T A R T U Ü L I K O O L
MATEMAATIKA-INFORMAATIKATEADUSKOND
Arvutiteaduse instituut
Informaatika eriala

Katharina Kahrs

Share Computing Protocols over Fields and Rings

Magistritöö (20 AP)

Juhendaja: Sven Laur

Autor: ..... "....." juuni 2009
Juhendaja: ..... "....." juuni 2009

Lubada kaitsmisele
Professor ..... "....." juuni 2009

TARTU 2009

Abstract

In this thesis, we explain linear secret sharing schemes, in particular multiplicative threshold linear secret sharing schemes, over fields and rings in a compact and concise way. We explain two characterisations of linear secret sharing schemes, and in particular, we characterise threshold linear secret sharing schemes. We develop an algorithm to generate all multiplicative $(t+1)$-out-of-n threshold linear secret sharing schemes over a field $\mathbb{Z}_p$. For the ring $\mathbb{Z}_{2^{32}}$, we explain the generation of secret sharing schemes for threshold access structures and prove the non-existence of $(t+1)$-out-of-n threshold linear secret sharing schemes with $n > t+1$.

Contents

Chapter 1

Introduction to Share Computing

This thesis is about the mathematical background of share computing protocols. Share computing protocols are used to aggregate sensitive data without revealing the content of individual data records. Examples of such databases and data aggregation problems are rather common. Databases containing personal, medical or financial information about an individual such as racial or ethnic origin, political views, religion, physical or mental health or criminal offences are usually classified as sensitive. Governmental bodies and researchers must be able to process such data in order to compute statistics about the population as a whole, but in many countries it is illegal to process such information without a special licence.

Privacy-preserving data mining provides a way of computing global properties from data without revealing properties of the data of an individual. One way of implementing privacy-preserving data mining is to use secure multi-party computation based on secret sharing (Figures 1.1-1.4). First, the individual data is split into shares (phase 1) that by themselves do not reveal any or marginally little secret information. Those shares are distributed to a number of miners (phase 2). This is called perfectly secure or ϵ-secure secret sharing. Each miner computes a function from its data shares and reveals the result (phase 3). Those results are themselves shares of a global function. The result of the global function may be reconstructed from the shares (phase 4).

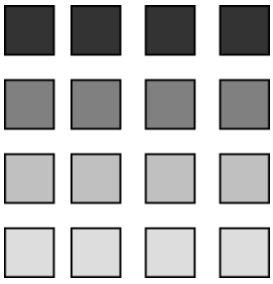

Figure 1.1: Phase 1

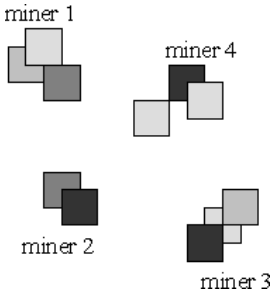

Figure 1.2: Phase 2

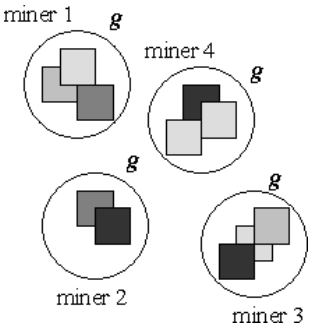

Figure 1.3: Phase 3

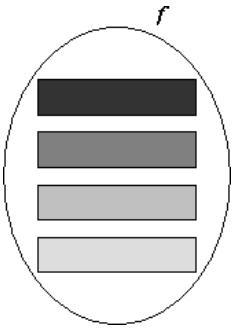

Figure 1.4: Phase 4

Most practical implementations of secure multi-party computation use linear secret sharing schemes, and in particular, threshold linear secret sharing schemes. In this thesis, we will explain linear secret sharing schemes and multiplicative linear secret sharing schemes and characterise them in two different ways. In particular, we will explain and characterise black box secret sharing schemes. Further, we will explain threshold linear secret sharing schemes and characterise those. We will use this characterisation to develop an algorithm to generate all $(t+1)$-out-of-n threshold linear secret sharing schemes with one share per miner over the field $\mathbb{Z}_p$ for a given threshold t and given parameters n and p.

The platform SHAREMIND [5], a virtual machine for privacy-preserving data processing developed at the University of Tartu, is an example of a practical implementation of privacy-preserving data mining. The first version of SHAREMIND was released in 2007. SHAREMIND securely computes sums, products, and scalar multiples of secret data. The computations in SHAREMIND are done over the ring $\mathbb{Z}_{2^{32}}$. The current implementation of SHAREMIND uses a 3-out-of-3 threshold linear secret sharing scheme over $\mathbb{Z}_{2^{32}}$. This means that there are three miners, and all three of them together should be able to reconstruct the result of a global function. No two of them together or one of them alone, however, should be able to deduce

any secret information from their shares of the individual data. For certain applications this is a rather weak security guarantee. Multiplicative $(t+1)$-out-of-n threshold linear secret sharing schemes provide a generic solution to this problem. We prove that there are no $(t+1)$-out-of-n threshold linear secret sharing schemes over $\mathbb{Z}_{2^{32}}$ with one share per miner if $n > t+1$. There do, however, exist multiplicative $(t+1)$-out-of-n threshold linear secret sharing schemes over $\mathbb{Z}_{2^{32}}$ for $n > t+1$ with more than one share per miner. As an example, we estimate share sizes for multiplicative 3-out-of-5 and 4-out-of-7 threshold linear secret sharing schemes.

Most secret sharing schemes, however, are defined over a field, in particular the field $\mathbb{Z}_p$, where p is a prime. Shamir's secret sharing scheme from 1979 [17] is the oldest $(t+1)$-out-of-n threshold linear secret sharing scheme over $\mathbb{Z}_p$. In Shamir's secret sharing scheme, the size of a share is the same as the size of the secret. This is optimal for perfectly secure secret sharing schemes. Only in ϵ-secure secret sharing schemes, the size of a share may be smaller than the size of the secret. In Shamir's secret sharing scheme, the share of miner i is the evaluation of a random polynomial of degree t at the point i. A natural question: Are the shares of any $(t+1)$-out-of-n threshold linear secret sharing scheme over a field $\mathbb{Z}_p$ equal to the evaluation of a random polynomial of degree t at some points? The answer is no. We use our algorithm to generate many examples of Shamir and non-Shamir threshold linear secret sharing schemes, and characterise 2-out-of-n Shamir threshold linear secret sharing schemes.

Roadmap.

- Chapter 2 is a reference of important mathematical facts and definitions for the reader.
- In Chapter 3, we define secret sharing schemes, and in particular, linear secret sharing schemes. We characterise linear secret sharing schemes in two ways.
- In Chapter 4, we define multiplicative linear secret sharing schemes and again characterise multiplicative linear secret sharing schemes in two ways. We explain the proof of the existence of $(t+1)$-out-of-n threshold linear secret sharing schemes over $\mathbb{Z}_{2^{32}}$ with more than one share per miner.
- Chapter 5 is about threshold linear secret sharing schemes. We characterise threshold linear secret sharing schemes, and develop an algorithm to generate all $(t+1)$-out-of-n threshold linear secret sharing schemes over a field $\mathbb{Z}_p$. Further, we prove the non-existence of $(t+1)$-out-of-n threshold linear secret sharing schemes over $\mathbb{Z}_{2^{32}}$ with one share per miner for $n > t+1$.

Chapter 2

Preliminaries

2.1 Fields and Rings

Secret sharing schemes are usually defined over finite fields. We will extend this definition to commutative rings, and define black box secret sharing schemes over arbitrary Abelian groups. In this section, we will define Abelian groups, commutative rings, and fields.

Definition 2.1.1 An *Abelian group* $(\mathbb{G}; \star)$ is a set $\mathbb{G}$ together with a binary operation $\star : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$, such that the following hold:

- (Associativity)
  $\forall a, b, c \in \mathbb{G}, (a \star b) \star c = a \star (b \star c)$
- (Commutativity)
  $\forall a, b \in \mathbb{G}, a \star b = b \star a$
- (Identity element)
  $\exists e \in \mathbb{G}$ s.t. $\forall a \in \mathbb{G}, a \star e = e \star a = a$
- (Inverse element)
  $\forall a \in \mathbb{G}, \exists a^{-1} \in \mathbb{G}$ s.t. $a \star a^{-1} = a^{-1} \star a = e$

Definition 2.1.2 Let $\mathbb{G}$ be a group. A set $\mathbb{H}$ is said to be a *subgroup* of $\mathbb{G}$ if $\mathbb{H} \subset \mathbb{G}$ and $(\mathbb{H}; \star)$ is a group.

Definition 2.1.3 Let $(\mathbb{G}; \star)$ be an Abelian group, and let $\mathbb{H}$ be a subgroup of $\mathbb{G}$. Let $g \in \mathbb{G}$. The set $g \star \mathbb{H} = \{g \star h : h \in \mathbb{H}\}$ is said to be a *coset* of $\mathbb{G}$.

Definition 2.1.4 Let $(\mathbb{G}; \star)$ be an Abelian group, and let $\mathbb{H}$ be a subgroup of $\mathbb{G}$. The set $\mathbb{G}/\mathbb{H} = \{g \star \mathbb{H} : g \in \mathbb{G}\}$ is said to be a *quotient group* of $\mathbb{G}$.

Definition 2.1.5 A *group homomorphism* is a map $\phi : \mathbb{G} \to \mathbb{H}$ from a group $(\mathbb{G}; \star)$ to a group $(\mathbb{H}; \bullet)$ such that $\phi(a \star b) = \phi(a) \bullet \phi(b)$ for all $a, b \in \mathbb{G}$.

Definition 2.1.6 An *automorphism* is a group homomorphism from a group $\mathbb{G}$ to itself.

Definition 2.1.7 A group $(\mathbb{G}; \star)$ is said to be *cyclic* if there exists $g \in \mathbb{G}$ such that for all $a \in \mathbb{G}$, there exists $k \in \mathbb{N}$ such that $a = \underbrace{g \star g \star \cdots \star g}_{\text{k times}}$.

We say that g generates $\mathbb{G}$.

Definition 2.1.8 A characteristic subgroup of a group $\mathbb{G}$ is a subgroup $\mathbb{H}$ of $\mathbb{G}$ such that for each automorphism $\phi : \mathbb{G} \to \mathbb{G}$, $\phi(\mathbb{H}) = \mathbb{H}$.

Fact 2.1.9 *Every subgroup of a cyclic group is characteristic.*

The platform SHAREMIND is defined over the group $\mathbb{Z}_{2^{32}}$. We will use Corollary 2.1.12 below to prove the non-existence of certain secret sharing schemes over $\mathbb{Z}_{2^{32}}$.

Fact 2.1.10 *Let $n, k \in \mathbb{N}$. Then $(\mathbb{Z}_k; +)$ is a subgroup of $(\mathbb{Z}_n; +)$ if and only if k is a divisor of n.*

Fact 2.1.11 *$(\mathbb{Z}_n; +)$ is a cyclic group with generator 1 for all $n \in \mathbb{N}$.*

The following is a corollary of Facts 2.1.10, 2.1.11, and 2.1.9.

Corollary 2.1.12 *Let $n, k \in \mathbb{N}$. Then $(\mathbb{Z}_k; +)$ is a characteristic subgroup of $(\mathbb{Z}_n; +)$ if and only if k is a divisor of n.*

Definition 2.1.13 A *commutative ring* is a set $\mathbb{L}$ together with two binary operations addition $+ : \mathbb{L} \times \mathbb{L} \to \mathbb{L}$ and multiplication $\cdot : \mathbb{L} \times \mathbb{L} \to \mathbb{L}$, such that the following hold:

- $(\mathbb{L}; +)$ is an Abelian group with identity element 0
- (Associativity of multiplication)
  $\forall a, b, c \in \mathbb{L}, (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- (Commutativity of multiplication)
  $\forall a, b \in \mathbb{L}, a \cdot b = b \cdot a$
- (Identity element of multiplication)
  $\exists 1 \in \mathbb{L}$ s.t. $\forall a \in \mathbb{L}, a \cdot 1 = 1 \cdot a = a$
- (Distributivity)
  $\forall a, b, c \in \mathbb{L}$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

In this thesis, we will give examples of secret sharing schemes over the ring $\mathbb{Z}_N$.

Definition 2.1.14 Let $\mathbb{L}$ be a commutative ring. A set $\mathbb{M}$ is said to be a *subring* of $\mathbb{L}$ if $(\mathbb{M}; +)$ is a subgroup of $(\mathbb{L}; +)$, $1 \in \mathbb{M}$, and for all $a, b \in \mathbb{M}$, $a \cdot b \in \mathbb{M}$.

Definition 2.1.15 Let $\mathbb{L}$ be a commutative ring. If there exists a positive integer N such that $\underbrace{1 + \cdots + 1}_{N \text{ times}} = 0$ the *characteristic* of $\mathbb{L}$ is defined to be the smallest such N. If for all positive integers N, $\underbrace{1 + \cdots + 1}_{N \text{ times}} \neq 0$, we define the characteristic of $\mathbb{L}$ to be zero. We denote the characteristic of $\mathbb{L}$ by $\operatorname{char} \mathbb{L}$.

Fact 2.1.16 *The characteristic of a finite commutative ring is non-zero.*

Definition 2.1.17 Let $(\mathbb{L}; +, \cdot)$ be a commutative ring. An element $a \in \mathbb{L}$ is said to be *invertible* if there exists a (unique) element $b \in \mathbb{L}$ such that $a \cdot b = 1$. We say that b is the *inverse* of a.

Definition 2.1.18 Let $(\mathbb{L}; +, \cdot)$ be a commutative ring. A non-zero element $a \in \mathbb{L}$ is said to be a *zero divisor* if there exists a non-zero element $b \in \mathbb{L}$ such that $a \cdot b = 0$.

We will denote the number of zero divisors in a ring $\mathbb{L}$ by $ZD(\mathbb{L})$.

Fact 2.1.19 *Let $(\mathbb{L}; +, \cdot)$ be a finite commutative ring. Then $a \in \mathbb{L}$ is a zero divisor if and only if a is not invertible.*

The ring $\mathbb{Z}_N$ is an example of a finite commutative ring with characteristic N. The zero divisors of $\mathbb{Z}_N$ are those $a \in \mathbb{Z}_N$ such that a and N have a non-trivial common divisor. An element $a \in \mathbb{Z}_N$ is invertible if and only if the greatest common divisor of a and N is 1.

Definition 2.1.20 A *field* is a set $\mathbb{K}$ together with two binary operations addition $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ and multiplication $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$, such that the following hold:

- $(\mathbb{K}; +, \cdot)$ is a commutative ring
- (Inverse element of multiplication)
  $\forall a \in \mathbb{K} \exists a^{-1} \in \mathbb{K}$ s.t. $a \cdot a^{-1} = a^{-1} \cdot a = 1$

In this thesis, for all examples $\mathbb{K} = \mathbb{Z}_p$, where p is a prime.

2.2 Vector Spaces and Modules

In this section we will define vector spaces, which are defined over fields, and modules, which are defined over commutative rings. For a linear secret sharing scheme, the set of all shares is a vector space or a module. The set of shares for the secret 0 is a subspace of the vector space of all shares or a submodule of the module of all shares.

Definition 2.2.1 A vector space over a field $\mathbb{K}$ is a set $\mathbb{V}$ together with two binary operations addition $+ : \mathbb{V} \times \mathbb{V} \to \mathbb{V}$ and scalar multiplication $\cdot : \mathbb{K} \times \mathbb{V} \to \mathbb{V}$, such that the following hold:

- $(\mathbb{V}; +)$ is an Abelian group with identity element 0
- (Distributivity)
  1. $\forall \boldsymbol{v}, \boldsymbol{w} \in \mathbb{V}, a \in \mathbb{K}$, $a \cdot (\boldsymbol{v} + \boldsymbol{w}) = (a \cdot \boldsymbol{v}) + (a \cdot \boldsymbol{w})$, and
  2. $\forall \boldsymbol{v} \in \mathbb{V}, a, b \in \mathbb{K}$, $(a + b) \cdot \boldsymbol{v} = (a \cdot \boldsymbol{v}) + (b \cdot \boldsymbol{v})$
- $\forall \boldsymbol{v} \in \mathbb{V}, a, b \in \mathbb{K}$, $(a \cdot b) \cdot \boldsymbol{v} = a \cdot (b \cdot \boldsymbol{v})$
- $\forall \boldsymbol{v} \in \mathbb{V}, 1 \cdot \boldsymbol{v} = \boldsymbol{v}$

An element of $\mathbb{V}$ is called a *vector*.

In the following, we will consider the vector space $\mathbb{V} = \mathbb{K}^n$ for some $n < \infty$. A vector $\boldsymbol{v} \in \mathbb{K}^n$ is denoted by the tuple $(v_1, \ldots, v_n)$, with $v_1, \ldots, v_n \in \mathbb{K}$.

Notation 2.2.2 *We denote the vector* $(1, 1, \ldots, 1)$ *by* $\mathbf{1}$. *The ith* unit vector $(0, \ldots, 0, 1, 0, \ldots, 0)$ *with the ith element equal to 1 and all other elements equal to 0 is denoted by* $\boldsymbol{e_i}$.

Definition 2.2.3 Let $\mathbb{V}$ be a $\mathbb{K}$-vector space. A set $\mathbb{W}$ is said to be a *subspace* of $\mathbb{V}$ if $\mathbb{W} \subset \mathbb{V}$ and $(\mathbb{W}; +, \cdot)$ is a $\mathbb{K}$-vector space.

In this thesis, we will consider the vector space $\mathbb{Z}_p^n$ and its subspaces.

Definition 2.2.4 Let $(\mathbb{V}; +, \cdot)$ be a vector space, and let $\mathbb{W}$ be a subspace of $\mathbb{V}$. The set $\mathbb{V}/\mathbb{W} = \{\boldsymbol{v} + \mathbb{W} : v \in \mathbb{V}\}$ is said to be a *quotient space* of $\mathbb{V}$.

Definition 2.2.5 A *module* $\mathbb{M}$ over the commutative ring $\mathbb{L}$ is a set $\mathbb{M}$ together with two binary operations addition $+ : \mathbb{M} \times \mathbb{M} \to \mathbb{M}$ and scalar multiplication $\cdot : \mathbb{L} \times \mathbb{M} \to \mathbb{M}$, such that the following hold:

- $(\mathbb{M}; +)$ is an Abelian group with identity element 0
- (Distributivity)
  1. $\forall \boldsymbol{v}, \boldsymbol{w} \in \mathbb{M}, a \in \mathbb{L}$, $a \cdot (\boldsymbol{v} + \boldsymbol{w}) = (a \cdot \boldsymbol{v}) + (a \cdot \boldsymbol{w})$, and

2. $\forall \boldsymbol{v} \in \mathbb{M}, a, b \in \mathbb{L}$, $(a+b) \cdot \boldsymbol{v} = (a \cdot \boldsymbol{v}) + (b \cdot \boldsymbol{v})$

- $\forall \boldsymbol{v} \in \mathbb{M}, a, b \in \mathbb{L}$, $(a \cdot b) \cdot \boldsymbol{v} = a \cdot (b \cdot \boldsymbol{v})$
- $\forall \boldsymbol{v} \in \mathbb{M}, 1 \cdot \boldsymbol{v} = \boldsymbol{v}$

In the following, we will consider the module $\mathbb{M} = \mathbb{L}^n$ for some $n < \infty$. We denote an element $\boldsymbol{v} \in \mathbb{M}$ by the tuple $(v_1, \ldots, v_n)$, with $v_1, \ldots, v_n \in \mathbb{L}$.

Fact 2.2.6 *Every Abelian group $\mathbb{G}$ is a $\mathbb{Z}$-module.*

Definition 2.2.7 Let $\mathbb{M}$ be an $\mathbb{L}$-module. A set $\mathbb{O}$ is said to be a *submodule* of $\mathbb{M}$ if $\mathbb{O} \subset \mathbb{M}$ and $(\mathbb{O}; +, \cdot)$ is an $\mathbb{L}$-module.

We will in this thesis consider the module $\mathbb{Z}_N^n$ and its submodules.

Definition 2.2.8 Let $(\mathbb{M}; +, \cdot)$ be a module, and let $\mathbb{O}$ be a submodule of $\mathbb{M}$. The set $\mathbb{M}/\mathbb{O} = \{\boldsymbol{v} + \mathbb{O} : v \in \mathbb{M}\}$ is said to be a *quotient module* of $\mathbb{M}$.

Definition 2.2.9 Let $\mathbb{V}$ be a vector space, and let $\boldsymbol{v_1}, \ldots, \boldsymbol{v_n} \in \mathbb{V}$. The vectors $\boldsymbol{v_1}, \ldots, \boldsymbol{v_n}$ are said to be *linearly independent* if

$$\alpha_1 \boldsymbol{v_1} + \cdots + \alpha_n \boldsymbol{v_n} = \boldsymbol{0} \Rightarrow \alpha_1 = \cdots = \alpha_n = 0$$

Definition 2.2.10 Let $\mathbb{V}$ be a vector space, and let $\boldsymbol{v_1}, \ldots, \boldsymbol{v_n} \in \mathbb{V}$. The vectors $\boldsymbol{v_1}, \ldots, \boldsymbol{v_n}$ are said to *span* $\mathbb{V}$ if for all $\boldsymbol{v} \in \mathbb{V}$, there exist $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ such that $\boldsymbol{v} = \alpha_1 \boldsymbol{v_1} + \cdots + \alpha_n \boldsymbol{v_n}$. We say that the set $\{\boldsymbol{v_1}, \ldots, \boldsymbol{v_n}\}$ is a *spanning set* of $\mathbb{V}$.

Definition 2.2.11 Let $\mathbb{V}$ be a vector space, and let X be a subset of $\mathbb{V}$. We define the *span* of X to be the intersection of all subspaces of $\mathbb{V}$ containing X. The span of X is denoted by $\operatorname{span} X$.

Definition 2.2.12 Let $\mathbb{V}$ be a vector space, and let $\boldsymbol{v_1}, \ldots, \boldsymbol{v_n} \in \mathbb{V}$. The set $V = \{\boldsymbol{v_1}, \ldots, \boldsymbol{v_n}\}$ is said to be a *basis* of $\mathbb{V}$ if the vectors $\boldsymbol{v_1}, \ldots, \boldsymbol{v_n}$ are linearly independent and span $\mathbb{V}$.

We define linear independence, spanning set, and basis analogously for modules.

Fact 2.2.13 *Every vector space has a basis.*

Fact 2.2.14 *Let $\mathbb{V}$ be a vector space. For any two bases V_1 and V_2 of $\mathbb{V}$, $|V_1| = |V_2|$.*

Fact 2.2.15 *Not every module has a basis.*

Fact 2.2.16 *Let $\mathbb{M}$ be a module. For any two bases M_1 and M_2 of $\mathbb{M}$, $|M_1| = |M_2|$.*

Definition 2.2.17 Let $\mathbb{V}$ be a vector space over a field $\mathbb{K}$, and let V be a basis of $\mathbb{V}$. The *rank* of $\mathbb{V}$ is defined to be $|V|$.

Notation 2.2.18 *We denote the rank of a vector space $\mathbb{V}$ by* $\dim \mathbb{V}$.

For a module $\mathbb{M}$, we define the rank of $\mathbb{M}$ to be $\dim \mathbb{M} = |M|$ if $\mathbb{M}$ has a basis M.

Notation 2.2.19 *For two vectors $\boldsymbol{u}$ and $\boldsymbol{v}$, $\boldsymbol{u} \cdot \boldsymbol{v}$ denotes the standard inner product of $\boldsymbol{u}$ and $\boldsymbol{v}$. By $\boldsymbol{u} \star \boldsymbol{v}$, we denote the coordinatewise product of $\boldsymbol{u}$ and $\boldsymbol{v}$.*

Definition 2.2.20 Let $\mathbb{V}$ be a vector space, and let $\mathbb{W}$ be a subspace of $\mathbb{V}$. The *orthogonal complement* of $\mathbb{W}$ is defined to be the set $\mathbb{W}^{\perp} = \{\boldsymbol{v} \in \mathbb{V} : \boldsymbol{v} \cdot \boldsymbol{w} = 0 \text{ for all } \boldsymbol{w} \in \mathbb{W}\}$.

We define the orthogonal complement of a module $\mathbb{M}$ analogously.

Fact 2.2.21 *Let $\mathbb{V}$ be a finite dimensional vector space. Then $(\mathbb{V}^{\perp})^{\perp} = \mathbb{V}$.*

Fact 2.2.22 *Let $\mathbb{V}$ and $\mathbb{W}$ be finite dimensional vector spaces. Then*

$$\mathbb{W} \subset \mathbb{V} \Leftrightarrow \mathbb{V}^{\perp} \subset \mathbb{W}^{\perp}$$

2.3 Matrices

A linear secret sharing scheme may be defined in terms of matrices and vectors. A share in a linear secret sharing scheme is defined as the product of a matrix with elements in a field or a ring and a vector with elements in a field or a ring. In this section, we define matrices and matrix operations.

Notation 2.3.1 *Let M be a matrix. We denote the ith row of M by M_i, and by M^j we denote the jth column of M. The element in the ith row and in the jth column of M is denoted by m_{ij}.*

Notation 2.3.2 *For a vector $\boldsymbol{v}$ and a matrix M with e columns, $\boldsymbol{v} \star M$ denotes the matrix $(\boldsymbol{v} \star M^1 || \cdots || \boldsymbol{v} \star M^e)$. For a matrix M with e columns and a matrix N with f columns, $M \star N$ denotes the matrix $(M^1 \star N^1 || M^1 \star N^2 || \cdots || M^1 \star N^f || \cdots || M^e \star N^1 || M^e \star N^2 || \cdots || M^e \star N^f)$.*

Definition 2.3.3 The *column rank* of a matrix M is defined to be the number of linearly independent columns of M. The *row rank* of a matrix M is defined to be the number of linearly independent rows of M.

Fact 2.3.4 *The column rank and the row rank of a matrix M are equal.*

Notation 2.3.5 *We denote the rank of a matrix M by* $\operatorname{rank} M$.

Definition 2.3.6 We say that a matrix $M \in \mathbb{L}^{d\times e}$ has *full rank* if $\operatorname{rank} M = \min\{d, e\}$.

Fact 2.3.7 *A square matrix M has full rank if and only if it is invertible.*

Fact 2.3.8 *A square matrix M has full rank if and only if its determinant is invertible.*

Definition 2.3.9 The *image* of a matrix $M \in \mathbb{L}^{d\times e}$ is defined to be the set $\operatorname{Im} M = \{\boldsymbol{w} \in \mathbb{L}^d : \exists \boldsymbol{v} \in \mathbb{L}^e \text{ s.t. } M\boldsymbol{v} = \boldsymbol{w}\}$. The *kernel* of a matrix $M \in \mathbb{L}^{d\times e}$ is defined to be the set $\operatorname{Ker} M = \{\boldsymbol{v} \in \mathbb{L}^e : M\boldsymbol{v} = \boldsymbol{0}\}$.

Fact 2.3.10 $\operatorname{Im} M$ *is a submodule of* $\mathbb{L}^d$, *and* $\operatorname{Ker} M$ *is a submodule of* $\mathbb{L}^e$.

Fact 2.3.11 (Rank-nullity theorem) *Let M be a matrix with n columns over a field $\mathbb{K}$. Then* $\operatorname{rank} M + \dim \operatorname{Ker} M = n$.

Definition 2.3.12 The *transpose* of a $d \times e$ matrix $M = (m_{ij})$ is defined to be the $e \times d$ matrix $M^T = (m_{ji})$.

Fact 2.3.13 *Let M be a matrix over a ring $\mathbb{L}$.* $(\operatorname{Im} M^T)^\perp = \operatorname{Ker} M$.

Fact 2.3.14 *Let M be a matrix over a ring $\mathbb{L}$.* $\operatorname{Im} M^T \subset (\operatorname{Ker} M)^\perp$.

Fact 2.3.15 *Let M be a matrix over a field $\mathbb{K}$.* $\operatorname{Im} M^T = (\operatorname{Ker} M)^\perp$.

Note that if M is a matrix over a ring $\mathbb{L}$, then in general $\operatorname{Im} M^T \neq (\operatorname{Ker} M)^\perp$. Consider $\mathbb{L} = \mathbb{Z}$, and $M = \begin{pmatrix} 2 & 0 \end{pmatrix}^T$. Then $\operatorname{Im} M^T = \{2a : a \in \mathbb{Z}\}$, and $(\operatorname{Ker} M)^\perp = \mathbb{Z}$.

Definition 2.3.16 An *elementary row operation* on a matrix M is one of the following three operations on M:

- Row switching: $R_i \leftrightarrow R_j$
- Row multiplication: $R_i \to \alpha R_i$, where α is an invertible scalar
- Row addition: $R_i \to R_i + \alpha R_j$, where α is a non-zero scalar

We define elementary column operations analogously.

Fact 2.3.17 *If a square matrix M has full rank then it can be converted to the identity matrix with elementary row operations.*

Similarly, if a matrix M has full rank, then it can be converted to the identity matrix with elementary column operations.

Fact 2.3.18 *Elementary row or column operations do not change the rank of a matrix.*

Fact 2.3.19 *Let $N \in \mathbb{Z}^{a \times b}$. Then the linear system of equations $N\boldsymbol{x} = \boldsymbol{y}$ is solvable over $\mathbb{Z}$ if and only if it is solvable over $\mathbb{Z}_m$ for all integers $m \neq 0$ [10].*

2.4 Boolean Functions

In a secret sharing scheme, only certain subsets of players, the qualified subsets, should be able to reconstruct the secret from their shares, while any other subsets of players, the unqualified subsets, should not be able to deduce any information about the secret from their shares. The set of qualified subsets is called the access structure of the secret sharing scheme, and the set of unqualified subsets is called the adversary structure. The access and adversary structures of a secret sharing scheme may be defined in terms of a Boolean function. In this section, we will define Boolean functions.

Let n be a positive integer.

Definition 2.4.1 A *Boolean function* $f : \{0,1\}^n \rightarrow \{0,1\}$ is a function which maps n-bit strings to 0 or 1. The function f is said to be *monotone* if for all a_i, $b_i \in \{0,1\}$ such that $a_1 \leq b_1, \ldots, a_n \leq b_n, f(a_1 \cdots a_n) \leq f(b_1 \cdots b_n)$.

We denote by I_A the bit string whose ith bit is 1 if $i \in A$, and 0 if $i \notin A$. We will denote $f(I_A)$ simply by $f(A)$.

Definition 2.4.2 Let $f : \{0,1\}^n \rightarrow \{0,1\}$ be a monotone Boolean function. The *adversary structure* $\mathcal{A}$ of f is defined to be the set of bit strings A such that $f(A) = 0$. The *access structure* Γ of f is defined to be the set of bit strings A such that $f(A) = 1$.

Notation 2.4.3 *For a set $A \subset \{1, \ldots, n\}$, we will denote the complement of A by $\overline{A} = \{1, \ldots, n\} \setminus A$.*

Definition 2.4.4 Let $f : \{0,1\}^n \rightarrow \{0,1\}$ be a monotone Boolean function. Its *dual* $f^\star$ is defined by $f^\star(A) = \overline{f(\overline{A})}$.

Definition 2.4.5 Let $f : \{0,1\}^n \rightarrow \{0,1\}$ be a monotone Boolean function. f is said to be Q2 if for all A, $A' \subset \{1, \ldots, n\}$ such that $f(A) = f(A') = 0$, $A \cup A' \neq \{1, \ldots, n\}$. f is said to be Q3 if for all A, A', $A'' \subset \{1, \ldots, n\}$ such that $f(A) = f(A') = f(A'') = 0$, $A \cup A' \cup A'' \neq \{1, \ldots, n\}$.

Definition 2.4.6 Let Γ be an access structure, and let $\mathcal{A} = \overline{\Gamma}$ be an adversary structure. Γ is said to be *Q2* if for all sets A, $A' \in \mathcal{A}$ $A \cup A' \neq \{1, \ldots, n\}$. If for all sets A, A, $A'' \in \mathcal{A}$ $A \cup A' \cup A'' \neq \{1, \ldots, n\}$, Γ is said to be *Q3*.

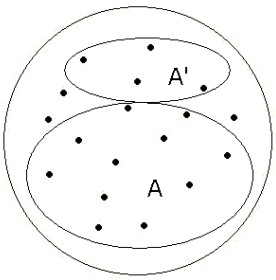

Figure 2.1: Q2

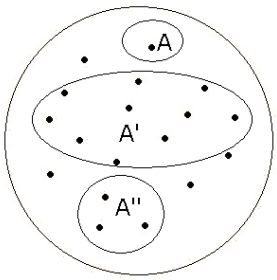

Figure 2.2: Q3

2.5 Probability

The security of a secret sharing scheme is defined in terms of probability distributions. A perfect secret sharing scheme is secure if for any two possible secrets s and s' and corresponding sets of shares, it is not possible for the unqualified subsets of players to deduce from their sets of shares for each secret which secret the shares correspond to: the sets of shares are identically distributed. In this section, we will define probability spaces, discrete random variables, elementary events, observable events, and probability distributions.

Definition 2.5.1 A *probability space* is a triple $(\Omega, \mathcal{F}(\Omega), \Pr)$, where Ω is a set, $\mathcal{F}(\Omega)$ is a set of subsets of Ω that is closed under complementation and countable unions, and a measure Pr on $(\Omega, \mathcal{F}(\Omega))$ such that $\Pr(\Omega) = 1$.

Definition 2.5.2 Let $(\Omega, \mathcal{F}(\Omega), \Pr)$ be a probability space. A *discrete random variable* is a measurable function $f : \Omega \to \{0, 1\}^\star$.

Definition 2.5.3 Let $(\Omega, \mathcal{F}(\Omega), \Pr)$ be a probability space, and let f be a random variable. An *elementary event* is a set $\Omega_y = \{\omega \in \Omega : f(\omega) = y\}$.

Definition 2.5.4 Let $(\Omega, \mathcal{F}(\Omega), \Pr)$ be a probability space, and let f be a random variable. An *observable event* $X \in \mathcal{F}(\Omega)$ is a union of elementary events, the empty set $\emptyset$, or the set Ω itself.

Definition 2.5.5 A *probability distribution* is a probability measure $\Pr : \mathcal{F}(\Omega) \rightarrow [0,1]$ that assigns a probability $\Pr[X] \in [0,1]$ to each observable event X such that

1. $\Pr[\{\}] = 0$
2. $\Pr[\Omega] = 1$
3. $\Pr[X_1 \cup X_2] = \Pr[X_1] + \Pr[X_2]$ if X_1 and X_2 are mutually exclusive

Definition 2.5.6 Let f and g be two random variables. We say that f and g are *identically distributed* if f and g have the same probability distribution.

Notation 2.5.7 *Let f and g be two random variables that are identically distributed. We will denote this by $f \equiv g$.*

Definition 2.5.8 Let $(\Omega, \mathcal{F}(\Omega), \Pr)$ be a probability space. The *statistical distance* between two random variables $f, g : \Omega \rightarrow \{0,1\}^\star$ is defined to be $\mathrm{SD}(f,g) = \frac{1}{2}\sum_{y \in \{0,1\}^\star} |\Pr[\omega \in \Omega : f(\omega) = y] - \Pr[\omega \in \Omega : g(\omega) = y]|$.

2.6 Polynomial Interpolation

Shamir's secret sharing scheme, defined over a field $\mathbb{K}$, is one of the oldest linear secret sharing schemes. Shamir's secret sharing scheme is a special case of linear secret sharing schemes – defined over a ring $\mathbb{L}$ – based on polynomial interpolation. In this section, we will define interpolation polynomials and Vandermonde matrices.

Definition 2.6.1 Let

$$V = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ 1 & \alpha_3 & \alpha_3^2 & \cdots & \alpha_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_m & \alpha_m^2 & \cdots & \alpha_m^{n-1} \end{pmatrix},$$

denoted by $V(\alpha_1, \ldots, \alpha_n)$, be an $m \times n$ matrix with $\alpha_i \in \mathbb{L}$ for all $1 \leq i \leq m$. V is said to be a *Vandermonde matrix*.

Fact 2.6.2 *The determinant of a square Vandermonde matrix V is given by* $\det V = \prod_{n \geq k > j \geq 1}(\alpha_j - \alpha_k)$.

Note that this determinant is invertible if (and only if) $\alpha_i \neq \alpha_j$ is invertible for all $1 \leq i, j \leq n$. This means that V is invertible.

Fact 2.6.3 *Let*

$$V = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}$$

be a square Vandermonde matrix. Define

$$r_i(x) = \prod_{j=1, j\neq i}^{n} \frac{x-\alpha_j}{\alpha_i - \alpha_j} = r_{in}x^{n-1} + \cdots + r_{i2}x + r_{i1},\ 1 \leq i \leq n.$$

The inverse of V is given by

$$V^{-1} = \begin{pmatrix} r_{11} & r_{21} & r_{31} & \cdots & r_{n1} \\ r_{12} & r_{22} & r_{32} & \cdots & r_{n2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r_{1n} & r_{2n} & r_{3n} & \cdots & r_{nn} \end{pmatrix}.$$

Example 2.6.4 Let

$$V = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 \\ 1 & \alpha_2 & \alpha_2^2 \\ 1 & \alpha_3 & \alpha_3^2 \end{pmatrix}$$

be a 3×3 Vandermonde matrix. The inverse of V is given by

$$V^{-1} = \begin{pmatrix} \frac{\alpha_2\alpha_3}{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)} & \frac{\alpha_1\alpha_3}{(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)} & \frac{\alpha_1\alpha_2}{(\alpha_3-\alpha_1)(\alpha_3-\alpha_2)} \\ \frac{-(\alpha_2+\alpha_3)}{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)} & \frac{-(\alpha_1+\alpha_3)}{(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)} & \frac{-(\alpha_1+\alpha_2)}{(\alpha_3-\alpha_1)(\alpha_3-\alpha_1)} \\ \frac{1}{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)} & \frac{1}{(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)} & \frac{1}{(\alpha_3-\alpha_1)(\alpha_3-\alpha_2)} \end{pmatrix}.$$

Fact 2.6.5 (Lagrange's interpolation theorem) *Let $\mathbb{K}$ be a field, and let $\alpha_0, \ldots, \alpha_n, y_0, \ldots, y_n \in \mathbb{K}$ such that $\alpha_i \neq \alpha_j$ for all $i \neq j$. Then there exists precisely one polynomial f over $\mathbb{K}$ such that $\deg f \leq n$ and $f(\alpha_i) = y_i$ for all i, $0 \leq i \leq n$. In particular, $f(x) = y_0 r_0(x) + \cdots + y_n r_n(x)$, where $r_i(x) = \prod_{j=0, j\neq i}^{n} \frac{x-\alpha_j}{\alpha_i-\alpha_j}$, $0 \leq i \leq n$.*

Definition 2.6.6 The polynomial f is said to be an *interpolation polynomial*.

Note that

$$\begin{pmatrix} f_0 \\ \vdots \\ f_n \end{pmatrix} = V^{-1} \begin{pmatrix} y_0 \\ \vdots \\ y_n \end{pmatrix}.$$

Chapter 3

Linear Secret Sharing Schemes

The concept of secret sharing was introduced by A. Shamir [17] and G. Blakley [4] in 1979. In a secret sharing scheme, a dealer splits a secret s into d shares $s_1, \ldots, s_d$. Those shares are given to n players $P_1, \ldots, P_n$. Each player is given one or more shares. Only the qualified subsets of players are able to reconstruct s from their shares. Unqualified subsets of players should not be able to deduce any information about s from their shares.

The set of qualified subsets is called an access structure, and the set of unqualified subsets is called an adversary structure. Below, we formally define monotone access structures and monotone adversary structures.

Let $\mathcal{P} = \{1, \ldots, n\}$ denote the set of players, and let $2^{\mathcal{P}}$ denote the set of all subsets of $\mathcal{P}$.

Definition 3.0.7 A subset Γ of the power set $2^{\mathcal{P}}$ is called a *monotone access structure* on $\mathcal{P}$ if $\emptyset \notin \Gamma$, and if for any $A \in \Gamma$, any superset of A, $A' \in 2^{\mathcal{P}}$, is also in Γ. A subset $\mathcal{A}$ of $2^{\mathcal{P}}$ is called an *adversary structure* on $\mathcal{P}$ if $2^{\mathcal{P}} \setminus \mathcal{A}$ is a monotone access structure.

This means that for any qualified subset of players, a larger subset of players is also qualified. Analogously, for any unqualified subset of players, a smaller subset of players is unqualified as well.

In section 3.1, we will formally define secret sharing schemes, and in particular linear secret sharing schemes. Four linear secret sharing schemes will be introduced as examples: Shamir's secret sharing scheme, the additive scheme, the CNF-based scheme (or replicated secret sharing scheme), and the DNF-based scheme. In sections 3.2 and 3.3 we will characterise linear secret sharing schemes in two ways. Finally, we will present a partial order on linear secret sharing schemes in section 3.4. In this ordering, the CNF-based scheme is maximal, while the DNF-based scheme is minimal.

Secret sharing schemes are usually defined over finite fields. We will extend this definition to commutative rings. In the following, we will use $\mathbb{K}$ to denote a finite field. $\mathbb{L}$ will denote a commutative ring, and $\mathbb{G}$ will denote an Abelian group.

3.1 Functional Definition

Formally, a *secret sharing scheme* is defined by a tuple

$$\mathcal{S} = (\mathbb{L}, (\mathbb{L}^{d_1}, \ldots, \mathbb{L}^{d_n}), \mathsf{Share})$$

where $\mathbb{L}$ is a finite *secret domain*, each $\mathbb{L}^{d_i}$ is a finite *share domain* with $d_i > 0$ for all $1 \leq i \leq n$, and $\mathsf{Share} : \mathbb{L} \to \mathbb{L}^{d_1} \times \cdots \times \mathbb{L}^{d_n}$ is a randomised *share distribution function* which maps a secret $s \in \mathbb{L}$ to an n-tuple of share vectors $\boldsymbol{s} = (\boldsymbol{s_1}, \ldots, \boldsymbol{s_n})$. Each share vector $\boldsymbol{s_i}$ is a d_i-tuple of shares $(s_{i1}, \ldots, s_{id_i})$.

Let $d = d_1 + \cdots + d_n$. For a subset of players $A = \{i_1, \ldots, i_k\} \subseteq \mathcal{P}$, let $d_A = d_{i_1} + \cdots + d_{i_k}$, and let $\boldsymbol{s_A} = (\boldsymbol{s_{i_1}} || \cdots || \boldsymbol{s_{i_k}})$ be the concatenation of the share vectors $\boldsymbol{s_{i_j}}$, $1 \leq j \leq k$.

Let Γ be an access structure.

Definition 3.1.1 A secret sharing scheme is said to be *functional* if for all $A = \{i_1, \ldots, i_k\} \in \Gamma$, there exists a *reconstruction function* $\mathsf{Rec_A} : \mathbb{L}^{d_{i_1}} \times \cdots \times \mathbb{L}^{d_{i_k}} \to \mathbb{L}$ such that for any secret $s \in \mathbb{L}$,

$$\mathsf{Rec_A}(\mathsf{Share}(s)_A) = s$$

Definition 3.1.2 A secret sharing scheme is said to be *perfectly secure* if for all $A \notin \Gamma$ and for any secrets s, $s' \in \mathbb{L}$,

$$\mathsf{Share}(s)_A \equiv \mathsf{Share}(s')_A$$

A secret sharing scheme is said to be ϵ-*secure* if for all $A \notin \Gamma$ and for any secrets s, $s' \in \mathbb{L}$,

$$\mathrm{SD}(\mathsf{Share}(s)_A, \mathsf{Share}(s')_A) \leq \epsilon$$

In this thesis, we will say that a secret sharing scheme is secure if (and only if) it is perfectly secure.

In general, there exist both linear and non-linear secret sharing schemes. Most practical secret sharing schemes are, however, linear.

Definition 3.1.3 A secret sharing scheme is said to be *linear* if for all secrets s, t and all scalars $\alpha \in \mathbb{L}$,

$$\mathsf{Share}(\alpha s + t) \equiv \alpha \mathsf{Share}(s) + \mathsf{Share}(t)$$

.

In fact, if the share distribution function is linear, then the reconstruction function is linear, too.

Lemma 3.1.4 *Let $\mathcal{S}$ be a linear secret sharing scheme over a ring $\mathbb{L}$. For any $A \in \Gamma$, and for all secrets s, t and all scalars $\alpha \in \mathbb{L}$*

$$\mathsf{Rec}_\mathsf{A}(\alpha\mathsf{Share}(s)_A + \mathsf{Share}(t)_A) = \alpha\mathsf{Rec}_\mathsf{A}(\mathsf{Share}(s)_A) + \mathsf{Rec}_\mathsf{A}(\mathsf{Share}(t)_A)$$

Proof. Let $A \in \Gamma$. Let s, $t \in \mathbb{L}$ be two secrets, and let $\alpha \in \mathbb{L}$ be a scalar. By linearity of Share, $\alpha\mathsf{Rec}_\mathsf{A}(\mathsf{Share}(s)_A) + \mathsf{Rec}_\mathsf{A}(\mathsf{Share}(t)_A)$ $= \alpha s + t = \mathsf{Rec}_\mathsf{A}(\mathsf{Share}(\alpha s + t)_A) = \mathsf{Rec}_\mathsf{A}(\alpha\mathsf{Share}(s)_A + \mathsf{Share}(t)_A)$. ■

The additive secret sharing scheme (Fig. 3.1), the replicated secret sharing scheme, or CNF-based secret sharing scheme (Fig. 3.2), and the DNF-based secret sharing scheme (Fig. 3.3) are three examples of linear secret sharing schemes (LSSSs).

Additive secret sharing scheme. Let Γ be the trivial monotone access structure $\{\{1, \ldots, n\}\}$, and let $s \in \mathbb{L}$ be the secret to be shared. For each $i \in \{1, \ldots, n\}$, $r_i \in \mathbb{L}$ is picked at random from $\mathbb{L}$ such that $r_1 + \cdots + r_n = s$. Each player P_i is given the share r_i.

Clearly, the players in the only qualified subset $\{1, \ldots, n\}$ are able to reconstruct s together. Let $A \notin \Gamma$ be an unqualified subset. Let $|A| = k < n$. Wlog $A = \{1, \ldots, k\}$. For any $k < n$, the shares $r_1, \ldots, r_k$ are uniformly distributed. Hence, $\mathsf{Share}(s)_A \equiv \mathsf{Share}(s')_A$ for all $s' \in \mathbb{L}$.

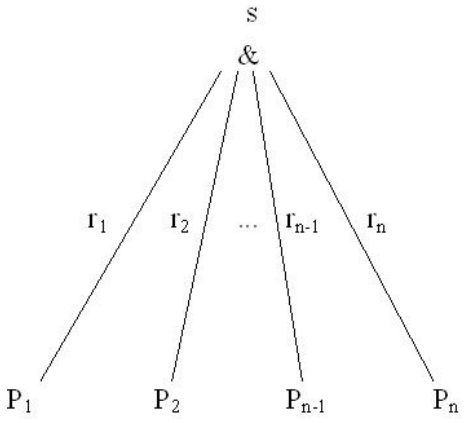

Figure 3.1: Additive scheme

CNF-based secret sharing scheme, or replicated secret sharing scheme $\mathcal{R}_\Gamma$. Let Γ be a monotone access structure, and let $\mathcal{T}$ be the set of all maximal unqualified subsets $T \in \overline{\Gamma}$. Let $s \in \mathbb{L}$ be the secret to

be shared. For each $T \in \mathcal{T}$, $r_T \in \mathbb{L}$ is picked at random from $\mathbb{L}$ such that $\sum_{T \in \mathcal{T}} r_T = s$. Each player P_j is given the shares r_T such that $j \notin T$.

Let $A \in \Gamma$ be a qualified subset. By the monotonicity of Γ, $A \not\subset T$ for all $T \in \mathcal{T}$. Thus, for all $T \in \mathcal{T}$, there exists $j \in A$ such that $j \notin T$. In other words, for each $T \in \mathcal{T}$, there exists $j \in A$ such that player P_j is given share r_T. Hence, the players in A are able to reconstruct s together. Let $A \notin \Gamma$ be an unqualified subset, then $A \subset T$ for some $T \in \mathcal{T}$. Thus, none of the players in A is given share r_T. Hence, $\mathsf{Share}(s)_A \equiv \mathsf{Share}(s')_A$ for all $s' \in \mathbb{L}$.

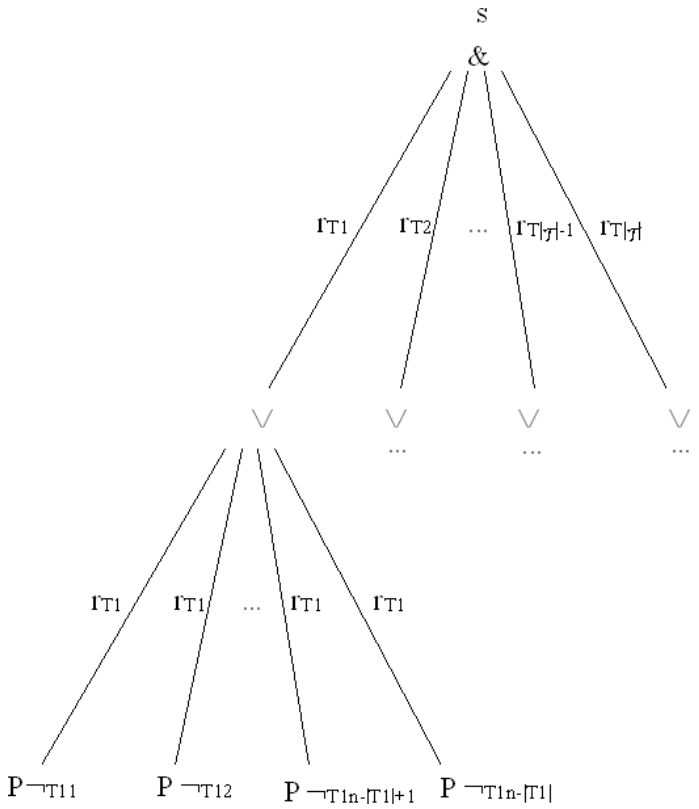

Figure 3.2: CNF-based scheme

DNF-based secret sharing scheme. Let Γ be a monotone access structure, and let $\mathcal{Q}$ be the set of all minimal qualified subsets $Q \in \Gamma$. Let $s \in \mathbb{L}$ be the secret to be shared. For each $Q \in \mathcal{Q}$, and for each $j \in Q$, r_{Qj} is randomly picked from $\mathbb{L}$ such that $\sum_{j \in Q} r_{Qj} = s$. Each player P_j is given the shares r_{Qj} such that $j \in Q$.

Let $A \in \Gamma$ be a qualified subset. Then $A \supseteq Q$ for some $Q \in \mathcal{Q}$. Thus, the players in A are able to reconstruct s. Let $A \notin \Gamma$ be an unqualified subset. By the monotonicity of Γ, $A \not\supseteq Q$ for all $Q \in \mathcal{Q}$. In other words, for each $Q \in \mathcal{Q}$, there exists a $j \in Q$ such that $j \notin A$. Thus, for each $Q \in \mathcal{Q}$,

there exists a share r_{Qj} such that no player in A is given r_{Qj}. Therefore, $\mathsf{Share}(s)_A \equiv \mathsf{Share}(s')_A$ for all $s' \in \mathbb{L}$.

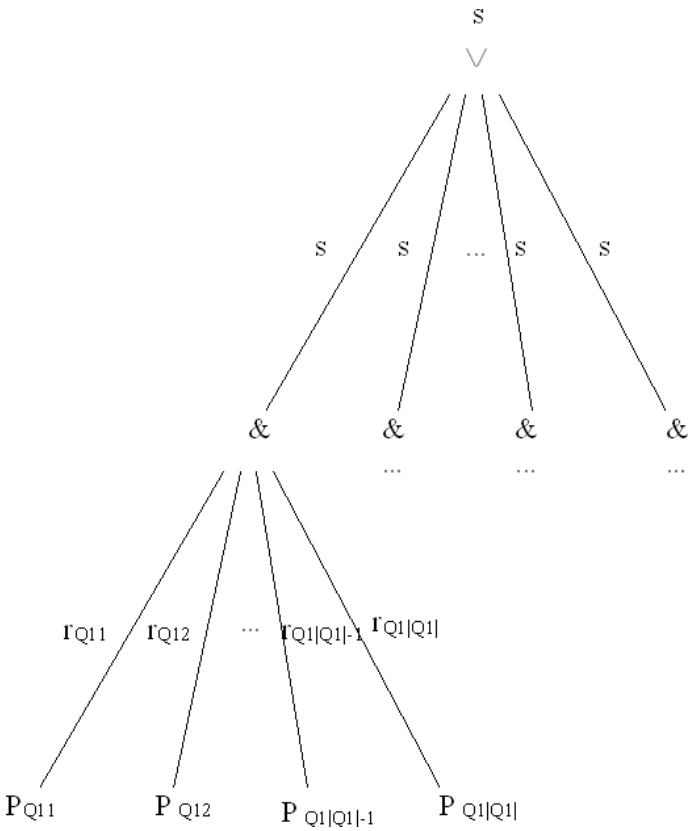

Figure 3.3: DNF-based scheme

Recall from linear algebra that a (deterministic) map α from an n-dimensional vector space $\mathbb{V}$ with basis $\{\boldsymbol{v_1}, \ldots, \boldsymbol{v}_n\}$ to an m-dimensional vector space $\mathbb{W}$ with basis $\{\boldsymbol{w_1}, \ldots, \boldsymbol{w_n}\}$ is linear if and only if there exists an $m \times n$ matrix M such that $\alpha(\boldsymbol{v_j}) = m_{1j}\boldsymbol{w_1} + \cdots + m_{mj}\boldsymbol{w_m}$ for all $1 \leq j \leq n$.

Over a field $\mathbb{K}$, the (non-deterministic) map Share is linear if and only there exist a matrix M with d rows and e columns whose first column is equal to a fixed share vector for the secret 1 and whose $e-1$ other columns form a basis of the span of the share vectors for the secret 0, and a vector $\boldsymbol{b}$ with e elements whose first element is equal to the secret s and whose $e-1$ other elements are random such that $\boldsymbol{s} = M\boldsymbol{b}$.

Lemma 3.1.5 *Let $\mathcal{S}$ be a linear secret sharing scheme over a commutative ring $\mathbb{L}$. Then $\mathbb{S} = \{\mathsf{Share}(s) : s \in \mathbb{L}\}$ is an $\mathbb{L}$-module, and $\mathsf{Share}(0)$ is a submodule of $\mathbb{S}$.*

Proof. By the linearity of $\mathcal{S}$, $\mathbb{S}$ is a module. Clearly, $\mathsf{Share}(0) \subset \mathbb{S}$. Again by the linearity of $\mathcal{S}$, $\mathsf{Share}(0)$ is a submodule of $\mathcal{S}$: Let $\boldsymbol{s}$, $\boldsymbol{t} \in \mathsf{Share}(0)$, and let $\alpha \in \mathbb{L}$. Then $\alpha\boldsymbol{s} \in \alpha\mathsf{Share}(0) \equiv \mathsf{Share}(\alpha 0) = \mathsf{Share}(0)$, and $\boldsymbol{s} + \boldsymbol{t} \in \mathsf{Share}(0) + \mathsf{Share}(0) \equiv \mathsf{Share}(0 + 0) = \mathsf{Share}(0)$. ■

Lemma 3.1.6 *Let $\mathcal{S}$ be a linear secret sharing scheme over a commutative ring $\mathbb{L}$. Let $\boldsymbol{m} \in \mathsf{Share}(1)$. Then for all $s \in \mathbb{L}$,*

$$\mathsf{Share}(s) \equiv s\boldsymbol{m} + \mathsf{Share}(0)$$

Proof. Let $\boldsymbol{s} \in \mathsf{Share}(s)$. Then $\boldsymbol{s} - s\boldsymbol{m} \in \mathsf{Share}(s) - s\mathsf{Share}(1) \equiv \mathsf{Share}(s - s1) = \mathsf{Share}(0)$ by linearity of $\mathcal{S}$. Hence, $\boldsymbol{s} \in s\boldsymbol{m} + \mathsf{Share}(0)$. Conversely, let $\boldsymbol{s} \in s\boldsymbol{m} + \mathsf{Share}(0)$. Then, $s\boldsymbol{m} + \mathsf{Share}(0) \subset s\mathsf{Share}(1) + \mathsf{Share}(0) \equiv \mathsf{Share}(s1 + 0) = \mathsf{Share}(s)$ by linearity of $\mathcal{S}$, and hence, $\boldsymbol{s} \in \mathsf{Share}(s)$. ■

A priori, by Fact 2.2.15, over a ring $\mathsf{Share}(0)$ may not have a basis. Over a field $\mathbb{K}$ however, $\mathsf{Share}(0)$ always has a basis by Fact 2.2.13.

Let e' be the rank of $\mathsf{Share}(0)$. Let $M' \in \mathbb{K}^{d \times e'}$ be a $d \times e'$-matrix whose e' columns are the e' basis vectors of $\mathsf{Share}(0)$. Fix $\boldsymbol{m} \in \mathsf{Share}(1)$. Let $s \in \mathbb{K}$, and let $\boldsymbol{s} \in \mathsf{Share}(s)$. By Lemma 3.1.6, $\boldsymbol{s} = \boldsymbol{m}s + M'\boldsymbol{b'}$, where $\boldsymbol{b'} \in \mathbb{K}^{e'}$ is a random e'-vector. Let $e = e' + 1$. Denote by $M \in \mathbb{K}^{d \times e}$ the concatenation $(\boldsymbol{m}||M')$, and by $\boldsymbol{b} \in \mathbb{K}^e$ the concatenation $(s||\boldsymbol{b'})$. This means that if

$$\boldsymbol{m} = \begin{pmatrix} m_1 \\ \vdots \\ m_d \end{pmatrix}, M' = \begin{pmatrix} m_{11} & \cdots & m_{1e-1} \\ \vdots & \ddots & \vdots \\ m_{d1} & \cdots & m_{de-1} \end{pmatrix}, \text{ and } \boldsymbol{b'} = \begin{pmatrix} b_1 \\ \vdots \\ b_{e-1} \end{pmatrix},$$

then

$$M = \begin{pmatrix} m_1 & m_{11} & \cdots & m_{1e-1} \\ \vdots & \vdots & \ddots & \vdots \\ m_d & m_{d1} & \cdots & m_{de-1} \end{pmatrix} \text{ and } \boldsymbol{b} = \begin{pmatrix} s \\ b_1 \\ \vdots \\ b_{e-1} \end{pmatrix}.$$

Finally, $\boldsymbol{s} = M\boldsymbol{b}$. We will say that M is a *share distribution matrix*. In the following, we will often define a linear secret sharing scheme over a field directly by $\boldsymbol{s} = M\boldsymbol{b}$, and denote it by $\mathcal{S}_M = (\mathbb{K}, M)$. We will denote the set $\{\mathsf{Share}_{\mathcal{S}_M}(s) : s \in \mathbb{K}\}$ by $\mathbb{S}_M$.

For a matrix M with d rows and e columns, let M_i be the matrix consisting of the d_i rows j of M such that share s_{ij} is given to player P_i. For $A = \{i_1, \ldots, i_k\} \subseteq \mathcal{P}$, we denote by M_A the $d_A \times e$-matrix

$$M_A = \begin{pmatrix} M_{i_1} \\ \vdots \\ M_{i_k} \end{pmatrix}.$$

Similarly, for a vector $\boldsymbol{m}$ with d elements, we denote by $\boldsymbol{m_i}$ the vector consisting of the d_i elements j of $\boldsymbol{m}$ such that share s_{ij} is given to player P_i, and for $A = \{i_1, \ldots, i_k\} \subseteq \mathcal{P}$ we denote by $\boldsymbol{m_A}$ the d_A-vector

$$\boldsymbol{m_A} = \begin{pmatrix} m_{i_1} \\ \vdots \\ m_{i_k} \end{pmatrix}.$$

Note that by Lemma 3.1.6, $\mathsf{Share}(1) = \boldsymbol{m} + \mathsf{Share}(0)$. This means that we can always replace the first column of M by linear combinations $\boldsymbol{m} + \gamma_1 M'^1 + \cdots \gamma_{e-1} M'^{e-1}$ of $\boldsymbol{m}$ and the $e-1$ columns of M'. Similarly, we can always replace M' by $M'C$, where C is an invertible $(e-1) \times (e-1)$ matrix.

Lemma 3.1.7 *Let $\mathcal{S}$ be a linear secret sharing scheme over a ring $\mathbb{L}$. Let $A \in \Gamma$. If there exists a vector $\boldsymbol{r_A} \in \mathbb{L}^{d_A}$ such that $\boldsymbol{r_A} \cdot \boldsymbol{m_A} = 1$ and such that $\boldsymbol{r_A} \cdot \boldsymbol{z} = 0$ for all $\boldsymbol{z} \in \mathsf{Share}(0)_A$, then $\boldsymbol{r_A} \cdot \boldsymbol{s_A} = s$ for all $s \in \mathbb{L}$ and $\boldsymbol{s_A} \in \mathsf{Share}(s)_A$.*

Proof. Let $s \in \mathbb{L}$, and let $\boldsymbol{s_A} \in \mathsf{Share}(s)_A$. By Lemma 3.1.6, there exists $\boldsymbol{z} \in \mathsf{Share}(0)_A$ such that $\boldsymbol{s_A} = s\boldsymbol{m_A} + \boldsymbol{z}$. Then, $\boldsymbol{r_A} \cdot \boldsymbol{s_A} = s(\boldsymbol{r_A} \cdot \boldsymbol{m_A}) + \boldsymbol{r_A} \cdot \boldsymbol{z} = s \cdot 1 + 0 = s$. ■

Note that if $\boldsymbol{r_A} \cdot \boldsymbol{m_A} = z$ and z is a zero divisor, then the players in A are able to reconstruct s partially: $s \in \{s' : zs' = \boldsymbol{r_A} \cdot \boldsymbol{s_A}\}$. Over a field, there are no zero divisors, and a subset of players can either reconstruct the whole secret or deduce no information at all about s.

Lemma 3.1.8 *Let $\mathcal{S}$ be a linear secret sharing scheme over a field $\mathbb{K}$. Let $A \in \Gamma$. Then there exists a vector $\boldsymbol{r_A} \in \mathbb{L}^{d_A}$ such that $\boldsymbol{r_A} \cdot \boldsymbol{s_A} = s$ for all $s \in \mathbb{K}$ and $\boldsymbol{s_A} \in \mathsf{Share}(s)_A$.*

Proof. By Fact 2.2.22, $\mathsf{Share}(0)_A^{\perp} \subset \boldsymbol{m_A}^{\perp}$ if and only if $\boldsymbol{m_A} \in \mathsf{Share}(0)_A$. Clearly, $\boldsymbol{m_A} \notin \mathsf{Share}(0)_A$. This implies that $\mathsf{Share}(0)_A^{\perp} \setminus \boldsymbol{m_A}^{\perp} \neq \emptyset$. Let $\boldsymbol{r'_A} \in \mathsf{Share}(0)_A^{\perp} \setminus \boldsymbol{m_A}^{\perp} \neq \emptyset$, and let $\boldsymbol{r_A} = \frac{1}{\boldsymbol{r'_A} \cdot \boldsymbol{m_A}} \boldsymbol{r'_A} \cdot \boldsymbol{m_A}$. Then, $\boldsymbol{r_A} \cdot \boldsymbol{m_A} = 1$ and $\boldsymbol{r_A} \cdot \boldsymbol{z} = 0$ for all $\boldsymbol{z} \in \mathsf{Share}(0)_A$. By Lemma 3.1.7, $\boldsymbol{r_A} \cdot \boldsymbol{s_A} = s$ for all $s \in \mathbb{K}$ and $\boldsymbol{s_A} \in \mathsf{Share}(s)_A$. ■

We say that $\boldsymbol{r_A}$ is a *reconstruction vector*. Note that there exists a d_A-vector $\boldsymbol{r_A}$ such that $\boldsymbol{r_A} \cdot \boldsymbol{s_A} = s$ if and only if there exists a d-vector $\boldsymbol{r} \in \mathbb{L}^d$ such that $\boldsymbol{r} \cdot \boldsymbol{s} = s$, and $r_i = 0$ for all $i \notin A$.

Lemma 3.1.9 *Let $\mathcal{S}_M = (\mathbb{L}, M)$ be a linear secret sharing scheme over a ring $\mathbb{L}$ with share distribution matrix $M = (\boldsymbol{m} || M')$. Then a vector $\boldsymbol{r}$ is a reconstruction vector for $\mathcal{S}_M$ if and only if $\boldsymbol{r}^T M' = \boldsymbol{0}$ and $\boldsymbol{r}^T \boldsymbol{m} = 1$.*

Proof. If $\boldsymbol{r}$ is a reconstruction vector then by definition $\boldsymbol{r} \cdot (M\boldsymbol{b}) = b_1$ for all $\boldsymbol{b}$. In particular,

$$\boldsymbol{r}^T(\underbrace{M\boldsymbol{e_1}}_{\boldsymbol{m}}) = 1, \text{ and}$$
$$\boldsymbol{r}^T(\underbrace{M\boldsymbol{e_i}}_{M^i}) = 0 \text{ for all } i > 1.$$

Hence, $\boldsymbol{r}^T M' = \boldsymbol{0}$ and $\boldsymbol{r}^T\boldsymbol{m} = 1$. Conversely, if $\boldsymbol{r}^T M' = \boldsymbol{0}$ and $\boldsymbol{r}^T\boldsymbol{m} = 1$, then for all $s \in \mathbb{L}$, $\boldsymbol{r}^T\mathsf{Share}(s) = \boldsymbol{r}^T(s\boldsymbol{m} + \mathsf{Share}(0)) = s\boldsymbol{r}^T\boldsymbol{m} + \boldsymbol{r}^T M' = s$. Hence, $\boldsymbol{r}$ is a reconstruction vector. ■

Shamir's secret sharing scheme. Let $s \in \mathbb{K}$ be the secret to be shared. Let $f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_t x^t$ be a polynomial of degree t over $\mathbb{K}$, with $|\mathbb{K}| > n$, $t < n$. The coefficients $f_1, f_2, \ldots, f_t$ are picked at random from $\mathbb{K}$, and $f_0 = s$. In particular, $s = f(0)$.

Each player P_i, $1 \leq i \leq n$, is given exactly one share. The share given to player P_i is $s_i = f(i)$. That means that $\boldsymbol{s} = (f(1), \ldots, f(n))$, and $\boldsymbol{s} = M\boldsymbol{b}$, where

$$M = \begin{pmatrix} 1 & 1 & 1^2 & \cdots & 1^t \\ 1 & 2 & 2^2 & \cdots & 2^t \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & n & n^2 & \cdots & n^t \end{pmatrix},$$

$\boldsymbol{b} = \begin{pmatrix} s & f_1 & \cdots & f_t \end{pmatrix}^T$, $e = t + 1$, and $d = n$.

The access structure Γ is the set of all subsets of $t + 1$ or more players, and the adversary structure $\mathcal{A}$ is the set of all subsets of t or fewer players.

By Fact 2.6.5, the reconstruction vector $\boldsymbol{r} = (r_1, \ldots, r_n)$ is such that

$$r_i = \begin{cases} \prod_{j \in A j \neq i} \frac{-j}{i-j} \text{ for } i \in A \\ 0 \text{ for } i \notin A \end{cases}. \tag{3.1}$$

Shamir's secret sharing scheme is defined over a field $\mathbb{K}$, and this definition may in general not be extended to a commutative ring $\mathbb{L}$. In the first example below we will show Shamir's secret sharing scheme over the field $\mathbb{K} = \mathbb{Z}_7$ for 5 players, and in the second example we will show that Shamir's secret sharing scheme is neither secure nor functional over the ring $\mathbb{L} = \mathbb{Z}_4$ for 3 players.

Example 3.1.10 Let $\mathbb{K} = \mathbb{Z}_7$, let $n = 5$, and let $t = 3$. Let $f(x) = s + 2x + 4x^2 + 5x^3$. The share vector $\boldsymbol{s} = (s_1, s_2, s_3, s_4, s_5)^T$ is given by

$$\boldsymbol{s} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 1 \\ 1 & 3 & 2 & 6 \\ 1 & 4 & 2 & 1 \\ 1 & 5 & 4 & 6 \end{pmatrix} \begin{pmatrix} s \\ 2 \\ 4 \\ 5 \end{pmatrix} = \begin{pmatrix} s+4 \\ s+4 \\ s+2 \\ s \\ s \end{pmatrix}.$$

The access structure Γ is given by

$$\Gamma = \{\{1,2,3,4\},\{1,2,3,5\},\{1,2,4,5\},\{1,3,4,5\},\{2,3,4,5\},\{1,2,3,4,5\}\},$$

and the adversary structure $\mathcal{A}$ is given by

$$\begin{aligned}\mathcal{A} = \{&\{1,2,3\},\{1,2,4\},\{1,2,5\},\{1,3,4\},\{1,3,5\},\{1,4,5\},\{2,3,4\},\{2,3,5\},\\ &\{2,4,5\},\{3,4,5\},\{1,2\},\{1,3\},\{1,4\},\{1,5\},\{2,3\},\{2,4\},\{2,5\},\{3,4\},\\ &\{3,5\},\{4,5\},\{1\},\{2\},\{3\},\{4\},\{5\},\emptyset\}.\end{aligned}$$

Now we consider the reconstruction ability of $A = \{1,2,3,4\} \in \Gamma$. By Formula (3.1), $\boldsymbol{r_A} = (4,1,4,6)$ is a reconstruction vector for A: $\boldsymbol{r_A} \cdot \boldsymbol{s_A} = (4,1,4,6) \cdot (s+4, s+4, s+2, s) = 4s + 2 + s + 4 + 4s + 1 + 6s = s$.

We now consider the reconstruction ability of $A = \{1,2,3\} \in \mathcal{A}$.

$$\boldsymbol{s_A} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 1 \\ 1 & 3 & 2 & 6 \end{pmatrix} \begin{pmatrix} s \\ f_1 \\ f_2 \\ f_3 \end{pmatrix}.$$

The coefficients f_1, f_2, and f_3 are random. The three players may therefore reconstruct s if and only if there exists a reconstruction vector $\boldsymbol{r_A} = (r_1, r_2, r_3)^T \in \mathbb{Z}_7^3$ such that $r_1 \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} + r_2 \begin{pmatrix} 1 & 2 & 4 & 1 \end{pmatrix} + r_3 \begin{pmatrix} 1 & 3 & 2 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}$.

Example 3.1.11 Let $\mathbb{L} = \mathbb{Z}_4$, let $n = 3$, and let $t = 1$. Let $f(x) = s + 3x$. The share vector $\boldsymbol{s} = (s_1, s_2, s_3)^T$ is given by

$$\boldsymbol{s} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} s \\ 3 \end{pmatrix} = \begin{pmatrix} s+3 \\ s+2 \\ s+1 \end{pmatrix}.$$

The access structure Γ is given by $\Gamma = \{\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$, and the adversary structure $\mathcal{A}$ is given by $\mathcal{A} = \{\{1\},\{2\},\{3\},\emptyset\}$.

Now we consider the reconstruction ability of $A = \{1,3\} \in \Gamma$. By Formula (3.1), the vector $(\frac{3}{2}, \frac{3}{2})$ should be a reconstruction vector for A. Over $\mathbb{Z}_4$, however, 2 is not invertible. The two players may reconstruct s if and

only if there exists a reconstruction vector $\boldsymbol{r_A} = (r_1, r_3)^T \in \mathbb{Z}_4^3$ such that $r_1 \begin{pmatrix} 1 & 1 \end{pmatrix} + r_3 \begin{pmatrix} 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \end{pmatrix}$. Such an $\boldsymbol{r_A}$, however, does not exist.

We now consider the reconstruction ability of $A = \{2\} \in \mathcal{A}$. $s_A = s + 2f_1$ for a random coefficient f_1. However, over $\mathbb{Z}_4$ 2 is a zero divisor: $2 \cdot 2 \equiv 0 \bmod 4$. Multiplying by 2, $2s_A = 2s$. If $s = 1$ or $s = 3$, then $2s_A = 2$. Player P_2 may therefore deduce that $2s = 2$, which is equivalent to $s \in \{1, 3\}$. If $s = 0$ or $s = 2$, then $2s_A = 0$. In this case player P_2 may deduce that $2s = 0$, and therefore that $s \in \{0, 2\}$.

In a standard secret sharing scheme over a ring $\mathbb{L}$, the secret s must be an element of $\mathbb{L}$. Black box secret sharing schemes are secret sharing schemes over the ring $\mathbb{Z}$. The secret s, however, may be an element of an arbitrary Abelian group $\mathbb{G}$. Note that by Fact 2.2.6, any finite Abelian group is a $\mathbb{Z}$-module.

Let Γ be a monotone access structure, and let $M \in \mathbb{Z}^{d \times e}$ be a $d \times e$ integer matrix. Let $\mathbb{G}$ be a finite Abelian group, let $s \in \mathbb{G}$ be a secret, and let $\boldsymbol{g} = \{g_1, \ldots, g_e\} \in \mathbb{G}^e$ be a random e-vector with $g_1 = s$. Define $\boldsymbol{s} = M\boldsymbol{g}$.

Definition 3.1.12 The tuple $\mathcal{B} = (M, \Gamma)$ is called a *black-box secret sharing scheme* for Γ if the following holds:

FUNCTIONALITY. For any qualified subset $A \in \Gamma$, there exists a reconstruction vector $\boldsymbol{r_A} \in \mathbb{Z}^{d_A}$ such that for any finite Abelian group $\mathbb{G}$ and for any secret $s \in \mathbb{G}$, $\boldsymbol{r_A} \cdot \boldsymbol{s_A} = s$

SECURITY. For any unqualified subset $A \notin \Gamma$ and for any secrets s, $s' \in \mathbb{G}$, $\boldsymbol{s_A}$ and $\boldsymbol{s'_A}$ are identically distributed.

The additive secret sharing scheme, the CNF-based secret sharing scheme, and the DNF-based secret sharing scheme are three examples of black-box secret sharing schemes. Shamir's secret sharing scheme, however, is not a black-box secret sharing scheme.

Example 3.1.13 Consider Shamir's secret sharing scheme with $n = 3$ and $t = 1$. Then

$$\boldsymbol{r_{\{1,3\}}} = \begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{3}{2} \\ -\frac{1}{2} \end{pmatrix} \notin \mathbb{Z}^2.$$

3.2 Characterisation through Monotone Span Programs

By Examples 3.1.10 and 3.1.11, for Shamir's secret sharing scheme to be functional, $(1, 0, \ldots, 0)$ must be a linear combination of the rows of M_A for every qualified subset $A \in \Gamma$, while for Shamir's secret sharing scheme to be secure, no scalar multiple of $(1, 0, \ldots, 0)$ should be a linear combination of the rows of M_A for any unqualified subset $A \in \mathcal{A}$.

More formally, Shamir's secret sharing scheme is functional if and only if for any $A \in \Gamma$, $(1, 0, \ldots, 0)^T \in \operatorname{Im} M_A^T$, and if Shamir's secret sharing scheme is secure, then for any $A \in \mathcal{A}$, $(\alpha, 0, \ldots, 0)^T \notin \operatorname{Im} M_A^T$ for all $\alpha \in \mathbb{L} \setminus \{0\}$.

In Lemma 3.2.1 below, we prove that if the first column of M_A is a linear combination of the $e - 1$ other columns of M_A, then no linear combination of the rows of M_A is a scalar multiple of $(1, 0, \ldots, 0)$.

Lemma 3.2.1 *If there exists* $\boldsymbol{\kappa} = (\kappa_1, \ldots, \kappa_e)^T \in \operatorname{Ker} M_A$ *with* $\kappa_1 = 1$, *then for all scalars* $\alpha \in \mathbb{L} \setminus \{0\}$, $(\alpha, 0, \ldots, 0)^T \notin \operatorname{Im} M_A^T$.

Proof. If there exists $\boldsymbol{\kappa} = (\kappa_1, \ldots, \kappa_e)^T \in \operatorname{Ker} M_A$ with $\kappa_1 = 1$, then for all $\alpha \in \mathbb{L} \setminus \{0\}$, $(\alpha, 0, \ldots, 0)^T \cdot \kappa = \alpha\kappa_1 \neq 0$. This is equivalent to $(\alpha, 0, \ldots, 0)^T \notin (\operatorname{Ker} M_A)^\perp$ for any $\alpha \in \mathbb{L} \setminus \{0\}$. By Fact 2.3.14, $\operatorname{Im} M_A^T \subset (\operatorname{Ker} M_A)^\perp$, and thus $(\alpha, 0, \ldots, 0)^T \notin \operatorname{Im} M_A^T$ for any $\alpha \in \mathbb{L} \setminus \{0\}$. ■

We may generalise this in terms of monotone span programs (MSPs). MSPs were introduced by M. Karchmer and A. Widgerson in 1993 [16]. Karchmer and Widgerson defined MSPs over finite fields. We will generalise this definition to commutative rings.

As in section 3.1, let $M \in \mathbb{L}^{d \times e}$ be a matrix with d rows and e columns.

A *labelling function* is a surjective function $\psi : \{1, \ldots, d\} \to \{1, \ldots, n\}$. We will say that row j of M is labelled by i if $\psi(j) = i$. Each row of M is labelled by an integer i with $1 \leq i \leq n$ for some n such that each i labels at least one row. Let d_i be the number of rows of M labelled by i. Denote by $M_i \in \mathbb{L}^{d_i \times e}$ the matrix consisting of those d_i rows. Similarly, for $\emptyset \neq A \subset \{1, \ldots, n\}$, d_A denotes the number of rows of M labelled by some $i \in A$. Let $M_A \in \mathbb{L}^{d_A \times e}$ be the matrix consisting of those d_A rows.

Let $\boldsymbol{a} \in \mathbb{L}^e \setminus \{\mathbf{0}\}$ be the fixed non-zero *target vector* $\boldsymbol{a} = (1, 0, \ldots, 0)$. Sometimes the target vector will be $\mathbf{1} = (1, 1, \ldots, 1)$.

Definition 3.2.2 A *monotone span program (MSP)* over a ring $\mathbb{L}$ is a tuple $\mathcal{M} = (\mathbb{L}, M, \boldsymbol{a}, \psi)$.

We define the *size* of $\mathcal{M}$ to be the number of rows of M.

Definition 3.2.3 The MSP $\mathcal{M} = (\mathbb{L}, M, \boldsymbol{a}, \psi)$ is said to *compute the monotone access structure* Γ if for all $\emptyset \neq A \subset \{1, \ldots, n\}$, the following holds:

- $A \in \Gamma \Rightarrow \boldsymbol{a} \in \operatorname{Im} M_A^T$, and
- $A \notin \Gamma \Rightarrow \exists \boldsymbol{\kappa} = (\kappa_1, \ldots, \kappa_e)^T \in \operatorname{Ker} M_A$ with $\kappa_1 = 1$.

Lemma 3.2.4 *Let* $\mathbb{K}$ *be a field. Then there exists* $\boldsymbol{\kappa} = (\kappa_1, \ldots, \kappa_e)^T \in \operatorname{Ker} M_A$ *with* $\kappa_1 = 1$ *if and only if* $\boldsymbol{a} \notin \operatorname{Im} M_A^T$.

Proof. By Fact 2.3.15, $\boldsymbol{a} \notin \operatorname{Im} M_A^T$ if and only if $\boldsymbol{a} \notin (\operatorname{Ker} M_A)\perp$. Hence, if $\boldsymbol{a} \notin \operatorname{Im} M_A^T$, then there exists $z \in \operatorname{Ker} M_A$ such that $\boldsymbol{a} \cdot \boldsymbol{z} \neq 0$, which is equivalent to $z_1 \neq 0$. Define $\boldsymbol{\kappa} = z_1^{-1}\boldsymbol{z} \in \operatorname{Ker} M_A$. Conversely, if there exists $\boldsymbol{\kappa} = (\kappa_1, \ldots, \kappa_e)^T \in \operatorname{Ker} M_A$ with $\kappa_1 = 1$, then $\boldsymbol{a} \cdot \boldsymbol{z} \neq 0$. Equivalently, $\boldsymbol{a} \notin (\operatorname{Ker} M_A)^T = \operatorname{Im} M_A^T$ by Fact 2.3.15. ■

Definition 3.2.5 We say that the MSP $\mathcal{M} = (\mathbb{K}, M, \boldsymbol{a}, \psi)$ *computes the monotone access structure* Γ if for all $\emptyset \neq A \subset \{1, \ldots, n\}$,

$$A \in \Gamma \Leftrightarrow \boldsymbol{a} \in \operatorname{Im} M_A^T$$

.

If $\mathbb{L}$ is a ring, then $\boldsymbol{a} \notin \operatorname{Im} M_A^T$ does not imply the existence of such a $\boldsymbol{\kappa}$.

Example 3.2.6 Let $M = \begin{pmatrix} 2 & 0 \end{pmatrix} \in \mathbb{Z}^{1\times 2}$. Then, $\operatorname{Im} M^T = \{2a : a \in \mathbb{Z}\}$, and $\operatorname{Ker} M = \{0\}$. Thus, $\boldsymbol{a} \notin \operatorname{Im} M^T$, and there does not exist a $\boldsymbol{\kappa} \in \operatorname{Ker} M$ such that $\kappa_1 = 1$.

A monotone access structure Γ may be defined in terms of a monotone Boolean function. For example, if $\Gamma = \{\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$, then the Boolean function $f(P_1, P_2, P_3) = (P_1 \wedge P_2) \vee (P_1 \wedge P_3) \vee (P_2 \wedge P_3)$ has access structure Γ.

Definition 3.2.7 The MSP $\mathcal{M}$ is said to *compute the monotone Boolean function* f if it computes the monotone access structure $\Gamma = \{A \subset \{1, \ldots, n\} : f(A) = 1\}$.

Fact 3.2.8 *Every monotone Boolean function* $f : \{0,1\}^n \to \{0,1\}$ *can be computed by an MSP [16].*

As an example, consider a 5×5 MSP over $\mathbb{Z}_2$ with $n = 3$.

Example 3.2.9 Let $\mathbb{K} = \mathbb{Z}_2$, $d = 5$, $e = 5$, $n = 3$, and let

$$M = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{matrix} 1 \\ 3 \\ 3 \\ 2 \\ 1 \end{matrix} .$$

Let the access structure computed by the MSP be Γ. For $A = \{2,3\}$, the corresponding matrix M_A is

$$M_A = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

The sum of row 1 and row 2 of M_A is equal to $\boldsymbol{a}$: $A \in \Gamma$.

Let $\mathcal{M} = (\mathbb{L}, M, \boldsymbol{a}, \psi)$ be an MSP computing the monotone access structure $\Gamma_{\mathcal{M}}$. Let $\mathcal{T}_{\mathcal{M}}$ be the set of maximal unqualified subsets of $\Gamma_{\mathcal{M}}$.

For each $T \in \mathcal{T}_{\mathcal{M}}$, there exists by definition 3.2.3 a d_T-vector $\boldsymbol{w_T}$ such that $M_T \boldsymbol{w_T} = \mathbf{0}$ and $\boldsymbol{a} \cdot \boldsymbol{w_T} = 1$. Let $\boldsymbol{c_T} = M\boldsymbol{w_T}$, and let $\hat{M}$ be the concatenation of those vectors $\boldsymbol{c_T}$, $T \in \mathcal{T}$. $\hat{M}$ has the same number of rows as M, $|\mathcal{T}|$ columns, and the same labelling as M.

Definition 3.2.10 We say that $\hat{\mathcal{M}} = (\hat{M}, \mathbb{L}, \mathbf{1}, \psi)$ is a *canonical MSP*.

We denote the monotone access structure computed by $\hat{M}$ by $\Gamma_{\hat{\mathcal{M}}}$.

Fact 3.2.11 $\Gamma_{\hat{\mathcal{M}}} = \Gamma_{\mathcal{M}}$.

As an example, consider again the 5×5 MSP over $\mathbb{Z}_2$ with $n = 3$ from Example 3.2.9.

Example 3.2.12 In Example 3.2.9, $\Gamma_{\mathcal{M}} = \{\{3\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$. Hence, $T = \{1,2\}$ is the only maximal unqualified subset. The corresponding matrix M_T is

$$M_T = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Clearly, $\boldsymbol{w_T} = (1,0,0,0,0)^T \in \operatorname{Ker} M_T$ with $\boldsymbol{a} \cdot \boldsymbol{w_T} = 1$, and hence

$$\boldsymbol{c_T} = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Hence,

$$\hat{M} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \begin{matrix} 1 \\ 3 \\ 3 \\ 2 \\ 1 \end{matrix}.$$

Note that $\Gamma_{\hat{\mathcal{M}}} = \{\{3\}, \{1,3\}, \{2,3\}, \{1,2,3\}\} = \Gamma_{\mathcal{M}}$.

We will now prove that LSSSs and MSPs over a finite field are in fact equivalent. That means that for each LSSS, we may construct a corresponding MSP, and for each MSP, we may construct a corresponding LSSS. The second part of the proof is due to [16].

Theorem 3.2.13 *Linear secret sharing schemes and monotone span programs over a finite field $\mathbb{K}$ are in one-to-one correspondence.*

Proof. Let Γ be the access structure. First we show that we may construct an MSP for a given LSSS.

Let the LSSS be defined by $\boldsymbol{s} = M\boldsymbol{b}$, $M \in \mathbb{K}^{d\times e}$ with $M = (\boldsymbol{m}||M')$, $\boldsymbol{b} \in \mathbb{K}^e$ with $b = (s||\boldsymbol{b'})$. For $1 \leq j \leq d$, $1 \leq i \leq n$, we label row j of M by i if s_j is given to player P_i. Denote the corresponding labelling function by ψ. Define an MSP $\mathcal{M}$ by the triple $(\mathbb{K}, M, \boldsymbol{a}, \psi)$. Below we prove that $\mathcal{M}$ computes Γ.

Firstly, $\boldsymbol{a} \in \operatorname{Im} M_A^T$ if and only if there exists a d_A-vector $\boldsymbol{r} \in \mathbb{K}^{d_A}$ such that $\boldsymbol{a} = M_A^T\boldsymbol{r}$. The latter implies that $\boldsymbol{r} \cdot \boldsymbol{s_A} = \boldsymbol{r} \cdot M_A\boldsymbol{b} = (M_A^T\boldsymbol{r})^T\boldsymbol{b} = \boldsymbol{a} \cdot \boldsymbol{b} = s$, and hence, $\boldsymbol{r}$ is a reconstruction vector for A. This means that $A \in \Gamma$.

Conversely, if $A \in \Gamma$ then there must exist a reconstruction vector $\boldsymbol{r}$ for A. Hence, $s = \boldsymbol{r} \cdot \boldsymbol{s_A} = \boldsymbol{r} \cdot M_A\boldsymbol{b} = (M_A^T\boldsymbol{r}) \cdot \boldsymbol{b} = (\boldsymbol{m} \cdot \boldsymbol{r})s + ({M'_A}^T\boldsymbol{r}) \cdot \boldsymbol{b'}$, implying that $\boldsymbol{m} \cdot \boldsymbol{r} = 1$ and ${M'_A}^T\boldsymbol{r} = \boldsymbol{0}$. This is equivalent to $\boldsymbol{a} = M_A^T\boldsymbol{r}$, which means that $\boldsymbol{a} \in \operatorname{Im} M_A^T$.

Next, we show how to construct an LSSS for a given MSP.

Pick a random vector $\boldsymbol{b} \in \mathbb{K}^e$ such that $b_1 = s$. Let $\boldsymbol{s_i} = M_i\boldsymbol{b}$ be the vector given to player P_i. This means that share s_j is given to player P_i if row j of M is labelled by i. Thus, $\boldsymbol{s} = M\boldsymbol{b}$.

We now prove that the LSSS is functional. For any $A \subset \{1, \ldots, n\}$, $A \in \Gamma$ if and only if $\boldsymbol{a} \in \operatorname{Im} M_A^T$. This implies that there exists a d_A-vector $\boldsymbol{r} \in K^{d_A}$ such that $\boldsymbol{a} = M_A^T\boldsymbol{r}$. Thus, $\boldsymbol{r} \cdot \boldsymbol{s_A} = \boldsymbol{r} \cdot (M_A\boldsymbol{b}) = (M_A^T\boldsymbol{r})^T\boldsymbol{b} = \boldsymbol{a} \cdot \boldsymbol{b} = s$, and thus $\boldsymbol{r}$ is a reconstruction vector for A.

Conversely, $A \notin \Gamma$ if and only if $\boldsymbol{a} \notin \operatorname{Im} M_A^T$, which is equivalent to $\boldsymbol{a} \notin (\operatorname{Ker} M_A)^\perp$. This means that there exists an e-vector $\boldsymbol{z} \in \mathbb{K}^e$ such that $M_A\boldsymbol{z} = \boldsymbol{0}$ and $z_1 = \boldsymbol{a} \cdot \boldsymbol{z} \neq 0$. Wlog $z_1 = 1$. For an arbitrary $s' \in \mathbb{K}$, define $\boldsymbol{s'} = M(\boldsymbol{b} + \boldsymbol{z}(s' - s))$. Then $\boldsymbol{s'}$ is a valid sharing of s', and $\boldsymbol{s_A} \equiv \boldsymbol{s'_A}$. This proves that the LSSS is secure. ■

Similarly, for each MSP over a commutative ring $\mathbb{L}$, there is a corresponding LSSS. This lemma is due to [11].

Lemma 3.2.14 *For each monotone span program over a commutative ring $\mathbb{L}$, there is a corresponding linear secret sharing scheme.*

Proof. Let Γ be a monotone access structure. Let an MSP $\mathcal{M}$ be defined by the tuple $(\mathbb{L}, M, \boldsymbol{a}, \psi)$, $M \in \mathbb{L}^{d\times e}$. Let $s \in \mathbb{L}$ be the secret to be shared. Define an LSSS as follows:

Pick a random vector $\boldsymbol{b'} \in \mathbb{L}^{e-1}$ and let $\boldsymbol{b} = (s||\boldsymbol{b'})$. Let $\boldsymbol{s_i} = M_i\boldsymbol{b}$ be the vector given to player P_i. This means that share s_j is given to player P_i if row j of M is labelled by i. Thus, $\boldsymbol{s} = M\boldsymbol{b}$.

Now, if $A \in \Gamma$, then $\boldsymbol{a} \in \operatorname{Im} M_A^T$. This implies that there exists a d_A-vector $\boldsymbol{r} \in \mathbb{L}^{d_A}$ such that $\boldsymbol{a} = M_A^T\boldsymbol{r}$. Thus, $\boldsymbol{r} \cdot \boldsymbol{s_A} = \boldsymbol{r} \cdot (M_A\boldsymbol{b}) = (M_A^T\boldsymbol{r})^T\boldsymbol{b} =$

$\boldsymbol{a} \cdot \boldsymbol{b} = s$, and thus $\boldsymbol{r}$ is a reconstruction vector for A. This proves that the LSSS is functional.

We now prove that the LSSS is secure. For any $A \subset \{1, \ldots, n\}$, $A \notin \Gamma$ implies that there exists an e-vector $\boldsymbol{\kappa} \in \mathbb{L}^e$ such that $M_A \boldsymbol{\kappa} = \mathbf{0}$ and $\kappa_1 = 1$. For an arbitrary $s' \in \mathbb{L}$, define $\boldsymbol{s'} = M(\boldsymbol{b} + \boldsymbol{\kappa}(s' - s))$. Then $\boldsymbol{s'}$ is a valid sharing of s', and $\boldsymbol{s_A} \equiv \boldsymbol{s'_A}$. This proves that the LSSS is secure. ■

In particular, an LSSS defined by $\boldsymbol{s} = M\boldsymbol{b}$ is functional if and only if $\boldsymbol{a} \in \operatorname{Im} M_A^T$ for all qualified subsets A. It is secure over a field if for all unqualified subsets A, $\boldsymbol{a} \notin \operatorname{Im} M_A^T$, and it is secure over a ring if for all unqualified subsets A, there exists $\boldsymbol{\kappa} \in \operatorname{Ker} M_A$ with $\kappa_1 = 1$. It is secure only if for all scalars α, $\alpha \boldsymbol{a} \notin \operatorname{Im} M_A^T$ for all unqualified subsets A.

MSPs over the ring $\mathbb{Z}$ are equivalent to black-box secret sharing schemes [10].

Definition 3.2.15 An MSP $\mathcal{M} = (\mathbb{Z}, M, \boldsymbol{a}, \psi)$ is said to be an *integer span program.*

Theorem 3.2.16 *Let Γ be a monotone access structure. Then $\mathcal{B} = (M, \Gamma)$ is a black-box secret sharing scheme for Γ if and only if $\mathcal{M} = (\mathbb{Z}, M, \boldsymbol{a})$ is an integer span program for Γ.*

Proof. First, we prove that if $\mathcal{M} = (\mathbb{Z}, M, \boldsymbol{a})$ is an ISP for Γ, then $\mathcal{B} = (M, \Gamma)$ is a black-box secret sharing scheme for Γ.

Let $\mathbb{G}$ be an arbitrary finite Abelian group, let $s \in \mathbb{G}$, and let $\boldsymbol{g} = (s, g_2, ..., g_e) \in \mathbb{G}^e$ for arbitrary $g_2, \ldots, g_e \in \mathbb{G}$. Define $\boldsymbol{s} = M\boldsymbol{g}$.

FUNCTIONALITY. If $A \in \Gamma$, then by definition 3.2.2, $\boldsymbol{a} \in \operatorname{Im} M_A^T$. Thus, there exists a vector $\boldsymbol{r_A} \in \mathbb{Z}^d$ such that $M_A^T \boldsymbol{r_A} = \boldsymbol{a}$. Then, $\boldsymbol{r_A} \cdot \boldsymbol{s_A} = \boldsymbol{r_A} \cdot (M_A \boldsymbol{g}) = (M_A^T \boldsymbol{r_A}) \cdot \boldsymbol{g} = \boldsymbol{a} \cdot \boldsymbol{g} = s$.

SECURITY. If $A \notin \Gamma$, then by definition 3.2.2, there exists a vector $\boldsymbol{\kappa} \in \operatorname{Ker} M_A$ with $\kappa_1 = 1$. For an arbitrary $s' \in \mathbb{G}$, define $\boldsymbol{g'} = \boldsymbol{g} + (s' - s)\boldsymbol{\kappa} \in \mathbb{G}^e$, and define $\boldsymbol{s'} = M\boldsymbol{g'} \in \mathbb{G}^d$. Then $\boldsymbol{s_A} = \boldsymbol{s'_A}$. Thus, $\boldsymbol{s_A}$ and $\boldsymbol{s'_A}$ are identically distributed.

Conversely, we prove that if $\mathcal{B} = (M, \Gamma)$ is a black-box secret sharing scheme for Γ, then $\mathcal{M} = (\mathbb{Z}, M, \boldsymbol{a})$ is an ISP for Γ.

Let $\mathbb{G} = \mathbb{Z}_p$ for an arbitrary prime p, let $s_1 = 1, s_2 = 0, \ldots, s_e = 0$, and let $G = (\boldsymbol{g_1} || \boldsymbol{g_2} || \cdots || \boldsymbol{g_e}) \in \mathbb{G}^{e \times e}$ with $\boldsymbol{g_1} = (s_1, 0, \ldots, 0)^T, \boldsymbol{g_2} = (s_2, 1, \ldots, 0)^T, \ldots, \boldsymbol{g_e} = (s_e, 0, \ldots, 1)^T$. Note that G is the $e \times e$ identity matrix. Define $\boldsymbol{s_1} = M\boldsymbol{g_1}, \ldots, \boldsymbol{s_e} = M\boldsymbol{g_e}$, and define $S = (\boldsymbol{s_1} || \cdots || \boldsymbol{s_e}) = MG \in \mathbb{G}^{d \times e}$.

If $A \in \Gamma$, then by definition 3.1.12 there exists a reconstruction vector

$\boldsymbol{r_A} \in \mathbb{Z}^{d_A}$ such that

$$\boldsymbol{a} \equiv \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \equiv \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_e \end{pmatrix} \equiv \begin{pmatrix} \boldsymbol{r_A} \cdot \boldsymbol{s_{1A}} \\ \boldsymbol{r_A} \cdot \boldsymbol{s_{2A}} \\ \vdots \\ \boldsymbol{r_A} \cdot \boldsymbol{s_{eA}} \end{pmatrix} \equiv (\boldsymbol{r_A}^T S_A)^T \equiv (\boldsymbol{r_A}^T M_A G)^T$$
$$\equiv (\boldsymbol{r_A}^T M_A)^T \equiv M_A^T \boldsymbol{r_A} \bmod p.$$

This holds for any prime p. Thus, $\boldsymbol{a} = M_A^T \boldsymbol{r_A}$, which implies that $\boldsymbol{a} \in \operatorname{Im} M_A^T$.

We will now show that if $A \notin \Gamma$, then there exists $\boldsymbol{\kappa} \in \operatorname{Ker} M_A$ with $\kappa_1 = 1$. Consider the system of linear equations $N_A \boldsymbol{x} = \boldsymbol{y}$, where $\boldsymbol{y}$ is the first column of M_A, and $N_A \in \mathbb{Z}^{d \times (e-1)}$ is the concatenation of the remaining $e-1$ columns. Note that $\boldsymbol{x}$ is a solution if and only if

$$M_A \begin{pmatrix} 1 \\ -\boldsymbol{x} \end{pmatrix} = \boldsymbol{y} - N_A \boldsymbol{x} = \boldsymbol{0}.$$

Let $\mathbb{G} = \mathbb{Z}_m$ for an arbitrary non-zero integer m. Let $s \in \mathbb{G}$, and let $s' \equiv s - 1$. Let the vector $\boldsymbol{g} \in \mathbb{G}^e$ be such that $g_1 \equiv s$. Then by definition 3.1.12, there exists a vector $\boldsymbol{g'} \in \mathbb{G}^e$ with $g'_1 \equiv s'$ such that $M_A \boldsymbol{g'} \equiv \boldsymbol{s_A} \equiv M_A \boldsymbol{g}$. Hence, $M_A(\boldsymbol{g} - \boldsymbol{g'}) \equiv \boldsymbol{0}$, and $(g - g')_1 \equiv 1$. Equivalently,

$$N_A \begin{pmatrix} -(g-g')_2 \\ \vdots \\ -(g-g')_e \end{pmatrix} \equiv \boldsymbol{y} \bmod m.$$

This holds for any non-zero integer m. Thus, $N_A \boldsymbol{x} = \boldsymbol{y}$ is solvable over $\mathbb{Z}_m$ for all non-zero integers m, and thus, by Fact 2.3.19, it is solvable over $\mathbb{Z}$. Let $\boldsymbol{x}$ be a solution. Define

$$\boldsymbol{\kappa} = \begin{pmatrix} 1 \\ -\boldsymbol{x} \end{pmatrix},$$

then $M_A \boldsymbol{\kappa} = \boldsymbol{0}$, and $\kappa_1 = 1$. ■

3.3 Characterisation through Projection

Notation 3.3.1 *Let $\mathcal{S}$ be a linear secret sharing scheme. We denote the set of reconstruction vectors of $\mathcal{S}$ by $\mathcal{R}(\mathcal{S})$.*

Clearly, every linear secret sharing scheme has a unique set of reconstruction vectors. Lemma 3.3.2 below gives the precise number of reconstruction vectors for an LSSS defined by $\boldsymbol{s} = M\boldsymbol{b}$.

Lemma 3.3.2 *Let $\mathcal{S}_M$ be an LSSS with share distribution matrix $M \in \mathbb{L}^{d\times e}$ over a ring $\mathbb{L}$. Then $|\mathcal{R}(\mathcal{S}_M)| = |\mathbb{L}|^{d-e}$.*

Proof. Note that a vector $\boldsymbol{r} \in \mathbb{L}^d$ is a reconstruction vector for $\mathcal{S}_M$ if and only if $\boldsymbol{r}^T M = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$. Thus, $\boldsymbol{r}$ is a reconstruction vector for $\mathcal{S}_M$ if and only if $\boldsymbol{r}$ is a solution of the system of linear equations

$$\begin{cases} r_1 m_{11} + r_2 m_{21} + \cdots + r_d m_{d1} = 1 \\ r_1 m_{12} + r_2 m_{22} + \cdots + r_d m_{d2} = 0 \\ \qquad\qquad \vdots \\ r_1 m_{1e} + r_2 m_{2e} + \cdots + r_d m_{de} = 0 \end{cases}.$$

Since the e columns of M are linearly independent, $\operatorname{rank} M = e$, and thus M has e linearly independent rows. Wlog the first e rows of M are linearly independent. Then for each $e+1 \leq i \leq d$, there exist scalars $\mu_{i1}, \ldots, \mu_{ie}$ such that $M_i = \mu_{i1} M_1 + \cdots + \mu_{ie} M_e$, where M_j denotes the jth row of M. Thus, the system of linear equations becomes

$$\begin{cases} (r_1 + \mu_{e+11} r_{e+1} + \cdots + \mu_{d1} r_d) m_{11} + \cdots + (r_e + \mu_{e+1e} r_{e+1} + \cdots + \mu_{de} r_d) m_{e1} = 1 \\ (r_1 + \mu_{e+11} r_{e+1} + \cdots + \mu_{d1} r_d) m_{12} + \cdots + (r_e + \mu_{e+1e} r_{e+1} + \cdots + \mu_{de} r_d) m_{e2} = 0 \\ \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\ (r_1 + \mu_{e+11} r_{e+1} + \cdots + \mu_{d1} r_d) m_{1e} + \cdots + (r_e + \mu_{e+1e} r_{e+1} + \cdots + \mu_{de} r_d) m_{ee} = 0 \end{cases}.$$

Equivalently,

$$\underbrace{\begin{pmatrix} m_{11} & \cdots & m_{1e} \\ m_{21} & \cdots & m_{2e} \\ \vdots & \ddots & \vdots \\ m_{e1} & \cdots & m_{ee} \end{pmatrix}}_{N} \begin{pmatrix} r_1 + \mu_{e+11} r_{e+1} + \cdots + \mu_{d1} r_d \\ r_2 + \mu_{e+12} r_{e+1} + \cdots + \mu_{d2} r_d \\ \vdots \\ r_e + \mu_{e+1e} r_{e+1} + \cdots + \mu_{de} r_d \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Thus, $\begin{pmatrix} r_1 + \mu_{e+11} r_{e+1} + \cdots + \mu_{d1} r_d & \cdots & r_e + \mu_{e+1e} r_{e+1} + \cdots + \mu_{de} r_d \end{pmatrix} = (N^{-1})_1$. The coefficients $r_{e+1}, \ldots, r_d$ are free. Once those are fixed, the coefficients $r_1, \ldots, r_e$ are uniquely determined. There are thus $|\mathbb{L}|^{d-e}$ solutions $\boldsymbol{r} \in \mathbb{L}^d$. ■

Shamir's secret sharing scheme. Recall that by Formula (3.1), a reconstruction vector for Shamir's secret sharing scheme for a qualified subset of players A is given by

$$r_i = \begin{cases} \prod_{j \in A j \neq i} \frac{-j}{i-j} \text{ for } i \in A \\ 0 \text{ for } i \notin A \end{cases}.$$

Note that since each subset of players A with $|A| > t$ is a qualified subset, Shamir's secret sharing scheme has precisely $\binom{n}{t+1} + \binom{n}{t+2} + \cdots + \binom{n}{n-1} + 1$ qualified subsets. However, by Lemma 3.3.2, Shamir's secret sharing scheme has $|\mathbb{K}|^{n-(t+1)} > \binom{n}{t+1} + \binom{n}{t+2} + \cdots + \binom{n}{n-1} + 1$ reconstruction vectors. In Example 3.3.3, we compute the reconstruction vectors of a generalised Shamir's secret sharing scheme with $n = 3$ and $t = 1$. Note that over $\mathbb{Z}_p$, $p \geq 5$, there are precisely $p > \binom{3}{2} + 1 = 4$ reconstruction vectors.

Example 3.3.3 Let

$$V = \begin{pmatrix} 1 & \alpha_1 \\ 1 & \alpha_2 \\ 1 & \alpha_3 \end{pmatrix}$$

for $\alpha_i \neq \alpha_j$ for $i \neq j$. A vector $\boldsymbol{r}$ is a reconstruction vector for $\mathcal{S}_V$ if and only if $\boldsymbol{r}^T V = \begin{pmatrix} 1 & 0 \end{pmatrix}$. Equivalently, $\boldsymbol{r}$ is a solution of the system of linear equations

$$\begin{cases} r_1 + r_2 + r_3 = 1 \\ r_1\alpha_1 + r_2\alpha_2 + r_3\alpha_3 = 0 \end{cases}.$$

Let $r_3 = k \in \mathbb{Z}_p$. Then $r_2 = \frac{k(\alpha_1 - \alpha_3)}{\alpha_2 - \alpha_1}$, and $r_3 = \frac{k(\alpha_3 - \alpha_2)}{\alpha_2 - \alpha_1}$.

If $k = 0$, then $\boldsymbol{r}^T = \begin{pmatrix} \frac{-\alpha_1}{\alpha_2 - \alpha_1} & \frac{\alpha_2}{\alpha_2 - \alpha_1} & 0 \end{pmatrix}$. Note that $\boldsymbol{r}_{1,2}^T = (V_{1,2}^{-1})_1$, where $(V_{1,2}^{-1})_1$ denotes the first row of the inverse of the Vandermonde matrix

$$V_{1,2} = \begin{pmatrix} 1 & \alpha_1 \\ 1 & \alpha_2 \end{pmatrix}.$$

If $k = \frac{\alpha_1}{\alpha_1 - \alpha_3}$, then $\boldsymbol{r}^T = \begin{pmatrix} \frac{-\alpha_3}{\alpha_1 - \alpha_3} & 0 & \frac{\alpha_1}{\alpha_1 - \alpha_3} \end{pmatrix}$, and $\boldsymbol{r}_{1,3}^T = (V_{1,3}^{-1})_1$.
If $k = \frac{-\alpha_2}{\alpha_3 - \alpha_2}$, then $\boldsymbol{r}^T = \begin{pmatrix} 0 & \frac{\alpha_3}{\alpha_3 - \alpha_2} & \frac{-\alpha_2}{\alpha_3 - \alpha_2} \end{pmatrix}$, and $\boldsymbol{r}_{2,3}^T = (V_{2,3}^{-1})_1$.
If $k = \frac{-\alpha_1\alpha_2}{(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)}$, then $\boldsymbol{r}^T = \begin{pmatrix} \frac{\alpha_2\alpha_3}{(\alpha_3 - \alpha_1)(\alpha_2 - \alpha_1)} & \frac{\alpha_1\alpha_3}{(\alpha_2 - \alpha_3)(\alpha_2 - \alpha_1)} & \frac{-\alpha_1\alpha_2}{(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)} \end{pmatrix}$.
Note that $\boldsymbol{r}^T = (V_{1,2,3}^{-1})_1$, where $(V_{1,2,3}^{-1})_1$ denotes the first row of the inverse of the Vandermonde matrix

$$V_{1,2,3} = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 \\ 1 & \alpha_2 & \alpha_2^2 \\ 1 & \alpha_3 & \alpha_3^2 \end{pmatrix}.$$

The four reconstruction vectors above are the reconstruction vectors from Formula (3.1). Let $k = 1$. For every field $\mathbb{Z}_p$, $p > 5$, a fifth reconstruction vector is given by $\boldsymbol{r}^T = \begin{pmatrix} \frac{\alpha_3}{\alpha_2 - \alpha_1} & \frac{-\alpha_3}{\alpha_2 - \alpha_1} & 1 \end{pmatrix}$.

Lemma 3.3.4 *Let $\mathcal{S}_M = (M, \mathbb{K})$ and $\mathcal{S}_N = (N, \mathbb{K})$ be two linear secret sharing schemes over the field $\mathbb{K}$ with share distribution matrices M and $N \in \mathbb{K}^{d \times e}$. Then $\mathcal{R}(\mathcal{S}_M) = \mathcal{R}(\mathcal{S}_N)$ if and only if there exists an invertible matrix $C \in \mathbb{K}^{e \times e}$ with $C_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$ such that $N = MC$.*

Proof. First we prove that if $\mathcal{R}(\mathcal{S}_M) = \mathcal{R}(\mathcal{S}_N)$ then there exists an invertible matrix $C \in \mathbb{K}^{e\times e}$ with $C_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$ such that $N = MC$. By Lemma 3.3.2, $|\mathcal{R}(\mathcal{S}_M)| = |\mathbb{K}|^{d-e}$. By Lemma 3.3.6 below, $\mathcal{R}(\mathcal{S}_M)^\perp = \mathsf{Share}_{\mathcal{S}_M}(0)$. Thus, the $e-1$ last columns of M $M^2, \ldots, M^e$ are a basis of $\mathcal{R}(\mathcal{S}_M)^\perp$. If $\mathcal{R}(\mathcal{S}_M) = \mathcal{R}(\mathcal{S}_N)$, then for all $\boldsymbol{r} \in \mathcal{R}(\mathcal{S}_M)$, $\boldsymbol{r}^T M^1 = \mathbf{1} = \boldsymbol{r}^T N^1$, and $\boldsymbol{r}^T M^i = \mathbf{0} = \boldsymbol{r}^T N^i$ for all $2 \leq i \leq e$. This implies that $N^1 - M^1, N^2, \ldots, N^e \in \mathcal{R}(\mathcal{S}_M)^\perp$. Thus, there exist $\gamma_2, \ldots, \gamma_e, \gamma_{2i}, \ldots, \gamma_{ei} \in \mathbb{K}$ such that $N^1 = M^1 + \gamma_2 M^2 + \cdots + \gamma_e M^e$, and $N^i = \gamma_{2i} M^2 + \cdots + \gamma_{ei} M^e$ for $2 \leq i \leq e$. Equivalently,

$$N = M \underbrace{\begin{pmatrix} 1 & 0 & \cdots & 0 \\ \gamma_2 & \gamma_{22} & \cdots & \gamma_{2e} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_e & \gamma_{e2} & \cdots & \gamma_{ee} \end{pmatrix}}_{C}.$$

By Lemma 3.3.7 below, C is invertible.

Conversely, if there exists an invertible matrix $C \in \mathbb{K}^{e\times e}$ with $C_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$ such that $N = MC$, then for any $\boldsymbol{r} \in \mathcal{R}(\mathcal{S}_M)$, $\boldsymbol{r}^T N = \boldsymbol{r}^T MC = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix} C = C_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$, and hence, $\boldsymbol{r} \in \mathcal{R}(\mathcal{S}_N)$. By Lemma 3.3.2, $|\mathcal{R}(\mathcal{S}_M)| = |\mathcal{R}(\mathcal{S}_N)|$. This proves that $\mathcal{R}(\mathcal{S}_M) = \mathcal{R}(\mathcal{S}_N)$. ■

Note that if $M = (\boldsymbol{m}||M')$ and $N = (\boldsymbol{n}||N')$, then $\boldsymbol{n} = \boldsymbol{m} + \gamma_2 M'^1 + \cdots + \gamma_e M'^{e-1}$ and $N' = M'C'$, where C' is the invertible matrix

$$\begin{pmatrix} \gamma_{22} & \cdots & \gamma_{2e} \\ \vdots & \ddots & \vdots \\ \gamma_{e2} & \cdots & \gamma_{ee} \end{pmatrix}.$$

Corollary 3.3.5 *Let $\mathcal{S}_M = (M, \mathbb{K})$ and $\mathcal{S}_N = (N, \mathbb{K})$ be two linear secret sharing schemes over the field $\mathbb{K}$ with share distribution matrices M and $N \in \mathbb{K}^{d\times e}$. Then $\mathcal{R}(\mathcal{S}_M) = \mathcal{R}(\mathcal{S}_N)$ if and only if $\mathcal{S}_M = \mathcal{S}_N$.*

By Corollary 3.3.5 above, a set of reconstruction vectors corresponds to a unique linear secret sharing scheme.

Lemma 3.3.6 *Let $\mathcal{S}_M$ be a linear secret sharing scheme over a ring $\mathbb{K}$ with share distribution matrix $M \in \mathbb{K}^{d\times e}$. Then $\mathcal{R}(\mathcal{S}_M)^\perp = \mathsf{Share}_{\mathcal{S}_M}(0)$.*

Proof. Clearly, $\mathsf{Share}_{\mathcal{S}_M}(0) \subseteq \mathcal{R}(\mathcal{S}_M)^\perp$. To prove that $\mathcal{R}(\mathcal{S}_M)^\perp \subseteq \mathsf{Share}_{\mathcal{S}_M}(0)$, suppose for a contradiction that there exists $\boldsymbol{z} \in \mathcal{R}(\mathcal{S}_M)^\perp \setminus \mathsf{Share}_{\mathcal{S}_M}(0)$. Then the columns of the matrix $(\boldsymbol{z}||M) \in \mathbb{K}^{d\times(e+1)}$ are $e+1$ linearly independent: if $c_1 M^1 + c_2 M^2 + \cdots + c_e M^e + c_{e+1}\boldsymbol{z} = \mathbf{0}$, where M^i denotes the ith column of M, then for all $\boldsymbol{r} \in \mathcal{R}(\mathcal{S}_M)$, $0 = c_1 \boldsymbol{r}^T M^1 + c_2 \boldsymbol{r}^T M^2 +$

$\cdots + c_e \boldsymbol{r}^T M^e + c_{e+1} \boldsymbol{r}^T \boldsymbol{z} = c_1$. This implies that $c_1 = 0$, which in turn implies, by the linear independence of $\boldsymbol{z}, M^2, \ldots, M^e$, that $c_2 = \cdots = c_{e+1} = 0$. The matrix $(\boldsymbol{z}||M)$ thus has $e+1$ linearly independent rows. Every $\boldsymbol{r} \in \mathcal{R}(\mathcal{S}_M)$ is a solution of the system of linear equations

$$\begin{cases} r_1 m_{11} + r_2 m_{21} + \cdots + r_d m_{d1} = 1 \\ r_1 m_{12} + r_2 m_{22} + \cdots + r_d m_{d2} = 0 \\ \vdots \\ r_1 m_{1e} + r_2 m_{2e} + \cdots + r_d m_{de} = 0 \\ r_1 z_1 + r_2 z_2 + \cdots + r_d z_d = 0 \end{cases},$$

which has precisely $|\mathbb{K}^{d-(e+1)}|$ solutions. This contradicts the fact that $|\mathcal{R}(\mathcal{S}_M)| = |\mathbb{K}|^{d-e}$. Thus, $\mathcal{R}(\mathcal{S}_M)^\perp \subseteq \mathsf{Share}_{\mathcal{S}_M}(0)$. ■

Lemma 3.3.7 *Let $M, N \in \mathbb{L}^{d \times e}$ be two matrices such that* $\operatorname{rank} M = e$*, and let $C \in \mathbb{L}^{e \times e}$ be a matrix such that $N = MC$. If* $\operatorname{rank} N = e$ *then the matrix C is invertible.*

Proof. If C is not invertible, then there exist scalars $c_1, \ldots, c_e \in \mathbb{L}$ such that $c_1 C^1 + \cdots + c_e C^e = \mathbf{0}$, and at least for one i, $c_i \neq 0$. Multiplying by M yields $\mathbf{0} = c_1 MC^1 + \cdots + c_e MC^e = c_1 N^1 + \cdots + c_e N^e$. Hence, the columns of N are linearly dependent. ■

Lemma 3.3.8 *Let $M, N \in \mathbb{K}^{d \times e}$ be two matrices such that* $\operatorname{rank} M = e$*, and let $C \in \mathbb{K}^{e \times e}$ be a matrix such that $N = MC$. If the matrix C is invertible then* $\operatorname{rank} N = e$*.*

Proof. If $\mathbf{0} = c_1 N^1 + \cdots + c_e N^e = M(c_1 C^1 + \cdots + c_e C^e)$ for scalars $c_1, \ldots, c_e \in \mathbb{K}$, then, by the rank-nullity theorem, $c_1 C^1 + \cdots + c_e C^e = \mathbf{0}$. If C is invertible, then $c_1 = \cdots = c_e = 0$, and hence, the columns of N are linearly independent. ■

For threshold linear secret sharing schemes, only subsets of reconstruction vectors rather than the complete sets of reconstruction vectors need to coincide for two threshold LSSSs to coincide.

Lemma 3.3.9 *Let A be a minimal qualified subset, and let $\boldsymbol{r} \in \mathbb{L}^{d_A}$ be a reconstruction vector for A. Then the elements $r_1, \ldots, r_{d_A}$ are invertible.*

Proof. For a contradiction, suppose wlog that r_{d_A} is not invertible. Then, by Fact 2.1.19, r_{d_A} is a zero divisor. Let $z \in \mathbb{L} \setminus 0$ be such that $r_{d_A} z = 0$. Then, $zs = z(r_1 s_1 + \cdots + r_{d_A - 1} s_{d_A - 1} + r_{d_A} s_{d_A}) = z(r_1 s_1 + \cdots + r_{d_A - 1} s_{d_A - 1})$. Hence, players $P_1, \ldots, P_{d_A - 1}$ are able to deduce partial information about

the secret s together. This contradicts the security of the LSSS. ■

Lemma 3.3.10 *Let $\mathcal{S}_1$ and $\mathcal{S}_2$ be two $(t+1)$-out-of-n threshold linear secret sharing schemes over the field $\mathbb{K}$ for the threshold access structure $\Gamma_{t,n} = \{|A| \subset \{1,\ldots,n\} : |A| > t\}$. Let $\mathcal{R} = \{\boldsymbol{r_1},\ldots,\boldsymbol{r_{n-t}}\} \subset \mathcal{R}(\mathcal{S}_1) \cap \mathcal{R}(\mathcal{S}_2)$ be such that for each i, $t+1 \leq i \leq n$ there exists $\boldsymbol{r} \in \mathcal{R}$ such that $\boldsymbol{r}$ is a reconstruction vector for some A of size i. Then $\mathcal{S}_1 = \mathcal{S}_2$.*

Proof. Let R_1 be the concatenation of all reconstruction vectors of $\mathcal{S}_1$, and let R_2 be the concatenation of all reconstruction vectors of $\mathcal{S}_2$. Note that by Lemmas 3.3.6 and 5.2.1, $\dim \operatorname{Ker} R_1^T = \dim \operatorname{Ker} R_2^T = t$. By the rank-nullity theorem, $\operatorname{rank} R_1^T = \operatorname{rank} R_2^T = n - t$. Wlog, $\boldsymbol{r_1} = \boldsymbol{r_{\{1,\ldots,t+1\}}}, \ldots, \boldsymbol{r_{n-t}} = \boldsymbol{r_{\{1,\ldots,n\}}}$. Let $R = (\boldsymbol{r}_1||\cdots||\boldsymbol{r}_{n-t})$. For a contradiction, suppose that $\operatorname{rank} R^T < n - t$. Then there exist $c_1,\ldots,c_{n-t} \in \mathbb{K}$ such that $c_i \neq 0$ for some i such that $c_{n-t}\boldsymbol{r_{\{1,\ldots,n\}}} = c_1\boldsymbol{r_{\{1,\ldots,t+1\}}} + \cdots + c_{n-t-1}\boldsymbol{r_{\{1,\ldots,n-1\}}}$. This implies that $c_1 r_{\{1,\ldots,n\}n} = 0$, which by Lemma 3.3.9 contradicts $r_{\{1,\ldots,n\}n} \neq 0$. Hence, $\operatorname{rank} R^T = n - t$, and hence, $\mathcal{R}(\mathcal{S}_1) = \mathcal{R} = \mathcal{R}(\mathcal{S}_2)$ By Corollary 3.3.5, $\mathcal{S}_1 = \mathcal{S}_2$. ■

Not every set of vectors, however, is a set of reconstruction vectors for some linear secret sharing scheme over a given field $\mathbb{K}$.

Lemma 3.3.11 *Let $\mathcal{R} = \{\boldsymbol{r_1},...,\boldsymbol{r_k}\} \subset \mathbb{K}^d$ be a set of vectors. Let $R = (\boldsymbol{r_1}||...||\boldsymbol{r_k})$. Then $\mathcal{R}$ is a set of reconstruction vectors if and only if*

- $\mathbf{1} \in \operatorname{Im} R^T$, *and*
- $\exists e \in \mathbb{Z}_+$ *such that* $k = |\mathbb{K}|^{d-e}$ *and* $\dim \operatorname{Ker} R^T = e - 1$.

Proof. If $\mathcal{R}$ is a set of reconstruction vectors then there exists a matrix $M \in \mathbb{K}^{d\times e}$ for some $e \in \mathbb{Z}_+$ such that $\mathcal{R} = \mathcal{R}(\mathcal{S}_M)$. By Lemma 3.3.2, $k = \mathcal{R}(\mathcal{S}_M) = |\mathbb{K}|^{d-e}$, and by Lemma 3.3.6, $\dim \operatorname{Ker} R^T = \dim \mathsf{Share}_{\mathcal{S}_M}(0) = e - 1$. For all $\boldsymbol{r} \in \mathcal{R}(\mathcal{S}_M)$, $\boldsymbol{r}^T M^1 = 1$, and hence, $R^T M^1 = \mathbf{1}$.

Conversely, if there exists $e \in \mathbb{Z}_+$ such that $\dim \operatorname{Ker} R^T = e - 1$, and $\mathbf{1} \in \operatorname{Im} R^T$, let $\boldsymbol{m} \in \mathbb{K}^d$ be such that $R^T\boldsymbol{m} = \mathbf{1}$, and let $\boldsymbol{m'_1},\ldots,\boldsymbol{m'_{e-1}}$ be a basis of $\operatorname{Ker} R^T$. Define $M = (\boldsymbol{m}||\boldsymbol{m'_1}||\cdots||\boldsymbol{m'_{e-1}})$. Then, for all $\boldsymbol{r} \in \mathcal{R}$, $\boldsymbol{r}^T M = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$. Hence, $\mathcal{R}$ is a set of reconstruction vectors for $\mathcal{S}_M$. ■

Example 3.3.12 Let $\mathcal{R} = \{\boldsymbol{e_1},\boldsymbol{e_2},\boldsymbol{e_3},\boldsymbol{e_4}\}$, and let $\mathbb{K} = \mathbb{Z}_5$. Clearly, $4 \neq 5^{d-e}$ for all $d, e \in \mathbb{Z}_+$.

3.3.1 Algorithm: isRec($\boldsymbol{r}$,M)

Let $\mathcal{S}_{\mathcal{M}} = (\mathbb{L}, M)$ be a linear secret sharing scheme over a ring $\mathbb{L}$ with share distribution matrix M. In this subsection, we present an algorithm to check whether a vector r is a reconstruction vector for $\mathcal{S}_{\mathcal{M}}$.

Naively, we may do the following:

Algorithm 1 isRec($\boldsymbol{r}$,M)

for all $\boldsymbol{b}$ **do**
  if $\boldsymbol{r} \cdot (M\boldsymbol{b}) \neq b_1$ **then**
    return false
  end if
end for
return true

This algorithm is highly inefficient since the number of computations increases exponentially with the number of columns of M. Lemma 3.1.9 allows for a more efficient algorithm. The following algorithm is more efficient since the number of computations increases only linearly with the number of columns of M.

Algorithm 2 isRec($\boldsymbol{r}$,M)

if $\boldsymbol{r}^T M = \begin{pmatrix} 1 & 0 & \cdots 0 \end{pmatrix}$ **then**
  return true
end if
return false

Note that for both algorithms the number of computations increases linearly with the size of $\mathcal{S}$.

3.4 A Partial Order on Linear Secret Sharing Schemes

In this section, we will define a partial order on linear secret sharing schemes for a fixed access structure Γ. This partial order was first defined by R. Cramer, I. Damgård, and Y. Ishai in [7].

Definition 3.4.1 Let $\mathcal{S}, \mathcal{S}'$ be two secret sharing schemes over $\mathbb{L}$. $\mathcal{S}$ is said to be *locally convertible* to $\mathcal{S}'$ if there exist local conversion functions $g_1, ..., g_n$ such that if $(\boldsymbol{s_1}, \ldots, \boldsymbol{s_n})$ is a valid sharing of a secret s in $\mathcal{S}$, then $(g_1(\boldsymbol{s_1}), \ldots, g_n(\boldsymbol{s_n}))$ is a valid sharing of the same secret s in $\mathcal{S}'$. We define $g(\boldsymbol{s_1}, \ldots, \boldsymbol{s_n}) = (g_1(\boldsymbol{s_1}), \ldots, g_n(\boldsymbol{s_n}))$. The function g is said to be a *share conversion function.*

Notation 3.4.2 *Let $\mathcal{S}, \mathcal{S}'$ be two secret sharing schemes over $\mathbb{L}$. If $\mathcal{S}$ is locally convertible to $\mathcal{S}'$, we denote this by $\mathcal{S} \Rightarrow \mathcal{S}'$.*

Notation 3.4.3 *Let $\mathcal{S}, \mathcal{S}'$ be two secret sharing schemes over $\mathbb{L}$. If $\mathcal{S}$ is locally convertible to $\mathcal{S}'$ with share conversion function g such that for any secret $s \in \mathbb{L}$, $g(\mathsf{Share}_{\mathcal{S}}(s)) \equiv \mathsf{Share}_{\mathcal{S}'}(s)$, we denote this by $\mathcal{S} \geq \mathcal{S}'$.*

Notation 3.4.4 *Let $\mathcal{S}, \mathcal{S}'$ be two secret sharing schemes over $\mathbb{L}$. If there exists a permutation $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ such that for any secret $s \in \mathbb{L}$ and any valid sharing $(\boldsymbol{s_1}, \ldots, \boldsymbol{s_n})$ of s in $\mathcal{S}$, $(\boldsymbol{s_{\pi(1)}}, \ldots, \boldsymbol{s_{\pi(n)}})$ is a valid sharing of s in $\mathcal{S}'$, we denote this by $\mathcal{S} \cong \mathcal{S}'$.*

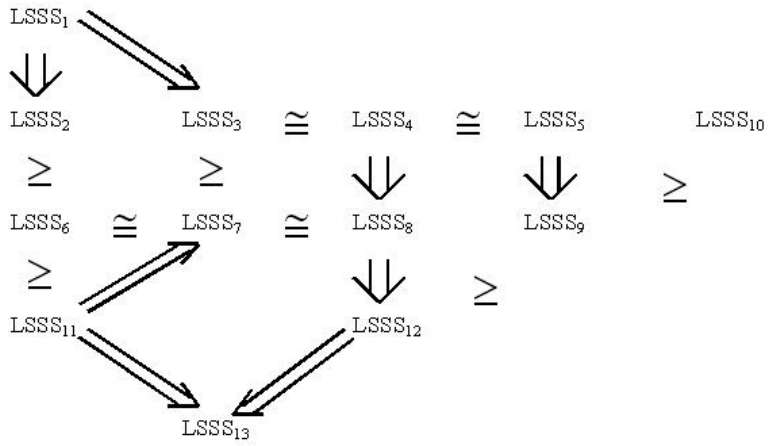

Figure 3.4: Partial ordering of LSSSs

In the ordering defined by Cramer, Damgård, and Ishai, an LSSS is said to be maximal if it is locally convertible to any other LSSS, and an LSSS is said to be minimal if any other LSSS is locally convertible to this LSSS. We will prove that the CNF-based scheme (or replicated secret sharing scheme) is maximal, and that the DNF-based scheme is minimal.

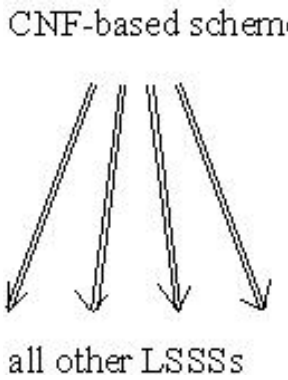

Figure 3.5: maximal LSSS

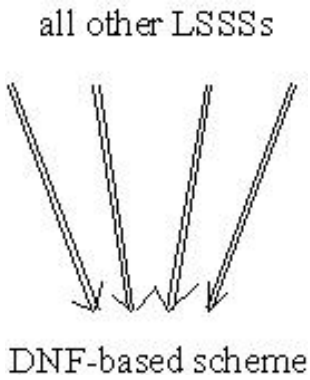

Figure 3.6: minimal LSSS

In the following, we will denote by $\mathcal{S}_{\mathcal{M}}$ the LSSS corresponding to the MSP $\mathcal{M} = (M, \mathbb{L}, \boldsymbol{a})$, and we will denote by $\mathcal{S}_{\hat{\mathcal{M}}}$ the LSSS corresponding to the canonical MSP $\hat{\mathcal{M}} = (\hat{M}, \mathbb{L}, \mathbf{1})$. Let $\boldsymbol{c_T}$ and $\boldsymbol{w_T}$ be as defined in section 3.2.

Lemma 3.4.5 *Let Γ be a monotone access structure. The CNF-based scheme $\mathcal{R}_\Gamma$ is locally convertible to the LSSS $\mathcal{S}_{\hat{\mathcal{M}}}$.*

Proof. Let $\mathcal{T}$ be the set of maximal unqualified subsets of Γ, let $s \in \mathbb{L}$ be a secret, and let $s = \sum_{T \in \mathcal{T}} r_T$ be a $\mathcal{R}_\Gamma$-sharing of s. Denote the vector of $\mathcal{R}_\Gamma$-shares by $\boldsymbol{r} = (r_T)_{T \in \mathcal{T}}$, and denote by $\boldsymbol{s_i} = (r_T)_{T \not\ni i}$ the vector of $\mathcal{R}_\Gamma$-shares given to player P_i. We denote by $\boldsymbol{s}$ the vector $(\boldsymbol{s_1}, \ldots, \boldsymbol{s_n})$.

For $1 \leq i \leq n$, we define the ith conversion function by

$$g_i(\boldsymbol{s_i}) = \sum_{T \not\ni i} r_T \cdot \boldsymbol{c_{T_i}},$$

and the share conversion function g by $g(\boldsymbol{s}) = (g_1(\boldsymbol{s_1}), \ldots, g_n(\boldsymbol{s_n}))$. Then,

$$\begin{aligned}\hat{M}\boldsymbol{r} &= \sum_{T \in \mathcal{T}} r_T \cdot \boldsymbol{c_T} = \sum_{T \in \mathcal{T}} r_T \cdot (M\boldsymbol{w_T}) = r_T \cdot (\sum_{T \not\ni 1} M_1 \boldsymbol{w_{T_1}}, \ldots, \sum_{T \not\ni n} M_n \boldsymbol{w_{T_n}}) \\ &= (\sum_{T \not\ni 1} r_T \cdot \boldsymbol{c_{T_1}}, \ldots, \sum_{T \not\ni n} r_T \cdot \boldsymbol{c_{T_n}}) = g(\boldsymbol{s}).\end{aligned}$$

Thus, $g(\boldsymbol{s})$ is a valid $\mathcal{S}_{\hat{\mathcal{M}}}$-sharing of s. ■

Lemma 3.4.6 *Let Γ be a monotone access structure. The LSSS $\mathcal{S}_{\hat{\mathcal{M}}}$ is locally convertible to the LSSS $\mathcal{S}_{\mathcal{M}}$.*

Proof. Let $s \in \mathbb{L}$ be a secret, and let $\boldsymbol{s} = \hat{M}\boldsymbol{r}$ be an $\mathcal{S}_{\hat{\mathcal{M}}}$-sharing of s. Let $\boldsymbol{b} = W\boldsymbol{r}$. Note that $\hat{M}\boldsymbol{r} = MW\boldsymbol{r} = M\boldsymbol{b}$, and that $\boldsymbol{a} \cdot \boldsymbol{b} = \boldsymbol{a} \cdot (W\boldsymbol{r}) = (W^T\boldsymbol{a}) \cdot \boldsymbol{r} = \mathbf{1} \cdot \boldsymbol{r} = s$. Thus, $\boldsymbol{s}$ is a valid $\mathcal{S}_{\mathcal{M}}$-sharing of s. ■

Theorem 3.4.7 *Let Γ be a monotone access structure. The CNF-based scheme $\mathcal{R}_\Gamma$ is locally convertible to any LSSS for Γ.*

Proof. Let $\mathcal{S}$ be an LSSS. By Theorem 3.2.13, $\mathcal{S} = \mathcal{S}_{\mathcal{M}}$ for some MSP $\mathcal{M}$. Let $\hat{\mathcal{M}}$ be the canonical MSP. By Lemma 3.4.5, $\mathcal{R}_\Gamma$ is locally convertable to $\mathcal{S}_{\hat{\mathcal{M}}}$, and by Lemma 3.4.6, $\mathcal{S}_{\hat{\mathcal{M}}}$ is locally convertable to $\mathcal{S}_{\mathcal{M}} = \mathcal{S}$. ■

Theorem 3.4.8 *Let Γ be a monotone access structure. Any LSSS for Γ is locally convertible to the DNF-based scheme for Γ.*

Proof. Let $\mathcal{S}$ be an LSSS. Let $s \in \mathbb{L}$ be a secret, and let $\boldsymbol{s}$ be an $\mathcal{S}$-sharing of s. Let $\mathcal{Q}$ be the set of all minimal qualified subsets of Γ. For $Q \in \mathcal{Q}$, let $\boldsymbol{r_Q}$ be a reconstruction vector for Q. Each player P_j computes $r_{Qj} = \boldsymbol{r_{Q_j}} \cdot \boldsymbol{s_{Q_j}}$ for each $Q \in \mathcal{Q}$ such that $j \in Q$. Then, for each $Q \in \mathcal{Q}$, $\sum_{j \in Q} r_{Qj} = \boldsymbol{r_Q} \cdot \boldsymbol{s_Q} = s$. ■

By Theorems 3.4.7 and 3.4.8, we may now define a partial ordering on linear secret sharing schemes. In this ordering, the DNF-based secret sharing scheme is minimal by Theorem 3.4.8, and the replicated secret sharing scheme, or CNF-based secret sharing scheme, is maximal by Theorem 3.4.7. Both theorems are due to [7].

As an example, we will prove directly that the CNF-based scheme (or replicated secret sharing scheme) is locally convertible to Shamir's secret sharing scheme. The proof is due to [7].

Proposition 3.4.9 *Let $\Gamma_{t,n}$ be a threshold access structure. The replicated secret sharing scheme $\mathcal{R}_{\Gamma_{t,n}}$ is locally convertible to Shamir's secret sharing scheme.*

Proof. Let $s \in \mathbb{K}$ be a secret. The maximal unqualified subsets of $\Gamma_{t,n}$ are precisely the unqualified subsets of cardinality t. This means that for each maximal unqualified subset A, a subset of players of cardinality $|\overline{A}| = n - |A| = n - t$ is given share r_A, namely the players in $\overline{A}$. Therefore,

$$s = \sum_{A \subseteq \{1,\ldots,n\} : |A| = n-t} r_A,$$

where r_A has been given to all players in A.

For each $A \subseteq \{1, \ldots, n\}$ of cardinality $n - t$, we define a polynomial f_A of degree t by $f_A(0) = 1$, and $f_A(i) = 0$ for all $i \notin A$. Further, we define the polynomial f by

$$f = \sum_{A \subseteq \{1,\ldots,n\} : |A| = n-t} r_A \cdot f_A.$$

Each player P_i, $1 \leq i \leq n$, computes

$$s_i = \sum_{A \subseteq \{1,\ldots,n\} : |A| = n-t, i \in A} r_A \cdot f_A(i).$$

Then, $f(0) = s$, $s_i = f(i)$, and f is of degree t. ■

Not all LSSSs for the same monotone access structure are locally convertible to each other. In particular, we prove that Shamir's secret sharing scheme is generally not locally convertible to the replicated secret sharing scheme [7].

Proposition 3.4.10 *Let* $\Gamma_{1,3}$ *be the threshold access structure* $\{\{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$. *Shamir's secret sharing scheme is not locally convertible to the replicated secret sharing scheme* $\mathcal{R}_{\Gamma_{1,3}}$.

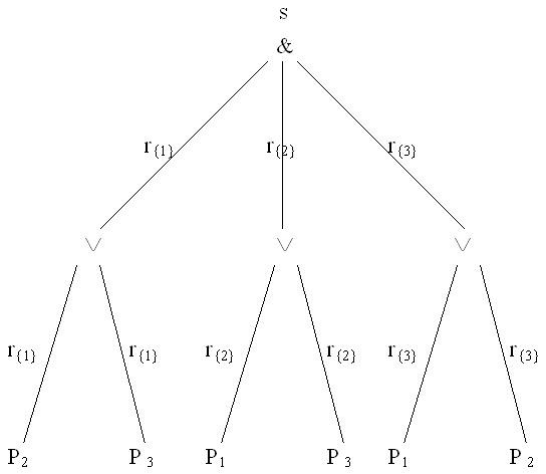

Figure 3.7: CNF-based scheme for the threshold access structure $\Gamma_{1,3}$

Proof. Let (s_1, s_2, s_3) be a valid tuple of Shamir shares. For any share conversion function g, $g(s_1, s_2, s_3) = ((g_1(s_1)_1, g_1(s_1)_2), (g_2(s_2)_1, g_2(s_2)_2), (g_3(s_3)_1, g_3(s_3)_2))$ is a valid tuple of $\mathcal{R}_{\Gamma_{1,3}}$-shares only if $g_1(s_1)_1 = g_3(s_1)_2$, $g_1(s_1)_2 = g_2(s_2)_2$, and $g_2(s_2)_1 = g_3(s_3)_1$.

We now prove by contradiction that any such g must be constant. If g is not constant, then one of the g_i is not constant. Wlog g_1 is not constant, and there exist $a, b \in \mathbb{K}$ such that $g_1(a) \neq g_1(b)$. Again wlog, $g_1(a)_1 \neq g_1(b)_1$. By Lemma 3.4.11 below, there exists a Shamir share s_2 such that (a, s_2, a) is a valid tuple of Shamir shares, and there exists a Shamir share s_2' such that (b, s_2', a) also is a valid tuple of Shamir shares. Now, $g(a, s_2, a) = ((g_1(a)_1, g_1(a)_2), (g_2(s_2)_1, g_2(s_2)_2), (g_3(a)_1, g_3(a)_2))$, and $g(b, s_2', a) = ((g_1(b)_1, g_1(b)_2), (g_2(s_2')_1, g_2(s_2')_2), (g_3(a)_1, g_3(a)_2))$. By the above, $g_1(a)_1 = g_3(a)_2 = g_1(b)_1$. This contradicts $g_1(a)_1 \neq g_1(b)_1$.

No share conversion function, however, can be constant. ■

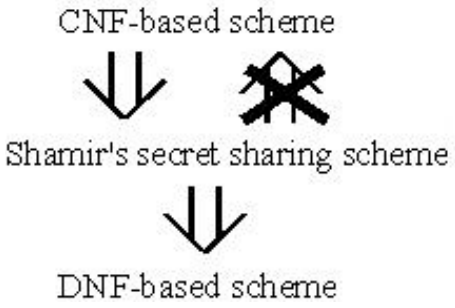

Figure 3.8: Shamir's secret sharing scheme in the partial ordering of LSSSs

Lemma 3.4.11 *For any $a, b \in \mathbb{K}$, there exists $s_2 \in \mathbb{K}$ such that (a, s_2, b) is a valid tuple of Shamir shares.*

Proof. A tuple (s_1, s_2, s_3) is a valid tuple of Shamir shares if and only if there exist $s, b_2 \in \mathbb{K}$ such that

$$\begin{cases} s_1 = s + b_2 \\ s_2 = s + 2b_2 \\ s_3 = s + 3b_2 \end{cases}.$$

Hence, (a, s_2, b) is a valid tuple of Shamir shares only if there exist $s, b_2 \in \mathbb{K}$ such that

$$\begin{cases} s + b_2 = a \\ s + 3b_2 = b \end{cases}.$$

The unique solution to this system of linear equations is $s = \frac{1}{2}(3a - b)$, and $b_2 = \frac{1}{2}(b - a)$. Define $s_2 = s + 2b_2 = \frac{1}{2}(a + b)$. ■

Chapter 4

Multiplicative Linear Secret Sharing Schemes

Secret sharing is an important concept in secure multi-party computation. Multi-party computation was first introduced by A. C. Yao in 1982 [18] and later extended to secret sharing by D. Chaum, C. Crépeau, and I. Damgård in 1988 [6].

Consider two secrets s and t which have been split into two sets of shares $\{s_1, s_2, \ldots, s_n\}$ and $\{t_1, t_2, \ldots, t_n\}$. Each player has been given one or more shares of each secret. Secure multi-party computation allows the players to do computations on s and t by doing computations on their shares.

In any linear secret sharing scheme, n shares of the sum of s and t may be computed by adding shares s_i and t_i for each $i = 1, \ldots, n$. These n shares may then be recombined into the sum of s and t.

In this chapter, we will define multiplicative linear secret sharing schemes. In a multiplicative LSSS, n shares of the product of s and t may be computed by computing the product of the shares s_i and t_i for each $i = 1, \ldots, n$. These n shares may then be recombined into the product of s and t.

Multiplication and addition are necessary and sufficient for secure multi-party computation: for any $a, b \in \{0, 1\}$,

$$a \wedge b = a \cdot b,\ a \vee b = a + b - a \cdot b, \text{ and } \neg a = 1 - a.$$

In section 4.1, we will formally define multiplicative linear secret sharing schemes. Shamir's secret sharing scheme will be presented as an example of a multiplicative LSSS. In sections 4.2 and 4.3, we will, as in sections 3.2 and 3.3, present two characterisations of multiplicative linear secret sharing schemes.

4.1 Functional Definition

Let s, $t \in \mathbb{L}$ be secrets that have been split into sets of shares $\boldsymbol{s}$, $\boldsymbol{t}$, respectively, by a linear secret sharing scheme. Let $\mathcal{A}$ be the adversary structure.

Definition 4.1.1 An LSSS is said to be *pointwise multiplicative* if there exists a fixed d-vector $\boldsymbol{r}$ such that $\boldsymbol{r} \cdot (\boldsymbol{s} \star \boldsymbol{t}) = st$.

Definition 4.1.2 We say that a matrix $D = (d_{ij}) \in \mathbb{L}^{d \times d}$ is a *local multiplicativity matrix* if $d_{ij} \neq 0$ only if both share s_i and share s_j are given to the same player P_k, $k \in \{1, \ldots, n\}$. For $1 \leq k \leq n$, we denote by $D_k \in \mathbb{L}^{d_k \times d_k}$ the submatrix of D with rows i and columns j of D such that both share s_i and share s_j are given to player P_k.

Definition 4.1.3 An LSSS is said to be *locally multiplicative* if there exist a fixed d-vector $\boldsymbol{r}$ and a local multiplicativity matrix $D \in \mathbb{L}^{d \times d}$ such that $\boldsymbol{r} \cdot (\boldsymbol{s} \star (D\boldsymbol{t})) = st$.

In general, in a multiplicative LSSS all players – the honest players as well as the dishonest ones – need to cooperate to reconstruct the product of s and t. In a strongly multiplicative LSSS, the dishonest players do not need to cooperate. Let $C \subset \mathcal{P}$ be the subset of dishonest players. Clearly, $C \in \mathcal{A}$. The remaining honest $n - |C|$ players in $\overline{C}$ should be able to reconstruct the product of s and t on their own.

Definition 4.1.4 An LSSS is said to be *pointwise strongly multiplicative* if for each $A \in \mathcal{A}$ there exists a $d_{\overline{A}}$-vector $\boldsymbol{r}_{\overline{\boldsymbol{A}}}$ such that $\boldsymbol{r}_{\overline{\boldsymbol{A}}} \cdot (\boldsymbol{s}_{\overline{\boldsymbol{A}}} \star \boldsymbol{t}_{\overline{\boldsymbol{A}}}) = st$.

Definition 4.1.5 An LSSS is said to be *locally strongly multiplicative* if for each $A \in \mathcal{A}$ there exist a $d_{\overline{A}}$-vector $\boldsymbol{r}_{\overline{\boldsymbol{A}}}$ and a local multiplicativity matrix $D_{\overline{A}} \in \mathbb{L}^{d_{\overline{A}} \times d_{\overline{A}}}$ such that $\boldsymbol{r}_{\overline{\boldsymbol{A}}} \cdot (\boldsymbol{s}_{\overline{\boldsymbol{A}}} \star (D_{\overline{A}} \boldsymbol{t}_{\overline{\boldsymbol{A}}})) = st$.

Lemma 4.1.6 *Let $\mathcal{S}_M = (\mathbb{L}, M)$ be a linear secret sharing scheme over a commutative ring $\mathbb{L}$ with share distribution matrix $M = (\boldsymbol{m}||M')$. Let $M'^{\star} = (M' \star M'||\boldsymbol{m} \star M')$, and let $M^{\star} = (\boldsymbol{m} \star \boldsymbol{m}||M'^{\star})$. Then $\mathcal{S}$ is multiplicative if and only if there exists a vector $\boldsymbol{r}$ such that $\boldsymbol{r}^T M'^{\star} = \boldsymbol{0}$ and $\boldsymbol{r}^T(\boldsymbol{m} \star \boldsymbol{m}) = 1$.*

Proof. If $\mathcal{S}$ is multiplicative then by definition there exists a vector $\boldsymbol{r}$ such that $\boldsymbol{r}^T((M\boldsymbol{b_1}) \star (M\boldsymbol{b_2})) = b_{11}b_{21}$ for all $\boldsymbol{b_1}, \boldsymbol{b_2}$. In particular,

$$\boldsymbol{r}^T(\underbrace{(M\boldsymbol{e_1}) \star (M\boldsymbol{e_1})}_{\boldsymbol{m} \star \boldsymbol{m}}) = 1,$$

$$\boldsymbol{r}^T(\underbrace{(M\boldsymbol{e_1}) \star (M\boldsymbol{e_i})}_{\boldsymbol{m} \star M^i}) = 0 \text{ for all } i > 1, \text{ and}$$

$$\boldsymbol{r}^T(\underbrace{(M\boldsymbol{e_i}) \star (M\boldsymbol{e_j})}_{M^i \star M^j}) = 0 \text{ for all } i, j > 1.$$

Hence, $\boldsymbol{r}^T M'^{\star} = \mathbf{0}$ and $\boldsymbol{r}^T(\boldsymbol{m} \star \boldsymbol{m}) = 1$.

Conversely, if there exists a vector $\boldsymbol{r}$ such that $\boldsymbol{r}^T M'^{\star} = \mathbf{0}$ and $\boldsymbol{r}^T(\boldsymbol{m} \star \boldsymbol{m}) = 1$ then for any $s, t \in \mathbb{L}$, $\boldsymbol{r}^T(\mathsf{Share}(s) \star \mathsf{Share}(t)) = \boldsymbol{r}^T(st(\boldsymbol{m} \star \boldsymbol{m}) + (s + t)(\boldsymbol{m} \star M') + M' \star M') = st$. Hence, $\mathcal{S}$ is multiplicative. ■

Note that, a priori, this $\boldsymbol{r}$ is not the same as the original $\boldsymbol{r}$ from section 3.1. In the following, we will say that $\boldsymbol{r}$ is a reconstruction vector for multiplication if $\boldsymbol{r} \cdot (\boldsymbol{s} \star \boldsymbol{t}) = st$ for all $s, t \in \mathbb{L}$, and we will say that $\boldsymbol{r}$ is a reconstruction vector for addition if $\boldsymbol{r} \cdot \boldsymbol{s} = s$ for all $s \in \mathbb{L}$.

Example 4.1.7 Let $\mathbb{L} = \mathbb{Z}_5$. Let M be the 3×2 share distribution matrix

$$M = \begin{pmatrix} 1 & 2 \\ 2 & 3 \\ 3 & 4 \end{pmatrix}$$

The reconstruction vectors for addition are

$$\begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \\ 4 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 3 \\ 2 \end{pmatrix},$$

and the only reconstruction vector for multiplication is

$$\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}.$$

Lemma 4.1.8 *Let $\mathcal{S}$ be a multiplicative LSSS over a commutative ring $\mathbb{L}$. Let $M = (\boldsymbol{m}||M) \in \mathbb{L}^{d \times e}$ be the share distribution matrix. For any reconstruction vector $\boldsymbol{r}$ for multiplication of $\mathcal{S}$, $\boldsymbol{r'} = \boldsymbol{m} \star \boldsymbol{r}$ is a reconstruction vector for addition of $\mathcal{S}$.*

Proof. If $\boldsymbol{r}$ is a reconstruction vector for multiplication of $\mathcal{S}$, then for all $\boldsymbol{b'_1}, \boldsymbol{b'_2} \in \mathbb{L}^{e-1}$ and for all $s, t \in \mathbb{L}$, $\boldsymbol{r} \cdot ((M(s||\boldsymbol{b'_1})) \star (M(t||\boldsymbol{b'_2}))) = st$. In particular, fix $t = 1$ and $\boldsymbol{b'_2} = \mathbf{0}$. Then $t = \boldsymbol{r} \cdot ((M(s||\boldsymbol{b'_1})) \star \boldsymbol{m}) = (\boldsymbol{m} \star \boldsymbol{r}) \cdot (M(s||\boldsymbol{b'_1}))$ for all $\boldsymbol{b'_1} \in \mathbb{L}^{e-1}$ and for all $s \in \mathbb{L}$. This proves that $\boldsymbol{r'}$ is a reconstruction vector for addition of $\mathcal{S}$. ■

Definition 4.1.9 We say that a pointwise multiplicative LSSS is *homomorphic* if there exists a reconstruction vector $\boldsymbol{r}$ such that $\boldsymbol{r} \cdot (\boldsymbol{s} \star \boldsymbol{t}) = (\boldsymbol{r} \cdot \boldsymbol{s})(\boldsymbol{r} \cdot \boldsymbol{t})$.

Definition 4.1.10 We say that a pointwise strongly multiplicative LSSS is *homomorphic* if for each $A \in \mathcal{A}$ there exists a reconstruction vector $\boldsymbol{r}_{\overline{A}}$ such that $\boldsymbol{r}_{\overline{A}} \cdot (\boldsymbol{s}_{\overline{A}} \star \boldsymbol{t}_{\overline{A}}) = (\boldsymbol{r}_{\overline{A}} \cdot \boldsymbol{s}_{\overline{A}})(\boldsymbol{r}_{\overline{A}} \cdot \boldsymbol{t}_{\overline{A}})$.

Lemma 4.1.11 *A linear secret sharing scheme $\mathcal{S}_{\mathcal{M}} = (\mathbb{L}, M)$ over a commutative ring $\mathbb{L}$ with share distribution matrix $M \in \mathbb{L}^{d \times e}$ is homomorphic if and only if there exists a reconstruction vector $\boldsymbol{r} = \begin{pmatrix} r_1 & \cdots & r_d \end{pmatrix}^T$ such that*

$$(\operatorname{Im} M)^T (\operatorname{diag} \boldsymbol{r} - \boldsymbol{r}^T \boldsymbol{r}) \operatorname{Im} M = 0.$$

Proof. By definition, $\mathcal{S}_{\mathcal{M}}$ is homomorphic if and only if there exists a reconstruction vector $\boldsymbol{r}$ such that $\boldsymbol{r} \cdot ((M\boldsymbol{b_1}) \star (M\boldsymbol{b_2})) = (\boldsymbol{r} \cdot (M\boldsymbol{b_1}))(\boldsymbol{r} \cdot (M\boldsymbol{b_2}))$ for all $\boldsymbol{b_1}, \boldsymbol{b_2} \in \mathbb{L}^e$. Note that $\boldsymbol{r} \cdot ((M\boldsymbol{b_1}) \star (M\boldsymbol{b_2})) = (M\boldsymbol{b_1})^T \operatorname{diag} \boldsymbol{r} (M\boldsymbol{b_2})$, and that $(\boldsymbol{r} \cdot (M\boldsymbol{b_1}))(\boldsymbol{r} \cdot (M\boldsymbol{b_2})) = (M\boldsymbol{b_1})^T \boldsymbol{r}^T \boldsymbol{r} (M\boldsymbol{b_2})$. Equivalently, $(\operatorname{Im} M)^T (\operatorname{diag} \boldsymbol{r} - \boldsymbol{r}^T \boldsymbol{r}) \operatorname{Im} M = 0$. ■

The following is a corollary of Lemma 4.1.8.

Corollary 4.1.12 *Let $\mathcal{S}$ be a multiplicative LSSS over a commutative ring $\mathbb{L}$. Let $M = (\boldsymbol{m} || M) \in \mathbb{L}^{d \times e}$ be the share distribution matrix. If $\mathbf{1} \in \mathsf{Share}(1)$ then $\mathcal{S}$ is homomorphic.*

However, if $\mathcal{S}$ is homomorphic, then it is not true in general that $\mathbf{1} \in \mathsf{Share}(1)$. Over $\mathbb{Z}_5$, there are 2323 homomorphic multiplicative linear secret sharing schemes with 3×2 share distribution matrices. Only for 421 of those, $\mathbf{1} \in \mathsf{Share}(1)$.

Example 4.1.13 Let $\mathbb{L} = \mathbb{Z}_5$. Let M be the 3×2 share distribution matrix

$$M = \begin{pmatrix} 2 & 4 \\ 3 & 2 \\ 1 & 0 \end{pmatrix}$$

Let $\mathcal{S}$ be the LSSS defined by $\boldsymbol{s} = M\boldsymbol{b}$. Note that $\mathcal{S}$ is homomorphic: the vector $(0, 0, 1)^T$ is a reconstruction vector for both addition and multiplication. However, the vector $\mathbf{1}$ is not in the image of M.

In Example 4.1.13, $\mathbf{1}$ is not even a valid share. If $\mathbf{1}$ is a valid share, however, then $\mathbf{1} \in \mathsf{Share}(1)$ if $\mathcal{S}$ is homomorphic.

Lemma 4.1.14 *Let $\mathcal{S}$ be a multiplicative LSSS over a commutative ring $\mathbb{L}$. If $\mathbf{1} \in \mathsf{Share}(s)$ for some $s \in \mathbb{L}$ and $\mathcal{S}$ is homomorphic, then $\mathbf{1} \in \mathsf{Share}(1)$.*

Proof. Suppose that $\mathbf{1} \in \mathsf{Share}(t)$ for some $t \in \mathbb{L}$. Then by the homomorphicity of $\mathcal{S}$ there exists a vector $\boldsymbol{r}$ such that for all $s \in \mathbb{L}$ and for all $\boldsymbol{s} \in \mathsf{Share}(s)$, $st = (\boldsymbol{r} \cdot \boldsymbol{s})(\boldsymbol{r} \cdot \mathbf{1}) = \boldsymbol{r} \cdot (\boldsymbol{s} \star \mathbf{1}) = \boldsymbol{r} \cdot \boldsymbol{s} = s$. In particular, for $s = 1$, $1t = 1$. This proves that $t = 1$, and hence that $\mathbf{1} \in \mathsf{Share}(1)$. ■

Shamir's secret sharing scheme is multiplicative if $n > 2t$, and strongly multiplicative if $n > 3t$. Clearly, the (strongly) multiplicative Shamir secret sharing scheme is homomorphic.

Shamir's secret sharing scheme. Let $s, t \in \mathbb{K}$ be two secrets that have been split into sets of shares $\boldsymbol{s}$ and $\boldsymbol{t}$, respectively, by Shamir's secret sharing scheme. Each player P_i, $1 \leq i \leq n$, has been given the two shares s_i and t_i.

Let f, g be the two polynomials over $\mathbb{K}$ of degree t with random coefficients $f_1, \ldots, f_n$ and $g_1, \ldots, g_n$, respectively, such that $s_i = f(i)$ and $t_i = g(i)$, and $f(0) = s$ and $g(0) = t$. Note that $st = f(0)g(0) = (fg)(0)$, and

$$\boldsymbol{s} \star \boldsymbol{t} = (f(1)g(1), \ldots, f(n)g(n)) = ((fg)(1), \ldots, (fg(n))).$$

The polynomial fg is of degree $2t$. Any subset of players of $t+1$ or more players is able to reconstruct the secrets s and t. Only the subsets of players of $2t+1$ players, however, are able to reconstruct st.

If $n > 2t$, Shamir's secret sharing scheme is multiplicative. The n-vector $\boldsymbol{r} = (R_1, \ldots, R_n)$ with $r_i = \prod_{j=1 j \neq i}^{n} \frac{-j}{i-j}$ for $1 \leq i \leq n$ is a fixed reconstruction vector. If $n > 3t$, Shamir's secret sharing scheme is strongly multiplicative, and the $d_{\overline{A}}$-vector $\boldsymbol{r_{\overline{A}}}$ with $r_{Ai} = \prod_{j \in \overline{A} j \neq i} \frac{-j}{i-j}$ for $i \in \overline{A}$ is a reconstruction vector for $A \in \mathcal{A}$.

4.2 Characterisation through Monotone Span Programs

In section 3.2, we proved that linear secret sharing schemes over a finite field are equivalent to monotone span programs. In this section, we will define monotone span programs with multiplication (mMSPs) and monotone span programs with strong multiplication (m*MSPs). We prove that over a finite field, multiplicative linear secret sharing schemes are equivalent to mMSPs, and strongly multiplicative linear secret sharing schemes are equivalent to m*MSPs.

Definition 4.2.1 An MSP $(\mathbb{L}, M, \boldsymbol{a}, \psi)$ is said to be a *monotone span program with pointwise multiplication (mMSP)* if there exists a d-vector $\boldsymbol{r}$ such that for all $\boldsymbol{b_1}$, $\boldsymbol{b_2} \in \mathbb{L}^e$

$$\boldsymbol{r} \cdot (M\boldsymbol{b_1} \star M\boldsymbol{b_2}) = (\boldsymbol{a} \cdot \boldsymbol{b_1})(\boldsymbol{a} \cdot \boldsymbol{b_2}).$$

Definition 4.2.2 An MSP $(\mathbb{L}, M, \boldsymbol{a}, \psi)$ is said to be a *monotone span program with pointwise strong multiplication (m*MSP)* if for all $A \in \mathcal{A}$, the MSP $(\mathbb{L}, M_{\overline{A}}, \boldsymbol{a})$ is multiplicative.

Example 4.2.3 Let $\mathbb{L} = \mathbb{Z}_2$, $d = 3$, $e = 2$, $n = 2$.
Let $\boldsymbol{r} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, and let $M = \begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{matrix} 1 \\ 2 \\ 2 \end{matrix}$.

Over $\mathbb{Z}_2$,

$$\boldsymbol{b_1}, \boldsymbol{b_2} \in \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}.$$

We have that

$$M \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, M \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, M \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, M \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix},$$

and

$$\boldsymbol{a} \cdot \begin{pmatrix} 0 \\ 0 \end{pmatrix} = 0, \boldsymbol{a} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0, \boldsymbol{a} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1, \boldsymbol{a} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1.$$

For all $\boldsymbol{b_1}, \boldsymbol{b_2} \in \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$,

$$\boldsymbol{r} \cdot (M\boldsymbol{b_1} \star M\boldsymbol{b_2}) = (\boldsymbol{a} \cdot \boldsymbol{b_1})(\boldsymbol{a} \cdot \boldsymbol{b_2}).$$

Definition 4.2.4 We say that a matrix $D = (d_{ij}) \in \mathbb{L}^{d \times d}$ is a *local multiplicativity matrix* if $d_{ij} \neq 0$ only if row i and column j are labelled by the same $k \in \{1, \ldots, n\}$. For $1 \leq k \leq n$, we denote by $D_k \in \mathbb{L}^{d_k \times d_k}$ the submatrix of D with rows i and columns j of D such that both row i and columns j are labelled by k.

Definition 4.2.5 An MSP $(\mathbb{L}, M, \boldsymbol{a}, \psi)$ is said to be a *monotone span program with local multiplication (mMSP)* if there exists a local multiplicativity matrix $D \in \mathbb{L}^{d \times d}$ such that $M^T D M = \boldsymbol{a}\boldsymbol{a}^T$.

Definition 4.2.6 An MSP $(\mathbb{L}, M, \boldsymbol{a}, \psi)$ is said to be a *monotone span program with local strong multiplication (m*MSP)* if for all $A \in \mathcal{A}$, the MSP $(\mathbb{L}, M_{\overline{A}}, \boldsymbol{a})$ is multiplicative.

We now prove that over any commutative ring $\mathbb{L}$, there is a corresponding pointwise multiplicative LSSS for each MSP with pointwise multiplication. This proof is due to [9]. In fact, m(*)LSSSs and m(*)MSPs over a finite field are in one-to-one correspondence.

Theorem 4.2.7 *For each monotone span program with pointwise multiplication over a commutative ring there is a corresponding pointwise multiplicative linear secret sharing scheme. For each monotone span program with pointwise strong multiplication over a commutative ring there is a corresponding pointwise strongly multiplicative linear secret sharing scheme.*

Proof. Let $(\mathbb{L}, M, \boldsymbol{a}, \psi, \boldsymbol{r})$ be an mMSP. Let s, $t \in \mathbb{L}$ be two secrets. Let $\boldsymbol{b_1} \in \mathbb{L}^e$ be a random e-vector with $b_{11} = s$. Similarly, let $\boldsymbol{b_2} \in \mathbb{L}^e$ be a

random e-vector with $b_{21} = t$. Let the sets of shares given to player P_i, $1 \leq i \leq n$, be $\boldsymbol{s_i} = M_i\boldsymbol{b_1}$ and $\boldsymbol{t_i} = M_i\boldsymbol{b_2}$, respectively. This means that $\boldsymbol{s} = M\boldsymbol{b_1}$ and $\boldsymbol{t} = M\boldsymbol{b_2}$. Then $\boldsymbol{r}\cdot(\boldsymbol{s}\star\boldsymbol{t}) = \boldsymbol{r}\cdot(M\boldsymbol{b_1}\star M\boldsymbol{b_2}) = (\boldsymbol{a}\cdot\boldsymbol{b_1})(\boldsymbol{a}\cdot\boldsymbol{b_2}) = st$. ■

The share multiplication protocol may be constructed as follows [9]:

Each player P_i picks a random vector $\boldsymbol{c'_k} \in \mathbb{L}^{e-1}$ for each row k of M labelled by i. Let $\boldsymbol{c_k} = (s_k t_k || \boldsymbol{c'_k})$. Player P_i computes for each player P_j, $1 \leq j \leq n$, $\boldsymbol{u_{kj}} = M_j\boldsymbol{c_k}$. $\boldsymbol{u_{kj}}$ is given to player P_j. Each player P_i then computes $\boldsymbol{v_i} = \sum_{k=1}^{d} r_k\boldsymbol{u_{ki}}$. Let $\boldsymbol{v} = (\boldsymbol{v_1}, \ldots, \boldsymbol{v_n})$. Then

$$\begin{aligned}\boldsymbol{r}\cdot\boldsymbol{v} &= \boldsymbol{r}\cdot(\sum_{k=1}^{d} r_k\boldsymbol{u_{k1}}, \ldots, \sum_{k=1}^{d} r_k\boldsymbol{u_{kn}}) = \boldsymbol{r}\cdot(\sum_{k=1}^{d} r_k M_1\boldsymbol{c_k}, \ldots, \sum_{k=1}^{d} r_k M_n\boldsymbol{c_k}) \\ &= \boldsymbol{r}\cdot(M\sum_{k=1}^{d} r_k\boldsymbol{c_k}) = \boldsymbol{r}\cdot(M(\boldsymbol{r}\cdot(\boldsymbol{s}\star\boldsymbol{t})||\sum_{k=1}^{d} r_k\boldsymbol{c'_k})) \\ &= \boldsymbol{r}\cdot(M(st||\sum_{k=1}^{d} r_k\boldsymbol{c'_k})) = st.\end{aligned}$$

Now we prove that over any commutative ring $\mathbb{L}$, there is a corresponding locally multiplicative LSSS for each MSP with local multiplication. This proof is due to [11].

Lemma 4.2.8 *For each monotone span program with local multiplication over a commutative ring $\mathbb{L}$, there is a corresponding locally multiplicative linear secret sharing scheme. For each monotone span program with local strong multiplication over a commutative ring $\mathbb{L}$, there is a corresponding locally strongly multiplicative linear secret sharing scheme.*

Proof. Let $(\mathbb{L}, M, \boldsymbol{a}, \psi, D)$ be an mMSP. Let s, $t \in \mathbb{L}$ be two secrets. Let $\boldsymbol{b_1} \in \mathbb{L}^e$ be a random e-vector with $b_{11} = s$. Similarly, let $\boldsymbol{b_2} \in \mathbb{L}^e$ be a random e-vector with $b_{21} = t$. Let the sets of shares given to player P_i, $1 \leq i \leq n$, be $\boldsymbol{s_i} = M_i\boldsymbol{b_1}$ and $\boldsymbol{t_i} = M_i\boldsymbol{b_2}$, respectively. This means that $\boldsymbol{s} = M\boldsymbol{b_1}$ and $\boldsymbol{t} = M\boldsymbol{b_2}$. Then $\sum_{i=1}^{n} \boldsymbol{s_i}^T D_i\boldsymbol{t_i} = \boldsymbol{s}^T D\boldsymbol{t} = (M\boldsymbol{b_1})^T DM\boldsymbol{b_2} = \boldsymbol{b_1}^T M^T DM\boldsymbol{b_2}^T = \boldsymbol{b_1}^T\boldsymbol{a}\boldsymbol{a}^T\boldsymbol{b_2} = st$. ■

The share multiplication protocol may be constructed as follows [11]:

Each player P_i picks a random vector $\boldsymbol{c'_i} \in \mathbb{L}^{e-1}$. Let $\boldsymbol{c_i} = (\boldsymbol{s_i}^T D_i\boldsymbol{t_i} || \boldsymbol{c'_i})$. Player P_i computes for each player P_j, $1 \leq j \leq n$, $\boldsymbol{u_{ij}} = M_j\boldsymbol{c_i}$. $\boldsymbol{u_{ij}}$ is given to player P_j. Each player P_i then computes $\boldsymbol{v_i} = \sum_{j=1}^{n} \boldsymbol{u_{ji}}$. Let $\boldsymbol{v} = (\boldsymbol{v_1}, \ldots, \boldsymbol{v_n})$. By definition 3.2.2, there exists a $\boldsymbol{r} \in \mathbb{L}^d$ such that

$M^T \boldsymbol{r} = \boldsymbol{a}$. Then

$$\begin{aligned}\boldsymbol{r} \cdot \boldsymbol{v} &= \boldsymbol{r} \cdot (\sum_{j=1}^{n} \boldsymbol{u_{j1}}, \ldots, \sum_{j=1}^{n} \boldsymbol{u_{jn}}) = \boldsymbol{r} \cdot (\sum_{j=1}^{n} M_1 \boldsymbol{c_j}, \ldots, \sum_{j=1}^{n} M_n \boldsymbol{c_j}) \\ &= \boldsymbol{r} \cdot (M \sum_{j=1}^{n} \boldsymbol{c_j}) = \boldsymbol{r} \cdot (M(\sum_{j=1}^{n} \boldsymbol{s_i}^T D_i \boldsymbol{t_i} || \sum_{j=1}^{n} \boldsymbol{c'_j})) \\ &= \boldsymbol{r} \cdot (M(st || \sum_{j=1}^{n} \boldsymbol{c'_j})) = st.\end{aligned}$$

In the following example, we will consider the mLSSSs corresponding to the mMSPs $(\mathbb{Z}_5, M, \boldsymbol{a}, \psi)$, where M is a 3×2-matrix with row 1 labelled by 1, row 2 labelled by 2, and row 3 labelled by 3.

Example 4.2.9 There are exactly $5^6 = 15625$ 3×2-matrices M over $\mathbb{Z}_5$. For 10204 of those, the MSP $(\mathbb{Z}_5, M, \boldsymbol{a}, \psi)$ is multiplicative.

We consider the access structure $\Gamma = \{\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$, or, in other words, the adversary structure $\mathcal{A} = \{\{1\},\{2\},\{3\},\emptyset\}$.

Precisely 3840 of the 10204 mMSPs have this adversary structure. For the other 6364 mMSPs, $\{1\} \in \Gamma$, $\{2\} \in \Gamma$, or $\{3\} \in \Gamma$.

Up to permutation of rows and multiplication by a non-zero scalar, there are thus $\frac{3840}{6 \times 4} = 160$ mMSPs with access structure Γ and adversary structure $\mathcal{A}$.

In the remainder of this section, we will present two theorems from [8].

Lemma 4.2.10 *Let $f : \{0,1\}^n \to \{0,1\}$ be a Q2 monotone Boolean function. Then $f = f \vee f^\star$, where $f^\star$ is the dual of f.*

Proof. Let $A \subseteq \{1, \ldots, n\}$. First, we prove by contradiction that $f(A) = 0 \Rightarrow \overline{f(\overline{A})} = 0$. Clearly, $A \cup \overline{A} = \{1, \ldots, n\}$. Now, $f(A) = 0 = f(\overline{A}) \Rightarrow A, \overline{A} \in \mathcal{A}'$. This contradicts the fact that f is Q2. It follows that $f(A) = 0 = \overline{f(\overline{A})} = f^\star(A)$ for all $A \subset \{1, \ldots, n\}$. Thus, $f = f \vee f^\star$. ■

Lemma 4.2.11 *Let $\mathcal{M} = (\mathbb{K}, M, \boldsymbol{a}, \psi)$ be an MSP of size d computing a monotone Boolean function f, with $\boldsymbol{a} = (1, 0, \ldots, 0)$. There exists an MSP $\mathcal{M}^\star = (\mathbb{K}, M^\star, \boldsymbol{a}, \psi)$ of size d computing $f^\star$ such that $M^T M^\star = \boldsymbol{a}\boldsymbol{a}^T$.*

Proof. In this proof, we consider an MSP with target vector $\boldsymbol{a'} = (1, \ldots, 1)$. We may construct an MSP $\mathcal{N}^\star = (\mathbb{K}, N^\star, \boldsymbol{a'}, \psi)$ computing the dual of a Boolean function f for a given MSP $\mathcal{N} = (\mathbb{K}, N, \boldsymbol{a'}, \psi)$ computing f[14]. We will first construct $\mathcal{N}$ from $\mathcal{M}$, and then construct $\mathcal{M}^\star$ from $\mathcal{N}^\star$.

Let

$$H = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Then

$$H^{-1} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ -1 & 1 & 0 & \cdots & 0 \\ -1 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Let $N = MH^T$, let $\mathcal{N} = (\mathbb{K}, N, \boldsymbol{a'}, \psi)$, with $\boldsymbol{a'} = (1, ..., 1)$. Then $\mathcal{N}$ computes f as $H\boldsymbol{a} = \boldsymbol{a'}$. As proved in [14], there exists an MSP $\mathcal{N}^\star = (\mathbb{K}, N^\star, \boldsymbol{a'}, \psi)$ of size d computing $f^\star$. $N^\star$ has d rows labelled like the rows of N, and one column $\boldsymbol{\lambda_A}$ for each A such that $f(A) = 1$, with $\boldsymbol{\lambda_A}$ such that $N^T\boldsymbol{\lambda_A} = \boldsymbol{a'}$. This $\boldsymbol{\lambda_A}$ exists since $f(A) = 1 \Leftrightarrow \boldsymbol{a'} \in \operatorname{Im} N_A^T$ by definition 3.2.7. Note that

$$N^T N^\star = \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix}.$$

Let $M^\star = N^\star(H^{-1})^T$. Then $\mathcal{M} = (\mathbb{K}, M, \boldsymbol{a})$ computes $f^\star$ as $H^{-1}\boldsymbol{a'} = \boldsymbol{a}$. Moreover, $M^T M^\star = H^{-1}N^T N^\star(H^{-1})^T = \boldsymbol{a}\boldsymbol{a}^T$. The matrix $M^\star$ may be computed directly and efficiently from M [13]. ■

Lemma 4.2.12 *Let f_0 and f_1 be monotone Boolean functions from $\{0,1\}^n$ to $\{0,1\}$ computed by the MSPs $\mathcal{M}_0 = (\mathbb{L}, M_0, \boldsymbol{a}, \psi)$ and $\mathcal{M}_1 = (\mathbb{L}, M_1, \boldsymbol{a}, \psi)$, respectively, with $\boldsymbol{a} = (1, 0, \ldots, 0)$ such that M_0 and M_1 are $d \times e$-matrices with the same labelling from $\{1, \ldots, n\}$, with $M_0^T M_1 = \boldsymbol{a}\boldsymbol{a}^T$. There exists an MSP $\mathcal{M}$ with local multiplication of size $2d$ computing $f_0 \vee f_1$.*

Proof. Let $M_1'' \in \mathbb{L}^{d \times e}$ be the matrix whose first column is equal to the first column of M_1 and whose other $e-1$ columns are equal to $\mathbf{0}$. Let $M_1' \in \mathbb{L}^{d \times e-1}$ be the matrix consisting of the last $e-1$ columns of M_1. We define a $2d \times (2e-1)$ matrix M as follows:

$$M = \begin{pmatrix} M_0 & 0 \\ M_1'' & M_1' \end{pmatrix}.$$

The first d rows of M are labelled like the d rows of M_0, and the last d rows of M are labelled like the d rows of M_1:

$$\psi'(i) = \begin{cases} \psi(i) \text{ for } 1 \leq i \leq d \\ \psi(i-d) \text{ for } d < i \leq 2d \end{cases}$$

Let Γ_0 and Γ_1 be the access structures of f_0 and f_1, respectively. Clearly, the access structure of $f_0 \vee f_1$ is $\Gamma_0 \cup \Gamma_1$. We now prove that $\mathcal{M} = (\mathbb{L}, M, \boldsymbol{a}, \psi')$ is an MSP with local multiplication computing $f_0 \vee f_1$.

Let $A \in \Gamma_0 \cup \Gamma_1$. Wlog $A \in \Gamma_0$. By definition, there exists $\boldsymbol{z_0} \in \mathbb{L}^{d_A}$ such that $M_{0_A}^T \boldsymbol{z_0} = \boldsymbol{a}$. Let $\boldsymbol{z} = (\boldsymbol{z_0}||\boldsymbol{0}) \in \mathbb{L}^{2d_A}$. Then

$$M_A^T \boldsymbol{z} = \begin{pmatrix} M_{0_A}^T & M''^T_{1_A} \\ 0 & M'^T_{1_A} \end{pmatrix} \begin{pmatrix} \boldsymbol{z_0} \\ \boldsymbol{0} \end{pmatrix} = \begin{pmatrix} M_{0_A}^T \boldsymbol{z_0} \\ \boldsymbol{0} \end{pmatrix} = \boldsymbol{a},$$

which means that $\boldsymbol{a} \in \operatorname{Im} M_A^T$.

Now let $A \in \overline{\Gamma_0 \cup \Gamma_1} = \overline{\Gamma_0} \cap \overline{\Gamma_1}$. By definition, there exist $\boldsymbol{\kappa_0} \in \operatorname{Ker} M_{0_A}$ with $\kappa_{01} = 1$ and $\boldsymbol{\kappa_1} \in \operatorname{Ker} M_{1_A}$ with $\kappa_{11} = 1$. Let $\boldsymbol{\kappa} = (\boldsymbol{\kappa_0}||\boldsymbol{\kappa_1'})$, where $\boldsymbol{\kappa_1'}$ is the vector consisting of the last $e-1$ elements of $\boldsymbol{\kappa_1}$. Then $\kappa_1 = 1$ and

$$M_A \boldsymbol{\kappa} = \begin{pmatrix} M_{0_A} & 0 \\ M''_{1_A} & M'_{1_A} \end{pmatrix} \begin{pmatrix} \boldsymbol{\kappa_0} \\ \boldsymbol{\kappa_1'} \end{pmatrix} = \begin{pmatrix} M_{0_A} \boldsymbol{\kappa_0} \\ M_{1_A} \boldsymbol{\kappa_1} \end{pmatrix} = \boldsymbol{0},$$

which means that $\boldsymbol{\kappa} \in \operatorname{Ker} M_A$.

This proves that $\mathcal{M}$ is an MSP computing $f_0 \vee f_1$. It remains to prove that $\mathcal{M}$ is locally multiplicative. Let

$$D = \begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix} \in \mathbb{L}^{2d \times 2d}.$$

Then

$$\begin{aligned} M^T D M &= \begin{pmatrix} M_0^T & M_1''^T \\ 0 & M_1'^T \end{pmatrix} \begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix} \begin{pmatrix} M_0 & 0 \\ M_1'' & M_1' \end{pmatrix} = \begin{pmatrix} M_0^T M_1'' & M_0^T M_1' \\ 0 & 0 \end{pmatrix} \\ &= \boldsymbol{a}\boldsymbol{a}^T. \end{aligned}$$

■

We will now present Theorem 7 from [8].

Theorem 4.2.13 *Let $\mathcal{M}$ be an MSP computing a Q2 function f. There exists a locally multiplicative MSP $\overline{\mathcal{M}}$ of size at most twice the size of $\mathcal{M}$ computing f. The algorithm with input $\mathcal{M}$ and output $\overline{\mathcal{M}}$ is efficient.*

Proof. Let $\mathcal{M} = (\mathbb{K}, M, \boldsymbol{a}, \psi)$, with $\boldsymbol{a} = (1, 0, \ldots, 0)$. By Lemma 4.2.10, $f = f \vee f^\star$. By Lemma 4.2.11, there exists an MSP $\mathcal{M}^\star = (\mathbb{K}, M^\star, \boldsymbol{a}, \psi)$ of size d computing $f^\star$ with $M^T M^\star = \boldsymbol{a}\boldsymbol{a}^T$. Then, by Lemma 4.2.12, there exists an mMSP of size $2d$ computing $f^\star \vee f = f$. ■

Now we present Theorem 6 from [8].

Theorem 4.2.14 *For every finite field $\mathbb{K}$ and every monotone function f, there exists a locally multiplicative MSP computing f if and only if f is Q2, and there exists a strongly locally multiplicative MSP computing f if and only if f is Q3.*

Proof. We do not prove that if f is Q3, then there exists an m*MSP computing f. By Fact 3.2.8 and Theorem 4.2.13, if f is Q2, then there exists an mMSP computing f of finite size.

For the converse, let $\mathcal{A}$ be the adversary structure for f, and let $\mathcal{M} = (\mathbb{K}, M, \boldsymbol{a}, \psi)$ be the mMSP computing f. If f is not Q2, there exists $A \subset \{1, \ldots, n\}$ with $A \cup \overline{A} = \{1, \ldots, n\}$ and $A, \overline{A} \in \mathcal{A}$. Note that $f(A) = 0 \Leftrightarrow \boldsymbol{a} \notin \operatorname{Im} M_A^T \Leftrightarrow \boldsymbol{a} \notin (\operatorname{Ker} M_A)^{\perp}$. Consequently, there exists an e-vector $\boldsymbol{z} \in \mathbb{K}^e$ such that $M_A \boldsymbol{z} = \boldsymbol{0}$ and $\boldsymbol{a} \cdot \boldsymbol{z} \neq 0$. Thus $z_1 \neq 0$, and wlog $z_1 = 1$. Similarly, there exists an e-vector $\boldsymbol{z'} \in \mathbb{K}^e$ such that $M_{\overline{A}} \boldsymbol{z'} = \boldsymbol{0}$ and $\boldsymbol{a} \cdot \boldsymbol{z'} \neq \boldsymbol{0}$, and wlog $z'_1 = 1$. Let D be the local multiplicativity matrix. Clearly, $(M\boldsymbol{z})^T D M \boldsymbol{z'} = 0$. By definition 4.2.5, $(M\boldsymbol{z})^T D M \boldsymbol{z'} = \boldsymbol{z}^T \boldsymbol{a} \boldsymbol{a}^T \boldsymbol{z'} = z_1 z'_1 = 1$. This is a contradiction. Hence, f must be Q2.

Let $\mathcal{M} = (\mathbb{K}, M, \boldsymbol{a}, \psi)$ be the m*MSP computing f. If f is not Q3, there exist A, A', $A'' \subset \{1, \ldots, n\}$ with $A' \cup A' \cup A'' = \{1, \ldots, n\}$ and $A, A', A'' \in \mathcal{A}$. Wlog A, A', A'' are disjoint. There exist e-vectors $\boldsymbol{z_A}$, $\boldsymbol{z_{A'}}$, $\boldsymbol{z_{A''}} \in \mathbb{K}^e$ such that $M_A \boldsymbol{z_A} = 0$, $M_{A'} \boldsymbol{z_{A'}} = 0$, $M_{A''} \boldsymbol{z_{A''}} = 0$, and $\boldsymbol{a} \cdot \boldsymbol{z_A} = 1$, $\boldsymbol{a} \cdot \boldsymbol{z_{A'}} = 1$, $\boldsymbol{a} \cdot \boldsymbol{z_{A''}} = 1$. Let D be the local multiplicativity matrix for $\overline{A''}$. Then, by definition 4.2.6, $(M_{\overline{A''}} \boldsymbol{z_A})^T D M_{\overline{A''}} \boldsymbol{z_{A'}} = \boldsymbol{z_A}^T \boldsymbol{a} \boldsymbol{a}^T \boldsymbol{z_{A'}} = 1$. Note that $\overline{A''} = A \cup A'$. Thus, $(M_{\overline{A''}} \boldsymbol{z_A})^T D M_{\overline{A''}} \boldsymbol{z_{A'}} = 0$. This is a contradiction. Hence, f must be Q3. ■

Both Theorem 4.2.13 and Theorem 4.2.14 may be generalised to commutative rings [15]. As an example, we construct a locally multiplicative MSP over the ring $\mathbb{Z}_{2^{32}}$.

Example 4.2.15 Let $\Gamma = (P_1 \wedge P_2) \vee (P_1 \wedge P_3) \vee (P_2 \wedge P_3)$.

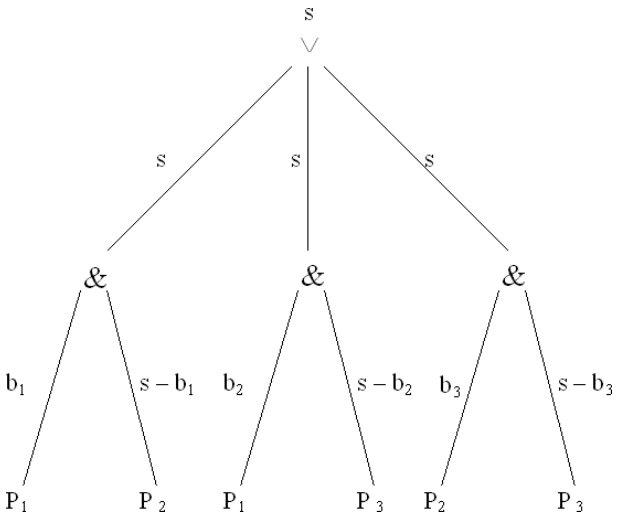

Figure 4.1: DNF-based scheme for $\Gamma = (P_1 \wedge P_2) \vee (P_1 \wedge P_3) \vee (P_2 \wedge P_3)$

1. First, we construct an MSP $\mathcal{M} = (M, \mathbb{Z}_{2^{32}}, \boldsymbol{a}, \psi)$ computing Γ.

$$M = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \end{pmatrix} \begin{matrix} 1 \\ 2 \\ 1 \\ 3 \\ 2 \\ 3 \end{matrix}$$

2. Secondly, we compute the MSP $\mathcal{N} = (N, \mathbb{Z}_{2^{32}}, \boldsymbol{a'}, \psi)$ from $\mathcal{M}$ according to Lemma 4.2.11.

$$N = MH^T = M \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \begin{matrix} 1 \\ 2 \\ 1 \\ 3 \\ 2 \\ 3 \end{matrix}$$

3. Thirdly, we construct, according to Lemma 4.2.11, the dual MSP $\mathcal{N}^\star = (N^\star, \mathbb{Z}_{2^{32}}, \boldsymbol{a'}, \psi)$ of $\mathcal{N}$.

$$N^\star = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \begin{matrix} 1 \\ 2 \\ 1 \\ 3 \\ 2 \\ 3 \end{matrix}$$

4. Fourthly, we compute the dual MSP $\mathcal{M}^\star = (M^\star, \mathbb{Z}_{2^{32}}, \boldsymbol{a}, \psi)$ of $\mathcal{M}$, again according to Lemma 4.2.11.

$$M^\star = N^\star H^{-T} = N^\star \begin{pmatrix} 1 & -1 & -1 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 & -1 & 0 \\ 1 & -1 & -1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \begin{matrix} 1 \\ 2 \\ 1 \\ 3 \\ 2 \\ 3 \end{matrix}$$

5. Finally, we construct the locally multiplicative MSP $\overline{\mathcal{M}} = (\overline{M}, \mathbb{Z}_{2^{32}}, \boldsymbol{a}, \psi')$

according to Lemma 4.2.12.

$$\overline{M} = \left(\begin{array}{ccccccc|c} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & -1 & 0 & 0 & 0 & 3 \\ 1 & 0 & 0 & 0 & -1 & -1 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1 & -1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 3 \end{array}\right)$$

Example 4.2.15 allows us, by Lemma 4.2.8, to construct a 2-out-of-3 locally multiplicative LSSS over the ring $\mathbb{Z}_{2^{32}}$. The size of this LSSS is 12, and each of the three players is given four shares. Similarly, we may construct a 3-out-of-5 mLSSS and a 4-out-of-7 mLSSS. The 3-out-of-5 mLSSS will be of size 60, with each player being given 12 shares, and the size of the 4-out-of-7 mLSSS will be 280 with 40 shares for each player.

4.3 Characterisation through Projection

Notation 4.3.1 *Let $\mathcal{S}$ be a multiplicative linear secret sharing scheme. We denote the set of reconstruction vectors for multiplication of $\mathcal{S}$ by $\mathcal{R}^\star(\mathcal{S})$.*

Notation 4.3.2 *Let $\mathbb{M}$ be a module over a ring $\mathbb{L}$, and let $X \subset \mathbb{M}$ be a finite subset of $\mathbb{M}$. We denote by* $\mathrm{nzi}(X)$ *the set of index sets I such that $I \in \mathrm{nzi}(X)$ if there exists $\boldsymbol{x} \in X$ such that I is the index set of all non-zero elements of $\boldsymbol{x}$.*

Bottom-up construction. Given a module $M_1 \subseteq \mathbb{L}^d$, it is possible to construct a possibly non-functional and insecure linear secret sharing scheme.

1. Fix a vector $\boldsymbol{m_0}$ and define $M_2 = \mathrm{span}\,(M_1 \star M_1 \cup \boldsymbol{m_0} \star M_1)$.
2. Define a linear secret sharing scheme by

   $$\mathsf{Share}(s) = s\boldsymbol{m_0} + M_1$$

   and the sets of reconstruction vectors for addition and multiplication by

   $$\mathcal{R}_1 = \{\boldsymbol{r} \in M_1^\perp : \boldsymbol{r}^T\boldsymbol{m_0} = 1\},$$
   $$\mathcal{R}_2 = \{\boldsymbol{r} \in M_2^\perp : \boldsymbol{r}^T(\boldsymbol{m_0} \star \boldsymbol{m_0}) = 1\}.$$

Theorem 4.3.3 *Every multiplicative linear secret sharing scheme can be generated by bottom up construction. If the sets of reconstruction vectors $\mathcal{R}_1$ and $\mathcal{R}_2$ are non-empty, the linear secret sharing scheme defined is functional. If $\mathbb{L}$ is a field, there exists an access structure Γ such that the original scheme is secure and functional wrt Γ. For rings $\mathbb{L}$ there might exist subsets of players that are only able to deduce partial information about a secret.*

Proof. First, we prove that there exists a bottom up construction for every multiplicative linear secret sharing scheme. Let $\mathcal{S}$ be an mLSSS. By Lemma 3.1.6, $\mathsf{Share}(s) = s\boldsymbol{m} + \mathsf{Share}(0)$ for a fixed vector $\boldsymbol{m} \in \mathsf{Share}(1)$. Let $M_1 = \mathsf{Share}(0)$, and let $\boldsymbol{m_0} = \boldsymbol{m}$. By Lemma 4.1.6, $\mathcal{R}_1 = \mathcal{R}(\mathcal{S})$, and $\mathcal{R}_2 = \mathcal{R}^\star(\mathcal{S})$.

FUNCTIONALITY. For any reconstruction vector $\boldsymbol{r_1} \in \mathcal{R}_1$ and $s \in \mathbb{L}$

$$\boldsymbol{r_1}^T\mathsf{Share}(s) = \boldsymbol{r}_1^T(s\boldsymbol{m_0} + M_1) = s\boldsymbol{r_1}^T\boldsymbol{m_0} + \boldsymbol{r_1}^T M_1 = s$$

and for any reconstruction vector $\boldsymbol{r_2} \in \mathcal{R}_2$ and $s, t \in \mathbb{L}$

$$\begin{aligned}\boldsymbol{r_2}^T(\mathsf{Share}(s) \star \mathsf{Share}(t)) &= \boldsymbol{r_2}^T(st(\boldsymbol{m_0} \star \boldsymbol{m_0}) + (s+t)(\boldsymbol{m_0} \star M_1) + M_1 \star M_1) \\ &= st.\end{aligned}$$

SECURITY. Define $\Gamma = \mathrm{nzi}(\mathcal{R}_1) \cup \{A \subseteq \mathcal{P} : \exists A' \in \mathrm{nzi}(\mathcal{R}_1) \text{ s.t. } A \supset A'\}$.

■

Lemma 4.3.4 *Let $\mathbb{K}$ be a field. The sets of reconstruction vectors $\mathcal{R}_1$ and $\mathcal{R}_2$ are non-empty if and only if $\boldsymbol{m_0} \notin M_1$ and $\boldsymbol{m_0} \star \boldsymbol{m_0} \notin M_2$.*

Proof. By Fact 2.2.22, $\boldsymbol{m_0} \notin M_1$ if and only if $M_1^\perp \not\subset \boldsymbol{m_0}^\perp$. Hence, there exists $\boldsymbol{r'} \in M_1^\perp \setminus \boldsymbol{m_0}^\perp$. Let $\boldsymbol{r} = \frac{1}{\boldsymbol{r'} \cdot \boldsymbol{m_0}}\boldsymbol{r'}$. Then $\boldsymbol{r} \in M_1^\perp$ and $\boldsymbol{r}^T\boldsymbol{m_0} = 1$. Hence, $\boldsymbol{r} \in \mathcal{R}_1$, and $\mathcal{R}_1 \neq \emptyset$.

Similarly, by Fact 2.2.22, $\boldsymbol{m_0} \star \boldsymbol{m_0} \notin M_2$ if and only if $M_2^\perp \not\subset (\boldsymbol{m_0} \star \boldsymbol{m_0})^\perp$. Hence, there exists $\boldsymbol{r'} \in M_2^\perp \setminus (\boldsymbol{m_0} \star \boldsymbol{m_0})^\perp$. Let $\boldsymbol{r} = \frac{1}{\boldsymbol{r'} \cdot (\boldsymbol{m_0} \star \boldsymbol{m_0})}\boldsymbol{r'}$. Then $\boldsymbol{r} \in M_2^\perp$ and $\boldsymbol{r}^T(\boldsymbol{m_0} \star \boldsymbol{m_0}) = 1$. Hence, $\boldsymbol{r} \in \mathcal{R}_2$, and $\mathcal{R}_2 \neq \emptyset$.

Clearly, if $\mathcal{R}_1$ and $\mathcal{R}_2$ are non-empty then $\boldsymbol{m_0} \notin M_1$ and $\boldsymbol{m_0} \star \boldsymbol{m_0} \notin M_2$.

■

4.3.1 Algorithm: isMult(M)

Let $\mathcal{S}_\mathcal{M} = (\mathbb{L}, M)$ be a linear secret sharing scheme over a ring $\mathbb{L}$ with share distribution matrix M. In this subsection, we present an algorithm to check whether $\mathcal{S}_\mathcal{M}$ is multiplicative. In other words, we need to check whether there exists a reconstruction vector $\boldsymbol{r}$ for multiplication for $\mathcal{S}_M$.

Naively, we may do the following:

Algorithm 3 isMult(M)

for all $\boldsymbol{r}$ **do**
  all_b $\leftarrow$ true
  for all $\boldsymbol{b_1}$, $\boldsymbol{b_2}$ **do**
    if $\boldsymbol{r} \cdot ((M\boldsymbol{b_1}) \star (M\boldsymbol{b_2})) \neq b_{11}b_{21}$ **then**
      all_b $\leftarrow$ false
      break
    end if
  end for
  if all_b **then**
    return true
  end if
end for
return false

This algorithm is highly inefficient since the number of computations increases exponentially with the number of columns of M. Lemma 4.1.6 allows for a more efficient algorithm. The following algorithm is more efficient since the number of computations increases only quadratically with the number of columns of M.

Algorithm 4 isMult(M)

$M^\star \leftarrow (\boldsymbol{m} \star \boldsymbol{m} || M' \star M' || \boldsymbol{m} \star M')$
for all $\boldsymbol{r}$ **do**
  if $\boldsymbol{r}^T M^\star = \begin{pmatrix} 1 & 0 & \cdots 0 \end{pmatrix}$ **then**
    return true
  end if
end for
return false

Note that for both algorithms the number of computations increases linearly with the size of $\mathcal{S}$.

Chapter 5

Threshold Linear Secret Sharing Schemes

5.1 Threshold Access Structures

A $(t+1)$-out-of-n threshold secret sharing scheme is a secret sharing scheme in which the secret may be reconstructed from any $t+1$ or more shares, whereas no information about the secret may be deduced from any t or fewer shares. A threshold access structure with threshold t is an access structure in which any $t+1$ or more players may reconstruct the secret, while no t or fewer players may deduce any information about the secret.

Let $\mathcal{P} = \{1, \ldots, n\}$ be a set of players.

Definition 5.1.1 A *threshold access structure* is a set $\Gamma_{t,n} = \{A \subseteq \mathcal{P} : |A| > t\}$ of subsets of $\mathcal{P}$ with $0 < t < n$. Analogously, a *threshold adversary structure* is a set $\mathcal{A}_{t,n} = \{A \subseteq \mathcal{P} : |A| \leq t\}$ of subsets of $\mathcal{P}$ with $0 < t < n$.

Note that any threshold access structure with threshold t may be implemented by a $(t+1)$-out-of-n threshold secret sharing scheme by giving precisely one share to each player. However, not all monotone access structures, no matter how many shares each player is given, may be implemented as threshold secret sharing schemes.

Lemma 5.1.2 *There exist monotone access structures for which there is no threshold secret sharing scheme.*

Proof. We prove that there is no threshold secret sharing scheme for the monotone access structure $\Gamma = \{\{1,2\}, \{3,4\}, \{1,2,3\}, \{1,2,4\}, \{2,3,4\}, \{1,3,4\}, \{1,2,3,4\}\} = (P_1 \wedge P_2) \vee (P_3 \wedge P_4)$. Let d_1, d_2, d_3, and d_4 denote the number of shares given to P_1, P_2, P_3, and P_4, respectively.

For a contradiction, we suppose that there is a threshold secret sharing scheme for Γ, with threshold t. Since P_1 and P_2 are able to reconstruct the

secret, $d_1 + d_2 > t$. Similarly, since P_3 and P_4 are able to reconstruct the secret together, $d_3 + d_4 > t$. Wlog we may assume that $d_1 \geq d_2$ and $d_3 \geq d_4$. Then, $d_1 + d_1 \geq d_1 + d_2 > t$, and $d_3 + d_3 \geq d_3 + d_4 > t$, which implies that $d_1 + d_3 > t/2 + t/2 = t$. P_1 and P_3 are thus able to reconstruct the secret together. This contradicts the fact that $\{1, 3\} \notin \Gamma$. ■

This lemma is due to [3]. Note that other non-threshold monotone access structures, in particular, Q2 non-threshold monotone access structures, may be implemented as threshold secret sharing schemes.

Lemma 5.1.3 *There exist Q2 non-threshold monotone access structures for which there is a threshold secret sharing scheme.*

Proof. We prove that there is a threshold secret sharing scheme for the Q2 monotone access structure $\Gamma = \{\{1\}, \{1,2\}, \{1,3\}, \{1,4\}, \{1,5\}, \{2,3\}, \{2,4\}, \{2,5\}, \{1,2,3\}, \{1,2,4\}, \{1,2,5\}, \{1,3,4\}, \{1,3,5\}, \{1,4,5\}, \{2,3,4\}, \{2,3,5\}, \{2,4,5\}, \{3,4,5\}, \{1,2,3,4\}, \{1,2,3,5\}, \{1,2,4,5\}, \{1,3,4,5\}, \{2,3,4,5\}, \{1,2,3,4,5\}\} = P_1 \vee (P_2 \wedge P_3) \vee (P_2 \wedge P_4) \vee (P_2 \wedge P_5) \vee (P_3 \wedge P_4 \wedge P_5)$. Let $d_1 = 3$, $d_2 = 2$, and $d_3 = d_4 = d_5 = 1$. This defines a 3-out-of-8 threshold secret sharing scheme for Γ. ■

By Theorem 4.2.14, there exists a multiplicative MSP for a monotone access structure Γ if and only if Γ is Q2. Note that a threshold access structure $\Gamma_{t,n}$ is Q2 if and only if $n > 2t$. There hence exists a multiplicative MSP for $\Gamma_{t,n}$ if and only if $n > 2t$.

5.2 Characterisation of Threshold Linear Secret Sharing Schemes

Lemma 5.2.1 *Let $\mathbb{L}$ be a commutative ring, and let $\mathcal{S}$ be a $(t+1)$-out-of-n threshold LSSS over $\mathbb{L}$. If $\mathsf{Share}(0)$ has a basis, then $\dim \mathsf{Share}(0) = t$.*

Proof. Let $k = \dim \mathsf{Share}(0)$, and denote the k basis vectors of $\mathsf{Share}(0)$ by $\boldsymbol{m'_1}, \ldots, \boldsymbol{m'_k}$. Let $s \in \mathbb{L}$, and let $\boldsymbol{m} \in \mathsf{Share}(1)$. Let $\boldsymbol{s} \in \mathsf{Share}(s)$. By Lemma 3.1.6, there exist $\mu_1, \ldots, \mu_k \in \mathbb{L}$ such that

$$\boldsymbol{s} = s\boldsymbol{m} + \mu_1 \boldsymbol{m'_1} + \cdots + \mu_k \boldsymbol{m'_k} = \underbrace{\begin{pmatrix} m_1 & \underbrace{\begin{matrix} m'_{11} & \cdots & m'_{1k} \\ m'_{21} & \cdots & m'_{k1} \\ \vdots & \ddots & \vdots \\ m'_{n1} & \cdots & m'_{nk} \end{matrix}}_{M'} \\ m_2 \\ \vdots \\ m_n \end{pmatrix}}_{M} \begin{pmatrix} s \\ \mu_1 \\ \vdots \\ \mu_k \end{pmatrix}.$$

Clearly, the columns of the matrix M' are linearly independent, and therefore $\operatorname{rank} M' = k$. Note that $\boldsymbol{m} \notin \mathsf{Share}(0)$. The columns of the matrix M are therefore linearly independent, too. Thus, $\operatorname{rank} M = k+1$.

For a contradiction, suppose that $k < t$. By Fact 2.3.4, M has $k+1$ linearly independent rows. Wlog, let those rows be the first $k+1$ rows. Then,

$$\begin{pmatrix} s_1 \\ \vdots \\ s_{k+1} \end{pmatrix} = \underbrace{\begin{pmatrix} m_1 & m'_{11} & \cdots & m'_{1k} \\ m_2 & m'_{21} & \cdots & m'_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ m_{k+1} & m'_{k+11} & \cdots & m'_{k+1k} \end{pmatrix}}_{N} \begin{pmatrix} s \\ \mu_1 \\ \vdots \\ \mu_k \end{pmatrix}.$$

By Fact 2.3.7, the matrix N is invertible. Thus,

$$\begin{pmatrix} s \\ \mu_1 \\ \vdots \\ \mu_k \end{pmatrix} = N^{-1} \begin{pmatrix} s_1 \\ \vdots \\ s_{k+1} \end{pmatrix}.$$

In particular, $s = (N^{-1})_1 \cdot \begin{pmatrix} s_1 & \cdots & s_{k+1} \end{pmatrix}$, where $(N^{-1})_1$ denotes the first row of N^{-1}. The secret s may thus be reconstructed from the $k+1 \leq t$ shares $s_1, \ldots, s_{k+1}$. This contradicts the security of $\mathcal{S}$.

Suppose, again for a contradiction, that $k > t$. By Fact 2.3.4, M' has k linearly independent rows. Wlog, let those rows be the first k rows. Then,

$$\begin{pmatrix} s_1 \\ \vdots \\ s_k \end{pmatrix} = \underbrace{\begin{pmatrix} m_1 & m'_{11} & \cdots & m'_{1k} \\ m_2 & m'_{21} & \cdots & m'_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ m_k & m'_{k1} & \cdots & m'_{kk} \end{pmatrix}}_{N'} \begin{pmatrix} s \\ \mu_1 \\ \vdots \\ \mu_k \end{pmatrix}.$$

For $\mathcal{S}$ to be functional, it must be possible to reconstruct the secret s from any $k > t$ shares, and thus there must exist a reconstruction vector $\boldsymbol{r} \in \mathbb{L}^k \setminus \{\mathbf{0}\}$ such that $r_1 \begin{pmatrix} m_1 & m'_{11} & \cdots & m'_{1k} \end{pmatrix} + \cdots + r_k \begin{pmatrix} m_k & m'_{k1} & \cdots & m'_{kk} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$. In particular,

$$r_1 \begin{pmatrix} m'_{11} & \cdots & m'_{1k} \end{pmatrix} + \cdots + r_k \begin{pmatrix} m'_{k1} & \cdots & m'_{kk} \end{pmatrix} = \mathbf{0}.$$

This contradicts the linear independence of the rows of N'. ■

By Lemma 5.2.1, we may assume in the following that for any $(t+1)$-out-of-n threshold LSSS the share distribution matrix M has precisely n rows and $t+1$ columns.

Lemma 5.2.2 *Let $\mathcal{S}_M = (\mathbb{L}, M)$ be a $(t+1)$-out-of-n threshold linear secret sharing scheme over a commutative ring $\mathbb{L}$ with share distribution matrix M. If $\mathcal{S}_M$ is secure and functional then any $t+1$ rows of M are linearly independent.*

Proof. For a contradiction, suppose wlog that the first $t+1$ rows of M are linearly dependent. Then there exist $\mu_1, \ldots, \mu_t, \mu_{t+1} \in \mathbb{L}$ not all equal to zero such that $\mu_{t+1}M_{t+1} = \mu_1 M_1 + \cdots + \mu_t M_t$, implying that $\mu_{t+1}s_{t+1} = \mu_1 s_1 + \cdots + \mu_t s_t$ for any share vector $\boldsymbol{s}$. Since $\mathcal{S}_M$ is functional, there exists a reconstruction vector $\boldsymbol{r} \in \mathbb{L}^{t+1}$ such that $r_1 s_1 + \cdots + r_t s_t + r_{t+1}s_{t+1} = s$. This implies that $\mu_{t+1}s = r_1\mu_{t+1}s_1 + \cdots + r_t\mu_{t+1}s_t + r_{t+1}\mu_{t+1}s_{t+1} = (r_1\mu_{t+1} + r_{t+1}\mu_1)s_1 + \cdots + (r_t\mu_{t+1} + r_{t+1}\mu_t)s_t$. Wlog, $\mu_{t+1} \neq 0$. Thus, at least partial information about the secret may be deduced from the first t shares. This contradicts the security of $\mathcal{S}_M$. ■

Lemma 5.2.3 *Let $\mathcal{S}_M = (\mathbb{L}, M)$ be a $(t+1)$-out-of-n threshold linear secret sharing scheme over a commutative ring $\mathbb{L}$ with share distribution matrix M. If any $t+1$ rows of M are linearly independent then $\mathcal{S}_M$ is functional.*

Proof. Let $s_{i_1}, \ldots, s_{i_{t+1}}$ be a subset of $t+1$ shares. Let $M_{\{i_1,\ldots,i_{t+1}\}}$ be the concatenation of the rows $M_{i_1}, \ldots, M_{i_{t+1}}$. Note that $M_{\{i_1,\ldots,i_{t+1}\}}$ is a square matrix. Since the rows $M_{i_1}, \ldots, M_{i_{t+1}}$ are linearly independent, $M_{i_1}, \ldots, M_{i_{t+1}}$ is invertible. Let $\boldsymbol{r} = M^{-T}_{\{i_1,\ldots,i_{t+1}\}} \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}^T$. Clearly, $\boldsymbol{r}^T M_{\{i_1,\ldots,i_{t+1}\}} = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$, which means that $\boldsymbol{r}$ is a reconstruction vector for the shares $s_{i_1}, \ldots, s_{i_{t+1}}$: $\mathcal{S}_M$ is functional. ■

Lemma 5.2.4 *Let $\mathcal{S}_M = (\mathbb{L}, M)$ be a $(t+1)$-out-of-n threshold linear secret sharing scheme over a commutative ring $\mathbb{L}$ with share distribution matrix $M = (\boldsymbol{m}||M')$. If $\mathcal{S}_M$ is secure and functional then any t rows of M' are linearly independent.*

Proof. Let $M'_{i_1}, \ldots, M'_{i_t}$ be a subset of t rows of M'. Let $i_{t+1} \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_t\}$. Since $\mathcal{S}_M$ is functional, there exists a reconstruction vector $\boldsymbol{r} \in \mathbb{L}^{t+1}$ such that $r_1 M_{i_1} + \cdots + r_{t+1}M_{i_{t+1}} = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$, implying that $r_1 M'_1 + \cdots + r_{t+1}M'_{i_{t+1}} = \mathbf{0}$. By Lemma 3.3.9, r_{t+1} is invertible since $\{i_1, \ldots, i_{t+1}\}$ is a minimal qualified subset. Hence, $M'_{i_{t+1}} = -r^{-1}_{t+1}(r_1 M'_{i_1} + \cdots + r_t M'_{i_t})$. By Lemma 5.2.2, the rows $M_{i_1}, \ldots, M_{i_{t+1}}$ are linearly independent, which means that the square matrix $(M_{i_1}|| \cdots ||M_{i_{t+1}})$ has maximal rank. By Fact 2.3.17, there exists an invertible square matrix $C \in \mathbb{L}^{(t+1)\times(t+1)}$ such that $I_{(t+1)\times(t+1)} = C(M_{i_1}|| \cdots ||M_{i_{t+1}})$. This implies

that

$$I_{t\times t} = \begin{pmatrix} c_{21} & \cdots & c_{2t+1} \\ c_{31} & \cdots & c_{3t+1} \\ \vdots & \ddots & \vdots \\ c_{t+11} & \cdots & c_{t+1t+1} \end{pmatrix} (M'_{i_1}||\cdots||M'_{i_{t+1}})$$

$$= \begin{pmatrix} c_{21} - r_{t+1}^{-1} r_1 c_{2t+1} & \cdots & c_{2t} - r_{t+1}^{-1} r_t c_{2t+1} \\ c_{31} - r_{t+1}^{-1} r_1 c_{3t+1} & \cdots & c_{3t} - r_{t+1}^{-1} r_t c_{3t+1} \\ \vdots & \ddots & \vdots \\ c_{t+11} - r_{t+1}^{-1} r_1 c_{t+1t+1} & \cdots & c_{t+1t} - r_{t+1}^{-1} r_t c_{t+1t+1} \end{pmatrix} (M'_{i_1}||\cdots||M'_{i_t}).$$

Hence, the square matrix $(M'_{i_1}||\cdots||M'_{i_t})$ is invertible. By Fact 2.3.7, this implies that $(M'_{i_1}||\cdots||M'_{i_t})$ has maximal rank, which means that the rows $M'_{i_1}, \ldots, M'_{i_t}$ are linearly independent. ■

Lemma 5.2.5 *Let $\mathcal{S}_M = (\mathbb{L}, M)$ be a $(t+1)$-out-of-n threshold linear secret sharing scheme over a commutative ring $\mathbb{L}$ with share distribution matrix $M = (\boldsymbol{m}||M')$. If any t rows of M' are linearly independent then $\mathcal{S}_M$ is secure.*

Proof. Let A be an unqualified subset, wlog $|A| = t$. Note that since any t rows of M' are linearly independent, the matrix M'_A is invertible. A vector $\boldsymbol{\kappa} \in \mathbb{L}^{t+1}$ with $\kappa_1 = 1$ is in the kernel of M_A if and only if $\boldsymbol{m_A} + M'\boldsymbol{\kappa'} = \mathbf{0}$, where $\boldsymbol{\kappa'} = (\kappa_2, \ldots, \kappa_{t+1})^T$. Equivalently, $M'\boldsymbol{\kappa'} = -\boldsymbol{m_A}$. Clearly, $\boldsymbol{\kappa'} = -M'^{-1}\boldsymbol{m_A}$ is a solution. Hence, $\mathcal{S}_M$ is secure. ■

The following is a corollary of Lemmas 5.2.2, 5.2.3, 5.2.4, and 5.2.5.

Corollary 5.2.6 *Let $\mathcal{S}_M = (\mathbb{L}, M)$ be a linear secret sharing scheme over a commutative ring $\mathbb{L}$ with share distribution matrix $M = (\boldsymbol{m}||M')$. Then $\mathcal{S}_M$ is a secure and functional $(t+1)$-out-of-n threshold LSSS if and only if any $t+1$ rows of M are linearly independent and any t rows of M' are linearly independent.*

The following definition is due to Z. Beerliova-Trubiniova and M. Hirt [1].

Definition 5.2.7 We say that a matrix M with d rows and e columns is *hyper-invertible* if for any index sets $D \subseteq \{1, \ldots, d\}$ and $E \subseteq \{1, \ldots, e\}$ with $|D| = |E| > 0$, the matrix M_D^E is invertible, where M_D denotes the matrix consisting of the rows $i \in D$ of M, M^C denotes the matrix consisting of the columns $j \in E$ of M, and $M_D^E = (M_D)^E$.

Lemma 5.2.8 *Let M be a $d \times e$ matrix over a commutative ring $\mathbb{L}$. Then any e rows of M are linearly independent if and only if there exist an invertible $e \times e$ matrix U and a $d \times e$ matrix B such that $M = BU$ with*

$$B = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ c_{11} & c_{12} & \cdots & c_{1e} \\ c_{21} & c_{22} & \cdots & c_{2e} \\ \vdots & \vdots & \ddots & \vdots \\ c_{k1} & c_{k2} & \cdots & c_{ke} \end{pmatrix},$$

where $k = d - e$ and the matrix C is hyper-invertible.

Proof. First suppose that $M = BU$. Let M' be an $e \times e$ submatrix of M. Then $M' = B'U$, where B' is an $e \times e$ submatrix of B. Since U is invertible, $\operatorname{rank} M' = \operatorname{rank}(B'U) = \operatorname{rank} B'$. To prove that M' is of rank e, it hence suffices to prove that $\operatorname{rank} B' = e$. By elementary row operations, we may convert B' into the matrix

$$B'' = \begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & \cdots & 0 \\ c_{11} & c_{12} & \cdots & c_{1j} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2j} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \cdots \\ c_{e-j1} & c_{e-j2} & \cdots & c_{e-jj} & \cdots & c_{e-je} \end{pmatrix}$$

for some $0 \leq j \leq e$. Again by elementary row operations, we may convert B'' into the matrix

$$B''' = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & c_{1j+1} & \cdots & c_{1n} \\ 0 & 0 & \cdots & 0 & c_{2j+1} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \cdots \\ 0 & 0 & \cdots & 0 & c_{e-jj+1} & \cdots & c_{e-je} \end{pmatrix}.$$

Note that by Fact 2.3.18,

$$\begin{aligned}\operatorname{rank} B' &= \operatorname{rank} B'' = \operatorname{rank} B''' \\ &= \operatorname{rank} \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} + \operatorname{rank} \underbrace{\begin{pmatrix} c_{1j+1} & c_{1j+2} & \cdots & c_{1e} \\ c_{2j+1} & c_{2j+2} & \cdots & c_{2e} \\ \vdots & \vdots & \ddots & \vdots \\ c_{e-jj+1} & c_{e-jj+2} & \cdots & c_{e-je} \end{pmatrix}}_{C'}.\end{aligned}$$

Since C is hyper-invertible, C' is invertible. Hence, $\operatorname{rank} B' = j + e - j = e$.

Conversely, suppose that that every subset of e rows of M is of rank e. In particular, the first e rows of M are linearly independent. Let M_1 be the invertible square matrix consisting of the first e rows of M, and let M_2 be the matrix consisting of the last $k = d - e$ rows of M. Let $U = M_1$, and let $C = M_2 U^{-1}$. Then $M = BU$, where B is the $d \times e$ matrix

$$B = \begin{pmatrix} I \\ C \end{pmatrix}.$$

It remains to prove that C is hyper-invertible. Let C' be a $j \times j$ square submatrix of C for some $1 \leq j \leq e$. Wlog

$$C' = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1j} \\ c_{21} & c_{22} & \cdots & c_{2j} \\ \vdots & \vdots & \ddots & \vdots \\ c_{j1} & c_{j2} & \cdots & c_{jj} \end{pmatrix}.$$

Since U^{-1} is invertible and any subset of e or fewer rows of M is of maximal rank, any subset of e or fewer rows of B is of maximal rank. For a contradiction, suppose that C' is not invertible. There hence exist $\gamma_1, \ldots, \gamma_j$ such that $\gamma_1 C'_1 + \cdots + \gamma_j C'_j = \mathbf{0}$. Note that, for $1 \leq i \leq j$, $B_{e+i} - (c_{ij+1}B_{j+1} + \cdots + c_{ie}B_e) = \begin{pmatrix} c_{i1} & \cdots & c_{ij} & 0 & \cdots & 0 \end{pmatrix}$. Hence, $\mathbf{0} = \gamma_1(B_{e+1} - (c_{1j+1}B_{j+1} + \cdots + c_{1e}B_e)) + \cdots + \gamma_j(B_{e+j} - (c_{jj+1}B_{j+1} + \cdots + c_{je}B_e)) = \gamma_1 B_{e+1} + \cdots + \gamma_j B_{e+j} - (\gamma_1 c_{1j+1} + \cdots + \gamma_j c_{jj+1})B_{j+1} - \cdots - (\gamma_1 c_{1e} + \cdots + \gamma_j c_{je})B_e$. Hence, the subset of rows $\{B_{j+1}, \ldots, B_e, B_{e+1}, \ldots, B_{e+j}\}$ of size e is of rank less than e. This is a contradiction. Hence, C' must be invertible. ■

The following is a corollary of Lemma 5.2.4 and Lemma 5.2.8.

Corollary 5.2.9 *Let $\mathbb{L}$ be a commutative ring. Let $\mathcal{S}$ be a $(t+1)$-out-of-n threshold linear secret sharing scheme over $\mathbb{L}$. Then there exists a hyper-invertible $(n-t) \times t$ matrix C such that $M = (\boldsymbol{m}||M')$ with*

$$M' = \begin{pmatrix} I \\ C \end{pmatrix}$$

is a share distribution matrix for $\mathcal{S}$ for any $\boldsymbol{m} \in \mathsf{Share}(1)$.

Lemma 5.2.10 *Let $\mathcal{S}_M = (\mathbb{L}, M)$ be a $(t+1)$-out-of-n threshold LSSS over a commutative ring $\mathbb{L}$ with share distribution matrix $M = (\boldsymbol{m}||M)$. Then at most t elements of $\boldsymbol{m}$ are equal to zero.*

Proof. For a contradiction suppose that $\boldsymbol{m}$ has $t+1$ zero elements. Wlog, by switching rows, the first $t+1$ elements of $\boldsymbol{m}$ are equal to zero. By elementary column operations, wlog $M'_i = \boldsymbol{e_i}$. Then clearly M_{t+1} is a linear combination of the first t rows. This contradicts Lemma 5.2.2. ■

Recall that $\mathsf{Share}(1) \equiv \boldsymbol{m} + \mathsf{Share}(0)$ for any $\boldsymbol{m} \in \mathsf{Share}(1)$. By Corollary 5.2.9 and Lemma 5.2.10, we may always assume that

$$M = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ m_{t+11} & m_{t+12} & m_{t+13} & \cdots & m_{t+1t+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & m_{n3} & \cdots & m_{nt+1} \end{pmatrix}, \tag{5.1}$$

where the elements $m_{t+11}, \ldots, m_{n1}$ are non-zero and the matrix

$$\begin{pmatrix} m_{t+12} & m_{t+13} & \cdots & m_{t+1t+1} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n2} & m_{n3} & \cdots & m_{nt+1} \end{pmatrix}$$

is hyper-invertible. In fact, the elements $m_{t+11}, \ldots, m_{n1}$ are invertible.

Lemma 5.2.11 *Let $\mathcal{S}_M = (\mathbb{L}, M)$ be a $(t+1)$-out-of-n threshold LSSS over a commutative ring $\mathbb{L}$ with share distribution matrix $M = (\boldsymbol{m}||M)$ such that the first t elements of $\boldsymbol{m}$ are equal to zero. Then the remaining $n-t$ elements of $\boldsymbol{m}$ are invertible.*

Proof. For a contradiction suppose that there exists i, $t+1 \leq i \leq n$, such that m_i is a zero divisor. Let $z \in \mathbb{L}$ such that $zm_i = 0$. Then clearly zM_i is a linear combination of the first t rows. This contradicts Lemma 5.2.2. ■

5.2.1 Algorithm: isThreshold(M)

Let $\mathcal{S}_M = (\mathbb{K}, M)$ be a linear secret sharing scheme over a field $\mathbb{K}$ with share distribution matrix M. In this subsection, we present an algorithm to check whether $\mathcal{S}_M$ is a $(t+1)$-out-of-n threshold linear secret sharing scheme. Naively, one could do the following:

Algorithm 5 isThreshold(M)

counter $\leftarrow 0$
for all $\boldsymbol{r}$ **do**
  if isRec($\boldsymbol{r}$,M) and $\boldsymbol{r}$ has more than $n-(t+1)$ zero elements **then**
    return false
  end if
end for
for all $\boldsymbol{r}$ **do**
  if isRec($\boldsymbol{r}$,M) and $\boldsymbol{r}$ has $n-(t+1)$ zero elements **then**
    counter $\leftarrow$ counter + 1
  end if
end for
if counter $= \binom{n}{n-(t+1)}$ **then**
  return true
else
  return false
end if

By Corollary 5.2.6, it suffices to check that any t rows of M' are linearly independent and that any $t+1$ rows of M are linearly independent.

Algorithm 6 isThreshold(M)

for all subsets of t rows $M'_{i_1}, \ldots, M'_{i_t}$ **do**
  if $\det M'_{\{i_1,\ldots,i_t\}} = 0$ **then**
    return false
  end if
end for
for all subsets of $t+1$ rows $M_{i_1}, \ldots, M_{i_{t+1}}$ **do**
  if $\det M_{\{i_1,\ldots,i_{t+1}\}} = 0$ **then**
    return false
  end if
end for
return true

5.3 Efficient Generation of Multiplicative Threshold Linear Secret Sharing Schemes

In this section, we will present an algorithm to generate all multiplicative $(t+1)$-out-of-n threshold linear secret sharing schemes over $\mathbb{Z}_p$, where p is a prime and $p \geq n-t+1$.

Fact 5.3.1 *If the rows or columns of a hyper-invertible matrix are multiplied by invertible elements, the matrix remains hyper-invertible.*

Lemma 5.3.2 *Let $\mathcal{S}_M = (\mathbb{L}, M)$ be a linear secret sharing scheme for an access structure Γ with share distribution matrix $M = (\boldsymbol{m}||M') \in \mathbb{L}^{d\times e}$. Let $\boldsymbol{c} \in \mathbb{L}^d$ be a vector with invertible elements $c_1, \ldots, c_d$. Let $\overline{M} = \boldsymbol{c} \star M$. Then $\boldsymbol{s} = \overline{M}\boldsymbol{b}$ defines a linear secret sharing scheme $\mathcal{S}_{\overline{M}} = (\mathbb{L}, \overline{M})$ for Γ. If $\mathcal{S}_M$ is multiplicative, then $\mathcal{S}_{\overline{M}}$ is also multiplicative.*

Proof. Define a map $\phi_1 : \mathcal{R}(\mathcal{S}_M) \rightarrow \mathcal{R}(\mathcal{S}_{\overline{M}})$ by $\boldsymbol{r} \mapsto \overline{\boldsymbol{r}}$, where $\overline{r}_i = c_i^{-1} r_i$. Clearly, ϕ_1 is a bijection that maps reconstruction vectors $\boldsymbol{r}$ for A in $\mathcal{S}_M$ to reconstruction vectors $\overline{\boldsymbol{r}} = \phi_1(\boldsymbol{r})$ for A in $\mathcal{S}_{\overline{M}}$ for any $A \in \Gamma$. This proves that $\mathcal{S}_{\overline{M}}$ is an LSSS for Γ.

Suppose that $\mathcal{S}_M$ is multiplicative. Define a map $\phi_2 : \mathcal{R}^\star(\mathcal{S}_M) \rightarrow \mathcal{R}^\star(\mathcal{S}_{\overline{M}})$ by $\boldsymbol{r}^\star \mapsto \overline{\boldsymbol{r}^\star}$, where $\overline{r^\star}_i = c_i^{-2} r_i^\star$. Clearly, ϕ_2 is a bijection that maps reconstruction vectors for multiplication $\boldsymbol{r}^\star$ for $\mathcal{S}_M$ to reconstruction vectors for multiplication $\overline{\boldsymbol{r}^\star} = \phi_2(\boldsymbol{r}^\star)$ for $\mathcal{S}_{\overline{M}}$. Hence, $\mathcal{S}_{\overline{M}}$ is multiplicative. ■

If $\mathcal{S}_M$ is homomorphic, then $\mathcal{S}_{\overline{M}}$ is not necessarily homomorphic.

Example 5.3.3 Let

$$M = \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 3 \end{pmatrix}.$$

Clearly, $\mathcal{S}_M$ is homomorphic. Let $\boldsymbol{c} = \begin{pmatrix} 2 & 3 & 4 \end{pmatrix}^T$. Then

$$\overline{M} = \begin{pmatrix} 2 & 2 \\ 3 & 1 \\ 4 & 2 \end{pmatrix}.$$

The reconstruction vectors for addition are

$$\begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 4 \\ 4 \end{pmatrix},$$

and the only reconstruction vector for multiplication is

$$\begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix}.$$

Hence, $\mathcal{S}_{\overline{M}}$ is not homomorphic.

Let $\boldsymbol{m}^\star = \begin{pmatrix} 0 & \cdots & 0 & 1 & \cdots & 1 \end{pmatrix}^T$ be the n-vector whose first t elements are equal to zero and whose remaining $n - t$ elements are equal to 1. The following is a corollary of Lemma 5.2.5.

Corollary 5.3.4 *Let $\mathbb{L}$ be a commutative ring. Let M' be the $n \times t$ matrix*

$$M' = \begin{pmatrix} I \\ C \end{pmatrix},$$

where C is a hyper-invertible matrix. Let $M = (\boldsymbol{m}^\star || M')$. Then $\boldsymbol{s} = M\boldsymbol{b}$ defines a secure $(t+1)$-out-of-n threshold linear secret sharing scheme $\mathcal{S}_M$.

Note that $\mathcal{S}_M$ is not necessarily functional.

Example 5.3.5 Let $M' \in \mathbb{Z}_7^{7\times 2}$ be the 7×2 matrix

$$M' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 2 & 6 \\ 6 & 2 \\ 5 & 3 \\ 3 & 4 \\ 4 & 5 \end{pmatrix}.$$

Note that

$$C = \begin{pmatrix} 2 & 6 \\ 6 & 2 \\ 5 & 3 \\ 3 & 4 \\ 4 & 5 \end{pmatrix}$$

is hyper-invertible. Consider the qualified subset $A = \{3, 4, 5\}$. A vector $\boldsymbol{r_A}$ is a reconstruction vector if and only if $\boldsymbol{r_A}$ is a solution of the system of linear equations

$$\begin{cases} r_1 + r_2 + r_3 = 1 \\ 2r_1 + 6r_2 + 5r_3 = 0 \\ 6r_1 + 2r_2 + 3r_3 = 0 \end{cases}$$

Equivalently, $\boldsymbol{r_A}$ is a solution of the system of linear equations

$$\begin{cases} r_1 + r_2 + r_3 = 1 \\ r_2 + 6r_3 = 3 \\ 0 = 2 \end{cases}$$

Clearly, there is no such solution $\boldsymbol{r_A}$.

Lemma 5.3.6 *We may generate all $(t+1)$-out-of-n threshold linear secret sharing schemes over $\mathbb{K}$ by generating all $(t+1)$-out-of-n threshold linear secret sharing schemes over $\mathbb{K}$ with $\boldsymbol{m}^\star \in \mathsf{Share}(1)$ and multiplying the last $n-t$ rows of the share distribution matrix M by non-zero elements.*

Proof. Let $\mathcal{S}_M = (\mathbb{K}, M)$ be a $(t+1)$-out-of-n threshold linear secret sharing scheme over $\mathbb{K}$ with share distribution matrix M. By Corollary 5.2.9 and Lemma 5.2.10, wlog $M = (\boldsymbol{m}||M')$, where the first t elements of $\boldsymbol{m}$ are equal to 0 and the remaining $n-t$ elements are non-zero and

$$M' = \begin{pmatrix} I \\ C \end{pmatrix},$$

where C is hyper-invertible. By Lemma 5.3.2, $\boldsymbol{s} = M^{\star}\boldsymbol{b}$, where $M_i^{\star} = \frac{1}{m_{i1}} M_i$ for $t+1 \leq i \leq n$, defines a $(t+1)$-out-of-n threshold linear secret sharing scheme $\mathcal{S}_{M^\star}$ over $\mathbb{K}$ with share distribution matrix $M^{\star} = (\boldsymbol{m}^{\star}||M'^{\star})$, where

$$M'^{\star} = \begin{pmatrix} I \\ C^{\star} \end{pmatrix}.$$

By Fact 5.3.1, $C^{\star}$ is hyper-invertible. Hence, $\mathcal{S}_{M^\star}$ is one of the $(t+1)$-out-of-n threshold linear secret sharing schemes with $\boldsymbol{m}^{\star} \in \mathsf{Share}(1)$ generated, and $\mathcal{S}_M$ will be generated from $\mathcal{S}_{M^\star}$ by multiplying the ith row of $M^{\star}$ by m_{i1}. ■

Naively, one would generate all $n \times (t+1)$ matrices M over $\mathbb{Z}_p$ and check for each matrix whether the linear secret sharing scheme with share distribution matrix M is a multiplicative $(t+1)$-out-of-n threshold linear secret sharing scheme. By Lemma 5.3.6 and Corollary 5.2.9, we do not need to generate all possible $n \times (t+1)$ matrices over $\mathbb{Z}_p$. It suffices to generate all possible $(n-t) \times t$ hyper-invertible matrices over $\mathbb{Z}_p$. By Lemma 5.3.2, it is sufficient to check whether $\mathcal{S}_M = (\mathbb{Z}_p, M)$ with

$$M = (\boldsymbol{m}^{\star}|| \begin{pmatrix} I \\ C \end{pmatrix})$$

is a multiplicative $(t+1)$-out-of-n threshold linear secret sharing scheme: a linear secret sharing scheme with share distribution matrix $\boldsymbol{c} \star M$, where $\boldsymbol{c}$ is a vector with the first t elements equal to 1 and the remaining $n-t$ elements not equal to zero, is a multiplicative $(t+1)$-out-of-n threshold linear secret sharing scheme if and only if the linear secret sharing scheme with share distribution matrix M is a multiplicative $(t+1)$-out-of-n threshold linear secret sharing scheme. If the generation of hyper-invertible matrices is efficient, the following algorithm is efficient:

Algorithm 7 MultThreshold

thresholdMatrices $\leftarrow \emptyset$
for $i_1 = 1$ to $p-1$ **do**
  for $i_2 = 1$ to $p-1$ **do**
    $\ddots$
    for $i_{(n-t)t} = 1$ to $p-1$ **do**
      $C[1][1] \leftarrow i_1$
      $C[1][2] \leftarrow i_2$
      $\vdots$
      $C[n-t][t] \leftarrow i_{(n-t)t}$
      if C is hyper-invertible **then**
        $M \leftarrow (\boldsymbol{m}^\star || \begin{pmatrix} I \\ C \end{pmatrix})$
        if isThreshold(M) and isMult(M) **then**
          for all $\boldsymbol{c}$ **do**
            thresholdMatrices $\leftarrow$ thresholdMatrices $\cup\ \boldsymbol{c} \star M$
          end for
        end if
      end if
    end for
    $\iddots$
  end for
end for

Note that all $(t+1)$-out-of-n threshold linear secret sharing schemes generated by algorithm MultThreshold are distinct. By Lemma 5.3.4, any $(t+1)$-out-of-n threshold linear secret sharing scheme over $\mathbb{Z}_p$ with share distribution matrix

$$M = (\boldsymbol{m}^\star || \begin{pmatrix} I \\ C \end{pmatrix})$$

is secure. It suffices to check whether the scheme is functional. Algorithm isThreshold(M) in section 5.2 checks both security and functionality. The algorithm below is sufficient:

Algorithm 8 isThreshold(M)

for all subsets of $t+1$ rows $M_{i_1}, \ldots, M_{i_{t+1}}$ **do**
  if $\det M_{\{i_1,\ldots,i_{t+1}\}} = 0$ **then**
    return false
  end if
end for
return true

The algorithm is implemented in the programs `MultThreshold2_3.java` for multiplicative 2-out-of-3 threshold LSSSs and `MultThreshold3_5.java` for multiplicative 3-out-of-5 threshold LSSSs. Both programs use the library `MultThresholdLib.java`.

Output of the program `MultThreshold2_3.java` for $\mathbb{Z}_5$ (runtime < 1 min):

```
Enter n: 5
Number of 3x2 2-out-of-3 multiplicative threshold LSSSs over ZZ_5:
192
```

Output of the program `MultThreshold2_3.java` for $\mathbb{Z}_7$ (runtime < 1 min):

```
Enter n: 7
Number of 3x2 2-out-of-3 multiplicative threshold LSSSs over ZZ_7:
1080
```

Output of the program `MultThreshold3_5.java` for $\mathbb{Z}_7$ (runtime < 5 mins):

```
Enter n: 7
Number of 5x3 3-out-of-5 multiplicative threshold LSSSs over ZZ_7:
418176
```

5.4 Existence of Threshold Linear Secret Sharing Schemes

In section section 4.2, we constructed a linear secret sharing scheme over $\mathbb{Z}_{2^{32}}$ for the threshold access structure $\Gamma_{1,3}$ in which each player is given 2 shares. In a 2-out-of-3 threshold linear secret sharing scheme for $\Gamma_{1,3}$, each player is given just one share. In this section, we prove that it is not possible to construct a 2-out-of-3 threshold linear secret sharing scheme over $\mathbb{Z}_{2^{32}}$.

Lemma 5.4.1 *Let $\mathbb{K}$ be a finite field. A $(t+1)$-out-of-n threshold linear secret sharing scheme over $\mathbb{K}$ can exist only if $|\mathbb{K}| \geq n - t + 1$.*

Proof. Let $\mathcal{S}_M = (\mathbb{K}, M)$ be a $(t+1)$-out-of-n threshold LSSS over $\mathbb{K}$. By (5.1), wlog

$$M = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ m_{t+11} & m_{t+12} & m_{t+13} & \cdots & m_{t+1t+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & m_{n3} & \cdots & m_{nt+1} \end{pmatrix}.$$

By Lemma 5.2.10, none of the elements m_{i1}, $t+1 \leq i \leq n$ can be equal to zero. By Lemma 5.3.2, there hence exists a $(t+1)$-out-of-n threshold LSSS $\mathcal{S}_{M^\star} = (\mathbb{K}, M^\star)$ with

$$M^\star = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & m^\star_{t+12} & m^\star_{t+13} & \cdots & m^\star_{t+1t+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & m^\star_{n2} & m^\star_{n3} & \cdots & m^\star_{nt+1} \end{pmatrix}.$$

Again by Lemma 5.2.10, the $n-t$ last elements of M'^1 have to be distinct. Note that none of the elements $m^\star_{ij}$, $t+1 \leq i \leq n$, $2 \leq j \leq t+1$, can be equal to zero: Wlog, suppose for a contradiction that $m^\star_{t+11} = 0$. Then $M^\star_{t+1} - m^\star_{t+13}M^\star_2 - ... - m^\star_{t+1t+1}M^\star_t = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$, which contradicts that the threshold is t. Hence, $|\mathbb{K}| \geq n-t+1$. ■

Corollary 5.4.2 *There does not exist a $(t+1)$-out-of-n threshold LSSS over $\mathbb{Z}_2$ for $n > t+1$.*

Note that there does exist an n-out-of-n threshold LSSS over $\mathbb{Z}_2$: the additive scheme.

Theorem 5.4.3 *Let $(\mathbb{G}; \star)$ be a finite Abelian group. If there exists a $(t+1)$-out-of-n threshold LSSS over $\mathbb{G}$, then there exists a $(t+1)$-out-of-n threshold LSSS over $\mathbb{H}$ for any characteristic subgroup $\mathbb{H}$ of $\mathbb{G}$.*

Proof. Let $\mathcal{S} = (\mathbb{G}, (\mathbb{G}, ..., \mathbb{G}), \mathsf{Share})$ be a $(t+1)$-out-of-n threshold LSSS over $(\mathbb{G}; \star)$. Let $\mathsf{Share_i} : \mathbb{G} \to \mathbb{G}$, $1 \leq i \leq n$, be defined by $\mathsf{Share_i}(s) = \mathsf{Share}(s)_i$. Note that since Share is a group homomorphism, each $\mathsf{Share_i}$ is a group automorphism. Define $\mathsf{Share}_\mathsf{i}^\mathbb{H}$ to be the restriction of $\mathsf{Share_i}$ to $\mathbb{H}$. Since $\mathbb{H}$ is a characteristic subgroup of $\mathbb{G}$, each $\mathsf{Share}_\mathsf{i}^\mathbb{H}$ is a group automorphism. Define $\mathsf{Share}^\mathbb{H} : \mathbb{H} \to (\mathbb{H}, ..., \mathbb{H})$ by $\mathsf{Share}^\mathbb{H}(s) = (\mathsf{Share}_\mathsf{1}^\mathbb{H}, ..., \mathsf{Share}_\mathsf{n}^\mathbb{H})$. Clearly, $\mathsf{Share}^\mathbb{H}$ is a group homomorphism. Define $\mathcal{S}^\mathbb{H} = (\mathbb{H}, (\mathbb{H}, ..., \mathbb{H}), \mathsf{Share}^\mathbb{H})$. Below we prove that $\mathcal{S}^\mathbb{H}$ is a $(t+1)$-out-of-n threshold LSSS over $(\mathbb{H}; \star)$.

First we prove that $\mathcal{S}^\mathbb{H}$ is functional. Let $A \in \Gamma_{t,n}$. By the functionality of $\mathcal{S}$, there exists a reconstruction function $\mathsf{Rec_A}$ such that $\mathsf{Rec_A}(\mathsf{Share}_A(s)) = s$ for all $s \in \mathbb{G}$. Define $\mathsf{Rec}_\mathsf{A}^\mathbb{H}$ to be the restriction of $\mathsf{Rec_A}$ to $\mathbb{H}$. Then, for all $s \in \mathbb{H}$, $\mathsf{Rec}_\mathsf{A}^\mathbb{H}(\mathsf{Share}^\mathbb{H}{}_A(s)) = s$. Hence, $\mathsf{Rec}_\mathsf{A}^\mathbb{H}$ is a reconstruction function.

Now we prove that $\mathcal{S}^\mathbb{H}$ is secure. Let $A \in \mathcal{A}_{t,n}$. Let $s, s' \in \mathbb{H}$. Clearly, if $\mathsf{Share}^\mathbb{H}(s)_A \not\equiv \mathsf{Share}^\mathbb{H}(s')_A$, then $\mathsf{Share}(s)_A \not\equiv \mathsf{Share}(s')_A$. Hence, since $\mathcal{S}$ is secure, $\mathcal{S}^\mathbb{H}$ must be secure. ■

Let $\mathbb{L}$ be a finite commutative ring, and let $N = \operatorname{char}\mathbb{L}$. By Fact 2.1.16, $N \neq 0$. Note that the ring $< 1 >= 1 \cdot \mathbb{Z} \cong \mathbb{Z}_N$ is a subring of $\mathbb{L}$. Further, note that the group $(< 1 >; +) \cong (\mathbb{Z}_N; +)$ is a characteristic subgroup of $(\mathbb{L}; +)$. By Theorem 5.4.3 above, in order to prove that there does not exist a $(t+1)$-out-of-n threshold linear secret sharing scheme over the ring $\mathbb{L}$, it is sufficient to prove that there does not exist a $(t+1)$-out-of-n threshold linear secret sharing scheme over the ring $\mathbb{Z}_N$. In fact, by Corollary 5.4.4 below, it is sufficient to prove non-existence of a $(t+1)$-out-of-n threshold linear secret sharing scheme over the field $\mathbb{Z}_p$, where p is a prime divisor of N.

Corollary 5.4.4 *If there exists a $(t+1)$-out-of-n threshold LSSS over $(\mathbb{Z}_N; +)$, then there exists a $(t+1)$-out-of-n threshold LSSS over $(\mathbb{Z}_p; +)$ for any prime divisor p of N.*

Proof. Let p be a prime divisor of N. By Corollary 2.1.12, $(\mathbb{Z}_p; +)$ is a characteristic subgroup of $(\mathbb{Z}_N; +)$. Hence, by Theorem 5.4.3, there exists a $(t+1)$-out-of-n threshold LSSS over $(\mathbb{Z}_p; +)$. ■

Corollary 5.4.5 *For $n > t+1$, there does not exist a $(t+1)$-out-of-n threshold LSSS over $(\mathbb{Z}_{2^k}; +)$ for any integer $k > 0$.*

Proof. For a contradiction, suppose that there exists an integer $k > 0$ such that there exists a $(t+1)$-out-of-n threshold LSSS over $(\mathbb{Z}_{2^k}; +)$. $\mathbb{Z}_2$ is a characteristic subgroup of $\mathbb{Z}_{2^k}$ for any $k > 0$. Hence, by Corollary 5.4.4, there exists a $(t+1)$-out-of-n threshold LSSS over $(\mathbb{Z}_2; +)$. This contradicts Corollary 5.4.2. ■

5.5 Polynomial Interpolation and Multiplicative Threshold Linear Secret Sharing Schemes

Shamir's secret sharing scheme is an example of a $(t+1)$-out-of-n threshold secret sharing scheme with threshold access structure $\Gamma_{t,n}$. Shamir's secret sharing scheme is optimal with respect to share size: each share is of the same size as the secret. In general, for perfectly secure linear secret sharing schemes, the size of a share is at least the size of the secret. Only for ϵ-secure linear secret sharing schemes, the size of a share may be less than the size of the secret. Recall that the ith Shamir share is equal to the evaluation of a polynomial of degree t at the point i, and the secret s is equal to the polynomial evaluated at the point 0. Shamir's secret sharing scheme is based on polynomial interpolation.

Definition 5.5.1 Let $\mathcal{S}$ be a linear secret sharing scheme for the threshold access structure $\Gamma_{t,n}$. We say that $\mathcal{S}$ is *based on polynomial interpolation* if there exist $\alpha_1, \ldots, \alpha_d \in \mathbb{L}$ such that for any valid sharing $(s_1, \ldots, s_d)$, there exists a polynomial f of degree t such that $s_i = f(\alpha_i)$ for all $1 \leq i \leq d$.

The ith share of a linear secret sharing scheme based on polynomial interpolation is equal to the evaluation of a polynomial of degree t at some point, and the secret s may or may not be equal to the polynomial evaluated at some point.

Lemma 5.5.2 *Let $\mathcal{S}$ be a linear secret sharing scheme for the threshold access structure $\Gamma_{t,n}$. There exists a polynomial f of degree t such that $f(\alpha_0) = s$ for some $\alpha_0 \in \mathbb{L}$ and $\mathcal{S}$ is based on polynomial interpolation with f if and only if there exists a polynomial f' of degree t such that $f'(0) = s$ and $\mathcal{S}$ is based on polynomial interpolation with f'.*

Proof. Suppose that there exists a polynomial f of degree t such that $f(\alpha_0) = s$ for some $\alpha_0 \in \mathbb{L}$ and $\mathcal{S}$ is based on polynomial interpolation with f. Let $\alpha_1, \ldots, \alpha_n$ be such that $f(\alpha_i) = s_i$ for all i, $1 \leq i \leq n$. Define $\beta_i = \alpha_i - \alpha_0$, and define $f'(x) = f(x + \alpha_0)$. Then, $f'(\beta_i) = f(\alpha_i) = s_i$, $f'(0) = f(\alpha_0) = s$, and $\deg f' = \deg f = t$. Thus, $\mathcal{S}$ is based on polynomial interpolation with f', and $f'(0) = s$.

Conversely, suppose that there exists a polynomial f' of degree t such that $f'(0) = s$ and $\mathcal{S}$ is based on polynomial interpolation with f'. Define $f = f'$, and define $\alpha_0 = 0$. Clearly, $\mathcal{S}$ is based on polynomial interpolation with f, and $f(\alpha_0) = s$. ■

Lemma 5.5.3 *Let $\mathcal{S}$ be a linear secret sharing scheme for the threshold access structure $\Gamma_{t,n}$. Let $\mathcal{S}$ be defined by $\boldsymbol{s} = M\boldsymbol{b}$ with $M \in \mathbb{L}^{d \times e}$. Then $\mathcal{S}$ is based on polynomial interpolation if and only if there exist a $d \times (t+1)$ Vandermonde matrix $V \in \mathbb{L}^{d \times (t+1)}$ and a $(t+1) \times e$ matrix $F \in \mathbb{L}^{(t+1) \times e}$ such that $M = VF$.*

Proof. Recall that by definition, $M^1 \in \mathsf{Share}(1)$ and $M^2, \ldots, M^e \in \mathsf{Share}(0)$. If $\mathcal{S}$ is based on polynomial interpolation, then there exist $\alpha_1, \ldots, \alpha_d \in \mathbb{L}$ and polynomials $f_1, \ldots, f_e$ of degree t such that $m_{ij} = f_j(\alpha_i)$. Let the coefficients of f_j be $f_{1j}, \ldots, f_{t+1j}$, and define $F = (f_{ij}) \in \mathbb{L}^{(t+1) \times e}$. Let V be the Vandermonde matrix $V = V(\alpha_1, \ldots, \alpha_d)$. Clearly, $M = VF$.

Conversely, let the Vandermonde matrix $V = V(\alpha_1, \ldots, \alpha_d) \in \mathbb{L}^{d \times (t+1)}$ and $F \in \mathbb{L}^{(t+1) \times e}$ be such that $M = VF$. Let $f_j(x) = f_{1j} + f_{2j}x + \cdots + f_{t+1j}x^t$ for $1 \leq j \leq e$, and define $f(x) = b_1 f_1(x) + \cdots + b_e f_e(x)$. Then f is of degree

t, and

$$\begin{aligned} s_i = M_i\boldsymbol{b} &= \begin{pmatrix} 1 & \alpha_i & \cdots & \alpha_i^t \end{pmatrix} F\boldsymbol{b} \\ &= \begin{pmatrix} f_{11} + \alpha_i f_{21} + \cdots + \alpha_i^t f_{t+11} & \cdots & f_{1e} + \alpha_i f_{2e} + \cdots + \alpha_i^t f_{t+1e} \end{pmatrix} \boldsymbol{b} \\ &= \begin{pmatrix} f_1(\alpha_i) & \cdots & f_e(\alpha_i) \end{pmatrix} \boldsymbol{b} = f(\alpha_i) \end{aligned}$$

for all $1 \leq i \leq d$. ■

Lemma 5.5.4 *Let $\mathbb{L}$ be a finite commutative ring, and let a (t+1)-out-of-n threshold LSSS $\mathcal{S}$ be defined by $\boldsymbol{s} = M\boldsymbol{b}$ with $M \in \mathbb{L}^{n\times(t+1)}$. Then there exists a polynomial f of degree t such that $\mathcal{S}$ is based on polynomial interpolation with f and $f(0) = s$ if and only if $M = VF$ for an $n \times (t+1)$ Vandermonde matrix V and a $(t+1) \times (t+1)$ invertible matrix F with $F_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$.*

Proof. If $\mathcal{S}$ is based on polynomial interpolation with f such that $f(0) = s$, then by Lemma 5.5.3, there exist an $n \times (t+1)$ Vandermonde matrix V and a $(t+1) \times (t+1)$ matrix F such that $M = VF$, and $f(x) = b_1 f_1(x) + \cdots + b_e f_e(x)$, where $f_j(x) = f_{1j} + f_{2j}x + \cdots + f_{t+1j}x^t$ for $1 \leq j \leq e$. Note that $s = f(0) = b_1 f_1(0) + \cdots + b_e f_e(0) = b_1 f_{11} + \cdots + b_e f_{1e}$. Recall that by definition $b_1 = s$. Hence, $f_{11} = 1$ and $f_{12} = \cdots = f_{1t+1} = 0$. By Lemma 3.3.7, the matrix F is invertible.

Conversely, if $M = VF$ for an $n \times (t+1)$ Vandermonde matrix V and a $(t+1) \times (t+1)$ invertible matrix F with $F_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$ then by Lemma 5.5.3, there exists a polynomial f of degree t such that $\mathcal{S}$ is based on polynomial interpolation with f, and $f(x) = s + (f_{21}b_1 + f_{22}b_2 + \cdots + f_{2t+1}b_{t+1})x + \cdots + (f_{t+11}b_1 + f_{t+12}b_2 + \cdots + f_{t+1t+1}b_{t+1})x^t$. Hence, $f(0) = s$. ■

Definition 5.5.5 Let $\mathbb{L}$ be a commutative ring, and let n be an integer, $n \geq 2$. We say that $\mathbb{L}$ is *n-interpolation friendly* if there exist invertible elements $\alpha_1, \ldots, \alpha_n \in \mathbb{L}$ such that for each $i \neq j$, $1 \leq i, j \leq n$, the element $\alpha_i - \alpha_j \in \mathbb{L}$ is invertible as well.

Theorem 5.5.6 below is due to R. Cramer, S. Fehr, Y. Ishai, and E. Kushilevitz [11]. This theorem proves that for any n-interpolation friendly ring $\mathbb{L}$, there exists a $t+1$-out-of-n threshold LSSS based on polynomial interpolation for any threshold access structure $\Gamma_{t,n}$.

Theorem 5.5.6 *Let $\Gamma_{t,n}$ be a threshold access structure. Let $\mathbb{L}$ be an n-interpolation friendly ring. Then there exists an MSP $\mathcal{M} = (\mathbb{L}, M, \boldsymbol{a}, \psi)$ for*

$\Gamma_{t,n}$ *of size* n*, with*

$$M = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^t \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^t \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^t \end{pmatrix},$$

and $\psi(i) = i$ *for each* i*,* $1 \leq i \leq n$*.* $\mathcal{M}$ *is multiplicative if and only if* $t < n/2$*, and strongly multiplicative if and only if* $t < n/3$*.*

Clearly, the LSSS corresponding to the MSP $\mathcal{M} = (\mathbb{L}, M, \boldsymbol{a}, \psi)$ is based on polynomial interpolation with $V = M$ and $F = I$, where I is the $(t+1) \times (t+1)$ identity matrix.

Proof. First, we prove that $\mathcal{M}$ is an MSP for $\Gamma_{t,n}$.

Let $A = \{i_1, i_2, \ldots, i_{t+1}\}$ be a subset of cardinality $t+1$, that is, $A \in \Gamma_{t,n}$. Then, M_A is a Vandermonde matrix with determinant $\det M_A = \prod_{j>k}(\alpha_{i_j} - \alpha_{i_k})$. By assumption on $\alpha_1, \ldots, \alpha_n$, $\det M_A$ is invertible, which implies that M_A is invertible. Thus, $\boldsymbol{a} \in \operatorname{Im} M_A^T$.

Now let $A = \{i_1, i_2, \ldots, i_t\}$ be a subset of cardinality t, that is, $A \notin \Gamma_{t,n}$. Denote the first column of M_A by $\boldsymbol{y}$, and denote the concatenation of the t last columns by $N_A \in \mathbb{L}^{t \times t}$. Then, $\det N_A = \alpha_{i_1} \cdots \alpha_{i_t} \prod_{j>k}(\alpha_{i_j} - \alpha_{i_k})$, which is invertible again by assumption on $\alpha_1, \ldots, \alpha_n$. This implies that N_A is invertible. Thus, $\boldsymbol{y} \in \operatorname{Im} N_A$. Thus, there exists a vector $\boldsymbol{x}$ such that $\mathbf{0} = \boldsymbol{y} - N_A\boldsymbol{x} = M_A(1 - \boldsymbol{x})^T$. Define

$$\boldsymbol{\kappa} = \begin{pmatrix} 1 \\ -\boldsymbol{x} \end{pmatrix},$$

then $M_A\boldsymbol{\kappa} = \mathbf{0}$, and $\kappa_1 = 1$.

Next, we prove that $\mathcal{M}$ is multiplicative if and only if $t < n/2$, and strongly multiplicative if and only if $t < n/3$.

If $2t < n$, then by the above there is a linear combination of the rows of the matrix

$$\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{2t} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{2t} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{2t} \end{pmatrix}$$

which yields $(1, 0, \ldots, 0)$. In other words, there exist $d_1, \ldots, d_n \in \mathbb{L}$ such that $\sum_{i=1}^n d_i(1, \alpha_i, \alpha_i^2, \ldots, \alpha_i^{2t}) = (1, 0, \ldots, 0)$. Let $D \in \mathbb{L}^{n \times n}$ be the diagonal

matrix diag $(d_1, \ldots, d_n)$. Then

$$
\begin{aligned}
M^T D M &= \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^t & \alpha_2^t & \cdots & \alpha_n^t \end{pmatrix} \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_n \end{pmatrix} \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^t \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^t \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^t \end{pmatrix} \\
&= \begin{pmatrix} d_1 & d_2 & \cdots & d_n \\ d_1\alpha_1 & d_2\alpha_2 & \cdots & d_n\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ d_1\alpha_1^t & d_2\alpha_2^t & \cdots & d_n\alpha_n^t \end{pmatrix} \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^t \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^t \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^t \end{pmatrix} \\
&= \begin{pmatrix} \sum_{i=1}^n d_i & \sum_{i=1}^n d_i\alpha_i & \cdots & \sum_{i=1}^n d_i\alpha_i^t \\ \sum_{i=1}^n d_i\alpha_i & \sum_{i=1}^n d_i\alpha_i^2 & \cdots & \sum_{i=1}^n d_i\alpha_i^{t+1} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^n d_i\alpha_i^t & \sum_{i=1}^n d_i\alpha_i^{t+1} & \cdots & \sum_{i=1}^n d_i\alpha_i^{2t} \end{pmatrix} \\
&= \sum_{i=1}^n d_i \begin{pmatrix} 1 & \alpha_i & \cdots & \alpha_i^t \\ \alpha_i & \alpha_i^2 & \cdots & \alpha_i^{t+1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_i^t & \alpha_i^{t+1} & \cdots & \alpha_i^{2t} \end{pmatrix} = \boldsymbol{a}\boldsymbol{a}^T.
\end{aligned}
$$

Note that $3t < n$ if and only if $2t < n - t$, and note that for all $A \in \mathcal{A}_{t,n}$, $|\overline{A}| \geq n - t$. Let $A \in \mathcal{A}_{t,n}$, that is, $\overline{A} = \{i_1, \ldots, i_k\}$ is a subset of cardinality $k \geq n - t$. Again by the above, there is a linear combination of the rows of the matrix

$$
\begin{pmatrix} 1 & \alpha_{i_1} & \alpha_{i_1}^2 & \cdots & \alpha_{i_1}^{2t} \\ 1 & \alpha_{i_2} & \alpha_{i_2}^2 & \cdots & \alpha_{i_2}^{2t} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{i_k} & \alpha_{i_k}^2 & \cdots & \alpha_{i_k}^{2t} \end{pmatrix}
$$

which yields $(1, 0, \ldots, 0)$. In other words, there exist $d_{i_1}, \ldots, d_{i_k} \in \mathbb{L}$ such that $\sum_{j=1}^k d_{i_j}(1, \alpha_{i_j}, \alpha_{i_j}^2, \ldots, \alpha_{i_j}^{2t}) = (1, 0, \ldots, 0)$. Let $D_{\overline{A}} \in \mathbb{L}^{k \times k}$ be the diagonal matrix $D_{\overline{A}} = \text{diag}\,(d_{i_1}, \ldots, d_{i_k})$. Then

$$
M_{\overline{A}}^T D_{\overline{A}} M_{\overline{A}} = \sum_{j=1}^k d_{i_j} \begin{pmatrix} 1 & \alpha_{i_j} & \cdots & \alpha_{i_j}^t \\ \alpha_{i_j} & \alpha_{i_j}^2 & \cdots & \alpha_{i_j}^{t+1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{i_j}^t & \alpha_{i_j}^{t+1} & \cdots & \alpha_{i_j}^{2t} \end{pmatrix} = \boldsymbol{a}\boldsymbol{a}^T.
$$

■

Theorem 5.5.6 only applies to n-interpolation friendly rings $\mathbb{L}$. We will now consider the applicability of the theorem to rings $\mathbb{L} = \mathbb{Z}_{p_1^{k_1} \ldots p_l^{k_l}}$ with p_i prime and $k_i \in \mathbb{N}_0$ for $1 \leq i \leq l$.

Lemma 5.5.7 *Let p be a prime. Theorem 5.5.6 applies to $\mathbb{L} = \mathbb{Z}_p$ if and only if $n < p$.*

Proof. If $\mathbb{L} = \mathbb{Z}_p$ for some prime p, then $\mathbb{L}$ is a field. Any non-zero element in a field is invertible. There are precisely $|\mathbb{L}| - 1 = p - 1$ such elements. For any two distinct non-zero elements a and b, $a - b \not\equiv 0$, which is equivalent to $a - b$ being invertible. Thus, $\mathbb{L} = \mathbb{Z}_p$ is n-interpolation friendly if and only if $n < p$. ■

Lemma 5.5.8 *Let p be a prime, and let $k \in \mathbb{N}$. Theorem 5.5.6 applies to $\mathbb{L} = \mathbb{Z}_{p^k}$ if and only if $n < p$.*

Proof. An element $a \in \mathbb{Z}_{p^k}$ is invertible in $(\mathbb{Z}_{p^k}, \cdot)$ if and only if $a \not\equiv 0 \bmod p$. There are $p^k - p^{k-1}$ such elements. Let b and c be two of them. Then $b - c$ is invertible in $(\mathbb{Z}_{p^k}, \cdot)$ if and only if $b - c \not\equiv 0 \bmod p$, which is equivalent to $b \not\equiv c \bmod p$. Note that $b \bmod p, c \bmod p \in \{1, \ldots, p-1\}$. Thus, $\mathbb{L} = \mathbb{Z}_{p^k}$ is n-interpolation friendly if and only if $n < p$. ■

Lemma 5.5.9 *Let p and q be two primes, $p \neq q$. Theorem 5.5.6 applies to $\mathbb{L} = \mathbb{Z}_{pq}$ if and only if $n < \min\{p, q\}$.*

Proof. An element $a \in \mathbb{Z}_{pq}$ is invertible in $(\mathbb{Z}_{pq}, \cdot)$ if and only if $a \not\equiv 0 \bmod p$ and $a \not\equiv 0 \bmod q$. There are $(p-1)(q-1)$ such elements. Let b and c be two of them. Then $b - c$ is invertible in $(\mathbb{Z}_{pq}, \cdot)$ if and only if $b - c \not\equiv 0 \bmod p$ and $b - c \not\equiv 0 \bmod q$, which is equivalent to $b \not\equiv c \bmod p$ and $b \not\equiv c \bmod q$. Note that $b \bmod p, c \bmod p \in \{1, \ldots, p-1\}$, and that $b \bmod q, c \bmod q \in \{1, \ldots, q-1\}$. Thus, $\mathbb{Z}_{pq}$ is n-interpolation friendly if and only if $n < \min\{p, q\}$. ■

In general, Theorem 5.5.6 applies to the ring $\mathbb{L} = \mathbb{Z}_{p_1^{k_1} \cdots p_l^{k_l}}$ with p_i prime and $k_i \in \mathbb{N}_0$ for $1 \leq i \leq l$ if and only if $n < \min\{p_1, \ldots, p_l\}$. In particular, the theorem does not apply to the ring $\mathbb{L} = \mathbb{Z}_{2^k}$.

Theorem 5.5.6 only proves the existence of a $(t+1)$-out-of-n threshold LSSS based on polynomial interpolation for the threshold access structure $\Gamma_{t,n}$. We will now prove that any n-out-of-n threshold LSSS over an n-interpolation friendly ring $\mathbb{L}$ for $\Gamma_{t,n}$ is based on polynomial interpolation.

Lemma 5.5.10 *Let $\Gamma_{t,n}$ be a threshold access structure with $n = t + 1$, and let $\mathbb{L}$ be an n-interpolation friendly ring. Let a $(t+1)$-out-of-n LSSS $\mathcal{S}$ over $\mathbb{L}$ for $\Gamma_{t,n}$ be defined by $\boldsymbol{s} = M\boldsymbol{b}$, with $M = (\boldsymbol{m}||M') \in \mathbb{L}^{n \times e}$ and $\boldsymbol{b} = (s||\boldsymbol{b'}) \in \mathbb{L}^e$. Then $\mathcal{S}$ is based on polynomial interpolation.*

Proof. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{L}$ be such that $\alpha_i - \alpha_j$ is invertible for all $i \neq j$, $1 \leq i, j \leq n$. Let V be the $n \times n$ Vandermonde matrix $V = V(\alpha_1, \ldots, \alpha_n)$.

Then, V is invertible with inverse V^{-1}. Define $F = V^{-1}M$. $\mathcal{S}$ is based on polynomial interpolation with $M = VF$. ■

Let $\mathcal{S}$, defined by $\boldsymbol{s} = M\boldsymbol{b}$, with $M = (\boldsymbol{m}||M') \in \mathbb{L}^{n\times(t+1)}$ and $\boldsymbol{b} = (s||\boldsymbol{b'}) \in \mathbb{L}^{t+1}$, be a $(t+1)$-out-of-n threshold LSSS over a ring $\mathbb{L}$ that is based on polynomial interpolation with $M = VF$. Let $\boldsymbol{r}$ be a reconstruction vector for $\mathcal{S}$. Then $s = \boldsymbol{r}\cdot\boldsymbol{s} = \boldsymbol{r}\cdot(M\boldsymbol{b}) = \boldsymbol{r}\cdot(VF\boldsymbol{b})$. Let $\mathcal{S}_V$ be the LSSS defined by $\boldsymbol{s} = V\boldsymbol{b}$. If $n = t+1$, there is, by Lemma 3.3.2, precisely one reconstruction vector $\boldsymbol{r_V}$ for $\mathcal{S}_V$ and precisely one reconstruction vector $\boldsymbol{r}$ for $\mathcal{S}$. Note that if $n = t+1$, V is invertible, and $\boldsymbol{b} = V^{-1}V\boldsymbol{b} = V^{-1}\boldsymbol{s}$. Hence, $\boldsymbol{r_V} = (V^{-1})_1$, where $(V^{-1})_1$ denotes the first row of the matrix V^{-1}. Further, note that $\boldsymbol{b} = F^{-1}V^{-1}VF\boldsymbol{b} = F^{-1}V^{-1}\boldsymbol{s}$. Hence, $\boldsymbol{r} = f_{11}^{-1}(V^{-1})_1 + \cdots + f_{1t+1}^{-1}(V^{-1})_{t+1}$, where f_{ij}^{-1} denotes the ijth element of the matrix F^{-1}, and $(V^{-1})_i$ denotes the ith row of the matrix V^{-1}. Note that $\boldsymbol{r} = \boldsymbol{r_V}$ if $F_1 = (1, 0, \ldots, 0)$.

Lemma 5.5.11 *Let $\mathcal{S}_M = (\mathbb{L}, M)$ be a $(t+1)$-out-of-n threshold LSSS with share distribution matrix $M \in \mathbb{L}^{n\times(t+1)}$ over a ring $\mathbb{L}$. If $\mathcal{S}_M$ is based on polynomial interpolation then $\mathbf{1} \in \mathbb{S}_M$.*

Proof. If $\mathcal{S}_M$ is based on polynomial interpolation then by Lemma 5.5.3, there exist an $n \times (t+1)$ Vandermonde matrix V and a $(t+1)\times(t+1)$ invertible matrix F such that $M = VF$. Clearly, $V \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}^T = \mathbf{1}$. Let $\boldsymbol{z} = F^{-1}\begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}^T$. Then $M\boldsymbol{z} = VFF^{-1}\begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}^T = V\begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}^T = \mathbf{1}$. This proves that $\mathbf{1} \in \mathbb{S}_M$. ■

Note that in general, the converse of 5.5.11 is not true: if $\mathbf{1} \in \mathbb{S}_M$, where $\mathbb{S}_M$ is a $(t+1)$-out-of-n threshold LSSS, then $\mathbb{S}_M$ is not necessarily based on polynomial interpolation.

Example 5.5.12 Let $\mathbb{K} = \mathbb{Z}_7$, let $t = 2$, and let $n = 5$. Let $\mathcal{S}_M$ be the 3-out-of-5 threshold LSSS with share distribution matrix

$$M = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 2 & 5 \end{pmatrix}.$$

Then clearly $\mathbf{1} \in \mathbb{S}_M$, but $\mathcal{S}_M$ is not based on polynomial interpolation.

Lemma 5.5.13 *Let $\mathcal{S}_M = (\mathbb{K}, M)$ be a $(t+1)$-out-of-n threshold LSSS with share distribution matrix $M \in \mathbb{K}^{n\times(t+1)}$ over a field $\mathbb{K}$. If $\mathcal{S}_M$ is based on polynomial interpolation with $M = VF$ then $F^1 = \begin{pmatrix} \frac{1}{c} & 0 & \cdots & 0 \end{pmatrix}^T$ if $\mathbf{1} \in \mathsf{Share}_{\mathcal{S}_M}(c)$ for $c \neq 0$, and $F^2 = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}^T$ if $\mathbf{1} \in \mathsf{Share}_{\mathcal{S}_M}(0)$.*

Proof. By Lemma 5.5.11, $\mathbf{1} \in \mathsf{Share}_{\mathcal{S}_M}(c)$ for some $c \in \mathbb{L}$. First suppose that $c \neq 0$. Let $\boldsymbol{z}$ be such that $M\boldsymbol{z} = \mathbf{1}$, and let $\boldsymbol{z'} = \frac{1}{c}\boldsymbol{z}$. Then $\frac{1}{c}\mathbf{1} = M\boldsymbol{z'} \in \mathsf{Share}_{\mathcal{S}_M}(1)$. Wlog $M^1 = \frac{1}{c}\mathbf{1} = \frac{1}{c}V^1$. Note that $\frac{1}{c}V^1 = M^1 = f_{11}V^1 + f_{21}V^2 + \cdots + f_{t+11}V^{t+1}$. By the linear independence of $V^1, \ldots, V^{t+1}$, $f_{11} = \frac{1}{c}, f_{21} = 0, \ldots, f_{t+11} = 0$. Suppose now that $c = 0$. Then wlog $M^2 = \mathbf{1}$. Note that $V^1 = M^2 = f_{12}V^1 + f_{22}V^2 + \cdots + f_{t+12}V^{t+1}$. By the linear independence of $V^1, \ldots, V^{t+1}$, $f_{12} = 1, f_{22} = 0, \ldots, f_{t+12} = 0$. ■

Lemma 5.5.14 *Let $\mathcal{S}_M = (\mathbb{K}, M)$ be a $(t+1)$-out-of-n threshold LSSS with share distribution matrix $M \in \mathbb{K}^{n\times(t+1)}$ over a field $\mathbb{K}$. If there exists a Vandermonde matrix $V \in \mathbb{K}^{n\times t+1}$ such that $\mathcal{R}(\mathcal{S}_M) = c\mathcal{R}(\mathcal{S}_V)$ for some $c \neq 0$ then $\mathcal{S}_M$ is based on polynomial interpolation.*

Proof. Note that $c\mathcal{R}(\mathcal{S}_V) = \mathcal{R}(\mathcal{S}_{\frac{1}{c}V})$. Hence, by Lemma 3.3.4, $\mathcal{R}(\mathcal{S}_M) = c\mathcal{R}(\mathcal{S}_V)$ if and only if there exists an invertible matrix $C \in \mathbb{K}^{(t+1)\times(t+1)}$ with $C_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$ such that $M = \frac{1}{c}VC$. Clearly, $\frac{1}{c}VC = V\frac{1}{c}C$. Let $F = \frac{1}{c}C$. Then $M = VF$, and by Lemma 5.5.3, $\mathcal{S}_M$ is based on polynomial interpolation. ■

Lemma 5.5.15 *Let $\mathbb{L}$ be a commutative ring, and and let a (t+1)-out-of-n threshold LSSS $\mathcal{S}_M$ be defined by $\boldsymbol{s} = M\boldsymbol{b}$ with $M \in \mathbb{L}^{n\times t+1}$. If $\mathcal{S}_M$ is based on polynomial interpolation with f such that $f(0) = s$ then $\mathbf{1} \in \mathsf{Share}_{\mathcal{S}_M}(1)$.*

Proof. By Lemma 5.5.4, $\mathcal{S}_M$ is based on polynomial interpolation with f such that $f(0) = s$ if and only if there exist a Vandermonde matrix $V \in \mathbb{L}^{n\times(t+1)}$ and an invertible matrix $F \in \mathbb{K}^{(t+1)\times(t+1)}$ with $F_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$ such that $M = VF$. Clearly, $\mathbf{1} \in \mathsf{Share}_{\mathcal{S}_V}(1)$. Hence there exists a vector $\boldsymbol{z} \in \mathbb{L}^{t+1}$ such that $V\boldsymbol{z} = \mathbf{1}$. Let $\boldsymbol{z'} = F^{-1}\boldsymbol{z}$. Then $M\boldsymbol{z'} = VFF^{-1}\boldsymbol{z} = \mathbf{1}$. Note that if $F_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$ then $F_1^{-1} = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$. Hence, $z'_1 = z_1 = 1$, and hence, $\mathbf{1} \in \mathsf{Share}_{\mathcal{S}_M}(1)$. ■

The following is a corollary of Lemma 5.5.15 and Corollary 4.1.12.

Corollary 5.5.16 *Let $\mathcal{S}$ be a $(t+1)$-out-of-n threshold LSSS over a commutative ring $\mathbb{L}$. If $\mathcal{S}$ is based on polynomial interpolation with f such that $f(0) = s$ then $\mathcal{S}$ is homomorphic.*

2-out-of-n threshold linear secret sharing schemes

The following is a corollary of Lemma 5.5.4.

Corollary 5.5.17 *Let $\mathbb{L}$ be a finite commutative ring, and let a 2-out-of-n threshold LSSS $\mathcal{S}$ be defined by $\boldsymbol{s} = M\boldsymbol{b}$ with $M \in \mathbb{L}^{n\times 2}$. Then there exists a polynomial f of degree 1 such that $\mathcal{S}$ is based on polynomial interpolation with f and $f(0) = s$ if and only if $M = VF$ for an $n \times 2$ Vandermonde matrix V and a 2×2-matrix F given by*

$$F = \begin{pmatrix} 1 & 0 \\ f_{21} & f_{22} \end{pmatrix}$$

for some $f_{21}, f_{22} \in \mathbb{L}$, with f_{22} invertible.

In general, V and F are not unique. In particular, there may exist V and F such that $s = f(0)$, and V' and F' such that $s \neq f'(0)$.

Example 5.5.18 Let $\mathbb{K} = \mathbb{Z}_5$, and let

$$M = \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 3 \end{pmatrix}.$$

Let $\mathcal{S}_M$ be the 2-out-of-3 threshold LSSS with share distribution matrix M. Then $\mathcal{S}_M$ is based on polynomial interpolation with $V = V(1, 2, 3)$ and $F = I$, and $\mathcal{S}_M$ is based on polynomial interpolation with $V = V(4, 1, 3)$ and

$$F = \begin{pmatrix} 1 & 4 \\ 0 & 3 \end{pmatrix}.$$

Lemma 5.5.19 below allows us to deduce from any pair (V, F) whether there exists a pair (V', F') such that $s = f'(0)$.

Lemma 5.5.19 *Let $\mathbb{L}$ be a finite commutative ring with $ZD(\mathbb{L}) < n - 1$, and let a 2-out-of-n threshold LSSS $\mathcal{S}$ be defined by $\boldsymbol{s} = M\boldsymbol{b}$ with $M \in \mathbb{L}^{n\times 2}$. Let $\mathcal{S}$ be based on polynomial interpolation with $M = VF$ for some Vandermonde matrix $V \in \mathbb{L}^{n\times 2}$ and an invertible matrix $F \in \mathbb{L}^{2\times 2}$. Then there exist a Vandermonde matrix $V' \in \mathbb{L}^{2\times n}$ and an invertible matrix $F' \in \mathbb{L}^{2\times 2}$ with $f'_{11} = 1$ and $f'_{12} = 0$ such that $\mathcal{S}$ is based on polynomial interpolation with $M = V'F'$ if and only if there exists $y \in \mathbb{L}$ such that $f_{11} = 1 + f_{12}y$ and $f_{21} = f_{22}y$.*

Proof. First we prove that if there exist a Vandermonde matrix $V' \in \mathbb{L}^{2\times n}$ and an invertible matrix $F' \in \mathbb{L}^{2\times 2}$ with $f'_{11} = 1$ and $f'_{12} = 0$ such that $\mathcal{S}$ is based on polynomial interpolation with $M = V'F'$ then there exists $y \in \mathbb{L}$ such that $f_{11} = 1 + f_{12}y$ and $f_{21} = f_{22}y$.

Note that $V' = VFF'^{-1}$. Let V be given by $V = V(\alpha_1, \ldots, \alpha_n)$. Then

$$V' = \begin{pmatrix} 1 & \alpha_1 \\ 1 & \alpha_2 \\ \vdots & \vdots \\ 1 & \alpha_n \end{pmatrix} \begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -f'_{21}{f'_{22}}^{-1} & {f'_{22}}^{-1} \end{pmatrix}$$

$$= \begin{pmatrix} f_{11} - f_{12}f'_{21}{f'_{22}}^{-1} + \alpha_1(f_{21} - f_{22}f'_{21}{f'_{22}}^{-1}) & f_{12}{f'_{22}}^{-1} + \alpha_1 f_{22}{f'_{22}}^{-1} \\ f_{11} - f_{12}f'_{21}{f'_{22}}^{-1} + \alpha_2(f_{21} - f_{22}f'_{21}{f'_{22}}^{-1}) & f_{12}{f'_{22}}^{-1} + \alpha_2 f_{22}{f'_{22}}^{-1} \\ \vdots & \vdots \\ f_{11} - f_{12}f'_{21}{f'_{22}}^{-1} + \alpha_n(f_{21} - f_{22}f'_{21}{f'_{22}}^{-1}) & f_{12}{f'_{22}}^{-1} + \alpha_n f_{22}{f'_{22}}^{-1} \end{pmatrix}.$$

Let $y = f'_{21}{f'_{22}}^{-1}$. Then we have, by the definition of a Vandermonde matrix, $f_{11} - f_{12}y + \alpha_i(f_{21} - f_{22}y) = 1$ for all $1 \leq i \leq n$. Note that $\alpha_i \neq \alpha_j$ for all $i \neq j$, and that hence at least two of the α_i are not zero divisors, and invertible by Fact 2.1.19. Hence, $f_{11} = 1 + f_{12}y$ and $f_{21} = f_{22}y$.

We now prove that if there exists $y \in \mathbb{L}$ such that $f_{11} = 1 + f_{12}y$ and $f_{21} = f_{22}y$, then there exist a Vandermonde matrix $V' \in \mathbb{L}^{2\times n}$ and an invertible matrix $F' \in \mathbb{L}^{2\times 2}$ with $f'_{11} = 1$ and $f'_{12} = 0$ such that $\mathcal{S}$ is based on polynomial interpolation with $M = V'F'$.

Define a 2×2 matrix F' by

$$F' = \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}.$$

Let V be given by $V = V(\alpha_1, \ldots, \alpha_n)$, and define an $n \times 2$ matrix V' by

$$V' = \begin{pmatrix} 1 & f_{12} + \alpha_1 f_{22} \\ 1 & f_{12} + \alpha_2 f_{22} \\ \vdots & \vdots \\ 1 & f_{12} + \alpha_n f_{22} \end{pmatrix}.$$

Then

$$V'F' = \begin{pmatrix} 1 + (f_{12} + \alpha_1 f_{22})y & f_{12} + \alpha_1 f_{22} \\ 1 + (f_{12} + \alpha_2 f_{22})y & f_{12} + \alpha_1 f_{22} \\ \vdots & \vdots \\ 1 + (f_{12} + \alpha_n f_{22})y & f_{12} + \alpha_1 f_{22} \end{pmatrix} = VF = M.$$

Hence, $\mathcal{S}$ is based on polynomial interpolation with $M = V'F'$. ■

Example 5.5.20 Let $\mathbb{L} = \mathbb{Z}_5$. Let M be the 3×2 share distribution matrix

$$M = \begin{pmatrix} 1 & 2 \\ 2 & 3 \\ 3 & 4 \end{pmatrix}$$

from Example 4.1.7, and let $\mathcal{S}$ be the 2-out-of-3 threshold LSSS defined by $\boldsymbol{s} = M\boldsymbol{b}$. Then

$$M = \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

and $\mathcal{S}$ is based on polynomial interpolation with $f(x) = b_2 + (s + b_2)x$.

Here, $f_{11} = 0$, $f_{12} = 1$, $f_{21} = 1$, and $f_{22} = 1$. Note that $f_{11} = 1 + f_{12}y$ if and only if $y = 4$, and that $f_{21} = f_{22}y$ if and only if $y = 1$. Over $\mathbb{Z}_5$, such a y does not exist. By Lemma 5.5.19, there does therefore not exist a polynomial f' of degree 1 such that $\mathcal{S}$ is based on polynomial interpolation with f' and $f'(0) = s$.

Lemma 5.5.21 below allows us to deduce directly from the matrix M whether the 2-out-of-n threshold LSSS with share distribution matrix M is based on polynomial interpolation with f such that $s = f(0)$.

Lemma 5.5.21 *Let $\mathbb{L}$ be a commutative ring, and and let a 2-out-of-n threshold LSSS $\mathcal{S}$ be defined by $\boldsymbol{s} = M\boldsymbol{b}$ with $M \in \mathbb{L}^{n\times 2}$. Then there exists a polynomial f of degree 1 such that $f(0) = s$ and $\mathcal{S}$ is based on polynomial interpolation with f if and only if there exists $y \in \mathbb{L}$ such that $m_{i1} = 1 + m_{i2}y$ for all $1 \leq i \leq n$.*

Proof. If a 2-out-of-n threshold LSSS over $\mathbb{L}$ is based on polynomial interpolation with f, and $f(0) = s$, then by Lemmas 5.5.3 and 5.5.17, there exist a Vandermonde matrix $V = V(\alpha_1, \ldots, \alpha_n)$ and a 2×2 matrix

$$F = \begin{pmatrix} 1 & 0 \\ f_{21} & f_{22} \end{pmatrix}$$

with f_{22} invertible such that $M = VF$. For each i, $1 \leq i \leq n$, we thus have the system of linear equations

$$\begin{cases} m_{i1} = 1 + \alpha_i f_{21} \\ m_{i2} = \alpha_i f_{22} \end{cases}$$

Thus, by the invertability of f_{22}, $m_{i1} = 1 + m_{i2}f_{22}^{-1}f_{21}$ for all $1 \leq i \leq n$. Define $y = f_{22}^{-1}f_{21}$.

Conversely, if there exists $y \in \mathbb{L}$ such that $m_{i1} = 1 + m_{i2}y$ for all $1 \leq i \leq n$, then define

$$F = \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix},$$

and

$$V = \begin{pmatrix} 1 & m_{12} \\ 1 & m_{22} \\ \vdots & \vdots \\ 1 & m_{n2} \end{pmatrix}.$$

Then, V is a $2 \times n$ Vandermonde matrix, and $M = VF$. Hence, by Lemma 5.5.17, there exists a polynomial f of degree 1 such that $f(0) = s$ and $\mathcal{S}$ is based on polynomial interpolation with f. ■

Recall that the converse of Lemmas 5.5.11 and 5.5.15 does not hold for general $(t+1)$-out-of-n threshold linear secret sharing schemes. In the following two lemmas, we prove that the converse does hold for 2-out-of-n threshold LSSSs.

Lemma 5.5.22 *Let $\mathbb{K}$ be a finite field, and and let a 2-out-of-n threshold LSSS $\mathcal{S}_M$ be defined by $\boldsymbol{s} = M\boldsymbol{b}$ with $M \in \mathbb{K}^{n \times 2}$. Then $\mathcal{S}_M$ is based on polynomial interpolation if and only if $\mathbf{1} \in \mathbb{S}_M$.*

Proof. By Lemma 5.5.11, if $\mathcal{S}$ is based on polynomial interpolation then $\mathbf{1} \in \mathbb{S}$. Conversely, suppose that $\mathbf{1} \in \mathbb{S}$. First suppose that $\mathbf{1} \in \mathsf{Share}(c)$ for $c \neq 0$. Wlog,

$$M = \begin{pmatrix} \frac{1}{c} & m_{12} \\ \frac{1}{c} & m_{22} \\ \vdots & \vdots \\ \frac{1}{c} & m_{n2} \end{pmatrix}.$$

Hence, $M = VF$ with

$$V = \begin{pmatrix} 1 & m_{12} \\ 1 & m_{22} \\ \vdots & \vdots \\ 1 & m_{n2} \end{pmatrix}$$

and

$$F = \begin{pmatrix} \frac{1}{c} & 0 \\ 0 & 1 \end{pmatrix}.$$

Note that for $\mathcal{S}$ to be secure, $m_{2i} \neq m_{2j}$ for all $i \neq j$. Hence, V is a Vandermonde matrix, and by Lemma 5.5.3, $\mathcal{S}$ is based on polynomial interpolation. Now suppose that $\mathbf{1} \in \mathsf{Share}(0)$. Wlog,

$$M = \begin{pmatrix} m_{11} & 1 \\ m_{21} & 1 \\ \vdots & \vdots \\ m_{n1} & 1 \end{pmatrix}.$$

Hence, $M = VF$ with

$$V = \begin{pmatrix} 1 & m_{11} \\ 1 & m_{21} \\ \vdots & \vdots \\ 1 & m_{n1} \end{pmatrix}$$

and

$$F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Note that for $\mathcal{S}$ to be secure, $m_{1i} \neq m_{1j}$ for all $i \neq j$. Hence, V is a Vandermonde matrix, and by Lemma 5.5.3, $\mathcal{S}$ is based on polynomial interpolation. ■

Lemma 5.5.23 *Let $\mathbb{K}$ be a finite field, and and let a 2-out-of-n threshold LSSS $\mathcal{S}_M$ be defined by $\boldsymbol{s} = M\boldsymbol{b}$ with $M \in \mathbb{K}^{n\times 2}$. Then $\mathcal{S}_M$ is based on polynomial interpolation with f such that $f(0) = s$ if and only if $\mathbf{1} \in \mathsf{Share}_{\mathcal{S}_M}(1)$.*

Proof. If $\mathbf{1} \in \mathsf{Share}_{\mathcal{S}_M}(1)$ then

$$M = \begin{pmatrix} 1 & m_{12} \\ 1 & m_{22} \\ \vdots & \vdots \\ 1 & m_{n2} \end{pmatrix}.$$

Note that for $\mathcal{S}_M$ to be secure, $m_{2i} \neq m_{2j}$ for all $i \neq j$. Hence, $V = M$ is a Vandermonde matrix, and $M = VF$ with $V = M$ and $F = I$. Clearly, $\mathcal{S}_M$ is based on polynomial interpolation with $f(x) = s + b_2 x$ and $f(0) = s$.

Conversely, if $\mathcal{S}_M$ is based on polynomial interpolation with f such that $f(0) = s$ then by Lemma 5.5.15, $\mathbf{1} \in \mathsf{Share}_{\mathcal{S}_M}(1)$. ■

The following is a corollary of Corollary 5.5.16.

Corollary 5.5.24 *Let $\mathcal{S}$ be a 2-out-of-n threshold LSSS over a commutative ring $\mathbb{L}$. If $\mathcal{S}$ is based on polynomial interpolation with f such that $f(0) = s$ then $\mathcal{S}$ is homomorphic.*

Over $\mathbb{Z}_5$ and $\mathbb{Z}_7$, all 2-out-of-3 homomorphic threshold LSSSs are based on polynomial interpolation with f such that $f(0) = s$. We conjecture the following:

Conjecture 5.5.25 *Let $\mathcal{S}$ be a 2-out-of-n threshold LSSS over a commutative ring $\mathbb{L}$. If $\mathcal{S}$ homomorphic then $\mathcal{S}$ is based on polynomial interpolation with f such that $f(0) = s$.*

5.5.1 Algorithm: isShamir(M,$V[]$)

In this subsection, we present an algorithm to check whether a $t+1$-out-of-n threshold linear secret sharing scheme is based on polynomial interpolation. Let $\mathcal{S}_M = (\mathbb{K}, M)$ be a $t+1$-out-of-n threshold LSSS over a field $\mathbb{K}$ with share distribution matrix M. By Lemma 5.5.3, it suffices to check whether there exist an $n \times (t+1)$ Vandermonde matrix V and an invertible $(t+1) \times (t+1)$ matrix F such that $M = VF$. Naively, one could do the following:

Algorithm 9 isShamir(M,$V[]$)

for all $n \times (t+1)$ Vandermonde matrices V **do**
  for all $(t+1) \times (t+1)$ matrices F **do**
    if $M = VF$ **then**
      return true
    end if
  end for
end for
return false

Note that $M = VF$ only if the top $t+1$ rows of M are equal to the top $t+1$ rows of V multiplied by F. It suffices therefore to check for each V whether $M = VF$ with $F = V_{\{1,\ldots,t+1\}}^{-1} M_{\{1,\ldots,t+1\}}$:

Algorithm 10 isShamir(M,$V[]$)

for all $n \times (t+1)$ Vandermonde matrices V **do**
  $F \leftarrow V_{\{1,\ldots,t+1\}}^{-1} M_{\{1,\ldots,t+1\}}$
  if $M = VF$ **then**
    return true
  end if
end for
return false

The algorithm is implemented in the programs `MultThreshold2_3Shamir.java` for multiplicative 2-out-of-3 threshold LSSSs and `MultThreshold3_5Shamir.java` for multiplicative 3-out-of-5 threshold LSSSs. Both programs use the library `MultThresholdLib.java`.

Output of the program `MultThreshold2_3Shamir.java` for $\mathbb{Z}_5$ (runtime $<$ 1 min):

```
Enter n: 5
Number of 3x2 2-out-of-3 multiplicative threshold LSSSs over ZZ_5: 192
Number of 3x2 2-out-of-3 multiplicative threshold LSSSs based on
polynomial interpolation over ZZ_5: 36
Number of 3x2 2-out-of-3 homomorphic threshold LSSSs over ZZ_5: 6
Number of 3x2 2-out-of-3 homomorphic threshold LSSSs based on
polynomial interpolation over ZZ_5: 6
```

Output of the program `MultThreshold2_3Shamir.java` for $\mathbb{Z}_7$ (runtime $<$ 1 min):

```
Enter n: 7
Number of 3x2 2-out-of-3 multiplicative threshold LSSSs over ZZ_7: 1080
Number of 3x2 2-out-of-3 multiplicative threshold LSSSs based on
```

```
polynomial interpolation over ZZ_7: 150
Number of 3x2 2-out-of-3 homomorphic threshold LSSSs over ZZ_7: 20
Number of 3x2 2-out-of-3 homomorphic threshold LSSSs based on
polynomial interpolation over ZZ_7: 20
```

Output of the program `MultThreshold3_5Shamir.java` for $\mathbb{Z}_7$ (runtime = 2.5 hours):

```
Enter n: 7
Number of 5x3 3-out-of-5 multiplicative threshold LSSSs over ZZ_7: 418176
Number of 5x3 3-out-of-5 multiplicative threshold LSSSs based on
polynomial interpolation over ZZ_7: 524
Number of 5x3 3-out-of-5 homomorphic threshold LSSSs over ZZ_7: 1286
Number of 5x3 3-out-of-5 homomorphic threshold LSSSs based on
polynomial interpolation over ZZ_7: 68
```

5.6 Existence of other Multiplicative Threshold Linear Secret Sharing Schemes

The output of programs `MultThreshold2_3Shamir.java` and `MultThreshold3_5Shamir.java` shows that only a small fraction of multiplicative $(t+1)$-out-of-n threshold linear secret sharing schemes are based on polynomial interpolation.

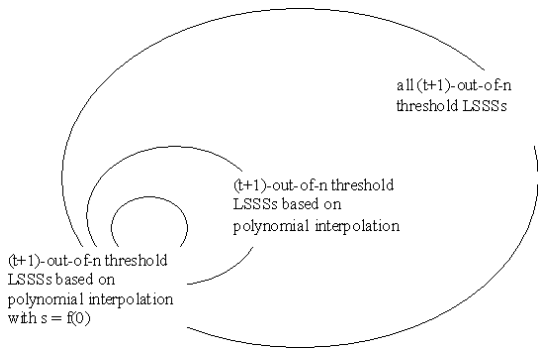

Figure 5.1: Venn diagram: $(t+1)$-out-of-n threshold LSSSs

Example 5.6.1 Let $\mathbb{K} = \mathbb{Z}_5$, and let M be the 3×2 share distribution matrix

$$M = \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 2 & 3 \end{pmatrix}.$$

Let $\mathcal{S}$ be the 2-out-of-3 threshold LSSS defined by $\boldsymbol{s} = M\boldsymbol{b}$. Note that $\mathcal{S}$ is not homomorphic. Here, $s_1 = s + b_2$, $s_2 = s + 2b_2$, and $s_3 = 2s + 3b_1$.

By Fact 2.6.5, for any $\alpha_1, \alpha_2 \in \mathbb{K}$, there exists an interpolation polynomial f of degree 1 such that $s_1 = f(\alpha_1)$ and $s_2 = f(\alpha_2)$. Further,

$$f(x) = (s + b_2)r_0(x) + (s + 2b_2)r_1(x),$$

where $r_0(x) = \frac{x-\alpha_2}{\alpha_1-\alpha_2}$, and $r_1(x) = \frac{x-\alpha_1}{\alpha_2-\alpha_1}$. Simplifying,

$$f(x) = s + \frac{b_2}{\alpha_1 - \alpha_2}(2\alpha_1 - \alpha_2 - x).$$

Clearly, for any $\alpha_3 \in \mathbb{K}$, $s_3 \neq f(\alpha_3)$.

Lemma 5.6.2 *Let $\mathbb{K}$ be a field, and and let a 2-out-of-n threshold LSSS $\mathcal{S}$ be defined by $\boldsymbol{s} = M\boldsymbol{b}$ with $M \in \mathbb{K}^{n\times 2}$. Then $\mathcal{S}$ is based on polynomial interpolation if and only if there exist $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ such that*

$$m_{i1} = \frac{1}{\alpha_1 - \alpha_2}(m_{11}(\alpha_i - \alpha_2) - m_{21}(\alpha_i - \alpha_1))$$

and

$$m_{i2} = \frac{1}{\alpha_1 - \alpha_2}(m_{12}(\alpha_i - \alpha_2) - m_{22}(\alpha_i - \alpha_1))$$

for all $3 \leq i \leq n$.

Proof. By Definition 5.5.1, $\mathcal{S}$ is based on polynomial interpolation if and only if there exist $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ such that $s_i = f(\alpha_i)$ for all $1 \leq i \leq n$. Note that $s_i = m_{i1}s + m_{i2}b_2$ for all $1 \leq i \leq n$. By Fact 2.6.5, for any $\alpha_1, \alpha_2 \in \mathbb{K}$, there exists an interpolation polynomial f of degree 1 such that $s_1 = f(\alpha_1)$ and $s_2 = f(\alpha_2)$. Further,

$$f(x) = (m_{11}s + m_{12}b_2)r_0(x) + (m_{21}s + m_{22}b_2)r_1(x),$$

where $r_0(x) = \frac{x-\alpha_2}{\alpha_1-\alpha_2}$, and $r_1(x) = \frac{x-\alpha_1}{\alpha_2-\alpha_1}$. Simplifying,

$$\begin{aligned} f(x) = &\frac{1}{\alpha_1 - \alpha_2}((m_{11} - m_{21})x + m_{21}\alpha_1 - m_{11}\alpha_2)s \\ &+ \frac{1}{\alpha_1 - \alpha_2}((m_{12} - m_{22})x + m_{22}\alpha_1 - m_{12}\alpha_2)b_2. \end{aligned}$$

Clearly, $f(\alpha_i) = s_i$ for $3 \leq i \leq n$ if and only if

$$m_{i1} = \frac{1}{\alpha_1 - \alpha_2}(m_{11}(\alpha_i - \alpha_2) - m_{21}(\alpha_i - \alpha_1))$$

and

$$m_{i2} = \frac{1}{\alpha_1 - \alpha_2}(m_{12}(\alpha_i - \alpha_2) - m_{22}(\alpha_i - \alpha_1)).$$

■

Chapter 6

Conclusion

In this thesis, we have explained the mathematical background of share computing protocols. In particular, we have explained linear secret sharing schemes over fields and rings. We have explained the characterisation of linear secret sharing schemes in terms of monotone span programs. Further, we have characterised linear secret sharing schemes in terms of projections. In particular, we have explained multiplicative linear secret sharing schemes. Most linear secret sharing schemes are defined over fields. One goal of this thesis was to generalise those definitions to rings where possible, and to prove the impossibility of this otherwise.

The platform SHAREMIND, a virtual machine for privacy-preserving data mining, is an example of an application that uses threshold linear secret sharing schemes. In fact, most practical applications use threshold linear secret sharing schemes. A goal of this thesis was to characterise threshold linear secret sharing schemes, and in particular, threshold linear secret sharing schemes with one share per miner. We have used this characterisation to develop an algorithm to generate all $(t+1)$-out-of-n threshold linear secret sharing schemes over a field $\mathbb{Z}_p$ for fixed n, t, and p. We have implemented this algorithm for $n = 5$ and $t = 2$, and for $n = 3$ and $t = 1$. One project for the future would be to implement the algorithm efficiently - the current implementation has a runtime of about 2.5 hours for 3-out-of-5 threshold linear secret sharing schemes over $\mathbb{Z}_7$.

SHAREMIND uses a 3-out-of-3 threshold linear secret sharing scheme over the ring $\mathbb{Z}_{2^{32}}$ with one share per miner. We have explained the proof of existence of $(t+1)$-out-of-n threshold linear secret sharing schemes over $\mathbb{Z}_{2^{32}}$ with more than one share per miner and have proved the non-existence of $(t+1)$-out-of-n threshold linear secret sharing schemes over $\mathbb{Z}_{2^{32}}$ with one share per miner.

Shamir's secret sharing scheme is the oldest $(t+1)$-out-of-n threshold linear secret sharing scheme over $\mathbb{Z}_p$ with one share per miner. Only a small fraction of threshold linear secret sharing schemes are generalised Shamir

secret sharing schemes. We have characterised those for 2-out-of-n threshold linear secret sharing schemes and have proved that this characterisation is not valid for general $(t+1)$-out-of-n threshold linear secret sharing schemes.

Ühissalastusskeemid üle korpuste ja ringide

Magistritöö (20 AP)

Katharina Kahrs

Resümee

Käesolev magistritöö käsitleb ühissalastusskeemide matemaatilisi aluseid. Töös pööratakse erilist tähelepanu üle korpuste ja ringide defineeritud lineaarsetele ühissalatusskeemidele. Esmalt kirjeldame lineaarsete ühissalastusskeemide ning monotoonsete maatriksprogrammide (*monotone span programs*) omavahelist vastavust. Järgnevalt kirjeldame lineaarseid ühissalastusskeeme projektsioonide terminites. Sealjuures pöörame erilist tähelepanu multiplikatiivsetele lineaarsetele ühissalastusskeemidele. Kuna enamik lineaarsetest ühissalastusskeemidest on defineeritud üle korpuste, siis käesoleva magistritöö üheks eesmärgiks on võimaluse korral nende definitsioonide üldistamine ringidele või siis selliste kontruktsioonide võimatuse tõestamine.

Enamik praktilistest rakendustest kasutab lineaarseid lävisalastusskeeme. Konkreetseks näiteks võib tuua privaatsust säilitava andmekaeve platvormi Sharemind. Teiseks käesoleva magistritöö eesmärgiks ongi selliste lävisalastusskeemide kirjeldamine. Eriti pöörame tähelepanu ühissalastusskeemidele, milles iga osapool saab ühe andmeosaku. Vastavaid kirjeldusi kasutasime algoritmi loomiseks, mis genereerib kõik lineaarsed (n, t)-lävisalastusskeemid üle korpuse $\mathbb{Z}_p$ fikseeritud parameetrite n, t ja p jaoks. Oleme realiseerinud selle algoritmi parameetrite $n = 5$ ja $t = 3$ ja $n = 3$ ja $t = 2$ jaoks. Tulevikus on plaanis oluliselt suurendada algoritmi efektiivsust: käesoleval realisatsioonil kulub umbes 2,5 tundi kõikide lineaarsete $(5, 3)$-lävisalastusskeemide leidmiseks üle $\mathbb{Z}_7$.

Kuna Sharemind kasutab ühissalastusskeemi, mis on defineeritud üle ringi $\mathbb{Z}_{2^{32}}$ ning toimib ainult kolme osapoole korral, siis vaatlesime töös üldiste multiplikatiivsete n osapoolega lävisalastusskeemide olemasolu ja konstruktsioone. Täpsemalt näitasime, et üle $\mathbb{Z}_{2^{32}}$ ei eksiteeri (n, t)-lävisalastusskeeme, kus iga osapool saab ühe osaku.

Shamiri ühissalastusskeem on kõige vanem lineaarne (n, t)-lävisalastusskeem üle $\mathbb{Z}_p$, kus iga osapool saab ühe osaku. Ainult väike murdosa lävisalastusskeemidest on Shamiri ühissalastusskeemid. Töös kirjeldame kõiki selliste $(n, 2)$-lävisalastusskeeme. See kirjeldus tugineb $(n, 2)$-lävisalastusskeemide lihtsal ehitusel. Näitame, et sama kirjeldus ei käi (n, t)- lävisalastusskeemide kohta, mille ehitus on üldjuhul oluliselt keerulisem.

Autor soovib tänada oma juhendajat, kelle entusiasm ja põhjalikkus olid väärtuslikuks panuseks käesoleva magistritöö valmisel.

Bibliography

[1] Z. Beerliova-Trubiniova, M. Hirt. *Perfectly-Secure MPC with Linear Communication Complexity*. Theory of Cryptography, LNCS, vol. 4948/2008, Springer, 2008.

[2] A. Beimel, E. Weinreb. *Separating the power of monotone span programs over different fields*. SIAM journal on computing, vol. 34, no. 5, pp. 1196-1215, 2005.

[3] J. C. Benaloh, J. Leichter. *Generalized Secret Sharing and Monotone Functions*. Advances in Cryptology - CRYPTO '88, LNCS, vol. 403, Springer, 1990.

[4] G. Blakley. *Safeguarding cryptographic keys*. Proc. AFIPS 1979 National Computer Conference, New York, pp. 313-317, June 1979.

[5] D. Bogdanov, S. Laur, J. Willemson. *Sharemind: a framework for fast privacy-preserving computations*. Proceedings of the 13th European Symposium on Research in Computer Security, ESORICS 2008, LNCS, vol. 5283, pp. 192-206, Springer, Heidelberg, 2008

[6] D. Chaum, C. Crépeau, I. Damgård. *Multiparty unconditionally secure protocols*. Proceedings of the 20th Annual ACM Symposium on Theory of Computing, pp. 11-19, ACM, 1988.

[7] R. Cramer, I. Damgård, Y. Ishai. *Share Conversion, Pseudorandom Secret-Sharing and Applications to Secure Computation*. Proceedings of the Second Theory of Cryptography Conference, pp. 342-362, Springer, 2005.

[8] R. Cramer, I. Damgård, U. Maurer. *General Secure Multi-Party Computation from any Linear Secret Sharing Scheme*. B. Preneel (Ed.), Advances in Cryptology–EUROCRYPT 2000, LNCS, vol. 1807, pp. 316-334, Springer, Berlin, 2000.

[9] R. Cramer, I. Damgård, U. Maurer. *Span Programs and General Secure Multi-Party Computation*. BRICS RS-97-28.

[10] R. Cramer, S. Fehr. *Optimal Black-Box Secret Sharing over Arbitrary Abelian Groups*. Proceedings of the 22nd Annual IACR CRYPTO, LNCS, vol. 2442, pp. 272-287, Springer, August 2002.

[11] R. Cramer, S. Fehr, Y. Ishai, E. Kushilevitz. *Efficient Multi-Party Computation over Rings*. Proceedings of the 22nd Annual IACR EUROCRYPT, LNCS, vol. 2656, pp. 596-613, Springer, May 2003.

[12] Y. Frankel, Y. Desmedt. *Classification of ideal homomorphic threshold schemes over finite abelian groups*. Advances in Cryptology – EUROCRYPT '92, LNCS, vol. 658, pp. 25-34, Springer, 1993.

[13] S. Fehr. *Efficient construction of dual MSP*. Manuscript 1999.

[14] A. Gal. *Combinatorial methods in Boolean function complexity*. PhD-thesis, University of Chicago, 1995.

[15] M. Hirt, U. Maurer. *Complete characterization of adversaries tolerable in secure multi-party computation* (extended abstract). Proc. of 16th PODC, pp. 25-34, 1997.

[16] M. Karchmer, A. Widgerson. *On Span Programs*. Proc. of Structure in Complexity'93.

[17] A. Shamir. *How to share a secret*. Comm. ACM 22, 11, pp. 612-613, November 1979.

[18] A. C. Yao. *Protocols for secure computations* (extended abstract). Proc. IEEE Symp. on Foundations of Computer Science, pp. 160-164, 1982.