


Constrained Submodular Minimisation

From Parity Families to Congruency Constraints

Master Thesis

Author(s):

Nägele, Martin 

Publication date:

2017

Permanent link:

<https://doi.org/10.3929/ethz-b-000518694>

Rights / license:

[In Copyright - Non-Commercial Use Permitted](#)

MARTIN NÄGELE

CONSTRAINED SUBMODULAR MINIMISATION

From Parity Families to Congruency Constraints

MASTER THESIS

ADVISER:

PROF. DR. RICO ZENKLUSEN

OCTOBER 2016 – MARCH 2017

INSTITUTE FOR OPERATIONS RESEARCH

DEPARTMENT OF MATHEMATICS

ETH ZÜRICH



Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Abstract

We study two classes of constrained submodular minimisation problems, where a submodular function f defined on a lattice family \mathcal{L} is to be minimised over a subfamily of \mathcal{L} . In the first class, so-called congruency constrained submodular minimisation (CSM) problems, the subfamilies are of the form $\mathcal{F} = \{S \in \mathcal{L} \mid |S| \equiv r \pmod{m}\}$. For the second class of problems, namely generalised congruency constrained submodular minimisation (GCSM) problems, we are given a constant number of fixed sets S_1, \dots, S_k and consider subfamilies of the form $\mathcal{F} = \{S \in \mathcal{L} \mid \forall i: |S_i \cap S| \equiv r_i \pmod{m}\}$.

If m is a prime power, we provide polynomial time algorithms to solve both CSM and GCSM problems. Our algorithms rely on guessing a constant number of elements that belong to an optimal solutions and a constant number that do not. While our approaches and algorithms for CSM and GCSM problems can be seen as generalisations of a result by Goemans and Ramakrishnan for minimising submodular functions over parity families, we introduce and apply new techniques for proving correctness of the algorithms. Among others, this includes handling purely combinatorial problems on existence of set systems with certain covering properties and restricted intersections modulo m .

We also show that for strong combinatorial reasons, our current methods do not generalise to CSM and GCSM problems with moduli other than prime powers.

Acknowledgement

First and foremost, I owe many thanks to Prof. Rico Zenklusen. It was him who awoke my interest in combinatorial optimisation in his lecture two years ago. Only his inspiring enthusiasm for research and his excellent support during a term project and this master thesis brought me to where I am now. Thank you, Rico!

I enjoyed the privilege of getting a workplace at the IFOR during my master studies and being part of a great research group. Thanks to everybody involved for making this time so enjoyable. I'm particularly grateful to Steve for his careful proofreading of this manuscript and his helpful remarks.

Moreover, I want to thank Benny Sudakov for sharing the interest in our research questions, some fruitful discussions and his valuable input.

Finally, I would like to express my deepest gratitude to my parents for their love and encouragement, and to my girlfriend Pia for her patience and understanding, her continuous support, and her love. Thank you for believing in me and always being there for me.

Contents

Contents	<i>iii</i>
1 Introduction	1
1.1 Unconstrained submodular minimisation	1
1.2 Constrained submodular minimisation and prior results	2
1.3 Our results	4
1.4 Organisation of the thesis	6
2 Partial enumeration procedures	7
3 Proving correctness of partial enumeration procedures	11
3.1 A first sufficient condition for partial enumeration	11
3.2 Set systems and a second sufficient condition	14
3.3 Set system transformations	16
3.4 A lower bound on the order	23
4 Congruency constrained submodular minimisation	25
4.1 Employing sufficient conditions for correctness: Set systems	25
4.2 An elementary solution for prime moduli	27
4.3 Polynomial set transformations and prime moduli	29
4.4 Binomial transformations and prime power moduli	32
4.5 Obstacles for transformations in the composite case	35
4.6 Computational experiments	36

5	Generalised congruency constrained submodular minimisation	39
5.1	Set systems in the generalised setting	39
5.2	A solution for prime power moduli	41
5.3	Reducing to disjoint conditions	43
5.4	A variation: Varying moduli	47
6	Conclusion	51
A	C++ code for computational experiments	53
	Bibliography	59

Chapter 1

Introduction

We begin this thesis by introducing unconstrained submodular minimisation and a general setting for constrained submodular minimisation problems. In particular, we describe a special type of constrained problems that was considered by Goemans and Ramakrishnan, namely minimisation of submodular functions over parity families. The two authors provided a polynomial time algorithm for solving such problems. Their algorithm forms the starting point of this master thesis project: We are able to extend parts of the results of Goemans and Ramakrishnan to considerably more general settings, which are introduced in this chapter.

1.1 Unconstrained submodular minimisation

We start by briefly reviewing the problem of unconstrained submodular minimisation. To this end, we recall the following definition.

Definition 1.1 (Lattice family, submodular function). *Let V be a finite set.*

- (i) *A family \mathcal{L} of subsets of V is called a lattice family on V , or simply a lattice, if for all $A, B \in \mathcal{L}$, we have $A \cap B \in \mathcal{L}$ and $A \cup B \in \mathcal{L}$.*
- (ii) *A lattice \mathcal{L}' on V is a sublattice of \mathcal{L} if $\mathcal{L}' \subseteq \mathcal{L}$.*
- (iii) *Let \mathcal{L} be a lattice family on V . A function $f: \mathcal{L} \rightarrow \mathbb{Z}$ is called submodular if for all $A, B \in \mathcal{L}$, we have*

$$f(A) + f(B) \geq f(A \cap B) + f(A \cup B) .$$

Submodular functions arise in many different areas in and outside mathematics, including, for example, rank functions of matroids [1], cut or s - t -cut functions in graph theory [15], coverage functions used in sensor placement or facility location problems [17], and many more. From an optimisation point of view, already the few examples given above motivate studying the problem of efficiently optimising a

submodular function. We concentrate on minimisation here, so we want to find a set $S^* \subseteq V$ such that

$$S^* \in \arg \min_{S \in \mathcal{L}} f(S) .$$

This problem is what we call *submodular minimisation* or, if we want to emphasise that there are no extra constraints, *unconstrained submodular minimisation*.

When talking about efficiently minimising a submodular function, we need to clarify what “efficient” means in this context. Usually, a submodular function $f: \mathcal{L} \rightarrow \mathbb{Z}$ is given by a *value oracle*, i.e., an oracle returning the value $f(S)$ for a given set $S \in \mathcal{L}$. An algorithm for minimising the submodular function f is said to be *polynomial time* if both its running time and the number of calls to the value oracle are bounded by polynomials in the size $|V|$ of the ground set. To emphasise the fact that there is a bound on the number of value oracle calls, such algorithms are also called *oracle-polynomial*.

There are different polynomial time algorithms known for submodular minimisation. The historically first such algorithm was found by Grötschel, Lovász and Schrijver in the 1980’s and is based on the ellipsoid method [6, 7]. Later, purely combinatorial procedures for submodular minimisation were developed [10, 14], and further publications reduced bounds on the time complexity considerably [2, 9, 13]. The currently best algorithm relies on fast cutting plane methods that were introduced by Lee, Sidford and Wong [11].

The results presented in this thesis all depend heavily on the fact that unconstrained submodular minimisation can be handled efficiently. To be precise, we use that given a submodular function f on a lattice family \mathcal{L} , it is even possible to find a minimal set with respect to inclusion among all sets in the lattice minimising f . To see this, we can for example consider the function $g: \mathcal{L} \rightarrow \mathbb{Z}$ given by $g(S) = (|V| + 1) \cdot f(S) + |S|$ for all $S \in \mathcal{L}$. It is easy to see that every set minimising g over \mathcal{L} is a minimal set minimising f over \mathcal{L} . As furthermore, g is itself a submodular function, a minimiser of g can be obtained efficiently.

1.2 Constrained submodular minimisation and prior results

As opposed to unconstrained submodular minimisation, where the goal is to minimise a submodular function $f: \mathcal{L} \rightarrow \mathbb{Z}$ over a lattice family \mathcal{L} , constrained submodular minimisation problems contain further constraints on the sets to which the optimisation should be restricted. These further constraints can be generally viewed as a restriction to optimising over a subfamily $\mathcal{F} \subseteq \mathcal{L}$ of the lattice, with the goal of finding a set $S^* \in \mathcal{F}$ such that

$$S^* \in \arg \min_{S \in \mathcal{F}} f(S) .$$

Already for seemingly “simple” constraints like cardinality constraints, such constrained submodular minimisation problems can get hard. To be more precise, if the

set family \mathcal{F} is of the form

$$\mathcal{F} = \{S \in \mathcal{L} \mid |S| < c\} \quad \text{or} \quad \mathcal{F} = \{S \in \mathcal{L} \mid |S| > c\}$$

for a constant integer c , then the corresponding constrained submodular minimisation problem is NP-hard, and even inapproximable within a factor of $o(\sqrt{n}/\log n)$ with a polynomial number of queries to a function-value oracle, where n is the size of the ground set [16].

Non-trivial examples for constrained families \mathcal{F} where an efficient solution of the corresponding submodular minimisation problem is possible were, among others, given by Grötschel, Lovász and Schrijver [7, Section 10.4] and Goemans and Ramakrishnan [4]. The first authors consider so-called triple families, while the second examine a generalisation thereof, namely parity families.

Definition 1.2 (Triple family, parity family). *Let V be a finite set and let \mathcal{L} be a lattice family on V .*

- (i) *A subfamily $\mathcal{T} \subseteq \mathcal{L}$ is called triple family if for any $A, B \in \mathcal{L}$, whenever three of the four sets*

$$A, B, A \cap B, \text{ and } A \cup B$$

are in $\mathcal{L} \setminus \mathcal{T}$, then the fourth set is in $\mathcal{L} \setminus \mathcal{T}$, as well.

- (ii) *A subfamily $\mathcal{P} \subseteq \mathcal{L}$ is called parity subfamily of \mathcal{L} , or simply a parity family, if*

$$\forall A, B \in \mathcal{L} \setminus \mathcal{P}: \quad A \cap B \in \mathcal{P} \iff A \cup B \in \mathcal{P} .$$

It is easy to see that every triple family is a parity family. An example for triple families (and hence also for parity families) is the following. Let $m \in \mathbb{Z}_{>0}$, let $r \in \mathbb{Z}$, and let \mathcal{L} be a lattice family on a finite set V . Then, the family \mathcal{P} defined by

$$\mathcal{P} = \{S \in \mathcal{L} \mid |S| \not\equiv r \pmod{m}\}$$

is a triple family.

As another example, parity families include complements of lattice families: If $\mathcal{L}_1 \subseteq \mathcal{L}_2$ are lattice families on a finite set V , it can be shown that $\mathcal{L}_2 \setminus \mathcal{L}_1$ is a parity subfamily of \mathcal{L}_2 . Using a chain for \mathcal{L}_1 , it can be shown that complements of lattice families are in general not triple families [4].

The main result of Goemans and Ramakrishnan in the context of parity families is that submodular function minimisation problems over parity families can be solved efficiently. More precisely, they prove the following theorem.

Theorem 1.3 (Goemans and Ramakrishnan, [4]). *For a finite set V , let \mathcal{L} be a lattice family on V , let \mathcal{P} be a parity subfamily of \mathcal{L} , and let f be a submodular function on \mathcal{L} . Then, a set minimising f over \mathcal{P} can be obtained in oracle-polynomial time by solving $\mathcal{O}(|V|^2)$ submodular function minimisation problems over sublattices of \mathcal{L} .*

The algorithm provided by Goemans and Ramakrishnan shows that we can drop the constraint of optimising over the parity family \mathcal{P} by replacing it with a condition of the following form: For two elements a and b of the ground set, optimise only over those sets in the lattice family \mathcal{L} that contain a but not b . Goemans and Ramakrishnan show that there exist two elements a and b such that this approach returns an optimal set. Consequently, enumeration over all $\mathcal{O}(|V|^2)$ possible pairs (a, b) gives the above theorem.

As we show in the next section, we are able to obtain results similar to Theorem 1.3 for new types of subfamilies of \mathcal{L} .

1.3 Our results

Our results origin in studying the problem of minimising submodular functions over intersections of parity families. We obtain efficient algorithms in two special cases, the first being so-called *congruency constrained families*. Congruency constrained families are set families of the form

$$\mathcal{F} = \{S \in \mathcal{L} \mid |S| \equiv r \pmod{m}\} ,$$

where \mathcal{L} is a lattice family, $m \in \mathbb{Z}_{>0}$, and $r \in \mathbb{Z}$. We call m the modulus of the family. To see that these families can be written as intersections of parity families, let

$$\mathcal{P}_{r,m} = \{S \in \mathcal{L} \mid |S| \not\equiv r \pmod{m}\}$$

denote the example parity family considered in the previous chapter. Then, we have

$$\mathcal{F} = \mathcal{P}_{r+1,m} \cap \mathcal{P}_{r+2,m} \cap \dots \cap \mathcal{P}_{r+m-1,m} ,$$

so congruency constrained families with modulus m can be written as an intersection of $m - 1$ parity families.

We call the problem of minimising submodular functions over congruency constrained families *congruency constrained submodular minimisation*. Formally, this problem is defined as follows.

Congruency constrained submodular minimisation (CSM)
<p>Let V be a finite set, let \mathcal{L} be a lattice family on V and let $f: \mathcal{L} \rightarrow \mathbb{Z}$ be a submodular function. Let $m \in \mathbb{Z}_{>0}$ and let $r \in \mathbb{Z}$. Find a set minimising f over the family</p> $\mathcal{F} = \{S \in \mathcal{L} \mid S \equiv r \pmod{m}\} .$

For easier referencing, we call the above setting a CSM problem with parameters $(V, \mathcal{L}, f, m, r)$. Additionally, we call m the *modulus* of the CSM problem.

Our main result in the context of CSM problems is the following.

Theorem 1.4. *Let m be a prime power. Consider a CSM problem with parameters $(V, \mathcal{L}, f, m, r)$. A set minimising f over \mathcal{F} can be obtained by solving $\mathcal{O}(|V|^{2(m-1)})$ submodular function minimisation problems over sublattices of \mathcal{L} .*

Note that if the modulus m is a constant, then the above theorem implies that CSM problems can be solved in oracle-polynomial time.

Already at this point, we emphasise an important detail in the above theorem: While CSM problems can be considered for arbitrary positive integral moduli m , our approaches yield the above result only for prime power moduli. It is not clear whether a transition to general composite moduli is possible. We are able to show that already with modulus 6, our current approaches are not strong enough.

We also introduce a generalisation of CSM problems, so-called *generalised congruency constrained submodular minimisation* (GCSM) problems, which allow putting congruency constraints on the size of intersections with certain fixed subsets of the ground set. The formal definition is given below.

**Generalised congruency constrained submodular
minimisation (GCSM)**

Let V be a finite set, let \mathcal{L} be a lattice family on V and let $f: \mathcal{L} \rightarrow \mathbb{Z}$ be a submodular function. Let $S_1, \dots, S_k \subseteq V$ be non-empty, where $k \in \mathbb{Z}_{>0}$. Let $m \in \mathbb{Z}_{>0}$ and let $r_1, \dots, r_k \in \mathbb{Z}$. Find a set minimising f over the family

$$\mathcal{F} = \{S \in \mathcal{L} \mid \forall i \in [k]: |S \cap S_i| \equiv r_i \pmod{m}\} .$$

Similar as for CSM problems, we call the above setting a GCSM problem with parameters $(V, \mathcal{L}, f, \{S_1, \dots, S_k\}, m, \{r_1, \dots, r_k\})$, where m is the *modulus* of the problem. Moreover, we say that in the above setting, \mathcal{F} is a generalised congruency constrained family with k constraints and modulus m . Obviously, GCSM problems generalise CSM problems: Every CSM problem with parameters $(V, \mathcal{L}, f, m, r)$ can be seen as a GCSM problem with parameters $(V, \mathcal{L}, f, \{V\}, m, \{r\})$.

Our main theorem for GCSM problems is the following.

Theorem 1.5. *Let m be a prime power. Consider a GCSM problem with parameters $(V, \mathcal{L}, f, \{S_1, \dots, S_k\}, m, \{r_1, \dots, r_k\})$. A set minimising f over \mathcal{F} can be obtained by solving $\mathcal{O}(|V|^{2k(m-1)})$ submodular function minimisation problems over sublattices of \mathcal{L} .*

As for CSM problems, our approaches for GCSM problems are limited to prime power moduli. In the case of prime power moduli, however, the above theorem show that GCSM problems can be solved in oracle-polynomial time provided that the modulus m and the number of constraints k are constant.

Note that again, the family \mathcal{F} in a GCSM problem can be written as an intersection of parity families. To see this, note that for every i , the family

$$\mathcal{P}_{r,m}^{(i)} = \{S \in \mathcal{L} \mid |S \cap S_i| \not\equiv r \pmod{m}\}$$

is a parity family, and we have

$$\mathcal{F} = \bigcap_{i \in [k]} \left(\mathcal{P}_{r_i+1,m}^{(i)} \cap \mathcal{P}_{r_i+2,m}^{(i)} \cap \dots \cap \mathcal{P}_{r_i+m-1,m}^{(i)} \right) .$$

Hence, \mathcal{F} is an intersection of $k(m-1)$ parity families.

Besides providing efficient algorithms for solving GCSM problems, we also explore structural results and reductions between GCSM problems of certain kinds. It turns out, for example, that GCSM problems can always be reduced to problems where the sets S_1, \dots, S_k are disjoint. Another interesting result is that the seemingly more general GCSM problems, where we allow a different modulus for each congruency constraint, can be reduced to GCSM problems with a single constraint given that the moduli are pairwise coprime. The modulus in the problem that we reduce to then is the product of the prior moduli.

1.4 Organisation of the thesis

The remaining part of this thesis is organised as follows. In Chapter 2, we introduce the algorithmic approach that we use to solve both CSM and GCSM problems, namely partial enumeration procedures. Aspects of running time and ideas towards proving correctness of such algorithms for specific problems are also discussed there.

Chapter 3 provides methods to prove correctness of partial enumeration procedures for minimisation of submodular functions over subfamilies of lattices. Among others, sufficient conditions for correctness in terms of existence of certain set systems are deduced. Besides that, a framework for working with and transforming set systems with certain relevant properties is introduced. As a side result, we also present a necessary condition for partial enumeration procedures to successfully solve the general problem of minimising submodular functions over intersections of parity families.

The next two chapters apply the results from Chapter 3 to the specific settings of CSM and GCSM problems. For both problems, we reduce showing correctness of certain partial enumeration procedures to showing inexistence of certain systems of sets with congruency constrained cardinalities. Remarkably, this reduces correctness proofs to purely combinatorial questions.

Chapter 4 focuses on CSM problems. We provide three proofs of different generality for correctness of certain partial enumeration procedures for solving CSM problems in the case of prime power moduli. For extensions beyond prime power moduli, we show that our current approaches reach their limits and can—for combinatorial reasons—not be immediately extended.

The more general GCSM problems are the focus of Chapter 5. Here, we extend the methods that we saw for CSM problems to also give the claimed result for GCSM problems in the case of prime power moduli. Additionally, two reductions between certain types of GCSM problems are shown.

Last but not least, Chapter 6 contains conclusions and hints at open problems in context with the topics discussed in this thesis.

Chapter 2

Partial enumeration procedures

The algorithmic approaches for the constrained submodular minimisation problems that we study in this thesis are all of the same type: They rely on simplifying constraints by guessing a certain number of elements that are contained in an optimal solution and some that are not. In this chapter, we formalise this guessing approach in what we call a partial enumeration procedure and briefly discuss the time complexity of the corresponding algorithms.

We consider a constrained submodular minimisation problem in its most general form. Let V be a finite set, let \mathcal{L} be a lattice family on V and let $f: \mathcal{L} \rightarrow \mathbb{Z}$ be a submodular function. Given a subfamily $\mathcal{F} \subseteq \mathcal{L}$, we want to find a set $S \in \mathcal{F}$ minimising the function f over \mathcal{F} .

As indicated in the introduction, Goemans and Ramakrishnan considered the case where the family \mathcal{F} is a parity subfamily of the lattice family \mathcal{L} and provided an efficient algorithm for solving such problems [4]. In their work, the main algorithmic idea is to fix two elements a and b of the ground set, and to minimise f over all sets in the lattice family \mathcal{L} that contain a but not b . They show that there exist elements a and b such that the minimal minimiser obtained this way is, in fact, a set minimising f over the parity family \mathcal{F} . Consequently, by trying all pairs (a, b) and comparing the results, an optimal solution for the initial problem can be found.

Inspired by this algorithm for parity families \mathcal{F} , we investigate more general approaches of a similar type. Instead of fixing single elements a and b , we fix subsets of bounded cardinality. The precise formulation is presented in Algorithm 2.1.

Algorithm 2.1: Partial enumeration procedure of order d

Input: A submodular function f on a lattice family \mathcal{L} on a finite set V , a subfamily \mathcal{F} of \mathcal{L} .

Output: A set $S^* \in \mathcal{F}$, or “*The problem is infeasible!*”.

1. For all $A, B \subseteq V$ with $|A|, |B| \leq d$ and $A \cap B = \emptyset$, let S_{AB} be a minimal set minimising f over the family

$$\mathcal{L}_{AB} := \{S \in \mathcal{L} \mid A \subseteq S \subseteq V \setminus B\} .$$

Let \mathcal{S} be the family of all these sets S_{AB} .

2. If none among the sets in \mathcal{S} lie in \mathcal{F} , then return “*The problem is infeasible!*”.
3. Otherwise, among the sets in \mathcal{S} , let S^* be one minimising f . Return S^* .

Note that in the first step of the partial enumeration procedure, where we minimise f over the family \mathcal{L}_{AB} , we in fact optimise over all sets containing all elements of A , but none from B . Also note that the *order d* of the guessing procedure is an upper bound on the number of elements that we fix inside and outside of the solution.

As in our settings, the goal is to find algorithms for prescribed constrained families while the submodular function is kept general, the following definition is natural.

Definition 2.1. *Let V be a finite set, let \mathcal{L} be a lattice family and let $\mathcal{F} \subseteq \mathcal{L}$ be a non-empty family. For $m \in \mathbb{Z}_{\geq 0}$, we say that the partial enumeration procedure of order m is correct on \mathcal{F} if for every submodular function $f: \mathcal{L} \rightarrow \mathbb{Z}$, it returns a set S^* such that*

$$f(S^*) = \min\{f(S) \mid S \in \mathcal{F}\} .$$

From an algorithmic point of view, we are not only interested in whether or not the partial enumeration procedure is correct on some family \mathcal{F} , but we are also interested in its running time.

In this context, a key property of the family \mathcal{L}_{AB} is that for all $A, B \subseteq V$, this family is itself a lattice family. To see this, let $S_1, S_2 \in \mathcal{L}_{AB}$. In particular, this implies that $S_1, S_2 \in \mathcal{L}$, so by definition of a lattice family, we get

$$S_1 \cap S_2 \in \mathcal{L} \text{ and } S_1 \cup S_2 \in \mathcal{L} .$$

Moreover, the property that $A \subseteq S_i \subseteq V \setminus B$ for $i \in \{1, 2\}$ is passed to $S_1 \cap S_2$ and $S_1 \cup S_2$. Hence, we indeed have $S_1 \cap S_2 \in \mathcal{L}_{AB}$ and $S_1 \cup S_2 \in \mathcal{L}_{AB}$, so \mathcal{L}_{AB} is a lattice family.

By this property, every minimisation problem in the first step of a partial enumeration procedure is an unconstrained submodular minimisation problem, and we know

that problems of this type can be solved in polynomial time. Consequently, the running time of the partial enumeration procedure of order m is a polynomial times the number of submodular minimisation problems solved in the first step. This number is in $\mathcal{O}(|V|^{2m})$, so we obtain the following corollary.

Corollary 2.2. *Let $|V|$ be a finite set, let \mathcal{L} be a lattice on V , let f be a submodular function on \mathcal{L} , and let $\mathcal{F} \subseteq \mathcal{L}$. If for some $d \in \mathbb{Z}_{>0}$, the partial enumeration procedure of order d is correct on \mathcal{F} , then a set minimising f over \mathcal{F} can be found by solving $\mathcal{O}(|V|^{2m})$ submodular function minimisation problems over sublattices of \mathcal{L} .*

Thus, we can minimise a submodular function over a family \mathcal{F} in oracle-polynomial time if a partial enumeration procedure of constant order is correct on \mathcal{F} .

We will show that partial enumeration procedures can be used to solve both congruency constrained submodular minimisation problems and generalised congruency constrained minimisation problems. More precisely, we show the following theorem.

Theorem 2.3. *Let \mathcal{F} be a congruency constrained subfamily of a lattice family \mathcal{L} with modulus m . Then the partial enumeration procedure of order $m - 1$ is correct on \mathcal{F} .*

The analogous theorem for generalised congruency constrained families is as follows.

Theorem 2.4. *Let \mathcal{F} be a generalised congruency constrained subfamily of a lattice family \mathcal{L} with k constraints and modulus m . Then the partial enumeration procedure of order $k(m - 1)$ is correct on \mathcal{F} .*

Proofs of these two theorems are shown in Chapter 4 and Chapter 5, respectively. Our arguments rely on general sufficient conditions for correctness of partial enumeration procedures, which are discussed in the next chapter.

In combination with Corollary 2.2, the above two theorems directly imply our main results, namely Theorem 1.4 and Theorem 1.5.

Last but not least, note that the sets S_{AB} depend only on the lattice \mathcal{L} and the submodular function f , but they are independent of the constrained subfamily \mathcal{F} . Consequently, once the sets S_{AB} are calculated, a minimiser of f over a family \mathcal{F} (assuming correctness of the partial enumeration procedure of order d on \mathcal{F}) can be found among the sets in $\mathcal{F} \cap \{S_{AB} \mid A, B \subseteq V \text{ s. t. } |A|, |B| \leq d\}$.

Proving correctness of partial enumeration procedures

In this chapter, we describe sufficient conditions for correctness of the partial enumeration procedures introduced in the previous chapter. Section 3.1 deduces a first sufficient condition on the set families underlying the minimisation problems. This sufficiency result is then further reduced to a condition in terms of inexistence of set systems with certain properties in Section 3.2. For applications of this last sufficient condition, we need tools to handle and transform set systems. These are introduced in Section 3.3. Besides sufficient conditions, we also treat a necessary condition for correctness in Section 3.4, namely a lower bound on the order of a partial enumeration procedure that is necessary to solve problems of a certain type.

3.1 A first sufficient condition for partial enumeration

Having Corollary 2.2 at hand, a natural step is to start looking for sufficient conditions on set families \mathcal{F} that guarantee correctness of a partial enumeration procedure of constant order on \mathcal{F} .

Given a lattice family \mathcal{L} on a finite set V , a subfamily $\mathcal{F} \subseteq \mathcal{L}$, and $d \in \mathbb{Z}_{>0}$, it will be important whether or not the triple $(\mathcal{L}, \mathcal{F}, d)$ has the following property.

Property 3.1. *For every submodular function $f: \mathcal{L} \rightarrow \mathbb{Z}$ and every minimiser $S^* \notin \{\emptyset, V\}$ of f over \mathcal{F} , there exists a set $A \subseteq S^*$ with $|A| \leq d$ such that*

$$\forall S \in \mathcal{L}: \quad A \subseteq S \subseteq S^* \implies f(S) \geq f(S^*) . \quad (3.1)$$

Before stating a theorem on sufficient conditions for correctness of a partial enumeration procedure, we need to introduce the following definition.

Definition 3.2. *Let \mathcal{F} be a family of sets on a finite set V . Then, we define the family $\text{comp}(\mathcal{F})$ to be the set family given by $\text{comp}(\mathcal{F}) = \{S \subseteq V \mid V \setminus S \in \mathcal{F}\}$.*

In other words, $\text{comp}(\mathcal{F})$ is the family of all complements of sets in \mathcal{F} . Note that if \mathcal{L} is a lattice family, then $\text{comp}(\mathcal{L})$ is a lattice family, as well. Moreover, if $\mathcal{F} \subseteq \mathcal{L}$, then we also have $\text{comp}(\mathcal{F}) \subseteq \text{comp}(\mathcal{L})$. With these observations, we are ready to state the main reduction theorem of this section.

Theorem 3.3. *Let V be a finite set, let \mathcal{L} be a lattice family and let $\mathcal{F} \subseteq \mathcal{L}$. For $d \in \mathbb{Z}_{>0}$, the partial enumeration procedure of order d is correct on \mathcal{F} if the triples $(\mathcal{L}, \mathcal{F}, d)$ and $(\text{comp}(\mathcal{L}), \text{comp}(\mathcal{F}), d)$ both have Property 3.1.*

In the rest of this section, we present a proof of Theorem 3.3. We first show two lemmas about implications of the assumption that $(\mathcal{L}, \mathcal{F}, d)$ and $(\text{comp}(\mathcal{L}), \text{comp}(\mathcal{F}), d)$ both have Property 3.1. The first lemma shows that if we restrict our attention to minimal minimisers S^* in Property 3.1, then we get the strict inequality in (3.1).

Lemma 3.4. *Let V be a finite set, let \mathcal{L} be a lattice family and let $\mathcal{F} \subseteq \mathcal{L}$. If the triple $(\mathcal{L}, \mathcal{F}, d)$ has Property 3.1, then for every submodular function $f: \mathcal{L} \rightarrow \mathbb{Z}$ and for all minimal minimisers $S^* \notin \{\emptyset, V\}$ of f over \mathcal{F} , there exists a set $A \subseteq S^*$ with $|A| \leq d$ such that*

$$\forall S \in \mathcal{L}: \quad A \subseteq S \subsetneq S^* \implies f(S) > f(S^*) .$$

Proof. Fix a submodular function $f: \mathcal{L} \rightarrow \mathbb{Z}$ and a minimal minimiser S^* of f over \mathcal{F} and let the function $g: \mathcal{L} \rightarrow \mathbb{Z}$ be defined by

$$g(S) = |V| \cdot f(S) + |V| \cdot |S \setminus S^*| + |S| \quad \text{for all } S \in \mathcal{L} .$$

We now prove the following two claims.

Claim 1: S^* is a minimiser of g over \mathcal{F} .

By definition of S^* , we know that for all $S \in \mathcal{F}$, we have $f(S) \geq f(S^*)$. We now distinguish two cases. If $f(S) \geq f(S^*) + 1$, we get

$$\begin{aligned} g(S) &\geq |V| \cdot f(S) \\ &\geq |V| \cdot (f(S^*) + 1) \\ &\geq |V| \cdot f(S^*) + |S^*| = g(S^*) . \end{aligned}$$

If, in the other case, $f(S) = f(S^*)$, we know from minimality of S^* that $S \setminus S^* \neq \emptyset$, hence $|S \setminus S^*| \geq 1$, so

$$\begin{aligned} g(S) &\geq |V| \cdot f(S) + |V| \cdot |S \setminus S^*| \\ &\geq |V| \cdot f(S^*) + |V| \\ &\geq |V| \cdot f(S^*) + |S^*| = g(S^*) . \end{aligned}$$

In both cases, we got $g(S) \geq g(S^*)$ for all $S \in \mathcal{F}$, so indeed, S^* is a minimiser of g over \mathcal{F} .

Claim 2: For all sets $S \subsetneq S^*$, $g(S) \geq g(S^*)$ implies $f(S) > f(S^*)$.

As we only consider sets $S \subsetneq S^*$, the term $|V| \cdot |S \setminus S^*|$ is always zero, so the inequality $g(S) \geq g(S^*)$ can be rewritten in the form

$$|V| \cdot f(S) + |S| \geq |V| \cdot f(S^*) + |S^*| .$$

As $S \subsetneq S^*$, we have $|S| < |S^*|$, so for the above inequality to hold true, we must have $f(S) > f(S^*)$, which is what we wanted to prove.

Now note that as a linear combination of the three submodular functions $S \mapsto f(S)$, $S \mapsto |S \cap S^*|$ and $S \mapsto |S|$, the function g is itself submodular. By the first claim, we can apply Property 3.1 to the triple $(\mathcal{L}, \mathcal{F}, d)$ with the function g and the minimiser S^* , so we get that there exists a set $A \subseteq S^*$ with $|A| \leq d$ such that

$$\forall S \in \mathcal{L}: \quad A \subseteq S \subseteq S^* \implies g(S) \geq g(S^*) .$$

By the second claim, the last inequality implies $f(S) > f(S^*)$ whenever $A \subseteq S \subsetneq S^*$, which is what we wanted to show. \square

The following lemma deals with implications of the second assumption in Theorem 3.3, namely that the triple $(\text{comp}(\mathcal{L}), \text{comp}(\mathcal{F}), d)$ has Property 3.1.

Lemma 3.5. *Let V be a finite set, let \mathcal{L} be a lattice family and let $\mathcal{F} \subseteq \mathcal{L}$. If the triple $(\text{comp}(\mathcal{L}), \text{comp}(\mathcal{F}), d)$ has Property 3.1, then for every submodular function $f: \mathcal{L} \rightarrow \mathbb{Z}$, either one of \emptyset and V is a minimiser of f over \mathcal{F} , or for all minimisers $S^* \notin \{\emptyset, V\}$ of f over \mathcal{F} , there exists a set $B \subseteq V \setminus S^*$ with $|B| \leq d$ such that*

$$\forall S \in \mathcal{L}: \quad S^* \subseteq S \subseteq V \setminus B \implies f(S) \geq f(S^*) .$$

Proof. Fix a minimiser S^* of f over \mathcal{F} . Let the function $f': \text{comp}(\mathcal{L}) \rightarrow \mathbb{Z}$ be given by $f'(S) = f(V \setminus S)$ for all $S \in \text{comp}(\mathcal{L})$. Note that then, f' is submodular, and $V \setminus S^*$ is a minimiser of f' over $\text{comp}(\mathcal{F})$. Invoking Property 3.1 for the triple $((\text{comp}(\mathcal{L}), \text{comp}(\mathcal{F}), d)$ with the submodular function f and the minimiser $V \setminus S^*$, we get the existence of a set $B \subseteq V \setminus S^*$ with $|B| \leq d$ such that

$$\forall S' \in \text{comp}(\mathcal{L}): \quad B \subseteq S' \subseteq V \setminus S^* \implies f'(S') \geq f'(V \setminus S^*) .$$

Rewriting the above with $S = V \setminus S'$, we get the equivalent statement

$$\forall S \in \mathcal{L}: \quad B \subseteq V \setminus S \subseteq V \setminus S^* \implies f(S) \geq f(S^*) .$$

As furthermore, $B \subseteq V \setminus S \subseteq V \setminus S^*$ is equivalent to $S^* \subseteq S \subseteq V \setminus B$, this is precisely the statement that we wanted to prove. \square

Using Lemma 3.4 and Lemma 3.5, we can now prove Theorem 3.3.

Proof of Theorem 3.3. Fix a submodular function $f: \mathcal{L} \rightarrow \mathbb{Z}$ and a minimal minimiser S^* of f over \mathcal{F} . By Lemma 3.4 and Lemma 3.5, there exist sets $A \subseteq S^*$ and $B \subseteq V \setminus S^*$ with $|A|, |B| \leq d$ and such that for all $S \in \mathcal{L}$, we have

$$A \subseteq S \subsetneq S^* \implies f(S) > f(S^*) , \quad (3.2)$$

$$\text{and } S^* \subseteq S \subseteq V \setminus B \implies f(S) \geq f(S^*) . \quad (3.3)$$

We claim that in the first step of the partial enumeration procedure of order d , we find $S_{AB} = S^*$. Assuming this claim, the partial enumeration procedure obviously also returns a correct solution, hence it is correct on \mathcal{F} .

Consequently, it only remains to show $S_{AB} = S^*$, where S_{AB} is a minimal minimiser of f over \mathcal{L}_{AB} . As $S^* \in \mathcal{L}_{AB}$, we have $f(S^*) \geq f(S_{AB})$. Together with submodularity of f , we get

$$2f(S^*) \geq f(S^*) + f(S_{AB}) \geq f(S^* \cap S_{AB}) + f(S^* \cup S_{AB}) . \quad (3.4)$$

Now note that $S^* \cup S_{AB}$ is a set in \mathcal{L}_{AB} with $S^* \subseteq S^* \cup S_{AB} \subseteq V \setminus B$, so by (3.3), we have $f(S^* \cup S_{AB}) \geq f(S^*)$. Using this inequality in (3.4) and subtracting $f(S^*)$, we get the chain

$$f(S^*) \geq f(S_{AB}) \geq f(S^* \cap S_{AB}) . \quad (3.5)$$

To finish the argument, note that $S^* \cap S_{AB}$ is a set in \mathcal{L}_{AB} with $A \subseteq S^* \cap S_{AB}$. Hence if $S^* \cap S_{AB} \subsetneq S^*$, then by (3.2), we get $f(S^* \cap S_{AB}) > f(S^*)$, contradicting (3.5). Consequently, we must have $S^* \cap S_{AB} = S^*$. This has two implications. On the one hand, it implies $f(S^* \cap S_{AB}) = f(S^*)$, and hence equality in (3.5). This gives $f(S^*) = f(S_{AB})$, so S^* is a minimiser of f over \mathcal{L}_{AB} . On the other hand, $S^* \cap S_{AB} = S^*$ also implies that $S^* \subseteq S_{AB}$, so minimality of S_{AB} lets us conclude $S_{AB} = S^*$. This proves Theorem 3.3. \square

Remark 3.6. We remark that in the above proof, we in fact show that under the assumptions of Theorem 3.3, *every* minimal set S^* minimising f over \mathcal{F} has the property that there exist $A, B \subseteq V$ with $|A|, |B| \leq d$ such that the partial enumeration procedure of order d finds $S_{AB} = S^*$. Consequently, the partial enumeration procedure of order d can be used to find all minimal sets minimising f over \mathcal{F} . This property was already remarked by Goemans and Ramakrishnan for their algorithm for submodular minimisation over parity families [4]. The above shows that our generalised approach of partial enumeration procedures allows for the same conclusion if correctness is proved through Theorem 3.3.

3.2 Set systems and a second sufficient condition

The next reduction of Theorem 3.3 that we show reduces correctness of a partial enumeration procedure on some family \mathcal{F} to inexistence of set systems with certain properties. Thus, we start by introducing terminology for set systems.

Definition 3.7. *Let \mathcal{S} be a family of sets and let T be a finite set.*

- (i) \mathcal{S} is a set system on T if for every $S \in \mathcal{S}$, we have $S \subseteq T$.
- (ii) \mathcal{S} is intersection-closed if for any $S_1, S_2 \in \mathcal{S}$, we have $S_1 \cap S_2 \in \mathcal{S}$.
- (iii) For $k \in \mathbb{Z}_{\geq 0}$, \mathcal{S} is a k -covering set system on T if

$$\forall U \subseteq T : |U| \leq k \implies \exists S \in \mathcal{S} : U \subseteq S .$$

In other words, \mathcal{S} is k -covering if for any at most k elements of T , there exists a set in \mathcal{S} containing all of them. Using this definition, we can state the following theorem.

Theorem 3.8. *Let \mathcal{L} be a lattice family on a finite set V , let $\mathcal{F} \subseteq \mathcal{L}$ and let $d \in \mathbb{Z}_{>0}$. The triple $(\mathcal{L}, \mathcal{F}, d)$ has Property 3.1 if there does not exist a d -covering intersection-closed set system \mathcal{S} on a non-empty finite ground set T with the property that $T \in \mathcal{F}$, but $S \in \mathcal{L} \setminus \mathcal{F}$ for all $S \in \mathcal{S}$.*

Combining the above theorem with Theorem 3.3, i.e., applying Theorem 3.8 to both $(\mathcal{L}, \mathcal{F}, d)$ and $(\text{comp}(\mathcal{L}), \text{comp}(\mathcal{F}), d)$, we immediately get the following corollary.

Corollary 3.9. *Let \mathcal{L} be a lattice family. The partial enumeration procedure of order d is correct on a subfamily $\mathcal{F} \subseteq \mathcal{L}$ if the following two properties hold true.*

- (i) *There does not exist a d -covering intersection-closed set system \mathcal{S} on a non-empty finite ground set T with the property that $T \in \mathcal{F}$, but $S \in \mathcal{L} \setminus \mathcal{F}$ for all $S \in \mathcal{S}$.*
- (ii) *There does not exist a d -covering intersection-closed set system \mathcal{S} on a non-empty finite ground set T with the property that $T \in \text{comp}(\mathcal{F})$, but $S \in \text{comp}(\mathcal{L}) \setminus \text{comp}(\mathcal{F})$ for all $S \in \mathcal{S}$.*

Corollary 3.9 will be applied in Chapter 4 and Chapter 5 to deduce our results on congruency constrained and generalised congruency constrained submodular minimisation problems. For a conclusion of this section, we prove Theorem 3.8.

Proof of Theorem 3.8. We show the contrapositive, namely that if the triple $(\mathcal{L}, \mathcal{F}, d)$ does not have Property 3.1, then there exists a d -covering intersection-closed set system \mathcal{S} on a non-empty finite ground set T with the property that $T \in \mathcal{F}$, but $S \in \mathcal{L} \setminus \mathcal{F}$ for all $S \in \mathcal{S}$.

By definition of Property 3.1, if the triple $(\mathcal{L}, \mathcal{F}, d)$ does not have that property, then for some minimiser $T \notin \{\emptyset, V\}$ of f over \mathcal{F} , we know that for every set $A \subseteq T$ with $|A| \leq d$, there is a set $S \in \mathcal{L}$ such that $A \subseteq S \subseteq T$, but $f(S) < f(T)$. Let S_A be a maximal such set.

Let $\mathcal{T} = \{Q \subseteq T \mid |Q| \leq d\} \setminus \emptyset$ denote the family of all non-empty subsets of T of cardinality at most d . Moreover, for a family $\mathcal{A} \subseteq \mathcal{T}$, we write $S_{\mathcal{A}} := \bigcap_{A \in \mathcal{A}} S_A$. We claim that the set system

$$\mathcal{S} := \{S_{\mathcal{A}} \mid \mathcal{A} \subseteq \mathcal{T}\}$$

is a d -covering intersection-closed set system on the non-empty ground set T with the property that $T \in \mathcal{F}$, but $S \notin \mathcal{F}$ for all $S \in \mathcal{S}$. We prove this in four steps.

Step 1: \mathcal{S} is a d -covering set system on T .

All sets S_A are subsets of T . Consequently, all sets in \mathcal{S} are subsets of T , as well, so \mathcal{S} is indeed a set system on T .

Let $A \subseteq T$ be a subset with $|A| \leq d$. Then, by definition, we have $A \subseteq S_A$ and $S_A \in \mathcal{S}$, hence \mathcal{S} is indeed a d -covering set system on T .

Step 2: \mathcal{S} is intersection-closed.

Let $\mathcal{A}, \mathcal{B} \subseteq \bigcup_{i=1}^d \binom{T}{i}$. By definition of $S_{\mathcal{A}}$ and $S_{\mathcal{B}}$, we have $S_{\mathcal{A}} \cap S_{\mathcal{B}} = S_{\mathcal{A} \cup \mathcal{B}}$. Consequently, as $\mathcal{A} \cup \mathcal{B} \subseteq \bigcup_{i=1}^d \binom{T}{i}$, this implies that $S_{\mathcal{A}} \cap S_{\mathcal{B}}$ is as well an element of \mathcal{S} , so \mathcal{S} is intersection-closed.

Step 3: $T \in \mathcal{F}$.

By definition, T is a set minimising f over \mathcal{F} , so in particular, we have $T \in \mathcal{F}$.

Step 4: For all $\mathcal{A} \subseteq \bigcup_{i=1}^d \binom{T}{i}$, we have $S_{\mathcal{A}} \in \mathcal{L} \setminus \mathcal{F}$.

Note that by definition, $S_{\mathcal{A}} \in \mathcal{L}$ for all $\mathcal{A} \subseteq T$ with $|\mathcal{A}| \leq d$. Hence, every set $S_{\mathcal{A}}$ is an intersection of sets from the lattice \mathcal{L} , and hence $S_{\mathcal{A}} \in \mathcal{L}$ holds true, as well.

Therefore, it remains to see $S_{\mathcal{A}} \notin \mathcal{F}$. To this end, we show that $f(S_{\mathcal{A}}) < f(T)$ for all $\mathcal{A} \subseteq \bigcup_{i=1}^d \binom{T}{i}$ by induction on $|\mathcal{A}|$. As T is a minimiser of f over \mathcal{F} , this immediately implies that $S_{\mathcal{A}} \notin \mathcal{F}$.

For $|\mathcal{A}| = 1$, i.e., \mathcal{A} consisting of a single set A , we have $S_{\mathcal{A}} = S_A$, and $f(S_A) < f(T)$ holds by definition of S_A . For the inductive step, consider some non-empty family $\mathcal{A} \subsetneq \bigcup_{i=1}^d \binom{T}{i}$ with $f(S_{\mathcal{A}}) < f(T)$ and a set $A \in \bigcup_{i=1}^d \binom{T}{i} \setminus \mathcal{A}$. We show that $f(S_{\mathcal{A} \cup \{A\}}) < f(T)$.

If $S_{\mathcal{A} \cup \{A\}} = S_{\mathcal{A}}$, there is nothing to show. Hence, we assume the opposite, namely $S_{\mathcal{A} \cup \{A\}} \subsetneq S_{\mathcal{A}}$. From the equivalence

$$S_{\mathcal{A} \cup \{A\}} \subsetneq S_{\mathcal{A}} \iff S_{\mathcal{A}} \cap S_A \subsetneq S_{\mathcal{A}} \iff S_{\mathcal{A}} \setminus S_A \neq \emptyset \iff S_{\mathcal{A}} \subsetneq S_{\mathcal{A}} \cup S_A$$

and the maximality of S_A , we get $f(S_{\mathcal{A}} \cup S_A) \geq f(T)$. Together with submodularity of f , we get

$$f(S_{\mathcal{A}}) + f(S_A) \geq f(S_{\mathcal{A}} \cap S_A) + f(S_{\mathcal{A}} \cup S_A) \geq f(S_{\mathcal{A} \cup \{A\}}) + f(T) .$$

Now note that by the induction basis and the inductive assumption, both terms on the left hand side are strictly smaller than $f(T)$, so we also get $f(T) > f(S_{\mathcal{A} \cup \{A\}})$. This completes the induction, and hence step 4.

The above steps show that the set system \mathcal{S} has all of the desired properties, so the proof of Theorem 3.8 is complete. \square

3.3 Set system transformations

When proving inexistence of the set systems raised in Corollary 3.9, we will repeatedly transform one set system to another. The goal of this section is to collect the theory of these transformations and to provide a basis for applying set system transformations in Chapter 4 and Chapter 5.

Cardinality transformation functions and their properties

We will use a special type of transformation maps that are characterised by the following definition.

Definition 3.10. *A map $g: \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$ is a cardinality transformation function if for every finite set V , there exists a finite set W and a map $G: 2^V \rightarrow 2^W$ with the following three properties.*

- (i) (ground set transformation) $G(V) = W$.
- (ii) (cardinality transformation) $\forall S \subseteq V: |G(S)| = g(|S|)$.
- (iii) (homomorphism w.r.t. intersection) $\forall S, T \subseteq V: G(S) \cap G(T) = G(S \cap T)$.

In this case, we call G a set transformation function for g on V .

We use cardinality transformation functions to transform set systems. If \mathcal{S} is a set system on the ground set V and g is a cardinality transformation function, then by definition, there exists a finite set W and a map $G: 2^V \rightarrow 2^W$ with properties as listed in the above definition. In particular, we can define a set system

$$\mathcal{T} := \{G(S) \mid S \in \mathcal{S}\} .$$

By definition of G , the new system \mathcal{T} is a set system on W . Slightly abusing notation, we will also write $\mathcal{T} = G(\mathcal{S})$.

Property (i) in Definition 3.10 makes sure that the ground set V of \mathcal{S} is mapped to the ground set W of \mathcal{T} , while property (ii) guarantees that cardinalities of sets are transformed via the cardinality transformation function g . The third property can be seen as a ‘‘homomorphism property’’ with respect to intersection: It states that the image of an intersection of two sets under the transformation map is the same as the intersection of the images of the two sets.

In Definition 3.7, we introduced two important properties of set systems: Intersection-closed set systems and k -covering set systems. Starting with intersection-closed systems in Lemma 3.11, we will now see how these properties are affected by set transformation functions.

Lemma 3.11. *Let \mathcal{S} be an intersection-closed set system on a finite ground set V . Let g be a cardinality transformation function and G a corresponding set transformation function $G: 2^V \rightarrow 2^W$. Then, the set system $\mathcal{T} = G(\mathcal{S})$ is intersection-closed.*

Proof. Let $T_1, T_2 \in \mathcal{T}$. By definition of \mathcal{T} , there exist two sets $S_1, S_2 \in \mathcal{S}$ such that $T_i = G(S_i)$ for $i \in \{1, 2\}$. By the homomorphism property of G with respect to intersection, we get

$$G(S_1) \cap G(S_2) = G(S_1 \cap S_2) .$$

As by assumption, \mathcal{S} is intersection-closed, we get $S_1 \cap S_2 \in \mathcal{S}$. Consequently, $G(S_1 \cap S_2) \in \mathcal{T}$, and hence also $G(S_1) \cap G(S_2) \in \mathcal{T}$, as desired. \square

While by the above lemma, the property of being intersection-closed is invariant under set transformation functions, a k -covering property is generally not. This motivates the following definition.

Definition 3.12. *Let $g: \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$ be a cardinality transformation function.*

- (i) *We say that g has covering coefficient $\alpha \in \mathbb{R}_{\geq 0}$ if for every finite set V , there exists a set transformation function G for g on V such that for every $k \in \mathbb{Z}_{\geq 0}$, the transformation $G(\mathcal{S})$ of a k -covering set system \mathcal{S} on V is an $\lfloor \alpha k \rfloor$ -covering set system on $G(V)$.*

- (ii) We say that g has level $\ell \in \mathbb{Z}_{\geq 0}$ if for every finite set V , there exists a set transformation function $G: 2^V \rightarrow 2^W$ for g on V such that for every $w \in W$, there is a set $S \subseteq V$ with $|S| \leq \ell$ and $w \in G(S)$.

Note that both the covering coefficient and the level are monotone properties in the sense that a cardinality transformation function g with covering coefficient α also has covering coefficient α' for all $\alpha' \leq \alpha$, and if g has level ℓ , then it also has level ℓ' for all $\ell' \geq \ell$. The following lemma creates a link from levels of a cardinality transformation function to covering coefficients.

Lemma 3.13. *If for some $\ell \in \mathbb{Z}_{>0}$, a cardinality transformation function has level ℓ , then it has covering coefficient $1/\ell$.*

Proof. Consider a k -covering set family \mathcal{S} on a finite ground set V and let g be a cardinality transformation function of level ℓ with a set transformation function $G: 2^V \rightarrow 2^W$ such that for all $w \in W$, there is a set $S_w \subseteq V$ with $|S_w| \leq \ell$ and $w \in G(S_w)$.

To show that $G(\mathcal{S})$ is a $\lfloor k/\ell \rfloor$ -covering set system on W , let $w_1, \dots, w_{k'}$ be $k' = \lfloor k/\ell \rfloor$ elements from W . Then,

$$\left| \bigcup_{i=1}^{k'} S_{w_i} \right| \leq k' \cdot \ell \leq k .$$

As \mathcal{S} is a k -covering set system, this implies that there exists a set $S \subseteq V$ with $\bigcup_{i=1}^{k'} S_{w_i} \subseteq S$. We claim that $G(S)$ is a set covering all the elements $w_1, \dots, w_{k'}$. Indeed, by the homomorphism property of G with respect to inclusion, we get for each $i \in [k']$ that

$$w_i \in G(S_{w_i}) = G(S_{w_i} \cap S) = G(S_{w_i}) \cap G(S) ,$$

so $w_i \in G(S)$ for all $i \in [k']$. This proves the claim and hence the lemma. \square

While the covering coefficient is what we are interested in when applying cardinality transformation functions, we will see in the next section that arguments in terms of levels are easier to handle.

Construction of cardinality transformation functions

We now provide methods for constructing cardinality transformation functions of certain types. For our constructions, we need three “elementary” cardinality transformation functions. These are presented in the following lemma.

Lemma 3.14. *The following statements hold true for every $\ell \in \mathbb{Z}_{>0}$.*

- (i) *The map $g: \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$ given by $g(x) = \ell$ is a cardinality transformation function with level 0.*
- (ii) *The map $g: \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$ given by $g(x) = x^\ell$ is a cardinality transformation function with level ℓ .*

(iii) The map $g: \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$ given by $g(x) = \binom{x}{\ell}$ is a cardinality transformation function with level ℓ .

Proof. To see that the given functions are cardinality transformation functions, we need to show that for every set V , there exists a set W and a map $G: 2^V \rightarrow 2^W$ such that properties (i), (ii) and (iii) from the definition of a cardinality transformation function hold. Additionally, we show that the levels are as indicated.

(i) Let W be a set of size ℓ and define G by $G(S) = W$ for every set $S \subseteq V$. Then, all three properties (i), (ii), and (iii) trivially hold true.

As by definition, $G(\emptyset) = W$, the cardinality transformation function in question has level 0.

(ii) For a set A , let A^ℓ denote the set of all ordered sequences of length ℓ over A . Using this notation, let $W = V^\ell$ and define $G(S) = S^\ell$ for all $S \subseteq V$. By definition, property (i) is satisfied. Moreover, a counting argument shows that $|S^\ell| = |S|^\ell$, hence

$$|G(S)| = |S^\ell| = |S|^\ell = g(|S|) ,$$

so property (ii) holds. Moreover, for all $S, T \subseteq V$, we have

$$\begin{aligned} G(S) \cap G(T) &= S^\ell \cap T^\ell = \{\text{sequences on } S\} \cap \{\text{sequences on } T\} \\ &= \{\text{sequences on elements that appear in } S \text{ and } T\} \\ &= (S \cap T)^\ell = G(S \cap T) , \end{aligned}$$

so property (iii) is satisfied as well.

The fact that g has level ℓ can be deduced from the definition of G : An element $w \in W$ is a sequence of ℓ elements of V , so the set S of all elements in w has size at most ℓ and satisfies $w \in G(S)$, as desired.

(iii) For a set A , let $\binom{A}{\ell}$ denote the set of all subsets of size ℓ of A (note that this set is empty if $\ell > |A|$). Using this notation, let $W = \binom{V}{\ell}$ and $G(S) = \binom{S}{\ell}$ for all $S \subseteq V$. By definition, this implies that property (i) holds. A counting argument shows that $|\binom{S}{\ell}| = \binom{|S|}{\ell}$, hence

$$|G(S)| = \left| \binom{S}{\ell} \right| = \binom{|S|}{\ell} = g(|S|) ,$$

so property (ii) is true. Moreover, for all $S, T \subseteq V$, we have

$$\begin{aligned} G(S) \cap G(T) &= S^\ell \cap T^\ell = \{\text{subsets of } S\} \cap \{\text{subsets of } T\} \\ &= \{\text{subsets containing only elements that appear in } S \text{ and } T\} \\ &= \binom{S \cap T}{\ell} = G(S \cap T) , \end{aligned}$$

so property (iii) is satisfied as well.

To show that g has level ℓ , we proceed similarly as before. By the above construction, an element $w \in W$ is a set of cardinality ℓ , so $S = w \subseteq V$ has the desired properties $|S| \leq \ell$ and $w \in G(S)$. \square

By Lemma 3.14, we know that constants, monomials and binomials are cardinality transformation functions. It turns out that these elementary cardinality transformation functions can be combined to obtain a larger class of functions with the same property.

Lemma 3.15. *Let g and h be cardinality transformation functions with levels ℓ_g and ℓ_h , respectively. Then, the function $g + h$ is a cardinality transformation function with level $\max\{\ell_g, \ell_h\}$.*

Proof. Let V be a finite set, and let $G: 2^V \rightarrow 2^{W_1}$ and $H: 2^V \rightarrow 2^{W_2}$ be set transformation functions for g and h on V .

We claim that the function $G \dot{\cup} H: 2^V \rightarrow 2^{W_1 \dot{\cup} W_2}$ defined by

$$(G \dot{\cup} H)(S) = G(S) \dot{\cup} H(S)$$

for all $S \subseteq V$ is a set transformation function for $g + h$ on V of level $\max\{\ell_g, \ell_h\}$. We use the symbol $\dot{\cup}$ to emphasise that we take disjoint unions of the two sets. In particular, there will be applications where elements $w \in W_1 \cap W_2$ exist – but nevertheless, we consider the union $W_1 \dot{\cup} W_2$ to contain two distinguishable copies of w , say w_1 and w_2 , that can be matched with their origin W_1 and W_2 .

For a proof of the above claim, we start with showing properties (i), (ii) and (iii) of Definition 3.10. By definition of G and H , we have $G(V) = W_1$ and $H(V) = W_2$, so $(G \dot{\cup} H)(V) = G(V) \dot{\cup} H(V) = W_1 \dot{\cup} W_2$, which is the first property.

As we consider disjoint unions, we get that for every set $S \subseteq V$,

$$|(G \dot{\cup} H)(S)| = |G(S) \dot{\cup} H(S)| = |G(S)| + |H(S)| = g(|S|) + h(|S|) = (g + h)(|S|) ,$$

so the second property holds true, as well. For showing the third one, let $S, T \subseteq V$ and observe that

$$\begin{aligned} (G \dot{\cup} H)(S) \cap (G \dot{\cup} H)(T) &= (G(S) \dot{\cup} H(S)) \cap (G(T) \dot{\cup} H(T)) \\ &= (G(S) \cap G(T)) \dot{\cup} (H(S) \cap H(T)) \\ &= G(S \cap T) \dot{\cup} H(S \cap T) \\ &= (G \dot{\cup} H)(S \cap T) , \end{aligned}$$

where we used that the homomorphism property with respect to intersection holds for G and H . This establishes the third property, so we proved that $g + h$ is a cardinality transformation function.

To see that $g + h$ has level $\ell := \max\{\ell_g, \ell_h\}$, consider let $w \in W$. Note that as $W = G(V) \dot{\cup} H(V)$, we have $w \in G(V)$ or $w \in H(V)$. If $w \in G(V)$, then from the fact that G has level $\ell_1 \leq \ell$, we know that there is a set $S \subseteq V$ such that $|S| \leq \ell$ and $w \in G(S)$. Consequently, we also have $w \in (G \dot{\cup} H)(S)$. If $w \in H(V)$, the same steps provide a set S with $|S| \leq \ell$ and $w \in (G \dot{\cup} H)(S)$.

This finishes the proof of the lemma. □

Of course, we can iteratively apply Lemma 3.15 to obtain results for linear combinations of cardinality transformation functions. Using the three elementary types of cardinality transformation functions shown in Lemma 3.14 and applying Lemma 3.13 to do the transition from levels to covering coefficients, we get the following last result of this preparatory chapter.

Corollary 3.16. *Let $k \in \mathbb{Z}_{\geq 0}$ and let $a_0, \dots, a_k \in \mathbb{Z}_{\geq 0}$ with $a_k > 0$. Then, the maps $g, h: \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$ given by*

$$g(x) = a_0 + a_1x + \dots + a_kx^k$$

and $h(x) = a_0 + a_1 \binom{x}{1} + \dots + a_k \binom{x}{k}$

are cardinality transformation functions with covering coefficient $1/k$.

Generalised cardinality transformation functions

Besides the cardinality transformation functions found above, we also use a more general form of such functions. These are introduced in the following definition.

Definition 3.17. *A map $g: \mathbb{Z}_{\geq 0}^k \rightarrow \mathbb{Z}_{\geq 0}$ is a generalised cardinality transformation function if for every finite set V and k subsets $S_1, \dots, S_k \subseteq V$, there exists a finite set W and a map $G: 2^V \rightarrow 2^W$ with the following three properties.*

- (i) (ground set transformation) $G(V) = W$.
- (ii) (cardinality transformation) $\forall S \subseteq V: |G(S)| = g(|S_1 \cap S|, \dots, |S_k \cap S|)$.
- (iii) (homomorphism w.r.t. intersection) $\forall S, T \subseteq V: G(S) \cap G(T) = G(S \cap T)$.

In this case, we call G a set transformation function for g on V with respect to S_1, \dots, S_k .

Note that this definition is compatible with Definition 3.10 for cardinality transformation functions, which we recover for $k = 1$ and $S_1 = V$. For a set system \mathcal{S} on a finite set V and a generalised cardinality transformation function g , we can use a corresponding set transformation function with respect to some fixed sets S_1, \dots, S_k to transform the system \mathcal{S} to the system $\mathcal{T} = G(\mathcal{S})$ as defined earlier.

As before, intersection-closedness is preserved under such transformations. Analogously to the situation with cardinality transformation functions, we can define covering coefficients and the level of generalised cardinality transformation functions following Definition 3.12, and we can observe that Lemma 3.13 extends the connection between level and covering coefficient to the generalised setting.

To get examples of cardinality transformation functions, the results of Corollary 3.16 can be easily generalised to obtain generalised cardinality transformation functions of the form

$$g(x_1, \dots, x_k) = p_1(x_1) + p_2(x_2) + \dots + p_k(x_k) ,$$

where p_i are polynomials or linear combinations of binomial coefficients, and the covering coefficient of such a generalised cardinality transformation is $1/\max_{i \in [k]} \deg(p_i)$.

We do not go into the details of proving these properties and only do so for a particular generalised cardinality transformation function that we need later, namely the product function $g(x_1, \dots, x_k) = x_1 \cdot \dots \cdot x_k$.

Lemma 3.18. *Let $k \in \mathbb{Z}_{\geq 0}$. The map $g: \mathbb{Z}_{\geq 0}^k \rightarrow \mathbb{Z}$ given by $g(x_1, \dots, x_k) = x_1 \cdot \dots \cdot x_k$ is a generalised cardinality transformation function with covering coefficient $1/k$.*

Proof. Let V be a finite set and let $S_1, \dots, S_k \subseteq V$. Let $W = S_1 \times \dots \times S_k$ and define $G: 2^V \rightarrow 2^W$ by

$$G(S) = (S_1 \cap S) \times (S_2 \cap S) \times \dots \times (S_k \cap S)$$

for all $S \subseteq V$. We claim that this map G is a set transformation function for g on V with respect to S_1, \dots, S_k . To check this, note that point (i) of Definition 3.17 is satisfied because $S_i \subseteq V$ for all $i \in [k]$ implies $S_i \cap V = S_i$, hence

$$G(V) = (S_1 \cap V) \times (S_2 \cap V) \times \dots \times (S_k \cap V) = S_1 \times S_2 \times \dots \times S_k = W .$$

For point (ii), observe that the cardinality of a product of sets equals the product of the cardinalities of the sets, and so for all $S \subseteq V$, we have

$$|G(S)| = |(S_1 \cap S) \times (S_2 \cap S) \times \dots \times (S_k \cap S)| = \prod_{i \in [k]} |S_i \cap S| = g(|S_1 \cap S|, \dots, |S_k \cap S|) .$$

To see that G also satisfies point (iii), note that for all $S, T \subseteq V$,

$$x \in \underbrace{(S_1 \cap S \cap T) \times \dots \times (S_k \cap S \cap T)}_{=G(S \cap T)}$$

is equivalent to having

$$x \in \underbrace{(S_1 \cap S) \times \dots \times (S_k \cap S)}_{=G(S)} \quad \text{and} \quad x \in \underbrace{(S_1 \cap T) \times \dots \times (S_k \cap T)}_{=G(T)} ,$$

hence $x \in G(S \cap T)$ iff $x \in G(S) \cap G(T)$. This proves $G(S \cap T) = G(S) \cap G(T)$.

To see that the covering coefficient of g is $1/k$, note that by Lemma 3.13, it is enough to show that the level of g is k . But this is obvious from the above: Any element $w \in W$ is a sequence of elements (s_1, \dots, s_k) with $s_i \in S_i$. Consider the set $S_w = \{s_1, \dots, s_k\}$, then $w \in G(S_w)$. As $|S_w| = k$, we conclude that g has level k , and hence covering coefficient $1/k$. \square

The methodes of the above proof combined with an adaption of Lemma 3.15 for generalised cardinality transformation functions, can be used to show, for example, that every polynomial g in k variables with positive coefficients is a generalised cardinality transformation function, and that the covering coefficient of such a polynomial is $1/\deg(g)$.

3.4 A lower bound on the order

As described in the introduction chapter, our results are efficient minimisation algorithms for special cases of a problem of the following general form: Given a lattice family \mathcal{L} , a submodular function $f: \mathcal{L} \rightarrow \mathbb{Z}$, and parity subfamilies $\mathcal{P}_1, \dots, \mathcal{P}_\ell$, find a set minimising f over the intersection $\mathcal{P}_1 \cap \dots \cap \mathcal{P}_\ell$.

For the two special cases that we consider, we show that a partial enumeration procedure of order ℓ solves the problem. The following proposition shows that in general, this order is best possible.

Proposition 3.19. *Let V be a finite set and let $\ell \in \mathbb{Z}_{>0}$. If a partial enumeration procedure of order d is correct on the family*

$$\mathcal{F} = \{S \subseteq V \mid |S| \equiv 0 \pmod{(\ell + 1)}\},$$

then $d \geq \ell$.

Note that the family \mathcal{F} in the above proposition is indeed an intersection of ℓ parity subfamilies of the lattice 2^V , namely of the families

$$\mathcal{P}_i = \{S \subseteq V \mid |S| \not\equiv i \pmod{(\ell + 1)}\}$$

for $i \in [\ell]$. Thus, the proposition indeed proves that for optimising over an intersection of ℓ parity families, the order of a correct enumeration procedure has to be at least ℓ .

Proof of Proposition 3.19. Without loss of generality, we assume that for some $n \in \mathbb{Z}_{>0}$, we have $V = \{0, 1, \dots, n\}$. To prove the above proposition, it is sufficient to provide a submodular function $f: 2^V \rightarrow \mathbb{Z}$ such that whenever we fix at most $\ell - 1$ elements of the ground set V , then every minimal set optimising f over all sets in 2^V containing these elements is not in \mathcal{F} .

To this end, we consider the submodular function $f: 2^V \rightarrow \mathbb{Z}$ given by

$$f(S) = \begin{cases} |S| & \text{if } 0 \notin S, \\ |S| - \ell - 2 & \text{if } 0 \in S. \end{cases}$$

This function corresponds to assigning weight $-(\ell + 1)$ to the element 0 and weight 1 to all other elements of V , so it is easy to see that f is submodular (and even modular). Minimising f over the congruency constrained family \mathcal{F} , we see that precisely the sets of cardinality $\ell + 1$ containing the element 0 are optimal solutions. However, if we try to find an optimal set in \mathcal{F} by fixing a set $A \subseteq V$ of at most $\ell - 1$ elements and optimising over all sets containing A , we always obtain the set $A \cup \{0\}$. For every choice of A , this set is of cardinality $\ell - 1$ or ℓ (depending on whether $0 \in A$ or not), so we never get a minimiser of f over \mathcal{F} . Thus, fixing at least ℓ elements is necessary, which means that a correct partial enumeration procedure needs order $d \geq \ell$. This proves the Proposition. \square

Congruency constrained submodular minimisation

In this Chapter, we show three different arguments of various generality that prove Theorem 2.3, namely correctness of partial enumeration procedures on congruency constrained families. All proofs rely on the reductions presented in Chapter 3 and show that set systems with certain properties do not exist. In Section 4.2, we start with an elementary approach that proves the result for prime moduli. Next, in Section 4.3, we use the previously introduced cardinality transformation functions for a first time to obtain a different proof for prime moduli. This approach using set system transformations is extended in Section 4.4 to give the result in its most general form, i.e., for prime power moduli. The penultimate section presents an argument why our current methods using set system transformations might not easily generalise to arbitrary moduli, and the last section collects result of computational experiments that we did in context with checking existence of particular set systems.

4.1 Employing sufficient conditions for correctness: Set systems

We want to prove Theorem 2.3, namely correctness of a partial enumeration procedure of order $m - 1$ on congruency constrained set families with modulus m . To this end, we use Corollary 3.9. By this result it is enough to see that for every congruency constrained subfamily \mathcal{F} of a lattice family \mathcal{L} with modulus m , the following two conditions hold true.

- (i) There does not exist an $(m - 1)$ -covering intersection-closed set system \mathcal{S} on a non-empty finite ground set T with the property that $T \in \mathcal{F}$, but $S \in \mathcal{L} \setminus \mathcal{F}$ for all $S \in \mathcal{S}$.
- (ii) There does not exist an $(m - 1)$ -covering intersection-closed set system \mathcal{S} on a non-empty finite ground set T with the property that $T \in \text{comp}(\mathcal{F})$, but $S \in \text{comp}(\mathcal{L}) \setminus \text{comp}(\mathcal{F})$ for all $S \in \mathcal{S}$.

We will see that by the following lemma, it is enough to check one of the above two points.

Lemma 4.1. *Let \mathcal{F} be a congruency constrained subfamily of a lattice family \mathcal{L} on the ground set V . Then, $\text{comp}(\mathcal{F})$ is a congruency constrained subfamily of the lattice $\text{comp}(\mathcal{L})$.*

Proof. First, note that by definition of $\text{comp}(\mathcal{F})$, every set $S \in \text{comp}(\mathcal{F})$ is the complement of a set in \mathcal{L} , so we obtain $\text{comp}(\mathcal{F}) \subseteq \text{comp}(\mathcal{L})$. Consequently, it suffices to see that $\text{comp}(\mathcal{F})$ can be written in the form of a congruency constrained subfamily of $\text{comp}(\mathcal{L})$.

Note that $\text{comp}(\mathcal{F})$ is precisely the family of all sets $S \in \text{comp}(\mathcal{L})$ of the form $S = V \setminus S'$, where $S' \in \mathcal{L}$ satisfies a constraint of the form

$$|S'| \equiv r \pmod{m} .$$

Plugging in $S' = V \setminus S$ and using $|S'| = |V| - |S|$, we can equivalently write this constraint in the form

$$|S| \equiv |V| - r \pmod{m} .$$

We obtain that $\text{comp}(\mathcal{F})$ is precisely the family of all sets $S \in \text{comp}(\mathcal{L})$ satisfying the above constraint, which is a congruency constraint. Hence, $\text{comp}(\mathcal{F})$ is a congruency constrained subfamily of $\text{comp}(\mathcal{L})$, which is what we wanted to show. \square

Using the above lemma, we see that it suffices to check that for every lattice \mathcal{L} and every congruency constrained subfamily $\mathcal{F} \subseteq \mathcal{L}$ with modulus m , there does not exist an $(m - 1)$ -covering intersection-closed set system \mathcal{S} on a non-empty finite ground set T with the property that $T \in \mathcal{F}$, but $S \in \mathcal{L} \setminus \mathcal{F}$ for all $S \in \mathcal{S}$. If we rewrite these conditions for a congruency constrained family of the form $\mathcal{F} = \{S \in \mathcal{L} \mid |S| \equiv r \pmod{m}\}$, we get

$$\begin{aligned} T \in \mathcal{F} &\iff T \in \mathcal{L} \wedge |T| \equiv r \pmod{m} , \\ S \in \mathcal{L} \setminus \mathcal{F} &\iff S \in \mathcal{L} \wedge |S| \not\equiv r \pmod{m} . \end{aligned}$$

It turns out that even without the requirements that $T \in \mathcal{L}$ and $S \in \mathcal{L}$ for all $S \in \mathcal{S}$, no set system of the prescribed type exists. More precisely, we prove the following theorem, which (by the above arguments) is sufficient for deducing correctness of partial enumeration procedures of order $m - 1$ on congruency constrained set families with modulus m , given that m is a prime power.

Theorem 4.2. *Let $m \in \mathbb{Z}_{>0}$ be a prime power and let $r \in \mathbb{Z}$. There does not exist an $(m - 1)$ -covering intersection-closed set system \mathcal{S} on a non-empty finite ground set T with the property that $|T| \equiv r \pmod{m}$, but $|S| \not\equiv r \pmod{m}$ for all $S \in \mathcal{S}$.*

In the following three sections, we will see three different proofs of Theorem 4.2, two of which only prove the special case where m is a prime number.

4.2 An elementary solution for prime moduli

The first proof of Theorem 4.2 that we show here is an elementary proof for the case where m is a prime number. To make clear that we are in the prime case here, we change notation and write p instead of m . The proof below uses a double counting argument, the inclusion-exclusion principle and Fermat's little theorem.

Proof of Theorem 4.2 (for prime moduli). Let $m = p$ be a prime number. We assume for contradiction that there exists a $(p - 1)$ -covering set system \mathcal{S} on a non-empty finite ground set T such that $|T| \equiv r \pmod{p}$, but $|S| \not\equiv r \pmod{p}$ for all $S \in \mathcal{S}$.

As a first step, we show that it suffices to consider the case where $r = 0$. Indeed, assume that there exists a set system \mathcal{S} on a non-empty finite ground set T with the prescribed properties for some $r \not\equiv 0 \pmod{p}$. Let X be a set of $p - r$ new elements and define a set system \mathcal{U} on the finite ground set $W := S \cup X$ by

$$\mathcal{U} := \{S \cup X \mid S \in \mathcal{S}\} .$$

The system \mathcal{U} inherits the properties of being $(p - 1)$ -covering and intersection-closed from \mathcal{S} . Moreover, and we have

$$|W| = |T| + |X| \equiv r + (p - r) \equiv 0 \pmod{p} ,$$

and every set $U \in \mathcal{U}$ satisfies $U = S \cup X$ for some $S \in \mathcal{S}$, hence

$$|U| = |S| + |X| \not\equiv r + (p - r) \equiv 0 \pmod{p} .$$

Altogether, we see that \mathcal{U} satisfies the set system properties in question with $r = 0$, so it suffices to prove inexistence in this case.

By the above argument, we now assume that $r = 0$ without loss of generality. We will reach a contradiction by finding two ways to count the quantity given by the sum

$$\sum_{A \in T^{p-2}} \left| \bigcup_{S \in \mathcal{S}, A \subseteq S} S \right| . \tag{4.1}$$

That is, for every ordered sequence A of $p - 2$ elements of the ground set T , we consider all sets S in the set family that contain all elements of the sequence A (which is, slightly abusing notation, denoted by $A \subseteq S$), and look at the union of these sets. Ultimately, we sum up the cardinalities of all unions obtained this way.

For a first way to calculate the above sum, fix a sequence $A = (t_1, \dots, t_{p-2}) \in T^{p-2}$ and consider only the term of the sum corresponding to A . This term is the union of all sets in \mathcal{S} containing all elements t_i for $i \in [p - 2]$. Let $t \in T$. Then, the set $\{t, t_1, \dots, t_{p-2}\}$ has cardinality at most $p - 1$, so as the set system \mathcal{S} is $(p - 1)$ -covering, there is a set in \mathcal{S} covering $\{t, t_1, \dots, t_{p-2}\}$. In particular, this set is a term in the union $\bigcup_{S \in \mathcal{S}, A \subseteq S} S$, so $t \in \bigcup_{S \in \mathcal{S}, A \subseteq S} S$. This holds for every element $t \in T$, so we conclude

$$T = \bigcup_{S \in \mathcal{S}, A \subseteq S} S ,$$

and consequently,

$$\sum_{A \in T^{p-2}} \left| \bigcup_{S \in \mathcal{S}, A \subseteq S} S \right| = \sum_{A \in T^{p-2}} |T| \equiv 0 \pmod{p}. \quad (4.2)$$

A second approach for calculating the term in (4.1) is to use the inclusion-exclusion principle for rewriting the unions. To do so, let \mathcal{S}_A , for every $A \in T^{p-2}$, be the subfamily of \mathcal{S} consisting of all the sets in \mathcal{S} containing all elements of A . We get

$$\begin{aligned} \sum_{A \in T^{p-2}} \left| \bigcup_{S \in \mathcal{S}, A \subseteq S} S \right| &= \sum_{A \in T^{p-2}} \sum_{k=1}^{|\mathcal{S}_A|} (-1)^{k+1} \sum_{\{S_1, \dots, S_k\} \subseteq \mathcal{S}_A} \left| \bigcap_{i=1}^k S_i \right| \\ &= \sum_{k=1}^{|\mathcal{S}|} \sum_{\{S_1, \dots, S_k\} \subseteq \mathcal{S}} \sum_{\substack{A \in T^{p-2}, \\ A \subseteq \bigcap_{i=1}^k S_i}} (-1)^{k+1} \left| \bigcap_{i=1}^k S_i \right|. \end{aligned}$$

To get the last representation, we changed the order of summation and adjusted summation boundaries correspondingly. Note that the summand does not depend on the innermost sum, hence

$$\sum_{A \in T^{p-2}} \left| \bigcup_{S \in \mathcal{S}, A \subseteq S} S \right| = \sum_{k=1}^{|\mathcal{S}|} \sum_{\{S_1, \dots, S_k\} \subseteq \mathcal{S}} \left| \left\{ A \in T^{p-2} \mid A \subseteq \bigcap_{i=1}^k S_i \right\} \right| (-1)^{k+1} \left| \bigcap_{i=1}^k S_i \right|.$$

The coefficient $\left| \left\{ A \in V^{p-2} \mid A \subseteq \bigcap_{i=1}^k S_i \right\} \right|$ counts the number of ways to choose an ordered sequence of $p-2$ not necessarily different elements from $\bigcap_{i=1}^k S_i$, which is equal to $\left| \bigcap_{i=1}^k S_i \right|^{p-2}$. Using this, we get

$$\sum_{A \in V^{p-2}} \left| \bigcup_{S \in \mathcal{S}, A \subseteq S} S \right| = \sum_{k=1}^{|\mathcal{S}|} \sum_{\{S_1, \dots, S_k\} \subseteq \mathcal{S}} (-1)^{k+1} \left| \bigcap_{i=1}^k S_i \right|^{p-1}.$$

By assumption, all intersections $\bigcap_{i=1}^k S_i$ have nonzero cardinality modulo p . In particular, their cardinalities are coprime to p , hence Fermat's Little Theorem implies $\left| \bigcap_{i=1}^k S_i \right|^{p-1} \equiv 1 \pmod{p}$. Plugging this in, we get

$$\begin{aligned} \sum_{A \in V^{p-2}} \left| \bigcup_{S \in \mathcal{S}, A \subseteq S} S \right| &\equiv \sum_{k=1}^{|\mathcal{S}|} \sum_{\{S_1, \dots, S_k\} \subseteq \mathcal{S}} (-1)^{k+1} \\ &\equiv \sum_{k=1}^{|\mathcal{S}|} (-1)^{k+1} \binom{|\mathcal{S}|}{k} \\ &\equiv - \left((1-1)^{|\mathcal{S}|} - 1 \right) \equiv 1 \pmod{p}. \end{aligned} \quad (4.3)$$

Here, we used that the number of choices for $\{S_1, \dots, S_k\} \subseteq \mathcal{S}$ is $\binom{|\mathcal{S}|}{k}$. The last step uses the binomial formula, where the correction -1 accounts for the missing term for $k=0$.

Comparing (4.2) and (4.3), we see that we reached a contradiction, so the set system \mathcal{S} cannot exist. This proves Theorem 4.2 for prime moduli. \square

With the above proof, we thus showed that partial enumeration procedures of order $p-1$ correctly solve congruency constrained submodular minimisation problems with prime modulus p .

4.3 Polynomial set transformations and prime moduli

In this section, we give a different proof of Theorem 4.2 for the case of prime moduli. For this proof, we use cardinality transformation functions as introduced in Section 3.3. To be precise, we use polynomial cardinality transformation functions. We show that with these functions, it is also possible to extend the result to $m = 4$, but not to any other non-prime modulus.

Before going to the details of applying cardinality transformation functions, we concentrate on the following useful lemma that will also have applications beyond this section.

Lemma 4.3. *Let $r \in \mathbb{Z}$, let $m \in \mathbb{Z}_{>0}$ and let \mathcal{S} be a 1-covering intersection-closed set system on a non-empty finite ground set T . If for all $S \in \mathcal{S}$, we have $|S| \equiv r \pmod{m}$, then we also have $|T| \equiv r \pmod{m}$.*

Proof. As \mathcal{S} is 1-covering, we have $T = \bigcup_{S \in \mathcal{S}} S$. By the inclusion-exclusion principle, we get

$$|T| = \left| \bigcup_{S \in \mathcal{S}} S \right| = \sum_{k=1}^{|\mathcal{S}|} (-1)^{k+1} \sum_{\{S_1, \dots, S_k\} \subseteq \mathcal{S}} \left| \bigcap_{i=1}^k S_i \right|.$$

By assumption, \mathcal{S} is intersection-closed, so every set of the form $\bigcap_{i=1}^k S_i$ is in fact a set in \mathcal{S} , so its cardinality is congruent to r modulo m . Plugging this in and observing that the inner sum has precisely $\binom{|\mathcal{S}|}{k}$ many terms, we get

$$\begin{aligned} |T| &\equiv \sum_{k=1}^{|\mathcal{S}|} (-1)^{k+1} \sum_{\{S_1, \dots, S_k\} \subseteq \mathcal{S}} r \\ &= \sum_{k=1}^{|\mathcal{S}|} (-1)^{k+1} \binom{|\mathcal{S}|}{k} \cdot r \\ &= - \left((1-1)^{|\mathcal{S}|} - 1 \right) \cdot r = r, \end{aligned}$$

which is what we wanted to prove. \square

With a slightly different phrasing, the above lemma was already proved by Goemans and Ramakrishnan in [4]. They use it to show correctness of the partial enumeration procedure of order 1 on parity subfamilies of a lattices \mathcal{L} of the form

$$\mathcal{P} = \{ \mathcal{S} \in \mathcal{L} \mid |\mathcal{S}| \not\equiv r \pmod{m} \},$$

where $r \in \mathbb{Z}$ and $m \in \mathbb{Z}_{>0}$. Their proof can be recovered by using Corollary 3.9 and then Lemma 4.3 for proving inexistence of the arising set systems.

We now use Lemma 4.3 for a proof of Theorem 4.2. As in the first proof that we saw, the idea is to assume for contradiction that a set system with the properties in

question exists. We will then apply a cardinality transformation function to obtain a new set system that conflicts with Lemma 4.3, giving the desired contradiction.

Second proof of Theorem 4.2 (for prime moduli). Let $m = p$ be a prime number. We assume for contradiction that there exists a $(p - 1)$ -covering set system \mathcal{S} on a non-empty finite ground set T such that $|T| \equiv r \pmod{p}$, but $|S| \not\equiv r \pmod{p}$ for all $S \in \mathcal{S}$. Moreover, we assume without loss of generality that $0 \leq r < p$.

By Corollary 3.16, we know that the map $g: \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$ defined by

$$g(x) = (x + (p - r))^{p-1} = \sum_{i=0}^{p-1} (p - r)^{p-i-1} \binom{p-1}{i} x^i$$

is a cardinality transformation function with covering coefficient $\alpha = 1/(p-1)$, as by the assumption $0 \leq r < p$, all coefficients $(p-r)^{p-i-1} \binom{p-1}{i}$ are positive. By definition of cardinality transformation functions and the covering coefficient, we know that there exists a finite set W and a map $G: 2^T \rightarrow 2^W$ such that the set system

$$\mathcal{U} = \{G(S) \mid S \in \mathcal{S}\}$$

is an $\alpha(p-1)$ -covering, i.e., 1-covering, intersection-closed set system on W . Moreover, note that by Fermat's Little Theorem, we get

$$g(x) = (x + (p - r))^{p-1} \equiv \begin{cases} 0 \pmod{p} & \text{if } x \equiv r \pmod{p} , \\ 1 \pmod{p} & \text{if } x \not\equiv r \pmod{p} . \end{cases} \quad (4.4)$$

Consequently, $|T| \equiv r \pmod{p}$ implies that we have

$$|W| = |G(T)| = g(|T|) \equiv 0 \pmod{p} , \quad (4.5)$$

while for every $U \in \mathcal{U}$, there is a set $S \in \mathcal{S}$ with $U = G(S)$, hence from $|S| \not\equiv r \pmod{p}$, we deduce

$$|U| = |G(S)| = g(|S|) \equiv 1 \pmod{p} . \quad (4.6)$$

By Lemma 4.3 applied to the 1-covering intersection-closed set system \mathcal{U} , (4.6) implies $|W| \equiv 1 \pmod{p}$, but this contradicts (4.5). That contradiction finishes this proof of Theorem 4.2 for prime moduli. \square

The crucial step in the above proof was to have a cardinality transformation function g with the property given in (4.4). In the general case with modulus m , we would need a cardinality transformation function with covering coefficient at least $1/(m-1)$ that maps all sets $S \in \mathcal{S}$ with cardinalities satisfying $|S| \not\equiv r \pmod{m}$ to sets with cardinalities equal to one common residue, and the ground set T to a set with cardinality equal to a different residue modulo m . If we restrict our attention to polynomial cardinality transformation functions, we saw that it is enough to find a polynomial g with the above properties for $r = 0$ because then, a polynomial for general r is given by $x \mapsto g(x + m - r)$.

Once we find a cardinality transformation function with these properties for some modulus m , a proof of Theorem 4.2 for that modulus can be deduced along the lines

of the above proof. For $m = 4$, for example, we see that the polynomial $g(x) = x^3 + x$ is a suitable choice, because

$$g(0) \equiv 0, \quad \text{and} \quad g(1) \equiv g(2) \equiv g(3) \equiv 2 \pmod{4} .$$

It turns out, though, that $m = 4$ this is the only case beyond prime numbers where polynomial cardinality transformation functions are sufficient for proving Theorem 4.2.

To see this, we assume for contradiction that g is a polynomial cardinality transformation function of degree k that has the desired properties. The covering coefficient of g is, by Corollary 3.16, equal to $\alpha = 1/k$. Recall that by Proposition 3.19 and its proof, a partial enumeration procedure of order $d < m - 1$ cannot generally be correct on congruency constrained families with modulus m . Using the function g , we could show correctness if $\alpha d \geq 1$ (i.e., if the transformed set system is a 1-cover, at least), so we conclude $\alpha d < 1$. In particular, for $d = m - 2$ and by plugging in $\alpha = \frac{1}{k}$, we get $k > m - 2$. Consequently, g needs degree at least $m - 1$ for the proof to work.

To reach a contradiction, we show that if there exists a polynomial cardinality transformation function g with the desired properties and degree $k > m - 2$, then there also exists such a function h with degree at most $m - 2$, which contradicts the above observation. We need the following lemma.

Lemma 4.4. *Let $m > 4$ not be prime and define the polynomial*

$$p_m(x) = (x - 1) \cdot (x - 2) \cdot (x - 3) \cdot \dots \cdot (x - m + 1) .$$

Then $p_m(j) \equiv 0 \pmod{m}$ for all $j \in \mathbb{Z}$.

Proof. Obviously, it suffices to check that $p_m(j) \equiv 0 \pmod{m}$ for $j \in \{0, \dots, m-1\}$. If $j \in \{1, 2, \dots, m-1\}$, then the factor $(x - j)$ appears in p_m , so $p_m(j) = 0$ trivially follows. Moreover,

$$\begin{aligned} p_m(0) &= (-1) \cdot (-2) \cdot (-3) \cdot \dots \cdot (-m + 1) \\ &= (-1)^{m-1} \cdot 2 \cdot 3 \cdot \dots \cdot (m - 1) = (-1)^{m-1} \cdot (m - 1)! . \end{aligned}$$

It is easy to see that for $m > 4$ not prime, we have $(m - 1)! \equiv 0 \pmod{m}$, so indeed, $p_m(j) \equiv 0 \pmod{m}$ for all $j \in \{1, 2, \dots, m - 1\}$. \square

Now, still assuming existence of the polynomial g above, for some non-prime number $m > 4$, note that by polynomial division, there exist polynomials h and q such that $\deg(h) < \deg(p_m) = m - 1$ and

$$g(x) = q(x)p_m(x) + h(x) .$$

As $p_m(x) \equiv 0 \pmod{m}$, we get $g(x) \equiv h(x) \pmod{m}$. So modulo m , h has the same values as g , and $\deg(h) < m - 1$. This is the desired contradiction. We thus know that no polynomial cardinality transformation function can extend the second proof of Theorem 4.2 to non-prime moduli other than 4.

4.4 Binomial transformations and prime power moduli

In Section 3.3, we did not only prove that polynomials are cardinality transformation functions, but also linear combinations of binomial coefficients. We will see in this section that the latter transformation functions can be used to obtain a proof of Theorem 4.2 even for prime power moduli $m = p^\alpha$. Before showing the proof, we provide some properties of binomial coefficients.

Lemma 4.5. *Let p be a prime number and let $a, b \in \mathbb{Z}_{>0}$.*

(i) *If p^α and p^β are the largest powers of p dividing a and b , respectively, and $\alpha > \beta$, then*

$$\binom{a}{b} \equiv 0 \pmod{p} .$$

(ii) *Let $\alpha \in \mathbb{Z}_{>0}$. If $b < p^\alpha$, then*

$$\binom{a + p^\alpha}{b} \equiv \binom{a}{b} \pmod{p} .$$

(iii) *Let $\alpha \in \mathbb{Z}_{>0}$. If $b < p^\alpha$, then*

$$\binom{a}{b} \equiv \binom{(a \bmod p^\alpha)}{b} \pmod{p} ,$$

where $(a \bmod p^\alpha)$ denotes the unique integer in $\{0, \dots, p^\alpha - 1\}$ congruent to a modulo p^α .

Proof. (i) Let $a = p^\alpha \cdot a'$ and $b = p^\beta \cdot b'$. Then, $p \nmid a'$ and $p \nmid b'$. By definition of the binomial coefficient, we have

$$\binom{a}{b} = \frac{a}{b} \binom{a-1}{b-1} = p^{\alpha-\beta} \frac{a'}{b'} \binom{a-1}{b-1} \in \mathbb{Z} .$$

Since $p \nmid b'$, we must have $\frac{a'}{b'} \binom{a-1}{b-1} \in \mathbb{Z}$, so as $\alpha - \beta > 0$ by assumption, the last expression is divisible by p , and hence also $\binom{a}{b}$, as desired.

(ii) Using Vandermonde's identity, we obtain

$$\binom{a + p^\alpha}{b} = \sum_{k=0}^b \binom{a}{b-k} \binom{p^\alpha}{k} . \quad (4.7)$$

Using the first part of this Lemma, we see that for $k \geq 1$, we have $\binom{p^\alpha}{k} \equiv 0 \pmod{p}$. Plugging this into (4.7), we get

$$\binom{a + p^\alpha}{b} = \sum_{k=0}^b \binom{a}{b-k} \underbrace{\binom{p^\alpha}{k}}_{\equiv 0 \text{ if } k > 0} \equiv \binom{a}{b} \pmod{p} ,$$

proving the second part of the Lemma.

(iii) The third part of this Lemma follows immediately by writing $a = (a \bmod p^\alpha) + k \cdot p^\alpha$ with $k = \lfloor \frac{a}{p^\alpha} \rfloor$ and repeated applications of the second part, namely

$$\begin{aligned} \binom{(a \bmod p^\alpha)}{b} &\equiv \binom{(a \bmod p^\alpha) + p^\alpha}{b} \equiv \binom{(a \bmod p^\alpha) + 2p^\alpha}{b} \\ &\equiv \dots \equiv \binom{(a \bmod p^\alpha) + kp^\alpha}{b} \equiv \binom{a}{b} \pmod{p}. \end{aligned}$$

This completes the proof of Lemma 4.5. \square

Alternatively, we could also use Lucas's Theorem [12] to prove the above result. Having Lemma 4.5 at hand, we are ready to give a full proof of Theorem 4.2.

Third proof of Theorem 4.2 (for prime power moduli). We denote the prime power m by $m = p^\alpha$ for a prime number p and $\alpha \in \mathbb{Z}_{>0}$. As in previous proofs, we assume for contradiction that there exists a $(p^\alpha - 1)$ -covering intersection-closed set system \mathcal{S} on a non-empty finite ground set T such that $|T| \equiv r \pmod{p^\alpha}$, but $|S| \not\equiv r \pmod{p^\alpha}$ for all $S \in \mathcal{S}$. Moreover, we assume without loss of generality that $0 \leq r < p^\alpha$.

The goal of this proof is to transform the set system \mathcal{S} to a 1-covering intersection-closed set system in which the cardinalities of all sets have the same residue, while the ground set has a different one. Then, we obtain a contradiction using Lemma 4.3.

Consider the function $g: \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$ defined by

$$g(x) = \sum_{\substack{k \text{ odd,} \\ 1 \leq k < p^\alpha}} \binom{x}{k} + \sum_{\substack{k \text{ even,} \\ 1 \leq k < p^\alpha}} (p-1) \binom{x}{k}$$

for all $x \in \mathbb{Z}_{\geq 0}$. We claim that g has the following property.

$$g(x) \equiv \begin{cases} 0 \pmod{p} & \text{if } x \equiv 0 \pmod{p^\alpha}, \\ 1 \pmod{p} & \text{if } x \not\equiv 0 \pmod{p^\alpha}. \end{cases} \quad (4.8)$$

Indeed, if $x \equiv 0 \pmod{p^\alpha}$, then by Lemma 4.5 (i), every binomial coefficient $\binom{x}{k}$ is divisible by p , so the whole sum $g(x)$ is divisible by p , as well. In other words, we have $g(x) \equiv 0 \pmod{p}$ if $x \equiv 0 \pmod{p^\alpha}$. For the case $x \not\equiv 0 \pmod{p^\alpha}$, we can apply Lemma 4.5 (iii) to reduce x modulo p^α and obtain

$$\begin{aligned} g(x) &= \sum_{\substack{k \text{ odd,} \\ 1 \leq k < p^\alpha}} \binom{x}{k} + \sum_{\substack{k \text{ even,} \\ 1 \leq k < p^\alpha}} (p-1) \binom{x}{k} \\ &\equiv \sum_{k=1}^{p^\alpha-1} (-1)^{k+1} \binom{x}{k} \equiv \sum_{k=1}^{p^\alpha-1} (-1)^{k+1} \binom{(x \bmod p^\alpha)}{k} \pmod{p}. \end{aligned}$$

Now note that $\binom{(x \bmod p^\alpha)}{k} = 0$ whenever $k > (x \bmod p^\alpha)$, so we can truncate the sum. Together with the binomial formula, we obtain

$$g(x) \equiv \sum_{k=1}^{(x \bmod p^\alpha)} (-1)^{k+1} \binom{(x \bmod p^\alpha)}{k} \equiv 1 - (1-1)^{(x \bmod p^\alpha)} \equiv 1 \pmod{p}.$$

This proves that $g(x) \equiv 1 \pmod{p}$ whenever $x \not\equiv 0 \pmod{p^\alpha}$, so we proved (4.8).

We would like to have a cardinality transformation function h with properties similar to those of g , namely

$$h(x) \equiv \begin{cases} 0 \pmod{p} & \text{if } x \equiv r \pmod{p^\alpha} , \\ 1 \pmod{p} & \text{if } x \not\equiv r \pmod{p^\alpha} . \end{cases} \quad (4.9)$$

It is easy to see that the map $h: \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$ defined by $h(x) = g(x + p^\alpha - r)$ has this property. This function h is of the form

$$h(x) = \sum_{\substack{k \text{ odd,} \\ 1 \leq k < p^\alpha}} \binom{x + p^\alpha - r}{k} + \sum_{\substack{k \text{ even,} \\ 1 \leq k < p^\alpha}} (p-1) \binom{x + p^\alpha - r}{k} .$$

Using Vandermonde's identity, namely

$$\binom{x + p^\alpha - r}{k} = \sum_{i=0}^k \binom{p^\alpha - r}{k-i} \binom{x}{i} ,$$

we see that $h(x)$ can be written as a linear combination of binomial coefficients with non-negative coefficients. The largest lower entry of these binomial coefficients with non-vanishing coefficient is $p^\alpha - 1$. Consequently, by Corollary 3.16, h is a cardinality transformation function with covering coefficient $\alpha = 1/(p^\alpha - 1)$. We use this cardinality transformation function to transform the $(p^\alpha - 1)$ -covering intersection-closed set system \mathcal{S} on the ground set T to a new set system \mathcal{U} .

As in the previous proof, the definitions of cardinality transformation functions and the covering coefficient let us deduce existence of a finite set W and a map $H: 2^T \rightarrow 2^W$ such that the set system

$$\mathcal{U} = \{G(S) \mid S \in \mathcal{S}\}$$

is an $\alpha(p^\alpha - 1)$ -covering, i.e. 1-covering, intersection-closed set system on W . Using (4.9) and $|T| \equiv 0 \pmod{p^\alpha}$, we have

$$|W| = |H(T)| = h(|T|) \equiv 0 \pmod{p} . \quad (4.10)$$

Moreover, note that every set $U \in \mathcal{U}$ can be written in the form $U = H(S)$ for some $S \in \mathcal{S}$. From (4.9) and $|S| \not\equiv 0 \pmod{p^\alpha}$, we deduce

$$|U| = |H(S)| = h(|S|) \equiv 1 \pmod{p} \quad (4.11)$$

for all $U \in \mathcal{U}$. By Lemma 4.3 applied to the 1-covering intersection-closed set system \mathcal{U} , (4.11) implies $|W| \equiv 1 \pmod{p}$, but this contradicts (4.10). This contradiction finishes this proof of Theorem 4.2 for prime power moduli. \square

The above proof finally finishes a long chain of arguments that prove correctness of partial enumeration procedures of order $m - 1$ for solving congruency constrained submodular minimisation problems with prime power modulus $m = p^\alpha$.

4.5 Obstacles for transformations in the composite case

We always emphasised that we show correctness of certain partial enumeration procedures on congruency constrained families only for the case of prime power moduli. The aim of this section is to point out that our current methods do not allow extensions beyond prime power moduli. To this end, we need two known results. The first one is a classical result by Frankl and Wilson on restricted intersections modulo primes in a set system.

Theorem 4.6 (Frankl and Wilson, [3]). *Let p be a prime number and $s \in \mathbb{Z}_{>0}$. Let $\mu_0, \mu_1, \dots, \mu_s \in \{0, 1, \dots, p-1\}$ be distinct, and let \mathcal{S} be a set system on a ground set of n elements such that there exists $k \in \mathbb{Z}$ with*

- (i) $\forall S \in \mathcal{S}: |S| = k \equiv \mu_0 \pmod{p}$,
- (ii) $\forall S_1, S_2 \in \mathcal{S}, S_1 \neq S_2: |S_1 \cap S_2| \equiv \mu_i \pmod{p}$ for some $i \in \{1, \dots, s\}$.

Then, $|\mathcal{S}| \leq \binom{n}{s}$.

While the above theorem shows that uniform set systems with restricted intersections modulo prime numbers are at most of polynomial size in the size of the ground set, it turns out that this is not true for composite moduli. Grolmusz showed the following result on large set systems with restricted intersections modulo 6.

Theorem 4.7 (Grolmusz, [5]). *There exists a constant $c > 0$ such that for every $n \in \mathbb{Z}_{\geq 0}$, there exists a set system \mathcal{S} on a ground set of n elements such that*

- (i) $|\mathcal{S}| \geq \exp\left(c \frac{\log(n)^2}{\log \log n}\right)$,
- (ii) $\forall S \in \mathcal{S}: |S| \equiv 0 \pmod{6}$,
- (iii) $\forall S_1, S_2 \in \mathcal{S}, S_1 \neq S_2: |S_1 \cap S_2| \not\equiv 0 \pmod{6}$.

To show that our set system transformation methods do not extend beyond prime power moduli, we will show that if they did, then we could transform a large set system given by Theorem 4.7 to a system contradicting Theorem 4.6.

Note that the set system transformations that we exploited in the previous sections to prove Theorem 4.2 all had a similar form. They were cardinality transformation functions $g: \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$ as provided by Corollary 3.16, namely polynomials or linear combinations of binomial coefficients. Moreover, they had the property that for some prime number p , an integer $c \not\equiv 0 \pmod{p}$ and an integer r ,

$$g(x) \equiv \begin{cases} 0 \pmod{p} & \text{if } x \equiv r \pmod{m} \\ c \pmod{p} & \text{if } x \not\equiv r \pmod{m} \end{cases} \quad (4.12)$$

holds for all $x \in \mathbb{Z}_{\geq 0}$. We now assume that such a function exists for $r = 0$. Let \mathcal{S} be a uniform set system on a finite ground set T of cardinality n that is obtained as follows: Consider the set system provided by Theorem 4.7, and let \mathcal{S} be the largest uniform subsystem. We observe that in this case, \mathcal{S} is of size at least $\frac{1}{n} \cdot \exp\left(c \frac{\log(n)^2}{\log \log n}\right)$. Furthermore, let G be a set transformation function for g on T . Using G , we can transform the system \mathcal{S} to a new system \mathcal{U} given by

$$\mathcal{U} = \{G(S) \mid S \in \mathcal{S}\}$$

on the ground set $W = G(T)$. Note that by definition of \mathcal{U} every set $U \in \mathcal{U}$ can be written in the form $U = G(S)$ for some $S \in \mathcal{S}$, and hence

$$|U| = |G(S)| = g(|S|) \equiv 0 \pmod{p}$$

holds for all $U \in \mathcal{U}$. Moreover, note that for all distinct $U_1, U_2 \in \mathcal{U}$, we can write $U_1 = g(S_1)$ and $U_2 = g(S_2)$ with $S_1, S_2 \in \mathcal{S}$ and get

$$|U_1 \cap U_2| = |G(S_1) \cap G(S_2)| = |G(S_1 \cap S_2)| = g(|S_1 \cap S_2|) \equiv c \pmod{p} .$$

The last two properties show that \mathcal{U} is a set system on the ground set W that satisfies the assumptions of Theorem 4.6 with $s = 1$, $\mu_0 = 0$, and $\mu_1 = c$, so we conclude that $|\mathcal{U}| \leq |W|$. We know that $|W| = g(|T|) = g(n)$, which is of polynomial size in n by our assumptions on the form of g .

On the other hand, by construction of \mathcal{U} , we have $|\mathcal{U}| = |\mathcal{S}| \geq \frac{1}{n} \cdot \exp\left(c \frac{\log(n)^2}{\log \log n}\right)$, which is a superpolynomial lower bound on the size of W in n . For n large enough, this lower bound is larger than the polynomial upper bound obtained before. This contradiction shows that no polynomial (or binomial) cardinality transformation function g with properties of the type stated in (4.12) can exist. More precisely, the construction shows that we would need to transform our set system with superpolynomial cardinality transformation functions to have a chance of getting the result.

The above discussion is not limited to modulus 6. In fact, Grolmusz proves a result generalising Theorem 4.7 to any modulus that is not a prime number [5]. The superpolynomial-size set systems guaranteed by this result can be used to obtain insights analogous to the above one, but for general composite moduli.

4.6 Computational experiments

While we could show Theorem 4.2 for prime power moduli, the question remains open for moduli with more than one prime divisor. This motivates checking existence of the set systems in question for general moduli using computers.

We checked computationally if for small moduli and small sizes of the ground set, there is a set system contradicting Theorem 4.2. In other words, we checked whether for given integers n , m and r , there exists a set system \mathcal{S} on the n -element ground set $[n]$ that has the following properties:

- (i) The system \mathcal{S} is closed under intersections.
- (ii) The ground set has cardinality congruent r modulo m , i.e., $n \equiv r \pmod{m}$.
- (iii) Every set in the family has cardinality not congruent to r modulo m .
- (iv) Any $m - 1$ elements are covered by a set in the family.

Testing existence of a system \mathcal{S} with these properties using the approach that we describe below is possible in reasonable time only for small values of n (we tested $n \leq 11$). In all cases that we tested, the software showed infeasibility of the problem.

The computation was set up as an integer program with one binary variable x_S per set $S \subseteq [n]$, indicating whether the set S is an element of \mathcal{S} (corresponding to $x_S = 1$) or not (corresponding to $x_S = 0$). In other words, we have

$$\mathcal{S} = \{S \subseteq [n] \mid x_S = 1\} .$$

The above four constraints are modelled as follows.

- (i) For enforcing that the system \mathcal{S} is closed under intersection, we add the following family of constraints:

$$\forall S_1, S_2 \subseteq [n]: \quad x_{S_1 \cap S_2} \geq x_{S_1} + x_{S_2} - 1.$$

If this constraint is satisfied, then the intersection variable has to be equal to 1 if both S_1 and S_2 are in the family, and it is unconstrained if at least one of the sets is not in the family.

- (ii) The condition that the ground set has cardinality $n \equiv r \pmod{m}$ is guaranteed by the input.
- (iii) For getting the property that every set in \mathcal{S} , i.e., every set S with $x_S = 1$, has cardinality not congruent to r modulo m , we add constraints $x_S = 0$ for all sets S with cardinality congruent to r modulo m .
- (iv) To guarantee the covering property for every $m-1$ elements, we require at least one set containing these elements to be in the family by adding the constraints

$$\forall A \in \binom{[n]}{m-1}: \quad \sum_{S: A \subseteq S \subseteq [n]} x_S \geq 1.$$

Altogether, we check feasibility of the following system, where we choose the parameters such that $n \equiv r \pmod{m}$.

$$\begin{array}{ll} x_S \in \{0, 1\} & \forall S \subseteq [n] , \\ x_S = 0 & \forall S \subseteq [n] \text{ such that } |S| \equiv r \pmod{m} , \\ x_{S_1 \cap S_2} - x_{S_1} - x_{S_2} \geq -1 & \forall S_1, S_2 \subseteq [n] , \\ \sum_{S: A \subseteq S \subseteq [n]} x_S \geq 1 & \forall A \in \binom{[n]}{m-1} . \end{array}$$

To test feasibility of the above system, we use the C++ interface of the Gurobi integer linear program solver [8]. The corresponding code is given in Listing A.1 in Appendix A, a sample output for the test with parameters $m = 6$, $n = 9$, and $r = 3$ is given in Listing A.2.

An overview of the parameters that we tried is given in Table 41. As indicated before, all systems were infeasible. Note that no tests were done for $n \leq m$. For $n < m$, it can be immediately seen that there is no set system with the desired properties: By the covering property, all $n \leq m-1$ elements need to be covered by a set of the system, but this would imply that the ground set is in the family,

but by the congruency constraints, this is impossible. In the case $m = n$, note that $r = 0$. Consequently, the intersection of all sets is non-empty, hence by removing an element common to all sets from the family, we get a new instance with n replaced by $n - 1$ and r replaced by $r - 1$, and it is sufficient to check this instance.

m	n	r	result
6	7	1	infeasible
6	8	2	infeasible
6	9	3	infeasible
6	10	4	infeasible
6	11	5	infeasible
10	11	1	infeasible

Table 41: Results of computational experiments for various inputs.

For modulus $m = 6$, we could check the relevant ground set sizes n up to and including $n = 11$, for $n = 13$, the program ran out of memory. The next modulus m that is not a prime power is $m = 10$, for which the model was infeasible with $n = 11$ and $r = 1$. For larger values of m and n , no results could be obtained in reasonable time.

Generalised congruency constrained submodular minimisation

In this chapter, we prove Theorem 2.4, namely that partial enumeration procedures of a certain order are correct on generalised congruency constrained families with prime power moduli. As for the results obtained for congruency constrained problems in the previous chapter, our proof relies on the methods presented in Chapter 3, so the main focus lies on showing inexistence of set systems with certain properties. Besides this proof, we also consider generalised congruency constrained problems with non-uniform moduli. We show that already a problem with two constraints, one with modulus 2 and the other with modulus 3, can be reduced to a congruency constrained problem with a single constraint with modulus 6.

5.1 Set systems in the generalised setting

We want to prove that for every k and every prime power $m = p^\alpha$, the partial enumeration procedure of order $k(m - 1)$ is correct on generalised congruency constrained families with k constraints and modulus m . By Corollary 3.9, we know that it is sufficient to check the following two points.

- (i) There does not exist a $k(m - 1)$ -covering intersection-closed set system \mathcal{S} on a finite non-empty ground set T with the property that $T \in \mathcal{F}$, but $S \in \mathcal{L} \setminus \mathcal{F}$ for all $S \in \mathcal{S}$.
- (ii) There does not exist a $k(m - 1)$ -covering intersection-closed set system \mathcal{S} on a finite non-empty ground set T with the property that $T \in \text{comp}(\mathcal{F})$, but $S \in \text{comp}(\mathcal{L}) \setminus \text{comp}(\mathcal{F})$ for all $S \in \mathcal{S}$.

We already saw that for simple congruency constrained families, checking one of the two constraints is enough. The following lemma allows for the same conclusion with generalised congruency constrained families.

Lemma 5.1. *Let \mathcal{F} be a generalised congruency constrained subfamily of a lattice family \mathcal{L} on the ground set V . Then, $\text{comp}(\mathcal{F})$ is a generalised congruency constrained subfamily of the lattice $\text{comp}(\mathcal{L})$.*

Proof. Assume that \mathcal{F} is of the form

$$\mathcal{F} = \{S \in \mathcal{L} \mid \forall i \in [k]: |S_i \cap S| \equiv r_i \pmod{m}\}$$

with parameters $m, k \in \mathbb{Z}_{>0}$, $r_1, \dots, r_k \in \mathbb{Z}$ and $S_1, \dots, S_k \subseteq V$. Then, we can write

$$\begin{aligned} \text{comp}(\mathcal{F}) &= \{S \subseteq V \mid V \setminus S \in \mathcal{F}\} \\ &= \{S \subseteq V \mid V \setminus S \in \mathcal{L}, |S_i \cap (V \setminus S)| \equiv r_i \pmod{m}\} . \end{aligned}$$

Now observe that $V \setminus S \in \mathcal{L}$ is equivalent to $S \in \text{comp}(\mathcal{L})$, and

$$|S_i \cap (V \setminus S)| \equiv r_i \pmod{m} \iff |S_i \cap S| \equiv |S_i \cap V| - r_i \pmod{m} .$$

Thus, the family $\text{comp}(\mathcal{F})$ can be written in the form

$$\text{comp}(\mathcal{F}) = \{S \in \text{comp}(\mathcal{L}) \mid \forall i \in [k]: |S_i \cap S| \equiv |S_i \cap V| - r_i \pmod{m}\} ,$$

which is the form of a generalised congruency constrained subfamily of $\text{comp}(\mathcal{L})$, as desired. \square

Now indeed, if we can prove that point (i) holds for every lattice family \mathcal{L} and every generalised congruency constrained subfamily $\mathcal{F} \subseteq \mathcal{L}$ with k constraints and modulus m , then by Lemma 5.1, point (ii) holds for all these families, as well.

Let us again consider \mathcal{F} to be of the form

$$\mathcal{F} = \{S \in \mathcal{L} \mid \forall i \in [k]: |S_i \cap S| \equiv r_i \pmod{m}\} ,$$

where \mathcal{L} is a lattice family on a finite set V , $S_1, \dots, S_k \subseteq V$ are non-empty and $r_1, \dots, r_k \in \mathbb{Z}$ for some $k \in \mathbb{Z}_{>0}$. Then point (i) is to prove inexistence of a $k(m-1)$ -covering intersection-closed set system \mathcal{S} on a finite ground set T with the property that $T \in \mathcal{F}$, or equivalently,

$$T \in \mathcal{L} \wedge (|S_1 \cap T|, \dots, |S_k \cap T|) \equiv (r_1, \dots, r_k) \pmod{m} ,$$

and, for all $S \in \mathcal{S}$, $S \in \mathcal{L} \setminus \mathcal{F}$, which can be written in the form

$$S \in \mathcal{L} \wedge (|S_1 \cap S|, \dots, |S_k \cap S|) \not\equiv (r_1, \dots, r_k) \pmod{m} .$$

Note that to prove inexistence of such a set system, we can prove the stronger result where the conditions $T \in \mathcal{L}$ and $S \in \mathcal{L}$ for all $S \in \mathcal{S}$ are omitted. Moreover, note that the properties of the system do not change if we replace S_i by $S_i \cap T$, so we can as well concentrate on the situation where $S_i \subseteq T$. In this case, $S_i \cap T = S_i$, so the first constraint above can be rewritten in the form $|S_i| \equiv r_i \pmod{m}$ for all $i \in [k]$.

Together, we see that it is sufficient to prove the following theorem, which can be viewed as an analogue of Theorem 4.2 for the generalised congruency constrained setting.

Theorem 5.2. *Let $m \in \mathbb{Z}_{>0}$ be a prime power, let $k \in \mathbb{Z}_{>0}$ and let $r_1, \dots, r_k \in \mathbb{Z}$. There does not exist a $k(m-1)$ -covering intersection-closed set system \mathcal{S} on a non-empty finite set T and sets $S_1, \dots, S_k \subseteq T$ with the property that $|S_i| \equiv r_i \pmod{m}$ for all $i \in [k]$ and, for all $S \in \mathcal{S}$,*

$$(|S_1 \cap S|, \dots, |S_k \cap S|) \not\equiv (r_1, \dots, r_k) \pmod{m} .$$

5.2 A solution for prime power moduli

In this section, we prove Theorem 5.2. Similar to the proofs of Theorem 4.2 that we presented, this proof is a proof by contradiction and relies on exploiting set system transformations as introduced in Chapter 3. As before, the final contradiction is reached by observing that the set system reached after some transformations contradicts Lemma 4.3.

Proof of Theorem 5.2. The proof is by contradiction, so we assume that for some prime power $m = p^\alpha \in \mathbb{Z}_{>0}$ and some integer $k \in \mathbb{Z}_{>0}$, there exists a $k(m-1)$ -covering intersection-closed set system \mathcal{S} on a finite ground set T and sets $S_1, \dots, S_k \subseteq T$ with the property that $|S_i| \equiv r_i \pmod{m}$ for all $i \in [k]$ and, for all $S \in \mathcal{S}$,

$$(|S_1 \cap S|, \dots, |S_k \cap S|) \not\equiv (r_1, \dots, r_k) \pmod{m} .$$

We now transform the system \mathcal{S} in three steps to obtain new set systems with simpler properties. Recall that the goal still is to obtain a contradiction.

Claim 1: *There exists a set system with the same properties as \mathcal{S} , but*

$$r_1 = \dots = r_k = 0 .$$

Proof of Claim 1. We first show how we can modify the set system \mathcal{S} to obtain a set system \mathcal{U} with the same properties as \mathcal{S} , but $r_k = 0$. To this end, let X be a set of $m - r_k$ new elements, and define the new set system \mathcal{U} on the ground set $W = T \cup X$ by

$$\mathcal{U} = \{S \cup X \mid S \in \mathcal{S}\} .$$

Additionally, let $U_i = S_i$ for $i \in [k-1]$ and $U_k = S_k \cup X$. Note that then, we have

$$(|U_1 \cap W|, \dots, |U_k \cap W|) \equiv (r_1, \dots, r_{k-1}, 0) \pmod{p^\alpha} ,$$

and, for all $U \in \mathcal{U}$,

$$(|U_1 \cap U|, \dots, |U_k \cap U|) \not\equiv (r_1, \dots, r_{k-1}, 0) \pmod{p^\alpha} .$$

As furthermore, adding the elements of X to all sets does not change the properties of being $k(m-1)$ -covering and intersection-closed, we see that \mathcal{U} indeed has the same properties as \mathcal{S} with $r_k = 0$. Repeating the above step for all other r_i one after another, we end up with a set system that has the same properties as \mathcal{S} with $r_1 = \dots = r_k = 0$. This proves the first claim. \square

Claim 2: *There exists a k -covering intersection-closed set system \mathcal{S} on a finite ground set T and sets $S_1, \dots, S_k \subseteq T$ with the property that $|S_i| \equiv 1 \pmod{p}$ for all $i \in [k]$ and, for all $S \in \mathcal{S}$,*

$$(|S_1 \cap S|, \dots, |S_k \cap S|) \in \{0, 1\}^k \setminus \{(1, \dots, 1)\} \pmod{p} .$$

Proof of Claim 2. We apply a transformation map to the set system that we obtain from Claim 1. Recall the cardinality transformation function g with covering

coefficient $1/(m-1)$ that we used in the proof of Theorem 4.2 in Section 4.4. This function $g: \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$ was defined by

$$g(x) = \sum_{\substack{k \text{ odd,} \\ 1 \leq k < p^\alpha}} \binom{x}{k} + \sum_{\substack{k \text{ even,} \\ 1 \leq k < p^\alpha}} (p-1) \binom{x}{k}$$

for all $x \in \mathbb{Z}_{\geq 0}$, and we showed that

$$g(x) \equiv \begin{cases} 0 \pmod{p} & \text{if } x \equiv 0 \pmod{p^\alpha}, \\ 1 \pmod{p} & \text{if } x \not\equiv 0 \pmod{p^\alpha}. \end{cases}$$

Note that as a consequence, the function $h(x) = 1 + (p-1)g(x)$ is a cardinality transformation function with covering coefficient $1/(m-1)$, and we have

$$h(x) \equiv 1 - g(x) \equiv \begin{cases} 1 \pmod{p} & \text{if } x \equiv 0 \pmod{p^\alpha}, \\ 0 \pmod{p} & \text{if } x \not\equiv 0 \pmod{p^\alpha}. \end{cases} \quad (5.1)$$

Applying a corresponding set transformation function H for h on T to the set system \mathcal{S} and letting $U_i = H(S_i)$ we see that

$$\mathcal{U} = \{H(S) \mid S \in \mathcal{S}\}$$

is a k -covering intersection-closed set system on the non-empty finite ground set $H(T)$ with the properties that for all $i \in [k]$, we have

$$|U_i| = |H(S_i)| = h(|S_i|) \equiv 1 \pmod{p}$$

because $|S_i| \equiv 0 \pmod{p^\alpha}$. Moreover, every set $U \in \mathcal{U}$ can be written in the form $U = H(S)$ for some $S \in \mathcal{S}$, hence

$$|U_i \cap U| = |H(S_i) \cap H(S)| = |H(S_i \cap S)| = h(|S_i \cap S|).$$

Combining the known

$$(|S_1 \cap S|, \dots, |S_k \cap S|) \not\equiv (0, \dots, 0) \pmod{p^\alpha}$$

with (5.1), we finally obtain

$$(|U_1 \cap U|, \dots, |U_k \cap U|) \in \{0, 1\}^k \setminus \{(1, \dots, 1)\} \pmod{p}$$

for all $U \in \mathcal{U}$. Thus, the system \mathcal{U} that we obtained satisfies all properties postulated by Claim 2. \square

Claim 3: *There exists a 1-covering intersection-closed set System \mathcal{S} on a non-empty finite ground set T such that $|T| \equiv 1 \pmod{p}$, and such that for every $S \in \mathcal{S}$, we have $|S| \equiv 0 \pmod{p}$.*

Proof of Claim 3. For a proof of the third claim, we use the generalised cardinality transformation function g from Lemma 3.18 given by $g(x_1, \dots, x_k) = x_1 \cdot \dots \cdot x_k$ to transform the system given by Claim 2.

More concretely, let \mathcal{S} be this system, namely a k -covering intersection-closed set system on a finite ground set T with sets $S_1, \dots, S_k \subseteq T$ such that $|S_i| \equiv 1 \pmod{m}$ for all $i \in [k]$ and, for all $S \in \mathcal{S}$,

$$(|S_1 \cap S|, \dots, |S_k \cap S|) \in \{0, 1\}^k \setminus \{(1, \dots, 1)\} \pmod{m} .$$

Let G be a set transformation function for g on T with respect to S_1, \dots, S_k , and define $W = G(T)$. We define a new set system \mathcal{U} on W by

$$\mathcal{U} = \{G(S) \mid S \in \mathcal{S}\} .$$

As before, we check that \mathcal{U} has the properties postulated by Claim 3. We have seen that as the image of the intersection-closed set system \mathcal{S} , \mathcal{U} is itself intersection-closed. Moreover, as g has covering coefficient $1/k$ and \mathcal{S} is k -covering, we can choose G such that \mathcal{U} is 1-covering. The ground set W satisfies

$$|W| = |G(T)| = g(|S_1 \cap T|, \dots, |S_k \cap T|) = \prod_{i \in [k]} |S_i \cap T| = \prod_{i \in [k]} |S_i| \equiv 1 \pmod{p} .$$

For all elements $U \in \mathcal{U}$, there is a set $S \in \mathcal{S}$ such that $U = G(S)$, and hence

$$|U| = |G(S)| = g(|S_1 \cap S|, \dots, |S_k \cap S|) = \prod_{i \in [k]} |S_i \cap S| \equiv 0 \pmod{p} ,$$

where the last equivalence follows from the fact that $(|S_1 \cap S|, \dots, |S_k \cap S|) \in \{0, 1\}^k \setminus \{(1, \dots, 1)\} \pmod{p}$, so at least one of the factors will be 0 modulo p . We thus see that the set system \mathcal{U} has all of the desired properties. \square

Last but not least, note that the set system guaranteed by Step 3 above contradicts Lemma 4.3. Thus, we obtained the desired contradiction, which proves Theorem 5.2. \square

5.3 Reducing to disjoint conditions

Recall that congruency constrained subfamilies of a lattice family \mathcal{L} on a finite set V have constraints of the form

$$|S \cap S_i| \equiv r_i \pmod{m} ,$$

where $S_i \subseteq V$ are some fixed subsets of the ground set. In particular, the constraints, i.e., the underlying sets S_i , can overlap. In this section, we show an argument that reduces overlapping problem settings to non-overlapping ones. In other words, we show that every constrained submodular minimisation problem can be solved by solving a similar problem with pairwise disjoint sets S_i .

For simplicity, we only present our construction for the case of two constraints, although all arguments immediately generalise to an arbitrary number of constraints.

Consider a generalised congruency constrained submodular minimisation problem with parameters $(V, \mathcal{L}, f, \{S_1, S_2\}, m, \{r_1, r_2\})$, i.e., we want to minimise f over the family

$$\mathcal{F} = \left\{ S \in \mathcal{L} \mid \begin{array}{l} |S_1 \cap S| \equiv r_1 \pmod{m} \\ \text{and } |S_2 \cap S| \equiv r_2 \pmod{m} \end{array} \right\}.$$

We will extend and modify the given instance to obtain a generalised congruency constrained problem with parameters $(V', \mathcal{L}', f', \{S'_1, S'_2\}, m, \{r_1, r_2\})$ for which we can guarantee that the ground sets S'_1 and S'_2 of the conditions are disjoint, and such that a solution of the initial problem can be deduced from a solution of the second. The idea of the extension is to increase the ground set by introducing copies of certain elements. In particular, copies of elements that appear in multiple constraint sets S_i can be used to assign one copy of every element to each of the involved constraints. Together with a mechanism that ensures that for every solution candidate, either all copies of an element or none are chosen, we arrive at the reduction. But let us introduce the modified problem step by step.

The new ground set is given by

$$V' := V \dot{\cup} S'_1 \dot{\cup} S'_2,$$

where S'_1 and S'_2 are copies of S_1 and S_2 , respectively. To avoid notational ambiguities, we write $x^{(1)} \in S'_1$ for the copy of an element $x \in S_1$, and $x^{(2)} \in S'_2$ for the copy of an element $x \in S_2$.

The idea for a link from subsets of the initial ground set V to subsets of V' is that any set $S \subseteq V$ corresponds to the set $S' \subseteq V'$ given by

$$S' = S \cup \left\{ x^{(1)} \mid x \in S_1 \cap S \right\} \cup \left\{ x^{(2)} \mid x \in S_2 \cap S \right\}. \quad (5.2)$$

By the natural partition of V' into V , S'_1 and S'_2 , every set $S' \subseteq V'$ has three parts: $|V \cap S'|$, $|S'_1 \cap S'|$ and $|S'_2 \cap S'|$. As indicated above, the idea is that we translate the original conditions $|S_1 \cap S| \equiv r_1 \pmod{m}$ and $|S_2 \cap S| \equiv r_2 \pmod{m}$ on subsets S of V to the conditions

$$|S'_1 \cap S'| \equiv r_1 \pmod{m} \quad \text{and} \quad |S'_2 \cap S'| \equiv r_2 \pmod{m}, \quad (5.3)$$

on the parts $|S'_1 \cap S'|$ and $|S'_2 \cap S'|$, where we see that, as desired, the new sets S'_1 and S'_2 are disjoint. While we use the parts $S'_1 \cap S'$ and $S'_2 \cap S'$ for separating the conditions, the remaining part $V \cap S'$ will be used to define the value of a submodular function on S' . This motivates the definition of the new lattice family

$$\mathcal{L}' := \{S' \subseteq V' \mid V \cap S' \in \mathcal{L}\}.$$

Note that with this definition, the function $S' \mapsto f(V \cap S')$ is a well-defined submodular function on \mathcal{L}' . The submodular function f' that we use in our reduction partially consists of the map $S' \mapsto f(V \cap S')$.

Note that a set S' of the form given in (5.2) is a set such that for every $x \in V$, S' either contains x and all available copies of x , or it contains none of these elements. For

such a sets S' , it is easy to see that $V \cap S'$ satisfies the initial conditions if and only if S' satisfies the new conditions (5.3). The goal is to define the new submodular function f' in such a way that a minimiser of f' over the new family always has the property of containing either all copies of an element or none. In other words, we want to have a penalty in the function value $f'(S')$ if two copies of an element are separated by S' . One way to achieve this is by adding a cut function.

To this end, let $G = (V', E)$ be the graph on vertices V' obtained by adding the edges $\{x, x^{(1)}\}$, $\{x, x^{(2)}\}$, and $\{x^{(1)}, x^{(2)}\}$ for all $x \in V$, whenever both endpoints are in V' . For a large constant $M \in \mathbb{Z}$, we then define the function $f': \mathcal{L}' \rightarrow \mathbb{Z}$ by

$$f'(S') := f(V \cap S') + M \cdot |\delta_G(S')| .$$

The function f' is a linear combination of the submodular function $S' \mapsto f(V \cap S')$ and the cut function $S' \mapsto |\delta_G(S')|$ (which is submodular), hence f' is itself submodular. By choosing M larger than any value of f can be, we see that no set S' that cuts an edge in G can be a minimiser of f' . Figure 51 illustrates the construction that we did so far.

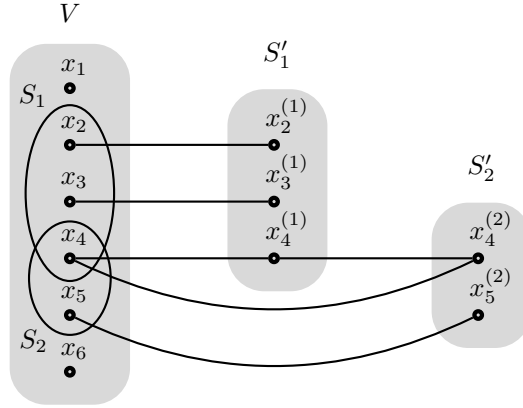


Figure 51: Construction of V' by duplicating elements, and the graph $G = (V', E)$.

We now formalise the intuition behind the above definitions in the following claim, which uses the notation introduced above.

Claim 5.3. *For a minimiser S' of f' over the family*

$$\mathcal{F}' = \left\{ S \in \mathcal{L}' \mid \begin{array}{l} |S'_1 \cap S| \equiv r_1 \pmod{m} \\ |S'_2 \cap S| \equiv r_2 \pmod{m} \end{array} \right\} ,$$

the set $V \cap S'$ is a minimiser of f over \mathcal{F} .

Proof. We first note that for every minimiser S of f over \mathcal{F} , the corresponding set $S' \subseteq V'$ that contains all copies of elements in S is feasible for \mathcal{F}' . Indeed, $S \in \mathcal{L}$ implies $S' \in \mathcal{L}'$, and as $|S'_1 \cap S| = |S'_1 \cap S'|$ and $|S'_2 \cap S| = |S'_2 \cap S'|$ implies validity of the new congruency constraints from validity of the old ones, we obtain feasibility. Moreover, as S' does, by definition, not cut any edges in the graph G , we

get $f'(S') = f(V \cap S') = f(S)$. As S is a minimiser of f over \mathcal{F} , this implies

$$\min_{S \in \mathcal{F}} f(S) \geq \min_{S' \in \mathcal{F}'} f'(S') . \quad (5.4)$$

For the other direction, let S' be a minimiser of f' over \mathcal{F}' . Note that if S' crosses an edge of G , then $f'(S') > M$, which is larger than any value of f on \mathcal{F} . But then, by the values of f' that we saw in the previous paragraph, we conclude that such a set S' cannot be a minimiser of f' . Thus, S' does not cross edges of G . In particular, we have $|S'_1 \cap S'| = |S_1 \cap S'|$, and hence

$$|S_1 \cap (V \cap S')| = |S_1 \cap S'| = |S'_1 \cap S'| \equiv r_1 \pmod{m} ,$$

so the set $V \cap S'$ satisfies the first congruency constraint of \mathcal{F} . The same argument shows that it also satisfies the second. As $S' \in \mathcal{L}'$, we also conclude that $V \cap S' \in \mathcal{L}$. Consequently, $V \cap S'$ is feasible for \mathcal{F} and $f(V \cap S') = f'(S')$. As this time, S' is defined as a minimiser of f' over \mathcal{F}' , we obtain

$$\min_{S \in \mathcal{F}} f(S) \leq \min_{S' \in \mathcal{F}'} f'(S') . \quad (5.5)$$

Combining (5.5) and (5.4), we see that the objective values of the two problems coincide, and a minimiser of one problem can be obtained from a minimiser of the other by adding or deleting all available copies of the elements contained in the minimiser, depending direction of the transformation. This proves the claim. \square

Remark 5.4. In the above arguments, we changed the submodular function so that separating two elements that are a copy of each other results in a penalty in terms of the function value. A different approach is to define the set family \mathcal{L}' in such a way that $S' \in \mathcal{L}'$ if and only if $V \cap S' \in \mathcal{L}$, and S' contains all available copies of the elements in $V \cap S'$. In other words, with this definition, the sets in \mathcal{L}' are precisely those that do not separate any copies and whose intersection with V lies in \mathcal{L} . The new submodular function f' can then be defined by mapping $S' \mapsto f(V \cap S')$. Also note that in the approach described here, the new lattice family is smaller. Than in our approach. If, for example, $\mathcal{L} = 2^V$, then the first approach leads to $\mathcal{L}' = 2^{V'}$, while the second results in a strict subset $\mathcal{L}' \subsetneq 2^{V'}$.

The proof given above shows that if we are given a GCSM problem with 2 constraints, then we can obtain a minimiser by solving a modified GCSM problem with 2 constraints on disjoint subsets of the ground set, where the size of the ground set in the new problem is bounded by 3 times the size of the initial ground set.

The above construction could be done in a more efficient way by duplicating only those elements that actually appear in more than one constraint set. Moreover, also note that a generalisation of the above to GCSM problems with k constraints is immediate, and a generalisation of the construction presented above requires a blow up of the ground set by a factor of $(k+1)$. Note that a blow up of this order can be necessary to separate the constraints if, for example, $S_i = V$ for all $i \in [k]$.

5.4 A variation: Varying moduli

Recall that congruency constrained subfamilies of a lattice family \mathcal{L} on a finite ground set V were defined as families of the form

$$\mathcal{F} = \{S \in \mathcal{L} \mid \forall i \in [k]: |S_i \cap S| \equiv r_i \pmod{m}\} ,$$

where $k \in \mathbb{Z}_{>0}$, $m \in \mathbb{Z}_{>0}$, $S_1, \dots, S_k \subseteq V$, and $r_1, \dots, r_k \in \mathbb{Z}$. In particular, we always used the same modulus m for all k constraints.

In this section, we want to study an aspect of the more general families of the form

$$\mathcal{F} = \{S \in \mathcal{L} \mid \forall i \in [k]: |S_i \cap S| \equiv r_i \pmod{m_i}\}$$

with different moduli $m_1, \dots, m_k \in \mathbb{Z}_{>0}$. For simplicity, we focus on a setting where $\mathcal{L} = 2^V$ and where the family has two constraints, one of which has modulus 2 and the other has modulus 3. In other words, we consider a family of the form

$$\mathcal{F} = \left\{ S \in \mathcal{L} \mid \begin{array}{l} |S_1 \cap S| \equiv r_1 \pmod{2} , \\ \text{and } |S_2 \cap S| \equiv r_2 \pmod{3} \end{array} \right\} . \quad (5.6)$$

Our main result is that a problem of this type can be reduced to a GCSM problem with modulus 6 and only one constraint. Note that the inverse direction of this statement is trivial: Given the problem of minimising a submodular function over a family of the form

$$\mathcal{F} = \{S \in \mathcal{L} \mid |S_0 \cap S| \equiv r \pmod{6}\}$$

on some ground set V , we can trivially rewrite the problem as minimising \mathcal{F} over

$$\mathcal{F} = \left\{ S \in \mathcal{L} \mid \begin{array}{l} |S_0 \cap S| \equiv r \pmod{2} \\ \text{and } |S_0 \cap S| \equiv r \pmod{3} \end{array} \right\} .$$

The other direction, however, is more interesting and requires a small construction.

Assume that we have a family \mathcal{F} as given in (5.6). First of all, by the result from the previous section, we can assume $S_1 \cap S_2 = \emptyset$. The main idea of the reduction is then to again duplicate certain elements of the ground set. To be precise, we will add two extra copies of every element in S_1 and one extra copy of every element in S_2 to the ground set V . As before, we will also modify the submodular function by adding a cut function to make sure that minimisers of the new function always contain an element together with all of its copies, or none of these elements. It turns out that then, as every element from S_1 that is contained in a minimiser comes with its two copies (hence in a group of three), while every element from S_2 that is contained in a minimiser comes together with one copy (hence in a group of two), there is a single constraint modulo 6 that can model the initial two constraints modulo 2 and modulo 3. But let us again formally introduce the new system before proving this result.

To make the setting clear, we repeat that we are given a finite ground set V , a lattice \mathcal{L} on V and a submodular function $f: \mathcal{L} \rightarrow \mathbb{Z}_{\geq 0}$. Moreover, we are given two disjoint

sets $S_1, S_2 \subseteq V$, $r_1, r_2 \in \mathbb{Z}$ and $m \in \mathbb{Z}_{>0}$. The problem is to minimise f over

$$\mathcal{F} = \left\{ S \in \mathcal{L} \mid \begin{array}{l} |S_1 \cap S| \equiv r_1 \pmod{2}, \\ \text{and } |S_2 \cap S| \equiv r_2 \pmod{3} \end{array} \right\}.$$

Let $S'_1 = \{x^{(1)} \mid x \in S_1\}$, $S''_1 = \{x^{(2)} \mid x \in S_1\}$ and $S'_2 = \{x^{(1)} \mid x \in S_2\}$ denote copies of the initial elements in S_1 and S_2 . Define a new ground set

$$V' := V \dot{\cup} S'_1 \dot{\cup} S''_1 \dot{\cup} S'_2.$$

Let the lattice family \mathcal{L}' be defined by

$$\mathcal{L}' := \{S' \subseteq V' \mid V \cap S' \in \mathcal{L}\}.$$

For defining a submodular function f' on \mathcal{L}' , we will use the submodular function $S' \mapsto f(V \cap S')$ on \mathcal{L}' and add a cut function. To do so, let $G = (V', E)$ be the graph obtained by adding the edges $\{x, x^{(1)}\}$, $\{x, x^{(2)}\}$ and $\{x^{(1)}, x^{(2)}\}$ for all $x \in S_1$, and the edges $\{x, x^{(1)}\}$ for all $x \in S_2$. For a large constant $M \in \mathbb{Z}$, we then define the function $f': \mathcal{L}' \rightarrow \mathbb{Z}$ by

$$f'(S') := f(V \cap S') + M \cdot |\delta_G(S')|.$$

As before, by choosing M larger than any value of f can be, we will see that no set S' minimising f' will cut an edge of G . The new setting is illustrated in Figure 52 for an example with $V = \{x_1, x_2, x_3, x_4, x_5, x_6\}$, $S_1 = \{x_1, x_2, x_3\}$, and $S_2 = \{x_4, x_5\}$.

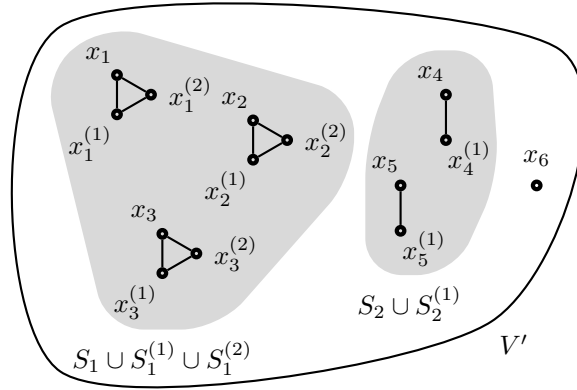


Figure 52: Construction of V' by duplicating elements, and the graph $G = (V', E)$.

The following claim specifies the reduction, building on the notation introduced above.

Claim 5.5. *Let $S_0 = S_1 \cup S'_1 \cup S''_1 \cup S_2 \cup S'_2$, and let S' be a minimiser of f' over the family*

$$\mathcal{F}' := \{S \in \mathcal{L}' \mid |S_0 \cap S| \equiv 3r_1 + 2r_2 \pmod{6}\}.$$

Then, the set $V \cap S'$ is a minimiser of f over the family \mathcal{F} .

Proof. We start by observing that for any set S minimising f over \mathcal{F} , the set $S' \subseteq V'$ that contains all copies of elements in S is feasible for \mathcal{F}' . Indeed, note that as S' contains all copies of elements in S , we have

$$\begin{aligned} |S_0 \cap S'| &= |S_1 \cap S'| + |S'_1 \cap S'| + |S''_1 \cap S'| + |S_2 \cap S'| + |S'_2 \cap S'| \\ &= 3 \cdot |S_1 \cap S| + 2 \cdot |S_2 \cap S| \equiv 3r_1 + 2r_2 \pmod{6}, \end{aligned} \quad (5.7)$$

where the last equivalence follows from $|S_1 \cap S| \equiv r_1 \pmod{2}$ and $|S_2 \cap S| \equiv r_2 \pmod{3}$, which holds by feasibility of S for \mathcal{F} . Moreover, by definition of f' , we have $f(S') = f(S' \cap V) = f(S)$. As S is a minimiser of f , this implies

$$\min_{S \in \mathcal{F}} f(S) \geq \min_{S' \in \mathcal{F}'} f'(S'). \quad (5.8)$$

For the other direction, let S' be a minimiser of f' over \mathcal{F}' . Again, if S' crosses an edge of G , then $f(S') \geq M$. But we saw in the first part of this proof that f' also attains values equal to values of f , which are smaller than M , so if S' is a minimiser of f' , then S' does not cross any edge of G . We thus conclude that if S' contains an element of V' , then it also contains all copies of that element.

In particular, we have $|S_1 \cap S'| = |S'_1 \cap S'| = |S''_1 \cap S'|$ and $|S_2 \cap S'| = |S'_2 \cap S'|$. Using (5.7) and denoting $|S_1 \cap S'| = a$ and $|S_2 \cap S'| = b$, we get

$$|S_0 \cap S'| = 3 \cdot |S_1 \cap S'| + 2 \cdot |S_2 \cap S'| = 3a + 2b,$$

and together with feasibility of S' for \mathcal{F}' , which gives $|S_0 \cap S'| \equiv 3r_1 + 2r_2 \pmod{6}$, we conclude

$$3a + 2b \equiv 3r_1 + 2r_2 \pmod{6}.$$

By reducing the last congruence to modulo 2 and modulo 3, we obtain $a \equiv r_1 \pmod{2}$ and $b \equiv r_2 \pmod{3}$, respectively. Plugging in $a = |S_1 \cap S'| = |S_1 \cap (V \cap S')|$ and $b = |S_2 \cap S'| = |S_2 \cap (V \cap S')|$, this reads as

$$|S_1 \cap (V \cap S')| \equiv r_1 \pmod{2} \quad \text{and} \quad |S_2 \cap (V \cap S')| \equiv r_2 \pmod{3}.$$

As additionally, $S' \in \mathcal{L}'$ implies $V \cap S' \in \mathcal{L}$, we have feasibility of $V \cap S'$ for \mathcal{F} . By observing $f'(S') = f(V \cap S')$, we obtain

$$\min_{S \in \mathcal{F}} f(S) \leq \min_{S' \in \mathcal{F}'} f'(S'). \quad (5.9)$$

Altogether, (5.8) and (5.9) imply that the minimum values of f and f' over \mathcal{F} and \mathcal{F}' , respectively, are equal, and an optimal set for one problem can be obtained from an optimal set of the other problem by adding or removing all of the elements in question. This proves our claim. \square

Remark 5.6. Analogously to what we remarked for the reduction to disjoint conditions in the precious section, we also remark here that for the above reduction, changing the submodular function by a cut function can be avoided by changing the underlying lattice family. More precisely, the argument yields the same conclusion if we let \mathcal{L}' be the family of all subsets $S' \subseteq V'$ with the property that for every element in S' , all available copies of that element are also contained in S' , and if we define f' by $f'(S') = f(V \cap S')$ for all $S' \subseteq V'$.

The reduction above can be generalised to settings with two arbitrary coprime moduli m_1 and m_2 instead of 2 and 3. Then, the blow up of the sets S_1 and S_2 has to be done with a factor of m_2 and m_1 , respectively. With pairwise coprime moduli, a generalisation to a larger number of constraints is possible, as well. As before, the modulus of the resulting constraint is equal to the product of the original moduli.

Chapter 6

Conclusion

The main contribution of this thesis is providing efficient algorithms for solving congruency constrained submodular minimisation problems (CSM problems) and a generalised version thereof (GCSM problems), where congruency constraints with prime power moduli are considered.

While the algorithms themselves were inspired by and generalised from prior work by Goemans and Ramakrishnan for minimising submodular functions over parity families, an adaption of the proofs to our settings required introducing new techniques, in particular for dealing with set systems with particular covering properties.

Our work leaves some open questions that require further research. First and foremost, an extension or a hardness result for CSM and GCSM problems with moduli m that are not prime powers would be interesting. We could only show arguments why our current methods cannot directly generalise beyond prime power moduli.

Even the special case of GCSM problems with a single constraint modulo a composite number that is not a prime power is an interesting open case. We could show that GCSM problems with different and pairwise coprime moduli for each congruency constraint reduce to that class of problems.

Another interesting aspect comes from a considerably more general perspective that initiated our interest to problems of this kind: The question whether or not a submodular function can be minimised efficiently over general intersections of parity families or triple families. The result of Goemans and Ramakrishnan as well as our two results fit in a framework that suggest the following open problem.

Open Problem. *For a finite set V , let \mathcal{L} be a lattice family on V and let f be a submodular function on \mathcal{L} . Let $\mathcal{P}_1, \dots, \mathcal{P}_\ell$ be parity subfamilies of \mathcal{L} . Can a set minimising f over the family*

$$\mathcal{F} = \mathcal{P}_1 \cap \dots \cap \mathcal{P}_\ell$$

be obtained through a partial enumeration procedure of order ℓ ?

We show that for all $\ell \in \mathbb{Z}_{>0}$, there exist examples of parity families such that a partial enumeration procedure needs order at least ℓ to solve above problem, and our results for CSM and GCSM problems achieve this lower bound.

Appendix A

C++ code for computational experiments

In this appendix, we present the C++ code for checking existence of certain set systems as described in Section 4.6. Listing A.1 contains the program code, while the output generated for the parameters $m = 6$, $n = 9$, and $r = 3$ is given as a sample output in Listing A.2.

Listing A.1: Code for checking whether a modular set family exists for input parameters.

```
5  /*
   * Congruency constrained set system
   * Checking whether set systems with the following properties exist:
   * - Grund set [n] with  $n \equiv r \pmod m$ .
   * - For any two sets, their intersection is in the set system, as well.
   * - All sets  $S$  in the set system satisfy  $|S| \not\equiv r \pmod m$ .
   * - For any  $m-1$  elements of the ground set, there exists a set containing  $\leftrightarrow$ 
   *   them all.
   */
10 #include <iostream>
   #include <vector>
   #include <cmath>
   #include "gurobi_c++.h"
15 using namespace std;

   bool is_residue ( const int& x, const int& r, const int& m ) {
       // check if the residue of x equals r mod m
       return x % m == r;
20 }

   int intersect ( const int& set1, const int& set2 ) {
       // intersection of two sets given in binary encoding as an integer
       return set1 & set2;
25 }

   int cardinality ( const int& set ) {
       // calculate the cardinality of a set given in binary encoding as an  $\leftrightarrow$ 
       integer
       if ( set == 0 )
30         return 0;
       return set%2 + cardinality( set/2 );
   }
```

A. C++ CODE FOR COMPUTATIONAL EXPERIMENTS

```

35 bool is_contained ( const int& x, const int& set ) {
    // check if element x is contained in a set given in binary encoding as ↔
    // an integer
    return set & 1<<x;
}

40 bool increase_e ( vector<int>& e, const int& l, const int& n ) {
    // simulates counting up l-digit numbers with strictly increasing digits↔
    // from {0,...,N-1}
    // PRE: e is of length l,
    //       e is either satisfies e[0] == -1 or contains strictly increasing↔
    //       digits from {0,...,N-1}
    // POST: true if
    //        - e[0] == -1, in this case e is set to [0,1,...,l-1]
    //        - e[0] != -1 and e can be increased, in which case e gets ↔
    //        increased
    //        false if e cannot be increased

    // check whether e is [-1,...] and if yes, increment to [0,1,...,l-1]
50 if ( e[0] == -1 ) {
    for ( int i = 0; i < l; ++i )
        e[i] = i;
    return true;
}

55 // find (form right to left) the first position that can be increased
int pos = l-1; // current position
int bound = n-1; // upper bound for current position
while ( e[pos] == bound ) {
60     // check if we are at leftmost position
    if ( pos == 0 )
        return false;
    // if not, move left and update bound
    --pos;
    --bound;
65 }
// increase digit at position found
++e[pos];
// set all digits to the right
70 while ( ++pos < l ) {
    e[pos] = e[pos-1]+1;
}
return true;
}

75 void test_instance( const int& n, const int& m, const int& r ) {

    cout << "Generating model." << endl;

80 // Obtain Gurobi environmnt and create model
GRBEnv env = GRBEnv();
GRBModel model = GRBModel(env);

// Create a variable for each set, indexed by binary representation of ↔
// the set
85 vector<GRBVar> X( pow(2,n)+1 );
for ( int set = 0; set < pow(2,n); ++set ) {
    string name = "x_" + to_string(set);
    if ( is_residue( cardinality ( set ), r, m ) ) {
        // set bounds such that the variable is zero
90     X[set] = model.addVar(0, 0, 0, GRB_BINARY, name);
    }
    else
        // set X[set] to a binary variable

```

```

95         X[set] = model.addVar(0, 1, 0, GRB_BINARY, name);
    }

    cout << "- Variables created." << endl;

    // Add intersection constraints I_s1_s2
    // --> For any sets s1 and s2 in the family, their intersection has to be
    // inside, as well
    // --> Modelled by the constraint  $X[s1 \cap s2] \geq X[s1] + X[s2] - 1$ 
100 for ( int set1 = 0; set1 < pow(2,n); ++set1 ) {
    for ( int set2 = set1+1; set2 < pow(2,n); ++set2 ) {
        // define constraint name
105 string name = "I_" + to_string(set1) + "_" + to_string(set2);
        // define constraint and add to model
        GRBLinExpr expr = X[intersect( set1, set2 )] - X[set1] - X[set2];
        model.addConstr( expr, GRB_GREATER_EQUAL, -1, name );
    }
110 }

    cout << "- Intersection constraints added." << endl;

    // Add covering constraints C_e1..._em-1
    // --> For all  $e_1, \dots, e_{m-1} \in \mathcal{N}$ , there is a set in the family containing
    // them all
    // --> Modelled by the constraint  $\sum_{s: \{e_1, \dots, e_{m-1}\} \subset s} X[s] \geq 1$ 
115 vector<int> e(m-1,-1);
    while ( increase_e( e, m-1, n ) ) {
        // define constraint name
120 string name = "C";
        for ( vector<int>::iterator it = e.begin(); it != e.end(); ++it ) {
            name += "_" + to_string(*it);
        }
        // define constraint
125 GRBLinExpr expr = 0;
        for ( int set = 0; set <= pow(2,n); ++set ) {
            bool contains_all = true;
            for ( vector<int>::iterator it = e.begin(); it != e.end(); ++it ) {
                contains_all &= is_contained( *it, set );
130 }
            if ( contains_all )
                expr += X[set];
        }
        // add constraint to model
135 model.addConstr( expr, GRB_GREATER_EQUAL, 1, name );
    }

    cout << "- Covering constraints added." << endl << endl;

140 // Optimise the model
    model.optimize();

    // Write model to file
145 model.write("modularSetSystem.lp");

    // Check the status
    int status = model.get(GRB_IntAttr_Status);

    // Print solution if feasible (status 2)
150 if ( status == 2 ) {
        cout << endl << "The system is feasible, one possible solution is as follows: " << endl;
        for ( int set = 0; set < pow(2,n); ++set ) {
            cout << " " << X[set].get(GRB_StringAttr_VarName) << " = "

```

A. C++ CODE FOR COMPUTATIONAL EXPERIMENTS

```

155         }
156     }
157 }
158
159 int main () {
160     // read in m, n and r
161
162     int m, n, r;
163     cout << "+-----+" << endl
164          << "|   Congruency constrained set systems   |" << endl
165          << "+-----+" << endl
166          << "Modulus: ";
167     cin >> m;
168     cout << m << endl
169          << "Ground set cardinality: ";
170     cin >> n;
171     cout << n << endl;
172     cout << "Residue class: ";
173     cin >> r;
174     cout << r << endl;
175     cout << endl;
176
177     test_instance( n, m, r);
178
179     return 0;
180 }

```

Listing A.2: Output for $m = 6$, $n = 9$ and $r = 3$.

```

+-----+
|   Congruency constrained set systems   |
+-----+
Modulus: 6
5 Ground set cardinality: 9
Residue class: 3

Generating model.
- Variables created.
10 - Intersection constraints added.
- Covering constraints added.

Optimize a model with 130942 rows, 512 columns and 356122 nonzeros
Variable types: 0 continuous, 512 integer (512 binary)
15 Coefficient statistics:
  Matrix range      [1e+00, 1e+00]
  Objective range   [0e+00, 0e+00]
  Bounds range      [1e+00, 1e+00]
  RHS range         [1e+00, 1e+00]
20 Presolve removed 110682 rows and 131 columns
Presolve time: 1.97s
Presolved: 20260 rows, 381 columns, 77736 nonzeros
Variable types: 0 continuous, 381 integer (381 binary)
25 Presolved: 381 rows, 20641 columns, 78117 nonzeros

Root relaxation: objective 0.000000e+00, 7 iterations, 0.02 seconds

30
  Nodes      |      Current Node      |      Objective Bounds      |      Work
  Expl Unexpl |  Obj  Depth IntInf | Incumbent    BestBd   Gap | It/Node Time
      0       0 | 0.00000   0   7   |         -    0.00000   -   -   -   2s
      0       0 | 0.00000   0  12   |         -    0.00000   -   -   -   2s
      0       0 | 0.00000   0   8   |         -    0.00000   -   -   -   2s
35      0       0 | 0.00000   0  13   |         -    0.00000   -   -   -   2s

```

	0	0	0.00000	0	10	-	0.00000	-	-	2s
	0	0	0.00000	0	7	-	0.00000	-	-	2s
	0	0	0.00000	0	8	-	0.00000	-	-	2s
40	0	0	0.00000	0	9	-	0.00000	-	-	2s
	0	0	0.00000	0	11	-	0.00000	-	-	2s
	0	0	0.00000	0	11	-	0.00000	-	-	2s
	0	0	0.00000	0	11	-	0.00000	-	-	3s
	0	0	0.00000	0	11	-	0.00000	-	-	3s
	0	2	0.00000	0	11	-	0.00000	-	-	4s
45	9	7	infeasible	5		-	0.00000	-	92.9	5s
	138	29	0.00000	3	11	-	0.00000	-	102	10s
	283	45	infeasible	11		-	0.00000	-	104	15s
	371	48	infeasible	21		-	0.00000	-	112	21s
	442	53	infeasible	11		-	0.00000	-	109	25s
50	585	50	infeasible	11		-	0.00000	-	112	30s
	694	56	infeasible	21		-	0.00000	-	113	35s
	820	54	0.00000	14	43	-	0.00000	-	113	41s
	984	50	0.00000	12	102	-	0.00000	-	111	47s
	1058	48	infeasible	22		-	0.00000	-	111	50s
55	1235	47	infeasible	27		-	0.00000	-	109	57s
	1295	47	0.00000	32	33	-	0.00000	-	111	60s
	1464	39	0.00000	9	60	-	0.00000	-	111	68s
	1524	32	infeasible	11		-	0.00000	-	112	72s
	1668	32	0.00000	12	31	-	0.00000	-	109	76s
60	1755	29	0.00000	14	61	-	0.00000	-	109	80s
	1901	0	0.00000	32	81	-	0.00000	-	110	86s
Cutting planes:										
	MIR: 4									
65	Inf proof: 1									
	Zero half: 38									
Explored 1959 nodes (217025 simplex iterations) in 86.44 seconds										
Thread count was 4 (of 4 available processors)										
70	Solution count 0									
	Pool objective bound 1e+100									
Model is infeasible										
75	Best objective -, best bound -, gap -									

Bibliography

- [1] G. Birkhoff. On the combination of subalgebras. *Proceedings of the Cambridge Philosophical Society*, 29(4):441–464, 1933.
- [2] L. Fleischer and S. Iwata. A push-relabel framework for submodular function minimization and applications to parametric optimization. *Discrete Applied Mathematics*, 131(2):311–322, 2003.
- [3] P. Frankl and R. M. Wilson. Intersection theorems with geometric consequences. *Combinatorica*, 1(4):357–368, 1981.
- [4] M. X. Goemans and V. S. Ramakrishnan. Minimizing submodular functions over families of sets. *Combinatorica*, 4(15):499–513, 1995.
- [5] V. Grolmusz. Superpolynomial Size Set-systems with Restricted Intersections mod 6 and Explicit Ramsey Graphs. *Combinatorica*, 20(1):71–86, 2000.
- [6] M. Grötschel, L. Lovász, and A. Schrijver. The ellipsoid method and its consequences in combinatorial optimization. *Combinatorica*, 1(2):169–197, 1981.
- [7] M. Grötschel, L. Lovász, and A. Schrijver. *Geometric algorithms and combinatorial optimization*, volume 2 of *Algorithms and combinatorics*. Springer, 2nd edition, 1993.
- [8] Gurobi Optimization, Inc. Gurobi Optimizer Reference Manual. <http://www.gurobi.com>, 2016.
- [9] S. Iwata. A Faster Scaling Algorithm for Minimizing Submodular Functions. *SIAM Journal on Computing*, 32(4):833–840, 2003.
- [10] S. Iwata, L. Fleischer, and S. Fujishige. A combinatorial strongly polynomial algorithm for minimizing submodular functions. *Journal of the ACM*, 48(4):761–777, 2001.
- [11] Y. T. Lee, A. Sidford, and S. C. Wai Wong. A Faster Cutting Plane Method and its Implications for Combinatorial and Convex Optimization. In *Proceedings of*

the 2015 IEEE 56th Annual Symposium on Foundations of Computer Science (FOCS '15), pages 1049–1065. IEEE Computer Society, 2015.

- [12] Edouard Lucas. Théorie des fonctions numériques simplement périodiques. *American Journal of Mathematics*, 1(3):197–240, 1878.
- [13] J. B. Orlin. A faster strongly polynomial time algorithm for submodular function minimization. *Mathematical Programming*, 118(2):237–251, 2009.
- [14] A. Schrijver. A Combinatorial Algorithm Minimizing Submodular Functions in Strongly Polynomial Time. *Journal of Combinatorial Theory Series B*, 80(2):346–355, 2000.
- [15] A. Schrijver. *Combinatorial Optimization – Polyhedra and Efficiency*, volume B. Springer, 2003.
- [16] Z. Svitkina and L. Fleischer. Submodular Approximation: Sampling-based Algorithms and Lower Bounds. *SIAM Journal on Computing*, 40(6):1715–1737, 2011.
- [17] Z. Svitkina and É. Tardos. Facility location with hierarchical facility costs. *ACM Transactions on Algorithms*, 6(2):37:1–37:22, 2010.



Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Declaration of originality

The signed declaration of originality is a component of every semester paper, Bachelor's thesis, Master's thesis and any other degree paper undertaken during the course of studies, including the respective electronic versions.

Lecturers may also require a declaration of originality for other written papers compiled for their courses.

I hereby confirm that I am the sole author of the written work here enclosed and that I have compiled it in my own words. Parts excepted are corrections of form and content by the supervisor.

Title of work (in block letters):

CONSTRAINED SUBMODULAR MINIMISATION
From Parity Families to Congruency Constraints

Authored by (in block letters):

For papers written by groups the names of all authors are required.

Name(s):

Nägele

First name(s):

Martin

With my signature I confirm that

- I have committed none of the forms of plagiarism described in the 'Citation etiquette' information sheet.
- I have documented all methods, data and processes truthfully.
- I have not manipulated any data.
- I have mentioned all persons who were significant facilitators of the work.

I am aware that the work may be screened electronically for plagiarism.

Place, date

Zürich, 10.03.2017

Signature(s)

For papers written by groups the names of all authors are required. Their signatures collectively guarantee the entire content of the written paper.