Threshold Schemes from Combinatorial Designs

P. J. Schellenberg and D. R. Stinson
University of Waterloo and University of Manitoba

Abstract Informally, a \((t, w, v; m)\)-threshold scheme is a way of distributing partial information (chosen from a set of \(v\) shadows) to \(w\) participants, so that any \(t\) of them can easily calculate one of \(m\) possible keys, but no subset of fewer than \(t\) participants can determine the key. A perfect threshold scheme is one in which no subset of fewer than \(t\) participants can determine any partial information regarding the key. In this paper, we study the number \(M(t, w, v)\), which denotes the maximum value of \(m\) such that a perfect \((t, w, v; m)\)-threshold scheme exists. It has been shown previously that \(M(t, w, v) \leq (v - t + 1) / (w - t + 1)\), with equality occurring if and only if there is a Steiner system \(S(t, w, v)\) that can be partitioned into Steiner systems \(S(t - 1, w, v)\). In this paper, we study the numbers \(M(t, w, v)\) in some cases where this upper bound cannot be attained. In particular, we determine improved bounds on the values \(M(3, 3, v)\) and \(M(4, 4, v)\).

1. Introduction

A \(w\)-uniform hypergraph is a pair \((X, \mathcal{A})\), where \(X\) is a set of elements called points, and \(\mathcal{A}\) is a collection of \(w\)-subsets (blocks) of \(X\). We allow \(\mathcal{A}\) to contain "repeated" blocks; the multiplicity of a block is the number of times it occurs in \(\mathcal{A}\). If every subset in \(\mathcal{A}\) has multiplicity one (i.e. \(\mathcal{A}\) is a set), then we say that \((X, \mathcal{A})\) is simple.

A perfect \((t, w, v; m)\)-threshold scheme is a simple \(w\)-uniform hypergraph \((X, \mathcal{A})\), where \(X\) is a set of \(v\) points (which we refer to as shadows), together with a partition of the block set \(\mathcal{A}\) into \(m\) parts, say \(\mathcal{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_m\}\), such that the following properties are satisfied:

1) if \(B \in \mathcal{A}_i\) and \(B' \in \mathcal{A}_j\), where \(i \neq j\), then \(B \cap B' < t\) (i.e. all blocks containing any fixed subset \(S\) of \(t\) shadows occur in the same \(\mathcal{A}_i\)),
2) for any subset \(S\) of \(t' < t\) shadows, there exists a non-negative integer \(\lambda(S)\) such that for every \(i\) \((1 \leq i \leq m)\) there are exactly \(\lambda(S)\) blocks \(B\) such that \(S \subseteq B \in \mathcal{A}_i\) (i.e. there are the same number of blocks containing a subset \(S\) of \(t' < t\) shadows in each of the \(m\) \(\mathcal{A}_i\)'s).

We note that property 2) implies that every \(\mathcal{A}_i\) contains the same number of blocks.

The application of threshold schemes is to give partial information (shadows) to \(w\) people, so that any \(t\) of them can determine a key, but no group of fewer than \(t\) can do so. For example, the key could be the combination of a safe, and we might desire that two of three specified people be required in order to determine this combination. This would correspond to a threshold scheme with \(t = 2\) and \(w = 3\).

Suppose there are m possible keys, namely the integers 1, 2, ..., m. Let \((X, \mathcal{A})\) be a perfect 
\((t, w, v; m)\)-threshold scheme, which is made known to all w participants. Now, suppose we 
want to distribute shadows corresponding to key \(k\) \((1 \leq k \leq m)\). We do this by choosing at 
random a block \(B \in \mathcal{A}_k\). Then, we give each of the w participants a different shadow in \(B\). 

Property 1) ensures that any \(t\) participants can determine the set \(\mathcal{A}_k\), and hence the key (namely, 
\(k\)), from the \(t\) shadows they collectively hold. Property 2) ensures that it is impossible for a 
group of \(t' (< t)\) participants to obtain any partial information about the key.

These ideas are made rigorous in terms of probability distributions, as follows. We assume that 
there is a fixed probability distribution on the set of keys \([1, \ldots, m]\), known to all the 
participants. Suppose a subset of the participants have been given the shadows in the set \(S \subseteq B\). 
They can then calculate a conditional probability distribution on the keys, given the shadows that 
they possess (see, for example, [24]). If it happened that \(p(k) \neq p(k \mid S)\) for some key \(k\), then 
these participants would have obtained some (partial) information regarding the actual key that 
was sent. Property 2) guarantees that \(p(k) = p(k \mid S)\), for every key \(k\), and for every subset \(S\) of 
fewer than \(t\) shadows that occur in some block.

Threshold schemes were first described by Shamir [12] and Blakley [3] in 1979. Since then, 
many constructions have been given for threshold schemes. Most of these constructions have 
employed techniques from linear algebra. In [14], Stinson and Vanstone investigated the 
combinatorial properties of threshold schemes, and gave some new constructions for threshold 
schemes based on combinatorial designs. They presented constructions for perfect threshold 
schemes with \(t = 3\) and \(w = 3\) and 4 that handled more keys than previously known schemes did.
The implementation of these schemes was also discussed. We continue this investigation in the 
remainder of this paper. We note that all threshold schemes discussed in this paper are perfect.

2. A combinatorial characterization of perfect threshold schemes

A characterization of perfect threshold schemes in terms of the blocks corresponding to each key 
was presented in [14]. Suppose \((X, \mathcal{A})\) is a \(w\)-uniform hypergraph. Given any integer \(t' \leq w\), 
define a \(t'\)-uniform hypergraph \((X, \mathcal{A}(t'))\), where \(\mathcal{A}(t')\) is the multiset union 
\[ \bigcup_{\mathcal{A} \in \mathcal{A}} \{S : |S| = t', S \subseteq \mathcal{A} \}. \]
Note that \(\mathcal{A}(t')\) need not be simple, even if \(\mathcal{A}\) is. We say that 
\((X, \mathcal{A}(t'))\) is the \(t'\)-induced hypergraph of \((X, \mathcal{A})\).

Two \(w\)-uniform hypergraphs \((X, \mathcal{A}_1)\) and \((X, \mathcal{A}_2)\) are defined to be \(t\)-compatible if the 
following two properties are satisfied:

1) \(\mathcal{A}_1(t-1) = \mathcal{A}_2(t-1)\), and
2) \(\mathcal{A}_1(t) \cap \mathcal{A}_2(t) = \emptyset\).

The following result characterizes perfect \((t, w, v; m)\)-threshold schemes in terms of \(t\)-compatible 
w-uniform hypergraphs.
Theorem 2.1 [14] There exists a perfect \((t, w, v; m)\)-threshold scheme if and only if there exist \(m\) mutually \(t\)-compatible \(w\)-uniform hypergraphs on \(v\) points.

Our interest is in finding the maximum number of keys, \(m\), that can be handled by a perfect threshold scheme, given \(t, w,\) and \(v\). We shall also require that every shadow occurs \(at least\) one block (otherwise, we can take the number of shadows to be some number less than \(v\)). This maximum number of keys is denoted \(M(t, w, v)\). In view of Theorem 2.1, \(M(t, w, v)\) also denotes the maximum number of mutually \(t\)-compatible \(w\)-uniform hypergraphs on \(v\) points (in which every point occurs in at least one block). The following upper bound on \(M(t, w, v)\) was presented in [14].

Theorem 2.2 [14] \(M(t, w, v) \leq (v - t + 1) / (w - t + 1)\).

In [14], a characterization of when equality can be met in the above bound is obtained. This characterization is given in terms of certain combinatorial designs (for a general reference on design theory, we mention [2]). Let \(1 \leq t \leq w < v\). A Steiner system \(S(t, w, v)\) is a simple \(w\)-uniform hypergraph \((X, \mathcal{A})\) on \(v\) points such that every \(t\)-subset of points occurs in a (unique) block. That is, \(\mathcal{A}(t)\) consists of every \(t\)-subset of \(X\), occurring once each. We say that the Steiner system is partitionable if we can partition the block set \(\mathcal{A}\) into sets \(\mathcal{A}_1, \ldots, \mathcal{A}_j\) (where \(j = (v - t + 1) / (w - t + 1)\)) such that each \((X, \mathcal{A}_i)\) \((1 \leq i \leq j)\) is a Steiner system \(S(t - 1, w, v)\).

Theorem 2.3 [14] \(M(t, w, v) = (v - t + 1) / (w - t + 1)\) if and only if there exists a Steiner system \(S(t, w, v)\) that can be partitioned into Steiner systems \(S(t - 1, w, v)\).

As a consequence of this theorem, the numbers \(M(t, w, v)\) can be determined exactly in certain circumstances.

Theorem 2.4 [7, 8] Suppose \(v \equiv 1\) or \(3\) modulo \(6\), \(v > 7\), and \(v \neq 141, 283, 501, 789, 1501,\) or \(2365\). Then \(M(3, 3, v) = v - 2\).

Proof: In [7, 8], Lu proves that the set of all \(3\)-subsets of a \(v\)-set (where \(v\) is as stated above) can be partitioned into \(S(2, 3, v)\).

It is worth remarking that, when \(v = 7\), it is impossible to partition the set of all \(3\)-subsets of a \(v\)-set into \(S(2, 3, v)\) (see, for example, [4]). The existence of such a partition for the remaining six exceptions of \(v\) in Theorem 2.4 is unresolved.

Theorem 2.5 [1, 18] For every integer \(j \geq 1\), \(M(3, 4, 2^j) = 2^{2j} - 1 - 1\).

Proof: In [1] and [18], it is shown that there exists a partition of the planes of the affine geometry \(AG(2j, 2)\) (which form an \(S(3, 4, 2^j)\)) into Steiner systems \(S(2, 4, 2^j)\).

Exact values of \(M(2, w, v)\) are known whenever a resolvable \((v, w, 1)\)-BIBD exists. For example, known results concerning resolvable BIBDs imply the following.
Theorem 2.6 1) For all \( v \equiv 3 \mod 6 \), \( M(2, 3, v) = \frac{(v - 1)}{2} \).
2) For all \( v \equiv 4 \mod 12 \), \( M(2, 4, v) = \frac{(v - 1)}{3} \).
3) For all \( v \equiv 5 \mod 20 \), \( v = 123105 \), \( M(2, 5, v) = \frac{(v - 1)}{4} \).
4) For any \( k \geq 3 \), there exists a constant \( c(k) \) such that \( M(2, k, v) = \frac{(v - 1)}{k - 1} \) for all \( v > c(k) \) such that \( v \equiv k \mod k(k - 1) \).
5) For any prime power \( q \), \( M(2, q, q^2) = q + 1 \).

Proof: Resolvable \((v, 3, 1)-\)BIBDs are shown to exist in [9]; resolvable \((v, 4, 1)-\)BIBDs in [5]; and resolvable \((v, 5, 1)-\)BIBDs in [19]. For any \( k \geq 3 \), asymptotic existence of resolvable \((v, k, 1)-\)BIBDs was shown in [10]. The resolvable BIBDs in 5) are affine planes.

3. Some upper bounds on \( M(t, w, v) \)

One way to approach the construction of a perfect \((t, w, v; m)-\)threshold scheme is to start with a fixed \((t - 1)-\)uniform hypergraph on \( v \) points, say \((X, \mathcal{S})\), and attempt to find \( t \)-compatible \( w \)-uniform hypergraphs \( \mathcal{A}_1, \ldots, \mathcal{A}_m \) such that \( \mathcal{A}_i(t - 1) = \mathcal{S}, 1 \leq i \leq m \) (that is, so that \((X, \mathcal{S})\) is the \((t - 1)-\)induced hypergraph of \((X, \mathcal{A}_i), 1 \leq i \leq m \)). Given \( t, w, \) and \( \mathcal{S} \), we would want to find the maximum number of such hypergraphs (= the maximum number of keys in the resulting threshold system). We denote this number by \( M(t, w, v, \mathcal{S}) \). Hence,

\[
M(t, w, v) = \max \{ M(t, w, v, \mathcal{S}) : (X, \mathcal{S}) \text{ is a } (t - 1)-\text{uniform hypergraph on } v \text{ points} \}.
\]

So, we might learn more about \( M(t, w, v) \) by studying the numbers \( M(t, w, v, \mathcal{S}) \). The following upper bound on \( M(t, w, v, \mathcal{S}) \) was presented in [14].

Theorem 3.1 [14] Suppose \((X, \mathcal{S})\) is a \((t - 1)-\)uniform hypergraph on \( v \) points. Let \( \lambda \) be the largest multiplicity of any \((t - 1)-\)subset in \( \mathcal{S} \). Let \( u \) denote the smallest positive integer such that

\[
\binom{u}{w - t + 1} \geq \lambda.
\]

Then \( M(t, w, v, \mathcal{S}) \leq \frac{(v - t + 1)}{u} \).

Corollary 3.2 Suppose \((X, \mathcal{S})\) is a \((t - 1)-\)uniform hypergraph on \( v \) points which is not simple. Then \( M(t, w, v, \mathcal{S}) \leq \frac{(v - t + 1)}{(w - t + 2)} \).

Proof: In Theorem 3.1, \( \lambda \geq 2 \), so \( u \geq w - t + 2 \).}

Corollary 3.2 suggests that we are most likely to maximize \( M(t, w, v, \mathcal{S}) \) when \((X, \mathcal{S})\) is simple, since the upper bound in Corollary 3.2 is already a factor of \( \frac{(v - t + 1)}{(w - t + 2)} \) less than the upper bound of Theorem 2.2.

Let's now try to improve the bound of Theorem 3.1, when \((X, \mathcal{S})\) is a simple \((t - 1)-\)uniform hypergraph on \( v \) points. For any induced \((t - 2)-\)subset \( B \in \mathcal{S}(t - 2) \), define
\[ N(B) = \{ x: B \cup \{x\} \notin \mathcal{S} \}. \]

We say that \( N(B) \) is the *neighbourhood* of \( B \). Also, define the *deficiency* of \( \mathcal{S} \) to be

\[ d(\mathcal{S}) = \max \left\{ \left| \bigcup_{x \in A} N(A \setminus \{x\}) \right| : A \in \mathcal{S} \right\}. \]

**Theorem 3.3** Suppose \((X, \mathcal{S})\) is a simple \((t-1)\)-uniform hypergraph on \( v \) points. Then

\[ M(t, v, \mathcal{S}) \leq (v - t + 1 - d(\mathcal{S})) / (w - t + 1). \]

**Proof:** Suppose there exist \( m \) \( t \)-compatible \( w \)-uniform hypergraphs, \( A_1, \ldots, A_m \), such that

\[ A_i(t-1) = \emptyset, \; 1 \leq i \leq m. \]

Choose \( A \in \mathcal{S} \) such that

\[ \left| \bigcup_{x \in A} N(A \setminus \{x\}) \right| = d(\mathcal{S}). \]

Each \( A_i \) contains a (unique) block \( A_i \) such that \( A \subseteq A_i \). Suppose \( x \in A \), and \( 1 \leq i \leq m \). Then

\[ |N(A \setminus \{x\}) \cap A_i| = 0. \]

Also, \( |A_i \setminus A| \cap (A_j \setminus A)| = 0 \) if \( i \neq j \). It follows that \( m(w - t + 1) \leq v - t + 1 - d(\mathcal{S}) \), which gives the desired inequality. \( \blacksquare \)

**4. The numbers \( M(3, 3, v) \)**

As indicated in Theorem 2.4, the numbers \( M(3, 3, v) \) are almost all determined when \( v \equiv 1 \) or 3 modulo 6. In this section, we investigate these numbers when \( v = 0, 2, 4, \) or 5 modulo 6. We establish upper bounds on \( M(3, 3, v) \) using the results proved in Section 3. First, let's note that \( M(3, 3, v) = 1 \) if \( v \leq 5 \); hence we shall assume that \( v \geq 6 \) for the remainder of this section.

\( (3, 3; v; m) \)-threshold schemes are related to packings of pairs into triples. It will be useful to define some terminology. A *\((2,3)\)-packing* is a 3-uniform hypergraph \((X, \mathcal{A})\), such that every pair of points is contained in at most one block (i.e. \( \mathcal{A}(2) \) is simple). The *leave* of the packing is the graph \( \mathcal{A}(2)^c \), where the superscript \( c \) denotes complement. That is, the leave consists of all pairs which do not occur in a block of the packing.

A \((2,3)\)-packing \((X, \mathcal{A})\) is said to be *maximum* if there does not exist any \((2,3)\)-packing on \(|X|\) points with more blocks. The packing number \( D(2,3,v) \) is defined to be the number of blocks in a maximum \((2,3)\)-packing on \( v \) points. The packing numbers \( D(2,3,v) \) and the leaves of the maximum packings have been determined exactly, in [11] and [13]. We summarize these results in the following two theorems.

**Theorem 4.1** [11, 13] The packing numbers \( D(2,3,v) \) are as follows:

1) If \( v \equiv 1 \) or 3 modulo 6, then \( D(2,3,v) = v(v-1)/6 \).
2) If \( v \equiv 5 \) modulo 6, then \( D(2,3,v) = (v(v-1)-8)/6 \).
3) If \( v \equiv 0 \) or 2 modulo 6, then \( D(2,3,v) = v(v-2)/6 \).
4) If \( v \equiv 4 \) modulo 6, then \( D(2,3,v) = (v(v-2)-2)/6 \).

**Theorem 4.2** [11, 13] Leaves of maximum \((2,3)\)-packings are isomorphic to the following graphs:
1) If \( v \equiv 1 \) or 3 modulo 6, then the leave is \((K_v)^c\).
2) If \( v \equiv 5 \) modulo 6, then the leave is a 4-cycle.
3) If \( v \equiv 0 \) or 2 modulo 6, then the leave is a one-factor.
4) If \( v \equiv 4 \) modulo 6, then the leave is the disjoint union of \((v - 4) / 2\) edges and one \(K_1, 3\).

In fact, the leave of any \((2, 3)\)-packing must satisfy certain obvious numerical properties, which we state without proof.

**Theorem 4.3** Suppose \( L \) is the leave of a \((2, 3)\)-packing on \( v \) points. Then the following properties hold:

i) for any point \( x \), \( d(x) \equiv (v - 1) \) modulo 2, where \( d(x) \) denotes the degree of \( x \) in \( L \), and
ii) \( e \equiv v(v - 1) / 2 \) modulo 3, where \( e \) denotes the number of edges in \( L \).

Now, suppose we have 3-compatible 3-uniform hypergraphs \( A_1, \ldots, A_m \) such that \( A_i(2) = S_i \), \( 1 \leq i \leq m \). \( S \) is a 2-hypergraph on \( v \) points (i.e. a graph with (possibly) repeated edges, but with no isolated vertices). If \( S \) has a repeated edge, then \( M(3, 3, v, S) \leq (v - 2) / 2 \), by Corollary 3.2. If \( S \) is simple, then each \( A_i \) is a \((2, 3)\)-packing with leave \( S_i \). Then, \( M(3, 3, v, S) \leq v - 2 - d(S) \), by Theorem 3.3. A lower bound on \( d(S) \) will give us an upper bound on \( M(3, 3, v, S) \). Properties of leaves will then allow us to find upper bounds on \( M(3, 3, v) \).

For example, when \( v \equiv 0 \) or 2 modulo 6, we have the following.

**Lemma 4.4** If \( v \equiv 0 \) or 2 modulo 6, then \( M(3, 3, v) \leq v - 4 \).

**Proof:** Suppose we have 3-compatible 3-uniform hypergraphs \( A_1, \ldots, A_m \) such that \( A_i(2) = S_i \), \( 1 \leq i \leq m \). As observed above, if \( S \) has a repeated edge, then \( M(3, 3, v, S) \leq (v - 2) / 2 \), and if \( S \) is simple, then \( M(3, 3, v, S) \leq v - 2 - d(S) \). Since we can assume \( v \geq 6 \), we will be done if we can show that \( d(S) \geq 2 \) if \( S \) is simple. Since \( v \) is even, each point \( x \) has odd degree in the leave, \( S \) (Theorem 4.3). It follows that we can find an edge \( xy \) of \( S \) such that \( |N(x) \cup N(y)| \geq 2 \) (note that this is not true if we allow \( S \) to contain isolated vertices). Hence, \( d(S) \geq 2 \), as required. \( \blacksquare \)

It is also easy to characterize \( S \) when equality occurs in the above bound.

**Lemma 4.5** If \( v \equiv 0 \) or 2 modulo 6 and \( M(3, 3, v, S) = v - 4 \), then each \( A_i \) is a maximum packing of pairs into triples.

**Proof:** For every edge \( xy \) of \( S \), we must have that \( |N(x) \cup N(y)| \leq d(S) = 2 \). Also, for every vertex \( x \), \( x \) has odd degree in \( S \). This can happen only when \( S \) is a one-factor of the point set. Hence, each \( A_i \) is a maximum packing, by Theorem 4.2. \( \blacksquare \)

**Corollary 4.6** If \( v \equiv 0 \) or 2 modulo 6 and \( M(3, 3, v, S) = v - 4 \), then there exists a partition of all triples which do not contain a pair from \( S \) into maximum packings of triples.
Proof: The number of such triples is \(v(v - 1)(v - 2)/6 - v(v - 2)/2 = v(v - 2)(v - 4)/6\). Each of the \(v - 4\) maximum packings uses \(v(v - 2)/6\) of these triples, which is all of them. We can construct such a set of maximum packings of triples whenever \(v \equiv 2\) or 6 modulo 12, as follows.

**Theorem 4.7** If \(v \equiv 2\) or 6 modulo 12, \(v \geq 6\), \(v \neq 14, 282, 566, 1002, 1578, 3002,\) or 4730, then \(M(3, 3, v) = v - 4\).

**Proof:** Let \(v = 2v';\) then \(v' \equiv 1\) or 3 modulo 6. Start with a Steiner system \(S(3, 3, v')\) which is partitionable into a set of \(v' - 2\) Steiner systems \(S(2, 3, v')\), say \(A_1, \ldots, A_{v' - 2}\), on point set \([1, \ldots, v']\). From each \(A_i, 1 \leq i \leq v' - 2\), construct two maximum packings, \(A_i,1\) and \(A_i,2\), on point set \([1, \ldots, v']\), as follows. Define

\[A_{i,1} = \{(x, y, z), (x + v', y, z + v'), (x, y + v', z + v'), (x + v', y + v', z): (x, y, z) \in A_i\}\]

and

\[A_{i,2} = \{(x, y, z + v'), (x, y + v', z), (x + v', y, z), (x + v', y + v', z + v'): (x, y, z) \in A_i\}.

It is easy to see that \(A_{i,1}\) and \(A_{i,2}\) are both maximum packings, covering every pair except those in the one-factor \(\mathcal{F} = \{(j, j + v'): 1 \leq j \leq v'\}\). Also, it is easy to see that no two of these \(2(v' - 2) = v - 4\) packings contain a common triple; hence they are 2-compatible.

We can also show that \(M(3, 3, 8) = 4\); see Example 4.1.

**Example 4.1** A \((3, 3, 8; 4)\)-threshold scheme. The leave \(\mathcal{F}\) is the one-factor \([\{1, 5\}, \{2, 6\}, \{3, 7\}, \{4, 8\}].\)

\[
\begin{array}{cccc}
A_1 & A_2 & A_3 & A_4 \\
[5, 6, 7] & [6, 7, 8] & [7, 8, 1] & [8, 1, 2] \\
\end{array}
\]

Next, we consider the case \(v \equiv 5\) modulo 6.

**Lemma 4.8** If \(v \equiv 5\) modulo 6, then \(M(3, 3, v) \leq v - 4\).

**Proof:** As in Lemma 4.4, it suffices to show that \(d(\mathcal{F}) \geq 2\) if \(\mathcal{F}\) is simple. Since \(v\) is odd, every point has even degree in \(\mathcal{F}\). As well, there must be some point \(x\) having positive degree in \(\mathcal{F}\), since \(\mathcal{F}\) has at least one edge (Theorem 4.3). Then, for any \(y\) such that such that \(xy\) is an edge
of $S$, we have that $|N(x) \cup N(y)| \geq 2$; hence, $d(S) \geq 2$, as required.

Again, equality can occur in the above bound only when each $A_i$ is a maximum packing.

**Lemma 4.9** If $v \equiv 5$ modulo 6 and $M(3, 3, v, S) = v - 4$, then each $A_i$ is a maximum packing of pairs into triples.

**Proof:** It is easy to see that if $d(S) = 2$, then $S$ is a 4-cycle.

**Lemma 4.10** If $v \equiv 4$ modulo 6, then $M(3, 3, v) \leq v - 6$.

**Proof:** Here, it suffices to show that $d(S) \geq 4$ if $S$ is simple. Since $v$ is even, every point has odd degree in $S$. Also, there must be some point $x$ having degree $\geq 3$ in $S$, since $S$ has more than $v / 2$ edges (Theorem 4.3). Then, there exists a $y$ such that $xy$ is an edge of $S$ having $|N(x) \cup N(y)| \geq 4$; hence, $d(S) \geq 4$, as required.

We now characterize when equality can occur in the above bound.

**Lemma 4.11** If $v \equiv 4$ modulo 6 and $M(3, 3, v) = v - 6$, then all the $A_i$'s are $(2, 3)$-packings having the same leave $S$ which must be isomorphic to one of the following four graphs:

Finally, we consider the case $v \equiv 4$ modulo 6.

**Lemma 4.10** If $v \equiv 4$ modulo 6, then $M(3, 3, v) \leq v - 6$.

**Proof:** Here, it suffices to show that $d(S) \geq 4$ if $S$ is simple. Since $v$ is even, every point has odd degree in $S$. Also, there must be some point $x$ having degree $\geq 3$ in $S$, since $S$ has more than $v / 2$ edges (Theorem 4.3). Then, there exists a $y$ such that $xy$ is an edge of $S$ having $|N(x) \cup N(y)| \geq 4$; hence, $d(S) \geq 4$, as required.

<table>
<thead>
<tr>
<th>$A_1$</th>
<th>$A_2$</th>
<th>$A_3$</th>
<th>$A_4$</th>
<th>$A_5$</th>
<th>$A_6$</th>
<th>$A_7$</th>
</tr>
</thead>
<tbody>
<tr>
<td>079</td>
<td>179</td>
<td>279</td>
<td>379</td>
<td>479</td>
<td>579</td>
<td>679</td>
</tr>
<tr>
<td>081</td>
<td>181</td>
<td>281</td>
<td>381</td>
<td>481</td>
<td>581</td>
<td>681</td>
</tr>
<tr>
<td>016</td>
<td>120</td>
<td>231</td>
<td>342</td>
<td>453</td>
<td>564</td>
<td>605</td>
</tr>
<tr>
<td>025</td>
<td>136</td>
<td>240</td>
<td>351</td>
<td>462</td>
<td>503</td>
<td>614</td>
</tr>
<tr>
<td>034</td>
<td>145</td>
<td>256</td>
<td>360</td>
<td>401</td>
<td>512</td>
<td>623</td>
</tr>
<tr>
<td>712</td>
<td>724</td>
<td>736</td>
<td>741</td>
<td>751</td>
<td>761</td>
<td>704</td>
</tr>
<tr>
<td>735</td>
<td>745</td>
<td>750</td>
<td>760</td>
<td>702</td>
<td>713</td>
<td></td>
</tr>
<tr>
<td>746</td>
<td>756</td>
<td>762</td>
<td>723</td>
<td>734</td>
<td>725</td>
<td></td>
</tr>
<tr>
<td>813</td>
<td>823</td>
<td>835</td>
<td>840</td>
<td>852</td>
<td>863</td>
<td>802</td>
</tr>
<tr>
<td>826</td>
<td>846</td>
<td>841</td>
<td>856</td>
<td>861</td>
<td>801</td>
<td>815</td>
</tr>
<tr>
<td>845</td>
<td>850</td>
<td>860</td>
<td>812</td>
<td>803</td>
<td>824</td>
<td>834</td>
</tr>
<tr>
<td>914</td>
<td>925</td>
<td>930</td>
<td>945</td>
<td>950</td>
<td>962</td>
<td>901</td>
</tr>
<tr>
<td>923</td>
<td>934</td>
<td>946</td>
<td>961</td>
<td>963</td>
<td>904</td>
<td>924</td>
</tr>
<tr>
<td>956</td>
<td>960</td>
<td>951</td>
<td>902</td>
<td>912</td>
<td>913</td>
<td>935</td>
</tr>
<tr>
<td>t15</td>
<td>t26</td>
<td>t34</td>
<td>t46</td>
<td>t56</td>
<td>t60</td>
<td>t03</td>
</tr>
<tr>
<td>t24</td>
<td>t35</td>
<td>t50</td>
<td>t52</td>
<td>t02</td>
<td>t14</td>
<td>t12</td>
</tr>
<tr>
<td>t36</td>
<td>t40</td>
<td>t61</td>
<td>t01</td>
<td>t13</td>
<td>t23</td>
<td>t45</td>
</tr>
</tbody>
</table>
where

\[
\begin{align*}
K_{1,3} & \cup (v - 4) / 2 K_2 \\
G_1 & \cup (v - 6) / 2 K_2 \\
K_4 & \cup (v - 4) / 2 K_2 \\
G_2 & \cup (v - 8) / 2 K_2
\end{align*}
\]

Proof: It is easy to see that for each $S^c$ above, $d(S^c) = 4$.

If $S^c$ has a vertex of degree 5, then $d(S^c) \geq 5$, and if $S^c$ has two vertices of degree 3 at a distance greater than 2, then $d(S^c) \geq 6$. Therefore, we only consider leaves $S^c$ having degrees 1 and 3, and in which the distance between any two vertices of degree 3 is at most 2. Furthermore, the number of vertices of degree 3 is congruent to 1 modulo 3 because $S^c$ is the leave of a $(2, 3)$-packing on $v \equiv 4$ modulo 6 elements.

Let $S^c$ be a leave for which $d(S^c) = 4$. Then the induced subgraph of the vertices of degree 3 in $S^c$ is a connected graph of diameter at most 2. Call this graph $T$.

To obtain a contradiction, assume $S^c$ has at least 7 vertices of degree 3. Then no vertex of $T$ can have degree 1 because of the diameter and degree constraints. If $T$ has a vertex $x$ of degree 2, then the diameter and degree constraints imply that $T$ contains a subgraph isomorphic to

![Diagram](image)

This completely determines the neighbourhoods of $u$ and $v$ in $S^c$. It follows that $|N(x) \cap N(y)| = 1$ and hence, $d(S^c) \geq 5$. This establishes that $T$ is a 3-regular graph.

If $x$ and $y$ are two nonadjacent vertices of $T$ and $|N(x) \cap N(y)| = 1$, then $d(S^c) \geq 5$. Hence, $T$ must contain a subgraph isomorphic to

![Diagram](image)
in which each of \( u, v \) and \( w \) has two common neighbours with \( x \). Now, the distance constraint implies that \( T \) contains no further vertices. Thus we must conclude that \( T \) has 7 vertices of degree 3, which is impossible.

This establishes that \( T \) has either 1 or 4 vertices. The result now follows by considering all possible induced subgraphs \( T \) on 4 vertices. ■

We now consider the construction of \((3, 3, 10; 4)\)-threshold schemes, for each of the four possible leaves of Lemma 4.11.

**Example 4.3** A \((3, 3, 10; 4)\)-threshold scheme. The leave of each packing is the disjoint union of \( K_4 \) with 3 \( K_2 \).

<table>
<thead>
<tr>
<th>( A_1 )</th>
<th>( A_2 )</th>
<th>( A_3 )</th>
<th>( A_4 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>157</td>
<td>257</td>
<td>357</td>
<td>457</td>
</tr>
<tr>
<td>169</td>
<td>269</td>
<td>369</td>
<td>469</td>
</tr>
<tr>
<td>180</td>
<td>280</td>
<td>380</td>
<td>480</td>
</tr>
<tr>
<td>258</td>
<td>358</td>
<td>458</td>
<td>158</td>
</tr>
<tr>
<td>260</td>
<td>360</td>
<td>460</td>
<td>160</td>
</tr>
<tr>
<td>279</td>
<td>379</td>
<td>479</td>
<td>179</td>
</tr>
<tr>
<td>359</td>
<td>459</td>
<td>159</td>
<td>259</td>
</tr>
<tr>
<td>368</td>
<td>468</td>
<td>168</td>
<td>268</td>
</tr>
<tr>
<td>370</td>
<td>470</td>
<td>170</td>
<td>270</td>
</tr>
<tr>
<td>450</td>
<td>150</td>
<td>250</td>
<td>350</td>
</tr>
<tr>
<td>467</td>
<td>167</td>
<td>267</td>
<td>367</td>
</tr>
<tr>
<td>489</td>
<td>189</td>
<td>289</td>
<td>389</td>
</tr>
</tbody>
</table>

Another \((3, 3, 10; 4)\)-threshold scheme is given by the following example.

**Example 4.4** The leave of each packing is the union of \( G_1 \) with 2 \( K_2 \).

<table>
<thead>
<tr>
<th>( A_1 )</th>
<th>( A_2 )</th>
<th>( A_3 )</th>
<th>( A_4 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>157</td>
<td>158</td>
<td>159</td>
<td>150</td>
</tr>
<tr>
<td>169</td>
<td>160</td>
<td>168</td>
<td>167</td>
</tr>
<tr>
<td>180</td>
<td>179</td>
<td>170</td>
<td>189</td>
</tr>
<tr>
<td>259</td>
<td>250</td>
<td>258</td>
<td>257</td>
</tr>
<tr>
<td>268</td>
<td>267</td>
<td>260</td>
<td>269</td>
</tr>
<tr>
<td>270</td>
<td>289</td>
<td>279</td>
<td>280</td>
</tr>
<tr>
<td>340</td>
<td>349</td>
<td>347</td>
<td>348</td>
</tr>
<tr>
<td>367</td>
<td>368</td>
<td>369</td>
<td>360</td>
</tr>
<tr>
<td>389</td>
<td>370</td>
<td>380</td>
<td>379</td>
</tr>
<tr>
<td>458</td>
<td>457</td>
<td>450</td>
<td>459</td>
</tr>
<tr>
<td>479</td>
<td>480</td>
<td>489</td>
<td>470</td>
</tr>
<tr>
<td>560</td>
<td>569</td>
<td>567</td>
<td>568</td>
</tr>
</tbody>
</table>
**Lemma 4.12** There do not exist four compatible packings on 10 points having leaves $K_{1,3} \cup 3K_2$.

**Proof:** We consider maximal $(2, 3)$-packings which have the graph

![Graph](attachment:image.png)

as their leave $S$. We will show that $K_{10} \setminus S$ does not admit 4 block-disjoint maximal $(2, 3)$-packings.

There are 2 types of maximal $(2, 3)$-packings, namely those that contain the block 234 and those that do not. In order to establish that there do not exist four block-disjoint maximal $(2, 3)$-packings, it is sufficient to prove that there do not exist three such packings which avoid the block 234.

It can be shown that every maximal $(2, 3)$-packing which avoids 234 is isomorphic to the following packing (1):

$$
\begin{align*}
uvw & 23u & 34v & 42w \\
1uW & 2vW & 3wU & 4uV \\
1vU & 2vU & 3wV & 4UW \\
1wV
\end{align*}
$$

where

$$
\{\{u, U\}, \{v, V\}, \{w, W\}\} = \{(5, 6), (7, 8), (9, 0)\}.
$$

Therefore, without loss of generality, we may assume that the set of block-disjoint packings we are seeking contains the particular packing (2):

$$
\begin{align*}
579 & 235 & 347 & 429 \\
150 & 270 & 396 & 458 \\
176 & 286 & 308 & 460 \\
198
\end{align*}
$$

It is easy to see that there are only 2 maximal $(2,3)$-packings which contain the 4 blocks

$$
uvw \ 23u \ 34v \ 42w;
$$

namely, the one exhibited above and one consisting of the blocks.

153
which we name (3). (Note that the permutation (2 3)(v w)(V W) is an isomorphism which maps packing (3) onto (1).) It can be shown that there are precisely 12 maximal (2, 3)-packings which are block-disjoint from packing (2) and avoid the block 234, namely,

\[
\begin{array}{cccccccc}
P_1 & P_2 & P_3 & P_4 & P_5 & P_6 \\
570 & 589 & 580 & 679 & 670 & 689 \\
237 & 238 & 238 & 237 & 236 & 239 \\
340 & 349 & 345 & 349 & 340 & 348 \\
245 & 245 & 240 & 246 & 247 & 246 \\
179 & 180 & 168 & 170 & 169 & 179 \\
160 & 169 & 159 & 159 & 180 & 158 \\
158 & 157 & 170 & 168 & 157 & 160 \\
280 & 279 & 257 & 289 & 250 & 280 \\
269 & 260 & 269 & 250 & 289 & 257 \\
368 & 367 & 379 & 358 & 358 & 350 \\
359 & 350 & 360 & 360 & 379 & 367 \\
467 & 468 & 489 & 457 & 468 & 459 \\
489 & 470 & 467 & 480 & 459 & 470 \\
\end{array}
\]

\[
\begin{array}{cccccccc}
P_7 & P_8 & P_9 & P_{10} & P_{11} & P_{12} \\
680 & 680 & 680 & 680 & 680 & 680 \\
236 & 236 & 238 & 238 & 230 & 230 \\
348 & 340 & 346 & 340 & 346 & 348 \\
240 & 248 & 240 & 246 & 248 & 246 \\
158 & 158 & 158 & 158 & 158 & 158 \\
169 & 169 & 169 & 169 & 169 & 169 \\
170 & 170 & 170 & 170 & 170 & 170 \\
257 & 250 & 267 & 279 & 259 & 289 \\
289 & 279 & 259 & 250 & 267 & 257 \\
350 & 357 & 379 & 367 & 389 & 359 \\
379 & 389 & 350 & 359 & 357 & 367 \\
467 & 467 & 489 & 489 & 450 & 450 \\
459 & 459 & 457 & 457 & 479 & 479 \\
\end{array}
\]

Now it is easy to check that every pair of these packings has at least one common block. Hence, there do not exist 3 block-disjoint maximal packings which avoid the block 234. 

**Lemma 4.13** There do not exist four compatible packings on 10 points having leaves \( G_2 \cup K_2 \).
Proof: Consider \((2, 3)\)-packings which have the graph

![Graph Image]

as their common leave \(\mathcal{S}\). Observe that each of the edges (pairs) 57, 68, 95, 96, 97, 98, 05, 06, 07 and 08 is contained in precisely four triples which avoid the 9 edges of \(\mathcal{S}\). Hence, if there are four \((2, 3)\)-packings having this graph as their common leave, then all 32 of these triples must appear in the packings. We now show that it is impossible to distribute these 32 pairs among four packings.

The four triples 572, 574, 579 and 570 must each be contained in a different packing. Let us call these four packings \(\mathcal{A}_2, \mathcal{A}_4, \mathcal{A}_9,\) and \(\mathcal{A}_0\) respectively. Now the triple 459 cannot be in either of \(\mathcal{A}_4\) or \(\mathcal{A}_9\). We have two cases to consider.

Case 1: \(459 \in \mathcal{A}_2\).

This implies that the packings have the following substructure:

<table>
<thead>
<tr>
<th></th>
<th>(\mathcal{A}_2)</th>
<th>(\mathcal{A}_4)</th>
<th>(\mathcal{A}_9)</th>
<th>(\mathcal{A}_0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>572</td>
<td>574</td>
<td>579</td>
<td>570</td>
<td></td>
</tr>
<tr>
<td>459</td>
<td>053</td>
<td>052</td>
<td>054</td>
<td>953</td>
</tr>
<tr>
<td>074</td>
<td>071</td>
<td>072</td>
<td>972</td>
<td>974</td>
</tr>
</tbody>
</table>

Now the triple 689 can go in any one of these four packings. Notice that two of these subcases are isomorphic under the isomorphism \((1\ 3)(2\ 4)(5\ 7)(6\ 8)\). In each case, the triples containing 69, 89 and 68 can be placed in these packings in only one way. Then the triples containing 08 cannot be placed without violating the definition of a \((2, 3)\)-packing.

Case 2: \(459 \in \mathcal{A}_0\).

This implies that the packings have the following substructure:

<table>
<thead>
<tr>
<th></th>
<th>(\mathcal{A}_2)</th>
<th>(\mathcal{A}_4)</th>
<th>(\mathcal{A}_9)</th>
<th>(\mathcal{A}_0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>572</td>
<td>574</td>
<td>579</td>
<td>570</td>
<td>459</td>
</tr>
</tbody>
</table>
This substructure is isomorphic to that in Case 1, by applying the permutation (2 4)(6 8). This establishes that there do not exist four packings which have $G_2 \cup K_2$ as their common leave.

We have presented examples where the bounds of Lemmata 4.8 and 4.10 are exact, though we know of no infinite classes of threshold schemes meeting these bounds with equality. However, by means of a generalization of Theorem 4.7, we can construct infinite classes of threshold schemes where the number of keys is close to these upper bounds.

Our construction is based on the trivial observation that one can easily construct $n$ Latin squares of order $n$, on the same symbol set, such that no two of these Latin squares contain the same symbol in the same cells. (For example, start with any Latin square $L$ of order $n$, with the symbol set $Z_n$. For every $i$, $0 \leq i \leq n-1$, define $L_i(a, b) = (L(a, b) + i) \text{modulo } n$.) We say that the $n$ Latin squares are disjoint. This immediately gives rise to the following recursive construction.

**Theorem 4.14** For all positive integers $n$ and $v$ such that $v \equiv 0 \pmod{n}$, $M(3, 3, v) \geq n \cdot M(3, 3, v/n)$.

**Proof:** Denote $v' = v \div n$ and $m = M(3, 3, v')$. Let $A_1, \ldots, A_m$ be $3$-compatible $3$-uniform hypergraphs on a $v'$-set $X$, such that $A_i(2) = 5$, $1 \leq i \leq m$. Let $L_i$, $1 \leq j \leq n$, be $n$ disjoint Latin squares of order $n$, on symbol set $\{1, 2, \ldots, n\}$. For every $x \in X$, we will take $n$ copies of $x$, named $x_j$, $1 \leq j \leq n$. Impose an arbitrary ordering on the elements of $X$.

Now, for every $A_i$, $1 \leq i \leq m$, we construct $n$ $3$-uniform hypergraphs on the $v$ points in $\{x_j; 1 \leq j \leq n, x \in X\}$, denoted $A_{i,j}$ ($1 \leq j \leq n$), as follows. Define

$$A_{i,j} = \{(x_a, y_b, z_c); (x, y, z) \in A_i, 1 \leq a \leq n, 1 \leq b \leq n, L_i(a, b) = c, x < y < z\}.$$

It is easy to see that $A_{i,j}(2) = A_{i',j}(2)$, for all $(i, j) \neq (i', j')$. As well $A_{i,j} \cap A_{i',j'} = \emptyset$ for all $(i, j) \neq (i', j')$. Hence, $M(3, 3, v) \geq n \cdot M(3, 3, v')$. 

We note that Theorem 4.7 is essentially the special case of Theorem 4.14 when $n = 2$.

**Corollary 4.15** Suppose $v \equiv 4$ or $12 \pmod{24}$, $v \div 4 \neq 7, 141, 283, 501, 789, 1501, \text{ or } 2365$. Then $M(3, 3, v) \geq v - 8$.

**Proof:** Apply Theorem 4.14 with $n = 4$. $M(3, 3, v/4) = (v - 8)/4$ by Theorem 2.4.

Letting $n = 5$, we obtain in a similar fashion the following corollary.
Corollary 4.16 Suppose \( v \equiv 5 \) modulo 30, \( v / 5 \neq 7, 141, 283, 501, 789, 1501, 2365 \). Then \( M(3, 3, v) \geq v - 10 \).

Finally, we summarize our results on \( M(3, 3, v) \) in Tables 1 and 2. Table 1 contains all values \( M(3, 3, v) \) that we know for \( v \leq 13 \). For the sake of completeness, we observe that \( M(3, 3, 7) = 3 \). It is well-known that the maximum number of disjoint \( S(2, 3, 7) \) designs is 2 (this was first shown by Cayley in [4]). However, we can obtain a \( (3, 3, 7; 3) \)-threshold scheme as follows.

Example 4.5 A \( (3, 3, 7; 3) \)-threshold scheme. The leave of each packing is the triangle 123.

<table>
<thead>
<tr>
<th>( A_1 )</th>
<th>( A_2 )</th>
<th>( A_3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>145</td>
<td>146</td>
<td>147</td>
</tr>
<tr>
<td>167</td>
<td>157</td>
<td>156</td>
</tr>
<tr>
<td>246</td>
<td>247</td>
<td>245</td>
</tr>
<tr>
<td>257</td>
<td>256</td>
<td>267</td>
</tr>
<tr>
<td>347</td>
<td>345</td>
<td>346</td>
</tr>
<tr>
<td>356</td>
<td>367</td>
<td>357</td>
</tr>
</tbody>
</table>

Table 1

\( M(3, 3, v) \) for \( v \leq 13 \)

<table>
<thead>
<tr>
<th>( v )</th>
<th>( M(3, 3, v) )</th>
<th>authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>2</td>
<td>Theorem 4.7</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>Example 4.5</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>Example 4.1</td>
</tr>
<tr>
<td>9</td>
<td>7</td>
<td>Theorem 2.4</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>Examples 4.3 and 4.4</td>
</tr>
<tr>
<td>11</td>
<td>7</td>
<td>Example 4.2</td>
</tr>
<tr>
<td>12</td>
<td>???</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>11</td>
<td>Theorem 2.4</td>
</tr>
</tbody>
</table>

Table 2

Bounds on \( M(3, 3, v) \)

<table>
<thead>
<tr>
<th>( v )</th>
<th>bounds on ( M(3, 3, v) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( v \equiv 1 ) or 3 modulo 6, ( v &gt; 1 )</td>
<td>( M(3, 3, v) \leq v - 2 )</td>
</tr>
<tr>
<td>( v \equiv 0, 2, ) or 5 modulo 6, ( v &gt; 2 )</td>
<td>( M(3, 3, v) \leq v - 4 )</td>
</tr>
<tr>
<td>( v \equiv 4 ) modulo 6, ( v &gt; 4 )</td>
<td>( M(3, 3, v) \leq v - 6 )</td>
</tr>
</tbody>
</table>

\( v \equiv 1 \) or 3 modulo 6, \( v \neq 1, 7, 141, 283, 501, 789, 1501, 2365 \)

\( v \equiv 2 \) or 6 modulo 12, \( v \neq 1, 7, 141, 283, 501, 789, 1501, 2365 \)

\( v \equiv 4 \) or 12 modulo 24, \( v \neq 7, 141, 283, 501, 789, 1501, 2365 \)

\( v \equiv 5 \) modulo 30, \( v \neq 7, 141, 283, 501, 789, 1501, 2365 \)

\( M(3, 3, v) \geq v - 8 \)

\( M(3, 3, v) \geq v - 10 \)
5. Some bounds on $M(4, 4, v)$

Shamir's construction for threshold schemes [12] gives lower bounds on $M(t, w, v)$ whenever $p = v/w$ is a prime and $p > w$. In this scheme, the key can be any $k \in GF(p)$ (so $m = p$). The set of shadows $X = \{(x, y) \in GF(p) \times GF(p), 1 \leq x \leq w\}$ (so $v = pw$). Now, for every polynomial $h(x) \in GF(p)[x]$ having degree at most $t - 1$, we construct a block $B(h)$ as follows. The shadows in $B(h)$ are $(u, h(u)), 1 \leq u \leq w$, and the key for $B(h)$ is $h(0)$. Hence, the number of blocks $b = p^t$.

It is not difficult to see that the scheme is perfect (see, for example, [14]). Hence, we obtain the following lower bound on $M(t, w, v)$.

**Theorem 5.1** Suppose $p = v/w$ is prime, $p > w$, and $t \leq w$. Then $M(t, w, v) \geq v/w$.

For $t = w = 3$, the bounds of Section 4 are superior. However, for most other values of $t$ and $w$, this result provides the best known lower bounds on $M(t, w, v)$. In the remainder of this section, we present some lower bounds on $M(4, 4, v)$.

From our general results, we know that $M(4, 4, v) \leq v - 3$, with equality occurring if and only if there is a Steiner system $S(4, 4, v)$ which can be partitioned into $v - 3$ Steiner systems $S(3, 4, v)$. This is of course equivalent to finding a set of $v - 3$ disjoint $S(3, 4, v)$ (on the same set of points). Aside from the trivial case $v = 4$, no example is known. The best result in this direction is a construction due to Lindner [6].

**Theorem 5.2** [6] For all $v \equiv 8$ or $16$ modulo $24$, there exist at least $3v/4$ disjoint $S(3, 4, v)$; hence $M(4, 4, v) \geq 3v/4$ for these values of $v$.

Note that this is a considerable improvement over the lower bound of $v/4$ given by Theorem 5.1.

The lower bound of $v/4$ for $M(4, 4, v)$ can also be improved when $v \equiv 0$ or $6$ modulo $12$, by means of a result of Teirlinck [15]. The result concerns designs with $\lambda > 1$; for our purposes it is sufficient to define an $S_{\lambda}(3, 4, v)$ to be a 4-uniform hypergraph on $v$ points such that every three points occur in exactly $\lambda$ blocks. Teirlinck proved the following.

**Theorem 5.3** [15] If $v \equiv 0$ or $6$ modulo $12$, then there exist $v/3$ disjoint simple $S_{\lambda}(3, 4, v)$; hence $M(4, 4, v) \geq v/3$ for these values of $v$.

We summarize our bounds on $M(4, 4, v)$ in Table 3.
Table 3

<table>
<thead>
<tr>
<th>v</th>
<th>bounds on M(4, 4, v)</th>
</tr>
</thead>
<tbody>
<tr>
<td>all v</td>
<td>M(4, 4, v) ≤ v - 3</td>
</tr>
<tr>
<td>v ≡ 8 or 16 modulo 24</td>
<td>M(4, 4, v) ≥ 3v / 4</td>
</tr>
<tr>
<td>v ≡ 0 or 6 modulo 12</td>
<td>M(4, 4, v) ≥ v / 3</td>
</tr>
<tr>
<td>v ≡ 4 or 20 modulo 24, v / 4 a prime power</td>
<td>M(4, 4, v) ≥ v / 4</td>
</tr>
</tbody>
</table>

6. Summary

A very interesting open problem is to improve the lower bounds on M(t, t, v) when t ≥ 4. Theorem 5.1 tells us that M(t, t, v) ≥ v / t under certain circumstances. On the other hand, the upper bound provided by Theorem 2.2 is M(t, t, v) ≤ v - t + 1. Hence, there is room for an improvement by a factor of almost t. One approach to take would be to attempt to decompose S(t, t, v) (the set of all t-subsets of a v-set) into Sλ(t - 1, t, v); then M(t, t, v) ≥ (v - t + 1) / λ. Teirlinck's remarkable results on the existence of t-designs for all t [16, 17] provide such decompositions; however, the values of the resulting λ's are too large. In order to improve upon the bound of Theorem 5.1, we would require that λ ≤ t - 1 in such a decomposition. This is undoubtedly a difficult problem!

A much more tractable open problem would be to finish the determination of the numbers M(3, 3, v). Can the upper bounds given in Table 2 always be attained, perhaps with finitely many exceptions?

References

1. R. D. Baker, *Partitioning the planes of AG_2m(2) into 2-designs*, Discrete Math. 15 (1976), 205-211.


