = \begin{array}{c} \begin{matrix} I & II & III \end{matrix} \\ \begin{pmatrix} \mathbf{T} & \mathbf{T} & \mathbf{0} \\ \mathbf{T} & \mathbf{T}^c & \mathbf{1} \end{pmatrix} \end{array}$$

Let the rows (i.e. elements) of $\mathbf{R}$ be labeled $a_1, \cdots, a_m, b_1, \cdots, b_m$ from top to bottom. Let there be three types of columns in $\mathbf{R}$. Type I columns are the first b columns from the left. Type II columns in $\mathbf{R}$ are the next b columns. Type III columns is the last column in the right where $\mathbf{0} = (0, \cdots, 0)^T, \mathbf{1} = (1, \cdots, 1)^T$, i.e. $\mathbf{0}$ and $\mathbf{1}$ are column vectors with m elements are all $0, 1$ respectively.

Let i, j, k, l and n be distinct integers between 1 and m, inclusive. We now prove that every 5-subset is split by some blocks(i.e. columns).

First, we check that the leftmost b columns forms the incidence matrix of $(2m, 5)$-*USS*. There are few cases:

(1) 5-subset of the form $\{a_i, a_j, a_k, a_l, a_n\}$ is split in type I columns. Since a_n and b_n are identical in type I columns, $\{a_i, a_j, a_k, a_l, b_n\}$ is also split in type I columns as is the set $\{a_i, a_j, a_k, b_l, b_n\}$.

(2) 5-subset of the form $\{a_i, a_j, a_k, a_l, b_i\}$ is split in type I columns as $\{a_i, a_j; a_k, a_l\}$ is (2,2) separated there and rows a_i and b_i are identical in those columns. $\{a_i, a_j, a_k, b_l, b_i\}$ is split in type I columns as in those columns a_i and b_i, a_l and b_l are identical.

(3) 5-subset of the form $\{a_i, a_j, a_k, b_j, b_i\}$ is also split in type I columns as $\{a_i; a_j, a_k\}$ is separated there. Since $\mathbf{T}$ is the incidence matrix of $(m, 2, 2)$-*USEPS* and Lemma 3.1 holds $\mathbf{T}$ is also an incidence matrix of $(m, 2, 1)$-*USEPS*, then there exists a block $B \in \mathcal{B}$ such that

$$\{a_i\} \subseteq B, \{a_j, a_k\} \cap B = \emptyset \text{ or } \{a_j, a_k\} \subseteq B, \{a_i\} \cap B = \emptyset.$$

Since a_i,b_i and a_j,b_j are identical in type I columns, we have

$$\{a_i, b_i\} \subseteq B, \{a_j, b_j, a_k\} \cap B = \emptyset \text{ or}$$
$$\{a_j, b_j, a_k\} \subseteq B, \{a_i, b_i\} \cap B = \emptyset,$$

i.e.

$$|\{a_i, a_j, a_k, b_j, b_i\} \cap B| = 2 \text{ or } |\{a_i, a_j, a_k, b_j, b_i\} \cap (X \backslash B)| = 2,$$

then $\{a_i, a_j, a_k, b_j, b_i\}$ is split in type I columns.

These are all distinct cases. So the first b columns of $\mathbf{R}$ from left form the incidence matrix of $(2m, 5)$-*USS*.

Second, we prove that $\mathbf{R}$ is the incidence matrix of an $(2m, 2, 2)$-*USEPS*. We have few cases:

(1) It is easy to check 4-subset of the form $\{a_i, a_j, a_k, a_l\}$, $\{a_i, a_j, a_k, b_l\}$, $\{a_i, a_j, b_k, b_l\}$ are (2,2) separated all three ways in type I columns. For example, $\{a_i, a_j, a_k, a_l\}$ is separated in $\{a_i, a_j; a_k, a_l\}$,$\{a_i, a_k; a_j, a_l\}$ and $\{a_i, a_l; a_k, a_j\}$ totally in three ways since $\mathbf{T}$ is the incidence matrix of the of $(m, 2, 2)$-*USEPS*.

(2) 4-subset of the form $\{a_i, a_j, a_k, b_i\}$,$\{a_i, a_j, b_k, b_i\}$ and $\{a_i, a_j, b_j, b_i\}$ deserve detailed discussion.

- $\{a_i, a_j, a_k, b_i\}$. $\{a_i, a_j; a_k, b_i\}$, $\{a_i, a_k; a_j, b_i\}$ are separated in type II columns as $\{a_i, a_j; a_k\}$, $\{a_i, a_k; a_j\}$ is respectively separated there and a_i, b_i have opposite value there. $\{a_i, b_i; a_k, a_j\}$ is separated in type I columns as $\{a_i; a_j, a_k\}$ is separated there and a_i, b_i are identical.
- $\{a_i, a_j, b_k, b_i\}$. $\{a_i, a_j; b_k, b_i\}$ is separated in type III columns. $\{a_i, b_i; a_j, b_k\}$ is separated in type I columns. The reason for $\{a_i, b_k; a_j, b_i\}$ is separated in type II columns as follows: on one hand, $\{a_i; a_j, a_k\}$ is separated in $\mathbf{T}$, then there exists a block $B \in \mathcal{B}$ such that

  $$\{a_i\} \subseteq B, \{a_j, a_k\} \cap B = \emptyset \text{ or } \{a_j, a_k\} \subseteq B, \{a_i\} \cap B = \emptyset.$$

  On the other hand, a_i, b_i and a_k, b_k has opposite value in type II columns, thus we have

  $$\{a_i, b_k\} \subseteq B, \{a_j, b_i\} \cap B = \emptyset \text{ or } \{a_j, b_i\} \subseteq B, \{a_i, b_k\} \cap B = \emptyset.$$

- $\{a_i, a_j, b_j, b_i\}$. $\{a_i, a_j; b_j, b_i\}$ is separated in type III columns. $\{a_i, b_i; a_j, b_j\}$ is separated in type I columns as $\{a_i, a_j\}$ is separated there. $\{a_i, b_j; a_j, b_i\}$ is separated in type II columns.

These are all distinct cases. □

If we denote by $TT(N; m, 5)$ an $(m, 5)$-*USS* on N blocks which is also an $(m, 2, 2)$-*USEPS*, and denote by $T(m, 5)$ the minimum N over all $TT(N; m, 5)$. Now we have the following two corollaries:

Corollary 3.2. $T(2^m q, 5) \leq 2T(2^{m-1} q, 5) + 1$ *for* q *odd.*

Corollary 3.3. $T(2^m, 5) \leq 2^m - 1$.

Proof. From Theorem 3.2 we can easily get the recurrence in Corollary 3.2. Solve the recurrence and let $q = 1$ to get Corollary 3.3. □

We have a similar result for $(m, 6)$-*USS*.

Theorem 3.3. *If there exists an* $(m, 2, 3)$-*USEPS on* b *blocks and which is also an* $(m, 6)$-*USS, and there exists an* $(m, 1, 2)$-*USEPS on* c *blocks, then there exists an* $(2m, 6)$-*USS on* $b + 1$ *blocks and an* $(2m, 6)$-*USS that is also an* $(2m, 2, 2)$-*USEPS on* $b + c + 1$ *blocks.*

Proof. Let $\mathbf{T}, \mathbf{S}$ be the incidence matrix of

$$(m, 2, 3)\text{-}USEPS\ ,\ (m, 1, 2)\text{-}USEPS$$

respectively where $(m, 2, 3)$-*USEPS* is also an $(m, 6)$-*USS*. Obviously $\mathbf{T}$ is $m \times b$ matrix and $\mathbf{S}$ is $m \times c$ matrix. Now we construct the incidence matrix, $\mathbf{R}$ of required systems as follows:

$$\mathbf{R} = \begin{array}{c} \begin{matrix} I & II & III \end{matrix} \\ \begin{pmatrix} \mathbf{T} & \mathbf{S} & \mathbf{0} \\ \mathbf{T} & \mathbf{S^c} & \mathbf{1} \end{pmatrix} \end{array}$$

where $\mathbf{S^c}$ is the complement matrix of $\mathbf{S}$ in which 0's and 1's have been interchanged. Obviously $\mathbf{R}$ is $2m \times (b + c + 1)$ matrix. Then we claim that the above matrix $\mathbf{R}$ is the incidence matrix of an $(2m, 6)$-*USS* that is also an $(2m, 2, 2)$-*USEPS* on $b + c + 1$ blocks and that the leftmost b columns and the rightmost one column constitute the incidence matrix of $(2m, 6)$-*USS*.

Let the rows(i.e. elements) of $\mathbf{R}$ be labeled:

$$a_1, \cdots, a_m, \ b_1, \cdots, b_m$$

from top to bottom. Let there be three types of columns in $\mathbf{R}$. Type I columns are the first b columns from the left. Type II columns are next c columns. Type III column is the last column on the right where $\mathbf{0} = (0, \cdots, 0)^T, \mathbf{1} = (1, \cdots, 1)^T$.

First, we prove type I and III columns constitute the incidence matrix of $(2m, 6)$-*USS*, i.e. every 6-subset is split by some blocks. Let i, j, k, l, n, p be distinct integers between 1 and m, inclusive. We have four different cases:

(1) 6-subset of the form $\{a_i, a_j, a_k, a_l, a_n, a_p\}$ is split in type I column since $\mathbf{T}$ is the incidence matrix of $(m, 6)$-*USS*. Since $\{a_p, b_p\}$, $\{a_n, b_n\}$, $\{a_k, b_k\}$, $\{a_l, b_l\}$ are identical in type I columns, the following three forms of 6-subset are also split in type I columns

$$\{a_i, a_j, a_k, a_l, a_n, b_p\}, \{a_i, a_j, a_k, a_l, b_n, b_p\}, \{a_i, a_j, a_k, b_l, b_n, b_p\}.$$

(2) 6-subset of the forms $\{a_i, a_j, a_k, a_l, a_n, b_i\}$, $\{a_i, a_j, a_k, a_l, b_n, b_i\}$ and $\{a_i, a_j, a_k, b_l, b_n, b_i\}$. 5-subset $\{a_i, a_j; a_k, a_l, a_n\}$ is separated in type I columns since $\mathbf{T}$ is the incidence matrix of $(m, 2, 3)$-*USEPS*, i.e. there is a column B in type I such that

$$\{a_i, a_j\} \subseteq B, \ \{a_k, a_l, a_n\} \cap B = \emptyset \ \text{ or}$$
$$\{a_i, a_j\} \cap B = \emptyset, \ \{a_k, a_l, a_n\} \subseteq B.$$

Since a_i and b_i are identical in type I columns, thus

$$\{a_i, a_j, b_i\} \subseteq B,\ \{a_k, a_l, a_n\} \cap B = \emptyset \text{ or}$$
$$\{a_i, a_j, b_i\} \cap B = \emptyset,\ \{a_k, a_l, a_n\} \subseteq B.$$

i.e. B splits $\{a_i, a_j, a_k, a_l, a_n, b_i\}$. Since $\{a_n, b_n\}$, $\{a_l, b_l\}$ are identical in type I columns, thus 6-subsets of the following forms are also split in type I columns: $\{a_i, a_j, a_k, a_l, b_n, b_i\}$ and $\{a_i, a_j, a_k, b_l, b_n, b_i\}$. .

(3) 6-subset of the forms $\{a_i, a_j, a_k, a_l, b_j, b_i\}$ and $\{a_i, a_j, a_k, b_l, b_j, b_i\}$. Applying Lemma 3.1, we know $\mathbf{T}$ is also the incidence matrix of $(m, 2, 2)$-*USEPS* thus there exists a column B in type I columns that separates $\{a_i, a_k; a_j, a_l\}$, i.e.

$$\{a_i, a_k\} \subseteq B,\ \{a_j, a_l\} \cap B = \emptyset \text{ or } \{a_i, a_k\} \cap B = \emptyset,\ \{a_j, a_l\} \subseteq B.$$

Since $\{a_i, b_i\}, \{a_j, b_j\}$ are identical in type I columns, we have

$$\{a_i, a_k, b_i\} \subseteq B,\ \{a_j, a_l, b_j\} \cap B = \emptyset \text{ or}$$
$$\{a_i, a_k, b_i\} \cap B = \emptyset,\ \{a_j, a_l, b_j\} \subseteq B$$

i.e. B splits 6-subset $\{a_i, a_j, a_k, a_l, b_j, b_i\}$. So do 6-subset of the form $\{a_i, a_j, a_k, b_l, b_j, b_i\}$.

(4) 6-subset of the form $\{a_i, a_j, a_k, b_k, b_j, b_i\}$ is split in type III column.

Above are all the distinct cases.

Second, we prove $\mathbf{R}$ is the incidence matrix of $(2m, 2, 2)$-*USEPS*. We have four distinct cases:

(1) 4-subset of the forms $\{a_i, a_j, a_k, a_l\}$, $\{a_i, a_j, a_k, b_l\}$ and $\{a_i, a_j, b_k, b_l\}$. It is easy to check that $\{a_i, a_j, a_k, a_l\}$ is separated in all three ways in type I columns since $\mathbf{T}$ is the incidence matrix of $(m, 2, 2)$-*USEPS*. i.e. $\{a_i, a_j; a_k, a_l\}$, $\{a_i, a_k; a_j, a_l\}$, $\{a_i, a_l; a_j, a_k\}$ are all separated in type I columns. The same is true with the 4-subset of the forms $\{a_i, a_j, a_k, b_l\}$ and $\{a_i, a_j, b_k, b_l\}$.

(2) 4-subset of the form $\{a_i, a_j, a_k, b_i\}$. This 4-subset is separated in all three ways in $\mathbf{R}$.

- $\{a_i, b_i; a_j, a_k\}$ is separated in type I columns. In fact, $\mathbf{T}$ is the incidence matrix of $(m, 1, 2)$-*USEPS*, thus $\{a_i; a_j, a_k\}$ is separated in type I columns, i.e. there exists one column B in type I such that

  $$\{a_i\} \subseteq B,\ \{a_j, a_k\} \cap B = \emptyset \quad \text{or} \quad \{a_i\} \cap B = \emptyset,\ \{a_j, a_k\} \subseteq B.$$

  Since a_i and b_i are identical in type I columns, we have

$$\{a_i, b_i\} \subseteq B,\ \{a_j, a_k\} \cap B = \emptyset \quad \text{or}$$
$$\{a_i, b_i\} \cap B = \emptyset,\ \{a_j, a_k\} \subseteq B.$$

- $\{a_i, a_j; b_i, a_k\}$ is separated in type II columns. $\mathbf{S}$ is the incidence matrix of $(m, 1, 2)$-*USEPS*, so $\{a_i, a_j; a_k\}$ is separated in type II column, i.e. there exists one column B in type II such that

  $$\{a_i, a_j\} \subseteq B,\ \{a_k\} \cap B = \emptyset \quad \text{or} \quad \{a_i, a_j\} \cap B = \emptyset,\ \{a_k\} \subseteq B.$$

  Since a_i and b_i are opposite in type II columns, we have

  $$\{a_i, a_j\} \subseteq B,\ \{b_i, a_k\} \cap B = \emptyset \quad \text{or}$$
  $$\{a_i, a_j\} \cap B = \emptyset,\ \{b_i, a_k\} \subseteq B.$$

- $\{a_i, a_k; b_i, a_j\}$ is separated in type II columns too. In fact, $\{a_i, a_k; a_j\}$ is separated in type II columns since $\mathbf{S}$ is the incidence matrix of $(m, 1, 2)$-*USEPS* and a_i,b_i have opposite value there.

(3) 4-subset of the form $\{a_i, a_j, b_k, b_i\}$. $\{a_i, a_j; b_k, b_i\}$ is separated in type III. $\{a_i, b_i; b_k, a_j\}$ and $\{a_i, b_k; b_i, a_j\}$ are separated in type I and II columns respectively and the reason is the same with (2).

(4) 4-subset of the form $\{a_i, a_j, b_j, b_i\}$. $\{a_i, a_j; b_j, b_i\}$ is separated in type III. $\{a_i, b_i; b_j, a_j\}$ and $\{a_i, b_j; b_i, a_j\}$ are separated in type I and II columns respectively and again the reason is the same with (2).

These are all distinct cases. □

Next, we generalize a theorem Friedman et al.[5] of separating system on the case $t = 5$.

Theorem 3.4. *Suppose m_1, m_2 be even integers, if there exists an $(m_1, 5)$-USS on b_1 blocks which is also an $(m_1, 2, 2)$-USEPS, and there exists an $(m_2, 5)$-USS on b_2 blocks which is also an $(m_2, 2, 2)$-USEPS such that $pm_1 = qm_2$ where $q, p \in \mathbb{Z}^+$ and $2 < p \leq m_2$, then*

(1) there exists an $(pm_1, 5)$-USS on $b_1 + b_2$ blocks;

(2) if q, p satisfies: $q \leq 2, p|m_2$, then there exists an $(pm_1, 2, 2)$-USEPS on $b_1 + 2b_2$ blocks which is also an $(pm_1, 5)$-USS.

Proof. Let $\mathbf{S_1}$ and $\mathbf{S_2}$ be the incidence matrix of $(m_1, 5)$-*USS* and $(m_2, 5)$-*USS* respectively. Obviously $\mathbf{S_1}$ is the $m_1 \times b_1$ matrix and $\mathbf{S_2}$ is $m_2 \times b_2$ matrix.

(1) We now construct the incidence matrix $\mathbf{R}$ of the required system as follows:

$$\mathbf{R} = \begin{array}{c} \begin{matrix} I & II \end{matrix} \\ \begin{pmatrix} \mathbf{S_{11}} & \mathbf{S_2} \\ \mathbf{S_{21}} & \mathbf{S_2} \\ \vdots & \vdots \\ \mathbf{S_{m_1 1}} & \mathbf{S_2} \end{pmatrix} \end{array}.$$

$\mathbf{R}$ consists of two types of columns. Type I columns contain the matrices $\mathbf{S}_{11}, \cdots, \mathbf{S}_{m_1 1}$ where $\mathbf{S}_{i1}$ contains p copies of the ith row of $\mathbf{S}_1$. Type II columns contains q copies of $\mathbf{S}_2$. There are b_1 and b_2 columns of type I and type II respectively. Thus $\mathbf{R}$ is $(pm_1) \times (b_1 + b_2)$ matrix. We claim $\mathbf{R}$ is the incidence matrix of $(pm_1, 5)$-*USS*.

First, it is easy to check every column in $\mathbf{R}$ has the same cardinality of $pm_1/2 (= qm_2/2)$.

Second, we need to verify every 5-subset is split in $\mathbf{R}$. Let i, j, k, l, n be distinct rows in $\mathbf{R}$. There 7 distinct cases as illustrated below:

$$\begin{aligned} 5 &= 1+1+1+1+1 && (11)\\ &= 2+1+1+1 && (12)\\ &= 2+2+1 && (13)\\ &= 3+1+1 && (14)\\ &= 3+2 && (15)\\ &= 4+1 && (16)\\ &= 5+0 && (17) \end{aligned}$$

where $5+0$ represents 5 rows come from one $\mathbf{S}_{d1} (1 \le d \le m_1)$. $4+1$ represents 4 out of 5 rows come from one $\mathbf{S}_{d1}$, the other one come from $\mathbf{S}_{e1} (1 \le e \le m_1, d \ne e)$ and so on and so forth. We discuss each of them in sequence. Suppose d, e, f used below are mutually distinct integers and satisfies:$1 \le d, e, f \le m_1$.

1) If the 5 rows come from different $\mathbf{S}_{d1}$, it is obvious that $\{i, j, k, l, n\}$ is split in type I columns.
2) If i, j come from one $\mathbf{S}_{d1}$, the other three rows come from three different $\mathbf{S}_{e1}$. $\{i, k; l, n\}$ is separated in type I column since $\mathbf{S}_1$ is the incidence matrix of $(m_1, 2, 2)$-*USEPS*, thus $\{i, j, k, n, l\}$ is split in type I columns.
3) If i, j come from one $\mathbf{S}_{d1}$, k, n from $\mathbf{S}_{e1}$, and l from $\mathbf{S}_{f1}$. Then i, j are identical in type I columns as are the k, n. $\{i, l; n\}$ is separated in type I columns and thus $\{i, j, k, n, l\}$ is split in type I columns.

4) If i,j,k come from one $\mathbf{S}_{d1}$, n from $\mathbf{S}_{e1}$, l from $\mathbf{S}_{f1}$. i,j,k are identical in type I columns. $\{i;l,n\}(\{j;l,n\}$ or $\{k;l,n\})$ is separated in type I columns since $\mathbf{S}_1$ is the incidence matrix of $(m_1,1,2)$-*USEPS*. Thus $\{i,j,k,n,l\}$ is split in type I columns.

5) If i,j come from one $\mathbf{S}_{d1}$, and the other three from one $\mathbf{S}_{e1}$. $\{i;k\}$ is separated in type I columns thus $\{i,j,k,n,l\}$ is split in type I columns.

6) If i,j,k,l come from $\mathbf{S}_{d1}$, n from $\mathbf{S}_{e1}$. Since $p \leq m_2$ then $\{i',j',k',l'\}$ must be distinct rows of $\mathbf{S}_2$ where $\{i',j',k',l'\}$ stands for the rows when $\{i,j,k,l\}$ limited to type II columns. If n' is distinct from any rows in $\{i',j',k',l'\}$, then $\{i',j',k',l',n'\}$ is split in type II columns. If n' is the same with one rows in $\{i',j',k',l'\}$, say n' is the same to i'. Then $\{i',j';k',l'\}$ is separated in type II columns and furthermore $\{i',j',n';k',l'\}$ is also separated there. Thus $\{i,j,k,l,n\}$ is split in type II columns.

7) If $\{i,j,k,n,l\}$ from the same one $\mathbf{S}_{d1}$, $\{i,j;k,l,n\}$ is separated in type II columns so $\{i,j,k,n,l\}$ is split in type II columns.

(2) When $q=1$, $pm_1 = m_2$ it is the obvious case. We only discuss the case $q=2$. We now construct the incidence matrix of required system as follows:

$$\mathbf{T} = \begin{array}{c} \begin{array}{ccc} I & II & III \end{array} \\ \begin{pmatrix} \mathbf{S_{11}} & \mathbf{S_2} & \mathbf{S_2} \\ \vdots & & \\ \mathbf{S_{m_1 1}} & \mathbf{S_2} & \mathbf{S_2^c} \end{pmatrix} \end{array}.$$

$\mathbf{T}$ consists of three types of columns. Type I columns contain the matrices $\mathbf{S}_{11},\cdots,\mathbf{S}_{m_1 1}$, where $\mathbf{S}_{i1}$ contains p copies of the ith row of $\mathbf{S}_1$. Type II columns contains 2 copies of $\mathbf{S}_2$. Type III columns contains 2 matrices: $\mathbf{S}_2$ and $\mathbf{S}_2^c$ where $\mathbf{S}_2^c$ is the complement matrix of $\mathbf{S}_2$. We claim $\mathbf{T}$ is the incidence matrix of $(pm_1,2,2)$-*USEPS* on b_1+2b_2 blocks which is also an $(pm_1,5)$-*USS*.

First, the first two types of columns is the incidence matrix of $(pm_1,5)$-*USS* as we have proved in (1). Second, we check $\mathbf{T}$ is the incidence matrix of $(pm_1,2,2)$-*USEPS*. Let $\{i,j,k,l\}$ be distinct rows from $\mathbf{T}$, There are five distinct cases as illustrated below:

$$4 = 4+0 \tag{18}$$
$$= 3+1 \tag{19}$$
$$= 2+2 \tag{20}$$
$$= 2+1+1 \tag{21}$$
$$= 1+1+1+1. \tag{22}$$

Let $\{i', j', k', l'\}$, $\{i'', j'', k'', l''\}$ be the rows when limit $\{i, j, k, l\}$ to type II and III. Let us see if $\{i, j; k, l\}$ is separated by a column of $\mathbf{T}$.

1) If $\{i, j, k, l\}$ come from one $\mathbf{S}_{d1}$. Since $p \leq m_2$, then $\{i', j', k', l'\}$ must be distinct rows of $\mathbf{S}_2$. Every 4-subset is separated in all three ways by $\mathbf{S}_2$, thus $\{i, j; k, l\}$ is separated in type II columns.

2) If i, j, k come from one $\mathbf{S}_{d1}$, l from another, say $\mathbf{S}_{e1}$. If l' is not identical to any one of i', j', k' or $l' = k'$(we mean l' is identical to k' in type II columns), then $\{i', j'; k', l'\}$ is separated in type II columns. So $\{i, j; k, l\}$ is separated in type II columns too. If l' is identical to i' or j', say $l' = i'$ (or j'), then l'' is opposite to i''(or j''). Let $\{i'', j'', k''\}$ be in the first m_2 rows of type III columns. Type II and III columns only have 2 matrices, then l'' must be in the last m_2 rows of type III columns. So $\{i'', j''; k''\}$ is separated in type III columns. Since l'' and i'' have opposite value in type III columns, $\{i'', j''; k'', l''\}$ is separated in type III columns and so does $\{i, j; k, l\}$.

3) If i, j, k, l come from different $\mathbf{S}_{d1}$. Obviously, $\{i, j; k, l\}$ is separated in type I columns.

4) If i, j come from one $\mathbf{S}_{d1}$, k from $\mathbf{S}_{e1}$ and l from $\mathbf{S}_{f1}$. It is easy to check that $\{i; k, l\}$ is separated in type I columns, so it is $\{i, j; k, l\}$.

   If i, k come from S_{d1}, j from $\mathbf{S}_{e1}$ and l from $\mathbf{S}_{f1}$. If $\{i', j', k', l'\}$ are mutually distinct or $i' = j'$(then $l' \neq i'$) or $l' = k'$ in type II columns, then $\{i, j; k, l\}$ is separated in type II columns.

   If $k' = j'$ and $i' = l'$, then i'', l'' and j'', k'' have opposite value in type III columns. Since $\{i''; k''\}$ is separated in type III columns, thus $\{i, j; k, l\}$ is separated in type III columns.

   If $k' = j'$ but $i' \neq l'$, then one of k'' and j'' must come from $\mathbf{S}_2$, the other come from $\mathbf{S}_2^c$ in type III columns. Let i'', k'' come from the first m_2 rows of type III columns, j'', l'' come from last m_2 rows of type III columns. We use l''_{S_2} to denote the row in $\mathbf{S}_2$ correspondent to the row l'' in $\mathbf{S}_2^c$. It is easy to check that $\{i'', l''_{S_2}; k''\}$ is $(2, 1)$ separated by one column, say, B in type III column since $\mathbf{S}_2$ is the incidence matrix of $(pm_1, 2, 1)$-*USEPS*, i.e.

$$\{i'', l''_{S_2}\} \subseteq B, \ \{k''\} \cap B = \emptyset$$

   or

$$\{k''\} \subseteq B, \ \{i'', l''_{S_2}\} \cap B = \emptyset.$$

   So

$$\{i'', j''\} \subseteq B, \ \{k'', l''\} \cap B = \emptyset$$

or

$$\{k'', l''\} \subseteq B,\ \{i'', j''\} \cap B = \emptyset.$$

i.e. $\{i, j; k, l\}$ is separated in $\mathbf{T}$.

If $k' \neq j'$ but $i' = l'$, the case is similar to the case $k' = j'$ but $i' \neq l'$ which was proved above. If $j' = l'$, then j' and l' come from different $\mathbf{S}_2$ in type II columns. Let i'', j'', k'' come from the first m_2 rows in type III columns, then l'' come from the last m_2 rows in type III columns. Since $\{i'', j''; k''\}$ is separated in type III columns, j'' and l'' have opposite value in type III columns, thus $\{i'', j''; k'', l''\}$ is separated there and so is $\{i, j; k, l\}$.

5) If i, j come from one $\mathbf{S}_{d1}$ and k, l come from one $\mathbf{S}_{e1}$. Since $\{i; k\}$ is separated in type I columns, then $\{i, j; k, l\}$ is separated there too. If i, k come from one $\mathbf{S}_{d1}$ and j, l come from one $\mathbf{S}_{e1}$. If i', j', k', l' are mutually different or $i' = j'$(then $l' \neq i'$) or $l' = k'$, then $\{i, j; k, l\}$ is separated in type II. If $k' = j'$ or $i' = l'$ or $l' = j'$, we have three different cases similar to the case 3):

$k' = j'$ and $i' = l'$,
$k' = j'$ but $i' \neq l'$,
$k' \neq j'$ but $i' = l'$. □

For $t = 6$, Theorem 3.4 seems to be much more complicated and we can only get part of the results as follows.

Theorem 3.5. *If there exists an* $(m_1, 2, 3)$*-USEPS on* b_1 *blocks which is also an* $(m_1, 6)$*-USS and there exists an* $(m_2, 2, 3)$*-USEPS on* b_2 *blocks which is also an* $(m_2, 6)$*-USS such that* $pm_1 = qm_2$ *where* $q, p \in \mathbb{Z}^+$ *and* $2 < p \leq m_2$*, then there exists an* $(pm_1, 6)$*-USS on* $b_1 + b_2$ *blocks.*

Proof. We now construct the incidence matrix, $\mathbf{R}$ of the required system as follows:

$$\mathbf{R} = \begin{array}{c} \begin{array}{cc} I & II \end{array} \\ \begin{pmatrix} \mathbf{S}_{11} & \mathbf{S}_2 \\ \mathbf{S}_{21} & \mathbf{S}_2 \\ \vdots & \vdots \\ \mathbf{S}_{m_1 1} & \mathbf{S}_2 \end{pmatrix} \end{array}$$

which consists of the same types of columns as stated in Theorem 3.4(1).

As have done before, we illustrated different cases as follows:

$$
\begin{aligned}
6 &= 6+0 && (23)\\
&= 5+1 && (24)\\
&= 4+2 && (25)\\
&= 4+1+1 && (26)\\
&= 3+3 && (27)\\
&= 3+2+1 && (28)\\
&= 3+1+1+1 && (29)\\
&= 2+2+2 && (30)\\
&= 2+2+1+1 && (31)\\
&= 2+1+1+1+1 && (32)\\
&= 1+1+1+1+1+1. && (33)
\end{aligned}
$$

We have totally 11 different cases. The proof will be easy but verbose. It is much more like what we have done in Theorem 3.4, so we omit it. □

4 Existence and Bounds

We now show the existence and bounds of splitting and separating systems. The following one theorem is the generalization of Theorem 2.17 in [2].

Theorem 4.1. *For a given integer $t \geq 2$, there exists*

(1) an (m,t)-USS on b blocks where b and t satisfies

$$I = \binom{m}{\lfloor \frac{m}{2} \rfloor}^b - \binom{m}{t} r^b > 0, \text{where}$$

$$r = \begin{cases} \binom{m}{\lfloor \frac{m}{2} \rfloor} - \binom{t}{\frac{t}{2}} \binom{m-t}{\lfloor \frac{m}{2} \rfloor - \frac{t}{2}} & t \text{ even,} \\ \binom{m}{\lfloor \frac{m}{2} \rfloor} - \binom{t}{\frac{t-1}{2}} \left(\binom{m-t}{\lfloor \frac{m}{2} \rfloor - \frac{t-1}{2}} + \binom{m-t}{\lfloor \frac{m}{2} \rfloor - \frac{t+1}{2}} \right) & t \text{ odd.} \end{cases} \quad (34)$$

(2) an (m,t)-USEPS on b blocks which is also an $(m, t_1, t_2 - 1)$-USEPS where b and t satisfies

$$J = \binom{m}{\lfloor \frac{m}{2} \rfloor}^b - \binom{m}{t} r^b - s^b \binom{m}{t-1} \binom{t-1}{t_1} > 0, \text{where}$$

$$t = t_1 + t_2,\ s = \binom{m}{\lfloor \frac{m}{2} \rfloor} - \binom{m-t-1}{\lfloor \frac{m}{2} \rfloor - t_1} - \binom{m-t-1}{\lfloor \frac{m}{2} \rfloor - t_2 + 1},\ r \text{ as above.} \tag{35}$$

Proof. (1) Any system of blocks can choose it blocks from a set of $\binom{m}{\lfloor \frac{m}{2} \rfloor}$ distinct blocks. So there are $\binom{m}{\lfloor \frac{m}{2} \rfloor}^b$ systems on b blocks. Since there are $\binom{t}{\frac{t}{2}}\binom{m-t}{\lfloor \frac{m}{2} \rfloor - \frac{t}{2}}$ blocks or $\binom{t}{\frac{t-1}{2}}\binom{m-t}{\lfloor \frac{m}{2} \rfloor - \frac{t-1}{2}} + \binom{t}{\frac{t+1}{2}}\binom{m-t}{\lfloor \frac{m}{2} \rfloor - \frac{t+1}{2}}$ blocks (when t even and odd respectively) that split a particular t-subset, thus we have

$$r = \begin{cases} \binom{m}{\lfloor \frac{m}{2} \rfloor} - \binom{t}{\frac{t}{2}}\binom{m-t}{\lfloor \frac{m}{2} \rfloor - \frac{t}{2}} & \text{for } t \text{ even,} \\ \binom{m}{\lfloor \frac{m}{2} \rfloor} - \binom{t}{\frac{t-1}{2}}\left(\binom{m-t}{\lfloor \frac{m}{2} \rfloor - \frac{t-1}{2}} + \binom{m-t}{\lfloor \frac{m}{2} \rfloor - \frac{t+1}{2}}\right) & \text{for } t \text{ odd.} \end{cases} \tag{36}$$

blocks that do not do the splitting. So there are r^b systems that do not split a particular t-subset. Since there are $\binom{m}{t}$ such t-subset, there $\binom{m}{t}r^b$ systems that do not split some t-subset. Therefore, the number of systems that split every t-subset is $I = \binom{m}{\lfloor \frac{m}{2} \rfloor}^b - \binom{m}{t}r^b$. If $I > 0$, then we have a t-splitting system on b blocks.

(2) We need to count the number of uniform systems that do not separate a particular t_1-subset from a particular $(t_2 - 1)$-subset. There are

$$\binom{m-t+1}{\lfloor \frac{m}{2} \rfloor - t_1} + \binom{m-t+1}{\lfloor \frac{m}{2} \rfloor - t_2 + 1}$$

blocks that do the separating, so there are

$$s = \binom{m}{\lfloor \frac{m}{2} \rfloor} - \binom{m-t+1}{\lfloor \frac{m}{2} \rfloor - t_1} - \binom{m-t+1}{\lfloor \frac{m}{2} \rfloor - t_2 + 1}$$

blocks that do not separate them. So there are s^b systems that do not separate a particular t_1-subset form a particular $t_2 - 1$-subset. Since there are $\binom{m}{t-1}\binom{t-1}{t_1}$ such pairs of t_1-subset and $(t_2 - 1)$-subset. So there

are $s^b\binom{m}{t-1}\binom{t-1}{t_1}$ systems that do not separate some pair of t_1-subset from (t_2-1)-subset. Therefore, if we want a system that is t-splitting and (t_1, t_2-1)-separating, we need

$$J = \binom{m}{\lfloor \frac{m}{2} \rfloor}^b - \binom{m}{t} r^b - s^b \binom{m}{t-1}\binom{t-1}{t_1} > 0.$$

This the desired result. □

Remark 4.1. In Theorem 4.1(2), we can change (m, t_1, t_2-1)-*USEPS* into (m, t_1-1, t_2)-*USEPS* with only slightly change in the proof but without change in results.

For the special case $t = 5$ and 6, we have the following two theorems: Theorem 4.2 and 4.3.

Theorem 4.2. *(1) There exists an* $(m, 5)$-*USS on* $b = \lfloor 3.53 \log_2 m \rfloor + 1$ *blocks.*
(2) There exists an $(m, 5)$-*USS which is also* $(m, 2, 2)$-*USEPS on* $b = \lfloor 25.95 \log_2 m \rfloor + 1$ *blocks.*

Proof. (1) From (34), if

$$I = \binom{m}{\lfloor \frac{m}{2} \rfloor}^b - \binom{m}{t} r^b > 0,$$

then there exists an (m, t)-*USS*. So let $t = 5$ and we get the following inequalities:

$$\binom{m}{5}\left(1 - \frac{5(m+1)(m-1)}{8m(m-2)}\right)^b < 1 \quad \text{for m odd} \tag{37}$$

and

$$\binom{m}{5}\left(1 - \frac{5m(m-2)}{8(m-1)(m-3)}\right)^b < 1 \quad \text{for m even.} \tag{38}$$

Since

$$1 - \frac{5(m+1)(m-1)}{8m(m-2)} < \frac{3}{8},\ 1 - \frac{5m(m-2)}{8(m-1)(m-3)} < \frac{3}{8},\ \binom{m}{5} < m^5,$$

therefore if

$$m^5\left(\frac{3}{8}\right)^b < 1,$$

then there exists a $(m,5)$-*USS* on b blocks. Taking logarithm we get

$$b > \frac{5\log_2 m}{\log_2 \frac{8}{3}},$$

i.e.

$$b > 3.53\log_2 m.$$

(2) From (35), if

$$J = \binom{m}{\lfloor \frac{m}{2} \rfloor}^b - \binom{m}{t} r^b - s^b \binom{m}{t-1}\binom{t-1}{t_1} > 0$$

then there exists an $(m,5)$-*USS* which is also $(m,2,2)$-*USEPS*. We let $t = 5$ and get the following inequalities for m even and odd respectively:

$$\binom{m}{5}\left(1-\frac{5m(m-2)}{16(m-1)(m-3)}\right)^b + 6\binom{m}{4}\left(1-\frac{m(m-2)}{8(m-1)(m-3)}\right)^b < 1 \quad (39)$$

and

$$\binom{m}{5}\left(1-\frac{5(m+1)(m-1)(m-3)}{16m(m-2)(m-4)}\right)^b + 6\binom{m}{4}\left(1-\frac{2(m+1)(m-1)}{16m(m-2)}\right)^b < 1. \quad (40)$$

Since

$$\binom{m}{5} < m^5 \quad \text{and} \quad 6\binom{m}{4} < m^4,$$

$$1 - \frac{5m(m-2)}{16(m-1)(m-3)} < \frac{11}{16} \quad \text{and} \quad 1 - \frac{5(m+1)(m-1)(m-3)}{16m(m-2)(m-4)} < \frac{11}{16},$$

$$1 - \frac{m(m-2)}{8(m-1)(m-3)} < \frac{7}{8} \quad \text{and} \quad 1 - \frac{(m+1)(m-1)}{8m(m-2)} < \frac{7}{8}.$$

So if

$$m^5\left(\frac{11}{16}\right)^b + m^4\left(\frac{7}{8}\right)^b < 1,$$

then there exists an $(m,5)$-*USS* which is also $(m,2,2)$-*USEPS*.
When $m \geq 14$, we have

$$m^5\left(\frac{7}{8}\right)^b < 1.$$

Taking logarithm at both side,

$$b > \frac{5\log_2 m}{\log_2 (\frac{8}{7})},$$

i.e.

$$b > 25.95 \log_2 m.$$

We get the result. □

If we denote by $S(m,t)$ the minimum N over all $(N;m,t)$-*USS*, then Theorem 4.2 gives the following corollary.

Corollary 4.1. *(1)* $S(m,5) \leq \lfloor 3.53 \log_2 m \rfloor + 1$.

(2) $T(m,5) \leq \lfloor 25.95 \log_2 m \rfloor + 1$.

Theorem 4.3. *(1) There exists an* $(m,6)$-*USS on* $b = \lfloor 11.10 \log_2 m \rfloor + 1$ *blocks.*
(2) There exists an $(m,6)$-*USS which is also* $(m,2,3)$-*USEPS on* $b = \lfloor 64.44 \log_2 m \rfloor + 1$ *blocks.*

Proof. (1) Let $t = 6$ in (34), we obtain the following two inequalities:

$$\binom{m}{6}\left(1 - \frac{5m(m-2)(m-4)}{16(m-1)(m-3)(m-5)}\right)^b < 1 \quad \text{for m even}$$

and

$$\binom{m}{6}\left(1 - \frac{5(m+1)(m-1)(m-5)}{16m(m-2)(m-4)}\right)^b < 1 \quad \text{for m odd.}$$

As the same reason we have stated in Theorem 4.2, if

$$m^6\left(\frac{11}{16}\right)^b < 1$$

then we get an $(m,6)$-*USS*. Taking logarithm, we get the desired result.

(2) Let $t = 6$ in (35), we obtain the following two inequalities:

$$\begin{aligned}&\binom{m}{6}\left(1 - \frac{5m(m-2)(m-4)}{16(m-1)(m-3)(m-5)}\right)^b \\ &+ 10\binom{m}{5}\left(1 - \frac{m(m-2)}{16(m-1)(m-3)}\right)^b < 1\end{aligned} \tag{41}$$

for m even and

$$\begin{aligned}&\binom{m}{6}\left(1 - \frac{5(m+1)(m-1)(m-5)}{16m(m-2)(m-4)}\right)^b \\ &+ 10\binom{m}{5}\left(1 - \frac{(m+1)(m-1)(m-5)}{16m(m-2)(m-4)}\right)^b < 1\end{aligned} \tag{42}$$

for m odd. Since

$$\binom{m}{6} < m^6 \quad \text{and} \quad 10\binom{m}{5} < m^5,$$

$$1 - \frac{5m(m-2)(m-4)}{16(m-1)(m-3)(m-5)} < \frac{5}{16} \quad \text{and} \quad 1 - \frac{m(m-2)}{16(m-1)(m-3)} < \frac{15}{16},$$

$$1 - \frac{5(m+1)(m-1)(m-5)}{16m(m-2)(m-4)} < \frac{5}{16} \quad \text{and} \quad 1 - \frac{(m+1)(m-1)(m-5)}{16m(m-2)(m-4)} < \frac{15}{16}.$$

So if

$$m^6\left(\frac{5}{16}\right)^b + m^5\left(\frac{15}{16}\right)^b < 1 \tag{43}$$

is held, then there exists an $(m,6)$-*USS* which is also an $(m,2,3)$-*USEPS*. Again, if

$$m^6\left(\frac{15}{16}\right)^b < 1$$

is held, then (43) is held too. Taking logarithm, we have

$$b > \frac{6\log_2 m}{\log_2\left(\frac{16}{15}\right)},$$

i.e.

$$b > 64.44\log_2 m.$$

We get the desired result. □

Corollary 4.2. *(1)* $S(m,6) \leq \lfloor 11.10\log_2 m \rfloor + 1$.

(2) $T(m,6) \leq \lfloor 64.44\log_2 m \rfloor + 1$.

Next, we will give a definite lower bound for splitting systems. First, let's have a look of existing results on the bounds of splitting systems.

D.R. Stinson in [1] had given an estimation of the bound of splitting systems as follows:

Theorem 4.4. *(Stinson [1]) Let m,t be even integers that satisfies $0 < t < m$, there exists an $(N;m,t)$-USS, if $N \approx c_0 t^{3/2}\log_2 m$ where c_0 is a constant.*

D.Deng and D.R. Stinson et al. proved in [3] that $S(m,t) \geq \lfloor \log_2(m-t+1) \rfloor + 1$ *for all* $m \geq t+1$, in the following section we will give an upper bound for $S(m,t)$.

Let's give two lemmas first.

Lemma 4.1. *For all* $m \geq t+1$, $2^t \binom{m-t}{\lfloor \frac{m}{2} \rfloor - \lfloor \frac{t}{2} \rfloor} > \binom{m}{\lfloor \frac{m}{2} \rfloor}$.

Proof. We only consider the case t, m are both even, the other three cases is similar. Therefore what we want to prove becomes

$$2^t \binom{m-t}{\frac{m-t}{2}} > \binom{m}{\frac{m}{2}}.$$

Divided by $\binom{m}{\frac{m}{2}}$ at both side, we get

$$2^t \frac{(m-t)!}{m!} \left(\frac{(m/2)!}{((m-t)/2)!} \right)^2 > 1,$$

i.e.

$$2^t \frac{\left(\frac{m}{2} \cdot \frac{m-2}{2} \cdot \cdots \cdot \frac{m-t+2}{2}\right)^2}{m(m-1)\cdots(m-t+1)} > 1.$$

Now we only need to prove that

$$\frac{m(m-2)\cdots(m-t+2)}{(m-1)(m-3)\cdots(m-t+1)} > 1.$$

This is obviously true. □

Lemma 4.2. *([1] Lemma 2.2) Suppose* m *and* λm *are both positive integers where* $0 < \lambda < 1$. *Let*

$$H(\lambda) = -\lambda \log_2 \lambda - (1-\lambda) \log_2 (1-\lambda), \tag{44}$$

then

$$\frac{1}{\sqrt{8m\lambda(1-\lambda)}} 2^{mH(\lambda)} \leq \binom{m}{m\lambda} \leq \frac{1}{\sqrt{2\pi m\lambda(1-\lambda)}} 2^{mH(\lambda)}. \tag{45}$$

Remark 4.2. If we let $\lambda = \frac{1}{2}$ in Lemma 4.2, then $H(\lambda) = 1$ and

$$\frac{1}{\sqrt{2m}} 2^m \leq \binom{m}{m/2} \leq \frac{1}{\sqrt{\pi m/2}} 2^m. \tag{46}$$

The following theorem gives a definite improvement of a theorem in [1] as stated above in Theorem 4.4.

Theorem 4.5. *For all* $m \geq t+1 \geq 7$, *we have*

$$S(m,t) \leq \lfloor \sqrt{2} t^{3/2} \log_2 m \rfloor.$$

Proof. Let $c = \left(1 - \binom{t}{\lfloor t/2 \rfloor} \Big/ 2^t\right)^{-1}$, Obviously $c > 0$. We only consider the case t, m are both even integers. From (34), the following inequality is held:

$$\binom{m}{t}\left(1 - \binom{t}{t/2}\binom{m-t}{(m-t)/2} \Big/ \binom{m}{m/2}\right)^b < 1. \tag{47}$$

Applying Lemma 4.1, we know

$$\binom{m-t}{(m-t)/2} \Big/ \binom{m}{m/2} > 1/2^t \quad \text{and} \quad \binom{m}{t} < m^t$$

are held. So if the following inequality is held, then(47) is held too, i.e.

$$m^t\left(1 - \binom{t}{t/2} \Big/ 2^t\right)^b < 1. \tag{48}$$

And finally, if (48) is held, there exists an (m,t)-*USS*. Taking logarithm, we have

$$b > \frac{t \log_2 m}{\log_2 c}.$$

From the primary differential and calculus knowledge, $-\log_2(1-x) > x$ and applying Lemma 4.2, we get

$$\frac{1}{\sqrt{2t}} \leq \binom{t}{t/2} \Big/ 2^t \leq \frac{1}{\sqrt{\pi t/2}},$$

i.e.

$$b \leq \sqrt{2}t^{3/2} \log_2 m,$$

$$S(m,t) \leq \lfloor \sqrt{2}t^{3/2} \log_2 m \rfloor .$$

This is the desired result. □

Acknowledgement

I would like to show my deepest gratitude to my supervisors Prof. Shen Hao and Dr. D.Deng who have provided me with valuable guidance in every stage of the writing of this paper. Without their enlightening instruction, impressive kindness and patience, I could not have completed my thesis. I shall extend my gratitude to my wife, Liu Fangfang, too. Without her consistent encouragement and support, I could not have completed this paper too.

References

[1] D.R. Stinson, Some baby-step giant-step algorithms for the low hamming weight discrete logarithm problem, Mathematics of Computation 2001,71,379-391.

[2] Alan C.H. Ling and P.C Li and G.H.J van Rees, Splitting systems and separating systems, Discrete Mathematics 2004,9(279),355-368.

[3] D.Deng and D.R. Stinson and P.C. Li and G.H.J van Rees and R. Wei, Constructions and Bounds for (m,t)-Splitting Systems, Discrete Mathematics 2004,29(3),307-311.

[4] M.L. Fredman and J.Komlos, On the size of separating systems and families of perfect hash functions, SIAM J. Algebraic Discrete Methods 1984,5,61-68.

[5] A.D. Friedman, R.L. Graham, J.D. Ullman, Universal single transition time asynchronous state assignments, IEEE Trans. Comput. C-18(6)(1969),541-547.

[6] D.R. Stinson, T. van Trung, R. Wei, Secure frameproof codes, key distribution patterns, group testing algorithms and related structures, J. Statist. Plann. Inference 86(2000),595-617.

[7] A.Renyi, On random generating elements of a finite Boolean algebra, Acta Sci. Math. Szeged 22(1961),75-81.

[8] P. Frankl and Z. Füredi, An exact result for 3-graphs, Discrete Mathematics 50 (1984), 323-328.

[9] P. Erdös, P. Frankl and Z.Füredi, Families of finite sets in which no set is covered by the union of two others, Journal of Combinatorial Theory A 33 (1982), 158-166.

[10] P. Erdös and E. Szemerèdi, Combinatorial properties of systems of sets, Journal of Combinatorial Theory A 24 (1978), 308-313.

[11] D. de Caen, Extension of a theorem of Moon and Moser on complete subgraphs, Ars Combinatoria 16 (1983), 5-10.

[12] C.J. Colbourn and J.H. Dinitz. The CRC Handbook of Combinatorial Designs, CRC Press, 1996.