A flaw in the use of minimal defining sets for secret sharing schemes

M. J. Grannell, T. S. Griggs
Department of Pure Mathematics
The Open University
Walton Hall, Milton Keynes, MK7 6AA
United Kingdom
{m.j.grannell, t.s.griggs}@open.ac.uk

A. P. Street
Department of Mathematics
University of Queensland
Queensland 4072
Australia
aps@maths.uq.edu.au

Abstract

It is shown that in some cases it is possible to reconstruct a block design $\mathcal{D}$ uniquely from incomplete knowledge of a minimal defining set for $\mathcal{D}$. This surprising result has implications for the use of minimal defining sets in secret sharing schemes.

AMS classifications:
Primary: 94A62, Secondary: 05B05.

Keywords:
block design, minimal defining set, secret sharing, strongbox.

Running head:
Secret sharing

1 Introduction

The basic principle of a secret sharing scheme is that a key or password is shared between different individuals in such a way that all the individuals are required to contribute their shares before the complete key can be recovered. Various methods have been proposed for secret sharing schemes including methods based on block designs; for examples see [11, 13, 14]. It has been suggested [12, 2] that such a scheme could be based on the use of minimal defining sets for block designs.

A $t-(v,k,\lambda)$ *block design* $\mathcal{D}$ consists of an ordered pair $(V,\mathcal{B})$, where V is a v-element set (the *points*) and $\mathcal{B}$ is a collection of k-element subsets of V (the *blocks*) which have the property that each t-element subset of V appears in precisely λ blocks. If $\mathcal{D}=(V,\mathcal{B})$ is such a block design and $\mathcal{S}$ is a sub-collection of $\mathcal{B}$ having the property that it is not a sub-collection of $\mathcal{B}'$ for any other $t-(v,k,\lambda)$ block design $\mathcal{D}'=(V,\mathcal{B}')$, then $\mathcal{S}$ is said to be a *defining set* for $\mathcal{D}$. In fact such a collection $\mathcal{S}$ need not be a set as it may be a multiset, i.e. it may contain repeated blocks, but the terminology seems to be fairly standard. A defining set for $\mathcal{D}$ having no sub-collection which is also a defining set for $\mathcal{D}$ is said to be a *minimal defining set* for $\mathcal{D}$. A minimal defining set $\mathcal{D}$ having smallest cardinality is called a *smallest defining set* for $\mathcal{D}$.

For secret sharing, the important property of a minimal defining set for a block design $\mathcal{D}$ is that the removal of any one of its blocks results in a collection of blocks which has more than one extension to block designs with the same parameters $t-(v,k,\lambda)$ as $\mathcal{D}$. If, for example, the minimal defining set $\mathcal{S}$ has s blocks (not necessarily distinct) and each is allocated to a separate individual, then it seems almost obvious that no group of $s-1$ of these individuals can with certainty reconstruct the block design $\mathcal{D}$.

For a secret sharing scheme of the type described, individuals would each receive a single block and would, in theory, have no knowledge of the parameters of $\mathcal{D}$, or even that the scheme was based on a block design. However, a coalition of these individuals might well be able to infer the basis of the scheme and the parameters of the design. We therefore ask the following question. Given the parameters $t-(v,k,\lambda)$ and a minimal defining set for a block design $\mathcal{D}$ having these parameters, is it possible to reconstruct $\mathcal{D}$ with certainty from a proper sub-collection $\mathcal{S}'$ of $\mathcal{S}$ ($\mathcal{S}'\neq\mathcal{S}$)? **We will see that, in some cases, the knowledge that $\mathcal{S}'$ is a sub-collection of a minimal defining set $\mathcal{S}$ is sufficient to make the unique reconstruction of $\mathcal{D}$ from $\mathcal{S}'$ possible, and even to determine $\mathcal{S}$ uniquely.**

In the development of secret sharing schemes based on minimal defining sets, the concept of a strongbox was introduced in [12]. Given a minimal defining set $\mathcal{S}$ for a $t-(v,k,\lambda)$ block design $\mathcal{D}=(V,\mathcal{B})$, the *strongbox*

of $\mathcal{S}$, denoted by $S(\mathcal{S})$, consists of those blocks $\mathbf{b} \in \mathcal{B}$ for which every proper sub-collection of $\mathcal{S}$ has an extension to a $t-(v,k,\lambda)$ block design $\mathcal{D}' = (V, \mathcal{B}')$ with $\mathbf{b} \notin \mathcal{B}'$. It is possible that $S(\mathcal{S}) = \emptyset$ and we have some specific examples of this given below. Informally, $S(\mathcal{S})$ consists of those blocks of $\mathcal{B}$ which are not forced by any proper sub-collection of $\mathcal{S}$ and so (apparently) cannot be recovered without knowledge of the entire minimal defining set $\mathcal{S}$. Thus it is argued that the strongbox (if non-empty) is the best place to hide secret information. For example, if $|\mathcal{S}| = s$ and if the blocks of $\mathcal{S}$ are distributed to s individuals, then the blocks of $S(\mathcal{S})$ might be used to define a password; determination of this password would appear to require every individual to contribute his or her block of $\mathcal{S}$ and any group of $s-1$ of the s individuals would be unable to determine the password unambiguously. However, as we have already remarked, in some cases $s-1$ individuals can determine the missing block of $\mathcal{S}$ and consequently are able to reconstruct the strongbox $S(\mathcal{S})$.

Before proceeding with our results and some necessary preliminaries, we point out that in a real practical situation additional complications may occur. In particular, consideration needs to be given to information regarding partial blocks and to the number of extensions of each proper sub-collection of a minimal defining set $\mathcal{S}$. The latter aspect makes it appropriate to use large block designs in order to ensure that the numbers of alternative extensions are very large and that, consequently, the probability of picking the original block design at random from amongst such extensions is low. However, enumeration of minimal defining sets has generally only been attempted for relatively small block designs. Since this current paper is concerned with analysing minimal defining sets rather than constructing them, we have concentrated on surveying known and tabulated minimal defining sets. The block designs we examine are therefore relatively small. Analysis of much larger block designs, even if minimal defining sets were available, would raise problems of its own since such analysis requires construction of all extensions of every sub-collection of a minimal defining set obtained by deleting each block in turn. Nevertheless, the range of block designs which we do examine suggests that the flaw identified in using minimal defining sets for secret sharing schemes occurs sufficiently frequently to be of real concern.

We now give some definitions, starting with clarifications of the meanings of $A \cup B$ and $A \setminus \{a\}$ for multisets A and B. If $m(a, A)$ denotes the multiplicity of the element a in the multiset A, then $A \cup B$ is defined by the requirement that $m(a, A \cup B) = m(a, A) + m(a, B)$, and $A \setminus \{a\}$ is defined by the requirements that

$$\begin{aligned} m(a, A \setminus \{a\}) &= \begin{cases} 0 & \text{if } m(a,A) = 0 \text{ or } 1, \\ m(a,A) - 1 & \text{if } m(a,A) > 1, \end{cases} \\ m(b, A \setminus \{a\}) &= m(b, A) \text{ if } b \neq a. \end{aligned}$$

From this point onwards, we assume that we are investigating a minimal defining set $\mathcal{S}$ having cardinality s for a $t-(v,k,\lambda)$ block design $\mathcal{D}=(V,\mathcal{B})$. Suppose that $\mathcal{T}_1,\mathcal{T}_2$ are multisets of k-tuples on the base set V, and that $(V,\mathcal{T})$, where $\mathcal{T}=\mathcal{T}_1\cup\mathcal{T}_2$, is a $t-(v,k,\lambda)$ block design. Then we will say that $\mathcal{T}$ is an *extension* of $\mathcal{T}_1$ (or of $\mathcal{T}_2$), and that $\mathcal{T}_2$ is a *supplement* of $\mathcal{T}_1$ (and vice-versa). Furthermore, we will say that a block $\mathbf{b}\in\mathcal{S}$ is *bad* for $\mathcal{S}$ if every k-tuple which appears in only one supplement of $\mathcal{S}\setminus\{\mathbf{b}\}$ appears in the same supplement $\mathcal{S}^*$ (in such a case, the extension $(\mathcal{S}\setminus\{\mathbf{b}\})\cup\mathcal{S}^*=\mathcal{B}$). The important aspect of this definition is that if $\mathcal{S}$ has a bad block $\mathbf{b}$, then by examining the extensions of $\mathcal{S}\setminus\{\mathbf{b}\}$ and noting which supplement contains all the uniquely occurring k-tuples, we can determine $\mathcal{D}$. If $\mathbf{b}$ is bad for $\mathcal{S}$ and if $\mathbf{b}$ is the only k-tuple which appears in only one supplement of $\mathcal{S}\setminus\{\mathbf{b}\}$, then we say that $\mathbf{b}$ is *recoverable*. If $\mathbf{b}$ is recoverable then not only can we reconstruct $\mathcal{D}$ from $\mathcal{S}\setminus\{\mathbf{b}\}$, but we can also determine $\mathcal{S}$ and hence the strongbox $S(\mathcal{S})$.

If $\mathcal{S}$ has at least one bad block, then we say that $\mathcal{S}$ itself is *bad*, and if every block of $\mathcal{S}$ is bad then we say that $\mathcal{S}$ is *very bad*. If $\mathcal{S}$ has no bad blocks, we say that $\mathcal{S}$ is *good*. We shall exhibit a variety of minimal defining sets, some good, some bad, and two very bad. Most of the bad blocks in our survey happen also to be recoverable.

In Section 2 we illustrate the above ideas by working through by hand two particular calculations. The first of these, for the unique minimal defining set of the Steiner triple system of order 7, is straightforward but provides a nice example to help understand the basic concepts of this paper. The second calculation is for the cyclically generated smallest defining set of the unique irreducible $2-(7,3,3)$ block design; it is included to give a non-computer proof of the existence of a defining set which is very bad. In Section 3 we give computer-based results for various small block designs. Where all minimal or all smallest defining sets are known, full details are given. For other parameter sets we summarize our findings. In Section 4 we present some results for the eighty $2-(15,3,1)$ block designs based on the smallest defining sets given in [10]. These are partial results because it is not known whether these smallest defining sets are unique. However, they perhaps better indicate the situation for a secret sharing scheme based on larger and less symmetric block designs. Finally in Section 5 we review our findings.

2 Two small examples

2.1 The unique $2-(7,3,1)$ design

This is the Steiner triple system of order 7, or Fano plane. It is easy to show that, up to isomorphism, there is just one minimal defining set which can be taken to be $\mathcal{S} = \{123, 145, 356\}$. Here and subsequently when listing blocks we omit brackets and commas so that, for example 123 denotes the block $\{1, 2, 3\}$. Removing each block in turn from $\mathcal{S}$ results in the following supplements, two in each case.

$$\begin{array}{lll} \mathcal{S}\setminus\{123\}: & \text{(i)} & \{257, 123, 167, 246, 347\} \\ & \text{(ii)} & \{257, 126, 137, 234, 467\} \\ \mathcal{S}\setminus\{145\}: & \text{(i)} & \{347, 145, 167, 246, 257\} \\ & \text{(ii)} & \{347, 146, 157, 245, 267\} \\ \mathcal{S}\setminus\{356\}: & \text{(i)} & \{167, 246, 257, 347, 356\} \\ & \text{(ii)} & \{167, 247, 256, 346, 357\} \end{array}$$

In each case there are uniquely occurring blocks in both supplements, so $\mathcal{S}$ contains no bad blocks and is therefore good. The blocks of the design which $\mathcal{S}$ defines are 123, 145, 167, 246, 257, 347 and 356. All of these except 246 are either members of the defining set or can be found in both supplements of $\mathcal{S}\setminus\{\mathbf{b}\}$ for one of $\mathbf{b} = 123, 145$ or 356. Hence the strongbox $S(\mathbf{S}) = \{246\}$.

2.2 The unique irreducible $2-(7,3,3)$ design

There are, up to isomorphism, ten $2-(7,3,3)$ designs only one of which is irreducible, i.e. cannot be partitioned into three Fano planes [9]. In [3], two non-isomorphic smallest defining sets, each containing precisely seven blocks, are given for the irreducible design. These have automorphism groups of orders 2 and 14 respectively. The latter set is block transitive and can be taken to be $\mathcal{S} = \{123, 234, 345, 456, 567, 671, 712\}$. We prove that this set is very bad.

First consider extensions of $\mathcal{S}\setminus\{712\}$ to a reducible $2-(7,3,3)$ design. Denote the sets of blocks of the three Fano planes into which such an extension can be partitioned by $\mathcal{X}, \mathcal{Y}$ and $\mathcal{Z}$. Note that every pair of blocks of a Fano plane intersect. Without loss of generality assume that $123 \in \mathcal{X}$ and $234 \in \mathcal{Y}$. Then either $345 \in \mathcal{X}$ or $345 \in \mathcal{Z}$. Assume the former. In that case then either $456 \in \mathcal{Y}$, in which case $567 \in \mathcal{Z}$ and it is impossible to assign 671; or $456 \in \mathcal{Z}$, in which case it is impossible to assign 567. So $345 \in \mathcal{Z}$, which implies that $456 \in \mathcal{Y},\ 567 \in \mathcal{Z},\ 671 \in \mathcal{X}$. There are thus

two possibilities for each of $\mathcal{X}, \mathcal{Y}$ and $\mathcal{Z}$ as follows.

$$\begin{array}{lll} \mathcal{X}: & \text{(i)} & \{123, 671, 145, 246, 257, 347, 356\} \\ & \text{(ii)} & \{123, 671, 145, 247, 256, 346, 357\} \\ \mathcal{Y}: & \text{(i)} & \{234, 456, 147, 125, 136, 267, 357\} \\ & \text{(ii)} & \{234, 456, 147, 126, 135, 257, 367\} \\ \mathcal{Z}: & \text{(i)} & \{345, 567, 125, 136, 147, 237, 246\} \\ & \text{(ii)} & \{345, 567, 125, 137, 146, 236, 247\} \end{array}$$

Thus $\mathcal{S} \setminus \{712\}$ extends to eight reducible $2-(7,3,3)$ designs and these give rise to eight supplements. But none of the blocks in these eight supplements occurs in a unique supplement.

Next consider extensions of $\mathcal{S} \setminus \{712\}$ to the irreducible $2-(7,3,3)$ design. We use the facts that this design contains no repeated blocks and that the omitted triples can be partitioned into two Fano planes. Denote the set of blocks of the irreducible $2-(7,3,3)$ design by $\mathcal{B}$, and the sets of triples of the omitted Fano planes by $\mathcal{F}_1$ and $\mathcal{F}_2$ respectively. We have one of 341, 346 or 347 $\in \mathcal{B}$, and one of 561, 562 or 563 $\in \mathcal{B}$. Consider the nine possibilities in turn.

1. 341 and 561 $\in \mathcal{B}$. Then 346 and 562 $\in \mathcal{F}_1$, 347 and 563 $\in \mathcal{F}_2$. Therefore 671 $\in \mathcal{F}_1$; a contradiction because 671 $\in \mathcal{S} \setminus \{712\} \subseteq \mathcal{B}$.

2. 341 and 562 $\in \mathcal{B}$. Then 346 and 561 $\in \mathcal{F}_1$, 347 and 563 $\in \mathcal{F}_2$. Therefore 123 $\in \mathcal{F}_2$; again a contradiction.

3. 341 and 563 $\in \mathcal{B}$. Then 346 $\in \mathcal{F}_1$, 347 $\in \mathcal{F}_2$. Therefore 561 $\notin \mathcal{F}_2$ and 562 $\notin \mathcal{F}_2$, but both cannot be assigned to $\mathcal{F}_1$.

4. 346 and 561 $\in \mathcal{B}$. Then 347 $\in \mathcal{F}_1$, 341 $\in \mathcal{F}_2$, and 562 cannot be assigned to either $\mathcal{F}_1$ or $\mathcal{F}_2$.

5. 346 and 562 $\in \mathcal{B}$. Then 347 and 563 $\in \mathcal{F}_1$, 341 and 561 $\in \mathcal{F}_2$. Therefore 123 $\in \mathcal{F}_1$; a contradiction.

6. 346 and 563 $\in \mathcal{B}$. Then 347 $\in \mathcal{F}_1$, 341 $\in \mathcal{F}_2$, and 562 cannot be assigned to either $\mathcal{F}_1$ or $\mathcal{F}_2$.

7. 347 and 561 $\in \mathcal{B}$. Then 341 and 563 $\in \mathcal{F}_1$, 346 and 562 $\in \mathcal{F}_2$. Therefore 671 $\in \mathcal{F}_2$; a contradiction.

8. 347 and 562 $\in \mathcal{B}$. Then 341 and 563 $\in \mathcal{F}_1$, 346 and 561 $\in \mathcal{F}_2$. Also, 327 $\in \mathcal{F}_1$ and 627 $\in \mathcal{F}_2$, and we pursue this option below.

9. 347 and 563 $\in \mathcal{B}$. Then 341 and 561 $\in \mathcal{F}_1$, 346 and 562 $\in \mathcal{F}_2$. Therefore 671 $\in \mathcal{F}_2$; a contradiction.

Therefore, option 8 is the only remaining possibility and there are two alternatives for each of $\mathcal{F}_1$ and $\mathcal{F}_2$, namely

$$\begin{array}{lll} \mathcal{F}_1: & \text{(i)} & \{341, 356, 327, 152, 167, 457, 462\} \\ & \text{(ii)} & \{341, 356, 327, 157, 162, 452, 467\} \\ \mathcal{F}_2: & \text{(i)} & \{634, 615, 627, 312, 357, 417, 452\} \\ & \text{(ii)} & \{634, 615, 627, 317, 352, 412, 457\}. \end{array}$$

But 167 and 312 $\in \mathcal{S} \setminus \{712\} \subseteq \mathcal{B}$, so we must have alternative (ii) for each of $\mathcal{F}_1$ and $\mathcal{F}_2$. Thus $\mathcal{B}$ is determined as follows, with the last 15 blocks listed forming the supplement of $\mathcal{S} \setminus \{712\}$:

$$123, 234, 345, 456, 567, 671,$$
$$125, 127, 135, 136, 145, 146, 147, 236, 246, 247, 256, 257, 347, 357, 367.$$

With the single exception of 127, all the blocks in this supplement occur in at least one of the eight supplements corresponding to the reducible $2-(7,3,3)$ extensions. Thus the block 127 is both bad and recoverable. But then, by the block transitivity of $\mathcal{S}$, all the blocks of $\mathcal{S}$ are bad and recoverable, and this defining set is therefore very bad.

3 Computer results for small designs

In this and the following section, the computational aspects of our results are presented. When a design is listed its points are numbered consecutively from 1 upwards and we use the letters a, b, c, d, e, f, g respectively to denote the points $10, 11, 12, 13, 14, 15, 16$. Our largest point set has 16 points. For each parameter set $t-(v,k,\lambda)$, we denote by N the number of non-isomorphic block designs having these parameters and we number these designs from 1 to N. For most of the designs examined, there is in existence no complete tabulation of all minimal defining sets and so our analysis is restricted to those minimal defining sets which have been determined; frequently these are smallest defining sets.

In selected cases, where either all minimal or all smallest defining sets are known, we give a complete analysis and, in these cases, the minimal defining sets examined for each design are denoted by $\mathcal{S}_1, \mathcal{S}_2, \ldots$, or simply by $\mathcal{S}$ if only one is examined. For each $\mathcal{S}_i$ we list its blocks. We place an asterisk beside each bad block and two asterisks if the block is also recoverable. We record the status of $\mathcal{S}$ as good, bad, or very bad. If the jth block of the minimal defining set $\mathcal{S}_i$ is deleted, denote by x_j the number of extensions of the resulting sub-collection of $\mathcal{S}_i$ to $t-(v,k,\lambda)$ block designs. In [12], the number x_j is called the *power* of the jth block. We record the *extensions vector* $\mathbf{x} = (x_1, x_2, \ldots, x_s)$ where $s = |\mathcal{S}_i|$. The

entries in this vector give some indication of the chances of reconstructing the original design at random from $s-1$ blocks of the minimal defining set. Finally in the selected cases, we also list the strongbox of each minimal defining set.

For the remaining cases which we have investigated, we simply summarize the results.

3.1 Parameters: $2-(7,3,1)$, $N=1$

This is the Steiner triple system of order 7 or Fano plane examined in section 2.

$\mathcal{S} = \{123, 145, 356\}$, $\mathcal{S}$ is good, $\mathbf{x} = (2, 2, 2)$, $S(\mathcal{S}) = \{246\}$.

3.2 Parameters: $2-(9,3,1)$, $N=1$

This is the Steiner triple system of order 9. Again it is easy to show that, up to isomorphism, there are two minimal defining sets.

$\mathcal{S}_1 = \{123, 147, 258, 456\}$, $\mathcal{S}_1$ is good, $\mathbf{x} = (4, 4, 4, 4)$, $S(\mathcal{S}_1) = \{159, 168, 249, 267, 348, 357\}$.
$\mathcal{S}_2 = \{123, 147, 168, 249, 267\}$, $\mathcal{S}_2$ is good, $\mathbf{x} = (2, 2, 2, 2, 2)$, $S(\mathcal{S}_2) = \{456\}$.

3.3 Parameters: $2-(13,3,1)$, $N=2$

The minimal defining sets in this subsection are taken from [5].

Design #1 (The cyclic Steiner triple system of order 13)
The 17 minimal defining sets analysed below comprise all the smallest defining sets for this design (up to isomorphism). Of these, three are bad and the remainder are good.

$\mathcal{S}_1 = \{125, 236, 2bc, 347, 35b, 458, 67a, 89c, 9ad\}$, $\mathcal{S}_1$ is good, $\mathbf{x} = (8, 15, 8, 7, 31, 8, 20, 10, 59)$, $S(\mathcal{S}_1) = \{14d, 24a, 279, 49b, 569, 57d, 6bd, 78b\}$.
$\mathcal{S}_2 = \{125, 236, 347, 35b, 458, 67a, 6bd, 89c, 9ad\}$, $\mathcal{S}_2$ is good, $\mathbf{x} = (14, 4, 8, 14, 16, 11, 8, 13, 20)$, $S(\mathcal{S}_2) = \{14d, 17c, 1ab, 24a, 279, 2bc\}$.
$\mathcal{S}_3 = \{125, 236, 347, 3cd, 458, 49b, 67a, 6bd, 89c\}$, $\mathcal{S}_3$ is good, $\mathbf{x} = (18, 16, 4, 15, 16, 13, 40, 24, 30)$, $S(\mathcal{S}_3) = \{139, 14d, 17c, 1ab, 24a, 279, 38a, 57d, 5ac, 78b, 9ad\}$.
$\mathcal{S}_4 = \{125, 1ab, 236, 347, 35b, 458, 46c, 89c, 9ad\}$, $\mathcal{S}_4$ is good, $\mathbf{x} = (8, 14, 23, 10, 15, 8, 11, 16, 32)$, $S(\mathcal{S}_4) = \{168, 28d, 38a, 3cd, 569, 57d, 78b\}$.

$\mathcal{S}_5 = \{125, 236, 347, 49b, 57d, 5ac, 67a, 6bd, 89c\}$, $\mathcal{S}_5$ is good,
$\mathbf{x} = (20, 12, 18, 24, 11, 12, 16, 14, 55)$,
$S(\mathcal{S}_5) = \{139, 14d, 168, 17c, 1ab, 24a, 279, 28d, 2bc, 35b, 38a, 3cd, 46c, 78b, 9ad\}$.

$\mathcal{S}_6 = \{125, 168, 1ab, 236, 347, 46c, 49b, 78b, 9ad\}$, $\mathcal{S}_6$ is good,
$\mathbf{x} = (19, 13, 16, 20, 10, 24, 14, 8, 33)$,
$S(\mathcal{S}_6) = \{279, 28d, 38a, 3cd, 57d, 5ac, 67a, 89c\}$.

$\mathcal{S}_7 = \{125, 236, 28d, 347, 46c, 49b, 5ac, 78b, 9ad\}$, $\mathcal{S}_7$ is good,
$\mathbf{x} = (28, 10, 15, 14, 11, 27, 12, 30, 10)$,
$S(\mathcal{S}_7) = \{139, 14d, 168, 17c, 1ab, 35b, 38a, 3cd, 458, 569, 57d, 67a, 6bd\}$.

$\mathcal{S}_8 = \{125, 168, 236, 2bc, 347, 46c, 57d, 89c, 9ad\}$, $\mathcal{S}_8$ is good,
$\mathbf{x} = (11, 12, 10, 8, 10, 11, 32, 10, 38)$,
$S(\mathcal{S}_8) = \{139, 14d, 17c, 1ab, 24a, 28d, 35b, 38a, 3cd, 458, 49b, 78b\}$.

$\mathcal{S}_9 = \{125, 168, 236, 347, 35b, 46c, 57d, 89c, 9ad\}$, $\mathcal{S}_9$ is good,
$\mathbf{x} = (9, 8, 8, 8, 8, 12, 22, 44, 5)$,
$S(\mathcal{S}_9) = \{17c, 279, 2bc, 78b\}$.

$\mathcal{S}_{10} = \{125^{**}, 168, 236, 347, 46c, 49b, 57d, 89c, 9ad\}$, $\mathcal{S}_{10}$ is bad,
$\mathbf{x} = (28, 22, 28, 8, 12, 8, 14, 17, 26)$,
$S(\mathcal{S}_{10}) = \{14d, 17c, 1ab, 24a, 28d, 2bc, 35b, 38a, 3cd, 5ac, 78b\}$.

$\mathcal{S}_{11} = \{125, 1ab, 236, 28d, 347, 35b, 49b, 57d, 89c\}$, $\mathcal{S}_{11}$ is good,
$\mathbf{x} = (12, 18, 20, 24, 12, 10, 32, 18, 31)$,
$S(\mathcal{S}_{11}) =$
$\{139, 14d, 168, 17c, 24a, 2bc, 38a, 3cd, 458, 46c, 569, 5ac, 67a, 6bd, 78b, 9ad\}$.

$\mathcal{S}_{12} = \{125, 1ab, 236, 347, 46c, 49b, 57d, 6bd, 89c\}$, $\mathcal{S}_{12}$ is good,
$\mathbf{x} = (40, 23, 13, 24, 12, 16, 31, 8, 41)$,
$S(\mathcal{S}_{12}) = \{139, 168, 17c, 279, 28d, 2bc, 35b, 38a, 3cd, 569, 5ac, 67a, 78b, 9ad\}$.

$\mathcal{S}_{13} = \{125, 1ab, 236, 279, 347, 57d, 5ac, 6bd, 89c\}$, $\mathcal{S}_{13}$ is good,
$\mathbf{x} = (8, 53, 24, 16, 38, 18, 16, 25, 27)$,
$S(\mathcal{S}_{13}) = \{139, 14d, 168, 17c, 28d, 2bc, 35b, 38a, 3cd, 458, 49b, 569, 67a, 78b, 9ad\}$.

$\mathcal{S}_{14} = \{125, 168, 17c, 236, 24a, 46c, 57d, 78b^{**}, 9ad\}$, $\mathcal{S}_{14}$ is bad,
$\mathbf{x} = (8, 8, 6, 13, 20, 22, 16, 27, 18)$,
$S(\mathcal{S}_{14}) = \{139, 14d, 1ab, 35b, 38a, 458, 49b, 5ac, 89c\}$.

$\mathcal{S}_{15} = \{125, 168, 17c, 236, 46c, 49b, 57d, 78b, 9ad\}$, $\mathcal{S}_{15}$ is good,
$\mathbf{x} = (26, 21, 10, 13, 16, 20, 6, 8, 66)$,
$S(\mathcal{S}_{15}) = \{279, 28d, 347, 38a, 3cd, 569, 5ac, 67a, 89c\}$.

$\mathcal{S}_{16} = \{125, 168, 17c, 236, 38a, 46c, 49b, 78b, 9ad^{**}\}$, $\mathcal{S}_{16}$ is bad,
$\mathbf{x} = (25, 6, 12, 16, 6, 21, 24, 11, 59)$,
$S(\mathcal{S}_{16}) = \{14d, 1ab, 24a, 279, 28d, 3cd, 458, 569, 57d, 5ac, 67a, 6bd, 89c\}$.

$\mathcal{S}_{17} = \{125, 17c, 236, 28d, 38a, 46c, 49b, 78b, 9ad\}$, $\mathcal{S}_{17}$ is good,
$\mathbf{x} = (6, 12, 8, 6, 14, 18, 12, 10, 14)$,
$S(\mathcal{S}_{17}) = \{14d, 1ab, 279, 2bc, 35b, 57d, 5ac, 67a, 6bd\}$.

Design #2 (The non-cyclic Steiner triple system of order 13)
The two minimal defining sets analysed below comprise all the smallest defining sets for this design (up to isomorphism). One is bad and the other is good.

$\mathcal{S}_1 = \{12d^{**}, 24a, 347, 35b, 5ac, 6bd, 78b^{**}, 9ad^{**}\}$, $\mathcal{S}_1$ is bad,
$\mathbf{x} = (88, 112, 96, 128, 16, 24, 248, 164)$,
$S(\mathcal{S}_1) = \{139, 145, 168, 17c, 236, 258, 279, 2bc, 3cd, 48d, 49b, 569, 57d, 89c\}$.

$\mathcal{S}_2 = \{12d, 145, 1ab, 24a, 3cd, 46c, 569, 89c\}$, $\mathcal{S}_2$ is good,
$\mathbf{x} = (112, 24, 336, 40, 16, 32, 40, 432,)$,
$S(\mathcal{S}_2) = \{236, 258, 279, 35b, 38a, 48d, 49b, 67a, 6bd, 78b, 9ad\}$.

3.4 Parameters: $2-(13,4,1)$, $N=1$

The two minimal defining sets in this subsection are taken from [6] and comprise all the smallest defining sets of this design (up to isomorphism). We find that both are good.

$\mathcal{S}_1 = \{124a, 139d, 235b, 2679, 346c, 457d\}$, $\mathcal{S}_1$ is good,
$\mathbf{x} = (2, 2, 2, 2, 2, 2)$,
$S(\mathcal{S}_1) = \{1568\}$.

$\mathcal{S}_2 = \{124a, 139d, 1568, 235b, 346c, 457d\}$, $\mathcal{S}_2$ is good,
$\mathbf{x} = (2, 2, 2, 2, 2, 2)$,
$S(\mathcal{S}_2) = \{2679, 28cd, 6abd\}$.

3.5 Parameters: $2-(16,4,1)$, $N=1$

The four minimal defining sets in this subsection are taken from [6] and comprise all the smallest defining sets of this design (up to isomorphism). We find that all four are good.

$\mathcal{S}_1 = \{1234, 159d, 26ae, 35ag, 37bf, 5678, 9abc\}$, $\mathcal{S}_1$ is good,
$\mathbf{x} = (4, 4, 4, 2, 4, 4, 4)$,
$S(\mathcal{S}_1) = \{16bg, 18af, 25cf, 279g, 36cd, 389e, 45be, 47ad\}$.

$\mathcal{S}_2 = \{1234, 159d, 17ce, 26ae, 45be, 469f, 5678\}$, $\mathcal{S}_2$ is good,
$\mathbf{x} = (4, 4, 4, 4, 2, 4, 4)$,
$S(\mathcal{S}_2) = \{279g, 28bd, 35ag, 37bf, 48cg, 9abc, defg\}$.

$\mathcal{S}_3 = \{1234, 159d, 17ce, 26ae, 35ag, 5678, 9abc\}$, $\mathcal{S}_3$ is good,
$\mathbf{x} = (4, 4, 4, 4, 4, 2, 4)$,
$S(\mathcal{S}_3) = \{25cf, 389e\}$.

$\mathcal{S}_4 = \{1234, 159d, 17ce, 26ae, 37bf, 5678, 9abc\}$, $\mathcal{S}_4$ is good,
$\mathbf{x} = (4, 4, 2, 4, 4, 4, 4)$,
$S(\mathcal{S}_4) = \{16bg, 18af, 25cf, 279g, 36cd, 389e, 45be, 47ad\}$.

3.6 Parameters: $2-(6,3,2)$, $N=1$

Up to isomorphism, there is one minimal defining set (see [4]). We find that this is good.

$\mathcal{S} = \{135, 145, 245\}$, $\mathcal{S}$ is good,
$\mathbf{x} = (2, 4, 2)$,
$S(\mathcal{S}) = \{146\}$.

3.7 Parameters: $2-(7,3,2)$, $N=4$

In [3], a smallest defining set, not necessarily unique, is given for each design. We find that each of these is good, although the strongbox is empty in each case.

3.8 Parameters: $2-(7,4,2)$, $N=1$

The blocks of this design form the complements of those of a $2-(7,3,1)$ design. It is easy to show that there is a one-to-one correspondence between the defining sets of these designs and that the $2-(7,4,2)$ design therefore has, up to isomorphism, a unique minimal defining set all of whose blocks are good, with the same extensions vector as that of the $2-(7,3,1)$ design and a strongbox containing precisely one quadruple, this being complementary to the triple of the earlier design.

3.9 Parameters: $2-(10,4,2)$, $N=3$

The three designs are taken from [6] where they are labelled H_1, H_2 and H_3 and it is shown that, up to isomorphism, H_1 has four smallest defining sets, H_2 has three, and H_3 has one. These are the minimal defining sets analysed below although the points have been relabelled as consecutive integers. We find that all eight of these defining sets are good although six of the strongboxes are empty.

Design #1 (H_1)

$\mathcal{S}_1 = \{1258, 1369, 147a, 189a, 2469, 2678, 3458, 456a\}$, $\mathcal{S}_1$ is good, $\mathbf{x} = (3,2,2,3,3,2,2,3)$, the strongbox of $\mathcal{S}_1$ is empty.
$\mathcal{S}_2 = \{1369, 147a, 1567, 3458, 3579, 368a, 456a, 4789\}$, $\mathcal{S}_2$ is good, $\mathbf{x} = (2,2,2,2,2,2,2,2)$, $S(\mathcal{S}_2) = \{189a\}$.
$\mathcal{S}_3 = \{1258, 1369, 147a, 1567, 2469, 2678, 3458, 4789\}$, $\mathcal{S}_3$ is good, $\mathbf{x} = (3,2,2,3,3,2,2,3)$, the strongbox of $\mathcal{S}_3$ is empty.
$\mathcal{S}_4 = \{1234, 1258, 1369, 147a, 1567, 3458, 3579, 4789\}$, $\mathcal{S}_4$ is good, $\mathbf{x} = (2,2,2,2,2,3,3,3)$, the strongbox of $\mathcal{S}_4$ is empty.

Design #2 (H_2)

$\mathcal{S}_1 = \{126a, 1358, 147a, 238a, 2468, 3469\}$, $\mathcal{S}_1$ is good, $\mathbf{x} = (3,3,3,3,3,3)$, the strongbox of $\mathcal{S}_1$ is empty.
$\mathcal{S}_2 = \{1358, 147a, 2468, 345a, 3469, 5678\}$, $\mathcal{S}_2$ is good, $\mathbf{x} = (3,6,3,3,3,3)$, the strongbox of $\mathcal{S}_2$ is empty.
$\mathcal{S}_3 = \{1367, 147a, 1489, 2468, 3469, 5678\}$, $\mathcal{S}_3$ is good, $\mathbf{x} = (3,3,3,3,6,3)$, the strongbox of $\mathcal{S}_3$ is empty.

Design #3 (H_3)

$\mathcal{S} = \{1367, 147a, 168a, 2679, 3469\}$, $\mathcal{S}$ is good, $\mathbf{x} = (8,8,8,8,8)$, $S(\mathcal{S}) = \{1235, 1289, 1459, 234a, 2478, 256a, 3578, 389a, 4568, 579a\}$.

3.10 Parameters: $2-(11,5,2)$, $N=1$

The two minimal defining sets in this subsection are taken from [6] and comprise all the smallest defining sets of this design (up to isomorphism). We find that both are good.

$\mathcal{S}_1 = \{13459, 14678, 2456a, 25789, 3567b\}$, $\mathcal{S}_1$ is good, $\mathbf{x} = (2,2,2,2,2)$, $S(\mathcal{S}_1) = \{479ab\}$.
$\mathcal{S}_2 = \{1269b, 13459, 2456a, 3567b, 479ab\}$, $\mathcal{S}_2$ is good, $\mathbf{x} = (2,2,2,2,2)$, $S(\mathcal{S}_2) = \{1237a\}$.

3.11 Parameters: $2-(7,3,3)$, $N=10$

The designs and defining sets analysed in this subsection are taken from [3] and we adopt the same numbering except that in the case of design #3 the defining set given in that paper is erroneous and we have substituted a correct one. The minimal defining sets for the designs numbered #1 to #9 are smallest defining sets, not necessarily unique. For design #10 (the unique indecomposable design with these parameters), there are, up to isomorphism, two smallest defining sets, the second of which was analysed in section 2.

Designs #1 to 9

The defining sets are good apart from those for design #5 which has a triplicated bad and recoverable block, and for design #9 which has a single bad (but not recoverable) block. All nine strongboxes are empty.

Design #10

Both defining sets are very bad.

$\mathcal{S}_1 = \{123^{**}, 125^{**}, 127^{**}, 135^{**}, 145^{**}, 345^{**}, 456^{**}\}$, $\mathcal{S}_1$ is very bad, $\mathbf{x} = (9,9,9,9,9,9,9)$, $S(\mathcal{S}_1) = \{147, 234, 236, 246, 247, 256, 347\}$.
$\mathcal{S}_2 = \{123^{**}, 127^{**}, 167^{**}, 234^{**}, 345^{**}, 456^{**}, 567^{**}\}$, $\mathcal{S}_2$ is very bad, $\mathbf{x} = (9,9,9,9,9,9,9)$, $S(\mathcal{S}_2) = \{135, 136, 146, 246, 247, 257, 357\}$.

3.12 Parameters: $2-(8,4,3)$, $N=4$

The four designs are given in [3] where they are labelled $\alpha*, \beta*, \delta*$ and $\gamma*$ and a smallest defining set of cardinality six is given for each. We find that all four of these defining sets are good, although the strongboxes for $\alpha*$ and $\delta*$ are empty.

3.13 Parameters: $2-(9,4,3)$, $N=11$

The eleven designs are given in [8] where they are labelled $M_1, M_2, \ldots, M_{11}$ and it is shown that two (M_8 and M_9) have smallest defining sets of cardinality six and the remaining nine have smallest defining sets of cardinality eight. In [8] all the smallest defining sets are determined, the number of non-isomorphic ones running to several thousands; we analyse just one smallest defining set for each of the eleven designs. Those for designs M_i with $i \neq 8, 9$ were found to be good, although three of the nine strongboxes are empty. Those for designs M_8 and M_9 are as follows; both are bad. The points of the designs have been relabelled as consecutive integers.

Design #8 (M_8)

$\mathcal{S} = \{1238^{**}, 1239^{**}, 1267, 1367, 2468, 2469\}$, $\mathcal{S}$ is bad,
$\mathbf{x} = (33, 33, 8, 8, 5, 5)$,
$S(\mathcal{S}) = \{2578, 2579, 3478, 3479, 3568, 3569\}$.

Design #9 (M_9)

$\mathcal{S} = \{1256^{**}, 1357^{**}, 1489, 2469^{**}, 3479^{**}, 6789\}$, $\mathcal{S}$ is bad,
$\mathbf{x} = (51, 51, 8, 51, 51, 8)$,
$S(\mathcal{S}) = \{1239, 1247, 1346, 1589, 1678, 2368, 2378, 2458, 2579, 3458, 3569, 4567\}$.

4 The $2-(15,3,1)$ block designs

There are 80 nonisomorphic $2-(15,3,1)$ block designs and we follow the standard numbering of these designs given in [7]. The minimal defining sets analysed are those given in [10] and these comprise one smallest defining set for each system. These smallest defining sets are almost certainly not unique. We find that the smallest defining sets for designs numbered #1, #2, #3, #4, #5 and #16 are good, but the remaining 74 are bad. Although none are very bad, #57 comes close with ten of the eleven blocks of the smallest defining set being bad. Altogether, amongst the 922 blocks of the 80 defining sets, 376 are bad and recoverable, and a further four are bad but not recoverable. It would not be a surprise if some alternative smallest defining sets for these designs were found to be very bad. To illustrate our results we give the details for designs numbered #1, #7, #57 and #80. The points have been relabelled to run from 1 upwards.

Design #1

$\mathcal{S} = \{123, 145, 189, 29b, 2df, 356, 3cf, 4ae, 4bf, 58d, 5af, 68e, 6ac, 79e, 7ad, 7bc\}$,
$\mathcal{S}$ is good, $\mathbf{x} = (4, 3, 4, 4, 3, 3, 3, 3, 3, 3, 3, 4, 3, 4, 3, 4)$,
the strongbox of $\mathcal{S}$ is empty.

Design #7

$\mathcal{S} = \{123, 145, 1cd, 257, 28a, 2df, 38b, 48c, 4af^*, 59d, 6ae, 6bc, 78e\}$,
$\mathcal{S}$ is bad, $\mathbf{x} = (16, 21, 19, 9, 13, 20, 39, 4, 7, 89, 30, 35, 65)$,
$S(\mathcal{S}) = \{246, 29b, 39a, 3cf, 3de, 4bd, 69f, 79c, 7ad, 7bf\}$.

Design #57

$\mathcal{S} = \{1ab^{**}, 1cd^{**}, 246^{**}, 348^{**}, 4be^{**}, 569, 5ac^{**}, 68d^{**}, 78e^{**}, 79c^{**}, 9af^{**}\}$,
$\mathcal{S}$ is bad, $\mathbf{x} = (217, 169, 339, 3311, 334, 22, 2361, 167, 334, 269, 564)$,
$S(\mathcal{S}) = \{123, 145, 167, 189, 1ef, 257, 29b, 2ce, 2df, 35b, 36c, 37f, 39e, 3ad,$
$47a, 49d, 5de, 6ae, 6bf\}$.

Design #80

$\mathcal{S} = \{145^{**}, 167^{**}, 1ef, 2ac^{**}, 357, 3ce^*, 4bf, 68c^{**}, 6ad^{**}, 7de, 8ae^{**}, 9bc^{**}\}$,
$\mathcal{S}$ is bad, $\mathbf{x} = (1327, 62, 74, 431, 37, 177, 56, 368, 173, 31, 100, 280)$,
$S(\mathcal{S}) = \{189, 1ab, 246, 258, 279, 2be, 2df, 34a, 36b, 38f, 39d, 48d, 49e,$
$56e, 59a, 5bd, 69f, 78b\}$.

5 Concluding Remarks

We have only examined defining sets for $t - (v, k, \lambda)$ block designs with $t = 2$. This is because a block design with $t > 2$ may be viewed as a block design with $t = 2$ and a higher value of λ. Generally, the number of extensions of a set of k-tuples will be much larger in the latter case, making the design better from the point of view of secret sharing.

The results from sections 3 and 4 indicate that larger designs, which are necessary if one is to have a large number of possible extensions of $\mathcal{S} \setminus \{\mathbf{b}\}$, are more prone to bad blocks than are smaller designs. Indeed, the larger the number of extensions of $\mathcal{S} \setminus \{\mathbf{b}\}$, the more likely it seems that $\mathbf{b}$ will be bad. A further trend observed, at least amongst the STS(15)s, is that designs with small automorphism groups seem generally to have more bad blocks in their smallest defining sets than designs having the same parameters but larger automorphism groups. The smallest defining sets of smallest cardinality amongst those for all designs with a given parameter set also seem to be more likely to have a greater proportion of bad blocks. Of course, we accept that our evidence for these being general rules is far from conclusive.

We have also examined a handful of $2 - (19, 3, 1)$ designs, using the smallest defining sets given in [1]. In some cases, the number of extensions of $\mathcal{S} \setminus \{\mathbf{b}\}$ can run into hundreds of thousands, which in itself might suggest a degree of security for an associated secret sharing scheme. However, we have found no instance of a good smallest defining set amongst the cases analysed. The computational difficulties of dealing with designs of this size make general observations risky. However, we remark that the designs

covered in [1] are those with the largest automorphism groups and it seems likely that those with smaller groups will be even less suitable.

We have considered the issue of recovering a block design from a minimal defining set with one block deleted, and we have shown that this is possible in some cases. From a design theory perspective, one might reasonably ask if it is ever possible to perform such a reconstruction from a minimal defining set with two (or more) blocks deleted.

Overall, our conclusion is that the prospects for secure secret sharing schemes based on minimal defining sets appear to be dubious.

References

[1] P. Adams, A. Khodkar and C. Ramsay, Smallest defining sets of some STS(19), *J. Combin. Math. Combin. Comput.* **38** (2001), 225-230.

[2] G. Gamble, B. M. Maenhaut, J. Seberry and A. P. Street, Further results on strongbox secured secret sharing schemes, *Util. Math.* **66** (2004), 165-193.

[3] K. Gray, On the minimum number of blocks defining a design, *Bull. Austral. Math. Soc.* **41** (1990), 97-112.

[4] K. Gray, Further results on smallest defining sets of well known designs, *Australas. J. Combin.* **1** (1990), 91-100.

[5] C. S. Greenhill, An algorithm for finding smallest defining sets of t-designs, *J. Combin. Math. Combin. Comput.* **14** (1993), 39-60.

[6] C. S. Greenhill and A. P. Street, Smallest defining sets of some small t-designs and relations to the Petersen graph, *Util. Math.* **48** (1995), 5-31.

[7] R. A. Mathon, K. T. Phelps and A. Rosa, Small Steiner triple systems and their properties, *Ars Combin.* **15** (1983), 3-110.

[8] T. Moran, Smallest defining sets for $2-(9,4,3)$ and $3-(10,5,3)$ designs, *Australas. J. Combin.* **10** (1994), 265-288.

[9] E. J. Morgan, Some small quasi-multiple designs, *Ars Combin.* **3** (1977), 233-250.

[10] C. Ramsay, An algorithm for completing partials , with an application to the smallest defining sets of the STS(15), *Util. Math.* **52** (1997), 205-221.

[11] P. J. Schellenberg and D. R. Stinson, Threshold schemes from combinatorial designs, *J. Combin. Math. Combin. Comput.* **5** (1989), 143-160.

[12] J. Seberry and A. P. Street, Strongbox secured secret sharing schemes, *Util. Math.* **57** (2000), 147-163.

[13] A. Shamir, How to share a secret, *Comm. ACM* **22** no. 11 (1979), 612-613.

[14] G. J. Simmons, Robust shared secret schemes, *Congr. Numer.* **68** (1989), 215-248.