MASTER THESIS

Nexuses of Uniforms: A Family of Uniform Hypergraphs Representing Ideal Access Structures

Sascha Hoppler

Supervised by:
Prof. Dr. Joachim Rosenthal

Co-Supervised by:
Simran Tinani

Department of Mathematics
University of Zurich

March 2, 2022

Abstract

Secret sharing is a cryptographical tool to split a piece of information called secret among several participants such that only certain qualified subsets of them can reconstruct the initial secret, while every other set of participants has no information about it. The collection of qualified sets, called access structure, can be uniquely described by hypergraphs, where the vertices and hyperedges correspond to the participants and the minimal sets in the access structure, respectively. An access structure is called ideal if it can be realized in a way that the size of each share is the same as the size of the secret, and a hypergraph is called ideal if it represents an ideal access structure.

In this thesis we focus on the problem of determining which connected uniform hypergraphs, i.e. hypergraphs where each hyperedge has the same size, are ideal. While for graphs it is known that they are ideal if and only if they are complete multipartite, a similar result has not yet been given for other uniform hypergraphs. We introduce a new operation for hypergraphs called region-expansion and with its help define the nexuses of uniforms, a family of ideal k-uniform hypergraphs. While in the 2-uniform case the nexuses of uniforms correspond exactly to the set of all ideal graphs, in the k-uniform case for $k > 2$ there are still hypergraphs which neither belong to this new family nor have they been shown to be non-ideal. We discuss in detail the case when $k = 3$ and provide the only two such hypergraphs on at most five vertices which are not yet characterized. They can serve as a basis for further work on a complete characterization of all ideal 3-uniform hypergraphs.

Acknowledgements

First, let me thank my supervisor Prof. Dr. Joachim Rosenthal for giving me the opportunity to write my master thesis in the field of cryptography and especially for giving me the freedom to write it about a topic which is not that tightly connected to his usual research areas. Also, I would like to thank him for his commitment in all his courses I have visited, from basic linear algebra up to more involved cryptography.
I would also like to thank Simran Tinani who has always supported me during the whole process of the thesis. I am sincerely grateful for all her inputs and her commitment, even though it was a new area for her as well.

From a personal point of view, I want to thank my fellow students, especially to everyone who accompanied me since the beginning and I still consider good friends. I feel lucky to have met them, for the mutual support during our studies on the one hand, but most important for our personal relationships.
Last but not least a huge thank you goes to my family who has never failed to support and encourage me during my studies, but especially have always been there for me in difficult times outside of the university. I am sincerely grateful for having such a great family.

Contents

1 Introduction **1**

2 Preliminaries **4**
2.1 Matroids 4
2.2 Hypergraphs 6
2.2.1 Basic Definitions and Concepts 6
2.2.2 Special Types of Hypergraphs 8
2.2.3 Independence, Vertex Covers and Regions 10

3 Introduction to Secret Sharing **12**
3.1 Basics of Secret Sharing 12
3.1.1 Access Structures and Secret Sharing Schemes 13
3.1.2 Ideal Secret Sharing 16
3.1.3 Linear and Multi-Linear Secret Sharing 17
3.2 Threshold Access Structures 18
3.3 Secret Sharing and Matroids 21
3.3.1 Matroid Ports, Access Structures and Minors 21
3.3.2 Idealness of Access Structure Minors 22
3.3.3 A Forbidden Minor Characterization 24
3.4 Secret Sharing and Hypergraphs 25
3.4.1 Hypergraph Minors and Idealness 25
3.4.2 Ideal Graph-Based Access Structures 29

4 Constructing Ideal Uniform Hypergraphs **33**
4.1 The Region-Expansion Operation 33
4.1.1 Definition and Basic Properties 33
4.1.2 Region-Expansion and Idealness 37
4.2 Simple Nexuses of Uniforms 41
4.2.1 Definition and Basic Properties 41
4.2.2 Idealness and Related Properties 42
4.3 Nexuses of Uniforms 45

5 On Ideal 3-Uniform Hypergraphs **49**
5.1 3-Uniform Nexuses of Uniforms 49
5.2 Ideal 3-Uniform Hyperstars 54
5.3 3-Uniform Ideal Region-Expansions 56
5.4 Counting 3-Uniform Hypergraphs 63
5.4.1 General 3-Uniform Hypergraphs 64
5.4.2 3-Uniform Hypergraphs on at Most Five Vertices 67

6 Discussion **69**
6.1 Summary 69
6.2 Open Problems 70

A Algorithms **71**
A.1 Ideal Graphs 71
A.2 Ideal 3-Uniform Hyperstars 72
A.3 3-Uniform Nexuses of Uniforms 73
A.3.1 Finding Candidates for Independent Vertex Sets 74
A.3.2 Complete Multipartite 3-uniform Hypergraphs 75
A.3.3 3-uniform Simple Nexuses of Uniforms 76

Bibliography **79**

Chapter 1

Introduction

The theory of secret sharing originated in 1979 when Shamir [4] and Blakley [3] independently introduced a solution for the same problem: how to share a piece of information between a set of participants such that at least a fixed number of them is needed to recreate the original information, while smaller sets of participants have no information about it. Having these *threshold schemes* as a starting point, the field of secret sharing has grown since and has also affected cryptography in the sense that it is used for multiparty computation protocols [15], access control [13, 30] and other subdisciplines.

In order to handle more complex situations than threshold schemes, the term of *access structures* has been established which is a monotone collection of sets of participants which shall be able to reveal the original information, often called *secret*, whereas sets which are not in this collection shall not gain any information even when they share their knowledge. We call the sets in the access structure *qualified*, while all other sets are called *unqualified*.

A *secret sharing scheme* realizing a given access structure is a method by which a secret is shared among the participants in a way the above mentioned conditions for that particular access structure are fulfilled. The pieces of information each participant gets are called *shares*. All parameters of the scheme except for some random elements are usually public. Hence, everybody knows how the shares are computed and how qualified sets can recompute the original information. However, because of these random elements in the computation of the shares, still only qualified sets can reveal the secret, whereas unqualified sets cannot.

Like for most protocols with real-world applications, also secret sharing schemes should fulfil certain condition in order that a practical usage is possible. First, computing the shares from the secret as well as computing the secret from the shares of a qualified set should not be too complex. And second, the sizes of the shares shall not be too large compared to the size of the secret. The first condition is apprehended for instance by *linear* and *multi-linear* schemes, where the computations are linear maps. For the sizes of the shares, a measurement called *information ratio* has been established which expresses the ratio of the size of the domains of shares with respect to the size of the domain of secrets. If, in particular, the sizes of those domains are equal, i.e. each share contains

the same amount of information like the secret, then a secret sharing scheme is called *ideal* which is the best possible case.

An access structure is said to be ideal if there exists an ideal secret sharing scheme realizing it. Idealness of access structures has been connected to the theory of *matroids* by Brickell and Davenport [18] in the sense that every ideal access structure is the *port* of a matroid. By a forbidden minor characterization [2], we can therefore identify non-ideal access structures. Unfortunately, there exist matroids whose ports are non-ideal access structures. Therefore, this characterization cannot be used to verify idealness.

In order to represent access structures in an easy way, we make use of *hypergraphs*. A hypergraph is a set of *vertices* V together with a family of non-empty subsets of V called *hyperedges*. While the vertices of a hypergraph can be seen as the participants, the hyperedges represent the minimal sets in the access structure. In this context, a hypergraph is said to be *linear* or *ideal* if the associated access structure can be realized by a linear or ideal secret sharing scheme respectively.

A hypergraph is called k-uniform if each of its hyperedges has size k. It has already been shown that in the special case of graphs, which are 2-uniform hypergraphs, the ideal connected graphs are exactly those which are complete multipartite, which is a special family of hypergraphs. While for $k > 2$ complete multipartite k-uniform hypergraphs are also ideal, this characterization is not complete, i.e. there exist ideal k-uniform hypergraphs which are not complete multipartite.

Ligeti [26] focused on 3-uniform hypergraphs and stated the following problem in the end of his paper:

Problem 1. *Give a characterization of the ideal 3-uniform hypergraph-based access structures, or at least the ideal 3-uniform hyperstars.*

In this master thesis we contribute to those questions for 3-uniform hypergraphs as well as for the general k-uniform case. We will answer the second part of Problem 1 by stating how, for a fixed $k \geq 2$, all ideal k-uniform hyperstars look like, given that we know all ideal k'-uniform hypergraphs for each $k' < k$. We will then give an explicit characterization of the ideal 3-uniform hyperstars.

In order to contribute to the first part of Problem 1, we will define an operation called *region-expansion* which combines two given hypergraphs, and use it to define two new families of ideal k-uniform hypergraphs. The first one is the family $\mathcal{L}^{(k)}$ which is called *simple nexuses of uniforms*, while the second one has the name *nexuses of uniforms* and is denoted by $\mathcal{N}^{(k)}$. We will show that $\mathcal{N}^{(k)}$ is the union of $\mathcal{L}^{(k)}$ and the set of complete multipartite k-uniform hypergraphs and is therefore a proper superset of the uniform hypergraphs which are trivially ideal.

In a further step, we will focus on the case where $k = 3$ and we will show that still there are 3-uniform hypergraphs which are not yet characterized, i.e. which neither have a forbidden minor nor are they nexuses of uniforms. In particular, we will provide the only two non-characterized hypergraphs (up to isomorphism) on at most five vertices, which can be taken as starting point for future work on that topic.

We start by giving a brief overview on the relevant theory of matroids and hypergraphs in Chapter 2.

Chapter 3 provides the basic concepts and known results about secret sharing, also in combination with matroids and hypergraphs.

In Chapter 4 we introduce the region-expansion operation (Section 4.1) as well as the simple nexuses of uniforms (Section 4.2) and nexuses of uniforms (Section 4.3) and we state our main results for general k-uniform hypergraphs.

The application of our results to 3-uniform hypergraphs is then discussed in Chapter 5. This includes an elaboration of 3-uniform nexuses of uniforms (Section 5.1), the characterization of the ideal 3-uniform hyperstars (Section 5.2), the question whether other ideal 3-uniform hypergraphs can be created from region-expansions (Section 5.3) and a discussion on whether there are 3-uniform hypergraphs which are still not known to be ideal or non-ideal (Section 5.4).

Eventually, in Chapter 6, we resume our results and provide an outline on possible future work which could be done on the topic of 3-uniform hypergraphs in the context of secret sharing.

In Appendix A, pseudo-code algorithms for various issues discussed throughout the thesis are provided together with complexity analyses.

Chapter 2

Preliminaries

In this chapter we will introduce the theory which this thesis is based on. In particular, we will talk about matroid theory and hypergraph theory, which both are helpful tools in the field of secret sharing.

As to the notation, we write $A - B$ for the set difference of two sets A and B in order to not confuse with the notation of a minor operation which we apply to matroids, access structures and hypergraphs, respectively, and which is denoted by a backslash.

2.1 Matroids

This section is an introduction to the basics of matroid theory. Later in this thesis we will see that there is a strong connection between matroids and secret sharing. The theory and notation we use is mainly based on [19, 22].

Definition 2.1 (Matroid)**.** A *matroid* $\mathcal{M}$ is a pair (Q, r), where Q is a finite set called *ground set* and $r : 2^Q \to \{0, 1, 2, \ldots\}$ is a mapping called *rank function* where the following properties are satisfied for any $A, B \subseteq Q$.

1. $0 \leq r(A) \leq |A|$
2. r is monotone increasing: if $A \subseteq B$, then $r(A) \leq r(B)$
3. r is submodular: $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$

For $A \subseteq Q$, $r(A)$ is called the *rank* of A and $r(\mathcal{M}) := r(Q)$ is called *rank of the matroid* $\mathcal{M}$.

Definition 2.2 (Independent/Dependent Set, Basis, Circuit)**.** For a matroid $\mathcal{M} = (Q, r)$, a set $A \subseteq Q$ is said to be *independent* if $r(A) = |A|$. Any subset $A \subseteq Q$ which is not independent is called *dependent*.
A maximal independent set (that is, an independent set which is not contained in any other independent set) is called *basis*, while a minimal dependent set (that is, a dependent set which does not contain any other dependent set) is called *circuit*.

Remark 2.3. Each basis has the same number of elements, namely $r(Q)$.

Remark 2.4. A rank function uniquely characterizes a set of bases and vice versa. The same is also true for independent sets. Therefore, matroids can equivalently be specified by its rank function, independent sets or set of bases. In this thesis, we will mainly use the rank notation.

Example 2.5. A simple example of a matroid is the *uniform matroid*. Given two integers k and n such that $1 \leq k < n$, we define the uniform matroid $U_{k,n}$ with ground set $Q = \{1, \ldots, n\}$ and rank function $r(A) = \min\{|A|, k\}$. It is easy to check that r fulfills all conditions for a rank function of a matroid. A set $A \subseteq Q$ is independent if and only if $|A| \leq k$.

Example 2.6. Another matroid which is especially known in the field of secret sharing is the *Vamos matroid* $\mathcal{V}$ [6] on the ground set $Q = \{1, \ldots, 8\}$. The collection of its independent sets is given by

$$\big\{A \subseteq Q \;\big|\; |A| \leq 4\big\} - \big\{\{1,2,3,4\}, \{1,2,5,6\}, \{3,4,5,6\}, \{3,4,7,8\}, \{5,6,7,8\}\big\}.$$

Definition 2.7 (Matroid Minor)**.** Let $\mathcal{M} = (Q, r)$ be a matroid and let $Z \subseteq Q$ be a subset of Q. We define two operations which yield new matroids.

- *Restriction:* $\mathcal{M} \setminus Z = (Q - Z, r_{\setminus Z})$, where $r_{\setminus Z}(A) = r(A)$ for each $A \subseteq Q - Z$.
- *Contraction:* $\mathcal{M} \,/\, Z = (Q - Z, r_{/Z})$, where $r_{/Z}(A) = r(A \cup Z) - r(Z)$ for each $A \subseteq Q - Z$.

Every matroid which can be obtained from $\mathcal{M}$ by repeatedly applying finitely many restrictions and contractions is called a *minor* of $\mathcal{M}$.

Lemma 2.8. *For a matroid $\mathcal{M} = (Q, r)$ and two disjoint sets $Z_1, Z_2 \subseteq Q$, the following rules for restriction and contraction hold.*

- $(\mathcal{M} \setminus Z_1) \setminus Z_2 = \mathcal{M} \setminus (Z_1 \cup Z_2)$ *and* $(\mathcal{M} \,/\, Z_1) \,/\, Z_2 = \mathcal{M} \,/\, (Z_1 \cup Z_2)$
- $(\mathcal{M} \setminus Z_1) \,/\, Z_2 = (\mathcal{M} \,/\, Z_1) \setminus Z_2$

The following result can be derived directly from Lemma 2.8.

Proposition 2.9. *For a matroid $\mathcal{M} = (Q, r)$, every minor of $\mathcal{M}$ can be written as $(\mathcal{M} \setminus Z_1) \,/\, Z_2$ with $Z_1, Z_2 \subseteq Q$ disjoint.*

Example 2.10. Let $U_{k,n}$ be the uniform matroid and let a be an element in the ground set. Then,

- $U_{k,n} \setminus \{a\} = U_{k,n-1}$ (as long as $k < n$), and
- $U_{k,n} \,/\, \{a\} = U_{k-1,n-1}$.

Next, we define *duals* of matroids. There are multiple equivalent definitions of this concept. We state one which uses the rank function and we will see in Proposition 2.12 how to use bases to describe a dual matroid.

Definition 2.11 (Dual Matroid)**.** Let $\mathcal{M} = (Q, r)$ be a matroid. Then, the *dual matroid* of $\mathcal{M}$, denoted by $\mathcal{M}^*$, is defined by $\mathcal{M}^* = (Q, r^*)$, where its rank function is given by $r^*(A) = |A| - r(Q) + r(Q - A)$ for every $A \subseteq Q$.

Proposition 2.12. *Let $\mathcal{M} = (Q, r)$ be a matroid. Let $\mathcal{B}$ be the family of bases of $\mathcal{M}$. Then, $\mathcal{B}^* = \{B \subseteq Q \mid Q - B \in \mathcal{B}\}$ is the family of bases of the dual matroid $\mathcal{M}^*$.*

Example 2.13. Consider the uniform matroid $U_{k,n}$ with ground set $Q = \{1, \dots, n\}$ and rank function $r(A) = \min\{|A|, k\}$ for every $A \subseteq Q$. Then, the dual of $U_{k,n}$ is the uniform matroid $U_{n-k,n}$. Indeed, the dual of the rank function r is given by

$$\begin{aligned} r^*(A) &= |A| - r(Q) + r(Q - A) \\ &= |A| - \min\{|Q|, k\} + \min\{|Q - A|, k\} \\ &= |A| - k + \min\{|Q - A|, k\} \\ &= \min\{|Q - A| + |A| - k, k + |A| - k\} \\ &= \min\{n - k, |A|\}. \end{aligned}$$

2.2 Hypergraphs

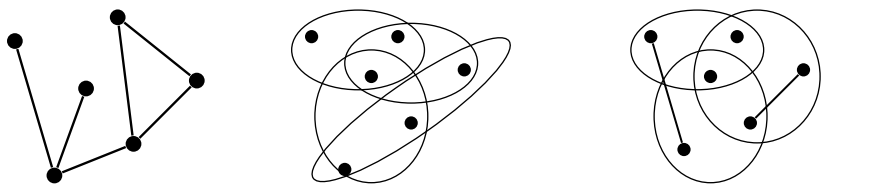
We will now give an introduction to the field of hypergraphs in order to get familiar with the basic definitions, notations and properties used in this thesis. The theory presented here is mainly based on [21, 26, 27].

2.2.1 Basic Definitions and Concepts

Definition 2.14 (Hypergraph)**.** A *hypergraph* H is an ordered pair $H = (V, E)$, where V is a set of elements called *vertices* or *nodes* and $E \subseteq 2^V - \{\emptyset\}$ is a set of non-empty unordered subsets of V called *hyperedges*.
For a hypergraph H we denote by $V(H)$ and $E(H)$ its vertex set and its hyperedge set, respectively.
A k-hyperedge is a hyperedge consisting of k vertices.
A vertex $v \in V(H)$ is said to be *adjacent* to a vertex $w \in V(H)$ if there is a hyperedge $e \in E(H)$ such that $v, w \in e$.

Definition 2.15 (k-Uniform Hypergraph)**.** A hypergraph H is called *k-uniform* for some $k \geq 1$ if each hyperedge $e \in E(H)$ is a k-hyperedge.
A 2-uniform hypergraph is called *graph* and its hyperedges are called *edges*.

Hypergraphs and graphs can be illustrated by dots for vertices and areas or borders around the vertices for each hyperedge. Edges (i.e. hyperedges consisting of only two vertices) are usually represented by a line connecting the two respective vertices. See Figure 2.1 for some examples.



(a) Graph (b) 3-uniform hypergraph (c) Non-uniform hypergraph

Figure 2.1: Examples of hypergraphs, each of them on six vertices.

Remark 2.16. While there also exist *directed hypergraphs* where the hyperedges are ordered sets, in this thesis all hypergraphs we use are *undirected*, i.e. the hyperedges are unordered sets.

Definition 2.17 (Vertex Degree)**.** Let $H = (V, E)$ be a hypergraph and $v \in V$ be a vertex. Then, the *degree of v in H*, denoted by $d_H(v)$, is given by the number of hyperedges containing v, i.e. $d_H(v) = \big|\{e \in E \mid v \in e\}\big|$.

Definition 2.18 (Isolated Vertex)**.** Let $H = (V, E)$ be a hypergraph. A vertex $v \in V$ is said to be an *isolated vertex* if $v \notin e$ for each $e \in E$.

Definition 2.19 (Subgraph)**.** Given a graph $G = (V, E)$ and any vertex set $A \subseteq V$, we define the *subgraph of G induced by A* as $G_A = \big(A, \{e \in E \mid e \subseteq A\}\big)$.

Definition 2.20 (Subhypergraph)**.** Given a hypergraph $H = (V, E)$ and a subset of the vertices $A \subseteq V$, we define the *subhypergraph of H induced by A* as $H_A = \big(A, \{e \cap A \mid e \in E \text{ and } e \cap A \neq \emptyset\}\big)$.

Example 2.21. Figure 2.2 illustrates an example of a hypergraph on six vertices and a subhypergraph of it induced by a set of four vertices.

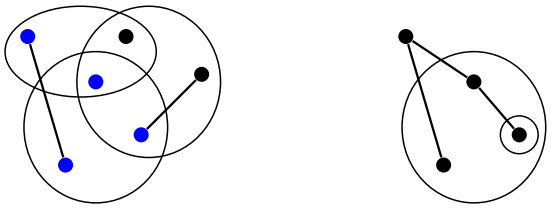


Figure 2.2: An example of a subhypergraph. The right hypergraph is the subhypergraph of the left one, induced by the blue vertices.

Remark 2.22. Note that the definitions of *subgraphs* and *subhypergraphs* given in Definitions 2.19 and 2.20 respectively are not compatible. For instance, the subgraph of $G = \big(\{1, 2, 3\}, \{\{1, 2\}, \{2, 3\}\}\big)$ induced by $\{1, 2\}$ is $\big(\{1, 2\}, \{\{1, 2\}\}\big)$ according to Definition 2.19, whereas the *subhypergraph* of G induced by $\{1, 2\}$ is given by $\big(\{1, 2\}, \{\{1, 2\}, \{2\}\}\big)$ using Definition 2.20.
Throughout this thesis we use Definition 2.20 if we talk about *subhypergraphs*, even if a hypergraph happens to be a graph. If we specifically mention *subgraphs*, we use Definition 2.19.

Definition 2.23 (Graph Complement)**.** Given a graph $G = (V, E)$, the *complement* of G is the graph $\overline{G} = (V, \overline{E})$, where $\overline{E} = \big\{\{e_1, e_2\} \subseteq V \mid \{e_1, e_2\} \notin E\big\}$.

Definition 2.24 (Hyperpath)**.** A *hyperpath* in a hypergraph $H = (V, E)$ is a sequence of distinct hyperedges $(e_1, \dots e_m)$ in E such that for $1 \leq i < j \leq m$ it holds that $e_i \cap e_j \neq \emptyset$ if and only if $j = i + 1$.
For vertices $x, y \in V$, a hyperpath $(e_1, \dots e_m)$ is said to be *between x and y* (or *from x to y*) if $x \in e_1$ and $y \in e_m$.
The *length* of a hyperpath is the length of the underlying sequence of hyperedges. If all hyperedges of the hyperpath are edges, i.e. all of them consist of two vertices, the hyperpath is simply be called *path*.

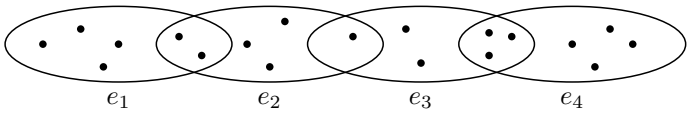


Figure 2.3: This hypergraph is a hyperpath of length 4.

Definition 2.25 (Connected Hypergraph)**.** A hypergraph $H = (V, E)$ is said to be *connected* if for each pair of vertices $x, y \in V$ there exists a hyperpath from x to y in H.
A *connected component* of a hypergraph H is a maximal connected subhypergraph Z of H, i.e. for each vertex $v \in V(H) - V(Z)$ the subhypergraph $H_{V(Z)\cup\{v\}}$ is not connected.

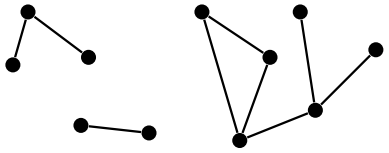


Figure 2.4: A graph with three connected components. The concept is the same for general hypergraphs.

Definition 2.26 (Hypergraph Union)**.** Let H_1 and H_2 be two hypergraphs on disjoint vertex sets. We define the *union* of H_1 and H_2 by

$$H_1 \cup H_2 = \big(V(H_1) \cup V(H_2), E(H_1) \cup E(H_2)\big).$$

Definition 2.27 (Hypergraph Isomorphism)**.** Let $H_1 = (V_1, E_1)$ and $H_2 = (V_2, E_2)$ be two hypergraphs. Then, a *hypergraph isomorphism* between H_1 and H_2 is a bijective map $p : V_1 \to V_2$ such that for every $k \geq 1$ it holds that $\{v_1, \ldots, v_k\} \in E(H_1)$ if and only if $\{p(v_1), \ldots, p(v_k)\} \in E(H_2)$.
Two hypergraphs H_1 and H_2 are called *isomorphic* and we write $H_1 \cong H_2$ if there exists a hypergraph isomorphism between them.

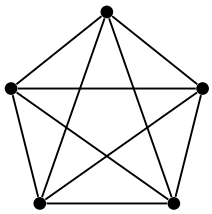
Remark 2.28. In this thesis, if nothing else is stated, we only consider hypergraphs up to isomorphism, so that the labelling is irrelevant. Hence, sometimes we use the terms *isomorphic* and *equal* interchangeably for hypergraphs.

2.2.2 Special Types of Hypergraphs

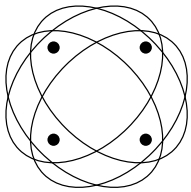
We now introduce some types of hypergraphs that will be used in this thesis. We start with the complete k-uniform hypergraphs, which are the hypergraphs where the hyperedge set is the set of all subsets of size k of the vertex set.

Definition 2.29 (Complete k-Uniform Hypergraph)**.** A k-uniform hypergraph $H = (V, E)$ is *complete* if $E = \{e \subseteq V \mid |e| = k\}$. We denote the k-uniform complete hypergraph on n vertices by $K_n^{(k)}$.

A generalization of complete k-uniform hypergraphs are the complete r-partite k-uniform hypergraphs.



(a) The complete graph $K_5^{(2)}$



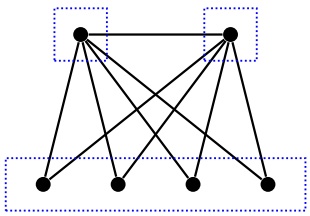
(b) The complete hypergraph $K_4^{(3)}$

Figure 2.5: Illustration of a complete graph and a complete 3-uniform hypergraph.

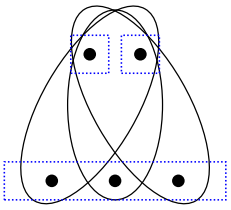
Definition 2.30 (Complete r-Partite k-Uniform Hypergraph)**.** For $r \geq k$, a k-uniform hypergraph $H = (V, E)$ is called *complete r-partite* if there is a partition $V = V_1 \cup \ldots \cup V_r$ of the vertex set into r pairwise disjoint sets such that

$$E = \big\{\{v_{i_1}, \ldots, v_{i_k}\} \;\big|\; i_j \in \{1, \ldots, r\} \text{ pairwise distinct, } v_{i_j} \in V_{i_j}\big\}.$$

A hypergraph H is called *complete multipartite k-uniform* if there exists an $r \geq k$ such that H is complete r-partite k-uniform.
We denote by $K^{(k)}_{n_1,\ldots,n_r}$ the complete r-partite k-uniform hypergraph with partition $V = V_1 \cup \ldots \cup V_r$, where $|V_i| = n_i$ for $i = 1 \ldots, r$.
If $r = 2$ we say *bipartite* instead of 2-partite and if $r = 3$ we say *tripartite* instead of 3-partite.
We denote by $\mathcal{K}^{(k)} = \big\{K^{(k)}_{n_1,\ldots,n_r} \;\big|\; r \geq k, n_1, \ldots, n_r > 0\big\}$ the set of all complete multipartite k-uniform hypergraphs.



(a) Complete 3-partite graph $K^{(2)}_{4,1,1}$



(b) Complete 3-partite hypergraph $K^{(3)}_{3,1,1}$

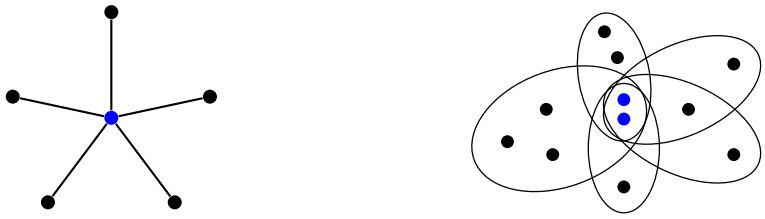
Figure 2.6: Two examples of complete multipartite hypergraphs. The independent sets are indicated by blue dashed frames.

Remark 2.31. Complete k-uniform hypergraphs are exactly the complete multipartite k-uniform hypergraphs of the form $K^{(k)}_{1,\ldots,1}$.

Definition 2.32 (Hyperstar)**.** A hypergraph $H = (V, E)$ is said to be a *hyperstar* if $\bigcap_{e \in E} e \neq \emptyset$. The intersection of all hyperedges is called the *center* of the hyperstar.
If all hyperedges of the hyperstar are edges, i.e. all of them consist of two vertices, it is simply called *star*.

Remark 2.33. Note that for any graph G it holds that G is a star if and only if it is a complete bipartite graph of the form $K^{(2)}_{1,s}$ for some $s \geq 1$. For $k \geq 3$

there is no such characterization of hyperstars in terms of complete multipartite hypergraphs.



(a) The star $K^{(2)}_{1,5}$ (b) Non-uniform hyperstar with center of size 2

Figure 2.7: Examples of hyperstars. The vertices in the center of the respective hyperstar are colored blue.

2.2.3 Independence, Vertex Covers and Regions

Definition 2.34 (Independent Set)**.** Let $H = (V, E)$ be a k-uniform hypergraph and let $1 \leq j \leq k$. A subset of the vertices $W \subseteq V$ is said to be *j-independent* if $|W \cap e| < j$ for all $e \in E$.
We call $W \subseteq V$ *independent* if it is 2-independent, i.e. no hyperedge contains more than one vertex in W.

Definition 2.35 (Vertex Cover)**.** Let $H = (V, E)$ be a hypergraph. A *vertex cover* of H is a subset of the vertices $C \subseteq V$ such that for each hyperedge $e \in E$ it holds that $e \cap C \neq \emptyset$. A vertex cover is called *minimal* if no proper subset of it is also a vertex cover.

Remark 2.36. If C is a vertex cover of a hypergraph H, then also every superset of C is a vertex cover of H.

Example 2.37. For any complete k-partite k-uniform hypergraph, every independent set V_i in the partition $V = V_1 \cup \ldots \cup V_k$ is a vertex cover. Note that this is not true for complete r-partite k-uniform hypergraphs with $r > k$.

Example 2.38. Consider the hypergraphs in Figure 2.8. All three subfigures show the same hypergraph but with different candidates for vertex covers. In the first two cases, the blue vertices form a vertex cover since every (hyper-)edge contains at least one of them. However, in the last subfigure, the blue vertices do not form a vertex cover, since the red colored edge has an empty intersection with them.

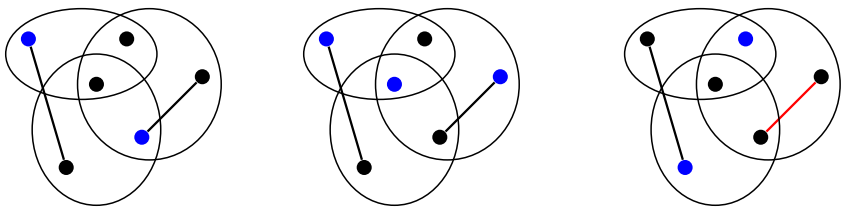


Figure 2.8: Illustration of different vertex covers of the same hypergraph. Note that in the last subfigure, the set of blue vertices is not a vertex cover.

Lemma 2.39. *Let $H = (V, E)$ be a hypergraph. Then, $C \subseteq V$ is an independent set and a vertex cover (short: independent vertex cover or IVC) if and only if $|C \cap e| = 1$ for all $e \in E$.*

Proof. First, assume C is an independent vertex cover. Let $e \in E$ be any hyperedge. Since C is a vertex cover, we know that $|C \cap e| \geq 1$. From independence (i.e. 2-independence) it follows that $|C \cap e| < 2$ which yields $|C \cap e| = 1$.

For the other direction of the claim, assume $|C \cap e| = 1$. Then, C trivially fulfills the conditions for being 2-independent and a vertex cover. □

Definition 2.40 (Region)**.** Let $H = (V, E)$ be a hypergraph. A set of vertices $R \subseteq V$ is called a *region* of H if there exists $F \subseteq E$ such that

$$R = \left(\bigcap_{e \in F} e \right) - \left(\bigcup_{e \in (E-F)} e \right).$$

We say that $F \subseteq E$ *determines* the region R.

Remark 2.41. Note that for a region R of a hypergraph H, each hyperedge in $E(H)$ either contains R or is disjoint from it. We will say that a hyperedge e determines R if e is in the hyperedge set which determines R.

In natural language, a region is a set of vertices which are all contained in exactly the same set of hyperedges.

When drawing a hypergraph, a region is a connected area in the drawing which contains at least one vertex (given that no unnecessary intersections of the hyperedge boundaries are drawn).

Remark 2.42. In complete r-partite k-uniform hypergraphs, if $r > k$, then each vertex is a region itself. If $r = k$, then the union of all parts of size 1 form one region, all other vertices are regions itself.

Example 2.43. The center C of a hyperstar $H = (V, E)$ is a region determined by E.

Example 2.44. A hypergraph which itself is a hyperpath of length l contains exactly $2l - 1$ regions. See Figure 2.9 for an illustration.

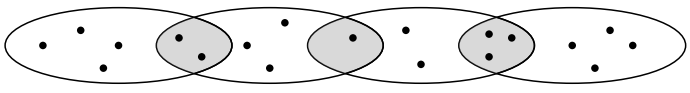


Figure 2.9: This hyperpath of length 4 contains four regions which are determined by one hyperedge, respectively (white), and three regions which are determined by two hyperedges, respectively (gray).

Chapter 3

Introduction to Secret Sharing

This chapter provides an introduction to the area of secret sharing, including the definitions, notations and previous results which are needed in the course of this thesis. We start in Section 3.1 with the basics of secret sharing and in Section 3.2 we present Shamir's scheme, an example of a secret sharing scheme which we will repeatedly use in the sequel. Afterwards, we describe the connection of this theory with the theory of matroids (Section 3.3) and hypergraphs (Section 3.4) and state the respective previous results we will need.

3.1 Basics of Secret Sharing

We mainly follow the definitions and notations used by Beimel in most of his papers [16, 23, 28, 31] which are some of the chief contributions in recent time to the area of secret sharing.

Secret sharing is the theory of sharing a piece of information called *secret* among a set of *participants* (also called *parties*), such that only certain subsets of these participants can recreate the original secret. At the same time, other subsets should have no information about the secret from their knowledge.

Secret sharing is a subdiscipline of cryptography. While it is not part of public-key nor private-key cryptography, it can use such protocols to encrypt and safely send information from one party to another. Secret sharing is a tool which is used in fields like multiparty computations [15] or access control [13, 30].

During this thesis we make the assumption that all parties are *honest-but-curious*. This means that they strictly follow the protocols but still will keep all the knowledge they get and try to find out some information about the secret. There are investigations of other cases where for instance an adversary can corrupt a certain amount of participants, or tries to find out other shares or the secret by not following the protocols and providing wrong information. However, the question whether a given scheme prevents such adversaries from

gaining any information is not part of this thesis. The only case which is considered here is that if an unqualified set of participants pools its knowledge, it should still have no information about the secret or parts of it.

3.1.1 Access Structures and Secret Sharing Schemes

Let us now introduce the formal definitions we will use.

Definition 3.1 (Access Structure)**.** Let $P = \{p_1, \ldots, p_n\}$ be a set of participants. A collection of subsets $\mathcal{A} \subseteq 2^P$ is said to be *monotone* if for each $B, C \subseteq P$ such that $B \in \mathcal{A}$ and $B \subseteq C$, also $C \in \mathcal{A}$. An *access structure* on P is a monotone collection $\mathcal{A} \subseteq 2^P - \emptyset$ of non-empty subsets of P.
A set of participants $A \subseteq P$ is called *qualified* if $A \in \mathcal{A}$ and *unqualified* if $A \notin \mathcal{A}$.

For an access structure $\mathcal{A}$ we define the family of its minimal qualified sets by $\min(\mathcal{A}) = \{B \in \mathcal{A} \mid B \not\subseteq C \text{ for all } C \in \mathcal{A} - \{B\}\}$. Note that, by monotonicity, an access structure is fully characterized by its family of minimal sets.

Definition 3.2 (Dual Access Structure)**.** Let P be a set of participants, $\mathcal{A}$ an access structure on P. Then, the *dual access structure* of $\mathcal{A}$ is defined by $\mathcal{A}^* = \{A \subseteq P \mid P - A \notin \mathcal{A}\}$.

Definition 3.3 (Distribution Scheme)**.** Let $P = \{p_1, \ldots, p_n\}$ be a set of participants, D a finite set called *domain of secrets* and, for each $i = 1, \ldots, n$, D_i a finite set called *domain of shares of* p_i. Let R be a finite set called the *set of random strings*, which will be used for random sampling, and let μ be a probability distribution on R. Finally, let $\Pi : D \times R \to D_1 \times \ldots \times D_n$ be the *distribution map*. Then, a *distribution scheme* is given by the pair $\Sigma = \langle \Pi, \mu \rangle$.
A *dealer* shares a secret $s \in D$ by sampling a string $r \in R$ according to μ, computing the vector of shares $(s_1, \ldots, s_n) = \Pi(s, r)$ and privately communicating each share $s_i \in D_i$ to participant p_i, respectively.

Definition 3.4 (Information Ratio)**.** Taking the notation of the above definition, the *information ratio* σ and the *average information ratio* $\tilde{\sigma}$ of a distribution scheme Σ are defined by

$$\sigma(\Sigma) = \frac{\max_{1 \le j \le n} \log |D_j|}{\log |D|} \quad \text{and} \quad \tilde{\sigma}(\Sigma) = \frac{\sum_{1 \le j \le n} \log |D_j|}{n \cdot \log |D|}.$$

The *(average) information rate*, which in some literature is used instead of the information ratio, is the inverse of the (average) information ratio.

Definition 3.5 (Secret Sharing Scheme)**.** Let $\Sigma = \langle \Pi, \mu \rangle$ be a distribution scheme for the set of participants $P = \{p_1, \ldots, p_n\}$ with domain of secrets D and domains of shares $D_1, \ldots, D_n$. For a set $A = \{p_{i_1}, \ldots, p_{i_r}\} \subseteq P$, denote by $\Pi_A(s, r)$ the vector of shares of participants in A, i.e. $\Pi_A(s, r)_j = \Pi(s, r)_{i_j}$ for $j = 1, \ldots, r$. Σ is said to be a *secret sharing scheme realizing an access structure* $\mathcal{A} \subseteq 2^P - \{\emptyset\}$ if it fulfills the following two conditions.

- *Correctness:* Any qualified set should be able to correctly reconstruct the secret, i.e. for each $Q = \{p_{i_1}, \ldots, p_{i_{|Q|}}\} \in \mathcal{A}$ there exists a *reconstruction function* $\Lambda_Q : D_{i_1} \times \ldots \times D_{i_{|Q|}} \to D$ such that for every secret $s \in D$,

$$\mathbb{P}\big[\Lambda_Q(\Pi_Q(s, r)) = s\big] = 1.$$

- *Perfectness:* Any unqualified set $U = \{p_{i_1}, \dots, p_{i_{|U|}}\} \notin \mathcal{A}$ should have no information about the secret, i.e. for any two secrets $a, b \in D$, any possible vector of shares $(s_j)_{p_j \in U}$ and a random variable $r \in R$ we have

$$\mathbb{P}\big[\Pi_U(a, r) = (s_j)_{p_j \in U}\big] = \mathbb{P}\big[\Pi_U(b, r) = (s_j)_{p_j \in U}\big].$$

Remark 3.6. Note that for the distribution map Π as well as for the reconstruction functions Λ_Q, we equip the set of participants (or subsets of it) with an order. For a formal definition, we could use tuples instead of sets to cope with this. However, in favor of readability and since it will always be clear from the context what is meant, we stick with the notation of sets. In this way, it does not matter how the participants are enumerated, i.e. a secret sharing scheme on the set of participants $P = \{p_1, \dots, p_n\}$ is equivalent to the same scheme on $P' = \{\pi(p_1), \dots, \pi(p_n)\}$, where π is any permutation of P.

Remark 3.7. We restrict the domain of secrets as well as the domains of shares to be finite. The reason is that in practice we do not want to cope with information transfer which can become arbitrarily large. Furthermore, the definition of the information ratio and average information ratio is not well-defined if the domains are infinite. Chor and Kushilevitz [8] proved that no secret sharing scheme with countable domain of secrets can exist and recently Dibert and Csirmaz [29] discussed how some definitions need to be adjusted and what problems are faced when using infinite domains as well as infinite sets of participants.

Remark 3.8. It has been shown by Blundo et al. [12] that correctness and perfectness are independent of the probability distribution used on the domain of secrets and the domains of shares. So usually we take the uniform distribution, where the probability of each element is the same, i.e. $\mathbb{P}(s) = \frac{1}{|D|}$ for each secret $s \in D$ and similarly for each share in its domain.

Remark 3.9. Given a secret sharing scheme $\Sigma = \langle \Pi, \mu \rangle$, it uniquely induces an access structure. Note that the other direction is not true in general: given an access structure $\mathcal{A}$, there are usually multiple secret sharing schemes realizing $\mathcal{A}$.

Example 3.10. Let us make a real world example where we construct two different distribution schemes, only one of it being a secret sharing scheme. Assume we have a combination lock with three digits, each in the range from 0 to 9. That is, our domain of secrets can be seen as the set $\{0, \dots, 999\}$. We want to share the combination among three participants $P = \{p_1, p_2, p_3\}$ such that only the three together can open the lock, i.e. the access structure is $\mathcal{A} = \{P\}$.

Approach 1: We share the secret by giving each participant one of the three digits. Hence, our distribution scheme is defined by $\Sigma_1 = \langle \Pi^{(1)}, \mu_1 \rangle$, where the set of random strings is given by $R_1 = \{0\}$ and $\mu_1(0) = 1$ is a probability distribution on R_1, and the distribution map is given by $\Pi^{(1)}(s, r) = (s_1, s_2, s_3)$, where

$$s_1 = \left\lfloor \frac{s}{100} \right\rfloor, \quad s_2 = \left\lfloor \frac{s - 100s_1}{10} \right\rfloor, \quad s_3 = s - 100s_1 - 10s_2$$

Note that here we do not make use of the set of random strings R_1 which makes it a deterministic distribution map.

For the only qualified set $P \in \mathcal{A}$ we define the reconstruction function as $\Lambda_P(s_1, s_2, s_3) = 100s_1 + 10s_2 + s_3$. Clearly, this implies correctness of the scheme.

However, perfectness is not given with this approach. Let $U = \{p_1\}$ be an unqualified set and consider any two possible secrets, e.g. $a = 184$ and $b = 236$, as well as a possible share $s_1 = 2$ of participant p_1. In order for the scheme to be perfect, it must hold that $\mathbb{P}\big[\Pi^{(1)}_{\{p_1\}}(184, r) = (2)\big] = \mathbb{P}\big[\Pi^{(1)}_{\{p_1\}}(236, r) = (2)\big]$. But it is easy to see that the probability on the left hand side is 0, while the one on the right hand side is 1. This is a consequence of the invertibility of the distribution function. Therefore, this scheme is not a secret sharing scheme.

Approach 2: We share the secret s by using another distribution scheme $\Sigma_2 = \langle \Pi^{(2)}, \mu_2 \rangle$, where the set of random strings is $R_2 = \{0, \dots, 999\}^2$, μ_2 is the uniform distribution on R_2 and $\Pi^{(2)}$ is given by

$$\Pi^{(2)}(s, (r_1, r_2)) = (r_1, r_2, s - r_1 - r_2 \bmod 1000).$$

The reconstruction function for the only qualified set $P \in \mathcal{A}$ is given by

$$\Lambda_P(s_1, s_2, s_3) = s_1 + s_2 + s_3 \bmod 1000$$

which shows correctness.

For perfectness, let us take for instance the unqualified set $U = \{p_2, p_3\}$, two secrets $a, b \in \{0, \dots, 99\}$ and let (s_2, s_3) be the vector of shares of U. Then,

$$\begin{aligned}\mathbb{P}\big[\Pi^{(2)}_U(a, (r_1, r_2)) = (s_2, s_3)\big] &= \mathbb{P}\big[s_2 = r_2,\ s_3 = a - r_1 - r_2 \bmod 1000\big] \\ &= \mathbb{P}\big[r_2 = s_2,\ r_1 = a - s_3 - r_2 \bmod 1000\big] \\ &= 0.001^2\end{aligned}$$

where we use that r_1 and r_2 are chosen uniformly at random and independently from $\{0, \dots, 999\}$. Since the exact same calculation can be done for b instead of a, we see that U has no information about the secret. The same reasoning holds for any other unqualified set. Therefore, Σ_2 is a secret sharing scheme realizing $\mathcal{A}$.

Definition 3.11 (Independent Secret Sharing Schemes)**.** We say that for $t \geq 1$, a collection of t secret sharing schemes $\big(\Sigma_i = \langle \Pi^{(i)}, \mu_i \rangle\big)_{i=1,\dots,t}$ is *independent* if the respective random strings $r_i \in R_i$ for Σ_i with $i = 1, \dots, t$ are sampled independently.

During this thesis, if multiple secret sharing schemes are involved in a result, they are always assumed to be independent if nothing else is stated.

Remark 3.12. Intuitively, if $(\Sigma_i)_{i=1,\dots,m}$ is a collection of independent secret sharing schemes, then for every $i \in \{1, \dots, m\}$ any unqualified set U of Σ_i does not gain any information from any set of shares from other schemes, since these shares have been computed independently from the secret of Σ_i.

3.1.2 Ideal Secret Sharing

The following result about share sizes was stated by Karnin et al. [5, Theorem 1] only for threshold schemes and has later been extended to general schemes by Capocelli et al. [7, Lemma 3.1], where both proofs base on an information theoretic approach.

Theorem 3.13. *In any secret sharing scheme the size of each domain of shares is at least as large as the size of the domain of secrets.*

Hence, the best possible case is when each domain of shares has the same size as the domain of secrets. Such schemes are called *ideal*.

Definition 3.14 (Ideal Secret Sharing Scheme)**.** Let Σ be a secret sharing scheme with domain of secrets D and domains of shares $D_1, \ldots, D_n$. Then, Σ is called *ideal* if $|D| = |D_1| = \ldots = |D_n|$, that is, each domain of shares has the same size as the domain of secrets.

Remark 3.15. Note that from Theorem 3.13 we see that a secret sharing scheme Σ is ideal if and only if $\sigma(\Sigma) = \tilde{\sigma}(\Sigma) = 1$.

Definition 3.16 (Ideal Access Structures)**.** For $m > 1$, an access structure $\mathcal{A}$ is said to be *m-ideal* if there is an ideal secret sharing scheme Σ where the size of the domain of secrets is $|D| = m$ (and therefore all domains of shares have size m too) and Σ realizes $\mathcal{A}$. If there exists $m > 1$ such that $\mathcal{A}$ is m-ideal, then $\mathcal{A}$ is called *ideal*.

In this thesis we focus on the question which access structures are ideal for some specific types of access structures. We do not discuss other bounds on the information ratio as it is done in some other literature [7, 11, 20, 31].

Proposition 3.17. *If an access structure $\mathcal{A}$ is m_1-ideal and m_2-ideal, where $m_1, m_2 > 1$, then $\mathcal{A}$ is also $(m_1 m_2)$-ideal.*

Proof. Let $\mathcal{A}$ be an access structure on the set of participants $P = \{p_1, \ldots, p_n\}$. We assume that there exist two secret sharing schemes $\Sigma_1 = \langle \Pi^{(1)}, \mu_1 \rangle$ and $\Sigma_2 = \langle \Pi^{(2)}, \mu_2 \rangle$ which are m_1-ideal and m_2-ideal, respectively, and both realize $\mathcal{A}$. For $i \in \{1, 2\}$ we use the following notations: For Σ_i denote the domain of secrets by D_i and for participant p_j the domain of shares by $D_{i,j}$. Note that, by m_i-idealness, $|D_i| = |D_{i,j}| = m_i$. We denote the set of random strings by R_i, equipped with probability distribution μ_i.

Define a secret sharing scheme $\Sigma = \langle \Pi, \mu \rangle$ on the set of participants P with domain of secrets $D_1 \times D_2$, domain of shares $D_{1,j} \times D_{2,j}$ for participant p_j and set of random strings $R_1 \times R_2$ with probability distribution $\mu(r_1, r_2) = \mu_1(r_1)\mu_2(r_2)$. Note that this is indeed a probability distribution since μ_1 and μ_2 are independent probability distributions.

Let the distribution map of Σ be

$$\Pi : (D_1 \times D_2) \times (R_1 \times R_2) \to (D_{1,1} \times D_{2,1}) \times \ldots \times (D_{1,n} \times D_{2,n}),$$
$$\Pi\big((s_1, s_2), (r_1, r_2)\big)_j = \big(\Pi^{(1)}(s_1, r_1)_j, \Pi^{(2)}(s_2, r_2)_j\big) \text{ for } j = 1 \ldots, n.$$

It is easy to verify that Σ is a secret sharing scheme realizing $\mathcal{A}$. Indeed, correctness and perfectness are given by the independence of the two schemes Σ_1

and Σ_2, where for each qualified set $Q = \{p_{j_1}, \ldots, p_{j_{|Q|}}\} \in \mathcal{A}$ the reconstruction function is given by

$$\begin{aligned}
&\Lambda_Q : (D_{1,j_1} \times D_{2,j_1}) \times \ldots \times (D_{1,j_{|Q|}} \times D_{2,j_{|Q|}}) \to (D_1, D_2),\\
&\Lambda_Q\big((s_{1,j_1}, s_{2,j_1}), \ldots, (s_{1,j_{|Q|}}, s_{2,j_{|Q|}})\big)\\
&\qquad = \big(\Lambda_Q^{(1)}(s_{1,j_1}, \ldots, s_{1,j_{|Q|}}), \Lambda_Q^{(2)}(s_{2,j_1}, \ldots, s_{2,j_{|Q|}})\big).
\end{aligned}$$

Note that $|D_1 \times D_2| = |D_{1,j} \times D_{2,j}| = m_1 m_2$ for each $j = 1, \ldots, n$ which shows $(m_1 m_2)$-idealness of the access structure $\mathcal{A}$. □

Corollary 3.18. *For each ideal access structure $\mathcal{A}$ and each $m > 1$ there exists $m' \geq m$ such that $\mathcal{A}$ is m-ideal.*

Beimel and Chor [9, Theorem 3.1] have stated the following interesting result about m-idealness.

Theorem 3.19. *An access structure is m-ideal for each $m > 1$ if and only if it is both 2-ideal and 3-ideal.*

In the same paper, some examples of access structures are discussed which are 2-ideal but not 3-ideal and vice versa. In general, m_1-idealness does not imply m_2-idealness for $m_1 \neq m_2$.

3.1.3 Linear and Multi-Linear Secret Sharing

Apart from a low information ratio it is also desirable that the computation of the shares and the reconstruction of the secret are both computationally inexpensive mappings. Linear and multi-linear schemes are two examples of such secret sharing schemes. A further advantage of them is that the mappings can be represented by matrices which makes them suitable and easy for practical implementation.

Definition 3.20 (Linear Secret Sharing Scheme)**.** Let $P = \{p_1, \ldots, p_n\}$ be a set of participants and let $\mathbb{F}$ be a finite field. Let $\Sigma = \langle \Pi, \mu \rangle$ be a secret sharing scheme where the domain of secrets is $\mathbb{F}$. For each $i = 1, \ldots, n$ the domain of shares of participant p_i is $\mathbb{F}^{k_i}$ for some $k_i \geq 1$ and the set of random strings is $\mathbb{F}^l$ for some $l \geq 1$. Then, Σ is said to be *linear over* $\mathbb{F}$ if Π is a linear map, i.e. if we can express the computation of the shares as

$$(\mathbf{s_1}, \ldots, \mathbf{s_n}) = (s, r_1, \ldots, r_l) \cdot A$$

where $\mathbf{s_1}, \ldots, \mathbf{s_n}$ are the vectors of shares (each $\mathbf{s_i}$ being a row vector of length k_i), s is the secret, $r_1, \ldots, r_l$ are random elements from R and A is a publicly known matrix of size $((l+1) \times (k_1 + \ldots + k_n))$ over $\mathbb{F}$.

Remark 3.21. If a linear secret sharing scheme is also ideal, that is, the domain of shares for each participant is $\mathbb{F}$, then the above computation writes as

$$(s_1 \ldots, s_n) = (s, r_1, \ldots, r_l) \cdot A$$

where $s_1, \ldots, s_n$ are the shares (each of them being an element in $\mathbb{F}$) and A has size $((l+1) \times n)$.

Remark 3.22. Linear secret sharing schemes can be equivalently defined by the linearity of the reconstruction map for each qualified set [10, Claim 4.3].

The idea of linear secret sharing schemes can be generalized to *multi-linear* schemes. While for linear schemes the secret is one element from the field $\mathbb{F}$, in this case it is a vector in $\mathbb{F}^t$ for some $t \geq 1$:

Definition 3.23 (Multi-linear Secret Sharing Scheme)**.** Let $P = \{p_1, \ldots, p_n\}$ be a set of participants and let $\mathbb{F}$ be a finite field. Let $\Sigma = \langle \Pi, \mu \rangle$ be a secret sharing scheme where the domain of secrets is $\mathbb{F}^t$ for some $t \geq 1$. For each $i = 1, \ldots, n$ the domain of shares of participant p_i is $\mathbb{F}^{k_i}$ for some $k_i \geq t$, and the set of random strings is $\mathbb{F}^l$ for some $l \geq 1$. Then, Σ is said to be *multi-linear over* $\mathbb{F}$ if Π is a linear map, i.e. if we can express the computation of the shares as

$$(\mathbf{s_1}, \ldots, \mathbf{s_n}) = (\mathbf{s}, r_1, \ldots, r_l) \cdot A$$

where $\mathbf{s_1}, \ldots, \mathbf{s_n}$ are the vectors of shares (each $\mathbf{s_i}$ being a row vector of length k_i), $\mathbf{s}$ is the secret vector, $r_1, \ldots, r_l$ are random elements from R and A is a publicly known matrix of size $((l + t) \times (k_1 + \ldots + k_n))$ over $\mathbb{F}$.

Remark 3.24. Every linear secret sharing scheme is multi-linear by setting $t = 1$.

Remark 3.25. If a multi-linear secret sharing scheme is also ideal, i.e. each participant's share is of the same size as the secret, then $k_i = t$ for each $1 \leq i \leq n$ and, therefore, the size of the matrix A is $((l + t) \times nt)$.

Remark 3.26. Note that we only use finite fields as domains of secrets and shares for linear (and multi-linear) secret sharing schemes. If the scheme allows it, i.e. if no inverses are needed in any computation within distribution and reconstruction, we could also consider using finite rings. However, in this thesis we restrict to finite fields since the schemes we will use in most cases need inverses.

Definition 3.27 ((Multi-)Linearly Ideal Access Structure)**.** Let q be a prime power. We say that an access structure $\mathcal{A}$ is *(multi-)linearly q-ideal* if it can be realized by some (multi-)linear q-ideal secret sharing scheme. $\mathcal{A}$ is called *(multi-)linearly ideal* if there exists $q > 1$ such that $\mathcal{A}$ is (multi-)linearly q-ideal.

Remark 3.28. Beimel et al. [28, Corollary 3.6] showed that there exist access structures which are multi-linearly ideal but not linearly ideal. Therefore, multi-linear schemes are strictly more powerful than linear schemes.

There are multiple other non-linear types of secret sharing schemes, which are however not yet discussed on a large scale [16, 17].

3.2 Threshold Access Structures

One of the early and most basic secret sharing schemes is the (t, n)-threshold scheme introduced by Shamir [4]. For this scheme on the set of participants P and a fixed integer t such that $1 \leq t \leq n$, the access structure is defined by $\mathcal{A} = \{A \subseteq 2^P \mid |A| \geq t\}$. We call such an access structure *threshold access structure*. In words, at least t out of n participants are required to reveal the

secret. In order to realize this access structure, Shamir's scheme makes use of the Lagrange interpolation of polynomials.

Let $P = \{p_1, \ldots, p_n\}$ be a set of participants and let $\mathbb{F}_q$ be a finite field of q elements for some prime power $q > n$. Let $a_1, \ldots, a_n \in \mathbb{F}_q - \{0\}$ be n pairwise distinct field elements. In order to share a secret $s \in \mathbb{F}_q$, the dealer samples $t-1$ random elements $r_1, \ldots, r_{t-1}$ from $\mathbb{F}_q$ and defines the polynomial $P(x) = s + \sum_{i=1}^{t-1} r_i x^i$. He then computes the shares $s_i = P(a_i)$ over $\mathbb{F}_q$ for $i \in \{1, \ldots, n\}$ and privately sends s_i to participant p_i. By Lagrange's interpolation theorem, we can determine the polynomial P by knowing at least t points $(a_i, P(a_i))$ on the function. When knowing P, the secret s is computed by $s = P(0)$.

Formally, let $Q = \{p_{i_1}, \ldots, p_{i_t}\} \subseteq P$ be a minimal qualified set of participants. Participant p_{i_j} has received the share $s_{i_j} = P(a_{i_j})$ for $j = 1, \ldots, t$. The participants in Q then compute the Lagrange polynomial

$$L(x) = \sum_{l=1}^{t} s_{i_l} \prod_{\substack{1 \le j \le t \\ i_j \neq i_l}} \frac{a_{i_j} - x}{a_{i_j} - a_{i_l}}.$$

By the interpolation theorem, $L(x) = P(x)$ and, in particular, $s = P(0) = L(0)$ which can be computed by the participants in Q. This shows *correctness* of the scheme.

For *perfectness*, consider an unauthorized set, i.e. a set $U = \{p_{i_1}, \ldots, p_{i_{t-1}}\} \subseteq 2^P$ (we take a maximal unauthorized set U here, the same works for subsets of U). By the interpolation theorem, for each possible secret $s \in \mathbb{F}_q$ there exists a unique polynomial P_s with degree $t-1$ such that $P_s(0) = s$ and $P_s(a_{i_j}) = s_{i_j}$ for $j = 1, \ldots, t-1$. Hence, the probability for each element of $\mathbb{F}_q$ being the secret (given the shares of U) is the same, namely $q^{-(t-1)}$.

Note that $q > n$ is required. Indeed, we need a dedicated field element for each of the n participant, plus the zero element for the secret.

Shamir [4] defined his scheme before the area of secret sharing has been developed and, hence, did not state anything about idealness or linearity. However, it is easy to see that Shamir's scheme is both linear and ideal. We state a proof of this result using the notation of this thesis.

Proposition 3.29. *Shamir's (t, n)-threshold scheme is linear and q-ideal for any prime power $q > n$.*

Proof. Let $P = \{p_1, \ldots, p_n\}$ be the set of participants, fix a finite field $\mathbb{F}_q$ for a prime power $q > n$ and let $a_1, \ldots, a_n \in \mathbb{F}_q - \{0\}$ be pairwise distinct field elements. Let $s \in \mathbb{F}_q$ be a secret to share and $r_1, \ldots, r_{t-1} \in \mathbb{F}_q$ be the random elements sampled by the dealer.

Then, the vector of shares can be written as $(s_1, \ldots, s_n) = (s, r_1, \ldots, r_l) \cdot V$, where

$$V = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ a_1 & a_2 & a_3 & \cdots & a_n \\ a_1^2 & a_2^2 & a_3^2 & \cdots & a_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1^{t-1} & a_2^{t-1} & a_3^{t-1} & \cdots & a_n^{t-1} \end{pmatrix}$$

is the transpose of a Vandermonde matrix over $\mathbb{F}_q$. Note that this matrix does not depend on the random elements $r_1, \ldots, r_{t-1}$ and is usually publicly known.

Since each share is a field element and we can express the computation with this linear map, the scheme is ideal and linear over any $\mathbb{F}_q$. □

Hence, each threshold access structure is linearly ideal. For the special case when $t = n$ or $t = 1$ we state an even stronger result:

Proposition 3.30. *For any $n \geq 1$, both the $(1, n)$-threshold access structure as well as the (n, n)-threshold access structure are m-ideal for each $m > 1$. If m is a prime power, they are also linearly m-ideal.*

Proof. In the $(1, n)$-threshold access structure, each participant itself can reveal the secret, i.e. the dealer sends the secret to each of them, no matter how large the domain of secret is. This is obviously an ideal and linear scheme.

For the (n, n)-access structure, fix any $m > 1$. Let the domain of secrets be $\mathbb{Z}/m\mathbb{Z}$ and let the set of random strings be $R = (\mathbb{Z}/m\mathbb{Z})^{n-1}$. Define a secret sharing scheme by its distribution map

$$\Pi : \mathbb{Z}/m\mathbb{Z} \times R \to \mathbb{Z}/m\mathbb{Z} \times \ldots \times \mathbb{Z}/m\mathbb{Z}$$
$$\Pi\big(s, (r_1, \ldots, r_{n-1})\big) = (r_1, \ldots, r_{n_1}, s - r_1 - \ldots - r_{n-1} \bmod m).$$

The secret can be reconstructed by adding up all shares. It is easy to verify that this scheme is correct, perfect and m-ideal. If m is a prime power, Π can be represented by a matrix over $\mathbb{F}_m$ and is therefore linear too. □

Lemma 3.31. *Any access structure can be realized by a linear secret sharing scheme.*

Proof. Let $\mathcal{A}$ be an access structure on some set of participants P. We can construct a linear secret sharing scheme Σ for $\mathcal{A}$ by combining multiple independent threshold schemes. Indeed, for each minimal qualified set $Q \in \min(\mathcal{A})$, let Σ_Q be a $(|Q|, |Q|)$-threshold scheme. Participant p gets one share of scheme Σ_Q if and only if $p \in Q$. It is easy to check that this is indeed a linear secret sharing scheme realizing $\mathcal{A}$.

If we write $c_p = \big|\{Q \in \min(\mathcal{A}) \mid p \in Q\}\big|$ for $p \in P$, then the information ratio σ and average information ratio $\tilde{\sigma}$ of this scheme are given by

$$\sigma(\Sigma) = \max_{p \in P} c_p \quad \text{and} \quad \tilde{\sigma}(\Sigma) = \frac{\sum_{p \in P} c_p}{|P|}.$$

□

Remark 3.32. Even though the proof of Lemma 3.31 shows a recipe how to construct a linear secret sharing scheme for any access structure, this is not a scheme we would use in practice, since with this construction the information ratio is extremely high in general. The goal should be having a linear scheme which also has low information ratio. If possible it should be ideal, that is, it should have an information ratio of 1.

3.3 Secret Sharing and Matroids

We now connect the theory of secret sharing with the one of matroids. In particular, we will see that each matroid automatically defines an access structure via its port. The connection to matroids is a useful tool to determine whether a given access structure is non-ideal.

Most of the notation we introduce here is based on [22, 19].

3.3.1 Matroid Ports, Access Structures and Minors

Definition 3.33 (Matroid Port)**.** Let $\mathcal{M} = (Q, r)$ be a matroid with ground set Q and let $p_0 \in Q$. The family of subsets

$$\Gamma_{p_0}(\mathcal{M}) = \big\{A \subseteq Q - \{p_0\} \mid r(A \cup \{p_0\}) = r(A)\big\}$$

is called the *port of* $\mathcal{M}$ *at point* p_0.

Lemma 3.34. *For any matroid* $\mathcal{M} = (Q, r)$ *and* $p_0 \in Q$*, the matroid port* $\Gamma_{p_0}(\mathcal{M})$ *is an access structure on the set of participants* $P = Q - \{p_0\}$*.*

Proof. We only need to show monotonicity of $\Gamma_{p_0}(\mathcal{M})$. So let $A \subseteq B \subseteq Q - \{p_0\}$ with $A \in \Gamma_{p_0}(\mathcal{M})$. By submodularity of the rank function r,

$$\begin{aligned} r(A) + r(B) &= r(A \cup \{p_0\}) + r(B) \\ &\geq r(A \cup \{p_0\} \cup B) + r((A \cup \{p_0\}) \cap B) \\ &= r(B \cup \{p_0\}) + r(A). \end{aligned}$$

Hence, $r(B) \geq r(B \cup \{p_0\})$ and, by monotonicity of the rank function r, equality holds. Therefore, $B \in \Gamma_{p_0}(\mathcal{M})$. □

We usually consider p_0 to be the dealer in the secret sharing scheme realizing the access structure $\Gamma_{p_0}(\mathcal{M})$.

Observe that $A \subseteq Q - \{p_0\}$ is a minimal qualified subset of $\Gamma_{p_0}(\mathcal{M})$ if and only if $A \cup \{p_0\}$ is a circuit of $\mathcal{M}$.

Lemma 3.35. *Let* $\Gamma_{p_0}(\mathcal{M})$ *be a matroid port (and therefore also an access structure). The dual of* $\Gamma_{p_0}(\mathcal{M})$ *(in terms of dual access structures) is the matroid port of the dual matroid* $\mathcal{M}$*, i.e.* $(\Gamma_{p_0}(\mathcal{M}))^* = \Gamma_{p_0}(\mathcal{M}^*)$*.*

The following connection between ideal access structures and matroid ports was proven by Brickell and Davenport [18, Theorem 1].

Theorem 3.36. *Any ideal access structure is a matroid port.*

In accordance with matroid minors, let us define the minor operations for access structures:

Definition 3.37 (Access Structure Minor)**.** Let $\mathcal{A}$ be an access structure on P and let $X \subseteq P$ be a subset. We define the following two operations on access structures.

- *Restriction:* $\mathcal{A} \setminus X = \{B \subseteq P - X \mid B \in \mathcal{A}\}$
- *Contraction:* $\mathcal{A} \,/\, X = \{B \subseteq P - X \mid B \cup X \in \mathcal{A},\ B \neq \emptyset\}$

Every access structure that can be obtained from $\mathcal{A}$ by a finite sequence of applications of restrictions and contractions is called a *minor* of $\mathcal{A}$.

Remark 3.38. Note the special condition $B \neq \emptyset$ in the definition of contraction. In the special case when $X \in \mathcal{A}$ we would otherwise get $\mathcal{A} \,/\, X = 2^{P-X}$. Since every minor of $\mathcal{A}$ should again be an access structure, we need to exclude the empty set. Also note that in this case every party itself is a qualified set and can reconstruct the secret. The condition $B \neq \emptyset$ is not present in the literature used as source for this thesis. Also, some of them do not explicitly exclude the empty set from access structures.

Similar to Lemma 2.8 and Proposition 2.9, the following properties hold for access structure minors.

Lemma 3.39. *For an access structure $\mathcal{A}$ on the set of participants P and $P_1, P_2 \subseteq P$ disjoint, the following rules for restriction and contraction hold.*

- $(\mathcal{A} \setminus P_1) \setminus P_2 = \mathcal{A} \setminus (P_1 \cup P_2)$ *and* $(\mathcal{A} \,/\, P_1) \,/\, P_2 = \mathcal{A} \,/\, (P_1 \cup P_2)$
- $(\mathcal{A} \setminus P_1) \,/\, P_2 = (\mathcal{A} \,/\, P_1) \setminus P_2$

Proposition 3.40. *For an access structure $\mathcal{A}$ on the set of participants P, every minor of $\mathcal{A}$ can be written as $(\mathcal{A} \setminus P_1) \,/\, P_2$ with $P_1, P_2 \subseteq P$ disjoint.*

Lemma 3.41. *Let $Q = \{p_0, \ldots, p_n\}$, $P = Q - \{p_0\}$, $\mathcal{M} = (Q, r)$ a matroid, $\Gamma_{p_0}(\mathcal{M})$ the port of $\mathcal{M}$ at point p_0 and $A \subseteq P$ a subset of the set of participants. Then, $\Gamma_{p_0}(\mathcal{M}) \setminus A = \Gamma_{p_0}(\mathcal{M} \setminus A)$ and $\Gamma_{p_0}(\mathcal{M}) \,/\, A = \Gamma_{p_0}(\mathcal{M} \,/\, A)$.*

Remark 3.42. The two minor operations on access structures have an intuitive meaning when talking about secret sharing. Let $\mathcal{A}$ be an access structure on P and $B \subseteq P$. If the participants in B are removed from the scheme, either they keep their shares secret, or they make them public.
In the first case, the new access structure on $P - B$ corresponds to the restriction $\mathcal{A} \setminus B$, that is, for each qualified set $Q \in \mathcal{A}$ such that $Q \cap B \neq \emptyset$, the set of participants $Q - B$ is not qualified in $\mathcal{A} \setminus B$.
In the second case, it corresponds to $\mathcal{A} \,/\, B$, i.e. for each qualified set $Q \in \mathcal{A}$ such that $Q \cap B \neq \emptyset$, the set of participants $Q - B$ is qualified after contraction.

3.3.2 Idealness of Access Structure Minors

The following result was stated by Martí-Farré et al. [19] without proof, where the authors presented it as a consequence of the natural interpretation of contraction and restriction we have described in Remark 3.42. They also used idealness instead of m-idealness. To the best of our knowledge, a formal proof of this proposition is not available in the literature, so we present one below.

Proposition 3.43. *If an access structure is m-ideal for some $m > 1$, then also every minor of it is m-ideal.*

Proof. Let $P = \{p_1, \ldots, p_n\}$ be a set of participants and $\mathcal{A} \subseteq 2^P - \{\emptyset\}$ an access structure. Let $\Sigma = \langle \Pi, \mu \rangle$ be an m-ideal secret sharing scheme realizing $\mathcal{A}$, with reconstruction function Λ_Q for each qualified set $Q \in \mathcal{A}$. Denote by s_i the share of participant p_i for $i = 1, \ldots, n$.

Consider the minor $\mathcal{A}' = \mathcal{A} \setminus \{p_n\}$ on the set of participants $P' = P - \{p_n\}$. We will construct a secret sharing scheme $\Sigma' = \langle \Pi', \mu' \rangle$ from Σ such that Σ' realizes $\mathcal{A}'$, using the same domain of secrets and domains of shares as Σ. Let $\mu' = \mu$ and define

$$\Pi'(s, r) = \Pi_{P'}(s, r)$$
$$\Lambda'_Q(s_{i_1}, \ldots, s_{i_{|Q|}}) = \Lambda_Q(s_{i_1}, \ldots, s_{i_{|Q|}}) \text{ for each } Q \in \mathcal{A}''.$$

Correctness: Let $Q \in \mathcal{A}'$. Then,

$$\begin{aligned} \mathbb{P}\big[\Lambda'_Q(\Pi'_Q(s, r)) = s\big] &= \mathbb{P}\big[\Lambda_Q((\Pi_{P'})_Q(s, r)) = s\big] \\ &= \mathbb{P}\big[\Lambda_Q(\Pi_Q(s, r)) = s\big] \\ &= 1, \end{aligned}$$

where the first equality follows from the definitions of Π' and Λ', the second one from $Q \subseteq P'$ and the third one from correctness of Σ.

Perfectness: Let $U \notin \mathcal{A}'$ be an unqualified set, $(s_j)_{p_j \in U}$ any vector of shares for U and a, b any two secrets. Then,

$$\mathbb{P}\big[\Pi'_U(a, r) = (s_j)_{p_j \in U}\big] = \mathbb{P}\big[(\Pi_{P'})_U(a, r) = (s_j)_{p_j \in U}\big] = \mathbb{P}\big[(\Pi_U(a, r) = (s_j)_{p_j \in U}\big],$$
$$\mathbb{P}\big[\Pi'_U(b, r) = (s_j)_{p_j \in U}\big] = \mathbb{P}\big[(\Pi_{P'})_U(b, r) = (s_j)_{p_j \in U}\big] = \mathbb{P}\big[(\Pi_U(b, r) = (s_j)_{p_j \in U}\big].$$

By perfectness of Σ, the last terms in each line are equal and, hence, we get that $\mathbb{P}\big[\Pi'_U(a, r) = (s_j)_{p_j \in U}\big] = \mathbb{P}\big[\Pi'_U(b, r) = (s_j)_{p_j \in U}\big]$, which shows perfectness of Σ'.

m-idealness: This is trivially given since the domains of secrets and shares stay the same for Σ' like they are for Σ which by assumption is m-ideal.

Now consider the minor $\mathcal{A}'' = \mathcal{A}/\{p_n\}$ on the set of participants $P' = P - \{p_n\}$. Again, we will construct a secret sharing scheme $\Sigma'' = \langle \Pi'', \mu'' \rangle$ from Σ such that Σ'' realizes $\mathcal{A}''$ and uses the same domain of secrets and domains of shares like Σ. Let $\mu'' = \mu$ and define

$$\Pi''(s, r) = \Pi_{P'}(s, r)$$
$$\Lambda''_Q(s_{i_1}, \ldots, s_{i_{|Q|}}) = \Lambda_{Q \cup \{p_n\}}\big(s_{i_1}, \ldots, s_{i_{|Q|}}, \Pi(s, r)_n\big) \text{ for each } Q \in \mathcal{A}''.$$

Perfectness and m-idealness of Σ'' is shown the same way as perfectness and idealness of Σ' above since $\Pi'' = \Pi'$.

For correctness, let $Q \in \mathcal{A}''$. Recall that this implies that $Q \cup \{p_n\} \in \mathcal{A}$. Then,

$$\begin{aligned} \mathbb{P}\big[\Lambda''_Q(\Pi''_Q(s, r)) = s\big] &= \mathbb{P}\big[\Lambda_{Q \cup \{p_n\}}\big((\Pi_{P'})_Q(s, r), \Pi(s, r)_n\big) = s\big] \\ &= \mathbb{P}\big[\Lambda_{Q \cup \{p_n\}}(\Pi_{Q \cup \{p_n\}}(s, r)) = s\big] \\ &= 1, \end{aligned}$$

where the first equality follows from the definitions of Π'' and Λ'', the second one from $Q \subseteq P'$ and the third one from correctness of Σ and the fact that $Q \cup \{p_n\} \in \mathcal{A}$.

Note that the above results are not dependent on the choice of p_n among the participants. Indeed, there is no fixed order on the set of participants and, therefore, we can consider any participant as being the last one in the list (see Remark 3.6).

By applying Lemma 3.39, we deduce that every possible minor of $\mathcal{A}$ is m-ideal. □

3.3.3 A Forbidden Minor Characterization

After focusing on ideal schemes, we will now state results which can help disproving idealness of a given access structure.

We make use of the fact that there are families of matroids which are closed under the operation of taking minors [2, 24]. A tool which is therefore frequently used to disprove membership of a matroid to a specific family is called *forbidden minor characterization*. Given a family F of matroids which is closed under the operation of taking minors, the goal is to find a collection of minor-minimal matroids which do not belong to F. Then, if for a matroid $\mathcal{M}$ any matroid of this collection is a minor, $\mathcal{M}$ cannot be in F.

In 1976, before the field of secret sharing has even been invented, Seymour [2] gave a characterization of matroid ports by forbidden minors. By Lemma 3.41, such a forbidden minor characterization can also be achieved for access structures with its minor operation. For this purpose, let us define the access structures Φ, $\widehat{\Phi}$, $\widehat{\Phi}^*$ and Ψ_s for $s \geq 3$ by its minimal sets.

$$\begin{aligned}
&\min(\Phi) = \big\{\{1,2\},\{2,3\},\{3,4\}\big\} && \text{on } P = \{1,2,3,4\}\\
&\min(\widehat{\Phi}) = \big\{\{1,2\},\{2,3\},\{3,4\},\{2,4\}\big\} && \text{on } P = \{1,2,3,4\}\\
&\min(\widehat{\Phi}^*) = \big\{\{1,3,4\},\{2,3\},\{2,4\}\big\} && \text{on } P = \{1,2,3,4\}\\
&\min(\Psi_s) = \big\{\{1,\ldots,s\}\big\} \cup \big\{\{i,s+1\} \mid 1 \leq i \leq s\big\} && \text{on } P = \{1,\ldots,s+1\}, s \geq 3
\end{aligned}$$

Note that this collection is closed under the operation of taking duals (up to isomorphism) since $\Phi^* \cong \Phi$ and $\Psi_s^* = \Psi_s$.

The following result has been stated by Seymour in different words as main theorem of his paper [2] about the forbidden minor characterization of matroid ports.

Theorem 3.44. *An access structure is a matroid port if and only if it has no minor isomorphic to Φ, $\widehat{\Phi}$, $\widehat{\Phi}^*$ or Ψ_s for $s \geq 3$.*

By Theorem 3.44 together with Theorem 3.36, the following corollary is an important tool to show that certain access structures are not ideal.

Corollary 3.45. *If an access structure $\mathcal{A}$ has a minor which is isomorphic to one of Φ, $\widehat{\Phi}$, $\widehat{\Phi}^*$ or Ψ_s for $s \geq 3$, then $\mathcal{A}$ is not ideal.*

Unfortunately, the opposite direction is not true in general. There exist access structures that have none of the four forbidden minors and are therefore matroid

ports, but still have been shown to be non-ideal. Two such examples are the port of the *Vamos* matroid [6] described in Example 2.6 and the *non-Desargues* matroid [14].

3.4 Secret Sharing and Hypergraphs

Next, we connect the theory of secret sharing and matroids with hypergraphs. In particular, hypergraphs are a useful tool to represent and visualize access structures. The hyperedge set of a hypergraph is a collection of subsets of its vertex set, and similarly an access structure is a collection of subsets of its set of participants. By identifying the participants with the vertices of a hypergraph and the minimal sets of the access structure with the hyperedge set, we can uniquely represent each access structure by a hypergraph.

We will misuse some notations from the fields of matroids and secret sharing for hypergraphs. For instance, we will say that a hypergraph H is *ideal* (or *m-ideal*) if H is the representation of an ideal (or m-ideal) access structure $\mathcal{A}$.

We will also introduce the minor operations for hypergraphs. It is important to note that this definition of minors does not correspond to the notion of subhypergraphs, neither are they compatible to the notion of graph minors and its generalization for hypergraphs [25] which are used in graph theory. Instead, we will stay consistent with the minor notation for matroids and access structures.

3.4.1 Hypergraph Minors and Idealness

We start by defining *minimized hypergraphs* which are hypergraphs where no hyperedge is a proper subset of another hyperedge.

Definition 3.46 (Minimized Hypergraph)**.** Let $H = (V, E)$ be a hypergraph. Define $m(H) = (V', E')$, where

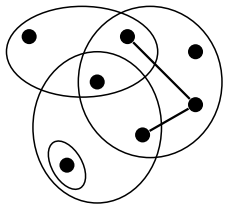
$$E' = \left\{ e \in E \;\middle|\; \text{for all } f \subsetneq e : f \notin E \right\} \quad \text{and} \quad V' = \bigcup_{e \in E'} e.$$

In words, E' is the set of all minimal hyperedges of E and V' is the set of all non-isolated vertices (i.e. all vertices but those which are not part of any hyperedge). A *minimized hypergraph* is a hypergraph H such that $H = m(H)$.

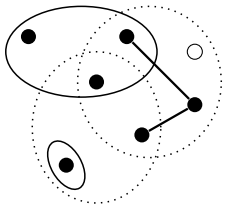
Lemma 3.47. *There is a one-to-one correspondence between the set of access structures and the set of (not necessarily connected) minimized hypergraphs.*

Definition 3.48 (Hypergraph Representing an Access Structure)**.** Let $\mathcal{A}$ be an access structure on the set of participants P. Then, the *hypergraph representing* $\mathcal{A}$ is defined as the hypergraph $HG(\mathcal{A}) = m((P, \mathcal{A}))$ with m being the minimization from Definition 3.46, i.e. the hyperedge set of $HG(\mathcal{A})$ is the collection of minimal sets in the access structure.

Remark 3.49. Note that for an access structure $\mathcal{A}$ on the set of participants P, it holds that $HG(\mathcal{A}) = m((P, \mathcal{A})) = (P, \min(\mathcal{A}))$.



The hypergraph H



The minimized hypergraph $m(H)$

Figure 3.1: Example of a minimization of a hypergraph. Note that two non-minimal hyperedges are removed as well as one vertex which would otherwise be an isolated vertex. The vertex at the very bottom which itself is a 1-hyperedge also stays in the minimized hypergraph.

Remark 3.50. Within this thesis we will always assume that the given hypergraphs are minimized. There is no point in looking at non-minimized hypergraphs in the context of secret sharing since they do not represent access structures according to Definition 3.48.

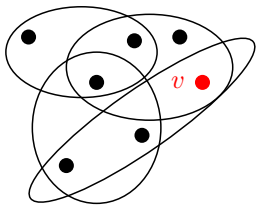
Additionally, if nothing else is stated, for our results we consider only connected hypergraphs. If a hypergraph is not connected, in most cases we apply our results independently to each of the connected components independently.

In accordance with Definitions 2.7 and 3.37 we define the minor operations for hypergraphs:

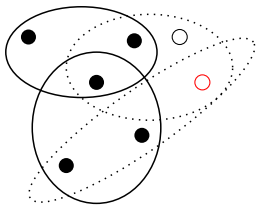
Definition 3.51 (Hypergraph Minor)**.** Let $H = (V, E)$ be a hypergraph and let $W \subseteq V$ be a vertex set. We define the following two operations.

- *Restriction:* $H \setminus W = m\big((V - W, \{e \in E \mid e \cap W = \emptyset\})\big)$
- *Contraction:* $H \,/\, W = m\big((V - W, E')\big)$, where
  $E' = \big\{e \subseteq V - W \;\big|\; e \cup W \supseteq f \text{ for some } f \in E, e \neq \emptyset\big\}$

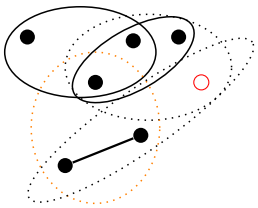
Every hypergraph that can be obtained from H by a finite sequence of application of restrictions and contractions is called a *minor* of H. We write $H' \prec H$ if H' is a minor of H.



Original hypergraph H



Restriction $H \setminus \{v\}$



Contraction $H \,/\, \{v\}$

Figure 3.2: Examples of restriction and contraction of a hypergraph. In both cases we remove the red colored vertex v. Note that with the restriction, a second vertex is removed by the minimization of the minor, while with the contraction, we remove a non-minimal 3-hyperedge. Observe that the subhypergraph $H_{V(H)-\{v\}}$ would look like the contraction $H \,/\, \{v\}$ but without removing this bottom left 3-hyperedge indicated by the orange color.

For illustration purposes, we use dotted lines for hyperedges which are removed or replaced when taking a minor. Removed vertices are drawn as circles which are not filled. See Figure 3.2 for an example.

Lemma 3.52. *For an access structure $\mathcal{A}$, it holds that $HG(\mathcal{A}\setminus B) = HG(\mathcal{A})\setminus B$ and $HG(\mathcal{A} \,/\, B) = HG(\mathcal{A}) \,/\, B$.*

Remark 3.53. In general, taking minors of hypergraphs does not preserve properties like k-uniformness and complete r-partiteness.

We define the following hypergraphs in accordance with the forbidden minors for ideal access structures used in Theorem 3.44. A visualization can be found in Figure 3.3.

$$\Phi = \big(\{1,2,3,4\}, \{\{1,2\},\{2,3\},\{3,4\}\}\big)$$
$$\widehat{\Phi} = \big(\{1,2,3,4\}, \{\{1,2\},\{2,3\},\{3,4\},\{2,4\}\}\big)$$
$$\widehat{\Phi}^* = \big(\{1,2,3,4\}, \{\{1,3,4\},\{2,3\},\{2,4\}\}\big)$$
$$\Psi_s = \big(\{1,\dots,s+1\}, \{\{1,\dots,s\}\} \cup \{\{i,s+1\} \mid 1 \le i \le s\}\big),\ s \ge 3$$

From the context, it will always be clear if we talk about hypergraphs or access structures when using Φ, $\widehat{\Phi}$, $\widehat{\Phi}^*$ or Ψ_s.

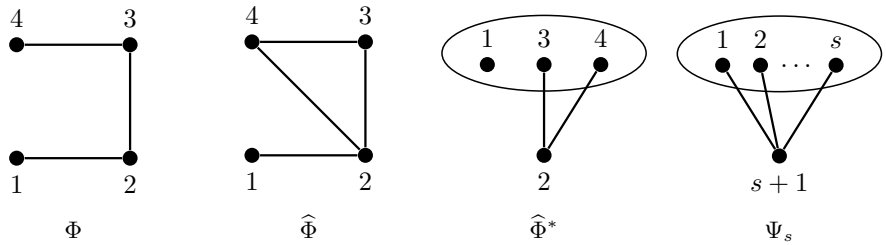


Figure 3.3: The forbidden minors for ideal hypergraphs. By Theorem 3.44, a hypergraph represents a matroid port if and only if it has no minor of one of these forms.

Using Corollary 3.45 together with Lemma 3.52, we derive that a hypergraph which has a minor isomorphic to one of Φ, $\widehat{\Phi}$, $\widehat{\Phi}^*$ or Ψ_s, $s \ge 3$ is not ideal. Sometimes it is tedious to search for them but results like Lemma 3.54 can act as shortcuts.

Lemma 3.54. *Let $H = (V, E)$ be a connected hypergraph. If there exists a pair of vertices $x, y \in V$ such that there is no hyperpath of length 1 or 2 from x to y, then H contains the forbidden minor Φ and is therefore not ideal.*

Proof. Let $H = (V, E)$ be a hypergraph and $x, y \in V$ such that there is no path of length 1 or 2 between them, i.e. there are no hyperedges $e_x, e_y \in E$ such that $x \in e_x$, $y \in e_y$ and $e_x \cap e_y \neq \emptyset$.

Without loss of generality there is a hyperpath from x to y of length 3. Indeed, if the shortest hyperpath from x to y is $(e_0, e_1, \dots, e_p)$, where $p \ge 3$ and $x \in e_0$ and $y \in e_p$, then we can consider the subhyperpath (e_0, e_1, e_2) and replace y by any vertex in $e_2 - e_1$.

Let (e_x, e, e_y) be a shortest hyperpath where $x \in e_x - e$ and $y \in e_y - e$. Since there is no hyperpath from x to y of length less than 3, there exists neither a hyperedge containing x and some vertex in e_y, nor a hyperedge containing y and some vertex in e_x.

Let $s \in e_x \cap e$, $t \in e_y \cap e$, $S = e_x \cup e \cup e_y$ and $T = S \setminus \{x, s, t, y\}$. Consider the minor $(H \setminus S^c) / T$, i.e. we first remove all vertices outside the three hyperedges by restriction and then remove all vertices but x, s, t and y within the three hyperedges by contraction. The resulting graph looks like the one in Figure 3.4.

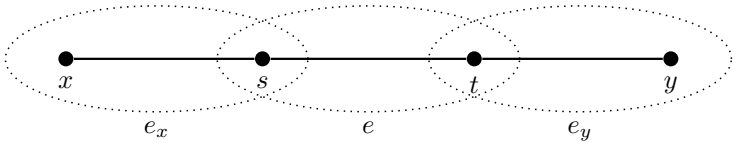


Figure 3.4: The minor $(H \setminus S^c) / T$ corresponds to the forbidden minor Φ.

Indeed, the three edges $\{x, s\}$, $\{s, t\}$ and $\{t, y\}$ remain from the hyperedges e_x, e and e_y, respectively. And since there is no hyperpath of length 1 or 2 from x to y, no other (hyper-)edge can be present in this minor. Hence, H contains the forbidden minor Φ and is therefore not ideal. □

Remark 3.55. Lemma 3.54 is not an "if and only if" statement, i.e. there are hypergraphs containing the forbidden minor Φ but between all pairs of vertices there exists a hyperpath of length strictly less than 3. For instance, consider the hypergraph $H = \big(\{v_1, \dots, v_5\}, \{\{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_4\}, \{v_1, v_4, v_5\}\}\big)$ in Figure 3.5, where $H \setminus \{v_5\}$ corresponds to Φ but for each pair of vertices there is a hyperpath of length strictly less than 3 between them.

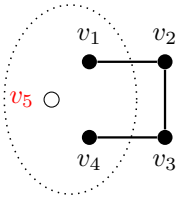


Figure 3.5: In this hypergraph H from Remark 3.55, there is a path of length at most 2 between each pair of vertices. However, its minor $H \setminus \{v_5\}$ is the forbidden minor Φ.

Definition 3.56. We denote by $\mathcal{F}^{(k)}$ the set of connected k-uniform hypergraphs which contain any of Φ, $\widehat{\Phi}$, $\widehat{\Phi}^*$ or Ψ_s for some $s \leq k$ as a minor, i.e.

$$\mathcal{F}^{(k)} = \Big\{ H = (V, E) \;\Big|\; H \text{ connected } k\text{-uniform and } \Phi \prec H \text{ or } \widehat{\Phi} \prec H \text{ or } \widehat{\Phi}^* \prec H \text{ or } \Psi_s \prec H \text{ for some } 3 \leq s \leq k \Big\}.$$

In this thesis we mainly focus on connected hypergraphs. In a non-connected hypergraph most of the results can be applied to each connected component individually. Likewise this is the case when we check for m-idealness.

Lemma 3.57. *A hypergraph H is m-ideal if and only if each connected component of H is m-ideal.*

Proof. First, note that each connected component C of H is a minor of H. Indeed, writing $W = V(H) - V(C)$, we have that $C = H \setminus W$. Therefore, by Proposition 3.43, if a connected component is not m-ideal, then also H is not m-ideal.

For the other direction, assume that each connected component is m-ideal. We need to show that there exists an m-ideal secret sharing scheme realizing H.

We realize this hypergraph by independently sharing the secret among each connected component, i.e. using the m-ideal secret sharing schemes which by assumption exist for each connected component. Clearly the information ratio is 1 and since the schemes are applied independently from each other, also all shares which are not in the same component are independent from each other. Therefore, unqualified sets within one component as well as unions of unqualified sets from different components still have no information about the secret which implies perfectness. □

Remark 3.58. Lemma 3.57 is stated for m-idealness and might be not true for idealness in general. If we have two disjoint hypergraphs H_1 and H_2 and there is no common $m > 1$ such that both of them are m-ideal, then there does not exist any $m > 1$ such that $H := H_1 \cup H_2$ is m-ideal and, therefore, H is not ideal.

Not much is known about a characterization of ideal hypergraphs or even ideal k-uniform hypergraphs. But we can show the idealness of a certain family of k-uniform hypergraphs.

Proposition 3.59. *Any complete multipartite k-uniform hypergraph is linearly ideal.*

Proof. Let $H = K^{(k)}_{n_1,\dots,n_r}$ be the complete r-partite k-uniform hypergraph for $2 \leq k \leq r$, with vertex partition $V = V_1 \cup \ldots \cup V_r$ such that $|V_i| = n_i$ for $i = 1, \dots, r$. We claim that this hypergraph is realizable by a slight variation of a (k, r)-threshold scheme like Shamir's secret sharing scheme.

Indeed, we use such a scheme to split the secret s into shares $s_1, \dots, s_r$. We then send the share s_i to all n_i participants in V_i for $i = 1, \dots, r$. Recall that k of the r shares are needed to reveal the secret. Therefore, a vertex set $Q \subseteq V$ is qualified if and only if $\left|\left\{i \in \{1, \dots, r\} \mid Q \cap V_i \neq \emptyset\right\}\right| \geq k$.

Recall that Shamir's threshold scheme is linear with the distribution function given by a Vandermonde matrix by Proposition 3.29. It is easy to verify that, if we use the same share for multiple participants, this is still a linear mapping.

Hence, this linear ideal scheme realizes $K^{(k)}_{n_1,\dots,n_r}$. □

3.4.2 Ideal Graph-Based Access Structures

This section discusses known results about graphs in combination with secret sharing. In particular, the most relevant result is a characterization of all ideal

graphs which we state in Theorem 3.66. This characterization has been introduced by Brickell and Davenport [18, Theorem 4]. The proof we give is an elaboration of the one given by Ligeti [26, Proposition 1] which is closer to our notations.

Remark 3.60. Using Theorem 3.44, in order to know if a graph represents a matroid port, we only need to check that it has none of the two forbidden minors Φ and $\widehat{\Phi}$. Indeed, $\widehat{\Phi}^*$ and Ψ_s for $s \geq 3$ contain hyperedges of size larger than 2 and, therefore, they cannot be minors of a graph.

Remark 3.61. For a graph $G = (V, E)$ and a vertex set $A \subseteq V$ the subgraph G_A (according to Definition 2.19) is equal to the minor $G \setminus (V - A)$. That is, each subgraph is also a minor.

The following results are easy to verify by just applying the respective definitions. We therefore omit some of the proofs.

Lemma 3.62. *Let $G = (V, E)$ be a graph and $A \subseteq V$. Then, $\overline{(G_A)} = (\overline{G})_A$, i.e. the complement of the subgraph induced by A equals the subgraph induced by A of the complement. In particular, G' is a subgraph of G if and only if $\overline{G'}$ is a subgraph of $\overline{G}$.*

Lemma 3.63. *A connected graph G is the complete r-partite graph $K^{(2)}_{n_1,\ldots,n_r}$ if and only if its complement $\overline{G}$ is a graph with r connected components, where for $i = 1, \ldots, r$ the i-th component is either a complete graph $K^{(2)}_{n_i}$ on the vertex set V_i or $|V_i| = 1$ in which case the component is an isolated vertex.*

Lemma 3.64. *A connected graph G is complete if and only if it has no subgraph of the form $P_3 = \big(\{1, 2, 3\}, \{\{1, 2\}, \{2, 3\}\}\big)$, i.e. the path with three vertices.*

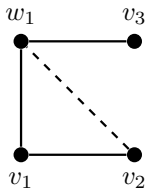
Lemma 3.65. *Let $\overline{P_3}$ be the graph $\big(\{v_1, v_2, v_3\}, \{\{v_1, v_2\}\}\big)$. For a connected graph G, if $\overline{P_3}$ is a subgraph of G (according to Definition 2.19), then either Φ or $\widehat{\Phi}$ is a subgraph of G too.*

Proof. Let $G = \big(\{v_1, \ldots, v_n\}, E\big)$ be a connected graph with $\overline{P_3}$ as a subgraph. Without loss of generality we may assume that this is the subgraph $G_{\{v_1,v_2,v_3\}} = \big(\{v_1, v_2, v_3\}, \{\{v_1, v_2\}\}\big)$. Otherwise, just relabel the vertices of G.

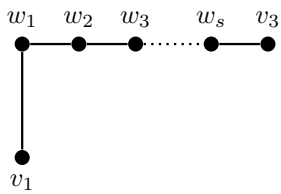
Let $\big(\{v_1, w_1\}, \{w_1, w_2\}, \ldots, \{w_{s-1}, w_s\}, \{w_s, v_3\}\big)$ be a path in G from vertex v_1 to vertex v_3 such that there is no shorter path from v_1 to v_3. Without loss of generality, the vertex v_2 is not in this path. Otherwise, we can use the same reasoning for the sub-path from v_2 to v_3.

We now distinguish two cases:

- $s = 1$, i.e. the path from v_1 to v_3 is $\big(\{v_1, w_1\}, \{w_1, v_3\}\big)$. This yields two possibilities for the minor $\big(G \setminus (V - \{v_1, v_2, v_3, w_1\})\big)$, either Φ or $\widehat{\Phi}$, as illustrated in Figure 3.6(a).
- $s > 1$, i.e. the shortest path from v_1 to v_3 has length at least 2. In this case, together with vertex v_2, the minor $\big(G \setminus (V - \{v_1, w_1, w_2, w_3\})\big)$ is Φ (if $s = 2$ we set $w_3 = v_3$). See Figure 3.6(b) for an illustration. Note that no other edge can be in this minor from the condition that there is no shorter path from v_1 to v_3.



(a) If $s = 1$, depending on whether $\{v_2, w_1\} \in E$, we have one of the minors Φ or $\widehat{\Phi}$.



(b) If $s > 1$, in any case we have a minor Φ if we consider the first three edges of the path from v_1 to v_3.

Figure 3.6: Illustrations for the proof of Lemma 3.65. The graphs only show the vertices which are involved in the proof. All other vertices are eliminated using restriction.

This completes the proof. □

Theorem 3.66. *A connected graph G is ideal if and only if $G \in \mathcal{K}^{(2)}$.*

Proof. First, we already know that each complete multipartite graph is ideal by Proposition 3.59. It can be realized by a $(2, r)$-threshold scheme like Shamir's secret sharing scheme, where each of the r parts in the partition is assigned one of the shares and each vertex in this part gets the same share.

It remains to show that any graph which is not complete multipartite cannot be ideal. By Lemma 3.63 at least one of the connected components in the complement $\overline{G}$ is not complete. By Lemma 3.64, P_3 is a subgraph of this component in $\overline{G}$ and, by Lemma 3.62, $\overline{P_3}$ is a subgraph of G. We conclude that Φ or $\widehat{\Phi}$ is a minor of G and, therefore, G cannot be ideal. □

A linear-time algorithm which verifies if a given connected graph is ideal is discussed in Appendix A.1.

Corollary 3.67. *A graph G is ideal if and only if each connected component of G is complete multipartite.*

Proof. Let G be a graph with connected components $G_1, \ldots, G_t$, where G_i is complete r_i-partite for $i \in \{1, \ldots, t\}$. In particular, G_i is q_i-ideal for any prime power $q_i > n_i$, by Proposition 3.29 and since we can realize it by a $(2, n_i)$-threshold scheme. Therefore, let q be a prime power such that $q > n_i$ for each $i \in \{1, \ldots, t\}$. All connected components of G are q-ideal and, therefore, so is G.

For the other direction, observe that each connected component of G is a minor of G and, therefore, by Proposition 3.43 each of them has to be ideal if G is. □

Corollary 3.68. *Any star is ideal.*

Remark 3.69. While Theorem 3.66 characterizes all ideal graphs, we can similarly state that all 1-uniform hypergraphs are trivially ideal. Indeed, any 1-uniform hypergraph has the form $\big(V, \{\{v\} \mid v \in V\}\big)$ which is realized just by sending the secret to each participant $v \in V$.

In the course of this thesis we will see that for general k-uniform hypergraphs only one direction of Theorem 3.66 is true since there exist ideal uniform hypergraphs which are not complete multipartite.

Furthermore, there is a more involved characterization of general ideal uniform hyperstars than for stars. This topic is discussed in Section 5.2.

Chapter 4

Constructing Ideal Uniform Hypergraphs

In this chapter we will introduce two new families of ideal uniform hypergraphs which are composed of other uniform hypergraphs. We will start in Section 4.1 by defining the *region-expansion* operation which combines two given hypergraphs and has a natural interpretation in terms of secret sharing. Afterwards, in Section 4.2 we will use this operation to construct a new family of ideal uniform hypergraphs from other uniform hypergraphs, called *simple nexus of uniforms*. Section 4.3 then provides the definition of *nexuses of uniforms*, which also contains the complete multipartite hypergraphs and is therefore the collection of all ideal k-uniform hypergraphs we discuss in this thesis.

From now on, if in any result we use multiple hypergraphs and nothing else is stated, we assume that they are disjoint. That is, they do not have common vertices. We emphasize on this fact by writing $A \sqcup B$ instead of $A \cup B$ for the union of disjoint sets A and B. However, this does not mean that $A \cup B$ cannot be a disjoint union too.

4.1 The Region-Expansion Operation

4.1.1 Definition and Basic Properties

First, let us introduce a new operation on hypergraphs. Given two hypergraphs, we substitute a subset of a region of one hypergraph by the other hypergraph. Formally, the operation is defined as follows:

Definition 4.1 (Region-Expansion)**.** Let $H = (V, E)$ be a hypergraph, $R \subseteq V$ a region of H and $A \subseteq R$ a non-empty vertex set. Let Z be another non-empty hypergraph such that $V(Z) \cap V(H) = \emptyset$. We define the *region-expansion* as the hypergraph $H[A \to Z] = (V', E')$, where $V' = (V - A) \cup V(Z)$ and

$$E' = \big\{e \in E \mid e \cap A = \emptyset\big\} \cup \big\{(e - A) \cup f \mid e \in E, A \subseteq e, f \in E(Z)\big\}.$$

A region-expansion $H' = H[A \to Z]$ is said to be *trivial* if $A = V(H)$ and, therefore, $H' = Z$.

Beimel and Chor gave an example [9, Example 4.3] of an access structure built with a similar operation like the region-expansion, but the set A was a single vertex only. The authors did not elaborate details and the further potential of this operation.

In order to better understand the intuition behind the region-expansion operation, let us make some examples.

Example 4.2. Let $H = K^{(2)}_{1,2} = \big(\{a,b,c\}, \{\{a,b\},\{a,c\}\}\big)$, $A = \{a\}$ a region of H and $Z = \big(\{u,v,w\}, \{\{u\},\{v,w\}\}\big)$. Then, by definition,

$$H[\{a\} \to Z] = \big(\{b,c,u,v,w\}, \{\{b,u\},\{b,v,w\},\{\{c,u\},\{c,v,w\}\}\big).$$

Figure 4.1 is an illustration of this example.

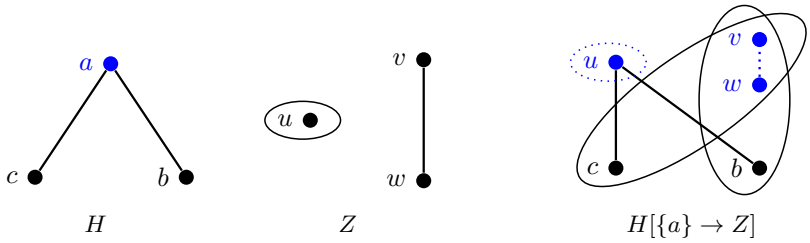


Figure 4.1: In this example, the region $\{a\}$ of the graph H is expanded by the hypergraph Z. The blue dotted hyperedges and edges are not part of $H[\{a\} \to Z]$, they only indicate how Z is inserted as replacement for $\{a\}$.

Example 4.3. Consider a complete hypergraph $K^{(k)}_r$ and let w be in its vertex set. Let $Z = \big(V, \{\{v\} \mid v \in V\}\big)$ for a vertex set V. Then, $K^{(k)}_r[\{w\} \to Z]$ is the complete r-partite hypergraph $K^{(k)}_{|V|,1,\dots,1}$.

Remark 4.4. We will sometimes use region-expansion recursively on different sets of vertices. We always apply the operations from left to right, i.e. writing $H[A_1 \to Z_1][A_2 \to Z_2]$ is equivalent to $(H[A_1 \to Z_1])[A_2 \to Z_2]$, given that $A_1 \subseteq V(H)$ and $A_2 \subseteq V(H[A_1 \to Z_1])$ are subsets of a region in the respective hypergraphs.

The following lemma shows how we can construct complete multipartite hypergraphs by a sequence of region-expansions on a complete hypergraph.

Lemma 4.5. *Let $k \geq 2$ and let $H = K^{(k)}_{n_1,\dots,n_s}$ be the complete multipartite k-uniform hypergraph with independent parts $V_1, \dots, V_s$. Then, H can be written as $H = K^{(k)}_s[\{1\} \to Z_1] \cdots [\{s\} \to Z_s]$, where we choose $V(K^{(k)}_s) = \{1,\dots,s\}$ and $Z_i = \big(V_i, \{\{v\} \mid v \in V_i\}\big)$ for $i = 1,\dots,s$.*

A region-expansion $H[A \to Z]$ can be interpreted in the following way in terms of distribution schemes: we share a secret using the scheme realizing H. The information of the participants in the subset $A \subseteq V(H)$ is then shared between participants in $V(Z)$ by the rules of the scheme realizing Z. This is only possible since all participants in A were in the same region of H. So for each qualified set, either A is a subset of it or none of the participants from A are in it.

Note that if the schemes for H and Z use different domains of secrets and shares, we need to use mappings between them to represent elements within other domains. Furthermore, correctness and perfectness need to be verified for such a new scheme to prove that it is indeed a secret sharing scheme. We will prove this for some specific cases in later results.

Lemma 4.6. *Let H and Z be hypergraphs, $A \subseteq R \subseteq V(H)$ a vertex set, where R is a region of H. Then, $H[A \to Z]$ is a k-uniform hypergraph if and only if Z is l-uniform for some $l \leq k$ and for each hyperedge $e \in E(H)$ it holds that*

$$|e| = \begin{cases} k + |A| - l & \text{if } e \cap A \neq \emptyset \text{ (i.e. } A \subseteq e \text{ and } e \text{ does determine } R) \\ k & \text{if } e \cap A = \emptyset \text{ (i.e. } e \text{ does not determine } R). \end{cases}$$

Proof. Let H and Z be hypergraphs, $A \subseteq R \subseteq V(H)$, where R is a region of H and let $H' = H[A \to Z]$.

First, assume H' is a k-uniform hypergraph. We will prove uniformness of Z and the condition on the size of hyperedges $e \in E(H)$.

Let $e \in E(H)$ such that $A \subseteq e$ and let $f_1, f_2 \in E(Z)$ be two arbitrary hyperedges. Then, $e_1 := (e - A) \sqcup f_1$ and $e_2 := (e - A) \sqcup f_2$ are in $E(H')$. By k-uniformness of H', we derive that

$$k = |e| - |A| + |f_1| = |e| - |A| + |f_2|$$

and, in particular, $|f_1| = |f_2|$. Hence, all hyperedges in Z have the same size and Z is l-uniform for some $l \leq k$. In addition, it directly follows that $|e| = k + |A| - l$.

If $e \in E(H)$ does not determine R (i.e. $e \cap A = \emptyset$) it follows that $e \in E(H')$ since it is not affected by the region-expansion. By k-uniformness, $|e| = k$.

For the other direction of the claim, we now assume that Z is l-uniform and that for each $e \in E(H)$ we have

$$|e| = \begin{cases} k + |A| - l & \text{if } e \cap A \neq \emptyset \\ k & \text{if } e \cap A = \emptyset. \end{cases}$$

Any hyperedge $e' \in E(H')$ either has the form $e' \in E(H)$ if $e' \cap A = \emptyset$ (in which case $|e'| = k$), or $e' = (e - A) \sqcup f$, where $e \in E(H)$ with $A \subseteq e$, and $f \in E(Z)$, (in which case $|e'| = |e| - |A| + l = k$, where the second equality is given by the assumption). Hence, H' is k-uniform proving the statement of the lemma. □

The next lemma shows a connection between region-expansion and contraction of vertices within the same region.

Lemma 4.7. *Let H and Z be hypergraphs, $A \subseteq V(H)$ a subset of a region of H. Let $B \subsetneq A$ and define $H' = H \,/\, B$. Then, $H[A \to Z] = H'[(A - B) \to Z]$.*

Proof. First note that B might be empty (for instance if $|A| = 1$) in which case the claim is trivially true.

With the requirements stated in the lemma, let us define $H_1 = H[A \to Z]$ and $H_2 = H'[(A - B) \to Z]$. We will compare the vertex sets and hyperedge sets of H_1 and H_2 to show their equality.

First, observe that their vertex sets are indeed equal:

$$\begin{aligned} V(H_2) &\overset{\text{def}}{=} \big(V(H') - (A - B)\big) \cup V(Z) \\ &= \big((V(H) - B) - (A - B)\big) \cup V(Z) \\ &= \big(V(H) - A\big) \cup V(Z) \\ &\overset{\text{def}}{=} V(H_1), \end{aligned}$$

where we used that $B \subsetneq A$.

For the hyperedge sets, consider the following sequence of equalities.

$$\begin{aligned} E(H_1) &\overset{\text{def}}{=} \big\{e \in E(H) \;\big|\; e \cap A = \emptyset\big\} \cup \big\{(e - A) \cup f \;\big|\; e \in E(H), A \subseteq e, f \in E(Z)\big\} \\ &\overset{(1)}{=} \big\{e \in E(H') \;\big|\; e \cap A = \emptyset\big\} \cup \big\{(e - A) \cup f \;\big|\; e \in E(H), A \subseteq e, f \in E(Z)\big\} \\ &\overset{(2)}{=} \big\{e \in E(H') \;\big|\; e \cap A = \emptyset\big\} \\ &\quad \cup \big\{((e - B) - (A - B)) \cup f \;\big|\; e \in E(H), A \subseteq e, f \in E(Z)\big\} \\ &\overset{(3)}{=} \big\{e \in E(H') \;\big|\; e \cap A = \emptyset\big\} \\ &\quad \cup \big\{(e' - (A - B)) \cup f \;\big|\; e' \in E(H'), (A - B) \subseteq e', f \in E(Z)\big\} \\ &\overset{\text{def}}{=} E(H_2), \end{aligned}$$

where Equation (1) is true since hyperedges not containing A (and therefore not containing B) are not affected by the contraction $H' = H \,/\, B$, Equation (2) is true since $e - A = (e - B) - (A - B)$ if $B \subsetneq A$ and Equation (3) follows from the fact that B is a subset of a region and it holds that $e \in E(H)$ such that $A \subseteq e$ if and only if $e - B \in E(H')$ and $(A - B) \subseteq (e - B)$.

Having the same vertex set and the same hyperedge set, we deduce that $H_1 = H_2$ which concludes the proof. □

The next result shows that the order of region-expansions does not matter as long as the subsets of regions are in the vertex set of the initial hypergraph and they are pairwise disjoint.

Lemma 4.8. *Let H, Z_1 and Z_2 be hypergraphs, $A_1, A_2 \subseteq V(H)$ subsets of regions of H such that $A_1 \cap A_2 = \emptyset$. Then,*

$$H[A_1 \to Z_1][A_2 \to Z_2] = H[A_2 \to Z_2][A_1 \to Z_1].$$

Proof. First, note that both sides of the equation are well-defined. Indeed, A_2 is a subset of a region in $H[A_1 \to Z_1]$ and A_1 is a subset of a region in $H[A_2 \to Z_2]$ since $A_1 \cap A_2 = \emptyset$.

Denote $H' = H[A_1 \to Z_1][A_2 \to Z_2]$ and $H'' = H[A_2 \to Z_2][A_1 \to Z_1]$. We will show that the vertex sets and hyperedge sets of H' and H'' are equal. We observe that

$$\begin{aligned} V(H') &\overset{\text{def}}{=} \big(((V(H) - A_1) \cup V(Z_1)) - A_2\big) \cup V(Z_2) \\ &= \big(V(H) - (A_1 \cup A_2)\big) \cup \big(V(Z_1) \cup V(Z_2)\big) \\ &= \big(((V(H) - A_2) \cup V(Z_2)) - A_1\big) \cup V(Z_1) \overset{\text{def}}{=} V(H'') \end{aligned}$$

where the two intermediate equalities follow from pairwise disjointness of $V(Z_1)$, $V(Z_2)$, A_1 and A_2.

Moreover, the hyperedge set $E(H')$ is the union of the following four sets.

$$\begin{aligned}
E_1 &= \big\{e \in E(H) \;\big|\; A_1 \cap e = \emptyset, A_2 \cap e = \emptyset\big\} \\
E_2 &= \big\{(e - A_1) \cup f_1 \;\big|\; A_1 \subseteq e, A_2 \cap e = \emptyset, f_1 \in E(Z_1)\big\} \\
E_3 &= \big\{(e - A_2) \cup f_2 \;\big|\; A_2 \subseteq e, A_1 \cap e = \emptyset, f_2 \in E(Z_2)\big\} \\
E_4 &= \big\{(((e - A_1) \cup f_1) - A_2) \cup f_2 \;\big|\; A_1, A_2 \subseteq e, f_1 \in E(Z_1), f_2 \in E(Z_2)\big\} \\
&\overset{(1)}{=} \big\{(((e - A_2) \cup f_2) - A_1) \cup f_1 \;\big|\; A_1, A_2 \subseteq e, f_1 \in E(Z_1), f_2 \in E(Z_2)\big\}
\end{aligned}$$

The order of region-expansion does not influence E_1. In addition, E_2 and E_3 are symmetric to each other and E_4 itself is symmetric as we see from Equation (1) which is a consequence of the fact that A_1, A_2, f_1, f_2 are pairwise disjoint by assumption.

Hence, the vertex sets as well as the hyperedge sets of H' and H'' are equal and, therefore, $H' = H''$. □

Lemma 4.9. *Let H, Z_1 and Z_2 be hypergraphs, $A_1 \subseteq V(H)$ a subset of a region of H and $A_2 \subseteq V(Z_1)$. Then,*

$$H[A_1 \to Z_1][A_2 \to Z_2] = H[A_1 \to Z_1[A_2 \to Z_2]].$$

Proof. Denote $H' = H[A_1 \to Z_1][A_2 \to Z_2]$ and $H'' = H[A_1 \to Z_1[A_2 \to Z_2]]$. Then,

$$\begin{aligned}
V(H') &\overset{\text{def}}{=} \big(((V(H) - A_1) \cup V(Z_1)) - A_2\big) \cup V(Z_2) \\
&= \big(V(H) - A_1\big) \cup \big((V(Z_1) - A_2) \cup V(Z_2)\big) \overset{\text{def}}{=} V(H'')
\end{aligned}$$

where we use that $A_2 \subseteq V(Z_1)$. Moreover, the hyperedge set $E(H')$ is the union of the following three sets.

$$\begin{aligned}
E_1 &= \big\{e \in E(H) \;\big|\; A_1 \cap e = \emptyset\big\} \\
E_2 &= \big\{(e - A_1) \cup f_1 \;\big|\; A_1 \subseteq e, f_1 \in E(Z_1), A_2 \cap f_1 = \emptyset\big\} \\
E_3 &= \big\{(((e - A_1) \cup f_1) - A_2) \cup f_2 \;\big|\; A_1 \subseteq e, f_1 \in E(Z_1), A_2 \subseteq f_1\big\} \\
&= \big\{(e - A_1) \cup ((f_1 - A_2) \cup f_2) \;\big|\; A_1 \subseteq e, f_1 \in E(Z_1), A_2 \subseteq f_1\big\}
\end{aligned}$$

We note that the hyperedge set of H'' is also $E_1 \cup E_2 \cup E_3$. The equality for E_3 is a consequence of $A_2 \subseteq V(Z_1)$.

Hence, the vertex sets as well as the hyperedge sets of H' and H'' are equal and, therefore, $H' = H''$. □

4.1.2 Region-Expansion and Idealness

We now provide a result showing that the region-expansion operation preserves m-idealness.

Theorem 4.10. *Let H and Z be hypergraphs, $A \subseteq V(H)$ a subset of a region of H and let $m > 1$. Then, $H[A \to Z]$ is m-ideal if and only if H and Z are m-ideal.*

Proof. Let $H = (V, E)$ be a hypergraph, R a region of H, $A \subseteq R$ and Z another hypergraph. For now, assume that $A = \{v\}$, i.e. it is only one vertex (the generalization for arbitrary $A \subseteq R$ will be done at the end of the proof). Let s be the secret to share and let s_v be the share of v in the scheme realizing H.

First, assume H and Z are m-ideal, i.e. there are ideal secret sharing schemes Σ_H and Σ_Z realizing H and Z, respectively, with respective domains of secrets D_H and D_Z, both of the same size m. The schemes are independent of each other in the sense that their sets of random strings are chosen independently. We define the distribution scheme Σ as follows: share the secret $s \in D_H$ by using Σ_H, and then further share the share s_v of v by using Σ_Z. We may assume that the domain of shares of v is equal to D_Z. Indeed, we know that at least they both have size m and, if the elements are different, use a 1-to-1 mapping to convert s_v. The inverse of the mapping can be used later when s_v has to be reconstructed from shares in $V(Z)$.

We now need to show correctness, perfectness and m-idealness of this new scheme.

- *Correctness*: For any qualified set $e' \in E(H[\{v\} \to Z])$ it either holds that $e' \cap V(Z) = \emptyset$ or $e' = (e - \{v\}) \cup f$, where $e \in E(H)$ and $f \in E(Z)$ are qualified sets in the respective schemes. In the former case, e can still reconstruct the secret using Σ_H. In the latter case, f can reconstruct s_v by using Σ_Z and togheter with $e - \{v\}$ reveal the secret s using the scheme Σ_H.
- *Perfectness*: Unqualified subsets in $H[\{v\} \to Z]$ still have no information about the secret. Indeed, this is a consequence of the independence of Σ_H and Σ_Z. No set U_Z of participants in $V(Z)$ can add any information to the knowledge of a set of participants U_H in $V(H) - \{v\}$, except if U_Z is qualified in Z and can reveal s_v. But s_v is only useful for U_H if $U_H \cup \{v\}$ is qualified in H, in which case $U_Z \cup U_H$ is qualified in $H[\{v\} \to Z]$. This contradicts the assumption of $U_Z \cup U_H$ being unqualified.
- *m-idealness*: By m-idealness of Σ_H, s_v as well as the shares of participants in $V(H) - \{v\}$ are in a domain of size m and, by m-idealness of Σ_Z, the domains of shares of this new scheme are of size m. Therefore, $H[\{v\} \to Z]$ is also m-ideal.

For the other direction, assume now that $H' = H[\{v\} \to Z] = (V', E')$ is m-ideal. Recall that $V' = (V - \{v\}) \cup V(Z)$ and that

$$E' = \big\{e \in E \;\big|\; v \notin e\big\} \cup \big\{(e - \{v\}) \cup f \;\big|\; e \in E, v \in e, f \in E(Z)\big\}.$$

Let $e \in E(H)$ such that $v \in e$. Then, $Z = (H' \setminus (V(H) - e)) / (e - \{v\})$ is a minor of H'. Hence, m-idealness of H' implies m-idealness of Z by Proposition 3.43.

In order to prove that H is m-ideal, we show that H can be seen as a minor of H' in the following way: let $w \in V(Z)$ be an arbitrary vertex and let

$$N_Z(w) = \big\{v \in V(Z) \;\big|\; \text{ there exists } e \in E(Z) \text{ such that } \{v, w\} \subseteq e \;\big\}$$

be the neighbourhood of w in Z, i.e. the set of all vertices which are adjacent to w (including w itself). Consider the minor

$$M = \big(H' \setminus (V(Z) - N_Z(w))\big) \,/\, \big(N_Z(w) - \{w\}\big).$$

In words, we use restriction to remove all vertices of Z which are not in the neighbourhood of w, and then we use contraction to remove all other vertices of Z except of w. The vertex set of M is given by $V(M) = V - \{v\} \cup \{w\}$, while the hyperedge set is

$$\begin{aligned} E(M) =& \big\{e \in E \;\big|\; v \notin e\big\} \cup \big\{(e - \{v\}) \cup \{w\} \;\big|\; e \in E, v \in e\big\} \\ \cong& \big\{e \in E \;\big|\; v \notin e\big\} \cup \big\{e \in E \;\big|\; v \in e\big\} \\ =& E(H). \end{aligned}$$

Therefore, $M \cong H$ is a minor of H' and m-idealness of H' implies m-idealness of H, by Proposition 3.43.

It remains to show that the implications also hold if $|A| > 1$. Let $A \subseteq V(H)$ be a subset of a region, $v \in A$, define the minor $M_v := H \,/\, (A - \{v\})$ and note that $H[A \to Z] = M_v[\{v\} \to Z]$, by Lemma 4.7. Also observe that we have $H = M_v[\{v\} \to (A, \{A\})]$. Since $(A, \{A\})$ is trivially m-ideal, we conclude that H is m-ideal if and only if M_v is m-ideal if and only if H' is m-ideal, where we use the first part of the proof for both "if and only if's". See Figure 4.2 for an illustration.

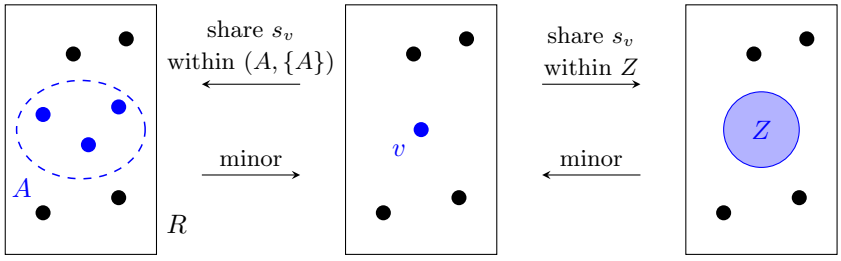


Figure 4.2: All four steps indicated by arrows preserve m-idealness. Therefore, we have that $H = M_v[\{v\} \to (A, \{A\})]$ (left) is m-ideal if and only if M_v (middle) is m-ideal if and only if $H[A \to Z] = M_v[\{v\} \to Z]$ (right) is m-ideal. Note that these sketches only show parts of the respective hypergraphs, not the whole ones.

□

Proposition 4.11. *Let H and Z be two hypergraphs, both realizable by an ideal linear secret sharing scheme over the same finite field $\mathbb{F}_q$, and let $v \in V(H)$. Then, also $H[\{v\} \to Z]$ is realizable by an ideal linear secret sharing scheme over $\mathbb{F}_q$.*

Proof. Let $V(H) = \{v_1, \ldots, v_n\}$ and $V(Z) = \{w_1, \ldots, w_m\}$. Let s be the secret shared in H, t be the secret shared in Z, s_i be the share of v_i in H for $i = 1, \ldots, n$, and let t_j be the share of w_j in Z for $j = 1, \ldots, m$.

Since H and Z realize ideal linear secret sharing schemes over $\mathbb{F}_q$, the shares $(s_1, \ldots, s_n)$ of H and $(t_1, \ldots, t_m)$ of Z can be computed by the linear maps

$$(s_1, \ldots, s_n) = (s, p_1, \ldots, p_k) \cdot \mathbf{A}$$
$$(t_1, \ldots, t_m) = (t, q_1, \ldots, q_l) \cdot \mathbf{B},$$

where $\mathbf{A} = (a_{i,j})_{0 \le i \le k,\, 1 \le j \le n}$ and $\mathbf{B} = (b_{i,j})_{0 \le i \le l,\, 1 \le j \le m}$ are publicly known matrices of size $((k+1) \times n)$ and $((l+1) \times m)$ over $\mathbb{F}_q$, respectively, and $(p_1, \ldots, p_k)$ and $(q_1, \ldots, q_l)$ are random vectors over $\mathbb{F}_q$. Note that, for both $\mathbf{A}$ and $\mathbf{B}$, the row indexed by 0 is related to the secret and the other rows are indexed with the indices of the random elements, respectively.

We now construct a linear scheme realizing the hypergraph $H' = H[\{v_1\} \to Z]$ with vertex set $V(H') = (V(H) - \{v_1\}) \sqcup V(Z) = \{v_2, \ldots, v_n, w_1, \ldots, v_m\}$. We need to show that there exists a matrix $\mathbf{C}$ over $\mathbb{F}_q$ such that the shares can be computed as

$$(s_2, \ldots, s_n, t_1, \ldots, t_m) = (s', r_1, \ldots, r_d) \cdot \mathbf{C},$$

where s' is the secret to share and $(r_1, \ldots, r_d)$ is a random vector. Note that the same can be done for any other $v \in V(H)$ instead of v_1 by just permuting the order of the participants.

We share the secret s' by computing shares $(s_1, \ldots, s_n) = (s', p_1, \ldots, p_k) \cdot \mathbf{A}$ and then share s_1 of v_1 among the participants in Z by computing the vector of shares $(t_1, \ldots, t_m) = (s_1, q_1, \ldots, q_l) \cdot \mathbf{B}$.

In the end, the shares s_j of participants v_j for $j = 2, \ldots, n$ and the shares t_j of participants w_j for $j = 1, \ldots, m$ have the following forms.

$$\begin{aligned}
s_j &= s' \cdot a_{0,j} + \sum_{i=1}^{k} p_i \cdot a_{i,j} \\
t_j &= s_1 \cdot b_{0,j} + \sum_{i=1}^{l} q_i \cdot b_{i,j} \\
&= \left(s' \cdot a_{0,1} + \sum_{i=1}^{k} p_i \cdot a_{i,1} \right) \cdot b_{0,j} + \sum_{i=1}^{l} q_i \cdot b_{i,j} \\
&= s' \cdot a_{0,1} b_{0,j} + \sum_{i=1}^{k} p_i \cdot a_{i,1} b_{0,j} + \sum_{i=1}^{l} q_i \cdot b_{i,j}
\end{aligned}$$

It follows that the vector of shares can be computed as

$$(s_2, \ldots, s_n, t_1, \ldots, t_m) = (s', p_1, \ldots, p_k, q_1, \ldots, q_l) \cdot \mathbf{C}, \text{ where } \mathbf{C} \coloneqq \begin{pmatrix} \mathbf{A'} & \mathbf{a}^T \mathbf{b} \\ \mathbf{0} & \mathbf{B''} \end{pmatrix}$$

and $\mathbf{a} \coloneqq (a_{0,1}, \ldots, a_{l,1})$, $\mathbf{b} \coloneqq (b_{0,1}, \ldots, b_{0,m})$, $\mathbf{A'} \coloneqq (a_{i,j})_{0 \le i \le k,\, 2 \le j \le n}$ is the matrix $\mathbf{A}$ without the first column (indexed by 1) and $\mathbf{B''} \coloneqq (b_{i,j})_{1 \le i \le l,\, 1 \le j \le m}$ is the matrix $\mathbf{B}$ without the first row (indexed by 0).

In this way, each domain of shares in the final scheme is $\mathbb{F}_q$ and the computation of the shares is linear, which completes the proof. □

4.2 Simple Nexuses of Uniforms

In this section we introduce a family of k-uniform hypergraphs for $k \geq 2$, called *simple nexuses of uniforms*, constructed from a set of ideal uniform hypergraphs. We will then show idealness of hypergraphs in this new family as well as some other properties using the fact that simple nexuses of uniforms can be constructed by certain kinds of sequential region-expansions.

4.2.1 Definition and Basic Properties

Definition 4.12. Let $m, s > 1$ and $k_1, \ldots, k_s \geq 1$. Define the families $L^{(m)}_{k_1,\ldots,k_s}$ of hypergraphs by

$$L^{(m)}_{k_1,\ldots,k_s} = \Bigg\{ (V,E) \;\Big|\; \text{for } i \in \{1,\ldots,s\} \text{ there exists } Z_i = (V_i, E_i) \text{ } k_i\text{-uniform and } m\text{-ideal such that } V = \bigsqcup_{i=1}^{s} V_i \text{ and } E = \Big\{ \bigsqcup_{j=1}^{s} e_j \mid e_i \in E_i \Big\} \Bigg\}.$$

Also, define $L_{k_1,\ldots,k_s} = \bigcup_{m>1} L^{(m)}_{k_1,\ldots,k_s}$.

Lemma 4.13. *With $m, s > 1$, for each hypergraph H in $L^{(m)}_{k_1,\ldots,k_s}$ it holds that H is $(k_1 + \ldots + k_s)$-uniform.*

Proof. Let $H \in L^{(m)}_{k_1,\ldots,k_s}$, $e \in E(H)$, $k = k_1 + \ldots + k_s$. By definition, $e = \bigsqcup_{i=1}^{s} e_i$, where $e_i \in E_i$. Therefore, $|e| = |e_1| + \ldots + |e_s| = k_1 + \ldots + k_s = k$ and, hence, H is k-uniform. □

Based on Lemma 4.13 we introduce the following notation for all k-uniform hypergraphs which are members of a family of the form $L_{k_1,\ldots,k_s}$.

Definition 4.14 (Simple Nexus of Uniforms)**.** We say that a hypergraph is a *simple nexus of uniforms* if it belongs to some family $L_{k_1,\ldots,k_s}$ for $s > 1$. For $k \geq 2$, denote the set of k-uniform simple nexuses of uniforms by

$$\mathcal{L}^{(k)} = \bigcup_{\substack{s>1 \\ k_1+\ldots+k_s=k}} L_{k_1,\ldots,k_s}.$$

Remark 4.15. Note that we exclude the trivial case when $s = 1$ since L_k is the set of all (not necessarily connected) k-uniform hypergraphs, by definition. Hence, the family $\mathcal{L}^{(k)}$ can be determined if and only if we know the set of all ideal k'-uniform hypergraphs for each $k' < k$.

Example 4.16. The set $\mathcal{L}^{(2)}$ corresponds exactly to all complete bipartite graphs. Indeed, $\mathcal{L}^{(2)} = L_{1,1}$, i.e. each $H \in \mathcal{L}^{(2)}$ is composed of two 1-uniform hypergraphs with an edge between any two vertices which are not in the same part.

Remark 4.17. Example 4.16 shows that there are ideal k-uniform hypergraphs which are not in $\mathcal{L}^{(k)}$. For instance, in the case $k = 2$, all complete multipartite graphs which are not bipartite are not in $\mathcal{L}^{(2)}$. This result will be discussed more detailed in Proposition 4.25.

Proving the following result is straightforward.

Lemma 4.18. *Let $m, s > 1$, $k_1, \dots, k_s \geq 1$ and let π be any permutation of $\{1, \dots, s\}$. Then, $L^{(m)}_{k_1,\dots,k_s} = L^{(m)}_{k_{\pi(1)},\dots,k_{\pi(s)}}$.*

Proposition 4.19 connects the simple nexuses of uniforms to the region-expansion operation.

Proposition 4.19. *Let $m, s > 1$ and $k_1, \dots, k_s \geq 1$. A hypergraph H is in $L^{(m)}_{k_1,\dots,k_s}$ if and only if it can be written as $H = H'[\{1\} \to Z_1] \cdots [\{s\} \to Z_s]$, where $H' = \big(\{1, \dots, s\}, \{\{1, \dots, s\}\}\big)$ and Z_i is an m-ideal k_i-uniform hypergraph for all $i = 1, \dots, s$.*

Proof. By inductively applying region-expansion we find the following pattern.

$$E\big(H'[\{1\} \to Z_1]\big) = \big\{e_1 \sqcup \{2, \dots, s\} \;\big|\; e_1 \in E(Z_1)\big\}$$
$$E\big(H'[\{1\} \to Z_1][\{2\} \to Z_2]\big) = \big\{e_1 \sqcup e_2 \sqcup \{3, \dots, s\} \;\big|\; e_1 \in E(Z_1), e_2 \in E(Z_2)\big\}$$
$$\dots$$
$$E\big(H'[\{1\} \to Z_1] \dots [\{s\} \to Z_s]\big) = \big\{e_1 \sqcup \dots \sqcup e_s \;\big|\; e_i \in E(Z_i), i = 1, \dots, s\big\}.$$

Therefore, we observe that we can construct exactly all hypergraphs with hyperedge set $\big\{\bigsqcup_{i=1}^{s} e_i \mid e_i \in E_i\big\}$. This corresponds to the hypergraphs in $L^{(m)}_{k_1,\dots,k_s}$. □

4.2.2 Idealness and Related Properties

We now state the main result for simple nexuses of uniforms, namely that every such hypergraph is ideal.

Theorem 4.20. *Let $m, s > 1$ and $k_1, \dots, k_s \geq 1$. For each $H \in L^{(m)}_{k_1,\dots,k_s}$, H is m-ideal.*

Proof. By Proposition 4.19, each hypergraph $H' \in L^{(m)}_{k_1,\dots,k_s}$ can be written as $H[\{1\} \to Z_1] \dots [\{s\} \to Z_s]$, where $H = \big(\{1, \dots, s\}, \{\{1, \dots, s\}\}\big)$ (which is m-ideal by Proposition 3.30 since it corresponds to the (s, s)-threshold access structure) and Z_i is an m-ideal k_i-uniform hypergraph for all $i = 1, \dots, s$. Therefore, by iteratively applying Theorem 4.10, H' is m-ideal. □

Proposition 4.21. *If $k_i \in \{1, 2\}$ for $i = 1, \dots, s$, then each hypergraph in $L_{k_1,\dots,k_s}$ is linearly ideal.*

Proof. Each hypergraph $H' \in L_{k_1,\dots,k_s}$ with $k_i \in \{1, 2\}$ for $i = 1, \dots, s$ has the form $H' = H[\{1\} \to Z_1] \dots [\{s\} \to Z_s]$, where $H = \big(\{1, \dots, s\}, \{\{1, \dots, s\}\}\big)$ is q-ideal for each $q > 1$, by Proposition 3.30, and Z_i is either 1-uniform (i.e. of the form $\big(V, \{\{v\} \mid v \in V\}\big)$ or 2-uniform (i.e. each connected component is a complete multipartite graph). In both cases, Z_i can, in particular, be realized by Shamir's threshold scheme on each connected component over each finite field $\mathbb{F}_q$ with $q \geq |V(Z_i)|$. In particular, each of the connected components is realizable by Shamir over $\mathbb{F}_{q'}$, where q' is a prime power larger than $\max_{1 \leq i \leq s} \big(|V(Z_i)|\big)$. By Propositions 4.11 and 4.19, H' is also linearly ideal over $\mathbb{F}_{q'}$. □

In particular, this result is true for all hypergraphs in $\mathcal{L}^{(3)}$ which we will look at more in detail in Chapter 5.

Next, we derive a result which states that each k-uniform simple nexus of uniforms is in some family $L_{l,k-l}$ for some $1 \leq l < k$.

Proposition 4.22. *Let $s > 1$ and let $k_1, \dots, k_s \geq 1$. Then, it holds that $L_{k_1,\dots,k_s} \subseteq L_{k_1+k_2,k_3,\dots,k_s}$.*

Proof. Let $H \in L_{k_1,\dots,k_s}$, i.e. by definition there exists $Z_i = (V_i, E_i)$ k_i-uniform and m-ideal for $i \in \{1, \dots, s\}$ such that the vertex set and the hyperedge set of H are given by $V(H) = \bigsqcup_{i=1}^{s} V_i$ and $E(H) = \{\bigsqcup_{j=1}^{s} e_j \mid e_i \in E_i\}$, respectively.

Define $Z' = (V', E')$ with $V' = V_1 \sqcup V_2$ and $E' = \{e_1 \sqcup e_2 \mid e_1 \in E_1, e_2 \in E_2\}$. Clearly $Z' \in L^{(m)}_{k_1,k_2}$ and, therefore, Z' is $(k_1 + k_2)$-uniform by Lemma 4.13 and m-ideal by Theorem 4.20.

Also observe that

$$V(H) = \bigsqcup_{i=1}^{s} V_i = V' \sqcup \bigsqcup_{i=3}^{s} V_i \text{ and}$$

$$E(H) = \left\{ e' \sqcup \bigsqcup_{j=3}^{s} e_j \;\middle|\; e_i \in E_i \text{ for all } i = 3, \dots, s \text{ and } e' \in E' \right\}$$

which implies $H \in L_{k_1+k_2,k_3,\dots,k_s}$. □

Corollary 4.23. $\mathcal{L}^{(k)} = \bigcup_{l=1}^{k-1} L_{l,k-l}$.

Proposition 4.24. *Let $k \geq 2$, $H \in \mathcal{L}^{(k)}$, $A \subseteq V(H)$ a subset of a region and Z another hypergraph such that $H' = H[A \to Z]$ is ideal and k-uniform. Then, $H' \in \mathcal{L}^{(k)}$.*

Proof. Note that, by Lemma 4.6, Z needs to be $|A|$-uniform and, by Theorem 4.10, H and Z are both m-ideal for some $m > 1$.

By Corollary 4.23, $H \in L_{l,k-l}$ for some $1 \leq l \leq k-1$. By Proposition 4.19, we can write $H = H''[\{1\} \to Z_1][\{2\} \to Z_2]$, where $H'' = \big(\{1,2\}\{\{1,2\}\}\big)$, Z_1 is ideal l-uniform and Z_2 is ideal $(k-l)$-uniform.

Since $V(H[A \to Z]) = V(Z_1) \sqcup V(Z_2)$, we know that either $A \subseteq V(Z_1)$ or $A \subseteq V(Z_2)$. If $A \subseteq V(Z_2)$, then

$$\begin{aligned} H[A \to Z] &= H''[\{1\} \to Z_1][\{2\} \to Z_2][A \to Z] \\ &= H''[\{1\} \to Z_1][\{2\} \to Z_2[A \to Z]] \end{aligned}$$

where we first substitute H and then apply Lemma 4.9. $Z_2[A \to Z]$ is again ideal $(k-l)$-uniform which yields $H[A \to Z] \in L_{l,k-l}$, by Proposition 4.19.

Similarly, if $A \subseteq V(Z_1)$ we deduce

$$\begin{aligned} H[A \to Z] &= H''[\{1\} \to Z_1][\{2\} \to Z_2][A \to Z] \\ &= H''[\{2\} \to Z_2][\{1\} \to Z_1][A \to Z] \\ &= H''[\{2\} \to Z_2][\{1\} \to Z_1[A \to Z]] \end{aligned}$$

where we use Lemma 4.8 to change the order of the region-expansions and then we use Lemma 4.9. Again we note that $Z_1[A \to Z]$ is ideal l-uniform and, therefore, $H[A \to Z] \in L_{l,k-l}$.

Hence, in any case $H' \in L_{l,k-l} \subseteq \mathcal{L}^{(k)}$ which concludes the proof. □

Next, we show which complete multipartite hypergraphs are simple nexuses of uniforms.

Proposition 4.25. *Let $k \geq 2$ and let H be a hypergraph. Then, it holds that $H \in \mathcal{K}^{(k)} \cap \mathcal{L}^{(k)}$ if and only if H is complete k-partite.*

Proof. First, let $H \in \mathcal{K}^{(k)} \cap \mathcal{L}^{(k)}$. Since $H \in \mathcal{L}^{(k)}$, by Corollary 4.23, $H \in L_{l,k-l}$ for some $1 \leq l \leq k-1$. From Proposition 4.19 we know the H can be written as $H = H'[\{1\} \to Z_1][\{2\} \to Z_2]$, where $H' = \big(\{1,2\}, \{\{1,2\}\}\big)$, Z_1 is m-ideal l-uniform and Z_2 is m-ideal $(k-l)$-uniform for some $m \geq 2$.

Now note that, by definition, $E(H) = \big\{e \sqcup f \;\big|\; e \in E(Z_1),\ f \in E(Z_2)\big\}$. Furthermore, this implies that $H \,/\, V(Z_1) = Z_2$ and $H \,/\, V(Z_2) = Z_1$. Recall that $H \in \mathcal{K}^{(k)}$ as well, i.e. it is complete multipartite with independent parts $V_1, \ldots, V_s$. Note that each V_i is either a subset of $V(Z_1)$ or $V(Z_2)$. Otherwise it would not be independent, since each vertex in $V(Z_1)$ is adjacent to each vertex in $V(Z_2)$.

Since H is k-uniform, Z_1 is l-uniform and Z_2 is $(k-l)$-uniform, we deduce that $\big|\big\{i \in \{1,\ldots,s\} \mid V_i \subseteq V(Z_1)\big\}\big| = l$ and $\big|\big\{i \in \{1,\ldots,s\} \mid V_i \subseteq V(Z_2)\big\}\big| = k-l$ and, therefore, $s = l + (k-l) = k$. This shows that H is complete k-partite.

For the other direction of this proposition's claim, let H be complete k-partite with independent parts $V_1, \ldots, V_k$. Trivially, $H \in \mathcal{K}^{(k)}$. By Lemma 4.5 and Proposition 4.19, it holds that $H \in \mathcal{L}^{(k)}$ and, therefore, $H \in \mathcal{K}^{(k)} \cap \mathcal{L}^{(k)}$. □

Let us now look at two examples of simple nexuses of uniforms.

Example 4.26. With the two graphs $G_1 = \big(\{v_1, v_2, v_3\}, \{\{v_1, v_2\}, \{v_2, v_3\}\}\big)$ and $G_2 = \big(\{w_1, w_2, w_3\}, \{\{w_1, w_2\}, \{w_2, w_3\}\}\big)$ we construct the hypergraph $H = (V, E)$, where $V = V(G_1) \sqcup V(G_2)$ and $E = \big\{e_1 \sqcup e_2 \mid e_1 \in E(G_1), e_2 \in E(G_2)\big\}$. Note that H is 4-uniform and fulfills the conditions of Definition 4.12 for every $m \geq 3$, $s = 2$ and $k_1 = k_2 = 2$. Hence, $H \in L_{2,2}$ and, therefore, $H \in \mathcal{L}^{(4)}$.

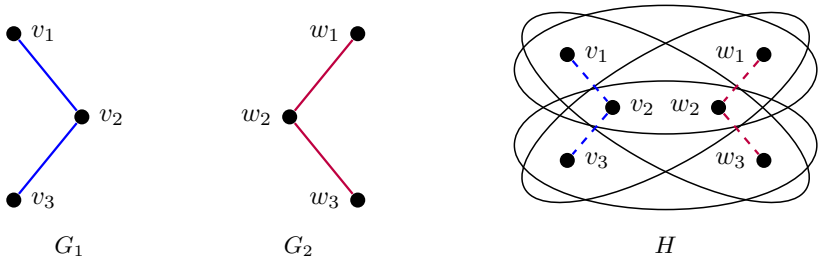


Figure 4.3: The construction of the hypergraph H in Example 4.26, given the two graphs G_1 and G_2. Note how we combine each edge of G_1 with each edge of G_2 to get the four 4-hyperedges in H.

See Figure 4.3 for an illustration. Note that H corresponds to the complete 4-partite 4-uniform hypergraph $K^{(4)}_{2,2,1,1}$ with independent parts $\{v_1, v_3\}$, $\{v_2\}$, $\{w_1, w_3\}$ and $\{w_2\}$.

Example 4.27. Consider the 5-uniform hypergraph $H = (V, E)$ with vertex set $V = \{v_1, v_2, v_3, v_4, w_1, w_2, w_3, w_4\}$ and hyperedge set

$$\begin{aligned} E = \big\{&\{v_1, v_2, v_3, w_1, w_2\}, \{v_1, v_2, v_3, w_3, w_4\}, \{v_1, v_2, v_4, w_1, w_2\}, \\ &\{v_1, v_2, v_4, w_3, w_4\}, \{v_1, v_3, v_4, w_1, w_2\}, \{v_1, v_3, v_4, w_3, w_4\}, \\ &\{v_2, v_3, v_4, w_1, w_2\}, \{v_2, v_3, v_4, w_3, w_4\}\big\}. \end{aligned}$$

Note that H can be written as $H = H'\big[\{1\} \to K_3^{(3)}\big]\big[\{2\} \to K\big]$, where $H' = \big(\{1, 2\}, \{\{1, 2\}\}\big)$, the complete 3-uniform hypergraph $K_3^{(3)}$ has vertex set $\{v_1, v_2, v_3\}$ and K is the union of two complete graphs $K_2^{(2)}$ with vertex sets $\{w_1, w_2\}$ and $\{w_3, w_4\}$, respectively. Therefore, by Proposition 4.19, $H \in \mathcal{L}^{(5)}$.

4.3 Nexuses of Uniforms

We now extend the definition of simple nexuses of uniforms in the sense that we include the complete multipartite hypergraphs which are known to be ideal too. The resulting family is called *nexuses of uniforms*.

Definition 4.28 (Nexus of Uniforms)**.** For a fixed $k \geq 2$, define the family of k-uniform *nexuses of uniforms* $\mathcal{N}^{(k)}$ by

$$\begin{aligned} \mathcal{N}^{(k)} = \Bigg\{ K_r^{(k)}[A_1 \to Z_1] \cdots [A_s \to Z_s] \;\Big|\; & s \geq 2,\, r \geq k, V(K_r^{(k)}) = A_1 \sqcup \ldots \sqcup A_s, \\ & \text{such that each } A_i \text{ is a subset of a region of } K_r^{(k)} \text{ and} \\ & \text{there exists } m > 1 \text{ such that } Z_i \text{ is } m\text{-ideal } |A_i|\text{-uniform, } i = 1, \ldots, s \Bigg\}. \end{aligned}$$

Remark 4.29. We require m-idealness for all Z_i in the definition for a common $m > 1$ so that we can, similar to the proof of Theorem 4.20, show that hypergraphs in $\mathcal{N}^{(k)}$ are ideal.

Remark 4.30. Like for the family of simple nexuses of uniforms (see Remark 4.15) we exclude $s = 1$ in the definition in order to avoid the trivial case where a nexus of uniforms would just equal Z_1 for any ideal k-uniform Z_1. Hence, also the family of k-uniform nexuses of uniforms $\mathcal{N}^{(k)}$ can be determined if and only if we know the set of all ideal k'-uniform hypergraphs for each $k' < k$.

Let us first prove that each simple nexus of uniforms is a nexus of uniforms.

Lemma 4.31. *For $k \geq 2$, $\mathcal{L}^{(k)} \subseteq \mathcal{N}^{(k)}$.*

Proof. Let $H \in \mathcal{L}^{(k)}$, i.e. $H \in L^{(m)}_{l,k-l}$ for some $m > 1$ and $1 \leq l < k$, by Corollary 4.23. By Proposition 4.19 we can write $H = H'[\{1\} \to Z_1][\{2\} \to Z_2]$, where $H' = \big(\{1, 2\}, \{\{1, 2\}\}\big)$, Z_1 is m-ideal l-uniform and Z_2 is m-ideal $(k-l)$-uniform.

We can rewrite H as $H = K_k^{(k)}[A_1 \to Z_1][A_2 \to Z_2]$, where $V(K_k^{(k)}) = A_1 \sqcup A_2$, $|A_1| = l$ and $|A_2| = k - l$. In this way, $|V(K_k^{(k)})| = l + (k - l) = k$ and A_1 and A_2 are both subsets of a region since $K_k^{(k)}$ consists of one hyperedge only and, therefore, it has only one region. By assumption, for $i \in \{1, 2\}$, Z_i is m-ideal and $|A_i|$-uniform and, hence, $H \in \mathcal{N}^{(k)}$, by Definition 4.28. □

Moreover, also complete multipartite hypergraphs are nexuses of uniforms, as the next lemma shows.

Lemma 4.32. *For $k \geq 2$, $\mathcal{K}^{(k)} \subseteq \mathcal{N}^{(k)}$.*

Proof. Let $H \in \mathcal{K}^{(k)}$, i.e. $H = K^{(k)}_{n_1,\dots,n_s}$ for $s \geq k$ and $n_1, \dots, n_s > 0$. Let $V(H) = V_1 \sqcup \dots \sqcup V_s$ be the partition of $V(H)$ into its independent parts. Then, we can write H as $H = K_s^{(k)}[\{1\} \to Z_1] \cdots [\{s\} \to Z_s]$, where $V(K_s^{(k)}) = \{1, \dots, s\}$ and $Z_i = \big(V_i, \{\{v\} \mid v \in V_i\}\big)$ for each $i \in \{1, \dots, s\}$. Note that the 1-uniform hypergraphs Z_i are trivially m-ideal for each $m > 1$. Therefore, $H \in \mathcal{N}^{(k)}$. □

Finally we prove that a hypergraph is a nexus of uniform if and only if it is complete multipartite or a simple nexus of uniforms.

Theorem 4.33. *For $k \geq 2$, $\mathcal{N}^{(k)} = \mathcal{K}^{(k)} \cup \mathcal{L}^{(k)}$.*

Proof. The inclusion $\mathcal{K}^{(k)} \cup \mathcal{L}^{(k)} \subseteq \mathcal{N}^{(k)}$ is proven by Lemmas 4.31 and 4.32.

For the opposite inclusion, let $H \in \mathcal{N}^{(k)}$, i.e. $H = K_r^{(k)}[A_1 \to Z_1] \cdots [A_s \to Z_s]$ for some $m, s > 1$, $r \geq k$, $V(K_r^{(k)}) = A_1 \sqcup \dots \sqcup A_s$ such that each A_i is a subset of a region and Z_i m-ideal and $|A_i|$-uniform for $i = 1, \dots, s$.

First, assume $r = k$. Then, by Proposition 4.19, $H \in L^{(m)}_{|A_1|,\dots,|A_s|}$ since

$$H = K_k^{(k)}[A_1 \to Z_1] \cdots [A_s \to Z_s] = H'[\{1\} \to Z_1] \cdots [\{s\} \to Z_s]$$

with $H' = \big(\{1, \dots, s\}, \{\{1, \dots, s\}\}\big)$, where we apply Lemma 4.7 for each A_i. Therefore, $H \in \mathcal{L}^{(k)}$.

If $r > k$ each region of $K_r^{(k)}$ has size 1 (see Remark 2.42). Hence, each Z_i is 1-uniform and $s = r$ (each A_i has size 1 and their disjoint union is the vertex set of $K_r^{(k)}$, hence, $s \cdot 1 = r$). Therefore, $H = K_s^{(k)}[\{1\} \to Z_1] \cdots [\{s\} \to Z_s]$, where $V(K_s^{(k)}) = \{1, \dots, s\}$ and $Z_i = \big(V_i, \{\{v\} \mid v \in V_i\}\big)$, given non-empty vertex sets V_i for $i = 1, \dots, s$. Hence, H corresponds to the complete s-partite k-uniform hypergraph with independent parts $V_1, \dots, V_s$, i.e. $H \in \mathcal{K}^{(k)}$. □

Corollary 4.34. *For any $k \geq 2$, if $H \in \mathcal{N}^{(k)}$ then H is ideal.*

Unfortunately, the converse is not yet known to be true, i.e. there could be ideal k-uniform hypergraphs which are not nexuses of uniforms.

The following result is similar to Proposition 4.24 but holds for the family $\mathcal{N}^{(k)}$. It shows that the family of k-uniform nexuses of uniforms is closed under region-expansions which preserve idealness and k-uniformness.

Proposition 4.35. *Let $k \geq 2$, $H \in \mathcal{N}^{(k)}$, $A \subseteq V(H)$ a subset of a region and Z another hypergraph such that $H' = H[A \to Z]$ is ideal and k-uniform. Then, $H' \in \mathcal{N}^{(k)}$.*

Proof. By definition, $H = K_r^{(k)}[A_1 \to Z_1] \cdots [A_s \to Z_s]$ for some $m, s > 1$, $r \geq k$, $V(K_r^{(k)}) = A_1 \sqcup \ldots \sqcup A_s$ such that each A_i is a subset of a region and Z_i is m-ideal and $|A_i|$-uniform for $i = 1, \ldots, s$. Furthermore, by Lemma 4.6 and the condition that H' is k-uniform, Z needs to be $|A|$-uniform.

Next, observe that, since the vertex sets A_i are pairwise disjoint, we can arbitrarily change the order of the region-expansions by application of Lemma 4.8, i.e. for each permutation π of $\{1, \ldots, s\}$ it holds that

$$H = K_r^{(k)}[A_{\pi(1)} \to Z_{\pi(1)}] \cdots [A_{\pi(s)} \to Z_{\pi(s)}].$$

Also note that $A \subseteq V(Z_i)$ for a certain $i \in \{1, \ldots, s\}$.

We now show that $H[A \to Z] = K_r^{(k)}[A_1 \to Z_1] \cdots [A_s \to Z_s][A \to Z]$ belongs to $\mathcal{N}^{(k)}$. Let π be any permutation of $\{1, \ldots, s\}$ such that $A \subseteq V(Z_{\pi(s)})$. Then,

$$\begin{aligned} H[A \to Z] &= \big(K_r^{(k)}[A_{\pi(1)} \to Z_{\pi(1)}] \cdots [A_{\pi(s)} \to Z_{\pi(s)}]\big)[A \to Z] \\ &= K_r^{(k)}\big[A_{\pi(1)} \to Z_{\pi(1)}\big] \cdots \big[A_{\pi(s)} \to Z_{\pi(s)}[A \to Z]\big] \end{aligned}$$

where we apply Lemma 4.9.

Observe that $Z_{\pi(s)}[A \to Z]$ is still $|A_{\pi(s)}|$-uniform since Z is $|A|$-uniform. In addition, every other $A_{\pi(i)}$ is replaced by an $|A_{\pi(i)}|$-uniform hypergraph. Hence, it follows that $H[A \to Z] \in \mathcal{N}^{(k)}$. □

Theorem 4.36. *The set of all connected ideal graphs is $\mathcal{N}^{(2)}$.*

Proof. By Theorem 3.66, the set of all connected ideal graphs is $\mathcal{K}^{(2)}$. We will now show that $\mathcal{L}^{(2)} \subseteq \mathcal{K}^{(2)}$ and, therefore, $\mathcal{N}^{(2)} = \mathcal{L}^{(2)} \cup \mathcal{K}^{(2)} = \mathcal{K}^{(2)}$.

Let $H \in \mathcal{L}^{(2)}$, i.e. $H = H'[\{1\} \to Z_1][\{2\} \to Z_2]$, where $H' = \big(\{1,2\}, \{\{1,2\}\}\big)$, $Z_i = \big(V_i, \{\{v\} \mid v \in V_i\}\big)$ for $i \in \{1,2\}$ and non-empty vertex sets V_1, V_2. We observe that H is a bipartite graph and, therefore, $H \in \mathcal{K}^{(2)}$ and thus $\mathcal{L}^{(2)} \subseteq \mathcal{K}^{(2)}$ which concludes the proof. □

Theorem 4.36 implies that the family of 2-uniform nexuses of uniforms corresponds exactly to the set of all ideal connected graphs. Since for $k \geq 3$ we know that $\mathcal{N}^{(k)}$ is a proper superset of $\mathcal{K}^{(k)}$, we found a family of ideal k-uniform hypergraphs which includes the complete multipartite hypergraphs but contains other ideal hypergraphs too.

Let us recall which families of ideal and non-ideal uniform hypergraphs we know by now and how they are connected to each other. For non-ideal hypergraphs we have only used the criterion of not containing any of the forbidden minors Φ, $\widehat{\Phi}$, $\widehat{\Phi}^*$ or Ψ_s for $s \geq 3$, i.e. they are in $\mathcal{F}^{(k)}$.

On the other hand, the families of ideal k-uniform hypergraphs we have looked at are the complete multipartite hypergraphs $\mathcal{K}^{(k)}$ and the simple nexuses of uniforms $\mathcal{L}^{(k)}$, which together form the nexuses of uniforms $\mathcal{N}^{(k)}$.

In Figure 4.4 we show a Venn diagram illustrating the relations between those known families. What remains to show is whether all k-uniform hypergraphs are either a nexus of uniforms or contain a forbidden minor, i.e. whether the gray area in in the Venn diagram is empty or not. For $k = 2$ we know that all graphs are either complete multipartite or contain a forbidden minor. The case $k = 3$ is discussed more in detail in Chapter 5.

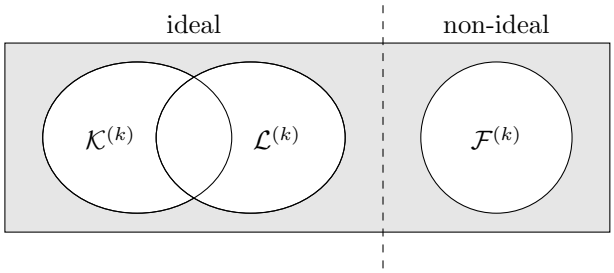


Figure 4.4: Illustration of the connected ideal and non-ideal k-uniform hypergraphs we can characterize so far for $k \geq 2$. Recall that $\mathcal{K}^{(k)} \cup \mathcal{L}^{(k)} = \mathcal{N}^{(k)}$ and that $\mathcal{K}^{(k)} \cap \mathcal{L}^{(k)}$ is the set of all complete k-partite k-uniform hypergraphs. Also note that the sizes of the areas do not represent the sizes of the respective sets.

Chapter 5

On Ideal 3-Uniform Hypergraphs

5.1 3-Uniform Nexuses of Uniforms

We now take a closer look at the families $\mathcal{L}^{(3)}$ and $\mathcal{N}^{(3)}$. Observe that, by Proposition 4.23, $\mathcal{L}^{(3)} = L_{1,2}$ and, therefore, $\mathcal{N}^{(3)} = \mathcal{K}^{(3)} \cup L_{1,2}$. Furthermore, since we know all ideal graphs and 1-uniform hypergraphs, we can fully describe each hypergraph in $\mathcal{L}^{(3)}$ and $\mathcal{N}^{(3)}$. Note that this is not possible for $\mathcal{L}^{(k)}$ for $k > 3$, since we do not have a characterization of all ideal k'-uniform hypergraphs for $k' \geq 3$ so far.

Proposition 5.1 provides an intuitive characterization of $\mathcal{L}^{(3)}$ which is equivalent to Definition 4.12.

Proposition 5.1. *Define the collection of hypergraphs $L'_{1,2}$ as*

$$L'_{1,2} = \Big\{(V,E) \;\Big|\; \text{there exists a vertex set } C \text{ and an ideal graph } G \text{ such that } V = C \sqcup V(G) \text{ and } E = \big\{\{c, v_1, v_2\} \mid c \in C, \{v_1, v_2\} \in E(G)\big\}\Big\}.$$

Then, $L'_{1,2} = L_{1,2}$ and, therefore, $\mathcal{L}^{(3)} = L'_{1,2}$.

Proof. First, let $H \in L'_{1,2}$, i.e. there exists a vertex set C and an ideal graph G such that $V(H) = C \sqcup V(G)$ and $E(H) = \big\{\{c, v_1, v_2\} \mid c \in C, \{v_1, v_2\} \in E(G)\big\}$.

Note that H can be expressed as $H = K^{(2)}_{1,1}\big[\{1\} \to H_C\big]\big[\{2\} \to G\big]$, where $H_C = \big(C, \{\{c\} \mid c \in C\}\big)$ and $K^{(2)}_{1,1} = \big(\{1,2\}, \{\{1,2\}\}\big)$. Hence, we only need to show that there exists an $m > 1$ such that H_C and G are both m-ideal. If this is the case, $H \in L^{(m)}_{1,2}$ and, by definition, $H \in L_{1,2}$.

The graph G is ideal which implies that each connected component is complete multipartite. Therefore, each connected component can independently be realized by Shamir's secret sharing scheme. In particular, each component is realizable by Shamir's scheme over each finite field $\mathbb{F}_q$, where $q > |V(G)|$ is a

prime power. Furthermore, the 1-uniform hypergraph H_C is trivially ideal over any field. Hence, fixing any prime power $m > |V(G)|$, H_C and G are m-ideal and therefore, by Proposition 4.19, $H \in L_{1,2}^{(m)}$ and thus $H \in L_{1,2}$.

Now, let $H \in L_{1,2}$. By definition, there exists an $m > 1$ such that there exist Z_1 1-uniform and Z_2 2-uniform and both m-ideal, $V(H) = V(Z_1) \sqcup V(Z_2)$ and $E(H) = \{e_1 \sqcup e_2 \mid e_1 \in E(Z_1), e_2 \in E(Z_2)\}$. Then, taking $C = V(Z_1)$ and $G = Z_2$, it is easily verified that the vertex set $V(H) = C \sqcup V(G)$ and the hyperedge set $E(H) = \{\{c, v_1, v_2\} \mid c \in C, \{v_1, v_2\} \in E(G)\}$ and, hence, $H \in L'_{1,2}$. □

By Proposition 5.1, each 3-uniform simple nexus of uniforms can be decomposed into two parts: an ideal (not necessarily connected) graph G (i.e. all connected components are complete multipartite) and a non-empty vertex set C, where each pair (c, e) with $c \in C$ and $e \in E(G)$ yields a hyperedge $\{c\} \sqcup e \in E(H)$.

Knowing that from a vertex set and an ideal graph we can uniquely define a hypergraph in $L_{1,2}$, we introduce the following notation.

Definition 5.2. Let C be a set of vertices and G an ideal, not necessarily connected graph. We denote by $L_{1,2}(C, G)$ the hypergraph in $L_{1,2}$ where the vertex set and the hyperedge set are given by $V(L_{1,2}(C, G)) = C \sqcup V(G)$ and $E(L_{1,2}(C, G)) = \{\{c, v_1, v_2\} \mid c \in C, \{v_1, v_2\} \in E(G)\}$, respectively.

By Proposition 5.1, the hypergraphs in $L_{1,2}$ are exactly those which can be written as $L_{1,2}(C, G)$ for some vertex set C and ideal graph G.

Lemma 5.3 provides some fundamental necessary conditions for hypergraphs to be in $L_{1,2}$.

Lemma 5.3. *Let $H = L_{1,2}(C, G)$ for a vertex set C and an ideal graph G. Then, the following properties hold.*

1. *Each vertex $c \in C$ is adjacent to each vertex $v \in V(G)$.*
2. *Each vertex $v \in V(G)$ with degree d in G has degree $d|C|$ in H.*
3. *Each vertex $c \in C$ has the same degree $d = |E(G)|$ in H.*
4. *C is an independent vertex cover of H.*
5. *$G = H \,/\, C$, i.e. $G \prec H$.*

Proof. We prove each property individually:

1. By Corollary 3.67, each connected component of G is in $\mathcal{K}^{(2)}$ and, hence, each vertex $v \in V(G)$ is contained in at least one edge $\{v, w\} \in E(G)$. By the characterization of $L_{1,2}$ in Proposition 5.1, $\{c, v, w\} \in E(H)$ for each $c \in C$ and, therefore, c is adjacent to v.
2. Let $v \in V(G)$ be a vertex with degree d in G, i.e. there are d edges in G which contain v. For each pair (c, e) with $c \in C$ and $e \in E(G)$, $\{c\} \sqcup e$ is a hyperedge in H. Hence, for each edge in G there are $|C|$ hyperedges in H and therefore $d|C|$ hyperedges containing v. Note that H does not contain any hyperedge which is not of that form.

3. For a fixed $c \in C$, the set of hyperedges $e \in E(H)$ such that $c \in e$ is exactly $\big\{\{c, e_1, e_2\} \mid \{e_1, e_2\} \in E(G)\big\}$, which has size $|E(G)|$.
4. Recall that every hyperedge in H has the form $\{c, v_1, v_2\}$ with $c \in C$ and $\{v_1, v_2\} \in E(G)$, i.e. each hyperedge contains exactly one vertex from C. By Lemma 2.39, C is an IVC.
5. It is easy to see that $V(H \,/\, C) = V(H) - C = V(G)$ and that in addition $E(H \,/\, C) = \big\{\{e_1, e_2\} \mid \{e_1, e_2\} \in E(G)\big\} = E(G)$. Hence, $G = H \,/\, C$.

□

In the further course of this thesis, when talking about a 3-uniform simple nexus of uniforms $H = L_{1,2}(C, G)$, we will refer to the vertex set C as *independent vertex cover* (or short: *IVC*) and to G as *graph part* of H.

Let us look at two examples of hypergraphs in $L_{1,2}$ which are both not complete multipartite.

Example 5.4. Consider the hypergraph in Figure 5.1, where $|C| = 2$ and G has two connected components which both are complete multipartite graphs $K^{(2)}_{1,1}$. We can therefore describe the hypergraph as $L_{1,2}(C, K^{(2)}_{1,1} \cup K^{(2)}_{1,1})$, where $|C| = 2$. The hypergraph fulfills the conditions of $L_{1,2}$ and is therefore a nexus of uniform.

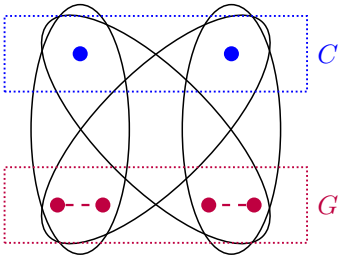


Figure 5.1: The hypergraph $L_{1,2}(C, K^{(2)}_{1,1} \cup K^{(2)}_{1,1})$ from Example 5.4 with independent vertex cover C of size 2 (blue) and graph part H/C (purple).

Example 5.5. Another example of a 3-uniform simple nexus of uniforms is the hypergraph $H = (V, E)$ defined by

$$\begin{aligned} V &= \{w_1, w_2, v_1, v_2, v_3\} \text{ and} \\ E &= \big\{\{w_1, v_1, v_2\}, \{w_1, v_1, v_3\}, \{w_1, v_2, v_3\}, \\ &\qquad \{w_2, v_1, v_2\}, \{w_2, v_1, v_3\}, \{w_2, v_2, v_3\}\big\}. \end{aligned}$$

Let $W = \{w_1, w_2\}$. First, observe that W is an independent vertex cover. Also note that $H/W = \big(\{v_1, v_2, v_3\}, E'\big)$ with $E' = \big\{\{v_1, v_2\}, \{v_1, v_3\}, \{v_2, v_3\}\big\}$, which corresponds to the complete multipartite graph $K^{(2)}_{1,1,1}$ and is therefore ideal. Finally, observe that $E = \big\{\{w\} \sqcup e \mid w \in W \text{ and } e \in E'\big\}$ which implies $H = L_{1,2}(W, K^{(2)}_{1,1,1})$.

In Proposition 5.8 we will see that this decomposition of 3-uniform simple nexuses of uniforms into IVC and graph part is unique with one exception,

namely if G is complete bipartite. Beforehand, we state two lemmas which help proving Proposition 5.8.

Lemma 5.6. *Let $H = L_{1,2}(C, G)$ for a vertex set C and an ideal graph G. Then, for each $C' \subsetneq C$, C' is not an IVC of H.*

Proof. Let $c \in C - C'$ be a vertex and let $\{v_1, v_2\} \in E(G)$, which implies that $e := \{c, v_1, v_2\} \in E(H)$, by Proposition 5.1. Now, for each $c' \in C' \subsetneq C$ we have that $c' \notin V(G)$ and, hence, $c' \notin e$. Therefore, $C' \cap e = \emptyset$ which, by Lemma 2.39, implies that C' is not an IVC. □

Lemma 5.7. *Let $H = L_{1,2}(C, G)$ for a vertex set C and an ideal graph G such that G is not complete bipartite. Let $C' \subseteq V(H)$ such that $C' - C \neq \emptyset$. Then, C' is not an IVC of H.*

Proof. Let us assume that C' is an IVC of H and let $c' \in C' - C$.

First, note that $C' \cap C = \emptyset$. By contradiction, assume that $c \in C \cap C'$. Since $c' \notin C$, we know that $c' \in V(G)$. Hence, c' is adjacent to c, by Property 1 of Lemma 5.3. But this contradicts the independence of C' since both $c, c' \in C'$. Therefore, $C' \cap C = \emptyset$.

Next, we show that G is a connected graph. Indeed, assume there is a connected component in G with vertex set $U \subseteq V(G)$ such that $c' \notin U$. Let $\{u_1, u_2\} \in E(G)$ with $u_1, u_2 \in U$. Then, c' is not adjacent to either of u_1 or u_2, since it is in another connected component of G. Hence, again by Property 1 of Lemma 5.3, both $u_1, u_2 \in C'$. But this contradicts the independence of C' since u_1 and u_2 would be adjacent in this case. Therefore, G must be connected.

We derive from connectedness and idealness of G that G is complete r-partite for some $r \geq 3$ (recall that we exclude the bipartite case in this lemma), by Theorem 3.66. Additionally, since C' is an independent set, C' needs to be one of the r parts in the partition of $V(G)$ into its independent sets. Since there are three or more parts, there is an edge $\{v_1, v_2\} \in E(G)$, where both v_1 and v_2 are not in the same part as c'. But then, $\{c, v_1, v_2\} \in E(H)$ for each $c \in C$. This hyperedge would not contain any vertex in C' which contradicts the fact that C' is a vertex cover.

Hence, C' cannot be a vertex cover which completes the proof. □

Using Lemmas 5.6 and 5.7 we derive the following result.

Proposition 5.8. *Let $H = (V, E)$ be a 3-uniform hypergraph. Then, the following are equivalent.*

1. $H \in \mathcal{K}^{(3)} \cap \mathcal{L}^{(3)}$
2. *H is complete tripartite*
3. *$H = L_{1,2}(C, G)$, where $C \subseteq V$ and $G = H \,/\, C$ is complete bipartite*
4. *H has two different decompositions into IVC and graph part, that is, $H = L_{1,2}(C, H \,/\, C) = L_{1,2}(C', H \,/\, C')$, where $C, C' \subseteq V$ and $C \neq C'$*

Proof. We show various implications between the four statements which ultimately imply their equivalence:

1 $\Leftrightarrow$ 2: True by Proposition 4.25 for $k = 3$.

3 $\Rightarrow$ 2: Since G is complete bipartite, $E(G) = \big\{\{v_1, v_2\} \mid v_1 \in V_1, v_2 \in V_2\big\}$ for some vertex sets V_1 and V_2. Using Definition 5.2, the vertex set of H is given by $E(H) = \big\{\{c, v_1, v_2\} \mid c \in C, v_1 \in V_1, v_2 \in V_2\big\}$ which corresponds to the tripartite hypergraph with partition $V = C \sqcup V_1 \sqcup V_2$.

2 $\Rightarrow$ 4: Since H is a complete tripartite hypergraph, its hyperedge set is given by $E(H) = \big\{\{v_1, v_2, v_3\} \mid v_1 \in V_1, v_2 \in V_2, v_3 \in V_3\big\}$, where $V = V_1 \sqcup V_2 \sqcup V_3$ is the partition of H. By Definition 5.2,

$$E(H) = E\big(L_{1,2}(V_1, H \,/\, V_1)\big) = E\big(L_{1,2}(V_2, H \,/\, V_2)\big) = E\big(L_{1,2}(V_3, H \,/\, V_3)\big).$$

Taking $C = V_1$ and $C' = V_2$, this implication follows.

4 $\Rightarrow$ 3: Assume that there exist vertex sets $C, C' \subseteq V(H)$ with $C \neq C'$ such that $H = L_{1,2}(C, H \,/\, C) = L_{1,2}(C', H \,/\, C')$. From Lemma 5.7 we derive that either G is complete bipartite or $C' - C = \emptyset$. Since by Lemma 5.6 $C' \not\subseteq C$, it follows that $C' - C \neq \emptyset$ and, therefore, G is complete bipartite.

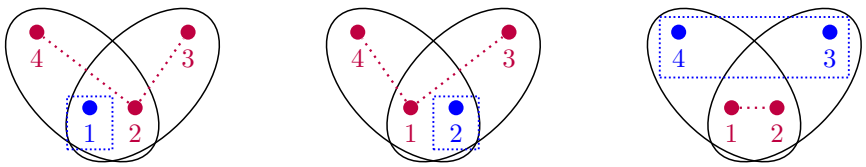
With these implications we have shown the equivalence of the four statements. □

Note that Proposition 5.8 states that the decomposition of any hypergraph $H \in L_{1,2}$ into IVC and graph part is unique except for the case where H is tripartite.

Example 5.9. Here is an example of a 3-uniform hypergraph fulfilling the conditions in Proposition 5.8. Hence, it is tripartite and the decomposition into IVC and graph part is not unique. Let $H = (V, E)$ with $V = \{1, 2, 3, 4\}$ and $E = \{\{1, 2, 3\}, \{1, 2, 4\}\}$. There are three different decompositions, where the first two are isomorphic. See Figure 5.2 for an illustration.

1. IVC $C_1 = \{1\}$, graph part $G_1 = (\{2, 3, 4\}, \{\{2, 3\}, \{2, 4\}\})$
2. IVC $C_2 = \{2\}$, graph part $G_2 = (\{1, 3, 4\}, \{\{1, 3\}, \{1, 4\}\})$
3. IVC $C_3 = \{3, 4\}$, graph part $G_3 = (\{1, 2\}, \{\{1, 2\}\})$

Note that for all three possibilities the graph part is complete bipartite. Also note that the three possible IVCs are pairwise disjoint.



(a) $H = L_{1,2}(C_1, G_1)$ (b) $H = L_{1,2}(C_2, G_2)$ (c) $H = L_{1,2}(C_3, G_3)$

Figure 5.2: Illustration of Example 5.9. The hypergraph H has three different representations in terms of IVC (blue) and graph part (purple).

Theorem 5.10. *Each 3-uniform nexus of uniforms is linearly ideal.*

Proof. We know that $\mathcal{N}^{(3)} = \mathcal{K}^{(3)} \cup \mathcal{L}^{(3)}$. Furthermore, each complete multipartite hypergraph as well as each hypergraph in $L_{1,2}$ is linearly ideal by Propositions 3.59 and 4.21, respectively. This proves the claim. □

From the results in this section we can easily describe each 3-uniform nexus of uniforms either as a complete multipartite 3-uniform hypergraph or as a hypergraph in $L_{1,2}$. We also know that each ideal 3-uniform nexus of uniforms is linearly ideal.

In Appendix A.3 we provide quadratic-time algorithms which check whether a given connected 3-uniform hypergraph H is complete multipartite (Algorithm 4) or a simple nexus of uniforms (Algorithm 5). Combining the two algorithms we can check whether H is a nexus of uniforms.

The next section will use the results on $L_{1,2}$ to characterize all ideal 3-uniform hyperstars.

5.2 Ideal 3-Uniform Hyperstars

Recall from Definition 2.32 that a *hyperstar* is a hypergraph with a non-empty intersection of all its hyperedges, called *center*. We have already seen in Corollary 3.68 that all stars, i.e. 2-uniform hyperstars, are ideal. In this section we give an answer to the question which 3-uniform hyperstars are ideal, which is also the second part of Problem 1 stated by Ligeti [26]. We provide an explicit characterization of all ideal 3-uniform hyperstars, show that they are a special subset of $L_{1,2}$ and eventually provide a polynomial-time algorithm to check whether a given 3-uniform hypergraph is an ideal hyperstar.

We start with a straightforward result that gives a description of any hyperstar by two region-expansions on the complete graph $K_2^{(2)}$.

Lemma 5.11. *Let S be a hyperstar with center C. Then, S can be written as*

$$S = K_2^{(2)}\big[\{1\} \to (C, \{C\})\big]\big[\{2\} \to (S \,/\, C)\big],$$

where $K_2^{(2)} = \big(\{1,2\}, \{\{1,2\}\}\big)$.

Our first main result on hyperstars also applies for general hyperstars but is especially useful for the k-uniform case as we will see in Corollary 5.13 and Theorem 5.15.

Theorem 5.12. *Let S be any hyperstar with center C such that $C \subsetneq V(S)$. Then, S is ideal if and only if $S \,/\, C$ is ideal.*

Proof. If S is ideal then, by Proposition 3.43, $S \,/\, C$ is also ideal.

For the other direction of the claim, assume $S \,/\, C$ is ideal. In particular, it is m-ideal for some $m > 1$. By Lemma 5.11 we can write

$$S = K_2^{(2)}\big[\{1\} \to (C, \{C\})\big]\big[\{2\} \to (S \,/\, C)\big],$$

where $K_2^{(2)} = \big(\{1,2\}, \{\{1,2\}\}\big)$ is the complete graph on two vertices. We observe that $K_2^{(2)}$ and $(C, \{C\})$ are m'-ideal for each $m' > 1$, by Proposition 3.30.

Hence, in particular, all involved hypergraphs are m-ideal and, therefore, S is also m-ideal, by Theorem 4.10. □

Corollary 5.13 is an interesting consequence of Theorem 5.12 in terms of characterizing ideal k-uniform hyperstars.

Corollary 5.13. *For $k \geq 2$, characterizing the ideal k-uniform hyperstars is equivalent to characterizing all ideal k'-uniform (not necessarily connected) hypergraphs for each $k' < k$.*

Proof. Let $k \geq 2$ and $m > 1$ and assume we can characterize all ideal not necessarily connected k'-uniform hypergraphs for $k' < k$. Let S be a hyperstar with center C. By Theorem 5.12, S is ideal if and only if $S \,/\, C$ is ideal. $S \,/\, C$ is a $(k - |C|)$-uniform hypergraph which, by assumption, we can characterize. Therefore, we can say whether S is ideal or not.

For the other direction, assume we can characterize all ideal k-uniform hyperstars and let H be any k'-uniform (not necessarily connected) hypergraph for $k' < k$. Let $H' = (V', E')$, where $V' = V(H) \sqcup C$ with C any vertex set of size $|C| = k - k'$ such that $C \cap V(H) = \emptyset$ and $E' = \big\{C \sqcup e \mid e \in E(H)\big\}$. Clearly, H' is a k-uniform hyperstar with center C which is ideal if and only if $H = H' \,/\, C$ is ideal, by Theorem 5.12. □

Remark 5.14. It is important that in Theorem 5.12 as well as in Corollary 5.13 we need to know idealness of the minor $S \,/\, C$ as a whole, not only idealness of each individual connected component. Indeed, if $S \,/\, C$ has multiple ideal components but there is no common $m > 1$ such that each of them is m-ideal, these results do not apply.

We have seen that all 1-uniform hypergraphs are ideal (Remark 3.69) and that a graph is ideal if and only if each connected component is complete multipartite (Corollary 3.67). Therefore, Theorem 5.15, which is a direct application of Theorem 5.12, provides a characterization of all ideal 3-uniform hyperstars which gives an answer to the second part of Problem 1 stated by Ligeti [26].

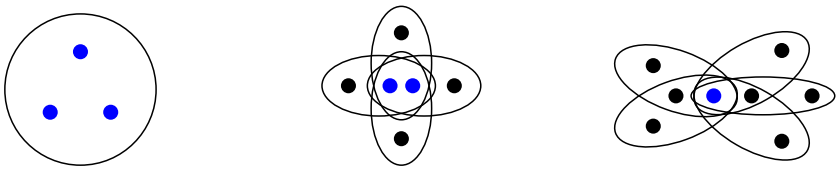
Theorem 5.15. *Let S be a 3-uniform hyperstar with center C. Then, S is ideal if and only if either $|C| \in \{2, 3\}$ or, if $|C| = 1$, each connected component in $S \,/\, C$ is a complete multipartite graph.*

As a corollary we can formulate the following result for any uniform hypergraph.

Corollary 5.16. *For $k \geq 3$, let S be a k-uniform hyperstar with center C such that $k \geq |C| \geq k - 2$. Then, S is ideal if and only if either $|C| \in \{k - 1, k\}$ or, if $|C| = k - 2$, each connected component in $S \,/\, C$ is a complete multipartite graph.*

Having the full characterization of ideal 3-uniform hyperstars in Theorem 5.15, we observe that they are a special subfamily of $L_{1,2}$.

Proposition 5.17. *A 3-uniform hypergraph S is an ideal hyperstar if and only if $S = L_{1,2}(C, G)$ for a vertex set C with $|C| = 1$ and an ideal graph G.*



(a) $|C| = 3$ (b) $|C| = 2$ (c) $|C| = 1$

Figure 5.3: Three examples of how an ideal 3-uniform hyperstar can look like, depending on the size of the center C (blue). Subfigure (a) shows the only possible hypergraph if $|C| = 3$. For $|C| = 2$, Subfigure (b) is an example with 4 hyperedges. There could be arbitrarily many vertices outside the center, each of them in a separate hyperedge together with the center. For the case $|C| = 1$, Subfigure (c) shows the case when $S \,/\, C = K^{(2)}_{1,2} \cup K^{(2)}_{1,3}$, but any ideal graph would be possible outside the center.

Proof. First, let $S = L_{1,2}(\{c\}, G)$ for any vertex c and an ideal graph G. By definition, $V(S) = \big(\{c\} \sqcup V(G)\big)$ and $E(S) = \big\{\{c, v_1, v_2\} \mid \{v_1, v_2\} \in E(G)\big\}$. Therefore, $\{c\}$ is in the intersection of all hyperedges of S, i.e. in the center of S. Note that c is not necessarily the only vertex in the center. If G is a star, the center of G is also in the center of H (see Figure 5.3(b)) and if G is the complete graph $K^{(2)}_2$ then $S \cong K^{(3)}_3$ (see Figure 5.3(a)). In any case, S is an ideal hyperstar.

For the other direction of the claim, let S be an ideal 3-uniform hyperstar and let c be a vertex in the center (which is non-empty since S is a hyperstar). Then, by idealness of S and Proposition 3.43, the minor $G = S \,/\, \{c\}$ is ideal too. Also note that G is a graph since we have removed exactly one vertex from each hyperedge of S. Therefore, $S = L_{1,2}(\{c\}, S \,/\, \{c\})$. □

In Appendix A.2 we provide a polynomial time algorithm which verifies whether a given 3-uniform hypergraph is an ideal hyperstar by using the conditions given in Theorem 5.15.

5.3 3-Uniform Ideal Region-Expansions

We have already seen which ideal 3-uniform hypergraphs can be constructed by region-expansions of certain kinds, namely the families $\mathcal{L}^{(3)}$ and, more generally, $\mathcal{N}^{(3)}$. In these cases, the starting point as well as all intermediate hypergraphs in the construction have always been complete multipartite 3-uniform hypergraphs and the region-expansions preserved this 3-uniformness.

In this section, we discuss the question: Which ideal connected 3-uniform hypergraphs can be obtained from a non-trivial region-expansion $H' = H[A \to Z]$ if we start from a hypergraph H which is itself not 3-uniform? In particular, we show that if the initial hypergraph H is a graph (Proposition 5.24) or a hypergraph containing edges and 3-hyperedges (Proposition 5.23) then any region-expansion from H yielding an ideal 3-uniform hypergraph creates a simple nexus of uniforms.

First we will show that if we have a region-expansion $H' = H[A \to Z]$ such that H' is 3-uniform, we may assume that H does not contain any hyperedge of size larger than 3. Otherwise, the region-expansion can be reduced to some equivalent case where each hyperedge has size smaller or equal to 3. The result is stated for general $k \geq 2$ but will be used later for $k = 3$ only in this thesis.

Lemma 5.18. *For a fixed $k \geq 2$, let H be a hypergraph, $A \subseteq V(H)$ a subset of a region of H, $a \in A$ and let Z be another hypergraph. Define the hypergraphs $H' := H[A \to Z]$ and $H'' := H \,/\, (A - \{a\})$. If H' is a k-uniform hypergraph, then $H' = H''[\{a\} \to Z]$ and for $e \in E(H'')$ it holds that $|e| \leq k$.*

Proof. Fix $k \geq 2$ and let H, $A \subseteq V(H)$ and Z be as required. Let $a \in A$ and $B := A - \{a\}$. Furthermore, define the hypergraph $H'' := H \,/\, B$. Applying Lemma 4.7 we get that $H[A \to Z] = H''[\{a\} \to Z]$. Hence, it only remains to show that for all hyperedges $e \in E(H'')$ it holds that $|e| \leq k$.

Applying Lemma 4.6 to $H[A \to Z]$, we observe that Z is l-uniform for some $l \leq k$. In addition, all hyperedges $e \in E(H)$ with $A \subseteq e$ have size $k + |A| - l$, while all hyperedges $e \in E(H)$ satisfying $A \cap e = \emptyset$ have size k.

Now let $e \in E(H'')$. If $e \cap \{a\} = \emptyset$ then $e \in E(H)$ with $A \cap e = \emptyset$ and, therefore, $|e| = k$. Otherwise, if $a \in e$, let $e' := e \sqcup B \in E(H)$. We know that $|e'| = k + |A| - l$. Since $e = e' - B$, where $B \subset e'$ and $|B| = |A| - 1$, we derive that

$$|e| = |e'| - (|A| - 1) = k + |A| - l - (|A| - 1) = k - l + 1 \leq k,$$

since $l \geq 1$.

Therefore, all hyperedges in H'' have size at most k which proves the claim. □

In this section we focus on the question which 3-uniform ideal hypergraphs can be constructed from any region-expansion $H[A \to Z]$ where H is not 3-uniform. Lemma 5.18 implies that for answering this question we only need to consider initial hypergraphs H where $|e| \leq 3$ for each $e \in H$. Since we exclude the cases when H is 1-uniform (otherwise this would yield a trivial region-expansion) or 3-uniform, we are only left with H containing edges and, possibly, 3-hyperedges. Note that if H contained 1-hyperedges it is either 1-uniform or not connected, so we do not need to consider that case either.

We need a set of lemmas which eventually help proving the main results of this section. As a starting point, Lemma 5.19 is a direct application of Lemma 4.6.

Lemma 5.19. *Let $H = (V, E)$ be a connected hypergraph such that for each $e \in E$ we have that $|e| \in \{2, 3\}$. Furthermore, assume that $\{e \in E \mid |e| = 2\} \neq \emptyset$ and $\{e \in E \mid |e| = 3\} \neq \emptyset$. Let $A \subseteq V$ be a subset of a region and Z a hypergraph such that $H[A \to Z]$ is an ideal 3-uniform hypergraph. Then, $A = \{c\}$ for some $c \in V$ (i.e. $|A| = 1$), Z is an ideal graph and the vertex set V can be uniquely partitioned into disjoint vertex sets $\{c\}$, S and W satisfying*

- $\big\{e \in E \;\big|\; |e| = 2\big\} = \big\{\{c, s\} \;\big|\; s \in S\big\}$
- $\big\{e \in E \;\big|\; |e| = 3\big\} \subseteq \big\{\{v_1, v_2, v_3\} \;\big|\; v_1, v_2, v_3 \in S \sqcup W \text{ pairwise distinct}\big\}$.

We will use the partitioning of the vertex set $V = \{c\} \sqcup S \sqcup W$ of a hypergraph H as in Lemma 5.19 in the subsequent proofs, so it makes sense to take a closer look at it. As shown in Figure 5.4, vertex c together with the vertices in S form a star with center $\{c\}$ and all 3-hyperedges are subsets of $S \sqcup W$.

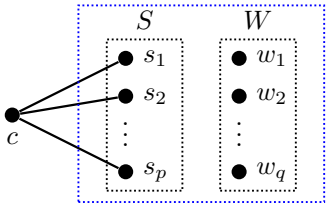
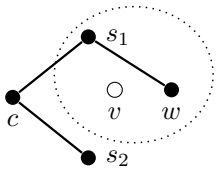


Figure 5.4: Illustration of the partition of a hypergraph H from Lemma 5.19. All 3-hyperedges of H are subsets of size 3 of the vertices within the blue rectangle.

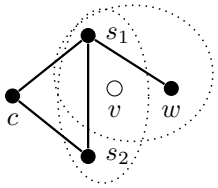
Lemma 5.20. *Let $H = (V - E)$ be an ideal hypergraph with only edges and 3-hyperedges and with the partition of the vertex set $V = \{c\} \sqcup S \sqcup W$ as described in Lemma 5.19. Then, each vertex $w \in W$ is adjacent to each vertex $s \in S$.*

Proof. Let $w \in W$. First, note that w has to be adjacent to at least one vertex in S. Indeed, if not, then, by connectedness of H, the shortest path from c to w has length at least 3 and therefore, by Lemma 3.54, H cannot be ideal.

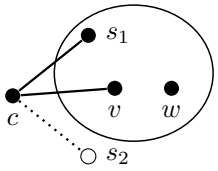
Observe that if w is not adjacent to $s_2 \in S$, but is adjacent to $s_1 \in S$, i.e. $\{w, s_1, v\} \in E(H)$ for some $v \in S \sqcup W$, then H contains a forbidden minor.



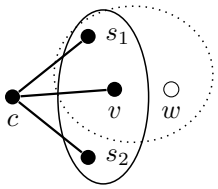
(a) If $v \in W$ and $\{s_1, s_2, v\} \notin E(H)$, then $\big(H \setminus (V - \{c, s_1, s_2, w, v\})\big) / \{v\} \cong \Phi$



(b) If $v \in W$ and $\{s_1, s_2, v\} \in E(H)$, then $\big(H \setminus (V - \{c, s_1, s_2, w, v\})\big) / \{v\} \cong \widehat{\Phi}$



(c) If $v \in S$ and $\{s_1, s_2, v\} \notin E(H)$, then $\big(H \setminus (V - \{c, s_1, s_2, w, v\})\big) \setminus \{s_2\} \cong \widehat{\Phi}^*$



(d) If $v \in S$ and $\{s_1, s_2, v\} \in E(H)$, then $\big(H \setminus (V - \{c, s_1, s_2, w, v\})\big) \setminus \{w\} \cong \Psi_3$

Figure 5.5: Illustration of various cases in the proof of Lemma 5.20. The dotted (hyper-)edges indicate the last contraction or restriction made in the minor.

Indeed, see Figure 5.5 for illustrations of the four cases when either $v \in S$ or $v \in W$ and either $\{s_1, s_2, v\} \in E(H)$ or $\{s_1, s_2, v\} \notin E(H)$. In each case we can find a forbidden minor which contradicts idealness of H. Note that the only

additional hyperedge which could be present in H fulfilling all assumptions is $e := \{s_1, s_2, w_1\}$. However, in none of the four cases the respective minor would change if $e \in E(H)$.

Hence, we conclude that w is adjacent to each $s \in S$. □

Lemma 5.21. *Let $H = (V - E)$ be an ideal hypergraph with only edges and 3-hyperedges and with the partition of the vertex set $V = \{c\} \sqcup S \sqcup W$ as described in Lemma 5.19. Then, for $s, s' \in S$ and $w_1, w_2 \in W$, if $\{s, w_1, w_2\} \in E(H)$ then also $\{s', w_1, w_2\} \in E(H)$.*

Proof. Let $s, s' \in S$ and $w_1, w_2 \in W$ and assume that $\{s, w_1, w_2\} \in E(H)$ but $\{s', w_1, w_2\} \notin E(H)$. Consider the minor

$$M = \big(H \setminus (V - \{c, s, s', w_1, w_2\})\big) \,/\, \{w_2\}$$

as illustrated in Figure 5.6. M is isomorphic to either Φ or $\widehat{\Phi}$, depending on whether or not $\{s, s', w_2\} \in E(H)$. Therefore, H is not ideal which contradicts the assumption. □

(a) If $\{s, s', w_2\} \notin E(H)$, then $M \cong \Phi$ (b) If $\{s, s', w_2\} \in E(H)$, then $M \cong \widehat{\Phi}$

Figure 5.6: Illustration of the proof of Lemma 5.21. The hyperedge $\{s, s', w_1\}$ would not affect the minor, since it would be non-minimal. Note that no other hyperedges can be present in the minor M in both situations due to the given assumptions.

Lemma 5.22. *Let $H = (V - E)$ be an ideal hypergraph with only edges and 3-hyperedges and with the partition of the vertex set $V = \{c\} \sqcup S \sqcup W$ as described in Lemma 5.19. Then, for each $e \in E(H)$, $|e \cap S| = 1$.*

Proof. First, note that the claim is true for all hyperedges of size 2 since they all have the form $\{c, s\}$ for $s \in S$. Hence, we now assume $|e| = 3$. Note that a priori $|e \cap S| \in \{0, 1, 2, 3\}$. We will show that $|e \cap S| \notin \{0, 2, 3\}$ and, therefore, $|e \cap S| = 1$.

If $|e \cap S| = 3$, i.e. $e = \{s_1, s_2, s_3\}$ with $s_1, s_2, s_3 \in S$, then, as illustrated in Figure 5.7(a), $H \setminus \big(V(H) - \{c, s_1, s_2, s_3\}\big)$ is the forbidden minor Ψ_3. No other hyperedge $e' \subseteq \{c, s_1, s_2, s_3\}$ can be in this minor. This contradicts the idealness of H.

Similarly, if $|e \cap S| = 2$, that is, $e = \{s_1, s_2, w\}$ with $s_1, s_2 \in S$ and $w \in W$, then $H \setminus \big(V(H) - \{c, s_1, s_2, w\}\big)$ is the forbidden minor $\widehat{\Phi}^*$ as we see in Figure 5.7(b). No other hyperedge $e' \subseteq \{c, s_1, s_2, w\}$ can be in this minor. This again contradicts the idealness of H.

(a) If $|e \cap S| = 3$, then $\Psi_3 \prec H$ (b) If $|e \cap S| = 2$, then $\widehat{\Phi}^* \prec H$

Figure 5.7: Illustration of the cases when $|e \cap S| \in \{2, 3\}$ in Lemma 5.22.

It remains to show that if $e \cap S = \emptyset$ then H is also non-ideal. So assume there exists a hyperedge $e = \{w_1, w_2, w_3\} \in E(H)$ with $w_1, w_2, w_3 \in W$ and let $s \in S$. By Lemma 5.20 we know that there is a 3-hyperedge $e' \in E(H)$ such that $\{s, w_1\} \subsetneq e'$. For better readability, we will split this part of the proof into different cases:

1. First, consider the case when $e' = \{s, w_1, w_2\} \in E(H)$ (the reasoning for $\{s, w_1, w_3\}$ is analogous). Figure 5.8(a) illustrates the subcase when $\{s, w_1, w_3\}, \{s, w_2, w_3\} \notin E(H)$. Then, the minor

$$M \coloneqq \big(H \setminus (V(H) - \{c, s, w_1, w_2, w_3\})\big) / \{w_2\}$$

   is isomorphic to Φ. Adding $\{s, w_1, w_3\}$ does not change this minor, since $\{s, w_1, w_3\}$ is not minimal in M, and adding $\{s, w_2, w_3\}$ changes M from Φ to $\widehat{\Phi}$ as one can see in Figure 5.8(b). In any of those cases, H contains a forbidden minor and is therefore not ideal.

(a) If $\{s, w_1, w_3\} \notin E(H)$, then $\Phi \prec H$ (b) If $\{s, w_1, w_3\} \in E(H)$, then $\widehat{\Phi} \prec H$

Figure 5.8: Illustration of the two subcases when $|e \cap S| = 0$ and $\{s, w_1, w_2\} \in E(H)$ in the proof of Lemma 5.22.

2. Now consider the other case, namely when $\{s, w_1, w_2\}, \{s, w_1, w_3\} \notin E(H)$. In this case, $e = \{s, w_1, w_4\} \in E(H)$ for some $w_4 \in W$ since w_1 must be adjacent to s by Lemma 5.20 and $w_4 \notin S$ since $|e \cap S| \neq 2$ as we have seen above.

   We will check that no matter which hyperedges are added, there is a forbidden minor in the minor $M \coloneqq H \setminus \big(V(H) - \{c, s, w_1, w_2, w_3, w_4\}\big)$. The base case of this minor with no hyperedges added can be seen in Figure 5.9. Note that the only possible additional hyperedges in this minor are the ones in

$$E_M \coloneqq \big\{\{s, w_2, w_4\}, \{s, w_3, w_4\}, \{w_1, w_2, w_4\}, \{w_1, w_3, w_4\}, \{w_2, w_3, w_4\}\big\}.$$

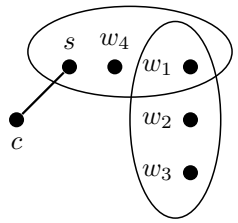
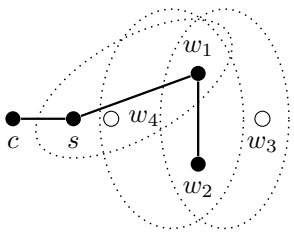


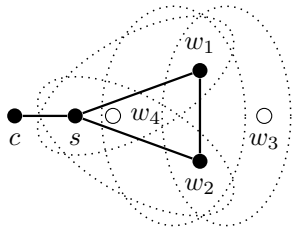
Figure 5.9: Illustration of the minor $MH \setminus \big(V(H) - \{c, v, w_1, w_2, w_3, w_4\}\big)$, used in all subcases of Case 2 if $|e \cap S| = 0$ in the proof of Lemma 5.22.

We split this case into three subcases, where in the first one we assume that $\{w_1, w_2, w_4\} \in E(H)$, in the second one that $\{w_1, w_3, w_4\} \in E(H)$ and in the last one that $\{w_1, w_2, w_4\}, \{w_1, w_3, w_4\} \notin E(H)$.

(a) Assume that $\{w_1, w_2, w_4\} \in E(H)$ and let us consider the minor $M' \coloneqq (M \setminus \{w_3\}) / \{w_4\}$ as illustrated in Figure 5.10. We prove that M' contains a forbidden minor regardless of whether the hyperedge $\{s, w_2, w_4\}$ is present or absent. Indeed, if $\{s, w_2, w_4\} \in E(H)$ then $M' \cong \widehat{\Phi}$ and otherwise $M' \cong \Phi$. Note that the other possible hyperedges in E_M have no effect on those minors if added, since all of them containing w_3 are removed by the restriction and $\{w_1, w_2, w_4\}$ would be dropped as it is not a minimal hyperedge in the minor.



(a) If $\{s, w_2, w_4\} \notin E(H)$, then $\Phi \prec M$



(b) If $\{s, w_2, w_4\} \in E(H)$, then $\widehat{\Phi} \prec M$

Figure 5.10: Illustration of the minor $M' = (M \setminus \{w_3\})/\{w_4\}$, used in Subcase 2a if $|e \cap S| = 0$ in the proof of Lemma 5.22.

(b) The case when $\{w_1, w_3, w_4\} \in E(H)$ is analogous to Case 2a. When replacing w_2 by w_3, the minor $M' \coloneqq (M \setminus \{w_2\}) / \{w_4\}$ is always a forbidden minor.

(c) Now we assume that $\{w_1, w_2, w_4\}, \{w_1, w_3, w_4\} \notin E(H)$. The remaining possible hyperedges of E_M are $\{v, w_2, w_4\}$, $\{v, w_3, w_4\}$ and $\{w_2, w_3, w_4\}$. There are $2^3 = 8$ combinations of these hyperedges (each of them either present or absent) which are summarized in Table 5.1. Each row depicts the case when the minor M (as shown in Figure 5.9) in addition contains the hyperedges marked with an 'x', and which forbidden minor is contained in that case. We deduce that H in any case is non-ideal.

$\{s, w_2, w_4\}$	$\{v, w_3, w_4\}$	$\{w_2, w_3, w_4\}$	Forbidden Minor
			$M \,/\, \{w_3, w_4\} \cong \Phi$
x			$(M \setminus \{c\}) \,/\, \{s\} \cong \widehat{\Phi}^*$
	x		$(M \setminus \{c\}) \,/\, \{s\} \cong \widehat{\Phi}^*$
		x	$(M \setminus \{c\}) \,/\, \{w_2\} \cong \widehat{\Phi}^*$
x	x		$(M \setminus \{c\}) \,/\, \{s\} \cong \Psi_3$
x		x	$(M \setminus \{w_1\}) \,/\, \{w_4\} \cong \Phi$
	x	x	$(M \setminus \{w_1\}) \,/\, \{w_4\} \cong \Phi$
x	x	x	$(M \setminus \{w_1\}) \,/\, \{w_4\} \cong \widehat{\Phi}$

Table 5.1: All possibilities for Case 2c. The basis is the hypergraph M as illustrated in Figure 5.9. For each row, we add the hyperedges marked with an 'x' to this basis hypergraph. The respective resulting hypergraph then contains the forbidden minor given in the last column.

Having covered each possibility, we derive that a hyperedge $\{w_1, w_2, w_3\}$ with $w_1, w_2, w_3 \in W$ cannot exist if H is ideal.

Hence, we have proven that for each $e \in E(H)$, $|e \cap S| \notin \{0, 2, 3\}$ and, therefore, $|e \cap S| = 1$. □

Now, with help of the previous lemmas, we can state the main results of this section. First, Proposition 5.23 shows which ideal 3-uniform hypergraphs exist of the form $H[A \to Z]$ for a hypergraph H which contains edges and 3-hyperedges:

Proposition 5.23. *Let $H = (V, E)$ be a connected hypergraph such that for each $e \in E$ we have that $|e| \in \{2, 3\}$. Furthermore, assume that $\{e \in E \mid |e| = 2\} \neq \emptyset$ and $\{e \in E \mid |e| = 3\} \neq \emptyset$. Let $A \subseteq V$ be a subset of a region and Z a hypergraph such that $H' := H[A \to Z]$ is an ideal 3-uniform hypergraph. Then, $H' \in \mathcal{L}^{(3)}$.*

Proof. By combining Lemmas 5.19, 5.20, 5.21 and 5.22 we know that $A = \{c\}$ for some $c \in V$ and we can partition the vertex set into $V = \{c\} \sqcup S \sqcup W$ such that $E = E_2 \sqcup E_3$, where

- $E_2 := \big\{e \in E \mid |e| = 2\big\} = \big\{\{c, s\} \mid s \in S\big\}$ and
- $E_3 := \big\{e \in E \mid |e| = 3\big\} \subseteq \big\{\{s, w_1, w_2\} \mid s \in S, w_1, w_2 \in W\big\}$ such that for $s, s' \in S$ and $w_1, w_2 \in W$: $\{s, w_1, w_2\} \in E_3 \Rightarrow \{s', w_1, w_2\} \in E_3$.

We will now show that the hypergraph $H \setminus \{c\} = (S \sqcup W, E_3)$ is a 3-uniform simple nexus of uniforms. Indeed, by the conditions for E_3 we observe that $G := (H \setminus \{c\}) / S$ is a graph on the vertex set W. By idealness of H and since $G \prec H$, G is an ideal graph. Hence, $E_3 = \big\{\{s, w_1, w_2\} \mid s \in S, \{w_1, w_2\} \in E(G)\big\}$ which yields $H \setminus \{c\} = L_{1,2}(S, G)$ by the characterization in Proposition 5.1.

Next consider the hypergraph $H' = H[\{c\} \to Z]$. The vertex set of H' is $V(H') = (V(H) - \{c\}) \sqcup V(Z) = S \sqcup W \sqcup V(Z)$, while the hyperedge set

is given by

$$\begin{aligned} E(H') &= E_3 \sqcup \big\{e \sqcup \{s\} \;\big|\; e \in E(Z), s \in S\big\} \\ &= \big\{e \sqcup \{s\} \;\big|\; e \in E(G), s \in S\big\} \sqcup \big\{e \sqcup \{s\} \;\big|\; e \in E(Z), s \in S\big\} \\ &= \big\{e \sqcup \{s\} \;\big|\; e \in E(G) \sqcup E(Z), s \in S\big\}. \end{aligned}$$

Knowing that G and Z are both ideal graphs, we deduce that the resulting hypergraph is $H' = L_{1,2}(S, G \cup Z)$ and, therefore, $H' \in \mathcal{L}^{(3)}$. □

Similar to Proposition 5.23, Proposition 5.24 covers the case of region-expansions of graphs which yield ideal 3-uniform hypergraphs.

Proposition 5.24. *Let G be an ideal connected graph and $v \in V(G)$, Z an ideal hypergraph such that $H := G[\{v\} \to Z]$ is an ideal 3-uniform hypergraph. Then, $H \in \mathcal{L}^{(3)}$.*

Proof. From Lemma 4.6, we derive that v has to be in each edge, i.e. G is a star with center $\{v\}$. Indeed, all hyperedges not determining the region $\{v\}$ need to be 3-hyperedges which are not present by assumption.

With $k = 3$ and $A = \{v\}$, Lemma 4.6 also implies that Z has to be 2-uniform. It follows that $G[A \to Z] = L_{1,2}(V(G) - \{v\}, Z) \in \mathcal{L}^{(3)}$. □

Let us summarize what we have shown in this section. The goal was to check which ideal 3-uniform hypergraphs H' can be constructed from any non-trivial region-expansion $H' = H[A \to Z]$ (i.e. Z is not 3-uniform), starting from different kinds of hypergraphs H which itself are not already 3-uniform. From Lemma 5.18 we know that we only need to consider initial hypergraphs H not containing any k'-hyperedges for $k' > 3$. Indeed, otherwise we can equivalently express the region-expansion starting with another hypergraph H'', where all hyperedges $e \in E(H'')$ have size $|e| \leq 3$.

We have shown in Propositions 5.23 and 5.24 that if H contains any edge and the region-expansion $H' = H[A \to Z]$ is 3-uniform, then H' is a simple nexus of uniforms. We do not need to consider initial hypergraphs H which contain 1-hyperedges since in this case the region-expansion would be trivial which is a case we exclude.

Note that we cannot yet answer the question whether there are other ideal 3-uniform hypergraphs that can be constructed by a region-expansion when starting with a 3-uniform hypergraph H. The problem here is that by choosing $w \in V(H)$ and $Z = \big(\{v\}, \{\{v\}\}\big)$, the region-expansion $H' = H[\{w\} \to Z]$ is isomorphic to H. Hence, this question can only be answered as soon as we know all ideal 3-uniform hypergraphs.

5.4 Counting 3-Uniform Hypergraphs

Let us recall the conditions on idealness and non-idealness that we have seen so far for 3-uniform hypergraphs. We know that the nexuses of uniforms $\mathcal{N}^{(3)}$ are ideal and, hence, all complete multipartite hypergraphs as well as hypergraphs

in $L_{1,2}$ are ideal. On the other hand, hypergraphs containing one of Φ, $\widehat{\Phi}$, $\widehat{\Phi}^*$ or Ψ_3 as a minor are known to be non-ideal.

The goal in this section is to analyze the sizes of these families of 3-uniform hypergraphs if their vertex set has a fixed size n. For hypergraphs on at most five vertices we then check whether each of them is known to be ideal or non-ideal. We will observe that we can by now prove or disprove idealness for all but two such hypergraphs, up to isomorphism.

5.4.1 General 3-Uniform Hypergraphs

We first state some results on 3-uniform hypergraphs on a fixed number of vertices. Unlike in the rest of this thesis, isomorphic hypergraphs are not considered to be equal in this section. This means that we count each representative of any isomorphism class as a separate hypergraph. For instance, there are six representatives of the complete 3-partite 3-uniform hypergraph $K^{(3)}_{1,1,2}$.

For $n \geq 3$ let us denote by $\mathcal{T}^{(3)}_n$ the set of all connected 3-uniform hypergraphs on the vertex set $\{1, \ldots, n\}$ with no isolated vertices, i.e. each vertex lies in at least one hyperedge. We also introduce the corresponding notations for the known families of ideal and non-ideal hypergraphs on a fixed number n of vertices:

$$\mathcal{K}^{(3)}_n := \mathcal{K}^{(3)} \cap \mathcal{T}^{(3)}_n \qquad \mathcal{L}^{(3)}_n := \mathcal{L}^{(3)} \cap \mathcal{T}^{(3)}_n$$
$$\mathcal{N}^{(3)}_n := \mathcal{N}^{(3)} \cap \mathcal{T}^{(3)}_n \qquad \mathcal{F}^{(3)}_n := \mathcal{F}^{(3)} \cap \mathcal{T}^{(3)}_n$$

The Venn diagram in Figure 5.11 depicts the situation with these families for a fixed $n \geq 3$. We see the non-ideal hypergraphs with forbidden minors $\mathcal{F}^{(3)}_n$ on the one hand, and on the other hand the complete multipartite hypergraphs $\mathcal{K}^{(3)}_n$ and the simple nexuses of uniforms $\mathcal{L}^{(3)}_n$. Recall that $\mathcal{K}^{(3)}_n \cup \mathcal{L}^{(3)}_n = \mathcal{N}^{(3)}_n$ and that $\mathcal{K}^{(3)}_n \cap \mathcal{L}^{(3)}_n$ is the set of complete tripartite 3-uniform hypergraphs. The question is whether the gray part outside of these families is empty or not.

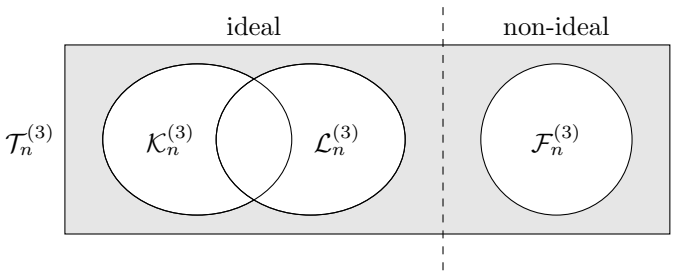


Figure 5.11: Venn diagram illustrating the ideal and non-ideal families of 3-uniform hypergraphs we know so far for a vertex set of fixed size n.

It is not straightforward to derive closed formulas for the sizes of the families $\mathcal{T}^{(3)}_n$, $\mathcal{L}^{(3)}_n$, $\mathcal{N}^{(3)}_n$ and $\mathcal{F}^{(3)}_n$ for arbitrary $n \geq 3$. For $\mathcal{K}^{(3)}_n$, however, we can make use of the Stirling numbers of the second kind to express its size in terms of n.

Lemma 5.25. *Using the Stirling number of the second kind $S(n,r)$, for $n \geq 3$ it holds that*

$$|\mathcal{K}_n^{(3)}| = \sum_{r=3}^{n} S(n,r).$$

Proof. The Stirling number of the second kind $S(n,r)$ counts the number of ways to partition a set of size n into r non-empty unlabelled subsets. This is exactly what we do with the vertices of a complete r-partite hypergraph, namely partitioning them into r non-empty independent vertex sets. For each $3 \leq r \leq n$ we therefore count the number of distinct complete r-partite 3-uniform hypergraphs and sum them up. Note that we exclude $r < 3$ since there are no 3-uniform hypergraphs on less than three vertices. □

For $|\mathcal{T}_n^{(3)}|$ we do not derive a closed formula but only a lower bound which implies that it grows exponentially in n.

Lemma 5.26. *For each $n \geq 3$ it holds that*

$$|\mathcal{T}_n^{(3)}| \geq \frac{2^{(n-1)(n-2)/2} - 1}{n-2}.$$

Proof. For $m \geq 2$ let

$$A_m \coloneqq \big\{G = (V,E) \;\big|\; V = \{1,\dots,m\},\ E \subseteq \{\{v_1,v_2\} \mid v_1,v_2 \in V\},\ E \neq \emptyset\big\}$$

be the set of not necessarily connected non-empty graphs on m vertices, where isolated vertices are allowed. Observe that $|A_n| = 2^{m(m-1)/2} - 1$, since each of the $m(m-1)/2$ possible edge can be either present or absent, and we exclude the case when no hyperedge is present.

Next, for $n \geq 3$, define the family of hypergraphs

$$B_n \coloneqq \big\{H = (V,E) \;\big|\; V = \{1,\dots,n\},\ E = \{\{n\} \sqcup e \mid e \in A_{n-1}\}\big\}.$$

It is easy to verify that $|B_n| = |A_{n-1}| = 2^{(n-1)(n-2)/2} - 1$. Furthermore, $B_n \subseteq \mathcal{T}_3^{(3)} \sqcup \cdots \sqcup \mathcal{T}_n^{(3)}$. Since $|\mathcal{T}_n^{(3)}| \geq |\mathcal{T}_l^{(3)}|$ for each $3 \leq l < n$ we derive that

$$|\mathcal{T}_n^{(3)}| \geq \frac{|\mathcal{T}_3^{(3)} \sqcup \cdots \sqcup \mathcal{T}_n^{(3)}|}{n-2} \geq \frac{|B_n|}{n-2} = \frac{|A_{n-1}|}{n-2} = \frac{2^{(n-1)(n-2)/2} - 1}{n-2}.$$

□

Next, we show that the family of 3-uniform simple nexuses of uniforms is larger than the family of complete multipartite 3-uniform hypergraphs which underlines the significance of this family in terms of the number of known ideal hypergraphs.

Proposition 5.27. $|\mathcal{K}_3^{(3)}| = |\mathcal{L}_3^{(3)}| = 1$ *and for* $n \geq 4$, $|\mathcal{K}_n^{(3)}| < |\mathcal{L}_n^{(3)}|$.

Proof. The first part of the claim is straightforward, since on three vertices the only 3-uniform hypergraph is the hypergraph $\big(\{1,2,3\},\{\{1,2,3\}\}\big)$ which is in $\mathcal{K}^{(3)}$ and in $\mathcal{L}^{(3)}$.

For the second claim, consider the case $n = 4$ separately. There are four possible 3-hyperedges on the set of four vertices. We observe that each 3-uniform hypergraph H on four vertices has one of the following forms (excluding the case when $|E(H)| = 1$ since in this case we only use three vertices).

$$H = \begin{cases} K^{(3)}_{1,1,2} & \text{if } |E(H)| = 2 \\ L_{1,2}(\{v\}, K^{(2)}_{1,1,1}) & \text{if } |E(H)| = 3 \\ K^{(3)}_{1,1,1,1} & \text{if } |E(H)| = 4 \end{cases} \tag{5.1}$$

where in the case $|E(H)| = 3$, v is the vertex which is in all three hyperedges.

In the case of $K^{(3)}_{1,1,2}$, this hypergraph is in both $\mathcal{K}^{(3)}_4$ and $\mathcal{L}^{(3)}_4$, by Proposition 4.25. While $K^{(3)}_{1,1,1,1}$ has only one representation on the vertex set $\{1,\dots,4\}$, $L_{1,2}(\{v\}, K^{(2)}_{1,1,1})$ has four representations depending on the choice of v among the four vertices. This shows that $|\mathcal{K}^{(3)}_4| \leq |\mathcal{L}^{(3)}_4|$.

For the case where $n \geq 5$, define $L'_n \subseteq \mathcal{L}^{(3)}_n$ by

$$L'_n := \big\{ L_{1,2}(C,G) \;\big|\; |C| > 0,\, C \sqcup V(G) = \{1,\dots,n\},\, G \text{ connected ideal graph} \big\}.$$

We define a surjective map $F_n : L'_n \to \mathcal{K}^{(3)}_n$ and show that $L'_n \subsetneq \mathcal{L}^{(3)}_n$. With that we derive that $|\mathcal{K}^{(3)}_n| \leq |L'_n| < |\mathcal{L}^{(3)}_n|$.

Let us define the notation $K^{(k)}(V_1,\dots,V_s) := K^{(k)}_{|V_1|,\dots,|V_s|}$ for $s \geq k$, where the independent parts are $V_1,\dots,V_s$. Therewith, we define the map $F_n : L'_n \to \mathcal{K}^{(3)}_n$ by

$$F_n\big(L_{1,2}(C, K^{(2)}(V_1,\dots,V_s))\big) = K^{(3)}(C, V_1,\dots,V_s).$$

First, note that this map is defined for each hypergraph in L'_n since the only connected ideal graphs are those which are complete multipartite and, hence, each hypergraph in L'_n has the form $L_{1,2}(C, K^{(2)}(V_1,\dots,V_s))$ for some pairwise disjoint independent vertex sets $C, V_1,\dots,V_s$ satisfying $|C|+|V_1|+\ldots+|V_s| = n$.

Now, we show that F_n is indeed surjective. Let $H = K^{(3)}(V_1,\dots,V_s) \in \mathcal{K}^{(3)}_n$ for $s \geq 3$ be any complete multipartite 3-uniform hypergraph. We observe that $H = F_n\big(L_{1,2}(V_1, K^{(2)}(V_2,\dots,V_s))\big)$ where $L_{1,2}(V_1, K^{(2)}(V_2,\dots,V_s)) \in L'_n$. Hence, each complete multipartite 3-uniform hypergraph is in the image of F_n.

It remains to show that $L'_n \subsetneq \mathcal{L}^{(3)}_n$. Consider the hypergraph

$$L := L_{1,2}\big(\{5,\dots,n\}, K^{(2)}(\{1\},\{2\}) \cup K^{(2)}(\{3\},\{4\})\big).$$

Note that L is the hypergraph in $L_{1,2}$ with IVC of size $n-4$ (which is non-empty since $n \geq 5$) and whose graph part is the union of two complete graphs on two vertices. Since all hypergraphs in L'_n have a connected graph part, $L \notin L'_n$ and, therefore, $|\mathcal{K}^{(3)}_n| \leq |L'_n| < |\mathcal{L}^{(3)}_n|$. □

5.4.2 3-Uniform Hypergraphs on at Most Five Vertices

Now the question is if for a fixed n, it holds that $\mathcal{T}_n^{(3)} = \mathcal{F}_n^{(3)} \sqcup \mathcal{N}_n^{(3)}$, i.e. whether the gray part in the Venn diagram in Figure 5.11 is empty or not.

We start by showing that this is true for $n \leq 4$.

Proposition 5.28. *$\mathcal{T}_3^{(3)} = \mathcal{K}_3^{(3)}$ and $\mathcal{T}_4^{(3)} = \mathcal{K}_4^{(3)} \cup \mathcal{L}_4^{(3)}$.*

Proof. First, let $n = 3$. There is only one hypergraph in $\mathcal{T}_3^{(3)}$, namely the complete 3-uniform hypergraph on three vertices $K_{1,1,1}^{(3)} = (\{1,2,3\}, \{\{1,2,3\}\})$ which is in $\mathcal{K}_3^{(3)}$ and, hence, $\mathcal{T}_3^{(3)} = \mathcal{K}_3^{(3)}$.

For $n = 4$, recall Equation (5.1) in the proof of Proposition 5.27. We see that all possible 3-uniform hypergraphs on four vertices are either in $\mathcal{K}_4^{(3)}$ or in $\mathcal{L}_4^{(3)}$ which concludes the proof. □

Hence, we have shown that each 3-uniform hypergraph on strictly less than five vertices is ideal. When looking at the Venn diagram in Figure 5.11, for the case when $n = 3$, every area except the intersection of $\mathcal{K}_3^{(3)}$ and $\mathcal{L}_3^{(3)}$ is empty. For $n = 4$ everything but the union of $\mathcal{K}_4^{(3)}$ and $\mathcal{L}_4^{(3)}$ is empty.

We have seen in Lemma 5.26 that the size of $\mathcal{T}_n^{(3)}$ grows exponentially with respect to n. While $|\mathcal{T}_3^{(3)}| = 1$ and $|\mathcal{T}_4^{(3)}| = 16$, the number of connected 3-uniform hypergraphs on exactly five vertices is already $|\mathcal{T}_5^{(3)}| = 958$ as we will see in Proposition 5.29. Deriving a closed formula for $|\mathcal{T}_n^{(3)}|$ is not trivial since we need to exclude all non-connected hypergraphs.

Also for the other families it becomes harder to characterize hypergraphs or even to just compute the size of a family for a given number n of vertices. In addition, other than for $n < 5$, now we also need to cope with hypergraphs containing forbidden minors.

We use Python code to calculate the sizes of $|\mathcal{T}_5^{(3)}|$, $|\mathcal{K}_5^{(3)}|$, $|\mathcal{L}_5^{(3)}|$, $|\mathcal{N}_5^{(3)}|$ and $|\mathcal{F}_5^{(3)}|$, respectively. While for the first four families this could also be done by hand by using combinatorics (e.g. for the complete multipartite hypergraphs we can use Lemma 5.25), $|\mathcal{F}_5^{(3)}|$ is a lot harder to compute. The main problem is that hypergraphs could contain multiple forbidden minors and we therefore need to be careful not to count them more than once.

The whole source code which is used for the computations can be found on GitHub[1]. There are several factory classes to construct all hypergraphs of each family as well as a Jupyter Notebook, where aside the code for computing the sizes of the respective families, also documentation about the code as well as its output can be found.

In particular, the code in the Notebook yields the following empirical results.

[1] Repository URL: https://github.com/sahopp/SecretSharing-Hypergraphs

Proposition 5.29. *The following values hold for 3-uniform connected hypergraphs on exactly five vertices.*

Total number of hypergraphs:	$\left\lvert\mathcal{T}_5^{(3)}\right\rvert = 958$
Number of complete multipartite hypergraphs:	$\left\lvert\mathcal{K}_5^{(3)}\right\rvert = 36$
Number of simple nexuses of uniforms:	$\left\lvert\mathcal{L}_5^{(3)}\right\rvert = 85$
Number of nexuses of uniforms:	$\left\lvert\mathcal{N}_5^{(3)}\right\rvert = 96$
Number of hypergraphs with forbidden minor:	$\left\lvert\mathcal{F}_5^{(3)}\right\rvert = 837$
Number of non-characterized hypergraphs:	$\left\lvert\mathcal{T}_5^{(3)} - (\mathcal{F}_5^{(3)} \sqcup \mathcal{N}_5^{(3)})\right\rvert = 25$

The numbers given in Proposition 5.29 reveal some interesting facts about the amount of ideal and non-ideal hypergraphs. For instance, while for $n < 5$ we only had ideal hypergraphs, now with $n = 5$ by far most of them contain some forbidden minor and are therefore non-ideal.

However, the most important number for us is the last one, namely the number of hypergraphs which are neither nexuses of uniforms nor do they contain any of the four forbidden minors Φ, $\widehat{\Phi}$, $\widehat{\Phi}^*$ or Ψ_3. In the Jupyter Notebook, these 25 hypergraphs are printed out and we observe that they all belong to one of two isomorphism classes. Hence, we are left with the question whether the two hypergraphs Θ_1 and Θ_2 are ideal, where

$$\begin{aligned} V(\Theta_1) = V(\Theta_2) &= \big\{1,2,3,4,5\big\} \\ E(\Theta_1) &= \big\{\{1,2,3\},\{1,2,4\},\{1,2,5\},\{1,3,4\},\{1,3,5\}, \\ &\qquad \{1,4,5\},\{2,3,4\},\{2,3,5\},\{2,4,5\}\big\} \\ E(\Theta_2) &= \big\{\{1,2,3\},\{1,2,4\},\{1,2,5\},\{1,3,4\}, \\ &\qquad \{1,3,5\},\{2,3,4\},\{2,4,5\},\{3,4,5\}\big\}. \end{aligned}$$

Note that Θ_1 is the complete 3-uniform hypergraph on five vertices with one hyperedge removed, while Θ_2 is the complete 3-uniform hypergraph on five vertices with two hyperedges removed which have an intersection of size 1. The question about the idealness of Θ_1 and Θ_2 stays unanswered within this thesis.

We do not further analyze the sizes of $|\mathcal{T}_n^{(3)}|$, $|\mathcal{K}_n^{(3)}|$, $|\mathcal{L}_n^{(3)}|$, $|\mathcal{N}_n^{(3)}|$ and $|\mathcal{F}_n^{(3)}|$ for $n > 5$. However, it is expected that the ratio of non-ideal hypergraphs grows rapidly and that there are more hypergraphs for which we cannot yet determine whether they are ideal or not.

Chapter 6

Discussion

6.1 Summary

In this thesis we worked towards the goal of characterizing uniform hypergraphs which represent ideal access structures and, in particular, focused on 3-uniform hypergraphs. Based on known results on ideal graphs, threshold access structures and the forbidden minor characterization of ideal access structures, we first defined an operation on hypergraphs called *region-expansion* $H[A \to Z]$ for hypergraphs H and Z and a subset of a region $A \subseteq V(H)$. We have proven that for $m > 1$, m-idealness of $H[A \to Z]$ is equivalent to m-idealness of H and Z.

We defined for any fixed $k \geq 2$ the k-uniform *simple nexuses of uniforms* $\mathcal{L}^{(k)}$ and *nexuses of uniforms* $\mathcal{N}^{(k)}$, two families of uniform hypergraphs. By using properties of the region-expansion we have proven that $\mathcal{N}^{(k)} = \mathcal{K}^{(k)} \cup \mathcal{L}^{(k)}$, where $\mathcal{K}^{(k)}$ is the set of complete multipartite k-uniform hypergraphs. Furthermore, all nexuses of uniforms have been shown to be ideal.

In a further step we saw that uniform hyperstars are a special subset of simple nexuses of uniforms and have therefore proven that characterizing ideal k-uniform hyperstars is equivalent to characterizing all ideal k'-uniform (not necessarily connected) hypergraphs for each $k' < k$. This also implies that a 3-uniform hyperstar S is ideal if and only if its center C has size 2 or 3 or, if C has size 1, each connected component in $S \,/\, C$ is a complete multipartite graph. We therewith answered one of the two parts of Problem 1 stated by Ligeti [26].

Focusing on general 3-uniform hypergraphs we have shown that each nexus of uniforms in this case is not only ideal but also linearly ideal, i.e. they can be realized by an ideal linear secret sharing scheme. In a last step we have analyzed the 3-uniform hypergraphs on at most five vertices and have empirically shown with a Python script that all of them except for two (up to isomorphism) are either nexuses of uniforms or contain a forbidden minor.

6.2 Open Problems

Based on the results of this thesis there are several open problems which might serve as a set of steps towards a full characterization of all ideal 3-uniform or even k-uniform hypergraphs.

The foremost open problem is to prove the idealness or non-idealness of the two hypergraphs Θ_1 and Θ_2 which are, up to isomorphism, the only 3-uniform hypergraphs on at most five vertices which are not in $\mathcal{N}^{(3)} \sqcup \mathcal{F}^{(3)}$.

Open Problem 1. *Prove or disprove idealness of Θ_1 and Θ_2, the only two 3-uniform hypergraphs on at most five vertices which are neither nexuses of uniforms nor do they contain one of the forbidden minors Φ, $\widehat{\Phi}$, $\widehat{\Phi}^*$ or Ψ_3. The hypergraphs Θ_1 and Θ_2 are given by*

$$\begin{aligned} V(\Theta_1) = V(\Theta_2) &= \big\{1,2,3,4,5\big\} \\ E(\Theta_1) &= \big\{\{1,2,3\},\{1,2,4\},\{1,2,5\},\{1,3,4\},\{1,3,5\}, \\ &\qquad \{1,4,5\},\{2,3,4\},\{2,3,5\},\{2,4,5\}\big\} \\ E(\Theta_2) &= \big\{\{1,2,3\},\{1,2,4\},\{1,2,5\},\{1,3,4\}, \\ &\qquad \{1,3,5\},\{2,3,4\},\{2,4,5\},\{3,4,5\}\big\}. \end{aligned}$$

An apparent question is whether the 3-uniform nexuses of uniforms are the only ideal 3-uniform hypergraphs. Note that this question would already be answered with "no" if we prove idealness of at least one of Θ_1 or Θ_2.

Open Problem 2. *Are there any ideal 3-uniform hypergraphs other than nexuses of uniforms?*

We saw that the 3-uniform nexuses of uniforms are compositions of threshold access structures and that they are therefore linearly ideal. Even if there were any ideal 3-uniform hypergraphs other than nexuses of uniforms, they might still not be linearly ideal. Hence, the following natural question arises.

Open Problem 3. *Are there any linearly ideal 3-uniform hypergraphs other than nexuses of uniforms?*

All the above problems are steps towards the Problem stated by Ligeti [26], which this thesis has contributed to but not entirely answered.

Open Problem 4. *Give a characterization of all ideal 3-uniform hypergraphs.*

Appendix A

Algorithms

The pseudo-code algorithms stated in this appendix are very high-level and sometimes do not elaborate details on how to implement them. However, for complexity analysis, we may state in words how some tasks are done in an efficient way. Complexities of algorithms on hypergraphs are given in terms of the number of vertices (usually denoted by n) and the number of hyperedges (usually denoted by m). Hence, for instance an algorithm has linear time complexity if it is $\mathcal{O}(n + m)$.

Within the pseudo-code algorithms, the following notations and supporting functions are used.

- Lists are initialized by "$L \leftarrow [\ ]$", and list elements are accessed by their position in the list, e.g. $L[2]$, where the first element is at position 0. Note that we apply set operations like intersection and union for lists, which can be executed in several programming languages for lists too.
- Apart from lists we also use dictionaries which are initialized by curly braces like "$D \leftarrow \{\ \}$". Elements in dictionaries are accessed by their key, e.g. $D[v]$.
- We use the notation "$y = x$.copy()" to indicate the creation of a copy of x with the name y. This is in particular useful if we need to modify an element on the run but also want to keep its original value.
- In loops, we use the statement *break* to immediately exit the current loop and go on with whatever comes after this loop. The statement *continue* only breaks one iteration of the loop and the algorithm continues at the start of the next iteration. Note that in nested loops only the inner loop is affected.

A.1 Ideal Graphs

First, we discuss an algorithm that checks whether a given connected graph G is ideal or, equivalently, is complete multipartite. The pseudo-code is given in

Algorithm 1, the discussion on the correctness of the output as well as the time complexity can be found in [32].

Algorithm 1: is_ideal_graph

Data: Connected graph $G = (V, E)$
Result: Boolean: is G ideal?

```
1  compute_all_degrees(G);
2  V_1 ← ∅, V_2 ← ∅;
3  for v ∈ V do
4  |   if deg(v) < n/2 − 1 then V_1 ← V_1 ∪ {v};
5  |   else V_2 ← V_2 ∪ {v};
6  end
7  if not is_independent_set(G, V_1) then return false;
8  if not each_is_adjacent_to_each(G, V_1, V_2) then return false;
9  if is_P3_free(complement(G \ V_1)) then return true;
10 return false;
```

The function *each_is_adjacent_to_each(G,V_1,V_2)* returns true if in the graph G each vertex in V_1 is adjacent to each vertex in V_2 and false otherwise. We omit details on all other functions used in the pseudo-code which should be self-explanatory.

Algorithm 1 is shown to have linear runtime, i.e. if $n = |V(G)|$ and $m = |E(G)|$, it has time complexity $\mathcal{O}(n + m)$. Furthermore, space complexity is also given by $\mathcal{O}(n + m)$.

A.2 Ideal 3-Uniform Hyperstars

With Algorithm 2, we provide a polynomial-time algorithm which checks whether a given 3-uniform hypergraph $H = (V, E)$ is an ideal hyperstar, by simply checking the conditions given in Theorem 5.15. Indeed, after determining the size of the intersection C of all hyperedges until line 6, we return *false* if this intersection is empty and return *true* if its size is either 2 or 3. If the intersection has size 1 we check whether each connected component in $H \,/\, C$ is ideal, where we can use a depth-first search approach to identify the connected components [1] and Algorithm 1 to check for their idealness.

Proposition A.1. *Algorithm 2 can be implemented with worst-case time complexity $\mathcal{O}(\max(n^2, m))$ and space complexity $\mathcal{O}(n^2)$, where n and m are the sizes of the vertex set and hyperedge set of the input graph, respectively.*

Proof. For an input hypergraph $H = (V, E)$, let $n = |V|$ and $m = |E|$.

Computing the intersection of the hyperedges until line 6 needs time $\mathcal{O}(m)$ since each iteration of the *for*-loop is a constant time task and we loop over each hyperedge. The next step, namely checking whether $|C| > 2$, is a constant-time task which is only executed once.

Then, on line 8, we first need to compute the minor $H \,/\, C$ which can be done in time $\mathcal{O}(m)$ by going through all hyperedges and remove the vertex which

Algorithm 2: is_ideal_hyperstar(H)

Data: 3-uniform hypergraph $H = (V, E)$
Result: Boolean: is H an ideal hyperstar?

```
1  e' ← E[0];
2  C ← e';
3  for e ∈ E − {e'} do
4  |   C ← C ∩ e;
5  |   if C = ∅ then return false;
6  end
7  if |C| ≥ 2 then return true;
8  A ← connected_components_list(H / C);
9  for G ∈ A  do
10 |   if not is_ideal_graph(G) then return false;
11 end
12 return true;
```

is in the center C. Splitting this minor into its connected components can be done in time $\mathcal{O}(\max(n, m))$ with a depth-first search [1], where we first need to construct the adjacency matrix of H / C. The adjacency matrix of a graph G on the vertex set $\{v_1, \ldots, v_n\}$ is an $n \times n$ binary matrix $A = (a_{i,j})_{1 \leq i,j \leq n}$, where $a_{i,j} = 1$ if and only if $\{v_i, v_j\} \in E(G)$.

Filling in the values in the adjacency matrix for H / C takes $\mathcal{O}(|E(H / C)|) = \mathcal{O}(m)$ time, and storing the matrix takes $\mathcal{O}(|V(H / C)|^2)$ space which corresponds to $\mathcal{O}(n^2)$.

Now let $G_1, \ldots, G_t$ be the connected components of H / C computed on line 8. The i-th iteration of the last loop, i.e. line 10, has worst case time complexity $\mathcal{O}(|V(G_i)| + |E(G_i)|)$ when using Algorithm 1. Hence, the whole *for*-loop has complexity

$$\mathcal{O}\big(|V(G_1)| + |E(G_1)| + \ldots + |V(G_t)| + |E(G_t)|\big) = \mathcal{O}\big(n + m\big).$$

Therefore, the *for*-loop from line 9 to line 11 is the most expensive part of the algorithm and uses $\mathcal{O}(n(n + m)) = \mathcal{O}(\max(n^2, m))$ time in the worst case.

Space complexity is given by $\mathcal{O}(n^2)$ for the adjacency matrix. □

A.3 3-Uniform Nexuses of Uniforms

In this section we derive algorithms to determine whether a given connected 3-uniform hypergraph is complete multipartite (Algorithm 4), a simple nexus of uniforms (Algorithm 5) or a nexus of uniforms (combining Algorithms 4 and 5).

We will use a function called *graph_part(H, c)* which takes as arguments a 3-uniform hypergraph H and a vertex $c \in H$. It returns the minimized graph G with hyperedge set $E(G) = \{e - \{c\} \mid e \in E(H)\}$. We do not provide pseudocode for this function, since it is self-explanatory. Time complexity is given by $\mathcal{O}(|E(H)|)$ as we need to loop through all hyperedges.

A.3.1 Finding Candidates for Independent Vertex Sets

The core of both algorithms in this section is a common function which we use as a first step to build on. Namely, given a hypergraph H, we define a function *get_indep_sets_of_universally_adjacent_vertices(H)* given in Algorithm 3 which returns a list S of vertex sets such that for each $C \in S$

1. C is an independent set in H and
2. each $c \in C$ is adjacent to each $v \in V(H) - C$.

Note that for H to be in $L_{1,2}$, by Lemma 5.3, it is necessary that $S \neq \emptyset$, i.e. that there exists at least one $C \subseteq V(H)$ satisfying the above two conditions. However, these two conditions are not sufficient. Hence, further checks need to be done for each candidate $C \in S$.

Algorithm 3: get_indep_sets_of_universally_adjacent_vertices

Data: Connected 3-uniform hypergraph $H = (V, E)$
Result: List of IVCs C such that each vertex in C is adjacent to each vertex in $V(H) - C$

```
1  D ← { };
2  for v ∈ V do
3  |  D[v] = V;
4  end
5  for e ∈ E do
6  |  for v ∈ e do
7  |  |  D[v] ← D[v] − e;
8  |  end
9  end
10 S ← ∅;
11 V′ ← V.copy();
12 while V′ ≠ ∅ do
13 |  v ← V′[0];
14 |  if D[v] − V′ = ∅ then
15 |  |  is_valid ← true;
16 |  |  for w ∈ D[v] ∩ V′ do
17 |  |  |  if (D[v] − {w}) ∪ {v} ≠ D[w]  then
18 |  |  |  |  is_valid ← false;
19 |  |  |  |  break;
20 |  |  |  end
21 |  |  end
22 |  |  if is_valid then S ← S ∪ {D[v] ∪ {v}};
23 |  end
24 |  V′ ← V′ − (D[v] ∪ {v});
25 end
26 return S;
```

Until line 9 we construct a dictionary D containing for each $v \in V$ the list of all vertices to which v is independent. Hence, the vertices to which v is adjacent is given by $V - D[v]$. In the second half of the algorithm we check for vertices $v \in V$

whether $D[v] \cup \{v\}$ is an independent set and whether each vertex in $D[v] \cup \{v\}$ is adjacent to each vertex outside this set. If this is the case, $D[v] \cup \{v\}$ is added to S and we repeat the previous steps excluding the vertices which have already been encountered, as long as there are vertices left. Eventually, the list S of vertex sets is returned. Note that S is the empty list if no subset of the vertex set fulfills the two necessary conditions.

Lemma A.2. *Algorithm 3 has time complexity* $\mathcal{O}(\max(n^2, m))$. *Space complexity is also given by* $\mathcal{O}(\max(n^2, m))$.

Proof. The first loop on lines 2 to 4 needs time $\mathcal{O}(n)$, while the second one from line 5 to 9 needs time $\mathcal{O}(m)$ (where we assume the hyperedge sizes are bounded by a constant).

The *while*-loop from line 12 to line 25 has time complexity $\mathcal{O}(n^2)$. Indeed, note that here each vertex is only processed once, either in the outer *while*-loop or in the inner *for*-loop, but not in both since we remove all vertices which have been processed from V' on line 24. Hence, the check in the *if*-statement on line 17 is executed at most n times. Assuming that the lists in the dictionary D are ordered, each of those checks needs $\mathcal{O}(n)$ element comparisons. Hence, we have an overall time complexity $\mathcal{O}(\max(n^2, m))$.

We need $\mathcal{O}(n^2)$ space to store the initial dictionary, where after the first *for*-loop we have n entries, each of size n. Hence, space complexity is given by $\mathcal{O}(\max(n^2, m))$, where we take into consideration that the number of hyperedges can be of higher order than the number of vertices. □

With Algorithm 3 as a basis we can now state the algorithms which check whether a given connected 3-uniform hypergraph belongs to one of $\mathcal{K}^{(3)}$, $\mathcal{L}^{(3)}$ or $\mathcal{N}^{(3)}$.

A.3.2 Complete Multipartite 3-uniform Hypergraphs

Algorithm 4 verifies for a connected 3-uniform hypergraph H whether it is complete multipartite or not. We start by using Algorithm 3 in order to get all independent sets C in H such that each vertex in C is adjacent to each vertex in $V(H) - C$.

Algorithm 4: is_complete_multipartite

```
   Data: Connected 3-uniform hypergraph H = (V, E)
   Result: Boolean: is H complete multipartite?
1  S ← get_indep_sets_of_universally_adjacent_vertices(H);
2  if |{s ∈ A | A ∈ S}| ≠ |V| then return false;
3  for v ∈ V do
4  |  if not is_complete_graph(graph_part(H, v)) then return false;
5  end
6  return true;
```

Note that for complete multipartite hypergraphs each part in the partition needs to be an independent set of this kind which we check on line 2. In a further

step, we verify whether the graph part for each vertex $v \in V$ corresponds to the complete graph on all vertices which are not in the same part as v. This check can be done by verifying that the number of edges in the graph is $N(N-1)/2$, where N is the number of vertices of the graph.

If all the above conditions are fulfilled, H is a complete multipartite 3-uniform hypergraph.

Proposition A.3. *Algorithm 4 has time complexity* $\mathcal{O}(\max(n^2, nm))$ *and space complexity* $\mathcal{O}(\max(n^2, m))$.

Proof. We know that the function call on line 1 has complexity $\mathcal{O}(\max(n^2, m))$ and the check on line 2 is doable in $\mathcal{O}(n)$ time. Afterwards, we loop over each vertex in V, compute the graph part G (which takes $\mathcal{O}(m)$ time) and check whether $|E(G)| = N(N-1)/2$, where $N = |V(G)|$ in order to check whether G is a complete graph. This is a constant time task. Hence, altogether this *for*-loop takes $\mathcal{O}(nm)$ operations, which is why the overall time complexity of Algorithm 4 is $\mathcal{O}(\max(n^2, m, nm)) = \mathcal{O}(\max(n^2, nm))$.

Space complexity of Algorithm 4 is given by the space complexity of Algorithm 3 and is $\mathcal{O}(\max(n^2, m))$. □

A.3.3 3-uniform Simple Nexuses of Uniforms

Like for Algorithm 4, also for the algorithm to check whether a given connected 3-uniform hypergraph is a simple nexus of uniforms we start by using Algorithm 3 to get the set S of all independent sets C in H such that each vertex in C is adjacent to each vertex in $V(H) - C$. Algorithm 5 then checks for each such vertex set $C \in S$ whether it qualifies as IVC of a hypergraph in $L_{1,2}$. If it finds one such valid decomposition with IVC C and graph part $H \,/\, C$ it returns true, otherwise it returns false.

Let us examine an iteration of the outer *for*-loop in Algorithm 5. Let $C \in S$ be a vertex set returned by *get_indep_sets_of_universally_adjacent_vertices(H)*. First, we check whether C is an IVC of H which can be done by verifying that $|C \cap e| = 1$ for each hyperedge $e \in E(H)$. If this is the case, we pick one vertex within C, compute its graph part G and check whether G is ideal (i.e. whether each connected component is ideal) until line 13. If not, we go on with the next possible set in S.

If G is ideal, in the remaining part of the code we check whether the graph part of each vertex in C is equal to G. If this is the case, we return true, else we go on looking at the remaining possible IVCs.

Note that graph equality can be checked in $\mathcal{O}(m)$ time, for instance via a hash function which is invariant with respect to the order of the edges and vertices within the edges.

Proposition A.4. *Algorithm 5 has time complexity* $\mathcal{O}(\max(n^2, nm))$ *and space complexity* $\mathcal{O}(\max(n^2, m))$.

Proof. Again, from Lemma A.2 we know that the function call on line 1 has complexity $\mathcal{O}(\max(n^2, m))$. Afterwards, we loop through S whose size is upper

Algorithm 5: is_simple_nexus_of_uniforms

```
   Data: Connected 3-uniform hypergraph H = (V, E)
   Result: Boolean: is H in L_{1,2}?
 1 S ← get_indep_sets_of_universally_adjacent_vertices(H);
 2 for C ∈ S do
 3     if is_IVC(C, H) then return true;
 4     Let c' ∈ C arbitrary;
 5     G ← graph_part(H, c');
 6     non_ideal_component_found ← false;
 7     for G' ∈ connected_components_list(G) do
 8         if not is_ideal_graph(G') then
 9             non_ideal_component_found ← true;
10             break;
11         end
12     end
13     if non_ideal_component_found then continue;
14     all_graph_parts_equal ← true;
15     for c ∈ C do
16         if graph_part(H, c) ≠ G then
17             all_graph_parts_equal ← false;
18             break;
19         end
20     end
21     if all_graph_parts_equal then return true;
22 end
23 return false;
```

bounded by n. For $C \in S$, checking whether C is an IVC takes $\mathcal{O}(m)$ steps by finding out if $|C \cap e| = 1$ for each $e \in E(H)$. Afterwards, computing G on line 5 takes $\mathcal{O}(m)$ steps and computing the connected components to iterate over takes $\mathcal{O}(\max(n, m))$ steps (see proof of Proposition A.1 for details) and is done at most n times (at most once for each $C \in S$).

Next, for the first inner *for*-loop on lines 7 to 12, each check on line 8 has complexity $\mathcal{O}(|V(G')| + |E(G')|)$. This is done for each connected component, hence the total complexity of this loop is $\mathcal{O}(|V(G)| + |E(G)|)$ which we can bound by $\mathcal{O}(n + m)$. we reach this loop at most n times (namely at most once for each $C \in S$). Hence, adding up all executions of this loop, we get worst case time complexity $\mathcal{O}(n(n + m)) = \mathcal{O}(\max(n^2, nm))$.

Let us now focus on the second inner *for*-loop between lines 15 and 20. Note that this loop is executed at most n times in total, since each vertex can be in at most one IVC $C \in S$. Each iteration of this loop has complexity $\mathcal{O}(m)$ for the calculation of the graph part and for checking whether the two graphs are equal.

Hence, we conclude that the most expensive parts of the algorithm are computing the connected components on line 7 up to n times and checking idealness

of graphs on line 8 which in total can take up to $\mathcal{O}(n(n+m))$ steps during the whole execution of the algorithm.

We deduce that Algorithm 5 has time complexity $\mathcal{O}(n(n+m)) = \mathcal{O}(\max(n^2, nm))$.

For space usage, again the most expensive part is the call of Algorithm 3 with complexity $\mathcal{O}(\max(n^2, m))$. □

Bibliography

[1] J. E. Hopcroft and R. E. Tarjan. "Algorithm 447: Efficient Algorithms for Graph Manipulation". In: *Commun. ACM* 16 (1973), pp. 372–378.

[2] P. Seymour. "A Forbidden Minor Characterization of Matroid Ports". In: *Quarterly Journal of Mathematics* 27.4 (1976), pp. 407–413.

[3] G. R. Blakley. "Safeguarding Cryptographic Keys". In: *1979 International Workshop on Managing Requirements Knowledge (MARK)*. 1979, pp. 313–318.

[4] A. Shamir. "How to Share a Secret". In: *Commun. ACM* 22.11 (1979), pp. 612–613.

[5] E. Karnin, J. Greene, and M. Hellman. "On Secret Sharing Systems". In: *Information Theory, IEEE Transactions on* IT-29 (1983), pp. 35–41.

[6] P. Seymour. "On Secret-Sharing Matroids". In: *J. Comb. Theory, Ser. B* 56 (1992), pp. 69–73.

[7] R. Capocelli et al. "On the Size of Shares for Secret Sharing Schemes". In: *Journal of Cryptology* 6 (1993), pp. 157–167.

[8] B. Chor and E. Kushilevitz. "Secret Sharing Over Infinite Domains". In: *Journal of Cryptology* 6.2 (1993), pp. 87–95.

[9] A. Beimel and B. Chor. "Universally Ideal Secret-Sharing Schemes". In: *IEEE Transactions on Information Theory* 40.3 (1994), pp. 786–794.

[10] A. Beimel et al. "Secure Schemes for Secret Sharing and Key Distribution". PhD thesis. 1996.

[11] L. Csirmaz. "The Size of a Share Must Be Large". In: *J. Cryptology* 10 (1997), pp. 223–231.

[12] C. Blundo, A. De Santis, and U. Vaccaro. "On Secret Sharing Schemes". In: *Information Processing Letters* 65.1 (1998), pp. 25–32.

[13] M. Naor and A. Wool. "Access Control and Signatures via Quorum Secret Sharing". In: *IEEE Transactions on Parallel and Distributed Systems* 9.9 (1998), pp. 909–922.

[14] F. Matúš. "Matroid Representations by Partitions". In: *Discrete Mathematics* 203.1 (1999), pp. 169–194.

[15] R. Cramer, I. Damgård, and U. Maurer. "General Secure Multi-Party Computation from any Linear Secret-Sharing Scheme". In: *LNCS* 1807 (2000), pp. 316–334.

[16] A. Beimel and Y. Ishai. "On the Power of Nonlinear Secret-Sharing". In: *Proceedings 16th Annual IEEE Conference on Computational Complexity*. 2001, pp. 188–202.

[17] J. Pieprzyk and X.-M. Zhang. "Nonlinear Secret Sharing Immune Against Cheating". In: *DMS 2001*. Tamkang University, 2001, pp. 154–161.

[18] E. F. Brickell and D. M. Davenport. "On the Classification of Ideal Secret Sharing Schemes". In: *Journal of Cryptology* 4 (2004), pp. 123–134.

[19] J. Martí-Farré and C. Padró. "On Secret Sharing Schemes, Matroids and Polymatroids". In: *Theory of Cryptography*. Ed. by S. P. Vadhan. Springer Berlin Heidelberg, 2007, pp. 273–290.

[20] A. Beimel, N. Livne, and C. Padró. "Matroids Can be Far from Ideal Secret Sharing". In: *Theory of Cryptography Conference*. Springer. 2008, pp. 194–212.

[21] G. Di Crescenzo and C. Galdi. "Hypergraph Decomposition and Secret Sharing". In: *Discrete Applied Mathematics* 157.5 (2009), pp. 928–946.

[22] J. Martí-Farré and C. Padró. "Ideal Secret Sharing Schemes whose Minimal Qualified Subsets Have at Most Three Participants". In: *Designs, Codes and Cryptography* 52.1 (2009), pp. 1–14.

[23] A. Beimel. "Secret-Sharing Schemes: A Survey". In: *Coding and Cryptology*. Ed. by Y. M. Chee et al. Springer Berlin Heidelberg, 2011, pp. 11–46.

[24] D. Mayhew et al. "The Excluded Minors for the Class of Matroids That Are Binary or Ternary". In: *European Journal of Combinatorics* 32.6 (2011), pp. 891–930.

[25] I. Adler, T. Gavenčiak, and T. Klimošová. "Hypertree-Depth and Minors in Hypergraphs". In: *Theoretical Computer Science* 463 (2012), pp. 84–95.

[26] P. Ligeti. "On Secret Sharing and 3-Uniform Hypergraphs". In: *Tatra Mountains Mathematical Publications* 53 (2012).

[27] J. Cutler and A. Radcliffe. "Hypergraph Independent Sets". In: *Combinatorics, Probability and Computing* 22.1 (2013), pp. 9–20.

[28] A. Beimel et al. "Multi-linear Secret-Sharing Schemes". In: *Theory of Cryptography*. Ed. by Y. Lindell. Springer Berlin Heidelberg, 2014, pp. 394–418.

[29] A. Dibert and L. Csirmaz. "Infinite Secret Sharing – Examples". In: *Journal of Mathematical Cryptology* 8.2 (2014), pp. 141–168.

[30] N. Helil and K. Rahman. "Secret Sharing Scheme Based Approach for Access Control Constraint Against Similar Users' Collusive Attack". In: *Journal of Information Science and Engineering* 32 (2016), pp. 1455–1470.

[31] A. Beimel and O. Farràs. “The Share Size of Secret-Sharing Schemes for Almost All Access Structures and Graphs”. In: *Theory of Cryptography*. Ed. by R. Pass and K. Pietrzak. Springer International Publishing, 2020, pp. 499–529.

[32] T. Koana and A. Nichterlein. “Detecting and Enumerating Small Induced Subgraphs in c-Closed Graphs”. In: 302 (2021), pp. 198–207.