

Revisiting the Karnin, Greene and Hellman Bounds

Yvo Desmedt¹, Brian King², and Berry Schoenmakers³

¹ Department of Computer Science

University College London

y.desmedt@cs.ucl.ac.uk

² Dept. of Elec. & Comp. Eng.

Indiana University - Purdue University Indianapolis

briking@iupui.edu

³ Dept. of Mathematics and Computer Science

Technical University of Eindhoven

berry@win.tue.nl

Abstract. The algebraic setting for threshold secret sharing scheme can vary, dependent on the application. This algebraic setting can limit the number of participants of an *ideal secret sharing scheme*. Thus it is important to know for which thresholds one could utilize an *ideal threshold sharing scheme* and for which thresholds one would have to use non-ideal schemes. The implication is that more than one share may have to be dealt to some or all parties. Karnin, Greene and Hellman constructed several bounds concerning the maximal number of participants in threshold sharing scheme. There has been a number of researchers who have noted the relationship between k -arcs in projective spaces and ideal linear threshold secret schemes, as well as between MDS codes and ideal linear threshold secret sharing schemes. Further, researchers have constructed optimal bounds concerning the size of k -arcs in projective spaces, MDS codes, etc. for various finite fields. Unfortunately, the application of these results on the Karnin, Greene and Hellman bounds has not been widely disseminated. Our contribution in this paper is revisiting and updating the Karnin, Greene, and Hellman bounds, providing optimal bounds on the number of participants in ideal linear threshold secret sharing schemes for various finite fields, and constructing these bounds using the same tools that Karnin, Greene, and Hellman introduced in their seminal paper. We provide optimal bounds for the maximal number of players for a t out of n ideal linear threshold scheme when $t = 3$, for all possible finite fields. We also provide bounds for infinitely many t and infinitely many fields and a unifying relationship between this problem and the MDS (maximum distance separable) codes that shows that any improvement on bounds for ideal linear threshold secret sharing scheme will impact bounds on MDS codes, for which there is a number of conjectured (but open) problems.

1 Introduction

Threshold secret sharing is an important cryptographic tool that is used in many applications in cryptography. It provides group access control of secret keys, and it can be used to provide group signatures and group authentication, it is used in e-voting, e-government, as well as many other applications. The problem that we will consider is to determine the maximal number of players (participants) that can participate in a t out of n linear threshold sharing scheme over a finite field. This number depends on both t and the field \mathbb{F} . Bounds for this problem were introduced almost 25 years ago in [14], but since then few improvements have been made. Meanwhile, there has been considerable work on the bounds of the size of shares for sharing schemes over general access structures, for example [7, 8, 12]. Moreover, there has been significant amount of work concerning bounds on information rate [3, 18, 22]. However, our focus is on *ideal threshold schemes*. An ideal threshold scheme is a threshold sharing scheme for which the size of the shares is the same as the size of the secret.

The problem of determining the maximal number of participants in a t out of n ideal linear threshold scheme is related to a coding theory problem, but the goals are different. In a t out of n threshold scheme we require completeness (any t or more participants can compute the secret) and privacy (any $t - 1$ or less participants learn nothing about the secret). Whereas in coding theory the goal is primarily a “completeness problem”. In [16], McEliece and Sarwate first discussed the relationship between coding theory and secret sharing, however they did not provide any bounds concerning the limitations on the number of participants. In Section 7 we discuss the relationship to the problem we pose and the problem concerning the maximal size of a MDS code for a finite field \mathbb{F} . A considerable amount of research has been conducted on the problem concerning the maximal size of a MDS code for a finite field \mathbb{F} , in particular for many finite fields the maximal size has been known [11, 17, 20], as we discuss in Section 7. Further there is a direct relationship between MDS codes and ideal linear threshold secret sharing schemes. Unfortunately, as far as we know, the Karnin, Greene and Hellman bounds. were not updated. Several other problems, such as k -arcs in a projective space [13], and orthogonal arrays [6] have been shown to be equivalent to MDS codes and/or ideal linear threshold secret sharing schemes, and thus under the equivalence, results concerning maximal size in a finite field would impact the problem of determining the maximal number of participants in a t out of n ideal linear threshold scheme.

Summary of our results The problem posed in this paper is to determine the maximal n for t out of n linear, ideal threshold sharing scheme over a finite field \mathbb{F} , which we denote by $n_{max,t}$ or in short n_{max} . Our results provide improved bounds on the maximal number of participants in a perfect ideal linear secret sharing scheme. Moreover, we are able to construct these bounds using many of the “tools” that Karnin, Greene and Hellman introduced in their ground breaking paper on secret sharing [14]. In this paper we provide optimal solutions for $n_{max,t}$ for $t = 3$ for both fields of characteristic 2 and odd characteristic. We provide upper bounds for $n_{max,t}$ for infinitely many cases of t and \mathbb{F} . We provide a unification of this problem to a coding theory problem and pose open problems that have an implication in threshold secret sharing and coding theory.

2 Background

Shamir [21] and Blakley [1] independently introduced the concept of threshold secret sharing over a finite field.

Definition 1. [22] *A t out of n threshold sharing scheme is a scheme for sharing a secret key k to n participants in such a way that any t participants can reconstruct the key but no group of $t - 1$ or less can reconstruct the key. A t out of n threshold sharing scheme will consist of two phases: the distribution phase where some entity called the dealer, using a distribution algorithm D , constructs shares s_1, \dots, s_n and for $i = 1, \dots, n$. For each i , the dealer privately sends share s_i to participant P_i . The second phase called the reconstruction phase, occurs when t participants P_{i_1}, \dots, P_{i_t} want to reconstruct the secret key. Using reconstruction algorithm R and shares s_{i_1}, \dots, s_{i_t} they reconstruct the secret key k .*

Definition 2. [22] *A t out of n threshold sharing scheme is called a perfect sharing scheme provided that given a secret k , any set of at least t participants can compute k , and any subset of $t - 1$ or less participants gain no information about k . That is, if s_1, \dots, s_n represent the shares distributed to the n participants, then the security conditions are:*

(i) (completeness) $\text{Prob}(\mathbf{k} = k | \mathbf{s}_{i_1} = s_{i_1}, \dots, \mathbf{s}_{i_t} = s_{i_t}) = 1$

(ii) (privacy) $\text{Prob}(\mathbf{k} = k | \mathbf{s}_{i_1} = s_{i_1}, \dots, \mathbf{s}_{i_{t-1}} = s_{i_{t-1}}) = \text{Prob}(\mathbf{k} = k)$

The set Γ which consists of all sets of t or more participants is called the access structure for a threshold scheme.

A linear secret sharing scheme is such that the reconstruction of the secret key by the t participants is performed by taking linear combination of the t shares [22]. In a t out of n linear threshold sharing scheme over finite field \mathbb{F} the shares $\{s_1, \dots, s_n\}$ can be constructed using the *distribution matrix* D as follows.

$$\begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{bmatrix} = \begin{bmatrix} x_{11} & x_{12} & x_{13} & \cdots & x_{1m} \\ x_{21} & x_{22} & x_{23} & \cdots & x_{2m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & x_{n3} & \cdots & x_{nm} \end{bmatrix} \cdot \begin{bmatrix} k \\ a_1 \\ \vdots \\ a_{m-1} \end{bmatrix} \quad (1)$$

Here k is the secret. Equation (1) can be abbreviated as $\bar{S} = D \cdot \bar{y}$ (we use \bar{y} to denote the column matrix). Note that if a perfect linear scheme is defined over a finite field then the number of columns of D will be t .

An *ideal threshold sharing scheme* is a threshold sharing scheme such that the size of the shares is the same as the size of the secret.

Note In the context of this paper, all threshold sharing schemes that are discussed will be perfect, ideal and linear t out on n threshold sharing schemes. We will use the acronym **t out of n PIL threshold sharing scheme** to denote a perfect, ideal and linear t out on n threshold sharing scheme.

Since a t out of n PIL threshold secret sharing scheme must satisfy Definition 1, we can restate the requirements in terms of characteristics of the distribution matrix D .

1. *Completeness.* Any set of participants containing at least t participants can compute the secret k . Thus any t rows of the distributor's matrix D given in (1) must have a row span that includes the row $[1,0,0,\dots,0]$.

2. *Privacy.* No subset of less than t participants can determine any information about the secret k . Thus any $t - 1$ or less rows of D cannot have a row span that includes $[1,0,0,\dots,0]$.

An important tool used in many threshold schemes is the Vandermonde matrix. The Vandermonde matrix is a matrix of the form

$$\begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{l-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{l-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_l & x_l^2 & \cdots & x_l^{l-1} \end{bmatrix}.$$

The determinant of the Vandermonde matrix denoted by $\Delta(x_1, x_2, \dots, x_l)$, over a finite field \mathbb{F} is non-zero provided $x_i \neq x_j$, for $i \neq j$. Thus the Vandermonde matrix is invertible over any field.

Shamir Secret Sharing scheme is an effective tool to share out the secret key whenever the key space is isomorphic to some finite field \mathbb{F} . The essential tool used in Shamir Secret Sharing is the Lagrange interpolation polynomial. Shamir's scheme constructs a t out of n threshold sharing scheme as follows. For secret k belonging to finite field \mathbb{F} , a dealer selects $t - 1$ random elements from \mathbb{F} , denoted by a_1, \dots, a_{t-1} , and computes the polynomial $f(x) = k + a_1x + \dots + a_{t-1}x^{t-1}$. The dealer selects n distinct non-zero elements from \mathbb{F} , x_1, x_2, \dots, x_n and computes $f(x_i)$, for $i = 1, \dots, n$. The dealer then privately sends each participant P_i the share $f(x_i)$. Later when t participants $P_{i_1}, P_{i_2}, \dots, P_{i_t}$ wish to reconstruct the secret key k , they send their shares to a combiner who computes the secret using Lagrange Interpolation: $k = \sum_{j=1}^t f(x_{i_j}) \cdot \prod_{l=1, l \neq j}^t \frac{-x_{i_l}}{x_{i_j} - x_{i_l}}$. Observe that the distribution matrix of Shamir's scheme is the Vandermonde matrix. A limitation imposed by the Shamir secret sharing scheme concerns the limit on the number of participants of a threshold sharing scheme over finite field \mathbb{F} , that is there is an implicit bound that $n \leq |\mathbb{F}| - 1$.

In [14], Karnin, Greene and Hellman described the following threshold sharing scheme which we will call the *Karnin-Greene-Hellman secret sharing scheme*. The scheme is as follows. Consider the finite field $GF(q^m)$. Let α be a primitive element of $GF(q^m)$, and let α_i denote α^i , for $i = 1, \dots, q^m - 1$. The dealer selects a_1, a_2, \dots, a_{t-1} at random from $GF(q^m)$. The dealer then constructs the n shares s_i as follows

$$\begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_r \\ s_{r+1} \end{bmatrix} = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{t-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{t-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_r & \alpha_r^2 & \cdots & \alpha_r^{t-1} \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix} \begin{bmatrix} k \\ a_1 \\ a_2 \\ \vdots \\ a_{t-1} \end{bmatrix} \quad (2)$$

Here $n = r + 1$ and $r \leq q^m - 1$. The dealer then sends s_i privately to participant P_i . Observe that given any t rows of D , denoted by D_{i_1, i_2, \dots, i_t} , the

resulting matrix is a $t \times t$ invertible matrix. Hence $\bar{y} = D_{i_1, i_2, \dots, i_t}^{-1} \cdot \bar{S}_{i_1, i_2, \dots, i_t}$, here $\bar{S}_{i_1, i_2, \dots, i_t}$ denotes the column vector consisting of the shares $s_{i_1}, s_{i_2}, \dots, s_{i_t}$. Thus the secret k can be computed. Further, given any $t - 1$ rows of D , the row $[\gamma, 0, 0, \dots, 0]$ for all $\gamma \in GF(q^m) \setminus \{0\}$, will not be in the row span of $D_{i_1, i_2, \dots, i_{t-1}}$. Thus no information concerning the secret k will be revealed by $t - 1$ or less shares. Consequently, one can construct a t out of $r + 1$ threshold sharing, where $r + 1 = |\mathbb{F}|$. Thus the number of participants n can be as large as the field and so from the perspective of determining the maximal n that can be used in a t out of n threshold secret sharing scheme, we see that the Karnin-Green-Hellman secret sharing scheme is more efficient than the Shamir secret sharing scheme.

We define $n_{max,t}$ to be the largest n for which one can construct a t out of n PIL threshold sharing scheme over finite field \mathbb{F} .

In [14], Karnin, Greene and Hellman established the following.

Theorem 1 (KGH). [14] *Suppose the secret space $S = \mathbb{F} = GF(q^m)$, then $n_{max,t}$ satisfies*

$$|\mathbb{F}| \leq n_{max,t} \leq |\mathbb{F}| + t - 2, \quad q^m > t, \quad (3)$$

$$n_{max,t} = t, \quad q^m \leq t, \quad (4)$$

The proof of this result is provided in [14]. The lower bound given in (3) is established by using the sharing scheme constructed by Karnin, Greene and Hellman. The upper bound can be understood by applying the following representation described by Karnin, Green and Hellman in [14], which we define as the *KGH normal form*.

Definition 3. *Let D be the distribution matrix of a t out of n PIL threshold sharing scheme over finite field \mathbb{F} . Then D is in KGH normal form provided that the distribution matrix D satisfies the following equation*

$$D = \begin{bmatrix} 1 & x_{12} & x_{13} & \cdots & x_{1t} \\ 1 & x_{22} & x_{23} & \cdots & x_{2t} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{r2} & x_{r3} & \cdots & x_{rt} \\ 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}. \quad (5)$$

Recall that the shares are computed via the matrix equation $\bar{s} = D \cdot \bar{y}$, where $\bar{y}^T = [k, a_1, \dots, a_t]$. Observe that the first column of the matrix D given in (5) represents the use of the secret key k .

Lemma 1 (KGH). [14] *For every t out of n PIL threshold sharing scheme over a finite field, one can always express the distribution matrix D in KGH normal form (as illustrated in equation (5)).*

Lemma 1 and its proof are provided in [14, proof of Theorem 4, p. 39].

There exists a great similarity between linear codes and threshold secret sharing schemes.

Definition 4. [17, 20] A linear code of length n and rank k is a linear subspace with dimension k of the vector space \mathbb{F}_q^n where \mathbb{F}_q is the finite field with q elements. The linear code of length n and rank k is often denoted as a $[n, k, d]$ linear code, where d is the minimum distance between codes.

As noted above, there is a similarity between linear codes and the completeness property of a t out of n linear threshold sharing schemes. The threshold t in a t out of n threshold sharing scheme corresponds to the k of a $[n, k, d]$ linear code, and the distribution matrix D corresponds to the transpose of the generator matrix of the linear code. The difference between threshold sharing scheme and a linear code is that the privacy condition is also a necessary requirement for a t out of n PIL threshold sharing schemes.

Example 1. Consider a $[3, 2, 2]$ linear code with generator matrix G , given by:

$$G = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

Consider the matrix G^T , and interpret it as a distribution matrix of a 2 out of 3 threshold secret sharing scheme. Clearly it would satisfy the completeness property, since any two rows would contain the row span $[1, 0]$. However it violates the privacy condition since one row would generate $[1, 0]$.

3 Some preliminary results

Consider the distribution matrix D written in KGH normal form, as described in (5). Then D can be represented as

$$D = \begin{bmatrix} & A \\ \hline 0_{1 \times (t-1)} & I_{(t-1) \times (t-1)} \end{bmatrix} = \begin{bmatrix} 1 & x_{12} & x_{13} & \cdots & x_{1t} \\ 1 & x_{22} & x_{23} & \cdots & x_{2t} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{r2} & x_{r3} & \cdots & x_{rt} \\ \hline 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix} \quad (6)$$

where A is a $(r+1) \times t$ matrix (here $r = n - t$), $0_{1 \times (t-1)}$ is the column matrix consisting of zeros, and $I_{(t-1) \times (t-1)}$ is the $(t-1) \times (t-1)$ identity matrix.

A necessary and sufficient condition for a t out of n PIL threshold sharing scheme is the following.

Lemma 2 (KGH). [14] Let D be a matrix in KGH normal form (6), then D is the distribution matrix of a t out of n PIL threshold scheme if and only if every $j \times j$ minor of A (for $j = 1, \dots, \min(t, n - t + 1)$) is nonzero.

The proof is provided in [14, proof of Theorem 4, p. 39].

The dual of a t out of n threshold scheme is a $n - t + 1$ out of n threshold scheme. The dual has been studied extensively in literature, for more information on the dual see [10]. It is straightforward to go from a t out of n threshold scheme and construct its dual, with the same number of players. In [10], Cramer and Fehr provided the algebraic conditions for constructing the dual of a t out of n threshold scheme which is defined over a ring (such conditions would of course have to be satisfied for a dual over a field). The distribution matrix of the dual is related to the reconstruction matrix. That is, a series of matrix operations including a transpose of the reconstruction matrix will provide the distribution matrix of the dual.

Thus if $v = n_{max,t} - t + 1$ then there exists a v out of $n_{max,t}$ PIL threshold scheme. Therefore $n_{max,v} \geq n_{max,t}$.

We now discuss a result concerning the properties of a distribution matrix written in KGH form.

Lemma 3. Let D be a matrix in KGH normal form. If D is a distribution matrix of a t out of n threshold scheme the following must be true.

(1) for all i, j , with $1 \leq i \leq r$ and $2 \leq j \leq t$, the i, j entry of A satisfies $x_{i,j} \neq 0$ and $x_{ij} \neq 1$.

(2) for $i, v \in \{1, \dots, r\}$, $i \neq v$, and for each $j = 2, \dots, t$, we have $x_{ij} \neq x_{vj}$.

(3) for $j, l \in \{2, \dots, t\}$, $j \neq l$. and for each $i = 1, \dots, r$, we have $x_{ij} \neq x_{il}$, and

(4) for $i, v \in \{1, \dots, r\}$, $i \neq v$, and for $j, l \in \{1, \dots, t\}$, $j \neq l$, the field elements $\frac{x_{vj}}{x_{vl}} \neq \frac{x_{ij}}{x_{il}}$.

Proof. In [14] Karnin, Greene and Hellman established that every $j \times j$ minor of A is nonzero. The proof of Lemma 3 is established by considering various 1×1 and 2×2 minors of A .

For example to establish that every $x_{i,j}$ is nonzero, consider a 1×1 minor of A . To establish that $x_{i,j}$ does not equal 1, consider a 2×2 minor consisting of the i^{th} row, the $r + 1^{st}$ row, the 1^{st} column and the j^{th} column of D . The resulting minor $\begin{vmatrix} 1 & x_{i,j} \\ 1 & 1 \end{vmatrix} \neq 0$, which implies $x_{i,j} \neq 1$. The remaining cases (2), (3), and (4) of Lemma 3 can be established in a similar manner.

Theorem 2. Let \mathbb{F} be a finite field and let $t \geq 2$, then

(1) $n_{max,t} \leq 1 + n_{max,t-1}$, and

(2) for positive integer θ and $t \geq \theta + 1$, $n_{max,t} \leq \theta + n_{max,t-\theta}$.

Proof. To prove (1) let D represent a distribution matrix written in KGH form for a t out of $n_{max,t}$ PIL threshold secret sharing scheme over field \mathbb{F} . Let \tilde{D} represents the matrix formed by removing the t^{th} column of D and the last row of

D . The last row of D is of the form $[0, 0, \dots, 0, 1]$. Thus \tilde{D} is a $(n_{max,t}-1) \times (t-1)$ matrix. Therefore, it is trivial that any $t-1$ rows of \tilde{D} contain the row $[1, 0, \dots, 0]$ in its row span. Further it is trivial that any $t-2$ or less rows of \tilde{D} do not contain $[\gamma, 0, 0, \dots, 0]$ with $\gamma \neq 0$, in its row span. Thus \tilde{D} is a $t-1$ out of $n_{max,t}-1$ threshold scheme. Hence $n_{max,t-1} \geq n_{max,t}-1$.

The proof of (2) follows from (1), by applying it θ many times.

Note: the Karnin-Green-Hellman [14] bounds (see Theorem 1) are tight for $t = 2$, so we focus on $t > 2$.

4 An $n_{max,t}$ optimal scheme for $GF(2^m)$ when $t = 3$

We now construct a 3 out of n PIL threshold sharing scheme over the field $GF(2^m)$ for which $n = n_{max,3}$. Important tools in our construction will be the KGH normal form and the Vandermonde matrix.

Theorem 3. *Let $\mathbb{F} = GF(2^m)$ be a finite field and let $n = |\mathbb{F}| + 1$, then there exists a secure 3 out of n PIL threshold sharing scheme over \mathbb{F} .*

Proof. Since the characteristic of $\mathbb{F} = GF(2^m)$ is 2, all nonzero nontrivial elements (elements not equal to 0 or 1) of \mathbb{F} have (multiplicative) order⁴ greater than 2. Let $x_1, x_2, \dots, x_{|\mathbb{F}|-2}$ denote the distinct elements of \mathbb{F} not equal to 0 or 1. Consider the following matrix

$$D = \begin{bmatrix} 1 & x_1 & x_1^2 \\ \vdots & \vdots & \vdots \\ 1 & x_{|\mathbb{F}|-2} & x_{|\mathbb{F}|-2}^2 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (7)$$

Thus D is a $(|\mathbb{F}| + 1) \times 3$ matrix. We now establish that D is a distribution matrix of a 3 out of n PIL threshold sharing scheme.

We first consider *completeness*. We will show that any three participants can construct the secret. Label the rows of the distribution matrix (7) from 1 to n in a top-to-down manner.

case (i) Given any 3 rows from $\{1, \dots, n-2\}$, the secret can be constructed due to the invertibility of the Vandermonde matrix.

case (ii) Suppose we are given the row $[0,1,0]$ and the row $[0,0,1]$ and one additional row selected from $\{1, \dots, n-2\}$ then it is trivial that one can construct the secret.

case (iii) Suppose one of the rows belongs to $\{[0, 1, 0], [0, 0, 1]\}$ and the two other rows selected from rows $\{1, \dots, n-2\}$. Then reduce the system by using row operations utilizing the row from the set $\{[0, 1, 0], [0, 0, 1]\}$. The resulting system is a 2 by 2 Vandermonde system and hence invertible.

⁴ The order of an element $a \in \mathbb{F}^*$ is the smallest positive integer e such that $a^e = 1$.

So the completeness property is established. The proof for *privacy* follows in a very similar manner.

Thus for all fields \mathbb{F} of characteristic 2, we have $n_{max,3} = |\mathbb{F}| + 1 = |\mathbb{F}| + 3 - 2 = |\mathbb{F}| + t - 2$. Consequently for fields of characteristic 2, we find that the Karmin, Greene, and Hellman upper bound given in equation (3) for $n_{max,3}$ is tight.

Recall the *dual* of a t out of n threshold scheme is a $n - t + 1$ out of n threshold scheme. Suppose D is the distribution matrix of a t out of $n_{max,t}$ scheme. Then $Dual(D)$ is a distribution matrix for a $n_{max,t} - t + 1$ out of $n_{max,t}$ scheme. Thus if we let $v = n_{max,t} - t + 1$, then $Dual(D)$ is the distribution matrix of a v out of $n_{max,t}$ scheme. Hence $n_{max,v} \geq n_{max,t}$. Consequently we have $n_{max,|\mathbb{F}|-2} \geq |\mathbb{F}| + 1$ (since $|\mathbb{F}| - 2 = n_{max,3} - 3 + 1$. It is trivial to show that $n_{max,|\mathbb{F}|-2} \leq |\mathbb{F}| + 1$ Therefore we have:

Corollary 1. *Let \mathbb{F} be a field of characteristic 2, and consider a $|\mathbb{F}| - 2$ out of n PIL threshold sharing scheme, then $n_{max,|\mathbb{F}|-2} \geq |\mathbb{F}| + 1$.*

5 Bounds of $n_{max,t}$ for fields of odd characteristic when $t = 3$

The construction of a 3 out of $|\mathbb{F}| + 1$ PIL threshold sharing scheme (where characteristic of \mathbb{F} is even) is such that the upper $|\mathbb{F}| - 2$ rows of the distribution matrix D (what we denoted earlier as matrix A) is a Vandermonde matrix. This construction does not violate Lemma 3 because no element of \mathbb{F} has order 2. In a finite field with odd characteristic, we are guaranteed to have the element -1 (the additive inverse of 1) and $-1 \neq 1$ (a condition that is false in fields of characteristic 2). Thus attempting to utilize this construction for 3 out of $|\mathbb{F}| + 1$ scheme, would violate Lemma 3. This observation does not imply anything about $n_{max,3}$ for a field of odd characteristic. However the following result establishes the precise value for $n_{max,3}$.

Theorem 4. *Consider a field $\mathbb{F} = GF(p^m)$, where p is prime with $p > 2$, and consider all 3 out of n PIL threshold sharing schemes, then $n \leq |\mathbb{F}|$. Thus we have that $n_{max,3} = |\mathbb{F}|$.*

Proof. Without loss of generality assume that $\mathbb{F} = \mathbb{Z}_p$ for p prime > 2 . The proof for the case where $\mathbb{F} = GF(p^m)$ with $m > 1$ follows in a similar manner.

By Theorem 1, $n_{max,3}$ satisfies that $|\mathbb{F}| \leq n_{max,3} \leq |\mathbb{F}| + 3 - 2 = |\mathbb{F}| + 1$. So we are left to show that $n_{max,3} < |\mathbb{F}| + 1$. Suppose $n_{max,3} = |\mathbb{F}| + 1$. If $n_{max,3} = |\mathbb{F}| + 1$ where $t = 3$, then r as described in the equation (5) satisfies $r = |\mathbb{F}| + 1 - 3 = |\mathbb{F}| - 2$. Note that $|\mathbb{F}| - 2$ is the number of elements of \mathbb{F} that are not equal to 0 or 1. By Lemma 3 the $(i, 1)$ entry x_{i1} of A is unique and is not equal to 0 or 1, for $i = 1, \dots, r$. Then the set of x_{i1} , for $i = 1, \dots, r$, represents the $|\mathbb{F}| - 2$ elements not equal to 0 or 1. Similarly the set of x_{i2} , for $i = 1, \dots, r$, represents the $|\mathbb{F}| - 2$ elements not equal to 0 or 1 and the set of $\frac{x_{i2}}{x_{i1}}$, for $i = 1, \dots, r$, represents the $|\mathbb{F}| - 2$ elements not equal to 0 or 1. By Wilson's Theorem [4], the product all the nonzero elements of \mathbb{Z}_p reduced modulo p will equal -1 .

Therefore the product of all the elements x_{i1} satisfies $\prod_{i=1}^r x_{i1} = -1 \pmod{p}$. Similarly both $\prod_{i=1}^r x_{i2} = -1 \pmod{p}$ and $\prod_{i=1}^r \frac{x_{i2}}{x_{i1}} = -1 \pmod{p}$.

Then

$$\prod_{i=1}^r \frac{x_{i2}}{x_{i1}} = -1 = \left(\prod_{i=1}^r x_{i1}\right) / \left(\prod_{i=1}^r x_{i2}\right) = (-1) / (-1) = 1$$

Therefore we have a contradiction and so $n_{max,3} \neq |\mathbb{F}| + 1$. Hence $n_{max,3} = |\mathbb{F}|$ when $\mathbb{F} = \mathbb{Z}_p$. The proof will be valid for all fields $\mathbb{F} = GF(p^m)$ where p prime and $p > 2$.

Thus $n_{max,3} = |\mathbb{F}|$ for fields of odd characteristic. Consequently, for 3 out of n PIL threshold sharing schemes, the characteristic of the field does affect the maximal number of participants that can participate in the threshold scheme.

Corollary 2. *The optimal scheme with $n = n_{max,t}$ for fields of odd characteristic when $t = 3$ is given by the Karnin, Greene and Hellman secret sharing scheme.*

Because we have reduced the bound for $n_{max,3}$ to $|\mathbb{F}|$ and since $1 + n_{max,t-1} \geq n_{max,t}$, we see that $n_{max,4} \leq |\mathbb{F}| + 1 = |\mathbb{F}| + 4 - 3 < |\mathbb{F}| + 4 - 2$ (the latter is the KGH upper bound). We can continue this process. For example $n_{max,5} \leq 1 + n_{max,4} \leq 2 + n_{max,3}$. We then have the following bound.

Corollary 3. *Suppose \mathbb{F} is a finite field of odd characteristic, then $n_{max,t} \leq |\mathbb{F}| + t - 3$.*

The bound is an improvement of the upper bound given Theorem 1 (as derived in [14]). Thus we have demonstrated an improved upper bound for $n_{max,t}$ for fields of odd characteristic when $t \geq 3$.

6 Implications of $n_{max,t}$ for $t \geq 4$

Recall that the nonzero elements of \mathbb{F} form a multiplicative cyclic group. Let α be a primitive element then for all $x \in \mathbb{F} \setminus \{0\}$ there exists an i such that $x = \alpha^i$.

We can then apply the fact that the multiplicative group of \mathbb{F} is cyclic, since the matrix A (submatrix of D) consists of nonzero elements they can each be expressed as α to a power. Further all elements in each row of A are distinct and all elements in each column j of A ($j = 2, \dots, t$) are distinct. We can interpret each power (the discrete log with respect to α) as a function of the row number i and that the column number j determines a permutation of the possible powers $\{1, \dots, |\mathbb{F}| - 2\}$, i.e. we can view it as $\pi_i(j)$. That is, the condition $x_{ij} \neq x_{il}$ (where neither is 0 or 1) can be interpreted as $\alpha^{\pi_j(i)} \neq \alpha^{\pi_l(i)}$ and that $\pi_j(i) \neq \pi_l(i)$

As a motivating example, consider the distribution matrix D of a 4 out of n PIL threshold sharing scheme. Then

$$D = \begin{bmatrix} 1 & x_{12} & x_{13} & x_{14} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & x_{r2} & x_{r3} & x_{r4} \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & \alpha^{\pi_2(1)} & \alpha^{\pi_3(1)} & \alpha^{\pi_4(1)} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{\pi_2(r)} & \alpha^{\pi_3(r)} & \alpha^{\pi_4(r)} \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (8)$$

Here π_w is a permutation of the set $\{1, 2, \dots, |\mathbb{F}| - 2\}$ and $\pi_w(i)$ is the i^{th} term of this function. Note we are only interested in the first $n - t$ terms of the function π_w (we view a function on $|\mathbb{F}| - 2$ terms as an $(|\mathbb{F}| - 2)$ -tuple).

We can then generalize equation (8) to any t out of n threshold scheme and then generalize Lemma 3 as follows.

Theorem 5. *Let D be a matrix in KGH normal form. If D is a distribution matrix of a t out of n threshold scheme for each of the columns $w = 2, \dots, t$ there exists a permutation π_w of the set $\{1, 2, \dots, |\mathbb{F}| - 2\}$ such that for $i = 1, \dots, n - t$ the (i, w) entry of D is $\alpha^{\pi_w(i)}$. Then each of the following must be true.*

- (1) for all $i \in \{1, \dots, n - t\}$ and $w \in \{2, \dots, t\}$, the discrete log of the i, w entry of A satisfies $\pi_w(i) \neq 0$,
- (2) for $j, l \in \{2, \dots, t\}$, with $j \neq l$ and for each row $i \in \{1, \dots, n - t\}$, we have $\pi_j(i) \neq \pi_l(i)$,
- (3) for $i, v \in \{1, \dots, n - t\}$, with $i \neq v$, and for $j, l \in \{2, \dots, t\}$, with $j \neq l$, we have $\pi_j(i) - \pi_l(i) \neq \pi_j(v) - \pi_l(v)$, and
- (4) $\pi_w^{-1} \circ \pi_j$ is a derangement on the first $n - t$ elements of the function $\pi_w^{-1} \circ \pi_j$.

Here a *derangement* π is a permutation on the set $\{1, \dots, T\}$ such that $\pi(i) \neq i$ for all i , we require derangement condition (4) to be satisfied on only the first $n - t$ elements of π .

The proof of Theorem 5 follows immediately from Lemma 2.

7 Unifying threshold sharing schemes with MDS codes

We now describe the relationship between the maximum $n_{max,t}$ for t out of n PIL threshold sharing schemes and $n_{MDS,max,t}$ MDS codes. Bounds on the maximal number of participants in a perfect ideal linear t out of n threshold sharing scheme and bounds on maximal size of MDS codes are very similar, where the former appears to be one less than the latter. In Theorem 6 we prove that this is true. First we introduce some terminology.

Recall the definition of a $[n, k, d]$ linear code. The Singleton Bound gives

$$d \leq n - k + 1. \quad (9)$$

A $[n, k, d]$ linear code is called a *maximum distance separable (MDS) code* if $d = n - k + 1$ [17, 20].

We now introduce some combinatorial constructions of MDS codes.

Some Combinatorial Constructions of MDS codes

An n -arc is a set of points in the projective geometry $\text{PG}(k-1, q)$ such that no k points lie in a hyperplane $\text{PG}(k-2, q)$, where $3 \leq k \leq n$. An $[n, k]$ MDS code over field \mathbb{F}_q exists iff there exists an n -arc in $\text{PG}(k-1, q)$.

Also, an $[n, k]$ MDS code over field \mathbb{F}_q exists iff the rows of a (q^k, n, q, k) linear orthogonal array of index unity and symbols from \mathbb{F}_q exists.

We now define $n_{MDS, max, k}$ as the maximum value of n for a $[n, k, d]$ MDS code for finite field \mathbb{F} .

Theorem 6. *For finite field \mathbb{F} , $n_{max, t} = n_{MDS, max, t} - 1$.*

We establish Theorem 6 via the following lemmas, Lemma 4 and Lemma 5. These lemmas have been established previously in [11] (other sources for similar arguments include [13, 17, 19]). We state the lemmas in a manner to fit the context of this paper and we provide the proof using our tools (KGH tools) and terminology.

Lemma 4. *Consider a $[n, k, d]$ linear MDS code C for which n is maximum and $d \geq 2$, then there exists a generator matrix G of the code C and a row R of G^T such that if D is the matrix formed by using all but the R^{th} row of G^T . Then D is a distribution matrix of a k out of $n_{max, k}$ PIL threshold sharing scheme.*

Proof. Consider

$$G^T = \begin{bmatrix} B_1 \\ B_2 \end{bmatrix}$$

where B_2 is a $k \times k$ matrix, and due to completeness invertible. Thus

$$G^T B_2^{-1} = \begin{bmatrix} B_1 \\ B_2 \end{bmatrix} B_2^{-1} = \begin{bmatrix} B_1 B_2^{-1} \\ I \end{bmatrix}$$

where I is the $k \times k$ identity matrix. Therefore we may assume without loss of generality that G^T is expressed in systematic form (i.e. the last k rows form the identity matrix). Label the columns of G^T from 1 to k and label the rows of G^T from 1 to n in a top to down fashion. Let R denote the row consisting of $[1, 0, 0, \dots, 0]$ and remove R from G^T and denote this matrix by D . Then clearly any k rows of D are invertible. Further, each $j \times j$ minor of D is nonzero. This follows from the fact that every k rows of D are invertible and that the last $k-1$ rows of D possess the form $[0, 0, \dots, 0, 1, 0, \dots, 0]$ where the 1 occurs in the ℓ columns for $\ell = 2, \dots, k$.

Thus every bound on a $[n, k, d]$ linear MDS code infers a bound on $n_{max, k}$ of a k out of n PIL threshold sharing scheme.

Lemma 5. *Let D be a distribution matrix of a k out of $n_{max, k}$ PIL threshold sharing scheme written in KGH normal form. Then by adding a row R to D , the resulting matrix is the transpose of a generator matrix for a $[n, k, d]$ MDS code.*

Proof. Since D is written in KGH normal form, it satisfies (3). We now add the row $[1, 0, \dots, 0]$ to D , denote this matrix by D' . Then

$$D' = \begin{bmatrix} 1 & x_{12} & x_{13} & \cdots & x_{1k} \\ 1 & x_{22} & x_{23} & \cdots & x_{2k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{r2} & x_{r3} & \cdots & x_{rk} \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}.$$

Now, $(D')^T$ forms a generator matrix of a $[n, k, d]$ MDS code where $n = n_{max,k} + 1$, as we now explain. We need to show that $(D')^T$ forms a $[n, k, d]$ linear code where $d = n - k + 1$. A codeword is a member of the row span of $(D')^T$. Recall that d is the minimum distance between codewords. Observe that column 1 of D' consists of $1 + n_{max,k} - (k - 1) = 1 + n_{max,k} - k + 1 = n - k + 1$ many nonzero elements. Thus $d \leq n - k + 1$. Since $[0, 0, \dots, 0]$ is a code word, and the code a linear code, we are left to show that any nontrivial linear combination of rows of $(D')^T$ consists of at least $d = n - k + 1$ nonzero elements. Now observe that $(D')^T = [A^T | I_{k \times k}]$ where A^T is a $k \times n - k$ matrix and $I_{k \times k}$ is the $k \times k$ identity matrix. Since there are only k rows of $(D')^T$, we need to show that any nontrivial linear combination of ρ many rows of $(D')^T$, contains at least $d = n - k + 1$ nonzero elements, where $\rho \leq k$. We partition the argument into two parts: if one takes a linear combination of ρ many rows from $I_{k \times k}$, then one is going to have exactly ρ many nonzero entries. Thus we are left to show that if one takes a linear combination of ρ many rows from A^T then one has at least $d - \rho$ many nonzero entries. Here $d = n - k + 1$ and there are $n - k$ many columns of A^T . We claim that any row which is a linear combination of ρ many rows of A^T contains at most $\rho - 1$ zero elements. This implies that there are at least $n - k - (\rho - 1) = n - k + 1 - \rho = d - \rho$ many nonzero elements. To prove this claim, suppose there is a linear combination ρ many rows of A^T for which there are at least ρ many zeros. Thus there is a $\rho \times \rho$ matrix formed by ρ many rows and ρ many columns of A^T for which a nontrivial linear combination of rows is $[0, 0, \dots, 0]$. This implies that there is a $\rho \times \rho$ minor of A^T which is zero. However, this contradicts a result noted in the proof of Lemma 3, that every $j \times j$ minor of A is nonzero. Hence there are at most $\rho - 1$ many zero elements of the linear combination of ρ many rows of A^T and so there are at least $d - \rho$ many nonzero elements. Consequently $(D')^T$ is a generator matrix of a MDS $[n, k, d]$ code.

Therefore bounds on $n_{max,k}$ of a k out of n PIL threshold sharing scheme infers bounds on $[n, k, d]$ linear MDS code.

The proof of Theorem 6 follows from the above Lemmas.

Thus we see that bounds concerning $n_{max,t}$ for t out of n PIL threshold sharing schemes directly impact bounds on linear MDS codes and vice versa.

There are several open problems concerning bounds on MDS codes. It is possible that the problem concerning constructing bounds for $n_{max,t}$ may be easier than problems concerning constructing bounds on MDS codes (since there are more constraints to this problem, i.e. both “completeness” and “privacy” must be satisfied for threshold sharing schemes). Thus any improvements in bounds concerning $n_{max,t}$ will directly impact bounds concerning linear MDS codes.

Some known results concerning MDS Codes The following is some results that are known concerning the maximal size of MDS codes for finite fields. Our work, which was derived using KGH tools, agree with the known results. If we let $n_{MDS,max,k}$ denote the maximum value of n for a $[n, k, d]$ MDS code for finite field \mathbb{F}_q , then by [11, 20]

$$n_{MDS,max,k} = \begin{cases} q + 1 & \text{when } k = 2 \\ q + 1 & \text{when } k = 3 \text{ or } k = q - 1 \text{ and } q \text{ odd} \\ q + 2 & \text{when } k = 3 \text{ and } q \text{ is even} \\ k + 1 & \text{when } k \geq q \end{cases}$$

For $k \geq q$ it is known that $n_{MDS,max,k} = k + 1$. The *well-known MDS conjecture* states that for $2 \leq k < q$,

$$n_{MDS,max,k} = \begin{cases} q + 2, & q \text{ even and } k = 3 \text{ or } k = q - 1, \\ q + 1, & \text{otherwise.} \end{cases}$$

This conjecture has been proved for small values of k (for example for $k \leq 5$), it has also been established for small values of q (for $q \leq 27$) and has been established for some other cases, see [11].

The following upper bounds for $n_{MDS,max,k}$ have been proved by Bush [5]. For $2 \leq k < q$,

$$n_{MDS,max,k} \leq \begin{cases} q + k - 2, & k \geq 3 \text{ and } q \text{ odd,} \\ q + k - 1, & \text{otherwise,} \end{cases}$$

These general upper bounds have been improved slightly according to [23] where it states that $q + k - 3$ is an upper bound in the case $k \geq 4$ and q even. They refer to [15].

As noted there exists a relationship between MDS codes and k -arcs in projective geometry. Thus there exists a relationship exists between linear threshold schemes and k -arcs in projective geometry. There is also a relationship between linear threshold schemes and orthogonal arrays. In [6], Dawson et. al. established several results concerning orthogonal arrays and threshold schemes, in particular that all linear threshold schemes are equivalent to orthogonal arrays.

8 Conclusion

We have discussed several bounds on the maximal number of players, $n_{max,t}$, in t out of n threshold schemes over a finite field. We have derived these bounds

using the same tools that Karnin, Greene and Hellman described in their original paper. We have formalized the notation for this problem and derived several results. We have also unified this problem to a problem in coding theory, namely linear MDS codes and have noted that improvements in constructing bounds on $n_{max,t}$ directly impact bounds concerning MDS codes.

References

1. G. R. Blakley, "Safeguarding cryptographic keys", Proceedings of the National Computer Conference, 1979, *American Federation of Information Processing Societies Proceedings* 48 (1979), pp. 313-317.
2. E. F. Brickell and D. M. Davenport, "On the classification of ideal secret sharing schemes", *J. Cryptology* 4 (1991), pp. 123-134.
3. E. F. Brickell and D. R. Stinson, "Some improved bounds on the information rate of perfect secret sharing schemes" *Journal of Cryptology* 1992, (5) pp. 153-166,
4. E. Bach, J. Shallit. *Algorithmic Number Theory*, Vol 1, MIT Press, Cambridge, MA, 1996
5. K. A. Bush "Orthogonal Arrays of Index Unity " *The Annals of Mathematical Statistics*, Vol. 23, No. 3 (Sep., 1952), pp. 426-434
6. E. Dawson, E. S. Mahmoodian and A. Rahilly, "Orthogonal arrays and ordered threshold schemes", *Australasian Journal of Combinatorics* 8 (1993), 27-44.
7. R.M. Capocelli, A. De Santis, L. Gargana, U. Vaccaro, "On the Size of shares for secret sharing schemes", *Journal of Cryptology*, 6:157-167, 1993.
8. C. Charnes, J. Pieprzyk, "Generalized cumulative arrays and their applications to secret sharing schemes", *Proceeding of the 18th Australasian Computer Science Conference, Australasian Computer Science Communications*, Vol. 17, No. 1, pp. 61-65, 1995.
9. R. Cramer, S. Fehr, M. Stam, "Primitive Sets over Number Fields and Black-Box Secret Sharing". *Proceedings of 25th Annual IACR CRYPTO 2005*, Springer Verlag LNCS, vol. 3621, pp. 344-360, August 2005.
10. R. Cramer and S. Fehr, "Optimal Black-Box Secret Sharing over Arbitrary Abelian Groups". *Proceedings of 22nd Annual IACR CRYPTO 2002*, Springer Verlag LNCS, vol. 2442, pp. 272-287, August 2002.
11. J.W.P. Hirschfeld and L. Storme. The packing problem in statistics, coding theory and finite projective spaces: update 2001. In A. Blokhuis, J.W.P. Hirschfeld, D. Jungnickel, and J.A. Thas, editors, *Finite Geometries: Proceedings of the Fourth Isle of Thorns Conference (Chelwood Gate, July 16-21, 2000)*, volume 3 of *Developments in Mathematics*, pages 201-246. Kluwer Academic Publishers, 2001.
12. M. Ito and A. Saito and T. Nishizeki "Secret sharing schemes realizing general access structures" *Proc. IEEE Global Telecommunications Conf., Globecom'87* 1987, IEEE Communications Soc. Press, pp.99-102
13. W. Jackson, K. Martin and C. O'Keefe, "Geometrical contributions to secret sharing theory", *Journal of Geometry*, 79 (2004), pp. 102-133.
14. E. D. Karnin, J. W. Greene and M. E. Hellman, "On secret sharing systems", *IEEE Transactions on Information Theory* 29 (1983), pp. 35-41.
15. S. Kounias and C. I. Petros. "Orthogonal arrays of strength three and four with index unity". *Sankhya: The Indian Journal of Statistics* 37:228-240, 1975. "
16. R. J. McEliece and D. V. Sarwate, "On Sharing Secrets and Reed-Solomon Codes", *Comm. ACM*, 1981, 24 (9), pp. 583-584.
17. F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1977.

18. J. Pieprzyk, T. Hardjono, and J. Seberry. *Fundamentals of Computer Security* Springer-Verlag, NY 2003.
19. J. Pieprzyk and X. Zhang, "Characterisations of Ideal Threshold Schemes", *Journal of Discrete Mathematics and Theoretical Computer Science (DMTCS)*, Vol.6, No.2, 2004, pp.471-482,
20. R. Roth. *Introduction to Coding Theory*, Cambridge Press, NY, 2006
21. A. Shamir, "How to share a secret", *Communications of the ACM* 22 (1979), pp. 612-613.
22. D. R. Stinson. *Cryptography: Theory and Practice*. CRC, Boca Raton, 1995.
23. "Bound for OAs with Index Unity" http://mint.sbg.ac.at/desc_CBoundT0.html