ORTHOGONAL ARRAYS AND ORDERED THRESHOLD SCHEMES

E. Dawson
Information Security Research Centre
Queensland University of Technology
GPO Box 2434
Brisbane Queensland 4001
Australia

E.S. Mahmoodian
Department of Mathematical Sciences
Sharif University of Technology
PO Box 11365 - 9415
Tehran
Iran

Alan Rahilly
Centre for Combinatorics
Department of Mathematics
University of Queensland
Brisbane Queensland 4072
Australia

ABSTRACT

Perfect threshold schemes whose blocks are ordered are introduced. For a given number of shadows v, participants w and threshold t, let M(t, w, v) be the maximum number of keys possible for an ordered perfect threshold scheme. We show that M(t, w, v) = v if and only if there exists an orthogonal array $(v^t, w + 1, v, t)$. The implementability of perfect ordered threshold schemes is considered. In certain cases they are implementable without problems of storage or undue difficulties in decoding.

1. INTRODUCTION

In informal terms, a perfect threshold scheme is a method of sharing a secret key among a number of participants in such a way that

(a) any t participants can determine the key from the t portions of the secret (shadows) that they hold, and

(b) if $t' < t$, it is impossible for any t' participants to obtain any partial information about the key using the t' shadows that they collectively hold.

Threshold schemes were first introduced independently in 1979 by Shamir and Blakley. Since then quite a number of papers have been published on them. (For a bibliography one may refer to Simmons (1989).) Most of the early constructions were linear algebraic in nature. Recently Stinson and Vanstone (1988) have developed a combinatorial design approach to threshold schemes. In their approach the shadows apportioned to the participants are taken to constitute an (unordered) set, and a threshold scheme is a certain sort of uniform hypergraph. In Section 2 we introduce an analogous approach to threshold schemes using ordered rather than unordered sets. In our approach the shadows apportioned to the participants are taken to constitute an ordered set and a perfect threshold scheme is a certain sort of block code. We refer to our perfect threshold schemes as being "ordered" to distinguish them from those of Stinson and Vanstone (1988). This characterisation for threshold schemes is similar to the approach taken by Brickell and Davenport (1991). In this paper Brickell and Davenport characterise secret sharing schemes in terms of matrices. They also mention that a 2-out-of-n threshold scheme can be constructed from orthogonal arrays of strength two. However the results in this paper goes beyond this and demonstrates that general t-out-of-n threshold schemes can be constructed from orthogonal arrays of strength t.

Given v shadows, w participants and threshold t (as in (a) and (b) above), it is natural to seek to determine the maximum value $M(t, w, v)$ that the number of keys can take. In the unordered case Stinson and Vanstone have established that $M(t, w, v) \leq \frac{v - t + 1}{w - t + 1}$ with equality if and only if there is a Steiner system $S(t, w, v)$ which can be partitioned into Steiner systems $S(t - 1, w, v)$. In Section 3 we adapt the methods of these authors to obtain: In the ordered case $M(t, w, v) \leq v$ with equality if and only if there is an orthogonal array based on v symbols of strength t, depth $w + 1$ and index one. This enables us to show that $M(t, t, v) = v$ for all relevant t and v. Clearly, this contrasts favourably with the unordered case, since $M(3, 3, v)$ is not yet completely determined in the unordered case, even after considerable effort, and relatively little seems to be known about (unordered) $M(t, t, v)$ for $t > 3$. (For a survey of results on unordered perfect threshold schemes Chen and Stinson (1990) should be consulted.) Also, using known results on orthogonal arrays we are able to show that $M(t, w, v) = v$ for a further range of t, w, v. For example, we show that, for given t and w such that $2 \le t \le w$, there are infinitely many v such that $M(t, w, v) = v$, and that, for every $t < p_1^{\alpha_1}$, $M(t, p_1^{\alpha_1}, v) = v$, where $p_1^{\alpha_1} \ge 3$ is the smallest prime power in the prime power factorization of v.

In Section 4 we discuss the implementation of ordered perfect threshold schemes. In particular, we show that ordered perfect threshold schemes with $t = w$ and v keys can be constructed having the following desirable features

(i) no ordered sets need to be constructed ahead of time,

(ii) large numbers of ordered sets need not be stored, and

(iii) the key is easily computable given t shadows in their correct positions.

2. ORDERED THRESHOLD SCHEMES

Let $w > 0$. A *w-uniform ordered hypergraph* is a pair $(X, \mathscr{A})$, where X is a non-empty set of elements (called *points*) and $\mathscr{A}$ is a multiset of w-tuples of elements of X (called *blocks*). Note here that our w-tuples are ordered and that an element of X may occur more than once in a given w-tuple. If every w-tuple of $(X, \mathscr{A})$ has multiplicity one (ie. $\mathscr{A}$ is a set), then we say that $(X, \mathscr{A})$ is *simple*. (A simple w-uniform ordered hypergraph is, of course, merely a block code.)

Given a w-uniform ordered hypergraph $(X, \mathscr{A})$, for the purposes of continuing our discussion, we adjoin a new element $*$ to X and define a partial order $\le$ on the w-tuples of elements of $X^* = X \cup \{*\}$ by

$$x = (x_1, x_2, ..., x_w) \le (y_1, y_2, ..., y_w) = y$$

if and only if, for all $x_i \neq *$, $x_i = y_i$. (We can think of an occurrence of $*$ in a w-tuple as the occurrence of a blank.) If $\mathbf{x} \leq \mathbf{y}$, then we say that $\mathbf{x}$ is *contained in* $\mathbf{y}$. We define the *width* $\omega(\mathbf{x})$ of $\mathbf{x}$ to be the number of coordinates of $\mathbf{x}$ not equal to $*$. (When we deal with w-tuples of specified width it should be understood that such w-tuples are from $X^* = X \cup \{*\}$.)

Now, let $1 \leq t \leq w$. We define the *t-induced* w-uniform ordered hypergraph of $(X, \mathscr{A})$ to be $(X^*, \mathscr{A}(t))$, where $\mathscr{A}(t)$ is the multiset union $\bigcup_{\mathbf{y} \in \mathscr{A}} \{\mathbf{x} : \mathbf{x} \leq \mathbf{y} \text{ and } \omega(\mathbf{x}) = t\}$.

Two w-uniform ordered hypergraphs $(X, \mathscr{A}_1)$ and $(X, \mathscr{A}_2)$ are said to be *t-disjoint* if the multiset $\mathscr{A}_1(t)$ and the multiset $\mathscr{A}_2(t)$ are disjoint. Also $(X, \mathscr{A}_1)$ and $(X, \mathscr{A}_2)$ are said to be *t-identical* if the multisets $\mathscr{A}_1(t)$ and $\mathscr{A}_2(t)$ are equal (that is, $\mathscr{A}_1(t)$ and $\mathscr{A}_2(t)$ contain the same w-tuples with the same multiplicities).

Let $1 < t \leq w$, $1 < v$ and $1 < m$. A *(t, w, v; m) - ordered threshold scheme* is a simple w-uniform ordered hypergraph $(X, \mathscr{A})$ such that $|X| = v$ and $\mathscr{A}$ can be partitioned into w-uniform ordered hypergraphs $(X, \mathscr{A}_i)$, $i = 0, \ldots, m-1$, (called *components* of $(X, \mathscr{A})$) such that

(1) the $(X, \mathscr{A}_i)$ are mutually t-disjoint, and

(2) no w-tuple of width $t' < t$ occurs in precisely one of the multisets $\mathscr{A}_i(t')$.

The points of a (t, w, v; m) - ordered threshold scheme are referred to as *shadows* and the parameter t is its *threshold*. Also, each element of $K = \{0, 1, \ldots, m-1\}$ is called a *key*. If the $(X, \mathscr{A}_i)$ are also mutually t'-identical for some t' such that $0 < t' < t$, then we say that $(X, \mathscr{A})$ is *t'-perfect*. A (t - 1) - perfect (t, w, v, m) - ordered threshold scheme is said to be *perfect*. Furthermore, an ordered threshold scheme is called *regular* if $|\mathscr{A}_i| = |\mathscr{A}_j|$ for all $i, j = 0, \ldots, m-1$. (Note here that our usage of the term 'regular' diverges somewhat from that in Stinson and Vanstone (1988).)

Example

$\mathcal{A}_0$	$\mathcal{A}_1$	$\mathcal{A}_2$	$\mathcal{A}_3$
0 0 0 0	0 1 3 2	0 2 1 3	0 3 2 1
1 1 1 1	1 0 2 3	1 3 0 2	1 2 3 0
2 2 2 2	2 3 1 0	2 0 3 1	2 1 0 3
3 3 3 3	3 2 0 1	3 1 2 0	3 0 1 2
0 1 2 3	0 0 1 1	0 3 3 0	0 2 0 2
1 0 3 2	1 1 0 0	1 2 2 1	1 3 1 3
2 3 0 1	2 2 3 3	2 1 1 2	2 0 2 0
3 2 1 0	3 3 2 2	3 0 0 3	3 1 3 1
0 2 3 1	0 3 0 3	0 0 2 2	0 1 1 0
1 3 2 0	1 2 1 2	1 1 3 3	1 0 0 1
2 0 1 3	2 1 2 1	2 2 0 0	2 3 3 2
3 1 0 2	3 0 3 0	3 3 1 1	3 2 2 3
0 3 1 2	0 2 2 0	0 1 0 1	0 0 3 3
1 2 0 3	1 3 3 1	1 0 1 0	1 1 2 2
2 1 3 0	2 0 0 2	2 3 2 3	2 2 1 1
3 0 2 1	3 1 1 3	3 2 3 2	3 3 0 0

A Perfect (3, 4, 4; 4) Ordered Threshold Scheme

The following proposition is basic.

Proposition 1

Let $(X, \mathcal{A})$ be a $(t, w, v; m)$ - ordered threshold scheme. If $(X, \mathcal{A})$ is t' - perfect for some t' such that $0 < t' < t$, then $(X, \mathcal{A})$ is regular and t'' - perfect for all t'' such that $1 \leq t'' \leq t'$.

Proof

Suppose $(X, \mathcal{A})$ is t'-perfect. Counting the number of w-tuples of width t' contained in the w-tuples of $\mathcal{A}_i$ yields $\binom{w}{t'} \mid \mathcal{A}_i \mid$. Since $(X, \mathcal{A})$ is t'-perfect this number is independent of i.

Consider any w-tuple $\mathbf{x}$ of $\mathcal{A}_i(t'')$. For any w-tuple $\mathbf{y}$ of $\mathcal{A}_i$ such that $\mathbf{x} \leq \mathbf{y}$, there are $\binom{w - t''}{t' - t''}$ w-tuples $\mathbf{z}$ of $\mathcal{A}_i(t')$ such that $\mathbf{x} \leq \mathbf{z} \leq \mathbf{y}$. Let $\lambda(\mathbf{z})$ be the multiplicity of $\mathbf{z}$ in $\mathcal{A}_i(t')$. Now $\Sigma\, \lambda(\mathbf{z})$, the summation being over all $\mathbf{z}$ such that $\mathbf{x} \leq \mathbf{z}$ and $\omega(\mathbf{z}) = t'$, is the number of times such w-tuples are contained in a w-tuple of $\mathcal{A}_i$. This sum is independent of i as $\mathcal{A}_i(t') = \mathcal{A}_j(t')$ for all $i, j \in \{0, 1, ..., m - 1\}$. So the multiplicity of $\mathbf{x}$ in $\mathcal{A}_i(t'')$ is $\Sigma\, \lambda(\mathbf{z}) \big/ \binom{w - t''}{t' - t''}$, which is independent of i. ◊

The following protocol might be used for secret sharing. Suppose $\mathcal{P}$ wants to 'share' a secret key k $(0 \leq k \leq m - 1)$ among a group of w people. The participants are ordered from first to wth, and we say that the ith participant holds *position* i. A participant's position need not be kept secret from the other participants. A suitable (t, w, v; m) - ordered threshold scheme $(X, \mathcal{A})$ is made known to all of the participants. $\mathcal{P}$ chooses at random a block $\mathbf{x} = (x_1, x_2, ..., x_w)$ of component $\mathcal{A}_k$ and then gives the participant holding position j the shadow x_j. Now, if t participants (holding positions i_j, j = 1, ..., t, say) wish to determine the key k, they search through the set of blocks of $(X, \mathcal{A})$. When a block $\mathbf{b}$ is found whose i_j-th co-ordinate is x_{i_j}, for each j = 1, ..., t, then the key is k, where $\mathbf{b} \in \mathcal{A}_k$.

We now turn briefly to a consideration of the security of the secret sharing schemes we are discussing.

Suppose that there is a probability distribution on the set $K = \{0, ..., m - 1\}$ of keys of the ordered threshold scheme $(X, \mathcal{A})$. We also suppose that, for every key k, the blocks in $\mathcal{A}_k$ are chosen with equal probability. Given t' such that $0 < t' < t$, $(X, \mathcal{A})$ is said to be *perfectly t'- secure* if, for every w-tuple $\mathbf{z}$ of width t' that has positive multiplicity in $\mathcal{A}(t')$ and for every key $k \in K$, we have that the conditional probability $p(k \mid \mathbf{z})$ equals $p(k)$.

Proposition 2

Let $\mathbf{z}$ be a w-tuple of width t' that has positive multiplicity in $\mathcal{A}(t')$ and $\lambda_k(\mathbf{z})$ be the multiplicity of $\mathbf{z}$ in $\mathcal{A}_k(t')$. $(X, \mathcal{A})$ is perfectly t'-secure if and only if $\lambda_k(\mathbf{z}) / \mid \mathcal{A}_k \mid$ is independent of k.

Proof

First, $p(k \mid \mathbf{z}) = \dfrac{p(k)\, p(\mathbf{z} \mid k)}{p(\mathbf{z})}$ for any $k \in K$ and $\mathbf{z}$ as in the statement of the proposition. Now $p(\mathbf{z} \mid k) = \dfrac{\lambda_k(\mathbf{z})}{\mathscr{A}_k(t')} = \dfrac{\lambda_k(\mathbf{z})}{\binom{w}{t'} |\mathscr{A}_k|}$ and

$$p(\mathbf{z}) = \sum_{h \in k} \frac{p(h)\, \lambda_h(\mathbf{z})}{\mathscr{A}_h(t')} = \sum_{h \in k} \frac{p(h)\, \lambda_h(\mathbf{z})}{\binom{w}{t'} |\mathscr{A}_h|} .$$

So we have

$$p(k \mid \mathbf{z}) = \left(\frac{p(k)\, \lambda_k(\mathbf{z})}{|\mathscr{A}_k|} \right) \Bigg/ \left(\sum_{h \in K} \frac{p(h)\, \lambda_h(\mathbf{z})}{|\mathscr{A}_h|} \right) . \tag{1}$$

Suppose $(X, \mathscr{A})$ is perfectly t'-secure. From (1), we obtain

$$\frac{\lambda_k(\mathbf{z})}{|\mathscr{A}_k|} = \sum_{h \in K} \frac{p(h)\, \lambda_h(\mathbf{z})}{|\mathscr{A}_h|} ,$$

whence $\dfrac{\lambda_k(\mathbf{z})}{|\mathscr{A}_k|}$ is independent of k.

Suppose $\dfrac{\lambda_k(\mathbf{z})}{|\mathscr{A}_k|}$ is independent of k. Then, from (1), we have

$$p(k \mid \mathbf{z}) = \left(\frac{p(k)\, \lambda_k(\mathbf{z})}{|\mathscr{A}_k|} \right) \Bigg/ \left(\sum_{h \in K} p(h) \left(\frac{\lambda_k(\mathbf{z})}{|\mathscr{A}_k|} \right) \right)$$

$$= \frac{p(k)}{\sum_{h \in K} p(h)} \qquad = p(k) . \Diamond$$

Corollary 1

$(X, \mathscr{A})$ is regular and perfectly t'-secure if and only if $(X, \mathscr{A})$ is t'-perfect.

Proof

Suppose $(X, \mathscr{A})$ is regular and perfectly t'-secure. Then $|\mathscr{A}_k|$ is independent of k. Using Proposition 2, $\lambda_k(\mathbf{z})$ is independent of k.

Suppose $(X, \mathscr{A})$ is t'-perfect. By Proposition 1, $(X, \mathscr{A})$ is regular. Also $\lambda_k(\mathbf{z})$ is independent of k for $\mathbf{z}$ as in the statement of Proposition 2. So $\dfrac{\lambda_k(\mathbf{z})}{|\mathscr{A}_k|}$ is independent of k, whence $(X, \mathscr{A})$ is perfectly t'-secure, by Proposition 2. ◊

Corollary 2

If a regular ordered threshold scheme is perfectly t'-secure, then it is perfectly t''-secure for all t'' such that $1 \leq t'' \leq t'$.

Proof

Suppose $(X, \mathscr{A})$ is regular and perfectly t'-secure. Then $(X, \mathscr{A})$ is t'-perfect, by Corollary 1. By Proposition 1, $(X, \mathscr{A})$ is t''-perfect for all t'' such that $1 \leq t'' \leq t'$. By Corollary 1, $(X, \mathscr{A})$ is perfectly t''-secure for all such t''. ◊

Remarks

(a) Proposition 2 applies no matter what probability distribution we have on K.

(b) Perfectly t'-secure ordered threshold schemes that are not t'-perfect can be obtained from a t'-perfect ordered threshold scheme $(X, \mathscr{A})$ by using unions of the components of $(X, \mathscr{A})$ as components.

3. ORTHOGONAL ARRAYS

Let $1 \leq t \leq w$ and $2 \leq v$. An *orthogonal array* of *strength* t, *depth* w and *index* λ based on v symbols (say 0, 1, ..., v - 1), is an $N \times w$ array such that for any $N \times t$ sub-array each ordered t-tuple from $X = \{0, 1, ..., v - 1\}$ occurs precisely λ times as a row of the sub-array. It is common for such an orthogonal array to be denoted by OA(N, w, v, t) or simply (N, w, v, t). We will use the notation t-(v, w, λ) OA. The number N of rows of a t-(v, w, λ) OA is λv^t. For $t > 1$, any t-(v, w, λ) OA is a (t - 1) - (v, w, vλ) OA. It is known (see MacWilliams and Sloan (1978) and Phelps (1984)) that a t-(v, w, 1) OA is equivalent to a (w, v^t, w - t + 1) code over an alphabet of v symbols (that is, to a "maximum distance separable" code) where the codewords are the row vectors.

Consider a t-(v, w, λ) OA A. The sub-array of A formed by deleting a column (say the j^{th}) of A and all rows of A except those that have a fixed element (say i) in the j^{th} column of A is a (t - 1) - (v, w - 1, λ) OA which we call the *(i, j) - contraction* of A.

A t - (v, w, λ) OA is said to be *(t', μ) - partitionable* if its set of rows can be partitioned into $\lambda v^{t-t'} / \mu$ t' - (v, w, μ) OAs. (Juxtaposing n t - (v, w, λ) OAs yields a (t, λ) - partitionable t - (v, w, nλ) OA.) The component t' - (v, w, μ) OAs are said to form a *(t', μ) - partition* of the t - (v, w, λ) OA. (Analogously to the unordered case, if $\lambda = 1$ and $t' < t = w$ we might refer to the set of components of a (t', μ) - partition as a 'large set' of t' - (v, w, μ) OAs.) The 64 rows in the example in Section 1 form a 3 - (4, 4, 1) OA. $\mathcal{A}_0$, $\mathcal{A}_1$, $\mathcal{A}_2$ and $\mathcal{A}_3$ are the components of a (2, 1) - partition of this orthogonal array.

Corresponding to an orthogonal array there is a w-uniform ordered hypergraph whose blocks are the rows of the orthogonal array. We say that an orthogonal array is *simple* if its corresponding ordered hypergraph is simple. It does no harm to identify an orthogonal array with its corresponding ordered hypergraph. Indeed, we will find it convenient at times to consider an orthogonal array to be an ordered hypergraph.

Let $1 \leq t' < t$ and $\mu < v$. A (t', μ) - partitionable t - (v, w, 1) OA (X, $\mathcal{A}$) is a t' - perfect $\left(t, w, v; \frac{v^{t-t'}}{\mu}\right)$ ordered threshold scheme. The components of the ordered threshold scheme here are, of course, the components of the (t', μ) - partition. For a construction of such ordered threshold schemes see Section 4.

Remark

Orthogonal arrays of index unity (in the guise of maximum distance separable codes) have been introduced by a number of authors into the study of secret sharing schemes; for example, McEliece and Sarwate (1981) and Karnin, Greene and Hellman (1983).

Let t, w, v be such that there is a perfect $(t, w, v; m)$ - ordered threshold scheme for some m. We define $M(t, w, v)$ by $M(t, w, v) = \max\{m:$ there is a perfect $(t, w, v; m)$ - ordered threshold scheme$\}$.

It is our aim to obtain an upper bound on $M(t, w, v)$ and to characterize the ordered threshold schemes which achieve the bound. In order to do this the following two lemmas are useful.

Lemma 1

Let $t \leq w$. There exists a t-$(v, w + 1, \lambda)$ OA if and only if there exists a $(t - 1, \lambda)$ - partitionable t - (v, w, λ) OA.

Proof

Suppose there exists a t - $(v, w + 1, \lambda)$ OA $(X, \mathscr{A})$. For each j the (i, j) - contractions of $(X, \mathscr{A})$, as i runs from 0 to $v - 1$, form a $(t - 1, \lambda)$ - partition of a t - (v, w, λ) OA.

Suppose there is a $(t - 1, \lambda)$ - partitionable t - (v, w, λ) OA $(X, \overline{\mathscr{A}})$ with components $(X, \overline{\mathscr{A}}_i)$, $i = 0, ..., v - 1$. Adding an extra column c to $(X, \overline{\mathscr{A}}_i)$ with entry i in c in the rows of $\overline{\mathscr{A}}_i$ yields a t - $(v, w + 1, \lambda)$ OA. ◊

Consider a w-tuple $\mathbf{x} = (x_1, ..., x_w)$ of X^* of width s such that $w - 1 \geq s \geq 1$ and a w-tuple of X^* $\mathbf{y} = (y_1, ..., y_w)$ of width $s + 1$. If $\mathbf{x} \leq \mathbf{y}$ and $y_k \neq x_k = *$, then we say $\mathbf{y}$ is a *1 - coordinate extension of* $\mathbf{x}$ *at* k. If $\mathscr{T}$ is a set of w-tuples, we denote the set of all 1 - coordinate extensions of $\mathscr{T}$ by $\mathscr{T}^+$.

Lemma 2
Let $(X, \mathscr{A})$ be a perfect $(t, w, v; v)$ - ordered threshold scheme with components $(X, \mathscr{A}_i)$, $i = 0, \ldots, v - 1$, where $\mathscr{A}_i(t - 1) = \mathscr{S}$ for all i. Then

(a) $(X^*, \mathscr{S})$ (and hence $(X^*, \mathscr{A}(t))$) is simple,

(b) $\mathscr{S}^+ = \mathscr{A}(t)$, and

(c) $\mathscr{A}_i(t)$, $i = 0, \ldots, v - 1$, is a partition of $\mathscr{S}^+$.

Proof
Consider $\mathbf{x} \in \mathscr{S}$. For $i = 0, \ldots, v - 1$, there is at least one block $\mathbf{x}_i$ of $\mathscr{A}_i$ such that $\mathbf{x} \le \mathbf{x}_i$. For any appropriate k, let $\mathbf{y}_i(k)$ be the 1 - coordinate extension at k of $\mathbf{x}$ such that $\mathbf{y}_i(k) \le \mathbf{x}_i$. Since the $\mathscr{A}_i(t)$ are v in number and mutually t-disjoint we have that:

$$\text{the } \mathbf{y}_i(k) \text{ are all of the 1 - coordinate extensions of } \mathbf{x} \text{ at } k. \qquad (2)$$

(a) Suppose $\overline{\mathbf{x}}_i \in \mathscr{A}_i$ such that $\mathbf{x} \le \overline{\mathbf{x}}_i$ and let $\overline{\mathbf{y}}_i(k)$ be the 1 - coordinate extension of $\mathbf{x}$ at k such that $\overline{\mathbf{y}}_i(k) \le \overline{\mathbf{x}}_i$. Since the $\mathscr{A}_i(t)$ are mutually t-disjoint and (2) applies we have that $\mathbf{y}_i(k) = \overline{\mathbf{y}}_i(k)$. But then we have $\overline{\mathbf{x}}_i = \mathbf{x}_i$. Since $(X, \mathscr{A})$ is simple, we infer that $(X^*, \mathscr{S})$ is simple. In consequence, $(X^*, \mathscr{A}(t))$ is also simple.

(b) Returning to (2), we see that $\mathscr{S}^+ = \mathscr{A}(t)$.

(c) The $\mathscr{A}_i(t)$ partition $\mathscr{A}(t) = \mathscr{S}^+$. ◊

We are now in a position to establish our main result.

Theorem 1
$M(t, w, v) \le v$ with equality if and only if there exists a t-$(v, w + 1, 1)$ OA.

Proof
The bound is well-known (see Brickell and Stinson (1991)) but a proof is given for the sake of completeness. Suppose $M(t, w, v) > v$. Consider a perfect $(t, w, v; M(t, w, v))$ - ordered threshold scheme $(X, \mathscr{A})$ with components $(X, \mathscr{A}_i)$ such that $\mathscr{A}_i(t - 1) = \mathscr{S}$ for all i. Let $\mathbf{x} \in \mathscr{S}$. For each appropriate k, we can obtain a 1 - coordinate extension $\mathbf{y}_i(k)$ of $\mathbf{x}$ at k from each $\mathscr{A}_i$. Since there are precisely v such 1 - coordinate extensions of $\mathbf{x}$ at k and $M(t, w, v) > v$, we have that the $\mathscr{A}_i$ are not t - disjoint, a contradiction.

Suppose there is a t - $(v, w + 1, 1)$ OA. By Lemma 1, there is a $(t - 1, 1)$ - partitionable t - $(v, w, 1)$ OA. The corresponding perfect $(t, w, v; m)$ - ordered threshold scheme has $m = v$. So $M(t, w, v) \geq v$, whence $M(t, w; v) = v$.

Suppose $M(t, w, v) = v$. Consider a perfect $(t, w, v; v)$ - ordered threshold scheme $(X, \mathscr{A})$. By Lemma 2(a), $(X^*, \mathscr{S})$ and $(X^*, \mathscr{A}(t))$ are simple.

Now, consider any w-tuple $\mathbf{x}''$ of width t. Let $\mathbf{x}'$ be a element of $\mathscr{S}^+$. We show that $\mathbf{x}'' \in \mathscr{A}(t)$ by reverse induction on the number n of coordinates at which $\mathbf{x}''$ and $\mathbf{x}'$ agree, that is, on the number of coordinates at which $x_i'' = x_i' \neq *$. If $n = t$, then $\mathbf{x}'' = \mathbf{x}'$ and so $\mathbf{x}'' \in \mathscr{A}(t)$, by Lemma 2(b). Our inductive hypothesis is: $\mathbf{x}'' \in \mathscr{A}(t)$ for all $\mathbf{x}''$ such that $n \geq t - j$, where $j \geq 0$.

Consider $\mathbf{x}''$ such that $n = t - j - 1$. Then (i) there are k and ℓ such that $x_k' \neq x_k'' = *$ and $* = x_\ell' \neq x_\ell''$ or (ii) k where $x'_k \neq x''_k$ and $x'_k , x''_k \neq *$.

(i) Consider $\mathbf{x}^*$ of width t defined by $x_h^* = x_h''$ for all $h \neq k, \ell$ and $x_k^* = x_k'$ and $x_\ell^* = *$. Now the number of coordinates at which $\mathbf{x}^*$ and $\mathbf{x}'$ agree is $t - j$. By the inductive hypothesis, $\mathbf{x}^* \in \mathscr{A}(t)$. Define $\overline{\mathbf{x}}$ by $\overline{x}_h = x^*_h$ for all $h \neq k$ and $\overline{x}_k = *$. Now $\overline{\mathbf{x}}$ is of width $t - 1$ and $\overline{\mathbf{x}} \leq \mathbf{x}^*$. So $\overline{\mathbf{x}} \in \mathscr{S}$. But $\mathbf{x}''$ is a 1 - coordinate extension of $\overline{\mathbf{x}}$ at ℓ, that is, $\mathbf{x}'' \in \mathscr{S}^+$. By Lemma 2(b), $\mathbf{x}'' \in \mathscr{A}(t)$.

(ii) Similarly it can be shown that $x'' \in \mathscr{A}(t)$. In the case where $x'_k \neq x''_k$ and $x'_k , x''_k \neq *$.

That the set $\mathscr{A}(t)$ equals the set $\{\mathbf{z} : \omega(\mathbf{z}) = t\}$ follows by induction and so $(X, \mathscr{A})$ is a t - $(v, w, 1)$ OA.

Finally, consider $\mathbf{u}$ of width $t - 1$. Let $\mathbf{v}$ be a 1 - coordinate extension of $\mathbf{u}$. Since $\mathbf{v} \in \mathscr{A}(t)$, we have $\mathbf{u} \in \mathscr{S}$. So the set $\mathscr{S}$ equals the set $\{\mathbf{z} : \omega(\mathbf{z}) = t - 1\}$ and therefore $(X, \mathscr{A}_i)$ is a $(t - 1)$ - $(v, w, 1)$ OA. Hence, $(X, \mathscr{A})$ is a $(t - 1, 1)$ - partitionable t - $(v, w, 1)$ OA. By Lemma 1, there exists a t - $(v, w + 1, 1)$ OA. ◊

Corollary 1

(a) For $t, v \geq 2$, $M(t, t, v) = v$.

(b) (i) For $w > t \geq 2$, if $M(t, w, v) = v$, then $M(t, w - 1, v) = v$.
(ii) For $t \geq 3$, if $M(t, w, v) = v$, then $M(t - 1, w - 1, v) = v$.

(c) Let $s \geq 2$. If $M(t, w_i, v_i) = v_i$ for $i = 1, \ldots, s$, then

$$M\left(t, \min w_i, \prod_{i=1}^{s} v_i\right) = \prod_{i=1}^{s} v_i .$$

(d) (i) For $t < q$ and q a prime power, $M(t, q, q) = q$.
(ii) For q an even prime power, $M(3, q + 1, q) = q$.

(e) If there is a Steiner system $S(3, q + 1, v + 1)$ with q a prime power, then $M(3, q, v) = v$.

Proof

(a) Take a t - $(v, t, 1)$OA, $(X, \mathcal{A})$, where $X = \{0, \ldots, v - 1\}$. (Here, of course, each t-tuple of X occurs precisely once as a block.) Add one extra column containing in a given row the sum modulo v of the entries in that row of $(X, \mathcal{A})$. The extended array is easily shown to be a t - $(v, t + 1, 1)$OA. That $M(t, t, v) = v$ then follows using Theorem 1.

(b) (i) Deleting a column of a t - $(v, w + 1, 1)$OA yields a t - $(v, w, 1)$ OA.
(ii) An (i, j) - contraction of a t - $(v, w + 1, 1)$OA is a $(t - 1)$ - $(v, w, 1)$ OA.

(c) This part follows from Theorem 1 and Raghavarao (1971).

(d) This follows from Theorem 1 and well known results of Bush (1952).

(e) Theorem 1 and Phelps (1981). ◊

Corollary 2

For all t and w such that $2 \leq t \leq w$, there are infinitely many values of v for which $M(t, w, v) = v$.

Proof

If $t = w$, then the result follows from Corollary 1(a). If $t < w$, then choose a prime power q such that $w < q$. By Corollary 1(d)(i), $M(t, q, q) = q$. Applying Corollary 1(b)(i) an appropriate number of times yields $M(t, w, q) = q$. ◊

Corollary 3

Let the prime power factorization of v be $p_1^{\alpha_1} \ldots p_s^{\alpha_s}$, where $p_i^{\alpha_i} < p_j^{\alpha_j}$ when $i < j$, and $3 \leq p_1^{\alpha_1}$. For every $t < p_1^{\alpha_1}$, $M(t, p_1^{\alpha_1}, v) = v$.

Proof

Using Corollary 1(d)(i), $M(t, p_i^{\alpha_i}, p_i^{\alpha_i}) = p_i^{\alpha_i}$, $i = 1, \ldots, s$. If $s = 1$ there is nothing to prove. If $s \geq 2$, then applying Corollary 1(c) yields $M(t, p_1^{\alpha_1}, v) = v$. ◊

A perfect (t, w, v; v) - threshold scheme is said to be *ideal.*

Remark

Maximizing m for given t, w and v is related to minimizing v given t, w and m. As for the unordered case, by minimizing v we are minimizing the amount of secret information to be communicated in the form of shadows.

4. CONCLUDING DISCUSSION

From the following proposition we can infer the existence of t'-perfect ordered threshold schemes.

Proposition 3

Let G be a finite group of order v, tG be the t-fold direct sum of G with itself and H be a subgroup of tG. If the elements of H form a t'- (v, t, μ) OA and $\mu < v$, then there is a t'-perfect $\left(t, t, v; \frac{v^{t-t'}}{\mu}\right)$ - ordered threshold scheme.

Proof

The left (or right) cosets of H in G are the components of a (t', μ) - partition of the t - $(v, t, 1)$ OA whose rows are the elements of tG. These cosets are clearly mutually t-disjoint.

Next, consider t'' such that $t' < t'' < t$. Each $\mathbf{x}''$ of width t'' is contained in precisely $v^{t - t''}$ elements of tG. Suppose such an $\mathbf{x}''$ is contained only in elements of a single left coset of H in G. Since $\mu < v \leq v^{t - t''}$, there are $\mathbf{x}'$ of width t' contained in more than μ elements of this coset, a contradiction. We infer that no $\mathbf{x}''$ of width $t'' < t$ is contained only in the elements of a single coset of H in G.

Clearly, the left cosets of H in G form the components of a t'-perfect $\left(t, t, v; \frac{v^{t - t'}}{\mu}\right)$ - ordered threshold scheme. ◊

Corollary

Let q be a prime power and $t' < t$. If there is a linear $(t, q^{t'}, t - t' + 1)$ code, then there is a t'-perfect $(t, t, q; q^{t - t'})$ - ordered threshold scheme.

Consider the group Z_v of integers modulo v, where $v \geq 2$. The rows of the t - $(v, t + 1, 1)$ OA constructed in the proof of Corollary 1(a) to Theorem 1 form a subgroup H_0 of $(t + 1) Z_v$. The cosets of H_0 in $(t + 1) Z_v$ are the components of a perfect $(t + 1, t + 1, v; v)$ - ordered threshold scheme. These cosets are $(0, ..., 0, i) + H_0$, $i = 0, ..., v - 1$. Now suppose a trusted authority chooses at random a $(t + 1)$ - tuple $\mathbf{x} = \left(x_1, ..., x_t, \sum_{j=1}^{t} x_j \ (\mathrm{mod}\ v)\right)$ of H_0 and distributes x_j to the j^{th} participant, $j = 1, ..., t$, and $\sum_{j=1}^{t} x_j + i \ (\mathrm{mod}\ v)$ to the $(t + 1)^{th}$ participant. The $t + 1$ participants can derive the secret i by subtracting the sum of the shadows assigned to the first t participants from that assigned to the $(t + 1)^{th}$ participant (working modulo v). Clearly this threshold scheme has the desirable features (i), (ii) and (iii) listed at the end of Section 1.

Stinson and Vanstone (1988) have interpreted the well known perfect threshold schemes of Shamir (1979) as unordered perfect threshold schemes. In that context Shamir's perfect threshold schemes are not ideal. It is, however, more natural to interpret Shamir's schemes as being perfect ordered threshold schemes. In the ordered context Shamir's schemes are ideal.

Let us consider this further. For any prime p and t and w such that $2 \leq t \leq w < p$ we construct a t - $(p, w + 1, 1)$ OA as follows: The rows of the array correspond bijectively to the polynomials of degree at most $t - 1$ over GF(p) and the columns to the elements of a subset of order $w + 1$ of GF(p) containing 0. The entry in a given row and given column is the value of the polynomial corresponding to that row taken at the element of GF(p) corresponding to that column. Suppose 0 corresponds to column j. Then the (i, j) - contractions as i ranges over GF(p) form the components of a perfect $(t, w, p; p)$ - ordered threshold scheme $(X, \mathcal{A})$. A block of $(X, \mathcal{A})$ whose coordinates are distributed to w participants corresponds to a polynomial $h(x)$ of degree at most $t - 1$ over GF(p). The secret may be taken to be $h(0)$. The secret may be recovered by any t participants by determining $h(x)$ using Lagrange interpolation and then evaluating $h(0)$. Clearly these ideal perfect ordered threshold schemes also have the desirable properties listed at the end of Section 1.

Remarks

(a) For any prime power q, we could work over GF(q).

(b) The close connection between the perfect threshold schemes of Shamir and orthogonal arrays of index unity of Bush (1952) is well known.

(c) The classification of structures with $M(t, v, w) = v$ (see Theorem 1) has also been done independently by Jackson and Martin (submitted), using t-transversal designs.

REFERENCES

Blakley, G.R. 1979. Safeguarding cryptographic keys, *Proc. N.C.C.*, 48, AFIPS, New York, USA, pp. 313-317.

Brickell, E.F. and Davenport, D.M. 1991. On the classification of Ideal Secret Sharing Schemes, J. Cryptology 4: 123-134.

Brickell, E.F. and Stinson, D.R. 1991. Some improved bounds on the information rate of perfect secret sharing schemes. *Advances in Cryptology: Proceedings of CRYPTO '90.* Springer-Verlag, pp. 242 - 252.

Bush, K.A. 1952. Orthogonal arrays of index unity, *Ann. Math. Statist.* 23: 426-434.

Chen, D. and Stinson, D.R. 1990. Recent results on combinatorial constructions for threshold schemes, *Australas. J. Combin.* 1 : 29-48.

Jackson, W.A. and Martin, K.M. (submitted). On Ideal Secret Sharing Schemes.

Karnin, E.D., Greene, J.W. and Hellman, M.E. 1983. On secret sharing systems, *IEEE Trans. on Inform. Theory* 29: 35-41.

McEliece, R. and Sarwate, D. 1981. On sharing secrets and Reed-Solomon codes, *Comm. ACM.* 24: 583-584.

MacWilliams, F.J. and Sloane, N.J.A. 1978. *The Theory of Error Correcting Codes.* Amsterdam: North-Holland Publishing Company, Chapter 11.

Phelps, K.T. 1981. Direct product of derived Steiner systems using inversive planes, *Canad. J. Math.* 33 : 1365-1369.

Phelps, K.T. 1984. A general product construction for error-correcting codes *SIAM J. Algebraic Discrete Methods,* 5: 224-228.

Raghavarao, D. 1971. *Constructions and Combinatorial Problems in the Design of Experiments.* New York: Wiley, Chapter 2, p. 28.

Schellenberg, P. and Stinson, D.R. 1989. Threshold schemes from combinatorial designs, *J. Combin. Math. Combin. Comput.* 5: 143-160.

Shamir, A. 1979. How to share a secret, *Comm. ACM* 22: 612-613.

Simmons, G.J. 1989. Robust shared secret schemes or "How to be sure you have the right answer even though you don't know the question", *Congr. Numer.* 68: 215-248.

Stinson, D.R. and Vanstone, S.A. 1988. A combinatorial approach to threshold schemes, *SIAM J. on Discrete Math.* 1: 230-236.

(Received 2/12/92)