Constructions and Bounds for (m, t)-Splitting Systems

D. Deng and D.R. Stinson
David R. Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario N2L 3G1, Canada

P.C. Li and G.H.J. van Rees
Department of Computer Science
University of Manitoba
Winnipeg, Manitoba R3T 2N2, Canada

R. Wei
Department of Computer Science
Lakehead University
Thunder Bay, Ontario P7B 5E1, Canada

Abstract

Let m and t be positive integers with $t \geq 2$. An (m,t)-*splitting system* is a pair $(X, \mathcal{B})$ where $|X| = m$ and $\mathcal{B}$ is a collection of subsets of X called *blocks*, such that, for every $Y \subseteq X$ with $|Y| = t$, there exists a block $B \in \mathcal{B}$ such that $|B \cap Y| = \left\lfloor \frac{t}{2} \right\rfloor$. An (m,t)-splitting system is *uniform* if every block has size $\left\lfloor \frac{m}{2} \right\rfloor$. In this paper, we give several constructions and bounds for splitting systems, concentrating mainly on the case $t = 3$. We consider uniform splitting systems as well as other splitting systems with special properties, including disjunct and regular splitting systems. Some of these systems have interesting connections with other types of set systems.

1 Introduction

1.1 Definitions

We begin with some definitions.

Definition 1.1 *A* set system *is a pair* $(X, \mathcal{B})$ *that satisfies the following properties:*

1. X *is a finite set of* points,
2. $\mathcal{B}$ *is a collection of subsets of* X, *called* blocks.

Definition 1.2 *Let* m *and* t *be integers such that* $m \geq 0$ *and* $t \geq 2$. *An* (m,t)-splitting system *is a set system* $(X, \mathcal{B})$ *that satisfies the following properties:*

1. $|X| = m$,
2. *for every* $Y \subseteq X$ *with* $|Y| = t$, *there exists a block* $B \in \mathcal{B}$ *such that* $|B \cap Y| = \left\lfloor \frac{t}{2} \right\rfloor$.

We will use the notation $(N;m,t)$-SS to denote an (m,t)-splitting system having N blocks.

Definition 1.3 *Let m and t be positive integers with $t \geq 2$. A* disjunct (m,t)-splitting system *is an (m,t)-splitting system $(X,\mathcal{B})$ such that, for all $x_1, x_2 \in X$, there exists a block $B \in \mathcal{B}$ such that $x_1 \in B$ and $x_2 \notin B$. We will use the notation $(N;m,t)$-disjunct SS to denote a disjunct (m,t)-splitting system having N blocks.*

Definition 1.4 *Let r, m and t be positive integers with $t \geq 2$. An* r-regular (m,t)-splitting system *is an (m,t)-splitting system in which every point occurs in exactly r blocks. We will use the notation $(N;m,t)$-r-regular SS to denote an r-regular (m,t)-splitting system having N blocks.*

Definition 1.5 *Let m and t be positive integers with $t \geq 2$. A* uniform (m,t)-splitting system *is an (m,t)-splitting system in which every block has cardinality $\lfloor \frac{m}{2} \rfloor$. We will use the notation $(N;m,t)$-uniform SS to denote a uniform (m,t)-splitting system having N blocks.*

In [10], uniform (m,t)-splitting systems were considered because of an application in baby-step giant-step algorithms for the so-called low hamming weight discrete logarithm problem. In these baby-step giant-step algorithms, better time complexity can be achieved if the splitting system used has a small number of blocks. In a recent paper, Ling, Li and van Rees [8] began a combinatorial study of uniform splitting systems and they gave some constructions for uniform $(m,4)$-splitting systems with m even.

In this paper, we mainly investigate the case $t = 3$, giving some constructions for both uniform and non-uniform splitting systems. We also give a general lower bound (a necessary condition) that holds for all t. For more details, see Section 1.4.

1.2 Preliminary results and examples

Let $N(m,t)$ denote the minimum number of blocks in any (m,t)-splitting system. Similarly, $N_d(m,t)$ denotes the minimum number of blocks in any disjunct (m,t)-splitting system, $N_u(m,t)$ denotes the minimum number of blocks in any uniform (m,t)-splitting system and $N_{\text{reg}}(r,m,t)$ denotes the minimum number of blocks in any r-regular (m,t)-splitting system. We say that an (m,t)-splitting system is *optimal* if it has exactly $N(m,t)$ blocks. Optimality of disjunct, uniform and r-regular (m,t)-splitting systems is defined in the obvious way.

Note that $N(m,t) = N_d(m,t) = N_u(m,t) = N_{\text{reg}}(0,m,t) = 0$ if $m < t$; in these cases they are splitting systems consisting of no blocks.

The following result follows immediately from the definitions.

Lemma 1.6 *For all m, t and r, it holds that $N_u(m,t) \geq N(m,t)$, $N_d(m,t) \geq N(m,t)$ and $N_{\text{reg}}(r,m,t) \geq N(m,t)$.*

The following result is also easy to prove.

Lemma 1.7 *For all m, t and r, it holds that $N(m+1,t) \geq N(m,t)$, $N_d(m+1,t) \geq N_d(m,t)$ and $N_{\text{reg}}(r,m+1,t) \geq N_{\text{reg}}(r,m,t)$.*

It is not the case that $N_u(m+1,t) \geq N_u(m,t)$ for all m, t. For example, it can be shown that $N_u(6,3) = 4 > N_u(7,3) = 3$.

Because the functions $N(m,t)$, $N_d(m,t)$ and $N_{\text{reg}}(r,m,t)$ are monotone nondecreasing for fixed r and t, it is useful to define $m(N,t) = \max\{m : N(m,t) \leq N\}$; $m_d(N,t)$ and $m_{\text{reg}}(r,N,t)$ are then defined in the obvious way.

Many constructions of splitting systems are conveniently described using the incidence matrix representation of a splitting system, which we define now.

Definition 1.8 *Let $(X,\mathcal{B})$ be an $(N;m,t)$-SS, where $X = \{x_j : 1 \leq j \leq m\}$ and $\mathcal{B} = \{B_i : 1 \leq i \leq N\}$. The* incidence matrix *of $(X,\mathcal{B})$ is the $N \times m$ matrix $A = (a_{i,j})$ where*

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

The following result is obvious.

Lemma 1.9 *Suppose $A = (a_{i,j})$ is an $N \times m$ matrix having entries in the set $\{0,1\}$. Then A is the incidence matrix of an $(N;m,3)$-SS if and only if, for all choices of three columns c_1, c_2, c_3 of A, the following property is satisfied:*

$$\text{There is a row } r \text{ such that } (a_{r,c_1}, a_{r,c_2}, a_{r,c_3}) \in \{(0,0,1),(0,1,0),(1,0,0)\}. \qquad (1)$$

Furthermore, we have the following:

1. *A is the incidence matrix of an $(N;m,3)$-disjunct SS if and only if, for all choices of two columns c_1, c_2 of A, there is a row r such that $a_{r,c_1} = 1$ and $a_{r,c_2} = 0$.*
2. *A is the incidence matrix of an $(N;m,3)$-uniform SS if and only if every row of A has hamming weight equal to $\lfloor \frac{m}{2} \rfloor$, and*
3. *A is the incidence matrix of an $(N;m,t)$-r-regular SS if and only if every column of A has hamming weight equal to r.*

Proof. Let $(X,\mathcal{B})$ denote the set system corresponding to the incidence matrix A. First, suppose that columns c_1, c_2, c_3 of A do not satisfy (1). Let the three corresponding points in $(X,\mathcal{B})$ be denoted x_1, x_2, x_3. Then no block in $\mathcal{B}$ intersects $\{x_1,x_2,x_3\}$ in exactly one point, and hence $(X,\mathcal{B})$ is not an $(m,3)$-splitting system.

Conversely, if $(X,\mathcal{B})$ is not an $(m,3)$-splitting system, then there exist three points x_1, x_2, x_3 such that no block in $\mathcal{B}$ intersects $\{x_1,x_2,x_3\}$ in exactly one point. Let the columns of A corresponding to x_1, x_2, x_3 be denoted c_1, c_2, c_3. Then it is clear that columns c_1, c_2, c_3 of A do not satisfy (1).

The remaining assertions (1, 2 and 3) are easy to prove. □

We now give a few small examples of splitting systems.

Example 1.1 *The blocks $\{1,5\}$, $\{2,5\}$ and $\{3,5\}$ form a $(3;5,3)$-uniform SS on the set $\{1,2,3,4,5\}$. The incidence matrix of this splitting system is*

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

▮

Example 1.2 *The blocks* $\{1,2\}$, $\{3,4\}$ *and* $\{5,6\}$ *form a* $(3;6,3)$-1-*regular* SS *on the set* $\{1,2,3,4,5,6\}$. *The incidence matrix of this splitting system is*

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

▮

Example 1.3 *The blocks* $\{1,2,3\}$, $\{1,4,5\}$, $\{1,6,7\}$, $\{2,4,6\}$ *and* $\{3,5,7\}$ *form a* $(5;7,3)$-*disjunct* SS *on the set* $\{1,2,3,4,5,6,7\}$. *The incidence matrix of this splitting system is*

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

▮

Example 1.4 *The blocks*

$$\{1,2,3,4,5\}, \{1,2,3,9,10\}, \{3,4,5,8,9\}, \{4,5,6,7,8\} \text{ and } \{6,7,8,9,10\}$$

form a $(5;10,3)$-*uniform* SS *on the set* $\{1,\dots,10\}$. ▮

Example 1.5 *The blocks*

$$\{1,2,5\}, \{3,4,5,8\}, \{5,6,7,8\} \text{ and } \{8,9,10\}$$

form a $(4;10,3)$-SS *on the set* $\{1,\dots,10\}$. ▮

1.3 Related set systems

Splitting systems are related to some other types of extremal set systems. We briefly discuss these connections now.

Let Y be a finite set and let $C_1,\dots,C_w \subseteq Y$. $\mathcal{C} = \{C_1, C_2, \dots, C_w\}$ is called a w-*sunflower* (also called a Δ-*system of size* w) if

$$C_i \cap C_j = \bigcap_{i=1}^{w} C_i$$

for all $1 \le i < j \le w$. See [5].

Lemma 1.10 *Suppose that* $(Y,\mathcal{C})$ *is a set system with* $|Y| = N$ *and* $|\mathcal{C}| = m$, *and let* D *be the* $m \times N$ *incidence matrix of* $(Y,\mathcal{C})$. *Define* A *to be the* $N \times m$ *matrix obtained by transposing* D *and then interchanging "0"s and "1"s. Then the following hold:*

1. $(Y,\mathcal{C})$ *does not contain a* 3-*sunflower if and only if* A *is the incidence matrix of an* $(N;m,3)$-SS.

2. *If $(Y, \mathcal{C})$ contains a w-sunflower, where $w \geq 4$, then A is not the incidence matrix of an $(N; m, w)$-SS.*

Proof. First, we observe that the incidence matrix of a w-sunflower has the property that every column contains $0, 1$ or w "1"s, and, conversely, a w-rowed binary matrix satisfying this property is the incidence matrix of a w-sunflower.

Now we prove 1., where we assume $w = 3$. To begin with, suppose that $(Y, \mathcal{C})$ contains a 3-sunflower. Then there are three rows r_1, r_2, r_3 of D such that the restriction of D to r_1, r_2, r_3 has the property that every column contains $0, 1$ or 3 "1"s. When we transpose and complement D, we obtain three columns of A such that the restriction of A to these three columns has the property that every row contains $0, 2$ or 3 "1"s. Thus property (1) from Lemma 1.9 is violated, and A is not the incidence matrix of an $(m, 3)$-splitting system.

Conversely, if A is not the incidence matrix of an $(m, 3)$-splitting system, then it is easy to see that $(Y, \mathcal{C})$ contains a 3-sunflower, by reversing the previous steps.

Finally, we prove 2., where $w \geq 4$. Suppose that $(Y, \mathcal{C})$ contains a w-sunflower; then there are w rows $r_1, \ldots, r_w$ of D such that the restriction of D to $r_1, \ldots, r_w$ has the property that every column contains $0, 1$ or w "1"s. When we transpose and complement D, we obtain w columns of A such that the restriction of A to these w columns has the property that every row contains $0, w-1$ or w "1"s. In particular, none of these rows contains $\lfloor \frac{w}{2} \rfloor$ "1"s. Thus the matrix A is not the incidence matrix of an (m, w)-splitting system. □

Remark 1.11 *It is easy to show that the converse of property 2. does not hold, by constructing a counterexample.*

There is also a connection between $(m, 3)$-splitting systems and the cover-free families introduced by Erdös, Frankl and Füredi [4]. (These are set systems with the property that no block is contained in the union of two other blocks.) The transpose of the $m \times N$ incidence matrix of a cover-free family on N points and m blocks satisfies the following property for all choices of three columns c_1, c_2, c_3:

$$\text{There is a row } r \text{ such that } (a_{r,c_1}, a_{r,c_2}, a_{r,c_3}) = (1, 0, 0). \tag{2}$$

(2) is a stronger condition than (1), so any cover-free family having N points and m blocks automatically yields an $(N; m, 3)$-SS. However, the constructions in this paper yield smaller splitting systems than the ones that can be obtained from known cover-free families.

Finally, 3-regular $(m, 3)$-splitting systems can be shown to be equivalent to the so-called $\{123, 124, 134\}$-free 3-hypergraphs. This is discussed further in Section 5.

1.4 Overview of the paper

The remainder of this paper is organized as follows. First, in Section 2, we prove a general necessary condition for the existence of (m, t)-splitting systems that holds for all integers $t \geq 2$.

The rest of the paper concerns $(m, 3)$-splitting systems. In Section 3, we present some good direct constructions for uniform $(m, 3)$-splitting systems.

In Section 4, we turn to recursive constructions for both uniform and nonuniform $(m, 3)$-splitting systems. In the nonuniform case, the best known results use disjunct systems and arise from the approach of Deuber, Erdös, Gunderson, Kostochka and Meyer [3]. We review their constructions and present a somewhat simplified treatment and a small extension of their asymptotic results.

In Section 5, we present some characterizations, constructions and necessary conditions for 2-regular and 3-regular $(m, 3)$-splitting systems. In particular, 3-regular $(m, 3)$-splitting systems are shown to be equivalent to $\{123, 124, 134\}$-free 3-hypergraphs. Some results on this problem are presented and extended.

Finally, in Section 6, we provide some tables summarizing the best known results for "small" $(m, 3)$-splitting systems of various special types. These tables are obtained using a combination of computer searches and applications of the results discussed in this paper.

2 Bounds for (m, t)-splitting systems

Ling, Li and van Rees proved in [8] that $N(m, t) \geq \lceil \log_2 m \rceil$ when $t = 2$ or 4. In this section, we prove that a similar type of bound holds for all $t \geq 2$.

Lemma 2.1 *Suppose that* $(X, \mathcal{B})$ *is an* $(N; m, t)$-SS *and suppose that* $B_0 \in \mathcal{B}$ *is a block such that* $\lfloor \frac{t}{2} \rfloor \leq |B_0| \leq m - \lfloor \frac{t+1}{2} \rfloor$. *Then there exists an* $(N-1; |B_0| + \lfloor \frac{t-1}{2} \rfloor, t)$-SS *and an* $(N-1; m - |B_0| + \lfloor \frac{t-2}{2} \rfloor, t)$-SS.

Proof. Let $Y \subseteq X \setminus B_0$, $|Y| = \lfloor \frac{t-1}{2} \rfloor$. Similarly, let $Z \subseteq B_0$, $|Z| = \lfloor \frac{t-2}{2} \rfloor$. For all blocks $B \in \mathcal{B}$, $B \neq B_0$, define $B^1 = B \cap (Y \cup B_0)$ and $B^2 = B \cap (Z \cup (X \setminus B_0))$. Then, for $i = 1, 2$, define $\mathcal{B}^i = \{B^i : B \in \mathcal{B}, B \neq B_0\}$. $(X, \mathcal{B}^1)$ is an $(N-1; |B_0| + \lfloor \frac{t-1}{2} \rfloor, t)$-SS and $(X, \mathcal{B}^2)$ is an $(N-1; m - |B_0| + \lfloor \frac{t-2}{2} \rfloor, t)$-SS. □

We mentioned in the introduction that $N(m, t) = N_u(m, t) = 0$ when $m < t$. It is trivial to see that $N(t, t) = N_u(t, t) = 1$. The case $m = t + 1$ is considered in the next lemma.

Lemma 2.2 *For all integers* $t \geq 2$, *it holds that* $N(t + 1, t) = 2$.

Proof. Suppose that $N(t+1, t) = 1$. Then there is a $(t+1, t)$-SS consisting of one block, say B. Let $X = \{1, \ldots, t\}$. Because $|B \cap X| = \lfloor \frac{t}{2} \rfloor$, we can assume, without loss of generality, that $B \cap X = \{1, \ldots, \lfloor \frac{t}{2} \rfloor\}$. Next, consider $X = \{2, \ldots, t+1\}$. The condition $|B \cap X| = \lfloor \frac{t}{2} \rfloor$ implies that $B = \{1, \ldots, \lfloor \frac{t}{2} \rfloor, t + 1\}$. Then, consider $X = \{1, \ldots, t-1, t+1\}$. Clearly $|B \cap X| = \lfloor \frac{t}{2} \rfloor + 1$, a contradiction.

Finally, if we take any two disjoint $\lfloor \frac{t}{2} \rfloor$-subsets of X, then we have a $(2; t+1, t)$-SS. □

Here is our general lower bound.

Theorem 2.3 *For all* $m \geq t + 1$, $N(m, t) \geq \lfloor \log_2 (m - t + 1) \rfloor + 1$.

Proof. The proof is by induction on m. Clearly the desired result is true for $m = t + 1$ by Lemma 2.2. Next, we consider integers m having the form $m = 2^i + t - 1$, where $i \geq 2$ (for these values of m, $\log_2 (m - t + 1)$ is an integer). Let $(X, \mathcal{B})$ be any $(N; 2^i + t - 1, t)$-SS in which $N = N(2^i + t - 1, t)$. It is clear that $\lfloor \frac{t}{2} \rfloor \leq |B_0| \leq m - \lfloor \frac{t+1}{2} \rfloor$ for all $B_o \in \mathcal{B}$, because any block whose size is not in this range splits no t-subsets and hence it can be deleted from $\mathcal{B}$.

It is easy to see that $\mathcal{B}$ contains a block B where either

$$|B| \geq 2^{i-1} + \left\lfloor \frac{t}{2} \right\rfloor$$

or

$$m - |B| \geq 2^{i-1} + \left\lfloor \frac{t+1}{2} \right\rfloor.$$

For, if this is not the case, then

$$\begin{aligned} m &= |B| + m - |B| \\ &\leq 2^{i-1} + \left\lfloor \frac{t}{2} \right\rfloor - 1 + 2^{i-1} + \left\lfloor \frac{t+1}{2} \right\rfloor - 1 \\ &= 2^i + t - 2, \end{aligned}$$

a contradiction.

Now, using Lemma 2.1, we obtain either an $(N-1, m_1, t)$-SS where

$$m_1 \geq 2^{i-1} + \left\lfloor \frac{t}{2} \right\rfloor + \left\lfloor \frac{t-1}{2} \right\rfloor = 2^{i-1} + t - 1;$$

or an $(N-1, m_2, t)$-SS where

$$m_2 \geq 2^{i-1} + \left\lfloor \frac{t+1}{2} \right\rfloor + \left\lfloor \frac{t-2}{2} \right\rfloor = 2^{i-1} + t - 1.$$

Therefore, by Lemma 1.7, there is an $(N-1; 2^{i-1}+t-1, t)$-SS. By induction, it holds that $N-1 \geq i-1+1 = i$. Therefore, $N \geq \lfloor \log_2 (m-t+1) \rfloor + 1 = i+1$, as required.

Finally, we consider an arbitrary integer $m \geq t+1$. Suppose that $2^i + t - 1 \leq m < 2^{i+1} + t - 1$, where $i \geq 1$. Applying Lemma 1.7 and the result proven above for integers m of the form $2^i + t - 1$, we have that

$$N(m,t) \geq N(2^i + t - 1, t) \geq i + 1 = \lfloor \log_2 (m-t+1) \rfloor + 1,$$

as required. □

Since our bounds apply to "general" splitting systems, they automatically apply to uniform splitting systems, as well.

Corollary 2.4 *For all $m \geq t+1$, it holds that $N_u(m,t) \geq \lfloor \log_2 (m-t+1) \rfloor + 1$.*

3 Direct constructions for $(m, 3)$-splitting systems

We begin with three easy constructions for $(m, 3)$-splitting systems. These constructions are, in general, not very good, but they do yield optimal systems for a few small values of m.

Theorem 3.1 *For all even $m \geq 4$, there exists an $\left(\frac{m}{2}; m, 3\right)$-SS,*

Proof. Let $X = \{1, 2, \ldots, m\}$ and let $\mathcal{B} = \{\{1,2\}, \{3,4\}, \ldots, \{m-1, m\}\}$. The blocks each have size two and partition X, so it is obvious that any 3-subset of X intersects one of the blocks in exactly one point. □

Theorem 3.2 *For all odd $m \geq 7$, there exists an* $\left(\frac{m-1}{2}; m, 3\right)$-SS,

Proof. Let $X = \{1, 2, \ldots, m\}$ and let $\mathcal{B} = \{\{1, 2, m\}, \{3, 4, m\}, \ldots, \{m-2, m-1, m\}\}$. It is obvious that any 3-subset of $X \backslash \{m\}$ intersects one of the blocks in exactly one point.

Consider a 3-subset of $Y \subseteq X$ that contains the point m. If Y is a block, then it intersects any other block in exactly one point. If Y is not a block, then it intersects two blocks in two points. There is at least one more block (because $m \geq 7$), and any such block will intersect Y in exactly one point. □

Theorem 3.3 *For all $m \geq 2$, there exists an $(m; m, 3)$-disjunct* SS,

Proof. Let $X = \{1, 2, \ldots, m\}$ and let $\mathcal{B} = \{\{i\} : 1 \leq i \leq m\}$. □

We now give direct constructions for uniform $(m, 3)$-splitting systems in which the number of blocks is $O(\log m)$.

Theorem 3.4 *Let $m \geq 4$ be even. Then there exists an $(N; m, 3)$-uniform* SS, *with* $N = 2\lceil \log_2 m \rceil - 2$.

Proof. Denote $\ell = \lceil \log_2 m \rceil - 2$. Construct an $\ell \times m/2$ binary matrix, named T_m, as follows. The columns of T_m are (in order) $c_0, \ldots, c_{m/2-1}$, where

$$c_i = \begin{cases} \text{the binary representation of } i & \text{if } i \leq 2^\ell - 1 \\ \text{the binary representation of } i - 2^\ell & \text{if } 2^\ell \leq i \leq m/2 - 1. \end{cases}$$

Each c_i is a column vector of length ℓ.

Now construct a $(2\ell + 2) \times m$ matrix A as follows:

$$A = \left(\begin{array}{c|c} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} \\ \hline T_m & {T_m}^c \\ \hline {T_m}^c & T_m \end{array} \right),$$

where ${T_m}^c$ is the complement of T_m (i.e., every entry "0" is replaced by "1" and vice versa). Here and elsewhere, $\mathbf{1}$ and $\mathbf{0}$ denote row or column vectors of "1"s and "0"s, respectively.

We prove that A is the incidence matrix of an $(m, 3)$-splitting system. Denote the left and right halves of A by L and R respectively. (1) is satisfied if we take two columns from L and one column from R, by letting r be the second row of A. Similarly, (1) is satisfied if we take two columns from R and one column from L, by letting r be the first row of A.

Suppose we take three columns from L, say c_1, c_2, c_3. Consider the three corresponding columns of T_m. Clearly these three columns of T_m are not all identical. Suppose without loss of generality that column c_1 of T_m is not identical to column c_2 of T_m. Then there exists a row r of T_m such that $t_{r,c_1} \neq t_{r,c_2}$, where the entries of T_m are denoted $t_{i,j}$. Now, if $t_{r,c_3} = 0$, then (1) is satisfied. On the other hand, if $t_{r,c_3} = 1$, then $(t_{r,c_1}, t_{r,c_2}, t_{r,c_3}) = (0, 1, 1)$ or $(1, 0, 1)$. In this case, (1) is satisfied by taking the rth row of ${T_m}^c$.

If we choose three columns from R, the proof is similar.

Finally, note that a row of T_m that contains i "1"s, say, is juxtaposed with a row of ${T_m}^c$ that contains $m - i$ "1"s. Hence, it is easily seen that every row of A contains exactly m "1"s, and therefore the splitting system is uniform. □

Example 3.1 *We construct the incidence matrix of a* $(6;14,3)$*-uniform* SS *using Theorem 3.4:*

$$\left(\begin{array}{ccccccc|ccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\hline
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
\hline
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0
\end{array}\right).$$

∎

The following result is obtained by modifying Theorem 3.4.

Theorem 3.5 *For any odd integer* $m \geq 7$*, there exists an* $(N;m,3)$*-uniform* SS *where* $N \leq 2\lceil \log_2(m-3)\rceil + 2$.

Proof. Denote $m' = m-3$. Construct the $(\lceil \log_2 m' \rceil - 2) \times m'/2$ matrix $T_{m'}$ as in Theorem 3.4. Then construct the following incidence matrix A:

$$A = \left(\begin{array}{c|c|ccc}
\mathbf{1} & \mathbf{0} & 1 & 0 & 0 \\
\mathbf{0} & \mathbf{1} & 1 & 0 & 0 \\
\mathbf{1} & \mathbf{0} & 0 & 1 & 0 \\
\mathbf{0} & \mathbf{1} & 0 & 1 & 0 \\
\mathbf{1} & \mathbf{0} & 0 & 0 & 1 \\
\mathbf{0} & \mathbf{1} & 0 & 0 & 1 \\
\hline
T_{m'} & {T_{m'}}^c & 0 & 0 & 1 \\
\hline
{T_{m'}}^c & T_{m'} & 0 & 0 & 1
\end{array}\right).$$

Let L denote the first $m'/2$ columns of A, Let M denote the next $m'/2$ columns of A, and let R denote the last 3 columns of A.

Observe that, if we delete the first four rows and the last three columns of A, then we obtain the incidence matrix of a $(2\lceil \log_2(m-3)\rceil - 2; m-3, 3)$-uniform SS which is constructed as in Theorem 3.4. Therefore (1) is satisfied if we choose any three columns in $L \cup M$.

If we choose the three columns in R, it is clear that (1) is satisfied. Also, if we choose two columns in R and one column in $L \cup M$, then (1) is satisfied, by taking one of the first six rows of A. Finally, if we choose two columns from $L \cup M$ and one column from R, then it is again the case that (1) is satisfied by taking one of the first six rows of A.

To complete the proof, we observe that every row of A contains exactly $m'/2 + 1 = (m-1)/2$ "1"s. □

Example 3.2 *We construct the incidence matrix of a* $(10;17,3)$*-uniform* SS *using Theorem*

3.5 and Example 3.1:

$$\left(\begin{array}{ccccccc|ccccccc|ccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\
\hline
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
\hline
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1
\end{array}\right).$$

∎

4 Recursive constructions for $(m, 3)$-splitting systems

First, we observe that we can construct a $(2m, 3)$-splitting system from an $(m, 3)$-splitting system, as follows.

Theorem 4.1 *If there exists an* $(N; m, 3)$-SS, *then there exists an* $(N + 2; 2m, 3)$-SS.

Proof. Let A be the $N \times m$ incidence matrix of the $(m, 3)$-splitting system. We construct the incidence matrix of the desired $(2m, 3)$-splitting system on $N + 2$ blocks as follows:

$$A' = \left(\begin{array}{c|c} A & A \\ \hline \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} \end{array}\right).$$

We prove that this matrix is the incidence matrix of a $(2m, 3)$-splitting system on $N + 2$ blocks.

Denote the left and right halves of A' by L and R, respectively. (1) is satisfied if we take two columns from L and one column from R, by letting r be the last row of A'. Similarly, (1) is satisfied if we take two columns from R and one column from L, by letting r be the second last row of A'. Suppose we take three columns from L, or three columns from R. Then one of the first N rows of A' will satisfy (1), because A is the incidence matrix of an $(m, 3)$-splitting system. □

Example 4.1 *A* $(5; 10, 3)$-SS, *obtained from Example 1.1 using Theorem 4.2. The incidence matrix is as follows:*

$$\left(\begin{array}{ccccc|ccccc}
1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
\hline
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1
\end{array}\right).$$

∎

Theorem 4.2 *Suppose that m is even. If there exists an $(N; m, 3)$-uniform* SS*, then there exists an $(N + 2; 2m, 3)$-uniform* SS*.*

Proof. We use the same construction as Theorem 4.1. It suffices to show that every row of A' contains exactly m "1"s. This is clear because m is even, and hence every row of an $(N; m, 3)$-uniform SS contains exactly $m/2$ "1"s. □

Theorem 4.3 *Suppose that m is even. If there exists an $(N; m, 3)$-uniform* SS*, then there exists an $(N + 1; m + 1, 3)$-uniform* SS*.*

Proof. Let A be the $N \times m$ incidence matrix of the uniform $(m, 3)$-splitting system. Observe that A may contain repeated columns; however, it does not contain three identical columns. Label the columns of A in such a way that columns i and j are identical only if $|i - j| = 1$. Now construct the incidence matrix of the desired uniform $(m + 1, 3)$-splitting system on $N + 1$ blocks as follows:

$$A' = \left(\begin{array}{ccccc|c} \multicolumn{5}{c|}{A} & \mathbf{0} \\ \hline 0 & 1 & 0 & 1 & \cdots & 0 \end{array}\right).$$

□

4.1 Product constructions

The best known recursive constructions for (non-uniform) $(m, 3)$-splitting systems are product constructions. Most of these product constructions make use of disjunct splitting systems. The next theorem is a restatement of [3, Lemma 3.1]; we include the proof for completeness because our notation is quite different from [3].

Theorem 4.4 *If there exists an $(N_1; m_1, 3)$-disjunct* SS *and an $(N_2; m_2, 3)$-disjunct* SS*, then there exists an $(N_1 + N_2; m_1 m_2, 3)$-disjunct* SS*.*

Proof. Let A and A' be the incidence matrices of the two splitting systems. Denote the columns of A by $\mathbf{c}_j$, $1 \le j \le m_1$, and denote the columns of A' by $\mathbf{c}'_j$, $1 \le j \le m_2$. We construct a matrix, which we denote by $A \oplus A'$, in which column (j, j') contains the column vector

$$\begin{pmatrix} \mathbf{c}_j \\ \mathbf{c}'_{j'} \end{pmatrix}.$$

We will show that $A \oplus A'$ is the incidence matrix of an $(N_1 + N_2; m_1 m_2, 3)$-disjunct SS. Pick three columns of $A \oplus A'$, say (j_1, j'_1), (j_2, j'_2) and (j_3, j'_3). If j_1, j_2 and j_3 are all distinct, then we can find a row r of A with the 3-splitting property for the three given columns, and then row r in $A \oplus A'$ also has the same 3-splitting property. Similarly, everything is all right if j'_1, j'_2 and j'_3 are all distinct.

If $|\{j_1, j_2, j_3\}| = 1$, then $|\{j'_1, j'_2, j'_3\}| = 3$; and if $|\{j'_1, j'_2, j'_3\}| = 1$, then $|\{j_1, j_2, j_3\}| = 3$. Hence, we need only to consider the case where $|\{j_1, j_2, j_3\}| = |\{j'_1, j'_2, j'_3\}| = 2$. Then the three column labels have the form (j_1, j'_1), (j_1, j'_2) and (j_2, j'_2), where $j_1 \ne j_2$ and $j'_1 \ne j'_2$. A is disjunct, so there is a row r in A such that $A(r, j_1) = 0$ and $A(r, j_2) = 1$. Then row r of $A \oplus A'$ has the desired 3-splitting property for the three given columns.

Finally, we need to show that $A \oplus A'$ is disjunct. Consider two columns, say columns (j_1, j'_1) and (j_2, j'_2). It must be the case that $j_1 \ne j_2$ or $j'_1 \ne j'_2$. If $j_1 \ne j_2$ then use the fact that A is disjunct to show that the two columns of $A \oplus A'$ satisfy the disjunct property. If $j'_1 \ne j'_2$, then use the fact that A' is disjunct to establish the desired result. □

Corollary 4.5 *If there exists an* $(N_0; m_0, 3)$*-disjunct* SS*, then there exists a* $(jN_0; {m_0}^j, 3)$*-disjunct* SS *for all integers* $j \geq 1$.

Given any $(N_0; m_0, 3)$-disjunct SS, define the *expansion coefficient* of the splitting system to be the value $c = {m_0}^{1/N_0}$. It is easy to see that Corollary 4.5 produces an infinite class of $(N; c^N, 3)$-SS, given an initial $(N_0; m_0, 3)$-disjunct SS, all of which have expansion coefficient equal to c. Thus we have the following result.

Corollary 4.6 *If there exists a disjunct* $(N_0; m_0, 3)$*-*SS *with expansion coefficient equal to* c*, then* $\limsup_{N\to\infty}(m(N,3))^{1/N} \geq c$.

Example 4.2 *The incidence matrix of a* $(6; 11, 3)$*-disjunct* SS *is as follows:*

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

∎

In some of the next examples, we make use of the incidence matrix of a $(6, 10, 5, 3, 2)$-BIBD. This balanced incomplete block design is unique up to isomorphism, and its 6×10 point-block incidence matrix, B, is as follows (see [1]): It is a disjunctive(6;10,3)-USS.

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

Example 4.3 *The incidence matrix of a* $(7; 16, 3)$*-disjunct* SS *is as follows:*

$$\begin{array}{c} \\ 6 \\ 1 \end{array} \begin{array}{c} \begin{array}{cc} 6 & 10 \end{array} \\ \begin{pmatrix} I_6 & B \\ \mathbf{1} & \mathbf{0} \end{pmatrix} \end{array},$$

where I_6 *is a* 6×6 *identity matrix,* B *is the incidence matrix of the* $(6, 10, 5, 3, 2)$*-BIBD,* $\mathbf{1}$ *is a* 1×6 *submatrix of "1"s and* $\mathbf{0}$ *is a* 1×10 *submatrix of "1"s.* ∎

Example 4.4 *The incidence matrix of a* $(8; 27, 3)$*-disjunct* SS *is as follows:*

$$\begin{array}{c} \\ 6 \\ 1 \\ 1 \end{array} \begin{array}{c} \begin{array}{cccc} 6 & 10 & 10 & 1 \end{array} \\ \begin{pmatrix} I_6 & B & B^c & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & 0 \\ \mathbf{1} & \mathbf{1} & \mathbf{0} & 0 \end{pmatrix} \end{array}.$$

All notation is the same as in Example 4.3 and B^c *denotes the complement of the matrix* B*.* ∎

Example 4.5 *The incidence matrix of a* $(9;43,3)$*-disjunct* SS *is as follows:*

$$\begin{array}{c} \\ 6 \\ 1 \\ 1 \\ 1 \end{array} \begin{array}{c} \begin{array}{cccccc} 10 & 10 & 10 & 6 & 6 & 1 \end{array} \\ \begin{pmatrix} B & B & B^c & I_6 & I_6 & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & 0 \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & 0 \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & 0 \end{pmatrix} \end{array},$$

where all notation is the same as in the preceding examples. ▮

Now we consider another product-type construction, also from [3]. Again, we include a proof for completeness, because our notation is different from [3].

Theorem 4.7 *[3, Lemma 4.4] If there exists an* $(N_1;m_1,3)$*-disjunct* SS *containing a block of size* k_1 *and an* $(N_2;m_2,3)$*-disjunct* SS *containing a block of size* k_2*, then there exists an* $(N_1+N_2-2;k_1(m_2-k_2)+k_2(m_1-k_1),3)$*-disjunct* SS*.*

Proof. Let A and A' be the incidence matrices of the two splitting systems. A contains a row having hamming weight k_1 and A' contains a row having hamming weight k_2. Permute the rows and columns of A and A' so that they have the following forms:

$$A = \begin{array}{c} \\ N_1-1 \\ 1 \end{array} \begin{array}{c} \begin{array}{cc} k_1 & m_1-k_1 \end{array} \\ \begin{pmatrix} A_1 & A_0 \\ \mathbf{1} & \mathbf{0} \end{pmatrix} \end{array}, \qquad A' = \begin{array}{c} \\ N_2-1 \\ 1 \end{array} \begin{array}{c} \begin{array}{cc} k_2 & m_2-k_2 \end{array} \\ \begin{pmatrix} A'_1 & A'_0 \\ \mathbf{1} & \mathbf{0} \end{pmatrix} \end{array}.$$

Define A^* to be the following matrix:

$$A^* = \begin{pmatrix} A_1 \oplus A'_0 & A_0 \oplus A'_1 \end{pmatrix} = \begin{pmatrix} A^*_1 & A^*_0 \end{pmatrix}.$$

We will show that A^* is the incidence matrix of an $(N_1+N_2-2;k_1(m_2-k_2)+k_2(m_1-k_1),3)$-disjunct SS. Pick three columns of A^*, say (j_1,j'_1), (j_2,j'_2) and (j_3,j'_3). If the three columns are all from A^*_1 or all from A^*_0, then the argument is similar to that used in the proof of Theorem 4.4.

Next, suppose that (j_1,j'_1) and (j_2,j'_2) are columns of A^*_1 and (j_3,j'_3) is a column of A^*_0. If $j_1 \neq j_2$, then j_1,j_2 and j_3 are distinct and there is a row of $\begin{pmatrix} A_1 & A_0 \end{pmatrix}$ that satisfies the 3-splitting property for the three given columns. On the other hand, suppose that $j_1 = j_2$. Because A is disjunct, there is a row r of $\begin{pmatrix} A_1 & A_0 \end{pmatrix}$ such that $A(r,j_1)=0$ and $A(r,j_3)=1$. This row establishes the truth of the 3-splitting property for the three given columns.

The last case, when two of the columns are from A^*_0 and one column is from A^*_1, is similar, and we conclude that we have a 3-splitting system.

We still have to show that this system is disjunct. Consider two columns, say columns (j_1,j'_1) and (j_2,j'_2). If both columns are from A^*_1 or both columns are from A^*_0, then it is easy to see that the disjunct property is satisfied. Therefore we can assume WLOG that (j_1,j'_1) is from A^*_1 and (j_2,j'_2) is from A^*_0. Clearly $j_1 \neq j_2$ and $j'_1 \neq j'_2$. Because $j_1 \neq j_2$, we can find a row r of $\begin{pmatrix} A_1 & A_0 \end{pmatrix}$ such that $A(r,j_1)=0$ and $A(r,j_2)=1$. Similarly, because $j'_1 \neq j'_2$, we can find a row r' of $\begin{pmatrix} A'_1 & A'_0 \end{pmatrix}$ such that $A'(r',j'_1)=1$ and $A'(r',j'_2)=0$. These two rows establish the desired disjunct property in A for the two given columns. □

Example 4.6 *Theorem 4.7 can produce different splitting systems depending on the sizes of the blocks that are used. We consider some examples now. Suppose we start with the* $(8; 27, 3)$*-disjunct* SS *from Example 4.4. This system contains blocks of size* 12 *and* 16*. We can therefore take* $N_1 = N_2 = 8$*,* $m_1 = m_2 = 27$ *and* $k_1, k_2 \in \{12, 16\}$*. If* $k_1 = k_2 = 12$*, then the result of applying Theorem 4.7 is a* $(14; 360, 3)$*-disjunct* SS *with block sizes 159 and 210 . If* $k_1 = k_2 = 16$*, then we get a* $(14; 352, 3)$*-disjunct* SS *with block sizes 162,226 and if* $k_1 = 12$*,* $k_2 = 16$*, then we get a* $(14; 372, 3)$*-disjunct* SS *with block sizes 162, 167, 210 and 226.*

The $(14; 352, 3)$*-disjunct* SS *obtained in this way is essentially the same as the system named* $\mathcal{L}$ *in [3]. However, we have obtained this system as a direct application of Theorem 4.7 and removed the need for a lengthy verification as was required in [3].*

In [3], the authors constructed a $(14; 388, 3)$*-disjunct* SS *with block sizes* 143 *and* 156*. If we use this splitting system and the* $(14; 372, 3)$*-disjunct* SS *in Theorem 4.7 with* $N_1 = N_2 = 14, m_1 = 388, m_2 = 372, k_1 = 143$ *and* $k_2 = 226$*, we get a* $(26; 76248, 3)$*-disjunct* SS *with block sizes which include* 47930 *and* 33978 *and with an expansion coefficient of* 1.5409*. If we use Theorem 4.7 with* $N_1 = N_2 = 26, m_1 = m_2 = 76248, k_1 = 47930$ *and* $k_2 = 33978$ *then we get a* $(50; 2988190104, 3)$*-disjunct* SS *with expansion coefficient* 1.54706 *and block sizes including 1870294024 and 1393602424.*

∎

Using the last two splitting systems from Example 4.6, we can get two infinite families of splitting systems, which we now record. The proof technique comes from Deuber et al. [3].

Theorem 4.8 *For every* n *of the form* $n = 24q+2$*, there exists a* $(n; 1.551^{n-2}, 3)$*-disjunct* SS *which has expansion coefficient* 1.551 *for asymptotic* n*. For every* n *of the form* $n = 48q+2$*, there exists a* $(n; 1.552^{n-2}, 3)$*-disjunct* SS *which has expansion coefficient* 1.552 *for asymptotic* n*.*

Proof. The proof is by math induction. To prove the first part we start with (26;76248,3)-disjunct SS with block sizes, a larger than half of 76248 and b smaller than half of 76248. Assuming that we have the $j-1$ case; i.e., there exists an $(24(j-1)+2; 1.551^{24(j-1)}, 3)$-disjunct SS, consider a row from the matrix representing this SS. If it has c 1's more than half of m then use $k_1 = b, k_2 = c, m_1 = 76248, m_2 = 1.551^{24(j-1)}$ in Theorem 4.7. We get a disjunct SS with

$$b(1.551^{48(j-1)} - c) + (76248 - b)c \geq 76248 * 1.551^{48(j-1)}/2 \geq 1.551^{24} * 1.551^{48(j-1)} = 1.551^{48j}.$$

So we have our $(24(j)+2; 1.551^{24(j)}, 3)$ disjunct SS. Note the first inequality is true as $ax + by \geq .5(a+b)(x+y)$ if $a \geq b, x \geq y$.

Now if c is less than half of 76248, then let $k_1 = a, k_2 = c, m_1 = 76248, m_2 = 1.551^{24(j-1)}$ in Theorem 4.7 and do the same procedure. The second case is done the same starting with (50;2988190104,3)-disjunct SS. Note there is a row in the disjunct SS whose number of 1's is less than than half of m and a row whose number of 1's is more than half of m. □

The first result has the same expansion coefficient as Deuber et al. [3] but occurs for twice as many n's. The second result has an expansion coefficient that is .001 bigger than the one obtained in Deuber et al. [3].

5 Regular splitting systems

Recall that an r-regular splitting system is one in which every point occurs in exactly r blocks. We begin by establishing some preliminary results that allow us to prove a bound for r-regular $(m,3)$-splitting systems. The first lemma and theorem in this section are obtained by easy counting arguments.

Lemma 5.1 *Suppose that A is an $N \times m$ binary matrix in which every column contains exactly r "1"s. Let $0 \leq \nu \leq r$. Then A contains a $\nu \times \mu$ submatrix of "1"s, where $\mu \geq m\binom{r}{\nu}/\binom{N}{\nu}$.*

Proof. Consider the set

$$P = \{(c, \{r_1, \ldots, r_\nu\}) : A_{r_i,c} = 1, i = 1, \ldots, \nu\}.$$

Then $|P| = m\binom{r}{\nu}$, because there are m choices for c, and for each c, there are $\binom{r}{\nu}$ choices for $\{r_1, \ldots, r_\nu\}$.

Let $\mathcal{R}$ denote the set of all $\binom{N}{\nu}$ possible ν-subsets of rows of A. For each $R \in \mathcal{R}$, let

$$\mu(R) = |\{c : (c, R) \in P\}|.$$

The average value of $\mu(R)$, over all the possible $R \in \mathcal{R}$, is $m\binom{r}{\nu}/\binom{N}{\nu}$. Hence, there exists a ν-subset $R \in \mathcal{R}$ such that $\mu(R) \geq m\binom{r}{\nu}/\binom{N}{\nu}$. The desired result follows. ∎

Theorem 5.2 *Suppose there exists an $(N; m, t)$-r-regular* SS. *Let $0 \leq \nu \leq r$. Then there exists an $(N-\nu; \mu, t)$-$(r-\nu)$-regular* SS, *where $\mu \geq m\binom{r}{\nu}/\binom{N}{\nu}$.*

Proof. Let A be the incidence matrix of an $(N; m, t)$-r-regular SS. Applying Lemma 5.1, let A_1 be a $\nu \times \mu$ submatrix of A consisting entirely of "1"s, where $\mu \geq m\binom{r}{\nu}/\binom{N}{\nu}$. Now let A' be the $N-\nu$ by μ matrix constructed by deleting the rows in A_1 and the columns not in A_1 from A. It is easy to see that A' is the incidence matrix of an $(N-\nu; \mu, t)$-$(r-\nu)$-regular SS. ∎

Recall that $m_{\text{reg}}(r, N, t)$ denotes the maximum integer m such that an $(N; m, t)$-r-regular SS exists. For brevity, let $m(r, N) = m_{\text{reg}}(r, N, 3)$. We have the following corollary of Theorem 5.2.

Corollary 5.3 *Suppose $0 \leq \nu \leq r$. Then*

$$m(r, N) \leq \frac{\binom{N}{\nu} m(r-\nu, N-\nu)}{\binom{r}{\nu}}.$$

The case $r = 2$ is easy, and will provide the base case for a general bound.

Lemma 5.4 *Let $N \geq 4$. Then $m(2, N) = 2\lfloor \frac{N}{2} \rfloor \lceil \frac{N}{2} \rceil$.*

Proof. Let A be an $N \times m$ binary matrix in which every column contains exactly two "1"s. Suppose that A is the incidence matrix of an $(N; m, 3)$-2-regular SS. No column of A is duplicated three times, and if we take one copy of every distinct column, then we obtain the incidence matrix of a triangle-free graph. Conversely, if we start with the incidence matrix of any triangle-free graph and repeat every column twice, then we obtain the incidence matrix of a 2-regular 3-splitting system. The maximum number of edges in any triangle-free graph on N vertices is $\lfloor \frac{N}{2} \rfloor \lceil \frac{N}{2} \rceil$, so the proof is complete. ∎

Iterating Corollary 5.3 and applying Lemma 5.4, we obtain the following general bound for r-regular splitting systems.

Theorem 5.5

$$m(r, N) \le \binom{N}{r} \frac{N - r + 2}{N - r + 1}.$$

We can say more about the case $r = 3$, which is related to another extremal hypergraph problem. A 3-*hypergraph* is a set system in which every block has size three and in which there do not exist repeated blocks. A 3-hypergraph is $\{123, 124, 134\}$-*free* if it does not contain three blocks isomorphic to the configuration $\{123, 124, 134\}$. The integer $\mathrm{ex}(N, \{123, 124, 134\})$ denotes the maximum number of blocks in any $\{123, 124, 134\}$-free 3-uniform hypergraph on N points. Some results on $\mathrm{ex}(N, \{123, 124, 134\})$ can be found in [6].

Theorem 5.6 $m(3, N) = 2\,\mathrm{ex}(N, \{123, 124, 134\})$.

Proof. Denote $m = m(3, N)$. Let A be the $N \times m$ incidence matrix of an $(N; m, 3)$-3-regular SS. Observe that A cannot contain three identical columns. Retaining one copy of every column in A, construct an $N \times m'$ incidence matrix, say A', where $m' \ge m/2$. Now construct a set system whose incidence matrix is the transpose of A'. This set system is a $\{123, 124, 134\}$-free 3-hypergraph on N points and m' blocks, so $\mathrm{ex}(N, \{123, 124, 134\}) \ge m(3, N)/2$.

Conversely, suppose that we have a $\{123, 124, 134\}$-free 3-hypergraph on N points and $m' = \mathrm{ex}(N, \{123, 124, 134\})$ blocks. Let A' be the transpose of the incidence matrix of this hypergraph. Then take two copies of every column in A', to form an $N \times 2m'$ binary matrix, say A. It is clear that every column of A contains exactly three "1"s. We show that A is 3-splitting. Choose three columns of A, say columns j_1, j_2, j_3. Suppose first that two of these columns are identical, say column j_1 and j_2. Since all columns have weight three and there do not exist three identical columns, there must exist a row r such that $A(r, j_1) = A(r, j_2) = 0$ and $A(r, j_3) = 1$. If all three of these columns are different, then the $\{123, 124, 134\}$-free property implies that there is a row r such that exactly two of the values $A(r, j_1)$, $A(r, j_2)$ and $A(r, j_3)$ are equal to 0. □

Some small values of $\mathrm{ex}(N, \{123, 124, 134\})$ are easy to determine. We have the following.

Theorem 5.7 $\mathrm{ex}(4, \{123, 124, 134\}) = 2$, $\mathrm{ex}(5, \{123, 124, 134\}) = 5$, $\mathrm{ex}(6, \{123, 124, 134\}) = 10$ *and* $\mathrm{ex}(7, \{123, 124, 134\}) = 15$.

Example 5.1 *We exhibit optimal* $\{123, 124, 134\}$*-free* 3*-hypergraphs on* 4, 5, 6 *and* 7 *points:*

N	*blocks*				
4	$\{1,2,3\}$	$\{1,2,4\}$			
5	$\{1,2,3\}$	$\{1,2,4\}$	$\{1,4,5\}$	$\{2,3,5\}$	$\{3,4,5\}$
6	$\{1,2,3\}$	$\{1,2,4\}$	$\{1,4,5\}$	$\{2,3,5\}$	$\{3,4,5\}$
	$\{1,3,6\}$	$\{2,4,6\}$	$\{2,5,6\}$	$\{3,4,6\}$	$\{1,5,6\}$
7	$\{1,2,3\}$	$\{1,2,4\}$	$\{1,4,5\}$	$\{2,3,5\}$	$\{3,4,5\}$
	$\{1,3,6\}$	$\{2,4,6\}$	$\{2,5,6\}$	$\{3,4,6\}$	$\{1,5,6\}$
	$\{1,3,7\}$	$\{2,4,7\}$	$\{2,5,7\}$	$\{3,4,7\}$	$\{1,5,7\}$

▮

The following construction is useful for constructing a $\{123, 124, 134\}$-free hypergraph on $N + 1$ points from a $\{123, 124, 134\}$-free hypergraph on N points.

Theorem 5.8 *Suppose there exists a $\{123, 124, 134\}$-free hypergraph on N points with b blocks and suppose $x \in X$ and x occurs in b_x blocks. Then there exists a $\{123, 124, 134\}$-free hypergraph on $N + 1$ points with at least $b + b_x$ blocks.*

Proof. Let $(X, \mathcal{B})$ the a $\{123, 124, 134\}$-free hypergraph on N points with b blocks. Let y be an element not in X. Let $\mathcal{C}$ be the set of blocks of $\mathcal{B}$ which contains the element x, but replace each occurrence of x with y. It is easy to see that $(X \cup \{y\}, \mathcal{B} \cup \mathcal{C})$ will be a $\{123, 124, 134\}$-free hypergraph on $N + 1$ points with $b + b_x$ blocks. □

Example 5.2 *A $\{123, 124, 134\}$-free hypergraph on 9 points with 32 blocks is given in Appendix A. It can be verified that the point 4 has frequency 12. Therefore, from Theorem 5.8, we have that* $\mathrm{ex}(10, \{123, 124, 134\}) \geq 32 + 12 = 44$. ▮

Clearly, there is always an element $x \in X$ whose frequency is at least $\lceil \frac{3b}{N} \rceil$. Hence, we have the following corollary.

Corollary 5.9 *Suppose there exists a $\{123, 124, 134\}$-free hypergraph on N points with b blocks. Then there exists a $\{123, 124, 134\}$-free hypergraph on $N + 1$ points with at least $b + \lceil \frac{3b}{N} \rceil$ blocks.*

The converse of Theorem 5.8 is also true. That is, if we take a $\{123, 124, 134\}$-free hypergraph on $N + 1$ points and remove all the blocks containing some fixed point x, the remaining blocks form a $\{123, 124, 134\}$-free hypergraph on N points. This is sometimes useful for improving upper bounds of $\mathrm{ex}(N, \{123, 124, 134\})$. We state this result in the following theorem.

Theorem 5.10 *Suppose there exists a $\{123, 124, 134\}$-free hypergraph on $N+1$ points with b blocks and suppose $x \in X$ and x occurs in b_x blocks. Then there exists a $\{123, 124, 134\}$-free hypergraph on N points with at least $b - b_x$ blocks.*

Corollary 5.11 *Let* $b = \mathrm{ex}(N+1, \{123, 124, 134\})$. *Then* $b - \lfloor \frac{3b}{N+1} \rfloor \leq \mathrm{ex}(N, \{123, 124, 134\})$.

Proof. Consider a $\{123, 124, 134\}$-free hypergraph on $N + 1$ points having $b = \mathrm{ex}(N + 1, \{123, 124, 134\})$ blocks. Clearly, there is an element $x \in X$ whose frequency is at most $\lfloor \frac{3b}{N+1} \rfloor$. Apply Theorem 5.10. □

Example 5.3 *We have shown by exhaustive computer search that* $\mathrm{ex}(8, \{123, 124, 134\}) = 22$. *We can use this result to get an upper bound on* $\mathrm{ex}(9, \{123, 124, 134\})$, *as follows. Suppose that* $\mathrm{ex}(9, \{123, 124, 134\}) \geq 34$. *Then Corollary 5.11 asserts that*

$$\mathrm{ex}(8, \{123, 124, 134\}) \geq 34 - \left\lfloor \frac{3 \times 34}{9} \right\rfloor = 34 - 11 = 23.$$

This contradicts the fact that $\mathrm{ex}(8, \{123, 124, 134\}) = 22$*; hence,* $\mathrm{ex}(9, \{123, 124, 134\}) \leq 33$.
▮

We now describe a useful product construction for $\{123, 124, 134\}$-free 3-hypergraphs which allows us to build big systems from small ones and prove some asymptotic results. This construction can be viewed as a generalization of the method outlined in [6, §2].

Theorem 5.12 *Suppose there exist* $\{123, 124, 134\}$*-free* 3*-hypergraphs on* N_i *points and* m_i *blocks,* $i = 1, 2$*. Then there exists a* $\{123, 124, 134\}$*-free* 3*-hypergraph on* $N_1 N_2$ *points and* $m_1 {N_2}^3 + m_2 N_1$ *blocks.*

Proof. Let $(X, \mathcal{B})$ and $(Y, \mathcal{C})$ be the two hypothesized 3-hypergraphs. We have $|X| = N_1$, $|Y| = N_2$, $|\mathcal{B}| = m_1$ and $|\mathcal{C}| = m_2$. Define $Z = Y \times X$, and construct a set of blocks as follows.

- For every block $\{u, v, w\} \in \mathcal{B}$, construct ${N_2}^3$ blocks, $\{(i, u), (j, v), (k, w)\}$, $i, j, k \in Y$ (these are called "type 1" blocks).
- For every block $\{i, j, k\} \in \mathcal{C}$, construct N_1 blocks, $\{(i, x), (j, x), (k, x)\}$, $x \in X$ (these are called "type 2" blocks).

Denote the resulting set of $m_1 {N_2}^3 + m_2 N_1$ blocks by $\mathcal{D}$.

Clearly $(Y \times X, \mathcal{D})$ is a 3-hypergraph; we prove that it is $\{123, 124, 134\}$-free. Suppose that $\mathcal{D}$ contains a subset of three blocks, say $\mathcal{D}_0 = \{D_1, D_2, D_3\}$, which are isomorphic to $\{123, 124, 134\}$. There are four cases to consider:

1. $\mathcal{D}_0$ contains no type 1 blocks and three type 2 blocks. This case is impossible because $(Y, \mathcal{C})$ is $\{123, 124, 134\}$-free.
2. $\mathcal{D}_0$ contains one type 1 blocks and two type 2 blocks. This case is impossible because the union of any type 1 block and any type 2 block contains at least five points.
3. $\mathcal{D}_0$ contains two type 1 blocks and one type 2 blocks. The argument used in the previous case applies here as well.
4. $\mathcal{D}_0$ contains three type 1 blocks and no type 2 blocks. Suppose WLOG that $D_1 = \{(i, u), (j, v), (k, w)\}$, $D_2 = \{(i, u), (j, v), (\ell, x)\}$, and $D_3 = \{(i, u), (k, w), (\ell, x)\}$. where $\{u, v, w\}, \{u, v, x\}, \{u, w, x\} \in \mathcal{B}$. Clearly u, v, w, x are distinct, so $(X, \mathcal{B})$ is not $\{123, 124, 134\}$-free, a contradiction.

This completes the proof. □

Corollary 5.13 *Suppose there exists a* $\{123, 124, 134\}$*-free* 3*-hypergraph on* N *points and* m *blocks. Then, for all integers* $j \geq 1$*, there exists a* $\{123, 124, 134\}$*-free* 3*-hypergraph on* N^j *points and* $\frac{m}{N(N^2-1)}(N^{3j} - N^j)$ *blocks.*

Proof. The proof is by induction on j. The result is trivially true for $j = 1$, while for $j = 2$ it follows from Theorem 5.12 with $m_1 = m_2 = m$ and $N_1 = N_2 = N$. Now let $j \geq 3$ and assume the result is true for $j - 1$. Apply Theorem 5.12 with $N_1 = N^{j-1}$, $m_1 = \frac{m}{N(N^2-1)}(N^{3(j-1)} - N^{j-1})$, $N_2 = N$ and $m_2 = m$. After some simple algebra, the result follows. □

The following corollary is now immediate.

Corollary 5.14 *Suppose there exists a* $\{123, 124, 134\}$*-free* 3*-hypergraph on* N_0 *points and* m_0 *blocks. Then*

$$\limsup_{N\to\infty} \frac{\text{ex}(N, \{123, 124, 134\})}{N^3} \geq \frac{m_0}{N_0({N_0}^2 - 1)}.$$

Example 5.4 *It is easy to compute the values* $\frac{m_0}{N_0({N_0}^2-1)}$ *for* $N_0 = 4, 5, 6, 7$ *by referring to the optimal hypergraphs in Theorem 5.7. The best value obtained is when* $N_0 = 6$ *and* $m_0 = 10$*; then* $\frac{m_0}{N_0({N_0}^2-1)} = \frac{1}{21}$*. Thus*

$$\limsup_{N\to\infty} \frac{\text{ex}(N, \{123, 124, 134\})}{N^3} \geq \frac{1}{21},$$

a result first obtained in [6]. The corresponding 3*-regular splitting systems show that*

$$\limsup_{N\to\infty} \frac{m(3, N)}{N^3} \geq \frac{2}{21}.$$

∎

We now discuss a bound quoted in [6]. This bound is attributed to de Caen and can be proven using methods discussed in [2]. For completeness, we provide a short proof of this bound as well as a slight extension.

Theorem 5.15 $\text{ex}(N, \{123, 124, 134\}) \leq N^2(N-1)/18$ *for all integers* $N \geq 2$.

Proof. Let $(X, \mathcal{B})$ be a $\{123, 124, 134\}$-free 3-hypergraph on N points and m blocks. For a positive integer j, let $\binom{X}{j}$ denote all the j-subsets of X. Define the following set $\mathcal{N}$:

$$\mathcal{N} = \left\{(B, T) : B \in \mathcal{B}, T \in \tbinom{X}{3} \backslash \mathcal{B}, |B \cap T| = 2\right\}.$$

For every pair $\{x, y\} \in \binom{X}{2}$, define

$$\lambda_{\{x,y\}} = |\{B \in \mathcal{B} : \{x, y\} \subseteq B\}|.$$

It is not difficult to see that

$$|\mathcal{N}| = \sum_{\{x,y\}\in \binom{X}{2}} \lambda_{\{x,y\}}(N - 2 - \lambda_{\{x,y\}}). \tag{3}$$

Let $B = \{x, y, z\} \in \mathcal{B}$ and let $w \in X\backslash\{x, y, z\}$. Consider the three triples $T_z = \{x, y, w\}$, $T_y = \{x, z, w\}$ and $T_x = \{y, z, w\}$. At most one of these three triples can be in $\mathcal{B}$ because $(X, \mathcal{B})$ is $\{123, 124, 134\}$-free. Therefore, at least two of the three pairs (B, T_x), (B, T_y) and (B, T_z) are in the set $\mathcal{N}$. It follows immediately that

$$|\mathcal{N}| \geq 2(N - 3)m. \tag{4}$$

Now, combining (3) and (4), we obtain

$$\sum_{\{x,y\}\in \binom{X}{2}} \lambda_{\{x,y\}}(N-2-\lambda_{\{x,y\}}) \geq 2(N-3)m. \tag{5}$$

By simple counting, we have

$$\sum_{\{x,y\}\in \binom{X}{2}} \lambda_{\{x,y\}} = 3m. \tag{6}$$

Also, $\sum \lambda_{\{x,y\}}{}^2$ is minimized when all the $\lambda_{\{x,y\}}$'s are equal, so we have

$$\sum_{\{x,y\}\in \binom{X}{2}} \lambda_{\{x,y\}}{}^2 \geq \frac{(3m)^2}{\binom{N}{2}}. \tag{7}$$

Substituting (6) and (7) into (5), we obtain

$$\begin{aligned} 3m(N-2) - 2(N-3)m &\geq \frac{(3m)^2}{\binom{N}{2}}, \\ mN &\geq \frac{(3m)^2}{\binom{N}{2}}, \quad \text{and hence} \\ m &\leq \frac{N^2(N-1)}{18}, \end{aligned}$$

as desired. □

Summarizing the results discussed so far, we have that

$$\frac{2}{21} \leq \limsup_{N\to\infty} \frac{m(3,N)}{N^3} \leq \frac{1}{9}. \tag{8}$$

We note that the upper bound in (8) has recently been improved; see Muyabi [9], Li, Stinson, van Rees and Wei [7] and Talbot [11].

Theorem 5.15 leads to the following improvement of Theorem 5.5.

Theorem 5.16

$$m(r,N) \leq \binom{N}{r}\frac{2(N-r+3)}{3(N-r+1)}.$$

We now observe that Theorem 5.15 can, in some instances, be strengthened by using integer arithmetic.

Theorem 5.17 *For all integers $N \geq 2$, it holds that*

$$m = \mathrm{ex}(N, \{123, 124, 134\}) \geq \frac{j(i+1)^2 + \left(\binom{N}{2} - j\right) i^2}{N},$$

where $i = \left\lfloor 3m/\binom{N}{2} \right\rfloor$ *and* $j = 3m - i\binom{N}{2}$.

Proof. In Theorem 5.15, a pair occurs $x = 3m/\binom{N}{2}$ times on average. The fact that x is usually not an integer was ignored. We now use this fact. Let $i = \lfloor x \rfloor$. Then the closest we can get to every pair occurring an equal number of times is to have j pairs occur $i+1$ times and $\binom{N}{2} - j$ pairs occur i times. Then, manipulating Equations (3), (4), (5) and (6) from Theorem 5.15, we get

$$Nm \geq \sum_{\{x,y\}} {\lambda_{\{x,y\}}}^2 \geq j(i+1)^2 + \left(\binom{N}{2} - j \right) i^2.$$

∎

Although the previous theorem does not look like an upper bound, it is. One tries the m and N obtained from Theorem 5.15 in Theorem 5.17. If they do not obey the integer restriction, then one decreases m until they do. As examples, for $N = 7$, the upper bound is reduced from 18 to 15; for $N = 10, 11, 13$ and 14, the upper bound is reduced by 1.

6 Tables of bounds

Table 1 records some upper bounds on $N_u(m, 3)$ for small values of m. For each entry in this table, we provide a method of constructing a splitting system with the stated number of blocks. For many of the entries in Table 1, it can be shown that all the upper bounds are also lower bounds. (We do not include the proofs, but they are all elementary case analysis and/or computer verifications.)

Table 2 lists bounds and constructions for $m(N, 3)$ and $m_d(N, 3)$. Again, several of the entries in this table are exact results, as indicated.

Table 3 records some lower and upper bounds on $\mathrm{ex}(N, \{123, 124, 134\})$ for small values of N. Each table entry is accompanied by an indication of

the method used to obtain the bound. The lower bounds for $N = 10, \ldots, 15$ are obtained inductively using Corollary 5.9, in a manner similar to Example 5.2. In each case, we identify a point with maximum frequency in the previously constructed system on $N - 1$ points, which allows the construction of the system on N points.

7 Conclusion

In this paper, we mainly have studied $(m, 3)$-splitting systems. Several interesting connections with other extremal problems were found. However, much less is known about (m, t)-splitting systems for $t \geq 4$. In particular, many of the connections presented in this paper do not extend or generalize to $t \geq 4$ in a natural way. In fact, the only known results on (m, t)-splitting systems, for $t \geq 4$, are as follows:

- the bound we proved in Section 2,
- some general recursive constructions, and an existence result using the probabilistic method (see [8]), and
- some special constructions in the case $t = 4$ (see [10]).

Finally, we note that several of the results in Section 5 and Table 3 have recently been extended; see [7].

Table 1: Bounds on $N_u(m,3)$

m	$N_u(m,3)$	construction
4	$=2$	Theorem 3.1
5	$=3$	Example 1.1
6	$=4$	Theorem 3.4
7	$=3$	Theorem 3.2
8	$=4$	Theorem 3.4
9	$=5$	Theorem 4.3
10	$=5$	Example 1.4
11	$=5$	Example A.1
12	$=6$	Theorem 4.2
13	$=6$	Example A.2
14	$=6$	Theorem 3.4
15	$=5$	Example A.3
16	$=6$	Theorem 3.4
17	$=6$	Example A.4
18	$\geq 6, \leq 7$	Example A.5
19	$\geq 6, \leq 8$	Theorem 4.3
20	$\geq 6, \leq 7$	Theorem 4.2
21	$\geq 6, \leq 8$	Theorem 4.3
22	$\geq 6, \leq 8$	Theorem 3.4
23	$\geq 6, \leq 7$	Example A.6
24	$\geq 6, \leq 8$	Theorem 4.2

Table 2: Bounds on $m(N,3)$ and $m_d(N,3)$

N	$m(N,3)$	construction	$m_d(N,3)$	construction	expansion coefficient
2	$=4$	Lemma 1.6	$=2$	Theorem 3.3	1.414214
3	$=7$	Lemma 1.6	$=3$	Theorem 3.3	1.442250
4	$=10$	Example 1.5	$=4$	Theorem 3.3	1.414214
5	$=14$	Theorem 4.1	$=7$	Example 1.3	1.475773
6	≥ 24	Example A.7	$=11$	Example 4.2	1.491301
7			$=16$	Example 4.3	1.485994
8			≥ 27	Example 4.4	1.509804
9			≥ 43	Example 4.5	1.518786

Table 3: Lower and Upper Bounds for ex(N, $\{123, 124, 134\}$)

N	Lower Bound	Comment	Upper Bound	Comment
4	2	Example 5.1	2	Example 5.1
5	5	Example 5.1	5	Example 5.1
6	10	Example 5.1	10	Example 5.1
7	15	Example 5.1	15	Example 5.1
8	22	Theorem 5.8	22	Computer search
9	32	Computer search, Example A.8	33	Example 5.3
10	44	Example 5.2	47	Corollary 5.11
11	60	Theorem 5.8, $x = 7, b_x = 16$	64	Corollary 5.11
12	80	Theorem 5.8, $x = 8, b_x = 20$	85	Corollary 5.11
13	100	Theorem 5.8, $x = 1, b_x = 20$	110	Corollary 5.11
14	124	Theorem 5.8, $x = 2, b_x = 24$	140	Theorem 5.17
15	153	Theorem 5.8, $x = 6, b_x = 29$	175	Theorem 5.15

Acknowledgements

Research of the authors is supported by the following grants: a University of Manitoba, Faculty of Science startup grant (PCL), NSERC grant 203114-02 (DRS), NSERC grant 003358-02 (JvR) and NSERC grant 239135-01 (RW). DRS would like to thank Zoltan Füredi for providing useful pointers to the literature.

References

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

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

[3] W.A. Deuber, P. Erdös, D.S. Gunderson, A.V. Kostochka and A.G. Meyer. Intersection statements for systems of sets, *Journal of Combinatorial Theory A* **79** (1997), 118–132.

[4] 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.

[5] P. Erdös and E. Szemerédi. Combinatorial properties of systems of sets, *Journal of Combinatorial Theory A* **24** (1978), 308–313.

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

[7] P.C. Li, D.R. Stinson, G.H.J. van Rees and R. Wei. On $\{123, 124, 134\}$-free hypergraphs, *Congressus Numerantium*, to appear.

[8] A.C.H. Ling, P.C. Li and G.H.J. van Rees. Splitting systems and separating systems, *Discrete Mathematics* **279** (2004), 355–368.

[9] D. Muyabi. On hypergraphs with every four points spanning at most two triples, *Electronic Journal of Combinatorics* **10** (2003), Research Note N10, 4 pp.

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

[11] J. Talbot. Chromatic Turán problems and a new upper bound for the Turán density of $\mathcal{K}_4^-$, *DMTCS Proc.* **AE** (2005), 77–80 (EuroComb 2005).

A Some examples of splitting systems

Example A.1 *The blocks*

$$\{1,2,3,4,11\},\{3,5,7,8,11\},\{4,6,7,8,11\},\{5,6,9,10,11\},\ \textit{and}\ \{7,8,9,10,11\}$$

form a $(5;11,3)$*-uniform* SS *on the set* $\{1,\ldots,11\}$. ∎

Example A.2 *The blocks*

$$\{1,7,8,9,10,13\},\{1,7,8,9,11,13\},\{1,6,8,9,11,12\},\{1,5,7,10,11,13\},$$
$$\{1,4,6,7,12,13\},\ \textit{and}\ \{1,2,3,4,5,10\}$$

form a $(6;13,3)$*-uniform* SS *on the set* $\{1,\ldots,13\}$. ∎

Example A.3 *The blocks*

$$\{1,2,3,8,9,10,15\},\{1,4,5,8,11,12,15\},\{1,6,7,8,13,14,15\},$$
$$\{2,4,6,9,11,13,15\},\ \textit{and}\ \{3,5,7,10,12,14,15\}$$

form a $(5;15,3)$*-uniform* SS *on the set* $\{1,\ldots,15\}$. ∎

Example A.4 *The blocks*

$$\{1,9,10,11,12,13,14,17\},\{1,8,10,11,12,13,15,16\},\{1,6,7,11,12,14,15,17\},$$
$$\{1,4,5,7,9,14,16,17\},\{1,2,3,6,8,9,15,16\},\ \textit{and}\ \{1,3,4,5,6,7,10,13\}$$

form a $(6;17,3)$*-uniform* SS *on the set* $\{1,\ldots,17\}$. ∎

Example A.5 *The blocks*

$$\{1,\ldots,9\},\{1,\ldots,5,15,\ldots,18\},\{1,2,3,6,7,13,14,17,18\},\{3,\ldots,9,12,13\},$$
$$\{4,5,8,\ldots,12,15,16\},\{6,\ldots,14\}\ \textit{and}\ \{10,\ldots,18\}$$

form a $(7;18,3)$*-uniform* SS *on the set* $\{1,\ldots,18\}$. ∎

Example A.6 *The blocks*

$$\{1,2,6,7,11,12,13,17,18,22,23\},\{1,3,6,8,11,12,14,17,19,22,23\},$$
$$\{1,4,6,9,11,12,15,17,20,22,23\},\{2,3,4,10,11,13,14,15,21,22,23\},$$
$$\{5,7,8,9,11,16,18,19,20,22,23\},\{6,7,8,9,10,17,18,19,20,21,23\}\ \textit{and}$$
$$\{1,2,3,4,5,12,13,14,15,16,23\}$$

form a $(7;23,3)$*-uniform* SS *on the set* $\{1,\ldots,23\}$. ∎

Example A.7 *The blocks*

$$\{1,\ldots,6,21,22,23,24,\},\{1,2,7,8,9,10,15,16,21,22\},\{3,4,7,8,11,12,17,18,21,23\},$$
$$\{5,6,7,8,13,14,19,20,21,24\},\{9,\ldots,14,22,23,24\},\ \textit{and}\ \{15,\ldots,24\}$$

form a $(6;24,3)$-SS *on the set* $\{1,\ldots,24\}$. ∎

Example A.8 *The* 32 *blocks*

$$\{1,2,6\},\{1,2,8\},\{1,2,9\},\{1,3,6\},\{1,3,8\},\{1,3,9\},\{1,4,7\},\{1,4,8\},\{1,6,7\},$$
$$\{1,7,9\},\{2,4,6\},\{2,4,7\},\{2,4,9\},\{2,5,6\},\{2,5,8\},\{2,5,9\},\{2,7,8\},\{3,4,6\},$$
$$\{3,4,7\},\{3,4,9\},\{3,5,6\},\{3,5,8\},\{3,5,9\},\{3,7,8\},\{4,5,7\},\{4,5,8\},\{4,6,8\},$$
$$\{4,8,9\},\{5,6,7\},\{5,7,9\},\{6,7,8\},\ \textit{and}\ \{7,8,9\}$$

form a $\{123,124,134\}$*-free hypergraph on the set* $\{1,\ldots,9\}$. ∎