Multi-Linear Secret-Sharing Schemes

Amos Beimel*, Aner Ben-Efraim*, Carles Padró, and Ilya Tyomkin

[1] Dept. of Computer Science, Ben Gurion University of the Negev, Be'er Sheva, Israel
[2] Dept. of Mathematics, Ben Gurion University of the Negev, Be'er Sheva, Israel
[3] Nanyang Technological University, Singapore
[4] Dept. of Mathematics, Ben Gurion University of the Negev, Be'er Sheva, Israel

Abstract. Multi-linear secret-sharing schemes are the most common secret-sharing schemes. In these schemes the secret is composed of some field elements and the sharing is done by applying some fixed linear mapping on the field elements of the secret and some randomly chosen field elements. If the secret contains one field element, then the scheme is called linear. The importance of multi-linear schemes is that they provide a simple non-interactive mechanism for computing shares of linear combinations of previously shared secrets. Thus, they can be easily used in cryptographic protocols.

In this work we study the power of multi-linear secret-sharing schemes. On one hand, we prove that ideal multi-linear secret-sharing schemes in which the secret is composed of p field elements are more powerful than schemes in which the secret is composed of less than p field elements (for every prime p). On the other hand, we prove super-polynomial lower bounds on the share size in multi-linear secret-sharing schemes. Previously, such lower bounds were known only for linear schemes.

Keywords: Ideal secret-sharing schemes, multi-linear matroids, Dowling geometries

1 Introduction

Consider a scenario where a user holds some secret information and wants to store it on some servers such that only some predefined sets of servers (i.e., trusted sets) can reconstruct this information. Secret-sharing schemes enable such storage, where the dealer – the user holding the secret – computes some strings, called shares, and privately gives one share to each server. In the sequence we will refer to the servers as the parties and to the collection of sets of parties that can reconstruct the secret as an access structure. Secret-sharing schemes are an important cryptographic primitive and they are used nowadays as a basic tool in many cryptographic protocols, e.g., [2, 9, 10, 12, 27, 18, 41, 34, 37].

In this work we study the most useful construction of secret-sharing schemes, namely, multi-linear secret-sharing schemes. In these schemes the secret is a

* Partially supported by ISF grants 938/09, 544/13 and by the Frankel Center for Computer Science.

sequence of elements from some finite field, and each share is a linear combination of these elements and some random elements from the field. If the secret contains exactly one element of the field, then the scheme is called linear. Linear and multi-linear secret-sharing schemes are very useful as they provide a simple non-interactive mechanism for computing shares of linear combinations of previously shared secrets.

We prove two results on the power of multi-linear secret-sharing schemes. Our first results shows advantages of multi-linear secret-sharing schemes compared to linear schemes, that is, we prove that ideal schemes in which the secret contains p elements of the field are more efficient than schemes in which the secret contains less than p field elements (for every prime p). Our second results proves super polynomial lower bounds on the size of shares in multi-linear secret-sharing schemes.

Previous Results. Threshold secret-sharing schemes, where all sets of parties whose size is at least some threshold, were introduced by Shamir [33] and Blakley [5]. Secret-sharing schemes for general access structures were introduced and constructed by Ito et al. [19]. Better constructions were introduced by Benaloh and Leichter [3]. Linear secret-sharing schemes were presented by Brickel [7] for the case that each share is one field element and by Krachmer and Wigderson [20] for the case that each share can contain more than one field element. Karchmer and Wigderson's motivation was studying a complexity model called span programs; in particular, they proved that monotone span programs are equivalent to linear secret-sharing schemes. It is important to note that all previously mentioned constructions of secret-sharing schemes are linear. Multi-linear secret-sharing schemes were studied by [4, 13], who gave the conditions when a multi-linear scheme realizes an access structure. Construction of multi-linear secret-sharing schemes were given by, e.g., [36, 6, 39, 38].

To explain why linear secret-sharing schemes are useful, we describe the basic idea in using secret-sharing schemes in protocols, starting from [2]. In such protocols the parties share their inputs among the other parties, and, thereafter, the shares of different secrets are "combined" to produce shares of some function of the original secrets. For example, the parties hold shares of two secrets a and b, and they want to compute shares of $a+b$ (without reconstructing the original secrets). If the schemes are multi-linear, the two secrets a and b are shared using the same multi-linear scheme, and each party sums the shares of the two secrets, then the resulting shares are of the secret $a+b$.

In any secret-sharing scheme, the size of the share of each party is at least the size of the secret [21]. An ideal secret-sharing scheme is a scheme in which the size of the share of each party is exactly the size of the secret. For example, Shamir's scheme [33] is ideal. Brickell [7] considered ideal schemes and constructed ideal schemes for some access structures, e.g., for hierarchical access structures. Brickell and Davenport [8] showed an interesting connection between ideal access structures and matroids, that is, (1) If an access structure is ideal then it is induced by a matroid, (2) If an access structure is induced by a representable matroid, then the access structure is ideal. Following this work, many

works have studied ideal access structures and matroids, e.g. [32, 35, 25, 24]. In particular, if an access structure is induced by a multi-linear representable matroid, then it is ideal [35].

Simonis and Ashikhmin [35] considered the access structure induced by the Non-Pappus matroid. They construct an ideal multi-linear secret-sharing scheme realizing this access structure, where the secret contains two field elements, and they prove (using known results about matroids) that there is no ideal linear secret-sharing realizing this access structure (that is, in any linear secret-sharing realizing this access structure at least one share must contain more than one field element). Pendavingh and van Zwam [29] (implicitly) provided another example of an access structure that can be realized by an ideal multi-linear secret-sharing scheme, where the secret contains two field elements, but cannot be realized by an ideal linear secret-sharing scheme. Their example is the access structure induced by the rank-3 Dowling matroid of the quaternion group. Note that the rank-3 Dowling matroid [15, 14] can be defined with an arbitrary group (see Definition 2.9); in this paper we will use it with properly chosen groups.

For a scheme to be efficient and useful, the size of the shares should be small (i.e., polynomial in the number of parties). The best known schemes for general access structures, e.g., [19, 3, 20, 13], are highly inefficient, that is, for most access structures the size of shares is $2^{O(n)}$ times the size of the secret, where n is the number of parties in the access structure. The best lower bound known on the total share size for an access structure is $\Omega(n^2/\log n)$ times the size of the secret [11]. Thus, there exists a large gap between the known upper and lower bounds. Bridging this gap is one of the most important questions in the study of secret-sharing schemes. In contrast to general secret-sharing schemes, super-polynomial lower bounds are known for linear secret-sharing schemes. That is, there exist explicit access structures such that the total share size of any linear secret-sharing scheme realizing them is $n^{\Omega(\log n)}$ times the size of the secret [1, 16, 17].

Our Results and Techniques. The simplest way to construct a multi-linear secret-sharing scheme, where the secret is composed of k field elements, is to share each field element independently using a linear secret-sharing scheme. This results in a multi-linear scheme whose information ratio (the ratio between the length of the shares and the length of the secret) is the same as the information ratio of the linear scheme. The question is if one can construct multi-linear secret-sharing schemes whose information ratio is better than linear schemes. Our first result gives a positive answer to this question. Our second result implies that in certain cases the answer is no – we show that the lower bound of [17] for linear secret-sharing schemes holds also for multi-linear secret-sharing schemes.

Our first results shows advantages of multi-linear secret-sharing schemes compared to linear schemes. For every prime $p > 2$, we show that there is an access structure such that: (1) It has an ideal multi-linear secret-sharing scheme in which the secret is composed of p field elements. (2) It does not have an ideal multi-linear secret-sharing scheme in which the secret is composed of k field elements, for every $k < p$. In other words, we prove that schemes in which the

secret is composed of p field elements are more efficient than schemes in which the secret is composed of less than p field elements. Previously, this was known only for $p = 2$.

To prove this result we consider the access structures induced by rank-3 Dowling matroids of various groups. By known results, it suffices to study when these matroids are k-linearly representable. We study this question and show that it can be answered using tools from representation theory. The important step in our proof is showing that the Dowling matroid of a group G is k-linearly representable if and only if the group G has a fixed-point free representation of dimension k (see Section 2.5 for definition of these terms). To complete our proof, we show that for every p there is a group G_p that has a fixed-point free representation of dimension p and does not have a fixed-point free representation of dimension $k < p$.

Our second results is super polynomial lower bounds on the size of shares in multi-linear secret-sharing schemes. Prior to our work, such lower bounds were known only for linear secret-sharing schemes. As proving super polynomial lower bounds for general secret-sharing schemes is a major open question, any extension of the lower bounds to a broader class of schemes is important. Specifically, as the class of multi-linear secret-sharing schemes is the class that is useful for applications, it is interesting to prove lower bounds for this class. We show that the method of Gál and Pudlák [17] for proving lower bounds for linear secret-sharing schemes applies also to multi-linear secret-sharing schemes. As a result, we get that there exist access structures such that the total share size of any *multi-linear* secret-sharing scheme realizing them is $n^{\Omega(\log n)}$ times the size of the secret (even when the secret contains any number of field elements).

2 Preliminaries

Notations. We will frequently use block matrices throughout this paper. To differentiate these block matrices, they will be inside square brackets, or in bold letters (e.g. $\mathbf{A} = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$, where A, B, C, D are matrices). In all the proofs and examples, except in the proof of Theorem 4.5, all blocks are of size $k \times k$. For a matrix A, we denote the i^{th} column of A by A_i. We denote fields by $\mathbb{F}$ or $\mathbb{E}$ (general fields), $\mathbb{C}$ (complex numbers), $\widetilde{\mathbb{F}}$ (algebraic closure of $\mathbb{F}$), and $\mathbb{F}_{p^m}$ (the unique field with p^m elements). We denote the integers by $\mathbb{Z}$ and the non-negative integers by $\mathbb{N}$.

2.1 Secret-Sharing Schemes

A secret-sharing scheme is, informally, an algorithm in which a dealer distributes a secret to a set of parties in such that only authorized subsets of parties can reconstruct the secret, while unauthorized subsets cannot learn anything about the secret. We next define secret-sharing schemes, starting with some notations.

Definition 2.1. *Let $\{p_1, \ldots, p_n\}$ be a set of parties. A collection $\mathcal{A} \subseteq 2^{\{p_1,\ldots,p_n\}}$ is* monotone *if $B \in \mathcal{A}$ and $B \subseteq C$ imply that $C \in \mathcal{A}$. An* access structure *is a monotone collection $\mathcal{A} \subseteq 2^{\{p_1,\ldots,p_n\}}$ of non-empty subsets of $\{p_1, \ldots, p_n\}$. Sets in $\mathcal{A}$ are called* authorized*, and sets not in $\mathcal{A}$ are called* unauthorized*.*

Definition 2.2 (secret-sharing). *A* secret-sharing scheme *Σ with domain of secrets S is a pair $\Sigma = \langle \Pi, \mu \rangle$, where μ is a probability distribution on some finite set R called the set of random strings and Π is a mapping from $S \times R$ to a set of n-tuples $K_1 \times K_2 \times \cdots \times K_n$, where K_j is called the* domain of shares *of p_j. A dealer distributes a secret $s \in S$ according to Σ by first sampling a random string $r \in R$ according to μ, and applying the mapping Π on s and r, that is, computing a vector of* shares *$\Pi(s, r) = (s_1, \ldots, s_n)$, and privately communicating each share s_j to party p_j. For a set $A \subseteq \{p_1, \ldots, p_n\}$, we denote $\Pi_A(s, r)$ as the restriction of $\Pi(s, r)$ to its A-entries.*

Correctness. *The secret s can be reconstructed by any authorized set of parties. That is, for any set $B \in \mathcal{A}$ (where $B = \{p_{i_1}, \ldots, p_{i_{|B|}}\}$), there exists a* reconstruction function *$\textsc{Recon}_B : K_{i_1} \times \ldots \times K_{i_{|B|}} \to S$ such that for every $s \in S$,*

$$\Pr[\, \textsc{Recon}_B(\Pi_B(s, r)) = s \,] = 1. \tag{1}$$

Perfect Privacy. *Every unauthorized set cannot learn anything about the secret (in the information theoretic sense) from their shares. Formally, for any set $T \notin \mathcal{A}$, for every two secrets $a, b \in S$, and for every possible vector of shares $\langle s_j \rangle_{p_j \in T}$:*

$$\Pr[\, \Pi_T(a, r) = \langle s_j \rangle_{p_j \in T} \,] = \Pr[\, \Pi_T(b, r) = \langle s_j \rangle_{p_j \in T} \,]. \tag{2}$$

The *information ratio* of a secret-sharing scheme is $\frac{\max_{1 \le j \le n} \log |K_j|}{\log |S|}$, where S is the domain of secrets and K_j is the domain of shares of p_j.

In every secret-sharing scheme, the information ratio is at least 1 [21]. Ideal secret-sharing schemes are those where the information ratio is exactly 1, which means that the size of the domain of the shares is exactly the size of the domain of the secret.

Multi-linear secret-sharing schemes are schemes in which the computation of the shares is a linear mapping. More formally, in a multi-linear secret-sharing scheme over a finite field $\mathbb{F}$, the secret is a vector of elements of the field. To share a secret $s \in \mathbb{F}^k$, the dealer first chooses a random vector $r \in \mathbb{F}^m$ with uniform distribution (for some integer m). Each share is a vector over the field such that each coordinate of this vector is some fixed linear combination of the coordinates of the secret s and the coordinates of the random string r.

2.2 Matroids

Matroids are combinatorial objects that can be defined in many equivalent ways. To make things simple, we will stick to one definition based on rank function.

Definition 2.3. *A matroid M is an ordered pair (E, r) with E a finite set (usually $E = \{1, ..., n\}$) called the ground set and a rank function $r\colon 2^E \to \mathbb{N}$ satisfying the following conditions, called the matroid axioms:*

1. $r(\emptyset) = 0$,
2. *If $X \subseteq E$ and $x \in E$, then $r(X) \leq r(X \cup \{x\}) \leq r(X) + 1$,*
3. *If $X \subseteq E$ and $x, y \in E$ such that $r(X \cup \{x\}) = r(X \cup \{y\}) = r(X)$ then $r(X \cup \{x\} \cup \{y\}) = r(X)$.*

A set $X \subseteq E$ is independent *if $r(X) = |X|$, otherwise X is* dependent. *The rank of the matroid is defined $r(M) := r(E)$. A* base *of M is an independent set $X \subseteq E$ such that $r(X) = r(M)$. The set of bases of a matroid uniquely identifies the matroid. A* circuit *is a minimal dependent set. The set of all circuits of a matroid also uniquely identifies the matroid. Throughout this paper we will assume that every set $X \subseteq E$ of size 2 is independent (called* simple matroids *or* geometries *in the literature).*

The simplest example of a matroid is the size of a group, i.e., let $E = \{1, ..., n\}$ and $r(X) = |X|$. The 3 axioms are trivially verified. In this matroid, all sets are independent. Matroids originated from trying to generalize axioms in graph theory and linear algebra.

Example 2.4. Let $E = \{v_1, ..., v_n\}$ be a set of vectors over some field $\mathbb{F}$. For $X \subseteq E$ let $r(X) = \dim(\text{span}(X))$. By linear algebra, the 3 matroid axioms hold. Furthermore, we can look at the matrix A, in which the i^{th} column is the vector v_i. In this case, $r(X)$ is the rank of the submatrix containing the columns of the vectors in X. Matroids that arise in this manner are called linearly representable (over $\mathbb{F}$). This can also be generalized as follows:

Definition 2.5. *Let $M = (E = \{1, ..., n\}, r)$ be a matroid and $\mathbb{F}$ a field. A k-*linear representation *of M over $\mathbb{F}$ is a matrix A with $k \cdot n$ columns $A_1, ..., A_{k \cdot n}$ such that the rank of every set $X = \{i_1, ..., i_j\} \subseteq E$ satisfies*

$$r(X) = \frac{\dim(\text{span}(U_{i_1} \cup \cdots \cup U_{i_j}))}{k},$$

*where $U_\ell = \{A_{(\ell-1)\cdot k+1}, A_{(\ell-1)\cdot k+2}, ..., A_{\ell \cdot k}\}$ for $1 \leq \ell \leq n$. If such a representation of M exists then M is k-*linearly representable. *One-linearly represetable matroids are called* linearly representable. *A matroid is* multi-linearly representable *if it is k-linearly representable for some $k \in \mathbb{N}$.*

An example of a multi-linear representation is given in Example 2.6.

Matroids of rank 3 can be expressed by a geometric representation on a plane as follows – the bases are the sets of 3 points that are not on a single line. For a diagram on the plane to represent a matroid it must satisfy the following condition: Every 2 distinct points lie on a single line. Since every 2 points lie on a line, usually only lines that pass through at least 3 points are drawn. See [28, Chapter 1.5] for more details and the more general statement.

Example 2.6. Let A and $\mathbf{B}$ be the following matrix and block matrix:

$$A = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & g_1' & g_1'' & g_1''' \end{matrix} \\ \begin{pmatrix} 1 & 0 & 0 & -1 & 0 & 1 \\ 0 & 1 & 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 & 1 & -1 \end{pmatrix} \end{array}, \mathbf{B} = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & g_1' & g_1'' & g_1''' \end{matrix} \\ \begin{bmatrix} I_k & 0 & 0 & -I_k & 0 & I_k \\ 0 & I_k & 0 & I_k & -I_k & 0 \\ 0 & 0 & I_k & 0 & I_k & -I_k \end{bmatrix} \end{array}.$$

For any field $\mathbb{F}$, the matrix A (resp. the block matrix $\mathbf{B}$) is a linear (k-linear) representation of the matroid with 6 points whose geometric representation is Figure 1 (a). For example, the columns labelled by $1, 2, g_1''$ are independent. Therefore, they do not lie on the same line in Figure 1 (a). On the other hand, the columns labelled by $1, 2, g_1'$ are dependent, thus, they lie on a line.

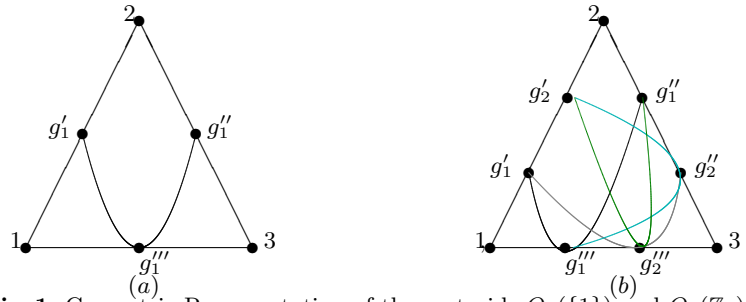


Fig. 1. Geometric Representation of the matroids $Q_3(\{1\})$ and $Q_3(\mathbb{Z}_2)$.

Definition 2.7. *Let M be a matroid and $\mathbb{F}$ a field. We say that that M is* k-minimally representable *over $\mathbb{F}$ if there is a k-linear representation of M over $\mathbb{F}$, but for every $j < k$ there is no j-linear representation of M over $\mathbb{F}$. We will say that M is k-minimally representable if it is k-minimally representable over some field $\mathbb{F}$, but not j-linearly representable over any field for $j < k$.*

Example 2.8. The Non-Pappus matroid (cf. [28, Example 1.5.15, page 39]) whose geometric representation appears in Figure 2 is not linearly representable over any field [28, Proposition 6.1.10], but has a 2-linear representation over $\mathbb{F}_3$ [35]. Therefore, the Non-Pappus matroid is 2-minimally representable.

Our primary focus in the first part of the paper will be the multi-linear representability of the rank-3 Dowling Matroids. These matroids were presented by Dowling [15, 14]. We will show that for every prime p there is a Dowling Matroid which is p-minimally representable, and furthermore, over a relatively small field. The Dowling Matroid is defined as follows:

Definition 2.9. *Let $G = \{1_G = g_1, g_2, \ldots, g_n\}$ be a finite group. The rank-3 Dowling Matroid of G, denoted $Q_3(G)$, is a matroid of rank 3 on the set $E = \{1, 2, 3, g_1', \ldots, g_n', g_1'', \ldots, g_n'', g_1''', \ldots, g_n'''\}$. That is, for every element $g_i \in G$, there are 3 elements in the ground set of the matroid $g_i', g_i'', g_i''' \in E$ and*

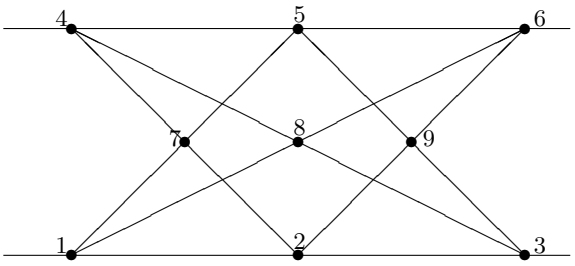
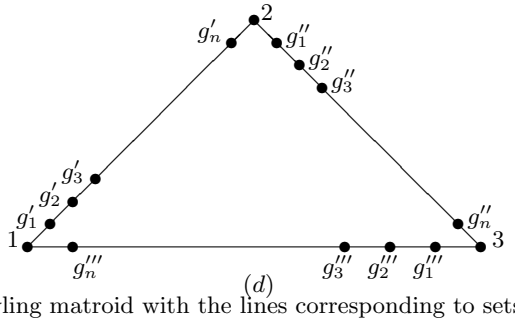


Fig. 2. The Non-Pappus matroid.

there are 3 additional ground set elements $1, 2, 3$ *not related to the group. Every subset of 3 elements not in* $C_1 \cup C_2 \cup C_3 \cup C_4$ *is a base of the matroid, where,*

$C_1 = \{\{1, 2, g_i'\} | 1 \leq i \leq n\} \cup \{\{1, g_i', g_j'\} | 1 \leq i < j \leq n\} \cup \{\{2, g_i', g_j'\} | 1 \leq i < j \leq n\},$
$C_2 = \{\{2, 3, g_i''\} | 1 \leq i \leq n\} \cup \{\{2, g_i'', g_j''\} | 1 \leq i < j \leq n\} \cup \{\{3, g_i'', g_j''\} | 1 \leq i < j \leq n\},$
$C_3 = \{\{1, 3, g_i'\} | 1 \leq i \leq n\} \cup \{\{1, g_i''', g_j'''\} | 1 \leq i < j \leq n\} \cup \{\{3, g_i''', g_j'''\} | 1 \leq i < j \leq n\},$
$C_4 = \{\{g_i', g_j'', g_\ell'''\} | g_j \cdot g_i \cdot g_\ell = 1\}.$

Alternatively, it can be defined by the geometric representation appearing in Figure 3, with additional lines that go through points g_i', g_j'', g_ℓ''' *if and only if* $g_j \cdot g_i \cdot g_\ell = 1_G$ *(e.g., there is always a line that goes through* g_1', g_1'', g_1''' *since* $g_1 = 1_G$ *and* $1_G \cdot 1_G \cdot 1_G = 1_G$*).*[5]



(*d*)

Fig. 3. The Rank-3 Dowling matroid with the lines corresponding to sets $\{g_i', g_j'', g_\ell'''\}$ such that $g_j \cdot g_i \cdot g_\ell = 1_G$ missing.

We note that the matroid in Example 2.6 is the Dowling matroid of the trivial group. Figure 1 (b) is a geometric representation of the Dowling matroid of the group $\mathbb{Z}_2$, the unique group with 2 elements. Dowling [15, 14] showed that $Q_3(G)$ is linearly representable over $\mathbb{F}$ if and only if G is isomorphic to a subgroup of $\mathbb{F}^*$, the group of invertible elements in $\mathbb{F}$. Our main theorem generalizes this

[5] In the literature, the matroid is sometimes defined a bit differently, e.g., a line goes through g_i', g_j'', g_ℓ''' if and only if $(g_j)^{-1} \cdot (g_i)^{-1} \cdot g_\ell = 1_G$. This is just a different naming of the ground set elements.

statement for multi-linear representability. Other forms of representability of $Q_3(G)$, namely representability over partial fields and skew partial fields, have been studied by Semple and Whittle [30] and Pendavingh and Van Zwam [29].

2.3 Ideal Secret-Sharing Schemes and Matroids

There is a strong connection between secret-sharing schemes and matroids. Every matroid with ground set $E = \{p_0, p_1, \ldots, p_n\}$ induces an access structure $\mathcal{A}$ with n parties $E' = \{p_1, \ldots, p_n\}$ by the rule $\forall A \subseteq E', A \in \mathcal{A}$ if and only if $r(A \cup \{p_0\}) = r(A)$. The access structure $\mathcal{A}$ is also known as the matroid port. In a sense, we think of p_0 as the dealer. Brickell and Davenport [8] showed that all access structures admitting ideal secret-sharing schemes are induced by matroids. However, not all access structures induced by matroids are ideal [32][25]. The class of matroids inducing ideal access structures are called secret-sharing matroids and also almost affinely representable, and discussed in [35]. Every multi-linearly representable matroid is a secret-sharing matroid. It is still open whether this inclusion is proper. There is also a strong connection between ideal multi-linear secret-sharing schemes and multi-linearly representable matroids [20, 13].

Proposition 2.10 *The class of access structures induced by multi-linearly representable matroids is exactly the access structures admitting an ideal multi-linear secret-sharing scheme.*

2.4 Basic Results in Linear Algebra and Multi-Linear Representability

In this section we give some basic results in linear algebra and matroid theory that are used in the paper. Recall that a matrix $A \in M_{n\times n}(\mathbb{F})$ is invertible if and only if it is of full rank if and only if $A\boldsymbol{v} \neq \mathbf{0}$ for every $\boldsymbol{v} \neq \mathbf{0}$. Also recall that block matrix multiplication can be carried out in block fashion, e.g., $\begin{bmatrix} A & B \\ C & D \end{bmatrix} \cdot \begin{bmatrix} E & F \\ G & H \end{bmatrix} = \begin{bmatrix} AE + BG & AF + BH \\ CE + BG & CF + DH \end{bmatrix}$, as long as the dimensions match (note that the order written is important as usually $AE \neq EA$, etc.).

Proposition 2.11 *Let A, B, C be $k \times k$ matrices then*

$$(a)\ \operatorname{rank} \begin{bmatrix} -I_k & 0 & C \\ A & -I_k & 0 \\ 0 & B & -I_k \end{bmatrix} = 2k + \operatorname{rank}(BAC - I).$$

$$(b)\ \operatorname{rank} \begin{bmatrix} -I_k & -I_k \\ A & B \\ 0 & 0 \end{bmatrix} = k + \operatorname{rank}(B - A).$$

Proof. Multiplying by invertible matrices does not change the rank of a matrix. Therefore,

$$\operatorname{rank}\begin{bmatrix} -I_k & 0 & C \\ A & -I_k & 0 \\ 0 & B & -I_k \end{bmatrix} = \operatorname{rank}\left(\begin{bmatrix} -I_k & 0 & C \\ A & -I_k & 0 \\ 0 & B & -I_k \end{bmatrix} \cdot \begin{bmatrix} I_k & 0 & C \\ 0 & I_k & A\cdot C \\ 0 & 0 & I_k \end{bmatrix}\right)$$
$$= \operatorname{rank}\begin{bmatrix} -I_k & 0 & 0 \\ A & -I_k & 0 \\ 0 & B & BAC - I_k \end{bmatrix} = 2k + \operatorname{rank}(BAC - I_k).$$

and

$$\operatorname{rank}\begin{bmatrix} -I_k & -I_k \\ A & B \\ 0 & 0 \end{bmatrix} = \operatorname{rank}\left(\begin{bmatrix} -I_k & -I_k \\ A & B \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} I_k & -I_k \\ 0 & I_k \end{bmatrix}\right)$$
$$= \operatorname{rank}\begin{bmatrix} -I_k & 0 \\ A & B - A \\ 0 & 0 \end{bmatrix} = k + \operatorname{rank}(B - A).$$

Proposition 2.12 *Let* $\mathbf{B} := \begin{bmatrix} B_{1,1} & \dots & B_{1,n} \\ \vdots & \ddots & \vdots \\ B_{m,1} & \dots & B_{m,n} \end{bmatrix}$ *be a k-linear representation of a matroid M, with $B_{i,j}$ being $k \times k$ block matrices, and let G be any invertible $k \times k$ matrix. Then:*

a) For every $1 \le i \le n$ then $\begin{bmatrix} B_{1,1} & \dots & B_{1,j}\cdot G & \dots & B_{1,n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ B_{m,1} & \dots & B_{m,j}\cdot G & \dots & B_{m,n} \end{bmatrix}$ *is a k-linear representation of M.*

b) For every $1 \le i \le m$ then $\begin{bmatrix} B_{1,1} & \dots & B_{1,n} \\ \vdots & \ddots & \vdots \\ G\cdot B_{i,1} & \dots & G\cdot B_{i,n} \\ \vdots & \ddots & \vdots \\ B_{m,1} & \dots & B_{m,n} \end{bmatrix}$ *is a k-linear representation of M.*

c) If $\{1, \dots, m\}$ is a base of M then there exists a matrix of the form $\begin{bmatrix} I_k & \dots & 0 & B'_{1,m+1} & \dots & B'_{1,n} \\ \vdots & \ddots & \vdots & \ddots & & \vdots \\ 0 & \dots & I_k & B'_{m,m+1} & \dots & B'_{m,n} \end{bmatrix}$ *that is also a k-linear representation of M.*

Proof. a) Since G is invertible, it is immediate from basic linear algebra that

$$\begin{aligned}
&\operatorname{rank}\begin{bmatrix} B_{1,i_1} & \dots & B_{1,i_\ell} & \dots & B_{1,i_s} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ B_{m,i_1} & \dots & B_{1,i_\ell} & \dots & B_{m,i_s} \end{bmatrix} \\
&= \operatorname{rank}\left(\begin{bmatrix} B_{1,i_1} & \dots & B_{1,i_\ell} & \dots & B_{1,i_s} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ B_{m,i_1} & \dots & B_{1,i_\ell} & \dots & B_{m,i_s} \end{bmatrix} \cdot \begin{bmatrix} I_k & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & G & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & I_k \end{bmatrix} \right) \\
&= \operatorname{rank}\begin{bmatrix} B_{1,i_1} & \dots & B_{1,i_\ell} \cdot G & \dots & B_{1,i_s} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ B_{m,i_1} & \dots & B_{1,i_\ell} \cdot G & \dots & B_{m,i_s} \end{bmatrix},
\end{aligned}$$

for any submatrix (with $j = i_\ell$), which is exactly what we need to prove.

b) Simillarly, for any submatrix,

$$\begin{aligned}
\operatorname{rank}\begin{bmatrix} B_{1,1} & \dots & B_{1,n} \\ \vdots & \ddots & \vdots \\ B_{i,1} & \dots & B_{i,n} \\ \vdots & \ddots & \vdots \\ B_{m,1} & \dots & B_{m,n} \end{bmatrix} &= \operatorname{rank}\left(\begin{bmatrix} I_k & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & G & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & I_k \end{bmatrix} \cdot \begin{bmatrix} B_{1,1} & \dots & B_{1,n} \\ \vdots & \ddots & \vdots \\ B_{i,1} & \dots & B_{i,n} \\ \vdots & \ddots & \vdots \\ B_{m,1} & \dots & B_{m,n} \end{bmatrix} \right) \\
&= \operatorname{rank}\begin{bmatrix} B_{1,1} & \dots & B_{1,n} \\ \vdots & \ddots & \vdots \\ G \cdot B_{i,1} & \dots & G \cdot B_{i,n} \\ \vdots & \ddots & \vdots \\ B_{m,1} & \dots & B_{m,n} \end{bmatrix}.
\end{aligned}$$

c) Since {1,...,m} is a base of M then the columns $c_1, \dots, c_{m \cdot k}$ of $\mathbf{B}$ are a basis of the column space of $\mathbf{B}$ (which is, therefore, $\mathbb{F}^{k \cdot m}$). Therefore, there is an invertible linear transformation T such that $\forall 1 \leq i \leq mk, T(c_i) = e_i$. Since T is invertible $\dim(\operatorname{span}\{T(c_{i_1}), \dots, T(c_{i_j})\}) = \dim(\operatorname{span}\{c_{i_1}, \dots, c_{i_j}\})$ for any set of columns $\{c_{i_1}, \dots, c_{i_j}\}$, which implies that by applying T to all the columns of $\mathbf{B}$ we get that

$$\begin{bmatrix} I_k & 0 & \dots & 0 & \vdots & \dots & \vdots \\ 0 & I_k & \dots & 0 & T(c_{km+1}) & \dots & T(c_{kn}) \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & I_k & \cdot & & \cdot \end{bmatrix}$$

is a k-linear representation of M

We will call operations Proposition 2.12(a) and 2.12(b) column and row *block-scaling* respectively.

2.5 Fixed-Point Free Representations

A standard tool in studying groups is representation theory. Our result relies heavily on theorems from this extensively researched field of mathematics. We will only give the necessary definitions and state the result. We then sketch the main ideas of the proof of this result. The complete proof, which requires much more representation theory, will appear in the full version.

Definition 2.13. *Let G be a finite group and $\mathbb{F}$ a field. A* representation *of G is a group homomorphism $\rho : G \to \mathrm{GL}_n(\mathbb{F})$ (the group of $n \times n$ invertible matrices). The* dimension *or* degree *of a representation is n. A representation is called* faithful *if it is injective. A representation $\rho : G \to \mathrm{GL}_n(\mathbb{F})$ is* fixed-point free *if for every $1 \neq g \in G$ the field element 1 is not an eigenvalue of $\rho(g)$, i.e., $\rho(g) \cdot v \neq v$ for every $g \neq 1$ and for every $v \neq 0$. A* fixed-point free group *is one which has a fixed-point free representation.*

We note that not all representations of a fixed-point free group G are fixed-point free, even if the representation is faithful. For example, cyclic groups are fixed-point free, but also admit non fixed-point free representations:

Example 2.14. Let $G = \mathbb{Z}_m$ be the additive group with m elements. Denote $\zeta = e^{\frac{2\pi i}{m}}$. If $\rho : G \to \mathrm{GL}_2(\mathbb{C})$ is defined by $\rho(k) = \begin{pmatrix} \zeta^k & 0 \\ 0 & 1 \end{pmatrix}$ then ρ is faithful (because $i \neq k \Rightarrow \rho(i) \neq \rho(k)$) but not fixed-point free because $\begin{pmatrix} \zeta^k & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ (and this should only happen for $k = 0$). However, if we define $\rho(k) = \begin{pmatrix} \zeta^k & 0 \\ 0 & \zeta^k \end{pmatrix}$ then ρ is fixed-point free, because if $k \neq 0$ then 1 is not an eigenvalue of $\begin{pmatrix} \zeta^k & 0 \\ 0 & \zeta^k \end{pmatrix}$. We note that the group $\mathbb{Z}_m$ also has a fixed-point free representation of dimension 1, by $\rho(k) = (e^{\frac{2k\pi i}{m}})$.

Fixed-point free groups have been completely classified by the works of Burnside and later Vincent [40] and Zassenhaus [44]. The classification can be found, for example, in [42]. For our purposes we will require only the following result, easily achieved from the classification:

Proposition 2.15 *For every prime $p > 2$, there exist a prime $q > p$ and a group G_p of order p^2q such that:*

1. *G_p has a fixed-point free representation of dimension p over the field $\mathbb{F}_{2^{pq}}$, i.e., the field of characteristic 2 with 2^{pq} elements.*
2. *The group G_p does not admit a fixed-point representation of dimension less than p over any field.*

Moreover, there exists such q with $q = O(p^{5.18})$, so the field $\mathbb{F}_{2^{pq}}$ has $2^{O(p^{6.18})}$ elements.

Our proof uses the construction of semidirect product of groups. The definition can be found in most group theory books. See for example [26]. It also requires some classical theorems from representation theory, which can be found, for example, in [31].

The complete proof of Proposition 2.15 will be given in the full version. We now sketch the main ideas of the proof.

Proof Sketch. Let $p > 2$ be a prime number. From Linnik's Theorem [22, 23], there exists a prime q such that $q = np + 1$ for some $n \in \mathbb{N}$, and q is polynomially bounded by p. The state of the art improvement, by Xylouris [43], shows that $q = O(p^{5.18})$.

From the fact that $q = np + 1$, it can be deduced that there exists a non-trivial semidirect product $G_p = \mathbb{Z}_q \rtimes \mathbb{Z}_{p^2}$, with the action of $\mathbb{Z}_p$ (we give a brief explanation of the construction of this group, and why this group works, in Appendix A). We then show, both directly and using the classification of fixed-point free groups, that the group G_p is fixed-point free, and, thus, has a fixed-point free representation.

Then, using classical theorems from representation theory, we show that a fixed-point free representation of G_p is of dimension at least p, and that there indeed exists a fixed-point free representation of dimension p. In particular, we show directly that there exists such a representation over the field $\mathbb{F}_{2^{pq}}$, which has $2^{pq} = 2^{O(p^{6.18})}$ elements.

3 Main Theorem and Result

In this section, we prove that there is an access structure that has an ideal p-linear secret-sharing scheme and does not have an ideal k-linear secret-sharing scheme for every $k < p$. As explained in Section 2.3, it suffices to prove that there is a matroid that is p-minimally representable. We prove this result for the Dowling matroid, for an appropriate group G. We next state our main theorem.

Theorem 3.1 *For a finite group G, the matroid $Q_3(G)$ is k-linearly representable over a field $\mathbb{F}$ if and only if there is a fixed-point free representation $\rho : G \to \mathrm{GL}_k(\mathbb{F})$.*

The main contribution of the theorem is the new connection between multi-linear representation of the Dowling matroid over G to the existence of a fixed-point free representation of the group G. The theorem transfers the problem of multi-linear representablity of $Q_3(G)$ to finding fixed-point free representations of G. Since fixed-point free groups and representations have been completely classified, it gives a complete answer to this problem.

To discuss the representations of $Q_3(G)$, we define the following block matrix $\mathbf{A}_\rho$. In Lemma 3.2, we will prove that if $Q_3(G)$ is multi-linearly representable,

then $\mathbf{A}_\rho$ is a multi-linear representation of $Q_3(G)$ for some representation ρ of G. Then we prove in Lemmas 3.3 and 3.4 that $\mathbf{A}_\rho$ represents $Q_3(G)$ if and only if ρ is fixed-point free.

For a finite group $G = \{1 = g_1, g_2, \ldots, g_n\}$, a field $\mathbb{F}$, and a faithful representation $\rho : G \to \mathrm{GL}_k(\mathbb{F})$ we denote by $\mathbf{A}_\rho$ the following block matrix, which contains $3k$ rows and $3(n+1)k$ columns.

$$\mathbf{A}_\rho := \begin{bmatrix} I_k & 0 & 0 & -I_k & \ldots & -I_k & 0 & \ldots & 0 & \rho(g_1) \ldots \rho(g_n) \\ 0 & I_k & 0 & \rho(g_1) \ldots \rho(g_n) & -I_k & \ldots & -I_k & 0 & \ldots & 0 \\ 0 & 0 & I_k & 0 & \ldots & 0 & \rho(g_1) \ldots \rho(g_n) & -I_k & \ldots & -I_k \end{bmatrix}.$$

Lemma 3.2. *If $M = Q_3(G)$ is k-linearly representable over $\mathbb{F}$, then there exists a faithful representation $\rho : G \to \mathrm{GL}_k(\mathbb{F})$ such that $\mathbf{A}_\rho$ is a k-linear representation of M.*

Proof. The technique we use to prove this lemma is a standard one (e.g., see the proofs of [28, Proposition 6.4.8, Lemma 6.8.5, Theorem 6.10.10] and [29, Lemma 3.35]). We generalize this technique to multi-linear representations by looking at the representation matrix as a block matrix and using Proposition 2.12. We repeatedly use the fact that for any multi-linear representation of M, if $X \subseteq E$ and $r(X) = n$ then the rank of the relevant sub-matrix of the representation (i.e., deleting the columns of elements not in X) is $n \cdot k$.

Suppose that

$$\mathbf{B} := \begin{bmatrix} B_{1,1} & B_{1,2} & B_{1,3} & B_{1,g'_1} & \ldots & B_{1,g'_n} & B_{1,g''_1} & \ldots & B_{1,g''_n} & B_{1,g'''_1} & \ldots & B_{1,g'''_n} \\ B_{2,1} & B_{2,2} & B_{2,3} & B_{2,g'_1} & \ldots & B_{2,g'_n} & B_{2,g''_1} & \ldots & B_{2,g''_n} & B_{2,g'''_1} & \ldots & B_{2,g'''_n} \\ B_{3,1} & B_{3,2} & B_{3,3} & B_{3,g'_1} & \ldots & B_{3,g'_n} & B_{3,g''_1} & \ldots & B_{3,g''_n} & B_{3,g'''_1} & \ldots & B_{3,g'''_n} \end{bmatrix}$$

is a k-linear representation of M. Then $r(\{1,2,3\}) = 3 = r(M)$ so $\mathbf{B}_1, \ldots, \mathbf{B}_{3k}$ span the columns of $\mathbf{B}$. By changing the basis of the column space of $\mathbf{B}$ (see Proposition 2.12(c)) there exists a block matrix $\mathbf{C}$ of the form

$$\mathbf{C} := \begin{bmatrix} I_k & 0 & 0 & C_{1,g'_1} & \ldots & C_{1,g'_n} & C_{1,g''_1} & \ldots & C_{1,g''_n} & C_{1,g'''_1} & \ldots & C_{1,g'''_n} \\ 0 & I_k & 0 & C_{2,g'_1} & \ldots & C_{1,g'_n} & C_{2,g''_1} & \ldots & C_{2,g''_n} & C_{2,g'''_1} & \ldots & C_{2,g'''_n} \\ 0 & 0 & I_k & C_{3,g'_1} & \ldots & C_{1,g'_n} & C_{3,g''_1} & \ldots & C_{3,g''_n} & C_{3,g'''_1} & \ldots & C_{3,g'''_n} \end{bmatrix}$$

that is a k-linear representation of M. As $\forall g \in G, r(\{1,2,g'\}) = 2$, we have that

$$\mathrm{rank} \begin{bmatrix} I_k & 0 & C_{1,g'} \\ 0 & I_k & C_{2,g'} \\ 0 & 0 & C_{3,g'} \end{bmatrix} = 2k.$$

Thus, $C_{3,g'} = 0$. Also $r(\{1,g'\}) = 2$, so

$$\mathrm{rank} \begin{bmatrix} I_k & C_{1,g'} \\ 0 & C_{2,g'} \\ 0 & C_{3,g'} \end{bmatrix} = 2k,$$

therefore, $C_{2,g'}$ is invertible (it has to be of full rank since $C_{3,g'} = 0$). Since $r(\{2, g'\}) = 2$, by the same argument $C_{1,g'}$ is also invertible. Similarly $\forall g \in G$, $C_{1,g''} = 0$, and $C_{3,g''}, C_{2,g''}$ are invertible, and $C_{2,g'''} = 0$, and $C_{1,g'''}, C_{3,g'''}$ are invertible.

We now apply column block-scaling (Proposition 2.12(a)) on the columns of $g'_1, \ldots, g'_n$ by $-(C_{1,g'_1})^{-1}, \ldots, -(C_{1,g'_n})^{-1}$ respectively to get that

$$\begin{bmatrix} I_k & 0 & 0 & C_{1,g'_1}(-(C_{1,g'_1})^{-1}) & \ldots & C_{1,g'_n}(-(C_{1,g'_n})^{-1}) & 0 & \ldots & 0 & C_{1,g'''_1} & \ldots & C_{1,g'''_n} \\ 0 & I_k & 0 & C_{2,g'_1}(-(C_{1,g'_1})^{-1}) & \ldots & C_{2,g'_n}(-(C_{1,g'_n})^{-1}) & C_{2,g''_1} & \ldots & C_{2,g''_n} & 0 & \ldots & 0 \\ 0 & 0 & I_k & 0 & \ldots & 0 & C_{3,g''_1} & \ldots & C_{3,g''_n} & C_{3,g'''_1} & \ldots & C_{3,g'''_n} \end{bmatrix}$$

$$= \begin{bmatrix} I_k & 0 & 0 & -I_k & \ldots & -I_k & 0 & \ldots & 0 & C_{1,g'''_1} & \ldots & C_{1,g'''_n} \\ 0 & I_k & 0 & C'_{2,g'_1} & \ldots & C'_{2,g'_n} & C_{2,g''_1} & \ldots & C_{2,g''_n} & 0 & \ldots & 0 \\ 0 & 0 & I_k & 0 & \ldots & 0 & C_{3,g''_1} & \ldots & C_{3,g''_n} & C_{3,g'''_1} & \ldots & C_{3,g'''_n} \end{bmatrix}$$

is a k-linear representation of M. Now by row block-scaling (Propostion 2.12(b)) on the second row by $(C'_{2,g'_1})^{-1}$ we get that

$$\begin{bmatrix} I_k & 0 & 0 & -I_k & \ldots & -I_k & 0 & \ldots & 0 & C_{1,g'''_1} & \ldots & C_{1,g'''_n} \\ 0 & (C'_{2,g'_1})^{-1} & 0 & I_k & \ldots & C'_{2,g'_n}(C'_{2,g'_1})^{-1} & C_{2,g''_1}(C'_{2,g'_1})^{-1} & \ldots & C_{2,g''_n}(C'_{2,g'_1})^{-1} & 0 & \ldots & 0 \\ 0 & 0 & I_k & 0 & \ldots & 0 & C_{3,g''_1} & \ldots & C_{3,g''_n} & C_{3,g'''_1} & \ldots & C_{3,g'''_n} \end{bmatrix}$$

is a k-linear representation of M. We continue in the same fashion by block-scaling on the columns of $g''_1, \ldots, g''_n$, then row block-scaling on the third row, then column block-scaling of columns $g'''_1, \ldots, g'''_n$, and finally column block scaling of columns $2, 3$ to get that

$$\mathbf{D} := \begin{bmatrix} I_k & 0 & 0 & -I_k & -I_k & \ldots & -I_k & 0 & 0 & \ldots & 0 & D_{1,g'''_1} & D_{1,g'''_2} & \ldots & D_{1,g'''_n} \\ 0 & I_k & 0 & I_k & D_{2,g'_2} & \ldots & D_{2,g'_n} & -I_k & -I_k & \ldots & -I_k & 0 & 0 & \ldots & 0 \\ 0 & 0 & I_k & 0 & 0 & \ldots & 0 & I_k & D_{3,g''_2} & \ldots & D_{3,g''_n} & -I_k & -I_k & \ldots & -I_k \end{bmatrix}$$

is a k-linear representation of M.

We next use the fact that $\mathbf{D}$ is a multi-linear representation of $Q_3(G)$ to prove that blocks in different parts of the representation are equal, e.g., $D_{3,g''} = D_{2,g'}$. Since $r(\{g'_1, g''_1, g'''_1\}) = 2$, we have that

$$\operatorname{rank} \begin{bmatrix} -I_k & 0 & D_{1,g'''_1} \\ I_k & -I_k & 0 \\ 0 & I_k & -I_k \end{bmatrix} = 2k,$$

and this forces $D_{1,g'''_1} = I_k$. For j, ℓ such that $g_j = g_\ell^{-1}$ (thus, $g_j \cdot g_1 \cdot g_\ell = 1$), we have that $r(\{g'_1, g''_j, g'''_\ell\}) = 2$. So,

$$\operatorname{rank} \begin{bmatrix} -I_k & 0 & D_{1,g'''_\ell} \\ I_k & -I_k & 0 \\ 0 & D_{3,g''_j} & -I_k \end{bmatrix} = 2k.$$

By Proposition 2.11(a) we get that $\operatorname{rank}(D_{3,g''_j} \cdot D_{1,g'''_\ell} - I_k) = 0$ so $D_{3,g''_j} = (D_{1,g'''_\ell})^{-1}$. By symmetric arguments, $D_{1,g'''_j} = (D_{2,g'_\ell})^{-1}$ and $D_{2,g'_j} = (D_{3,g''_\ell})^{-1}$.

Therefore,

$$\forall g \in G, D_{3,g''} = D_{2,g'} = D_{1,g'''}. \tag{3}$$

Now let $\rho : G \to \mathrm{GL}_k(\mathbb{F})$ be the map $\rho(g) = D_{2,g'}$. We see that $\rho(1) = I$ (because $D_{2,g'_1} = I$). By Proposition 2.11(a)

$$\begin{aligned}\operatorname{rank}\begin{bmatrix} -I_k & 0 & D_{1,g'''_\ell} \\ D_{2,g'_i} & -I_k & 0 \\ 0 & D_{3,g''_j} & -I_k \end{bmatrix} &= 2k + \operatorname{rank}(D_{3,g''_j} D_{2,g'_i} D_{1,g'''_\ell} - I) \\ &= 2k + \operatorname{rank}(\rho(g_j) \cdot \rho(g_i) \cdot \rho(g_\ell) - I). \end{aligned} \tag{4}$$

By the matroid rank, it is equal to $2k$ if $g_j \cdot g_i \cdot g_\ell = 1$ and $3k$ otherwise, thus,

$$\forall g_i, g_j, g_\ell \in G, g_j \cdot g_i \cdot g_\ell = 1 \Leftrightarrow \rho(g_j) \cdot \rho(g_i) \cdot \rho(g_\ell) = I. \tag{5}$$

We now use (5) to show that ρ is an injective group homomorphism, which completes the proof:

For every $g \in G$, since $1 \cdot g^{-1} \cdot g = 1$, we have $I = \rho(1) \cdot \rho(g^{-1}) \cdot \rho(g) = I \cdot \rho(g^{-1}) \cdot \rho(g)$, forcing $\rho(g)^{-1} = \rho(g^{-1})$.

Therefore, $\forall g, h \in G$, as $g \cdot h \cdot (gh)^{-1} = 1$, we have $I = \rho(g) \cdot \rho(h) \cdot \rho((gh)^{-1}) = \rho(g) \cdot \rho(h) \cdot \rho(gh)^{-1}$. Thus, $\rho(gh) = \rho(g) \cdot \rho(h)$. This proves that ρ is a group homomorphism.

For injectivity, if $g \neq h$ then $g \cdot h^{-1} \cdot 1 \neq 1$, which implies that $\rho(g) \cdot \rho(h)^{-1} \cdot \rho(1) \neq I$, so $\rho(g) \neq \rho(h)$.

Lemma 3.3. *Let $\rho : G \to \mathrm{GL}_k(\mathbb{F})$ be a faithful representation. If $\mathbf{A}_\rho$ is a k-linear representation of $Q_3(G)$ then ρ is fixed-point free.*

Proof. Since $\mathbf{A}_\rho$ is a k-linear representation of $Q_3(G)$, for every $g \neq 1_G$ we have that $r(\{g'_1, g'\}) = 2$. So

$$\operatorname{rank}\begin{bmatrix} -I_k & -I_k \\ I_k & \rho(g) \\ 0 & 0 \end{bmatrix} = 2k. \tag{6}$$

By Proposition 2.11(b) we have that

$$\operatorname{rank}\begin{bmatrix} -I_k & -I_k \\ I_k & \rho(g) \\ 0 & 0 \end{bmatrix} = k + \operatorname{rank}(\rho(g) - I_k). \tag{7}$$

By combining (6) and (7), $\operatorname{rank}(\rho(g) - I_k) = k$. This implies that $\rho(g) - I_k$ is invertible, so $\forall v \neq 0, (\rho(g) - I_k)v \neq 0$, therefore, $\forall v \neq 0, \rho(g)v \neq v$, which means that 1 is not an eigenvalue of $\rho(g)$. So, ρ is fixed-point free, as desired.

Lemma 3.4. *If $\rho : G \to \mathrm{GL}_k(\mathbb{F})$ is a fixed-point free representation, then $\mathbf{A}_\rho$ is a k-linear representation of $Q_3(G)$.*

Proof. To prove that $\mathbf{A}_\rho$ is a k-linear representation of M, we need to verify that $\forall X \subset E$, if $r(X) = n$ then the rank of the relevant sub-matrix of $\mathbf{A}_\rho$ (i.e., deleting the columns of elements not in X) is nk. Ranks of most sub-matrices are trivially verified, e.g.,

$$\text{rank}\begin{bmatrix} I_k & 0 & -I_k \\ 0 & I_k & 0 \\ 0 & 0 & \rho(g) \end{bmatrix} = \text{rank}\begin{bmatrix} I_k & -I_k & -I_k \\ 0 & \rho(g_i) & 0 \\ 0 & 0 & \rho(g_j) \end{bmatrix} = 3k, \text{rank}\begin{bmatrix} I_k & -I_k \\ 0 & \rho(g) \\ 0 & 0 \end{bmatrix} = 2k.$$

(Note that $\forall g \in G$, the matrix $\rho(g)$ is invertible, and, therefore, of rank k). So it is necessary and sufficient to ensure that the following 2 requirements hold:

1. For every two distinct elements $g_i \neq g_j$

$$\text{rank}\begin{bmatrix} -I_k & -I_k \\ \rho(g_i) & \rho(g_j) \\ 0 & 0 \end{bmatrix} = 2k, \tag{8}$$

2. For all $g_i, g_j, g_\ell \in G$ (not necessarily distinct)

$$\text{rank}\begin{bmatrix} -I_k & 0 & \rho(g_\ell) \\ \rho(g_i) & -I_k & 0 \\ 0 & \rho(g_j) & -I_k \end{bmatrix} = r(\{g_i', g_j'', g_\ell'''\}) = \begin{cases} 2k & \text{if } g_j \cdot g_i \cdot g_\ell = 1, \\ 3k & \text{otherwise.} \end{cases} \tag{9}$$

Ranks of all other relevant sub-matrices follow from similar arguments.

We first show that Equation (8) holds. By Proposition 2.11(b)

$$\text{rank}\begin{bmatrix} -I_k & -I_k \\ \rho(g_i) & \rho(g_j) \\ 0 & 0 \end{bmatrix} = k + \text{rank}(\rho(g_j) - \rho(g_i)), \tag{10}$$

so in order to show that Equation (8) holds, we need to verify that for every two distinct group elements g_i, g_j $\text{rank}(\rho(g_i) - \rho(g_j)) = k$. Since ρ is fixed-point free and $g_i^{-1} g_j \neq 1$, for every $v \neq 0, v \neq \rho(g_i^{-1} g_j)v = (\rho(g_i)^{-1}\rho(g_j))v$, so $\forall v \neq 0, \rho(g_i)v \neq \rho(g_j)v$, thus, $\forall v \neq 0, (\rho(g_i) - \rho(g_j))v \neq 0$, which implies that $\rho(g_i) - \rho(g_j)$ is invertible and, therefore, of rank k, so (8) holds.

We next show that Equation (9) holds. By Proposition 2.11(a) and the definition of a homomorphism,

$$\text{rank}\begin{bmatrix} -I_k & 0 & \rho(g_\ell) \\ \rho(g_i) & -I_k & 0 \\ 0 & \rho(g_j) & -I_k \end{bmatrix} = 2k + \text{rank}(\rho(g_j \cdot g_i \cdot g_\ell) - I_k). \tag{11}$$

So, to prove that (9) holds, we need to show that

$$\text{rank}(\rho(g_j \cdot g_i \cdot g_\ell) - I_k) = \begin{cases} 0 \text{ if } g_j \cdot g_i \cdot g_\ell = 1 \\ k \quad \text{otherwise.} \end{cases}$$

By arguments similar to the above

1. If $g_j \cdot g_i \cdot g_\ell \neq 1$ then $\text{rank}(\rho(g_j \cdot g_i \cdot g_\ell) - I_k) = k$, as ρ is fixed-point free.
2. If $g_j \cdot g_i \cdot g_\ell = 1$ then $\text{rank}(\rho(g_j \cdot g_i \cdot g_\ell) - I_k) = 0$. (This in fact true for any representation because $\rho(g_j \cdot g_i \cdot g_\ell) = \rho(1) = I_k$.)

*Proof (**Proof of Theorem 3.1**).* Combining the lemmas we get Theorem 3.1: If G has a fixed-point free representation ρ of dimension k, then by Lemma 3.4, the block matrix $\mathbf{A}_\rho$ is a k-linear representation of $Q_3(G)$, and, in particular, $Q_3(G)$ has a k-linear representation. On the other hand, if $Q_3(G)$ is k-linearly representable then, by Lemma 3.2, it has a faithful representation ρ of dimension k such that $\mathbf{A}_\rho$ is a k-linear representation of $Q_3(G)$, so, by Lemma 3.3, ρ is fixed-point free.

We combine Theorem 3.1 with Proposition 2.15 to get our desired result:

Corollary 3.5. *For every prime $p > 2$ there is a matroid that is p-minimally representable. Moreover, the matroid has* $\text{poly}(p)$ *ground points and this representation exists over a finite field with $2^{O(p^{6.18})}$ elements.*

Proof. Let q and G_p be as in Proposition 2.15. By Theorem 3.1 and Proposition 2.15, over the field $\mathbb{F}_{2^{pq}}$, the matroid $Q_3(G_p)$, which has $3p^2q+3$ elements in the ground set, is p-linearly representable. Furthermore, over any field, the matroid $Q_3(G_p)$ is not j-linearly representable for any $j < p$. So, $Q_3(G_p)$ is p-minimally representable. By Proposition 2.15, if we chose the appropriate q, then the field $\mathbb{F}_{2^{pq}}$ has $2^{O(p^{6.18})}$ elements.

We next rephrase the result in secret-sharing terms.

Corollary 3.6. *For every prime p, there exists an access structure with* $\text{poly}(p)$ *parties, which has an ideal p-linear secret-sharing scheme with secrets of length* $\text{poly}(n)$*, but has no ideal k-linear secret-sharing scheme for every $k < p$.*

Since the matroid has $3p^2q + 3$ elements in the ground set, the corresponding access structure has $3p^2q + 2$ parties. Therefore, for every prime p, the smallest access structure of this type has $O(p^{7.18})$ parties. Also note that the schemes is over a field with $2^{\text{poly}(p)}$ elements, so every share can be represented by $\text{poly}(p)$ bits.

4 Lower Bounds for Multi-Linear secret-sharing Schemes

The best known lower bounds for linear secret-sharing schemes is $n^{\Omega(\log n)}$ [1, 16, 17]. By modification of the claims in [17], we show that these lower bounds hold also for multi-linear secret-sharing schemes. Thus, even using multi-linear schemes one cannot construct efficient schemes for general access structures.

We will use the following alternative definition of multi-linear secret sharing schemes, proven to be equivalent in [13] (following [7, 20]).

Definition 4.1 (Multi-Target Monotone Span Program). *A multi-target monotone span program is a quadruple $\mathcal{M} = (\mathbb{F}, M, \rho, X)$, where $\mathbb{F}$ is a finite field, M is an $a \times b$ matrix over $\mathbb{F}$, the function $\rho : \{1, \ldots, a\} \to \{p_1, \ldots, p_n\}$ labels each row of M by a party, and X is a set of k independent vectors in $\mathbb{F}^b$ such that for every $A \subseteq \{p_1, \ldots, p_n\}$ either*

- *The rows of the sub-matrix obtained by restricting M to the rows labeled by parties in A, denoted M_A, span every vector in X. In this case, we say that $\mathcal{M}$ accepts A, or,*
- *The rows of M_A span no non-zero vector in the linear space spanned by X. In this case, we say that $\mathcal{M}$ rejects B.*

We say that $\mathcal{M}$ accepts an access structure $\mathcal{A}$ if $\mathcal{M}$ accepts a set B if $B \in \mathcal{A}$, and rejects every set $B \notin \mathcal{A}$. The size of a multi-target monotone span program is a/k, where a is the number of rows in the matrix and k is the number of vectors in the set X.

Note that not every labeled matrix is a multi-target span program. For example, if $k > 1$ and for some set A, the rows in M_A span exactly one vector in X, then this is not a multi-target span program. By [13] a multi-linear secret-sharing scheme realizing an access structure $\mathcal{A}$ with total share size a exists if and only if there exists a multi-target monotone span program accepting $\mathcal{A}$ that has a rows. In particular, if there exists a multi-target monotone span program accepting $\mathcal{A}$ with a_j rows labeled by p_j for $1 \leq j \leq n$ and k vectors in the set X, then the exists a multi-linear secret-sharing scheme realizing $\mathcal{A}$ with information ratio $\max_{1 \leq j \leq n} a_j/k$. In ideal multi-linear secret-sharing schemes $a_j = k$ for every j.

Assume, w.l.o.g., that $X = \{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k\}$. We make 2 observations regarding multi-target monotone span program.

Observation 4.2 *If $B \in \mathcal{A}$ and $N = M_B$ then the rows of N span X, thus $\forall 0 < s < k$ there exists some vector $\boldsymbol{v}_s$ such that $\boldsymbol{e}_s = \boldsymbol{v}_s N$.*

Observation 4.3 *If $T \notin \mathcal{A}$ then for every $s \in \{1, \ldots, k\}$ there exists a vector $\boldsymbol{w}_s \in \mathbb{F}^b$ such that the following hold: (1) $M_T \boldsymbol{w}_s = 0$, (2) $\forall i \neq s, \boldsymbol{e}_i \cdot \boldsymbol{w}_s = 0$, and (3) $\boldsymbol{e}_s \cdot \boldsymbol{w}_s = 1$ (that is, the coordinate s in $\boldsymbol{w}_s$ is 1).*

Proof. If $T \notin \mathcal{A}$, then the rows of M_T do not span any of the vectors in X. Let $M_{T,X}$ be the matrix containing the rows of M_T and additional rows $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k$ and $M_{T,X \setminus \{s\}}$ the same matrix with the row $\boldsymbol{e}_s$ deleted. By simple linear algebra, for every $1 \leq s \leq k$, we have that $\operatorname{rank} M_{T,X} < \operatorname{rank} M_{T,X \setminus \{s\}}$, which implies that $|\operatorname{kernel} M_{T,X}| > \left|\operatorname{kernel} M_{T,X \setminus \{s\}}\right|$, and so there is some vector $\boldsymbol{w}_s \in \mathbb{F}^b$ such that $\boldsymbol{e}_s \cdot \boldsymbol{w}_s = 1$ and $M_{T,X \setminus \{s\}} \boldsymbol{w}_s = \boldsymbol{0}$ (so evidently $M_T \boldsymbol{w}_s = 0$ and $\forall i \neq s, \boldsymbol{e}_i \cdot \boldsymbol{w}_s = 0$).

We next quote the definition of a collection with unique intersection from [17]. Such collections are used in [17] to prove lower bounds for monotone span programs; we show that the same lower bound holds for multi-target monotone span programs.

Definition 4.4. *Let $\mathcal{A}$ be a monotone access structure, with $\mathcal{B} = \{B_1, \ldots, B_\ell\}$ the collection of minimal authorized sets in $\mathcal{A}$. Let $\mathcal{C} = \{(C_{1,0}, C_{1,1}), (C_{2,0}, C_{2,1}), \ldots, (C_{t,0}, C_{t,1})\}$ be a collection of pairs of sets of parties. We say that $\mathcal{C}$ satisfies the* unique intersection *property for $\mathcal{A}$ if*

1. *For every $1 \leq j \leq t$, $\{p_1, \ldots, p_n\} \setminus (C_{j,0} \cup C_{j,1}) \notin \mathcal{A}$.*
2. *For every $1 \leq i \leq \ell$ and every $1 \leq j \leq t$, exactly one of the following conditions hold (1) $B_i \cap C_{j,0} \neq \emptyset$, (2) $B_i \cap C_{j,1} \neq \emptyset$.*

Note that if $B \in \mathcal{A}$ and $\{p_1, \ldots, p_n\} \setminus C \notin \mathcal{A}$, then $B \cap C \neq \emptyset$ (otherwise, $B \subseteq \{p_1, \ldots, p_n\} \setminus C$, contradicting the monotonicity of $\mathcal{A}$). Thus, Condition (2) in Definition 4.4 requires that B_i intersects at most one of the sets $C_{j,0}, C_{j,1}$.

Theorem 4.5. *Let $\mathcal{C}$ be a collection satisfying the unique intersection property for $\mathcal{A}$. Define a matrix D of size $\ell \times t$, with $D_{i,j} = 0$ if $B_i \cap C_{i,0} \neq \emptyset$ and $D_{i,j} = 1$ if $B_i \cap C_{i,1} \neq \emptyset$. Then, the size of every multi-target monotone span program accepting $\mathcal{A}$ is at least* $\mathrm{rank}_{\mathbb{F}}(D)$.

Proof. Let $\mathcal{M} = (\mathbb{F}, M, \rho, X = \{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k\})$ be a multi-target monotone span program accepting $\mathcal{A}$, and denote the number of rows of M by m. For every $1 \leq i \leq \ell$ since $B_i \in \mathcal{A}$ the rows of M labeled by the parties of B_i span X. By Observation 4.2, for every $1 \leq r \leq k$, there exists $\boldsymbol{v}_{i,r}$ such that $\boldsymbol{v}_{i,r} M = \boldsymbol{e}_r$ and the non-zero coordinates of $\boldsymbol{v}_{i,r}$ are only in rows labeled by B_i.
Fix $1 \leq j \leq t$ and let $T_j = \{p_1, \ldots, p_n\} \setminus (C_{j,0} \cup C_{j,1})$. Since $T_j \notin \mathcal{A}$, by Observation 4.3, for every $1 \leq s \leq k$ there exists a vector $\boldsymbol{w}_{j,s}$ such that $M_{T_j} \boldsymbol{w}_{j,s} = 0$, $\boldsymbol{e}_s \cdot \boldsymbol{w}_{j,s} = 1$ and $\forall r \neq s, \boldsymbol{e_r} \cdot \boldsymbol{w_{j,s}} = 0$. Let $\boldsymbol{y}_{j,s} := M \boldsymbol{w}_{j,s}$ and define $\boldsymbol{z}_{j,s}$ to be the column vector achieved from $\boldsymbol{y}_{j,s}$ by replacing all coordinates in $\boldsymbol{y}_{j,s}$ labeled by parties in $C_{j,0}$ with zero. The only non-zero coordinates in $\boldsymbol{z}_{j,s}$ are in coordinates labeled by $C_{j,1}$.
Define L as the matrix with rows $v_{1,1}, \ldots, v_{\ell,1}, v_{1,2}, \ldots, v_{\ell,2}, \ldots, v_{\ell,k}$ and R the matrix with columns $z_{1,1}, \ldots, z_{\ell,1}$, $z_{1,2}, \ldots, z_{\ell,2}, \ldots, z_{\ell,k}$. Note that by definition the rows of L are of length m, so L has m columns, thus, $\mathrm{rank}(L) \leq m$.

Let $\mathbf{D} = LR$. We next prove that $\mathbf{D}$ is a block matrix of the form:

$$\mathbf{D} = \begin{bmatrix} D & 0 & \ldots & 0 \\ 0 & D & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & D \end{bmatrix}, \tag{12}$$

where D is the matrix defined in the Theorem. We need to show that $\boldsymbol{v}_{i,r} \cdot \boldsymbol{z}_{s,j} = 0$ if $r \neq s$ (off the diagonal matrix block) and $\boldsymbol{v}_{i,r} \cdot \boldsymbol{z}_{s,j} = D_{i,j}$ if $r = s$.

- If $B_i \cap C_{j,0} \neq \emptyset$, $D_{i,j} = 0$. Furthermore, $B_i \cap C_j, 1 = \emptyset$, thus, $\boldsymbol{v}_{i,r}$ and $\boldsymbol{z}_{s,j}$ do not share non-zero coordinates and $\boldsymbol{v}_{i,r} \cdot \boldsymbol{z}_{s,j} = 0$. In particular, if $r = s$ then $\boldsymbol{v}_{i,r} \cdot \boldsymbol{z}_{r,j} = 0 = D_{i,j}$, and if $r \neq s$ then $\boldsymbol{v}_{i,r} \cdot \boldsymbol{z}_{s,j} = 0$ as desired.
- If $B_i \cap C_{j,1} \neq \emptyset$, then $D_{i,j} = 1$, $B_i \cap C_{j,0} = \emptyset$, and all coordinates in $\boldsymbol{v}_{i,r}$ labeled by $C_{j,0}$ are zero, thus,

$$\boldsymbol{v}_{i,r} \cdot \boldsymbol{z}_{s,j} = \boldsymbol{v}_{i,r} \cdot \boldsymbol{y}_{s,j} = \boldsymbol{v}_{i,r} M \boldsymbol{w}_{s,j} = \boldsymbol{e}_r \cdot \boldsymbol{w}_{s,j} = \begin{cases} 0 & r \neq s \\ 1 & r = s \end{cases}.$$

In particular, if $r = s$ then $\boldsymbol{v}_{i,r} \cdot \boldsymbol{z}_{r,j} = 1 = D_{i,j}$ and if $r \neq s$ then $\boldsymbol{v}_{i,r} \cdot \boldsymbol{z}_{s,j} = 0$.

So $\text{rank}_{\mathbb{F}}(\mathbf{D}) = k \cdot \text{rank}_{\mathbb{F}}(D)$, and since $\mathcal{M}$ is a k-linear representation, its size is $\frac{m}{k} \geq \frac{\text{rank}_{\mathbb{F}}(L)}{k} \geq \frac{\text{rank}_{\mathbb{F}}(\mathbf{D})}{k} = \text{rank}_{\mathbb{F}}(D)$.

By [17], for every n there is an access structure $\mathcal{A}$ with n parties, for which there exists a collection $\mathcal{C}$ satisfying the unique intersection property, such that $\text{rank}_{\mathbb{F}}(D) \geq n^{\Omega(\log n)}$ (where D is as defined in Theorem 4.5). So by Theorem 4.5,

Corollary 4.6. *For every n, there exists an access structure $\mathcal{N}_n$ with n parties such that every multi-target monotone span program over any field accepting it has size $n^{\Omega(\log n)}$.*

As multi-target monotone span program are equivalent to multi-linear secret-sharing schemes [20], the same lower bound applies to multi-linear secret-sharing schemes.

Corollary 4.7. *For every n, there exists an access structure $\mathcal{N}_n$ with n parties such that the information ratio of every multi-linear secret-sharing scheme realizing it is $n^{\Omega(\log n)}$.*

References

1. L. Babai, A. Gál, and A. Wigderson. Superpolynomial lower bounds for monotone span programs. *Combinatorica*, 19(3):301–319, 1999.
2. M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computations. In *Proc. of the 20th ACM Symp. on the Theory of Computing*, pages 1–10, 1988.
3. J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In S. Goldwasser, editor, *Advances in Cryptology – CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 27–35. Springer-Verlag, 1990.
4. M. Bertilsson and I. Ingemarsson. A construction of practical secret sharing schemes using linear block codes. In J. Seberry and Y. Zheng, editors, *Advances in Cryptology – AUSCRYPT '92*, volume 718 of *Lecture Notes in Computer Science*, pages 67–79. Springer-Verlag, 1993.
5. G. R. Blakley. Safeguarding cryptographic keys. In R. E. Merwin, J. T. Zanca, and M. Smith, editors, *Proc. of the 1979 AFIPS National Computer Conference*, volume 48 of *AFIPS Conference proceedings*, pages 313–317. AFIPS Press, 1979.
6. C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro. Graph decompositions and secret sharing schemes. *J. Cryptology*, 8(1):39–64, 1995.
7. E. F. Brickell. Some ideal secret sharing schemes. *Journal of Combin. Math. and Combin. Comput.*, 6:105–113, 1989.
8. E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *J. of Cryptology*, 4(73):123–134, 1991.
9. D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols. In *Proc. of the 20th ACM Symp. on the Theory of Computing*, pages 11–19, 1988.

10. R. Cramer, I. Damgård, and U. Maurer. General secure multi-party computation from any linear secret-sharing scheme. In B. Preneel, editor, *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 316–334. Springer-Verlag, 2000.
11. L. Csirmaz. The size of a share must be large. *J. of Cryptology*, 10(4):223–231, 1997.
12. Y. Desmedt and Y. Frankel. Shared generation of authenticators and signatures. In J. Feigenbaum, editor, *Advances in Cryptology – CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 457–469. Springer-Verlag, 1992.
13. M. van Dijk. A linear construction of secret sharing schemes. *Designs, Codes and Cryptography*, 12(2):161–201, 1997.
14. T. A. Dowling. A class of geometric lattices based on finite groups. *J. Comb. Theory, Ser. B*, 14(1):61–86, 1973.
15. T. A. Dowling. A q-analog of the partition lattice. *A survey of combinatorial theory*, pages 101–115, 1973.
16. A. Gál. A characterization of span program size and improved lower bounds for monotone span programs. *Computational Complexity*, 10(4):277–296, 2001.
17. A. Gál and P. Pudlák. A note on monotone complexity and the rank of matrices. *Inform. Process. Lett.*, 87:321–326, 2003.
18. V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proc. of the 13th ACM conference on Computer and communications security*, pages 89–98, 2006.
19. M. Ito, A. Saito, and T. Nishizeki. Secret sharing schemes realizing general access structure. In *Proc. of the IEEE Global Telecommunication Conf., Globecom 87*, pages 99–102, 1987. Journal version: Multiple assignment scheme for sharing secret. *J. of Cryptology*, 6(1):15-20, 1993.
20. M. Karchmer and A. Wigderson. On span programs. In *Proc. of the 8th IEEE Structure in Complexity Theory*, pages 102–111, 1993.
21. E. D. Karnin, J. W. Greene, and M. E. Hellman. On secret sharing systems. *IEEE Trans. on Information Theory*, 29(1):35–41, 1983.
22. Yu. V. Linnik. On the least prime in an arithmetic progression I. the basic theorem. *Rec. Math. (Mat. Sbornik) N.S.*, 15 (57):139–178, 1944.
23. Yu. V. Linnik. On the least prime in an arithmetic progression II. the deuring-heilbronn phenomenon. *Rec. Math. (Mat. Sbornik) N.S.*, 15 (57):347–368, 1944.
24. J. Martí-Farré and C. Padró. On secret sharing schemes, matroids and polymatroids. *Journal of Mathematical Cryptology*, 4(2):95–120, 2010.
25. F. Matúš. Matroid representations by partitions. *Discrete Mathematics*, 203:169–194, 1999.
26. J. S. Milne. Group theory (v3.12), 2012. Available at www.jmilne.org/math/.
27. M. Naor and A. Wool. Access control and signatures via quorum secret sharing. In *3rd ACM Conf. on Computer and Communications Security*, pages 157–167, 1996.
28. J. G. Oxley. *Matroid Theory*. Oxford University Press, 2011. Second Edition.
29. R. A. Pendavingh and S. H. M. van Zwam. Skew partial fields, multilinear representations of matroids, and a matrix tree theorem. *Advances in Applied Mathematics*, 50(1):201 – 227, 2013.
30. C. Semple and G. Whittle. Partial fields and matroid representation. *Advances in Applied Mathematics*, 17(2):184 – 208, 1996.
31. J.-P Serre. *Linear Representations of Finite Groups*. Springer, 1977.
32. P. D. Seymour. On secret-sharing matroids. *J. of Combinatorial Theory, Series B*, 56:69–73, 1992.

33. A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.
34. B. Shankar, K. Srinathan, and C. Pandu Rangan. Alternative protocols for generalized oblivious transfer. In *Proceedings of the 9th international conference on Distributed computing and networking*, ICDCN'08, pages 304–309, Berlin, Heidelberg, 2008. Springer-Verlag.
35. J. Simonis and A. Ashikhmin. Almost affine codes. *Designs, Codes and Cryptography*, 14(2):179–197, 1998.
36. D. R. Stinson. Decomposition construction for secret sharing schemes. *IEEE Trans. on Information Theory*, 40(1):118–125, 1994.
37. T. Tassa. Generalized oblivious transfer by secret sharing. *Des. Codes Cryptography*, 58(1):11–21, 2011.
38. M. van Dijk, W.-A. Jackson, and K. M. Martin. A general decomposition construction for incomplete secret sharing schemes. *Des. Codes Cryptography*, 15(3):301–321, 1998.
39. M. van Dijk, T. A. M. Kevenaar, G. J. Schrijen, and P. Tuyls. Improved constructions of secret sharing schemes by applying (lambda, omega)-decompositions. *Inform. Process. Lett.*, 99(4):154–157, 2006.
40. G. Vincent. Les groupes lineaires finis sans point fixes. *Commentarii Mathematici Helvetici*, 20:117–171, 1947.
41. B. Waters. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. In *Proc. of the 14th international conference on Practice and theory in public key cryptography*, volume 6571 of *Lecture Notes in Computer Science*, pages 53–70. Springer-Verlag, 2011.
42. J. A. Wolf. *Spaces of Constant Curvature*. Publish or Perish, Inc., 1984. Fifth Edition.
43. T. Xylouris. On the least prime in an arithmetic progression and estimates for the zeros of Dirichlet L-functions. *Acta Arith.*, 150(1):65–91, 2011.
44. H. Zassenhaus. Uber endliche faskorper. *Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universitat*, 11:187–220, 1935.

A The Construction of the Group G_p

In this section we briefly explain the construction of the group G_p (for any prime p), which appears in Proposition 2.15. We then give a partial explanation of why any fixed-point free representation of G_p is of dimension at least p. The complete proofs, and more details on the construction, will be given in the full version.

Semidirect products. We assume some familiarity with group basics, such as group homomorphisms and automorphisms. Let N be a group. Recall that the set of all automorphisms of N, denoted $Aut(N)$, is also a group, with group operation being composition, and the identity element being the identity map. We now recall the definition of an action of a group H on a group N.

Definition A.1. *Let H and N be two groups. By an* action *of H on N, denoted $H \curvearrowright N$, we mean a group homomorphism $\phi\colon H \to Aut(N)$.*

To simplify the notation, if no confusion is possible, we use shorter notation $x^g := (\phi(g))(x)$. Since ϕ is a homomorphism, the identity of G is mapped to the identity automorphism.

Example A.2. For any pair of groups H and N, there always exists the *trivial action* $\tau\colon H \to Aut(N)$, which maps every element of H to the identity automorphism. A non-trivial action, however, does not always exist, and depends on the choice of H and N.

Example A.3. Let $H = \mathbb{Z}_2$ and $N = \mathbb{Z}_3$. To avoid confusion we denote $N = \{0, 1, 2\}$ and $H = \{f_0, f_1\}$. Then H acts on N by $\phi(f_1)(1) = 2$. We note that this completely identifies the action because f_1 and 1 are generators of H and N respectively. Thus, for example, $f_1(2) = f_1(1+1) = f_1(1) + f_1(1) = 2+2 = 1$ and $f_0(1) = f_1 \circ f_1(1) = f_1(2) = 1$. So it remains to verify only that this is well defined, which is a very small task.

Lemma A.4. *Let $\psi\colon G_1 \to G_2$ be a group homomorphism, and $\phi\colon G_2 \curvearrowright N$ a group action. Then ψ induces a group action $\psi^*(\phi)\colon G_1 \curvearrowright N$, given by composition $(\psi^*(\phi))(x) := \phi(\psi(x))$. Furthermore, if ψ is surjective and the action ϕ is non-trivial then so is $\psi^*(\phi)$.*

Proof. Follows easily from the definitions.

The following proposition is well known.

Proposition A.5 *For any prime q, the group of automorphisms of $\mathbb{Z}_q$ is isomorphic to the group $\mathbb{Z}_{q-1}$.*

This allows us to build a non-trivial action of $\mathbb{Z}_p$ on $\mathbb{Z}_q$, if p, q are primes such that $q \equiv 1 \mod p$.

Proposition A.6 *Let $p, q \in \mathbb{N}$ be two primes such that $q \equiv 1 \mod p$. Then $\mathbb{Z}_p$ admits a non-trivial action on $\mathbb{Z}_q$.*

Proof. From Proposition A.5 $Aut(\mathbb{Z}_q) \simeq \mathbb{Z}_{q-1}$. Thus, it suffices to construct a non-trivial homomorphism $\phi\colon \mathbb{Z}_p \to \mathbb{Z}_{q-1}$. Let $n \in \mathbb{N}$ be such that $q - 1 = np$, and set $\phi(x) := nx \mod q$. Then ϕ is a non-trivial homomorphism.

Corollary A.7. *Let p, q be as in Proposition A.6. Then $\mathbb{Z}_{p^2}$ admits a non-trivial action on $\mathbb{Z}_q$.*

Proof. We have a natural surjective homomorphism $\psi\colon \mathbb{Z}_{p^2} \to \mathbb{Z}_p$ given by $\psi(x) := x \mod p$. Thus, by Proposition A.6 and Lemma A.4, $\psi^*(\phi)$ is a non-trivial action of $\mathbb{Z}_{p^2}$ on $\mathbb{Z}_q$.

There may exist other non-trivial actions of $\mathbb{Z}_{p^2}$ on $\mathbb{Z}_q$. However, from now on when we mention *the* action of $\mathbb{Z}_{p^2}$ on $\mathbb{Z}_q$, we mean that we have fixed an isomorphism $Aut(\mathbb{Z}_q) \simeq \mathbb{Z}_{q-1}$ and we refer to the non-trivial action $\psi^*(\phi)$ constructed in the proof of Corollary A.7.

Definition A.8. *Let H be a group acting on another group N, and $\phi\colon H \to Aut(N)$ the action. The* semidirect product*, denoted $N \rtimes_\phi H$, is the set $N \times H = \{(n, h) | n \in N, h \in H\}$ equipped with the following operation*

$$(n_1, h_1) \cdot (n_2, h_2) := (n_1 \cdot n_2^{h_1}, h_1 \cdot h_2). \tag{13}$$

We leave to the reader to verify that (13) indeed defines a group-law. We will often omit ϕ in the notation of the semidirect product, and write simply $N \rtimes G$. When the action of G on N is not trivial we will say that the semidirect product is *non-trivial*. An attractive property of non-trivial semidirect products is that they are not abelian, even if H and N are.

Lemma A.9. *If $N \rtimes G$ is a non-trivial semidirect product then it is not abelian.*

Proof. Since G acts non-trivially, there exist $g \in G$ and $h \in N$ such that $h^g \neq h$. Therefore $(e_N, g) \cdot (h, e_G) = (h^g, g) \neq (h, g) = (h, e_G) \cdot (e_N, g)$.

Proposition A.10 *Let p and q be prime integers satisfying $q \equiv 1 \mod p$. Then there exists a non-trivial semidirect product $G_p = \mathbb{Z}_q \rtimes \mathbb{Z}_{p^2}$. The group has $p^2 \cdot q$ elements.*

Proof. Follows immediately from the definitions and Corollary A.7.

Suitability of G_p. We now explain why the above construction works for us. Since a full proof requires quite a few pages of background in representation theory, we will only give a brief overview and refrain from proving the following claims, which rely on some classical theorems in representation theory. But first we state Linnik's theorem:

Theorem A.11 (Linnik's Theorem). *There exists constants c, L such that for any pair of co-prime integers a and d, with $1 \leq a < d$, the smallest prime of the form $a + nd$ ($n \geq 1$) is smaller than cd^L.*

Linnik didn't give an explicit bound on L, but later works have shown that L is in fact very small. The current state of the art is $L \leq 5.18$ due to Xylouris [43].

Corollary A.12. *For every prime p, there exists a prime q, with $q = O(p^{5.18})$, for which a non-trivial semidirect product $\mathbb{Z}_q \rtimes \mathbb{Z}_{p^2}$ exists.*

Now fix a prime p and a prime q such that $q \equiv 1 \mod p$, and let $G_p = \mathbb{Z}_q \rtimes \mathbb{Z}_{p^2}$ be the non-trivial semidirect product explained above.

Lemma A.13. *The group G_p is solvable and every proper subgroup of G_p is cyclic. Thus, from the classification of solvable fixed-point free groups (see for example [42, Theorem 6.1.11]), the group G_p admits a fixed-point free representation.*

Lemma A.14. *The group G_p is not abelian. This implies that G_p does not have fixed-point free representations of dimension 1.*

Lemma A.15. *The group G_p does not have any fixed-point free representations over fields of characteristic p, q.*

Lemma A.16. *Over fields of characteristic different from p, q, the dimension of the smallest fixed-point representation of G_p divides the order of G_p. Thus, since the dimension cannot be 1, G_p has a fixed-point free representation of dimension $\geq p$.*

The completion of Proposition 2.15 (i.e., bounding the size of the field) is done by explicitly building a fixed-point free representation of G_p of dimension p over the field $\mathbb{F}_{2^{pq}}$.