$(m, 3)$-Splitting Systems

G.H.J. van Rees and S.J. Lau
Department of Computer Science
University of Manitoba
Winnipeg, Manitoba R3T 2N2, Canada
vanrees@cs.umabitoba.ca and eijnuhs@gmail.com

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 $|B \cap Y| = \lfloor \frac{t}{2} \rfloor$. An (m,t)-splitting system is *uniform* if every block has size $\lfloor \frac{m}{2} \rfloor$ and an (m,t)-splitting system is *disjunct* or *sperner* if no block is a subset of another block. In this paper, we give several constructions and bounds for splitting systems, when $t = 3$. We consider uniform splitting systems as well as disjunct splitting systems. There are many connections with other types of set systems.

1 Introduction

First we need to know what a set system is.

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

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

Now we define our objects of interest.

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* $|B \cap Y| = \lfloor \frac{t}{2} \rfloor$.

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

In Deng, Stinson, Li, van Rees and Wei [3], there is a brief discussion on the relationship between splitting systems and w-sunflowers, see Erdös and Szemerédi [7]. If, in a set system, no block is in the union of two other blocks then the set system is also a splitting system. This leads to the connection between splitting systems and cover-free families, see Erdös, Frankl and Füredi [6].

Ling, Li and van Rees [10] studied splitting systems. Deng, Zhang, Li and van Rees [4] used the Stein-Lovász Theorem to get bounds on splitting sets. It easier to get good recursive constructions if the splitting system also has the disjunct property. This property is sometimes called the sperner property. So now we define this property.

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* $(N; m, t)$*-DSS to denote a disjunct* (m, t)*-splitting system having* N *blocks.*

If, in a set system, all points occur in exactly r blocks, the system is called *r-regular*. If the blocks in a regular set system are all unique then the set system is automatically disjunct. So this leads to the connection between 3-regular $(m, 3)$-splitting systems and {123,124,134}-free-3-hypergraphs. These hypergraphs were studied by Frankl and Füredi [8], Muyabi [11] and Li, Stinson, van Rees and Wei [9] and Talbot [14].

We will also consider another type of splitting system that we now define.

Definition 1.4 *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* $(N; m, t)$*-USS to denote a uniform* (m, t)*-splitting system having* N *blocks.*

In [13], 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. Ling, Li and van Rees [10] 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 extend some of the results of Deng, Stinson, Li, van Rees and Wei [3]. More particulary we give results on $(m,3)$-splitting systems by producing new results on disjunct $(m,3)$-splitting systems. If one were to complement the blocks of a disjunct $(m,3)$-splitting system then one would obtain the set system studied in Deuber, Erdos, Gunerson, Kostochka and Meyer [5].

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. We say that an (m,t)-splitting system is *optimal* if it has exactly $N(m,t)$ blocks. Optimality of disjunct or uniform (m,t)-splitting systems is defined in the same obvious way.

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

The following result follows immediately from the definitions.

Lemma 1.5 *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 $N_{\mathrm{reg}}(r,m,t) \geq N(m,t)$.*

The following result is also easy to prove.

Lemma 1.6 *For all m, t and r, it holds that $N(m+1,t) \geq N(m,t)$, $N_d(m+1,t) \geq N_d(m,t)$.*

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 $N(m,t)$ and $N_d(m,t)$ are monotone nondecreasing for fixed r and t, it is useful to define $m(N,t) = \max\{m : N(m,t) \leq N\}$ and $m_d(N,t)$ similarly. Many constructions of splitting systems are conveniently described using the incidence matrix representation of a splitting system and we will also refer to the incidence matrix as the splitting system.

Definition 1.7 *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 weight of a row or column is the number of 1's in it.

The following result is obvious.

Lemma 1.8 *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:*

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

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 $\lfloor \frac{m}{2} \rfloor$.*

We now give two small examples of splitting systems.

Example 1.1 *The following is the incidence matrix of a uniform (6;17,3)-splitting system.*

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

Note that any w columns can be deleted from this example to get a (6,17-w,3)-splitting system. ∎

Example 1.2 *The following is the incidence matrix of a uniform, disjunct (6;10,3)-splitting system.*

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

∎

The beautiful uniform, disjunct (6;10,3)-splitting system above is actually a (6,10,5,3,2)-Balanced Incomplete Block Design. But it has two additional properties that we will be interested in. Every two columns of the incidence matrix have a 00 row which we will call the *non-intersecting* property and every two columns of the incidence matrix have a 11 row which we call the *intersecting* property. These will occasionally be helpful.

The first theorem we present shows how to use disjunct $(m, 3)$-splitting systems to make disjunct or uniform $(m, 3)$-splitting systems.

Theorem 1.9

A	*The existence of*	*implies existence of*
1	$(N; m, 3)$-*DSS*	$(N; m+2, 3)$-*SS*
2	*uniform* $(N; m, 3)$-*DSS*	$(N; m+1, 3)$-*USS if* m *even*
3	*nonintersect.* $(N; m, 3)$-*DSS*	*(N;m+3,3)-SS*
4	*nonintersct., uniform* $(N; m, 3)$-*DSS*	$(N; m+2, 3)$-*USS*
5	*nonintersct., uniform* $(N; m, 3)$-*DSS*	$(N; m+3, 3)$-*USS if* m *even*

B	*The existence of*	*implies existence of*
1	$(N; m, 3)$-*DSS*	$(N; 2m, 3)$-*SS*
2	*uniform* $(N; m, 3)$-*DSS*	$(N; 2m, 3)$-*USS if* m *even*
3	*nonintersct.* $(N; m, 3)$-*DSS*	$(N; 2m+1, 3)$-*SS*
4	*nonintersct., uniform* $(N; m, 3)$-*DSS*	$(N; 2m+1, 3)$-*USS if* m *odd*

Proof. We note that in a disjunct $(N, m, 3)$-splitting system, there is no column of all 0's or all 1's. Further, no two columns are identical.

Consider the incidence matrix of the disjunct $(N, m, 3)$-splitting system. In case A1, add two columns of 0's. in case A2, add one column of 0's, in case A3 and A5 add two columns of 0's and a column of 1's, in case A4 add

a column of 0's and a column of 1's. Now just check that the new columns are three splitting and that the rows have the right number of 1's if the result is suppose to be uniform.

In Case B, we use each original column twice. Then in case B3 and B4 we add a column of 1's. Again just check that the properties hold. □

In the next section we give some bounds and results on disjunct $(m, 3)$-splitting systems. Any such system on N blocks we will designate with (N, m)-DSS. Then we will use those results and some others to get some results and bounds on uniform $(m, 3)$-splitting systems. Any such systems we will designate with with (N, m)-USS.

2 Bounds for $(m, 3)$-disjunct splitting systems

In order to compare splitting systems with different number of blocks and different number of elements we need a parameter that will tell us which system is better. To do this, we will use the expansion coefficient of a $(m, 3)$-splitting system as defined in [3]. The *expansion coefficient* of a $(N, m, 3)$-splitting system is $c = m^{1/N}$. The larger c is the better the splitting system.

There are two important product constructions first proved by [5].

Theorem 2.1 *If there exists a $(N_1; m_1, 3)$-DSS and an $(N_2; m_2, 3)$-DSS, then there exists an $(N_1 + N_2; m_1 m_2, 3)$-DSS.*

The construction, in terms of incidence matrices, just consists of putting every column of one matrix on top of every column of the other matrix. This is a straight forward product construction. The product expansion coefficient is between the coefficient coefficient of the two input splitting systems. Note also that if the two input systems are uniform then so is the product disjoint splitting system. One can iterate the above construction to get the following corollary.

Corollary 2.2 *If there exists an $(N_0; m_0, 3)$-DSS, then there exists a $(jN_0; {m_0}^j, 3)$-DSS for all integers $j \geq 1$.*

Given an initial $(N_0; m_0, 3)$-DSS with expansion coefficient c, it is easy to see that Corollary 2.2 implies that there is an infinite class of $(N; c^N, 3)$-

SS, all of which have expansion coefficient equal to c. Thus we have the following result.

Corollary 2.3 *If there exists a $(N_0; m_0, 3)$-DSS with expansion coefficient equal to c, then* $\limsup_{N\to\infty}(m(N,3))^{1/N} \geq c$.

Let A be an incidence matrix of a (N, m)-DSS and let $\begin{array}{|c|c|}\hline 1 & 0 \\ \hline 0 & 1 \\ \hline\end{array}$ be the incidence matrix of a (2,2)-DSS then when we multiply them together as in the product construction of Theorem 2.1 we get: $\begin{array}{|c|c|}\hline A & A \\ \hline \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} \\ \hline\end{array}$. This is the incidence matrix of an $(N+2, 2m)$-DSS. This is a doubling construction. If iterated then we get asymptotically, a DSS with expansion coefficient of $\sqrt{2} \cong 1.41421$. Further, in the construction, one of the A's could be replaced by the incidence matrix of any (N, m_1)-DSS, we still get a $(N+2, m+m_1)$-DSS. If A is only 3-splitting then the product is still 3-splitting.

There is a modified product construction that is a bit more subtle. We first need to define a concept. In a incidence matrix of of a (N, m)-DSS, a row is *heavy* if the number of 1's in it is equal to or greater than $\lceil m/2 \rceil$ 1's. If the number of 1's in the row is equal to or less than $\lceil m/2 \rceil$ then it is called *light*.

Theorem 2.4 *[5, Lemma 4.4] If there exists an $(N_1; m_1, 3)$-DSS containing a block of size k_1 and an $(N_2; m_2, 3)$-DSS containing a block of size k_2, then there exists an $(N_1 + N_2 - 2, k_1(m_2 - k_2) + k_2(m_1 - k_1))$-DSS.*

In terms of incidence matrices, the construction consists of putting every column under a 1 in row 1 of one splitting system on top of every column under a 0 in row 1 of the other the other splitting set along with putting every column under a 0 in row 1 of one splitting system on top of every column under a 1 in row 1 of the other the other splitting set. It is harder to keep track of what this modified product does to the expansion coefficient. But clearly, if there exists a $(N_1; m_1)$-DSS whose incidence matrix has a light row and there exists a $(N_2; m_2)$-DSS whose incidence matrix has a heavy row, then there is a $(N_1 + N_2; m_1 m_2, 3)$-DSS with expansion coefficient greater than expansion coefficient of the product splitting system. Just use the heavy and light rows for the modified product and the result comes from elementary arithmetic.

So if we have a splitting system with expansion coefficient c and it has a heavy row and a light row then we can iterate the product construction to get a power construction. We show this in an infinitesimally stronger version of the theorem in [5]. We show there is an extra factor of two which is useful when using this theorem for a non-asymptotic result. In anticipation of the result, we define the *asymptotic expansion coefficient* of a (N, m)-DSS to be $C = (m/2)^{1/N}$. This is only defined for (N, m)-DSS whose incidence matrices have both a light and a heavy row.

Theorem 2.5 *If there exists an $(N+2, m)$-DSS with a row with more than or equal to $m/2$ 1's and a row with more than or equal to $m/2$ 0's then there is an $(jN+2, 2C^j)$-DSS for any j a positive integer where $C = (m/2)^{1/N}$.*

Proof. Clearly the results holds for $j = 1$ and let us assume it holds for $j-1$; i.e., there exists an $((j-1)N+2, 2C^{(j-1)N})$-DSS. We need to prove this for a row which has at least $C^{(j-1)N}$ 0's and also for a row of at least $C^{(j-1)N}$ 1's as each incidence matrix has at least one such row. The proofs are similar so we will let the matrix have a row with $C^{(j-1)N} + e$ 0's where $e > 0$. Let the heavy row of the $(N+2, m)$-DSS have $m/2 + d$ 1's where $d > 0$. The modified product produces an incidence matrix with $jN + 2$ rows and at least the following number of columns,

$$\begin{aligned}
(\frac{m}{2} + d)(C^{(j-1)N} + e) + (\frac{m}{2} - d)(C^{(j-1)N} - e) &> 2(\frac{m}{2})C^{(j-1)N} \\
&= 2(\frac{m}{2})((\frac{m}{2})^{\frac{1}{N}})^{(j-1)N} \\
&= 2(\frac{m}{2})^j \\
&= 2C^j N
\end{aligned}$$

□

But how big can c or C be. In the incidence matrix of a (N, m)-DSS, the columns under the 1's in the first row must be the incidence matrix of a $(N-1, m')$-DSS. Similarly for the columns under the 0's in row 1, there must be the incidence matrix of a $(N-1, m'')$-DSS. So when we add a row we can at most double the number of columns in the incidence matrix of a DSS. This leads to the following lemma.

Lemma 2.6 *For any (N, m)-DSS, $c \leq 2$.*

So, if we are looking for optimal DSS's, then $\sqrt{2} \leq c \leq 2$ for any DSS. The obvious attack is to find splitting systems with heavy and light rows with as large an asymptotic expansion coefficient as possible. Then we know that a power of that matrix will have that asymptotic expansion coefficient as its expansion coefficient. Deuber et al. [5] got an asymptotic expansion coefficient of 1.5511 for a (50,2837219400)-DSS and Deng et al. [3] got a splitting system with $C = 1.5528$ for a (50,2988190104)-DSS. We construct one with a $C = 1.5529$ for a (28,186560)-DSS. The idea is to multiply small DSS's together keeping track of the lightest and heaviest row weights. This was done and recorded in the following tables.

#	N	m	c	C	wt	product	exten.	ref
1	3	3	1.4422	.	1	.	.	old
2	4	4	1.4142	.	1	1l,1l	1	old
3	4	4	1.4142	1.4142	2	(2,2),(2,2)	.	old
4	4	4	1.4142	4.4142	2,3	.	1	.
5	5	7	1.4757	.	3	1l,4h	4	.
6	6	10	1.4677	1.4953	5	.	.	BIBD
7	6	11	1.4913	.	4	.	5	.
8	7	15	1.4723	1.4962	7,10	.	6	.
9	7	16	1.4859	.	6	.	7	old
10	7	16	1.4859	1.5157	7,8	.	.	.
11	8	27	1.5098	1.5430	12,16	.	9	[5]
12	8	27	1.5098	.	11,12	.	10	.
13	9	43	1.5187	1.5500	16,22	1l,11h	11	.
14	10	65	1.5180	.	22,25	1l,13h	13	.
15	11	97	1.5157	1.5392	42,54	13l,4h	.	.
16	12	156	1.5232	1.5459	59,82	7l,11h	15	.
17	13	215	1.5115	1.5299	90,135	12l,8h	.	.
18	13	226	1.5173	1.5368	86,120	9l,11h	.	.
19	13	232	1.5204	1.5405	97,120	.	.	[5]
20	13	238	1.5243	.	82,93	1l,16h	16	.
21	13	245	1.5267	.	93,120	.	.	[5]
22	14	352	1.5201	1.5386	162,226	11h,11h	18	[5]
23	14	360	1.5226	1.5414	159,210	11l,11l	.	.
24	14	372	1.5261	1.5457	162,226	11l,11h	18	[3]
25	14	377	1.5276	1.5474	156,206	12l,11h	.	.
26	14	388	1.5307	.	143,156	.	19,21	[5]
27	15	608	1.5331	1.5523	256,322	13l,11h	22	.
28	16	930	1.5329	1.5507	322,478	1l,27h	27	.

Table 1

#	N	m	c	C	weight	product	ref
29	20	5493	1.5381	1.5525	2038,2900	26l,11h	.
30	22	13270	1.5395	1.5527	5152,6868	13l,27h	.
31	26	73338	1.5250	1.5346	27318,44588	22h,26l	[5]
32	26	76248	1.5409	1.5519	33978,47930	26l,24h	[3]
33	27	119788	1.5420	1.5527	44246,61958	26l,27h	.
34	28	186560	1.5425	**1.5529**	76926,102160	27l,27h	.
35	50	2837219400	1.5454	1.5511	.	31sl,31h	[5]
36	50	2837332260	1.5454	1.5511	.	31l,31h	.
37	50	2988190104	1.5470	1.5528	.	32l,32h	[3]

Table 2

We point out some of the salient features in the teo tables. We only list the lightest and heaviest rows for the splitting systems. Splitting systems 3 and 6 are uniform. whereas splitting system 5 has constant weight but is not uniform. Although splitting system 5 has constant weight, it is the product of two splitting system that are not both constant weight. Using optimal DSS's in the modified product construction does not necessarily give an optimal DSS. The DSSs above the single line in the first table are all optimal except for the (6,10) which has been given honorary optimal status. Exent. is a short form for *extension.* An extension of a splitting system consists of the incidence matrix of the splitting system having a row of 0's (or 1's) appended to it and then a collection of columns with 1 (or 0) in the last row adjoined to form a new splitting system. The term *old* means the configuration has been known for some time. Below the line in the first table and in the second table, the extensions listed do not necessarily use the splitting system listed in the tables. There is a row of weight of 352 in splitting system 28. It is not unusual for row weights to be also in the matrix size column. In [5] when, they used the modified construction to find splitting system 35 in the table, they did not use the lightest row of splitting system 31. Instead they used a row of weight 27518 to obtain their result. The results below the double line are more sporadic. The splitting systems in Table 2 have no known extensions.

If we look more carefully at the largest number of known columns for a particular number of columns as recorded in the following table, we are lead to a conjecture on $N_d(m, 3)$.

# of rows	3	4	5	6	7	8	9	10	11	12
# columns known	3	4	7	11	16	27	43	65	97	156

# of colunmns	13	14	15	16
# of columns known	245	388	608	930

Conjecture 2.7 *$N_d(m,3) \leq N_d(m-1,3) + N_d(m-2,3)$ and so $c <= \frac{1+\sqrt{5}}{2} < 1.6181$ for all (N,m)-DSS's.*

Optimal splitting systems are known with certainty for to 7 rows, see [3]. Let us try to extend this to 8 rows but first let us examine the smaller cases. It is very easy to write a backtrack program to put the columns in one at a time. Even the most straightforward program written by a mathematician can get the results for up to 6 rows. There are the unique (3,3), (5,7), (6,11) and the three (4,4) DSS's. For 7 rows, one has to be a bit more clever and do some isomorphism rejection by hand. When this is done, surprisingly, one finds three non-isomorphic copies of (7,16)-DSS. These are now listed as incidence matrices with their row and column weights.

3 non-isomorphic (7,16)-DSS's

0000000000111111	6	000111111110000	8	0000001111111010	8
0000001111000011	6	0001000001110111	7	0001110000011011	7
0000110011001100	6	0010001110001011	7	0010010001101101	7
0111010100010000	6	0100010010011101	7	0100100110010101	7
1001001001100100	6	1000100100101110	7	1001001010100111	8
1010100010100001	6	1111001001001100	8	1110000101000011	7
1100101000001010	6	1111110000000011	8	1111111000000100	8
3222323233323333		3333333333334444		3333333333333445	
a		b		c	

Doing 8 rows require even more cleverness and some number crunching. The first thing we will show is that not all columns need be considered in the search for an optimal $(8,m)$-DSS.

Theorem 2.8 *No optimal $(8,m)$-DSS has a column of weight 0,1,7 or 8.*

Proof. The disjunct property rules out the columns of weight 0 and 8. We know that there exists an (8,27)-DSS and that the optimal $(7,m)$-DSS has $m = 16$. Let us consider, in an optimal $(8,m)$-DSS, a column of weight 1 in the first column position where the 1 occurs in row 8. In order for other columns to be disjunct with it, those columns must have a zero in row 8. So those 7 rows above the 0's in row 8 form a $(7,m)$-DSS where $m \leq 16$. So the number of columns in our matrix is at most 17. This contradicts its optimality. A similar argument works if we assume a weight 7 column. $\square$

We can do a bit better.

Theorem 2.9 *If the incidence matrix of a $(8, m)$-DSS has a column of weight of 2 or 6, then $m \leq 27$ and if $m = 27$ then it is the (8,27)-DSS created in [5].*

Consider a column of weight 2 in an optimal $(8, m)$-DSS. Let the two 1's in this column be in rows 7 and 8. Then no other column can have 1's in those two rows as otherwise the matrix would not be disjunct. The other columns in the matrix either have 01 , 10 or 00 in those two rows. Call the columns above the 01's A, above the 10's B and above the 00's C. Let the number of columns in A, B, C be a, b, c respectively. Since the two rows under A are the same for every column of A, the columns of A must be a $(6, m)$-DSS so $m = a \leq 11$. Similarly, $b, c \leq 11$. Since the entry in row 7 under the columns of A and C is always a 0, the columns of A and C with a 1 or a 0 respectively adjoined to them, form a $(7, m)$-DSS so $m = a + c \leq 16$. Similarly $b + c \leq 16$. Now $a + b + c + 1 = 27 + e$ where $e \geq 0$. So $a+b+c = 26+e$ and $a+b+2c \leq 32$. So $c \leq 6-e$. So $a+b \geq 20$. So $a = 10$ or 11. If $a = 11$, then $c \leq 5$. But there is no (7,16)-DSS with weight 11 so $c \leq 4$. But then $c = 4$ and $b = 11$. But we know that A is the unique (6,11)-DSS. So the 6 by 11 was put over a row of 0's and a row of 1's. We ran a backtrack to extend this 8 by 11 matrix with columns that have a 0 in row 7 and in row 8. There were at most 2 columns that could be added so $c \leq 2$ and we could not get an optimal DSS in this way. So $a = b = 10$ and $c = 6$. But then the columns holding a and c in the rows 1-6,8 would be a (7,16)-DSS with a row of weight 10. Such a thing does not exist. So no (8,27)-DSS has a column of weight 2.

So assume there is a column of weight 6 in an optimal $(8, m)$-DSS. Let the two 0's in this column be in row 7 and 8. Then no other column can have 0's in those last two rows as otherwise the matrix would not be disjunct. The other columns in the matrix either have 01, 10 or 11 in those two rows. Call the columns above the 01's A, above the 10's B and above the 11's C. Let the number of columns in A, B, C be a, b, c respectively. As before, we have a solution: $a = b = 11, c = 5$. Again we tried to extend the 8 by 11 matrix containing the unique (6,11)-DSS sitting on a row of 0's and a row of 1's using columns that have a 1 in rows 7 and 8. Only one column could be added so no optimal DSS can be obtained this way. The other

possible solution is $a = b = 10, c = 6$. That means that columns containing A and C in the rows 1-7 form the (7,16)-DSS with a row of weight 6. There is only one such system. So we extended an 8 by 16 matrix consisting of the (7,16)-DSS with row weight 6 in the first 7 rows and a row of 1's in the eighth row with columns that contain a 0 in the last row. The largest splitting system found, and found only once, has 27 columns and is the one constructed by [5]. □

This approach of using a $(7, n)$-DSS to construct a $(8, m)$-DSS with m large can be used to find the optimal $(8, m)$-DSS. If one considers a particular row, say the last one, in an optimal $(8, m)$-DSS, the columns above the 0's must form a $(7, n)$-DSS. Similarly, the columns above the 1's form a $(7, n)$-DSS also. Since we know that there is a $(8, 27)$-DSS, then either the number of 0's or the number of 1's must be 14 or larger. So if we construct all non-isomorphic $(7, n)$-DSS where $n = 14, 15$ or 16, we can extend each one of them and then the matrices with the most columns will be optimal. This was done.

There were 4,953 $(7, \geq 14)$-DSS with no columns of weight 0,1,6,7 and with a column of weight 2. There were many isomorphic copies so we used McKay's software, Nauty [1, 2] to reduce it to 51 (7,14)-DSS's, 5 (7,15)-DSS's and 1 (7,16)-DSS. There were 217,962 $(7, \geq 14)$-DSS's with no column of weight 0,1,2,6,7 and with a column of weight 3 found. Again, using Nauty, we got 204 (7,14)-DSS's, 25 (7,15)-DSS's and the, surprisingly, 2 (7,16)-DSS's. Each one of these were extended by putting them on all 0's and later all 1's. None of the (7,14)-DSS's extended to an optimal (8,27)-DSS, whereas one of the five (7,15)'s as well as (7,16)-DSS, labelled a, extended to (8,27)-DSS, labelled d, created by [5]. Also the (7,16)-DSS, labelled b, extended to a new and surprising (8,27)-DSS, labelled e. We now display them.

We record this result in the following theorem.

Theorem 2.10 *There are two non-isomorphic optimal (8,27)-DSS's.*

This result was duplicated by constructing (8,27)-DSS's directly. Again, we used Theorem 2.8 and Theorem 2.9 to reduce the number of columns to be considered. We also used early isomorphic rejection in the search. Nevertheless, we had to use much parallelism to finally get the exact same result.

2 non-isomorphic (8,27)-DSS's

111111111111111100000000000	16	000000001111111100000001111	12
100000111110000000000111111	12	000011110000111100001110001	12
010000110001110000111000111	12	001100110011000100110010010	11
001000101001001101011011001	12	010101010101001001010100100	11
000100010100101110101101001	12	111111100000010000000001110	11
000010001010111011010100011	12	110000111100100011000011000	11
000001000111010111100010101	12	101010011010001010101000100	11
111111000000000011111111110	16	000000000000000011111111111	11
333333444444444444444444446		333333453333334333333344543	
d		e	

3 Uniform Three-Splitting Systems

For $m \leq 24$, there is the table by [3]. This has been improved by [12], by showing that there exist (7,m)-USS's for $m = 19, 21, 22, 24$. By Lemma 1.9, we know that the existence of the uniform (6,10)-DSS implies the existence of a (6,20)-USS which also improves the table. We can also match many entries in the table using Lemma 1.9. For instance, using the uniform (6,10)-DSS, we can get (6,12)-USS and from the uniform (5,7)-DSS we can get a (5,9)-USS and a (5,15)-USS. Further the uniform (4,4)-DSS can be modified multiplied by itself to give a uniform (6,8)-DSS which can be doubled to give a (6,16)-USS. Here is the up-dated table.

m	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$N_u(m,3)$	2	3	4	3	4	5	5	5	6	6	6	5	6	6

m	18	19	20	21	22	23	24
$N_u(m,3)$	6-7	6-7	6	6-7	6-7	6-7	6-7

Asymptotically, the constructions of [3] and [12] generally double the number of columns every 2 rows. This is an expansion coefficient of $\sqrt{2}$ which is approximately 1.4142. Whereas we can use the power construction in Theorem 2.5 on the (6,10)-DSS to prove that there exist an infinite family of $(4j+2, 2(1.4953^j))$-DSS from which we can construct $(4j+2, 4(1.4953^j))$-USS. This is a significantly better result.

If one is looking for bigger and better large $(m, 3)$-splitting systems, one should approach this problem by considering disjunct $(m, 3)$-splitting systems. However if one is looking for small systems or specific systems

then one will need to develop theorems and algorithms that apply only to the $(m, 3)$-splitting systems.

Acknowledgements

The authors would like to thank the referee(s) for there careful reading of the paper and pointing out errors in the paper.
Research of the first author is supported by NSERC grant 003358-02.

References

[1] B.D. McKay Practical Graph Isomorphism.*Comgressus Numerantium* **30** (1981) 45–87

[2] B.D. McKay http://cs.anu.edu.au/∼ bdm/nauty May 4 2009.

[3] D. Deng, D.R. Stinson, P.C. Li, G.H.J. van Rees and R. Wei. Constructions and Bounds for (m, t)-Splitting Systems, *Discrete Math.* **307** (2007) 18–37.

[4] D. Deng, Y. Zhang, P.C. Li and G.H.J. van Rees The Stein-Lovasz Theorem and its Application to Some Combinatorial Arrays, *J. of Combin. Math. Combin. Computing*, accepted.

[5] 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.

[6] 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.

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

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

[9] P.C. Li, D.R. Stinson, G.H.J. van Rees and R. Wei. On $\{123, 124, 134\}$-free hypergraphs, *Congressus Numerantium* bf 183 (2006), 161–174

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

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

[12] D. Roh, S.G. Hahn. Constructions for $(m, 3)$-uniform splitting systems, *preprint*.

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

[14] 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).