ARTICLE IN PRESS

Discrete Mathematics ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Ideal ramp schemes and related combinatorial objects

Douglas R. Stinson

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

ARTICLE INFO

Article history:
Received 18 May 2017
Received in revised form 28 August 2017
Accepted 29 August 2017
Available online xxxx

Keywords:
Orthogonal array
Ramp scheme
Threshold scheme

ABSTRACT

In 1996, Jackson and Martin (Jackson and Martin, 1996) proved that a strong ideal ramp scheme is equivalent to an orthogonal array. However, there was no good characterization of ideal ramp schemes that are not strong. Here we show the equivalence of ideal ramp schemes to a new variant of orthogonal arrays that we term *augmented orthogonal arrays*. We give some constructions for these new kinds of arrays, and, as a consequence, we also provide parameter situations where ideal ramp schemes exist but strong ideal ramp schemes do not exist.

1. Introduction

Informally, a (t, n)-*threshold scheme* [2,17] is a method of distributing secret information (called *shares*) to n players, in such a way that any t of the n players can compute a predetermined *secret*, but no subset of $t-1$ players can determine the secret. The integer t is called the *threshold*; we assume that $1 \leq t \leq n$.

It is well-known that the number of possible shares in a threshold scheme must be greater than or equal to the number of possible secrets. If the number of possible secrets in a threshold scheme equals the number of possible shares, the scheme is termed *ideal*.

Ramp schemes were invented in 1984 by Blakley and Meadows [4]. *An* (s, t, n)-*ramp scheme* is a generalization of a threshold scheme in which there are two thresholds. The value s is the *lower threshold* and t is the *upper threshold*. In a ramp scheme, any t of the n players can compute the secret (exactly as in a (t, n)-threshold scheme). It is also required that no subset of s players can determine the secret. We note that a $(t-1, t, n)$-ramp scheme is exactly the same thing as a (t, n)-threshold scheme. The parameters of a ramp scheme satisfy the conditions $0 \leq s < t \leq n$.

A ramp scheme with $s < t-1$ possibly permits a larger number of possible secrets (for a given number of shares) than is the case in a threshold scheme. (Equivalently, for a given secret size, a ramp scheme may incorporate smaller shares.) Thus, ramp schemes permit interesting and potentially useful ways to trade off security for efficiency (i.e., storage). Two examples of applications of ramp schemes are constructing efficient broadcast encryption schemes [20] and "repairing" shares in threshold schemes [19]. It is also worth noting that Rabin's *information dispersal algorithm* [16], which is used for distributed storage, is a special case of ramp schemes.

If there are v possible shares in an (s, t, n)-ramp scheme, then the number of possible secrets is bounded above by v^{t-s}. Of course, for $s < t-1$, it holds that $v^{t-s} > v$. When $s = t-1$, the bound is equal to v, agreeing with the above-mentioned bound for threshold schemes. If an (s, t, n)-ramp scheme can be constructed with v^{t-s} possible secrets (given v possible shares), then we say that the ramp scheme is *ideal*. Thus, an ideal $(t-1, t, n)$-ramp scheme is the same thing as an ideal (t, n)-threshold scheme.

One of the very first constructions for threshold schemes, the Shamir threshold scheme [17], yields ideal schemes. It is also well-known that ideal threshold schemes are equivalent to certain well-studied combinatorial structures, namely, orthogonal arrays and maximum distance separable (MDS) codes [14,6,3].

E-mail address: dstinson@uwaterloo.ca.

http://dx.doi.org/10.1016/j.disc.2017.08.041
0012-365X/

Please cite this article in press as: D.R. Stinson, Ideal ramp schemes and related combinatorial objects, Discrete Mathematics (2017), http://dx.doi.org/10.1016/j.disc.2017.08.041.

strong ideal(s,t,n)-ramp scheme defined over a set of v shares	$\Longleftrightarrow$	$\mathrm{OA}(t, n+t-s, v)$
$\Downarrow$		$\Downarrow$
ideal (s,t,n)-ramp scheme defined over a set of v shares	$\Longleftrightarrow$	$\mathrm{AOA}(s,t,n,v)$

Fig. 1. Relationships between ramp schemes and combinatorial structures.

There is less work on combinatorial characterizations of ideal ramp schemes. The main result in this direction is due to Jackson and Martin [10, Theorem 9], who show that an ideal (s, t, n)-ramp scheme that satisfies certain additional conditions (they call such a scheme a *strong* ramp scheme) is equivalent to an ideal $(t, n + t - s - 1)$-threshold scheme. This result is perhaps not completely satisfying because the additional conditions used to define strong ramp schemes are rather restrictive.[1] In [10], the authors ask if it is possible to construct ideal ramp schemes that are not strong. This is one of the open questions that we answer in this paper.

Our approach is to define a new type of combinatorial structure that we term an *augmented orthogonal array*, or *AOA*. We prove that any ideal ramp scheme is equivalent to a certain augmented orthogonal array. This equivalence can be proven in a relatively straightforward manner, analogous to the proof that an ideal threshold scheme is equivalent to an orthogonal array. We then investigate some methods of constructing augmented orthogonal arrays. There is a natural way to construct augmented orthogonal arrays from orthogonal arrays. (Roughly speaking, the resulting augmented orthogonal arrays correspond to the strong ramp schemes considered in [10,21].) However, we observe that there are also constructions of augmented orthogonal arrays which yield ideal ramp schemes that are not strong. Moreover, we show there are parameter situations for which there exist ideal ramp schemes, but where there do not exist strong ideal ramp schemes. These results provide answers to the questions that were first posed in [10].

For future reference, Fig. 1 shows the relationships between the ramp schemes and combinatorial structures we discuss in this paper.

The rest of this paper is organized as follows. In Section 2, we give formal definitions of ramp and threshold schemes, based on the "distribution rules" for the scheme. Section 3 reviews combinatorial structures equivalent to ideal threshold schemes (orthogonal arrays, MDS codes, etc.) in both the linear and general cases (in this context, the term "linear" means that the object in question can be viewed as a subspace of a vector space over a finite field). Section 4 introduces the new notion of an augmented orthogonal array (AOA). We then discuss the connection between AOAs and orthogonal arrays. We also provide some constructions for AOAs in situation where "associated" orthogonal arrays do not exist. Section 5 gives the proof that an ideal ramp scheme is equivalent to an AOA. We also provide examples of ideal ramp schemes that are not strong in this section. Finally, we conclude with some possible problems for future research in Section 6.

2. Formal definitions of ramp and threshold schemes

In this section, we provide formal definitions of ramp schemes in two flavours, namely, "weak" and "perfect". Our definitions are phrased in terms of "distribution rules", which is one of the standard ways of defining these types of schemes. (For a discussion of this model in relation to other models, we refer the reader to [11].)

Suppose there is an (s, t, n)-ramp scheme defined over a set of v secrets. We will assume without loss of generality that the set of possible shares for any player is $\mathcal{X} = \{1, \ldots, v\}$, and we denote the set of possible secrets by $\mathcal{K}$.

We now present a formal mathematical model for a ramp scheme. Denote the set of n *players* by $\mathcal{P} = \{P_1, \ldots, P_n\}$. A *distribution rule* d represents a possible distribution of shares to the n players. So we can view d as a function, i.e., $d : \mathcal{P} \to \mathcal{X}$. The share given to P_i is $d(P_i)$, $1 \le i \le n$. We may also represent d as an n-tuple $(d_1, \ldots, d_n)$, where $d_i = d(P_i)$, for $1 \le i \le n$. Finally, for a distribution rule d and a subset of players $\mathcal{P}_0 \subseteq \mathcal{P}$, we define the *projection of* d *to* $\mathcal{P}_0$, denoted $d|_{\mathcal{P}_0}$, to be the restriction of d to the subdomain $\mathcal{P}_0$. A projection can be represented as a tuple of length $|\mathcal{P}_0|$.

For every possible secret $K \in \mathcal{K}$, we have a non-empty collection of distribution rules denoted by $\mathcal{D}_K$. The collection $\mathcal{D}_K$ is the subset of distribution rules for which K is the value of the secret. The entire set of distribution rules is denoted by $\mathcal{D} = \bigcup_K \mathcal{D}_K$. We assume without loss of generality that the distribution rules in $\mathcal{D}$ are all distinct.

When the *dealer* wishes to share a secret $K \in \mathcal{K}$, they first choose a distribution rule $d \in \mathcal{D}_K$ and then they use d to distribute shares to the n players. The choice of the secret K and the distribution rule d will be determined by appropriate probability distributions. The only property that we will require moving forward is that every possible distribution rule is used with positive probability (which implies that every possible secret occurs with positive probability).

Definition 2.1. A set of distribution rules $\mathcal{D}$ is a *weak* (s, t, n)*-ramp scheme* if the following two properties are satisfied:

(1) Suppose $K, L \in \mathcal{K}$, $|\mathcal{P}_0| \ge t$, $d \in \mathcal{D}_K$, $e \in \mathcal{D}_L$ and $d|_{\mathcal{P}_0} = e|_{\mathcal{P}_0}$. Then $K = L$. (This property is saying that t or more shares determine a unique secret.)

[1] Since the definition of a strong ramp scheme is complicated and we do not require the details for the purposes of this paper, we refer the reader to [10, §3] for the definition.

Please cite this article in press as: D.R. Stinson, Ideal ramp schemes and related combinatorial objects, Discrete Mathematics (2017), http://dx.doi.org/10.1016/j.disc.2017.08.041.