Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

An Optimal Monotone Contention Resolution Scheme for Uniform and Partition Matroids

Danish Kashaev

Master Thesis

Supervised by: Dr. Richard Santiago Torres, Prof. Rico Zenklusen
Department of Mathematics, ETH Zurich

March 28, 2021

Abstract

Submodular function maximization became a very interesting and well-studied area in recent years due to a vast number of applications. A relaxation and rounding framework is now a standard and effective way to tackle the constrained submodular maximization problem subject to independence constraints. In particular, a general and successful tool for the rounding part are *contention resolution schemes* (or *CR schemes*). These take a fractional point in a relaxation polytope, round each coordinate of that point independently to get a possibly non-feasible set, and then drop some elements randomly in order to satisfy the independence constraints. A CR scheme is *c-balanced* if each element included in the randomly rounded set is kept with probability at least c. Another important property for a CR scheme to have is *monotonicity*.

A $1-(1-1/n)^n$-balanced CR scheme is already known for the uniform matroid of rank one, and it is also known that this is optimal. Moreover, a $(1-1/e)$-balanced CR scheme has been provided for a general matroid and is asymptotically optimal, in the sense that one cannot hope to get a better balancedness factor by designing a CR scheme for any general matroid.

The main goal of this thesis is to find classes of matroids where the above $1-1/e$ balancedness factor can be improved. We provide simple monotone CR schemes with an improved balancedness factor for three classes of matroids: uniform matroids (of any rank), partition matroids, and matroids with pairwise disjoint circuits. In addition, we prove that the balancedness that we get for each of them is *optimal*, i.e. one cannot hope to design higher-balanced CR schemes for these three cases. In particular, for uniform matroids, the factor we provide generalizes the previously known result of $1-(1-1/n)^n$ for the rank one case to $1-\binom{n}{k}\left(1-\frac{k}{n}\right)^{n+1-k}\left(\frac{k}{n}\right)^k$ for the rank k case. For a fixed value of k, this expression converges to $1-e^{-k}\frac{k^k}{k!}$ as n tends to infinity, which also generalizes the asymptotical $1-1/e$ for the rank one case.

Acknowledgments

Firstly, I would like to thank Prof. Rico Zenklusen and the IFOR group for the opportunity of writing my Master thesis there. I would also like to thank my supervisor Dr. Richard Santiago Torres for his help during this project and some helpful discussions.

Contents

1 Introduction

1.1 Constrained submodular maximization

Submodular functions have received a lot of attention in recent years in very diverse fields. This is due to the fact that they capture a natural property of set functions: *diminishing marginal returns*. Applications of submodular functions are very vast: algorithmic game theory, machine learning and combinatorial optimization are three of the main fields where they are used, see for example [15], [16], [19]. The formal definition is the following.

Definition 1.1. Given a ground set $N = \{1, \ldots, n\}$, a set function $f : 2^N \mapsto \mathbb{R}$ is *submodular* if:

$$f(A \cup \{i\}) - f(A) \geq f(B \cup \{i\}) - f(B) \qquad \forall A \subset B \subset N,\ i \notin B.$$

In words, we take two subsets $A, B \subset N$, where one is contained in the other ($A \subset B$), as well as an element $i \in N$ which does not lie in either of A and B. The submodularity property states that the marginal gain obtained by adding i to A is always bigger than the marginal gain obtained by adding i to B.

Remark. The submodularity property can equivalently be restated as

$$f(A) + f(B) \geq f(A \cup B) + f(A \cap B) \qquad \forall A, B \subset N.$$

Even though this statement might seem simpler, it is harder to understand intuitively.

Let us now describe the framework for the *constrained submodular maximization problem*. We are given:

- A finite set $N = \{1, ..., n\}$, called a *ground set*.
- A family $\mathcal{I} \subset 2^N$ of *feasible sets* (or *independent sets*).
- A non-negative submodular set function $f : 2^N \mapsto \mathbb{R}_{\geq 0}$. We can equivalently see this mapping as $f : \{0,1\}^N \mapsto \mathbb{R}_{\geq 0}$ by associating to every set $A \subset N$ its characteristic vector $\mathbf{1}_A \in \{0,1\}^N$.

The *constrained submodular maximization problem* is then

$$\max_{S \in \mathcal{I}} f(S). \tag{1.1}$$

In words, we want to maximize a non-negative submodular function subject to *independence constraints* captured by $\mathcal{I}$. We will assume throughout this thesis that $\mathcal{I}$ is a *down-closed* family, i.e. if $B \subset A$ and $A \in \mathcal{I}$, then $B \in \mathcal{I}$. A successful approach for tackling this problem consists of a relaxation and rounding framework (see [4]). We need the following definition before stating this approach.

Definition 1.2. The polytope $P_{\mathcal{I}} \subset [0,1]^N$ corresponding to the independence family $\mathcal{I}$ is the convex hull of the characteristic vectors of independent sets, i.e.

$$P_{\mathcal{I}} := \operatorname{conv}(\{\mathbf{1}_S \mid S \in \mathcal{I}\}).$$

Moreover, a polytope $P \subset [0,1]^N$ is a *relaxation* of $P_{\mathcal{I}}$ (or a *relaxation of* $\mathcal{I}$) if the integer points are the same, i.e. $P \cap \{0,1\}^N = P_{\mathcal{I}} \cap \{0,1\}^N$. Notice this implies that $P_{\mathcal{I}} \subset P$.

We now state the relaxation and rounding framework for the constrained submodular maximization problem.

1. We first relax the problem $\max_{S \in \mathcal{I}} f(S)$ to the problem

$$\max F(x)$$
$$x \in P$$

   where $F : [0,1]^N \mapsto \mathbb{R}_{\geq 0}$ is a suitable extension of $f : \{0,1\}^N \mapsto \mathbb{R}_{\geq 0}$, i.e. the function F needs to satisfy $F|_{\{0,1\}^N} = f$.

   We approximately solve this maximization problem and get a fractional point $x \in P$.

2. We then round this fractional point $x \in P$ into an integral feasible solution $\mathbf{1}_S \in P \cap \{0,1\}^N$ corresponding to an independent set $S \in \mathcal{I}$.

If f is *modular*, there exists a weight function $w : N \mapsto \mathbb{R}$ such that for any $A \subset N$, $f(A) = \sum_{i \in A} w_i$. Hence, a natural choice for the extension F is simply the linear function $F(x) = w^T x$. The relaxation problem is then a linear program for which we can compute an exact solution x^* in polynomial time (provided that P is a *solvable polytope*).

If f is *submodular*, a successful extension for maximization problems is the multilinear extension F_{ML} (first introduced in [4]). It is defined as follows:

$$F_{ML}(x) = \mathbb{E}[f(R(x))] = \sum_{A \subset N} f(A) \prod_{i \in A} x_i \prod_{j \notin A} (1 - x_j)$$

where $R(x) \subset N$ is a random set obtained by independently picking each element i with probability x_i. Moreover, it was shown in [3] that if P is the matroid polytope and f is monotone (i.e. $f(A) \leq f(B)$ for $A \subset B$), there is an approximation algorithm of a factor of $(1 - 1/e)$ for the first part of the relaxation and rounding framework: maximizing the multilinear extension over the matroid polytope. Other approximation factors for the non-monotone case and different constraints were shown in [5].

We are in this thesis interested in the second part of this relaxation and rounding recipe. Hence the main question of interest is the following. *Given a fractional point $x \in P$, how can we round this point into an integral point $\mathbf{1}_S \in P \cap \{0,1\}^N$ corresponding to an independent set $S \in \mathcal{I}$ without losing much objective value?* Contention resolution schemes, introduced in [5], are a powerful and versatile tool to tackle this problem.

1.2 Contention resolution schemes

We present in this subsection a general framework, called *contention resolution schemes* (or *CR schemes*) and introduced in [5], as one possible answer to the aforementioned question. We are given a fractional point $x \in P$ and round it to a feasible integral point in the following way.

1. We first obtain a random set $R(x) \subset N$ by independently including each element $i \in N$ with probability x_i.

2. We then remove some elements from the set $R(x)$ using an algorithm π_x such that the returned set $I := \pi_x(R(x))$ is an independent set. This algorithm can either be deterministic or randomized.

Definition 1.3 ([5]). $\pi = (\pi_x)_{x \in P_\mathcal{I}}$ is a c-balanced *contention resolution scheme* for the polytope P if for every $x \in P$, π_x is an algorithm that takes as input a subset $A \subset \text{supp}(x)$ and outputs an independent set $I := \pi_x(A) \in \mathcal{I}$ contained in A such that

$$\mathbb{P}\Big[i \in \pi_x(R(x)) \mid i \in R(x)\Big] \geq c \quad \forall i \in \text{supp}(x). \tag{1.2}$$

Moreover, a contention resolution scheme is *monotone* if for any $x \in P$:

$$\mathbb{P}[i \in \pi_x(A)] \geq \mathbb{P}[i \in \pi_x(B)] \quad \text{for any } i \in A \subset B \subset \text{supp}(x). \tag{1.3}$$

Remark. Condition (1.2) can be equivalently restated as:

$$\mathbb{P}\Big[i \in \pi_x(R(x))\Big] \geq c\, x_i \qquad \forall i \in N. \tag{1.4}$$

Indeed,

$$\begin{aligned}
\mathbb{P}\Big[i \in \pi_x(R(x)) \mid i \in R(x)\Big] \geq c \iff & \frac{1}{x_i}\mathbb{P}\Big[i \in \pi_x(R(x)), i \in R(x)\Big] \geq c \\
\iff & \frac{1}{x_i}\mathbb{P}\Big[i \in \pi_x(R(x))\Big] \geq c \\
\iff & \mathbb{P}\Big[i \in \pi_x(R(x))\Big] \geq c\, x_i.
\end{aligned}$$

Remark. In all the results in our thesis, we work directly with an inequality description of $P_\mathcal{I} = P$. Therefore, when the polytope $P_\mathcal{I}$ is clear from the context, we will sometimes omit to say that the contention resolution scheme is with respect to that polytope. For example, we will say "a contention resolution scheme for uniform matroids" instead of "a contention resolution scheme for the matroid polytope of a uniform matroid".

A c-balanced CR scheme then gives rise to a natural approximation algorithm for the problem $\max_{S \in \mathcal{I}} f(S)$ if f is a *modular* function, provided that the relaxation polytope P for $\mathcal{I}$ is solvable.

Theorem 1.1 ([5]). *Let $\pi = (\pi_x)_{x \in P}$ be a c-balanced CR scheme for a solvable relaxation P of a down-closed family $\mathcal{I}$ on a ground set N. Let $f : 2^N \mapsto \mathbb{R}_{\geq 0}$ be a modular function. Using the relaxation and rounding framework, we obtain a randomized algorithm returning a set $I \in \mathcal{I}$ satisfying $\mathbb{E}(f(I)) \geq c\ \max_{S \in \mathcal{I}} f(S)$.*

Proof. Since f is *modular*, there exists a weight function $w : N \mapsto \mathbb{R}$ such that for any $A \subset N$, $f(A) = \sum_{i \in A} w_i$. As mentioned in Subsection 1.1, we define the relaxation $\max_{x \in P} w^T x$ and get an optimal solution $x^* \in P$ using linear programming if P is a solvable polytope. We then apply the CR scheme π to get a feasible set $I := \pi_{x^*}(R(x^*))$.

$$\begin{aligned}
\mathbb{E}[f(I)] &= \mathbb{E}\left[\sum_{i \in I} w_i\right] = \mathbb{E}\left[\sum_{i \in N} \mathbf{1}_{\{i \in I\}} w_i\right] = \sum_{i \in N} \mathbb{P}[i \in I]\, w_i \\
&\geq \sum_{i \in N} c\, x_i^*\, w_i = c \sum_{i \in N} x_i^*\, w_i = c\,(w^T x^*) \\
&= c\, \max_{x \in P} w^T x \geq c\, \max_{S \in \mathcal{I}} f(S)
\end{aligned}$$

where the first inequality follows from the c-balancedness of the scheme π and the second one from the relaxation problem. □

A natural question that arises is the following. Can we extend Theorem 1.1 to the setting where f is *submodular* and the relaxation problem is $\max_{x\in P} F_{ML}(x)$, where F_{ML} is the multilinear relaxation defined in Subsection 1.1? It turns the answer is yes, *provided that the CR scheme* π *is monotone.*

Theorem 1.2 ([5])**.** *Let* $\pi = (\pi_x)_{x\in P_{\mathcal{I}}}$ *be a c-balanced monotone CR scheme for a relaxation* P *of a down-closed family* $\mathcal{I}$ *on a ground set* N*. Let* $f : 2^N \mapsto \mathbb{R}_{\geq 0}$ *be a non-negative submodular function. We suppose we have an* α*-approximation algorithm for the relaxation problem* $\max_{x\in P} F_{ML}(x)$ *and let* $x^* \in P$ *be an* α*-approximate optimal solution. Then* $I := \pi^*_x(R(x^*))$ *satisfies* $\mathbb{E}(f(I)) \geq c\, F_{ML}(x^*) \geq \alpha c\, \max_{S\in\mathcal{I}} f(S)$*.*

Thus, monotonicity is an important and desirable property for a CR scheme to have if we want to apply it in the context of constrained submodular maximization.

1.3 Matroids

We introduce in this subsection a general background on matroids. For more on matroids, the interested reader is invited to consult [17].

Definition 1.4. A *matroid* $\mathcal{M}$ is a pair $(N, \mathcal{I})$ consisting of a ground set N and a non-empty family of *independent sets* $\mathcal{I} \subset 2^N$ which satisfy:

- If $A \in \mathcal{I}$ and $B \subset A$, then $B \in \mathcal{I}$.
- If $A \in \mathcal{I}$ and $B \in \mathcal{I}$ with $|A| > |B|$, then $\exists\, i \in A\backslash B$ such that $B \cup \{i\} \in \mathcal{I}$.

The first condition simply means that $\mathcal{I}$ is a down-closed family. The second condition can be stated in words as: if B is independent, and there exists a larger independent set A, then B can be extended by adding an element of A. Therefore, any non-maximum (cardinality-wise) independent set can be extended. This means that every *maximal* (inclusion-wise) independent set is *maximum* (i.e. of maximum cardinality). Such a set is called a *base* of the matroid.

Definition 1.5. A *base* of the matroid $\mathcal{M} = (N, \mathcal{I})$ is an independent set $B \in \mathcal{I}$ of maximum cardinality. Equivalently, it is a maximal inclusion-wise independent set.

A base of a matroid can thus be found by a greedy process: start with the empty set and add elements one by one arbitrarily while keeping independence.

Definition 1.6. Let $\mathcal{M} = (N, \mathcal{I})$ be a matroid. The *rank function* $r : 2^N \mapsto \mathbb{N}$ is defined as $r(A) = \max\{|S| : S \subset A, S \in \mathcal{I}\}$

The rank function computes, for any subset A of the ground set, the cardinality of a maximal independent set included in A.

Definition 1.7. A *circuit* C of a matroid $\mathcal{M} = (N, \mathcal{I})$ is an inclusion-wise minimal dependent set.

Therefore, if we remove any element from a circuit, we get an independent set.

Definition 1.8. The *girth* g of a matroid $\mathcal{M} = (N, \mathcal{I})$ is the length of a shortest circuit.

Remark. We have introduced matroids using Definition 1.4, which are called *independence axioms*. However, this is not the only way we can define matroids. Indeed, one could have used other sets of axioms, such as *base axioms*, or even *circuit axioms* (see [13] for more details).

Definition 1.9. (Base axioms) A matroid $\mathcal{M}$ is a pair $(N, \mathcal{B})$ where N is a ground set and $\mathcal{B}$ is a non-empty collection of subsets of N, called *bases*, satisfying:

- For any distinct $B_1, B_2 \in \mathcal{B}$, we have $B_1 \not\subset B_2$ and $B_2 \not\subset B_1$, i.e. no base properly contains another.
- For any $B_1, B_2 \in \mathcal{B}$, and any $x \in B_1$, there exists $y \in B_2$ such that $B_1 - x + y \in \mathcal{B}$

Definition 1.10. (Circuit axioms) A matroid $\mathcal{M}$ is a pair $(N, \mathcal{C})$ where N is a ground set and $\mathcal{C}$ is a non-empty collection of subsets of N, called *circuits*, satisfying:

- For any distinct $C_1, C_2 \in \mathcal{C}$, we have $C_1 \not\subset C_2$ and $C_2 \not\subset C_1$, i.e. no circuit properly contains another.
- For any $C_1, C_2 \in \mathcal{C}$, and any $x \in C_1 \cap C_2$, we have that $(C_1 \cup C_2) - x$ contains a member of $\mathcal{C}$.

We now introduce the matroid polytope and give an inequality description for it. The proof of the inequality description can be found in [6].

Definition 1.11. Let $(N, \mathcal{I})$ be a matroid. The *matroid polytope* is defined as:

$$P_{\mathcal{I}} := \text{conv}(\{\mathbf{1}_S : S \in \mathcal{I}\}) = \{x \in \mathbb{R}^N_{\geq 0} \mid x(A) \leq r(A) \quad \forall A \subset N\}. \tag{1.5}$$

Let us now give some examples of matroids that will interest us in this thesis. These examples also nicely illustrate all the different concepts introduced above.

Example 1.1 (Graphic matroids)**.** Let $G = (V, E)$ be a graph. The graphic matroid $\mathcal{M}_G := (E, \mathcal{I})$ is the matroid where the ground set is E and the independent sets are

$$\mathcal{I} := \{F \subset E \mid F \text{ is a forest}\}.$$

In other words, the independent sets are all the acyclic subgraphs of G. If the graph G is connected, a *base* of the graphic matroid is a spanning tree. If G has several connected components, a *base* corresponds to a spanning tree for each component. The *rank* of a subset of edges outputs the size of the maximal forest (or acyclic graph) contained in those edges. A *circuit* of the graphic matroid simply corresponds to a cycle of the graph. The *girth* of this matroid coincides with the usual notion of girth g for a graph, i.e. the length of a shortest cycle.

Example 1.2 (Uniform matroids)**.** Let $N = \{1, \ldots, n\}$ be a ground set. The uniform matroid of rank k on n elements $U_n^k := (N, \mathcal{I})$ is the matroid whose independent sets are all the subsets of the ground set of cardinality at most k:

$$\mathcal{I} := \{A \subset N \mid |A| \leq k\}.$$

A *base* of U_n^k is simply a subset of size exactly k, and a *circuit* is subset of size $k + 1$. The *rank* of an independent set is the cardinality of that set, and the rank of a dependent set is k. The *girth* of U_n^k is clearly equal to $k + 1$.

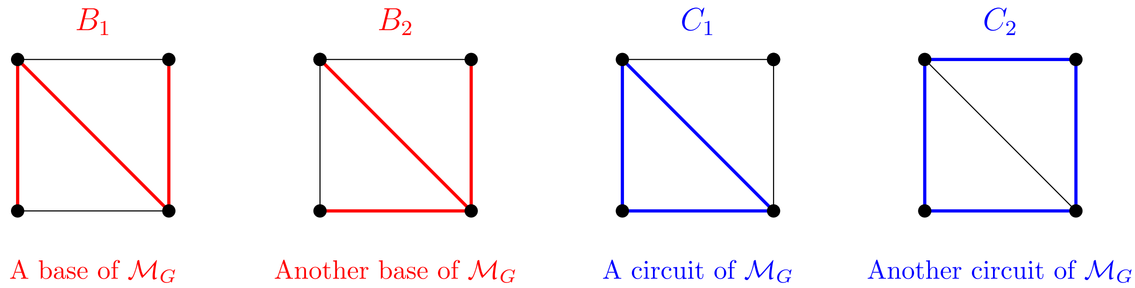


Figure 1: Some bases and circuits for the graphic matroid of a specific graph.

Example 1.3 (Partition Matroids)**.** Partition matroids are a generalization of uniform matroids. Suppose the ground set $N = \{1, \dots, n\}$ is partitioned into k blocks: $N = D_1 \sqcup \cdots \sqcup D_k$ and each block D_i has a certain capacity $d_i \in \mathbb{Z}_{\geq 0}$. The independent sets are then:

$$\mathcal{I} := \Big\{ A \subset N \mid |A \cap D_i| \leq d_i \qquad \forall i \in \{1, \dots, k\} \Big\}.$$

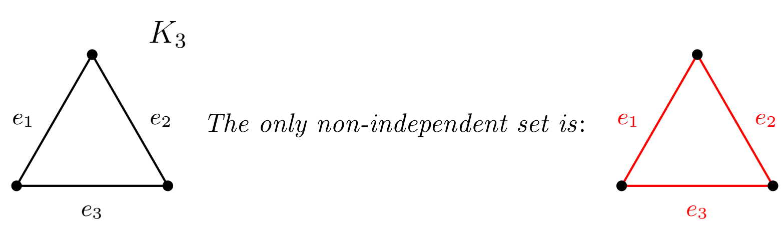
The uniform matroid U_n^k is simply a partition matroid with one block N and one capacity k. Moreover, the restriction of a partition matroid to each block D_i is a uniform matroid of rank d_i on the ground set D_i.

1.4 An introductory example

We start by giving a very easy and natural CR scheme for the graphic matroid polytope of the graph K_3. We believe this nicely exemplifies the concept of a CR scheme and will help build intuition for the main results of this thesis.

Let $G = K_3$ and let $\mathcal{M}_G = (E, \mathcal{I})$ be the graphic matroid. We can explicitly write all the elements, as well as the independent sets.

- $E = \{e_1, e_2, e_3\}$
- $\mathcal{I} = \Big\{ \emptyset, \{e_1\}, \{e_2\}, \{e_3\}, \{e_1, e_2\}, \{e_1, e_3\}, \{e_2, e_3\} \Big\}$



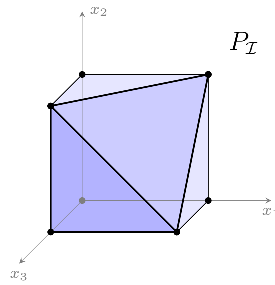
Notice the only set $A \in 2^E$ which is not an independent set is the full set $E = \{e_1, e_2, e_3\}$. That is the only "problematic" set if $R(x)$ happens to be rounded to it in the first step of a CR scheme, and we will have to build an algorithm which removes at least one element if that happens.

Let's now explicitly compute the inequality description of the corresponding matroid polytope by using (1.5).

$$P_{\mathcal{I}} := \{x \in \mathbb{R}^E_{\geq 0} \mid x(A) \leq r(A) \quad \forall A \subset E\}.$$

For notational simplicity, we denote $x_i = x(e_i)$ for each $i \in \{1,2,3\}$. By writing down all the constraints and removing the redundant ones, we arrive at the following simple description.

$$P_{\mathcal{I}} = \left\{ x \in \mathbb{R}^E_{\geq 0} \;\middle|\; \begin{array}{c} x_1 \leq 1 \\ x_2 \leq 1 \\ x_3 \leq 1 \\ x_1 + x_2 + x_3 \leq 2 \end{array} \right\} \tag{1.6}$$



Each subset of edges $A \subset E$ corresponds to one constraint of the matroid polytope. Hence, there are 2^E constraints (in addition to the non-negativity constraints) in the original inequality description. However, as is the case in this example, some constraints can be *redundant*. In particular, we did not write the constraints corresponding to $\{e_1, e_2\} : x_1 + x_2 \leq 2$; $\{e_1, e_3\} : x_1 + x_3 \leq 2$; $\{e_2, e_3\} : x_2 + x_3 \leq 2$. Indeed, these can be obtained by summing the constraints $\{e_1\} + \{e_2\}$; $\{e_1\} + \{e_3\}$; $\{e_2\} + \{e_3\}$.

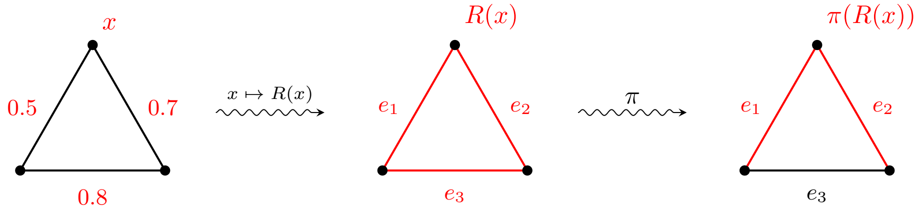
Let's now define the CR scheme. We give a brief reminder of the framework. We are given a fractional point $x \in P_{\mathcal{I}}$. This point can be seen as a weight x_i on each edge e_i in the graph K_3. We then obtain $R(x)$ by rounding each coordinate independently to 1 with probability x_i. $R(x)$ is now a random vector in $\{0,1\}^E$, or, equivalently, a random subset of the edges. However, this obtained set might not be independent, in which case we need to (randomly) remove some elements from it in order to make it independent. As mentioned above, the only non-independent set is $E = \{e_1, e_2, e_3\}$. Therefore a very natural oblivious (i.e. which does not depend on the input point $x \in P_{\mathcal{I}}$) randomized CR scheme is the following.

Algorithm 1.1.

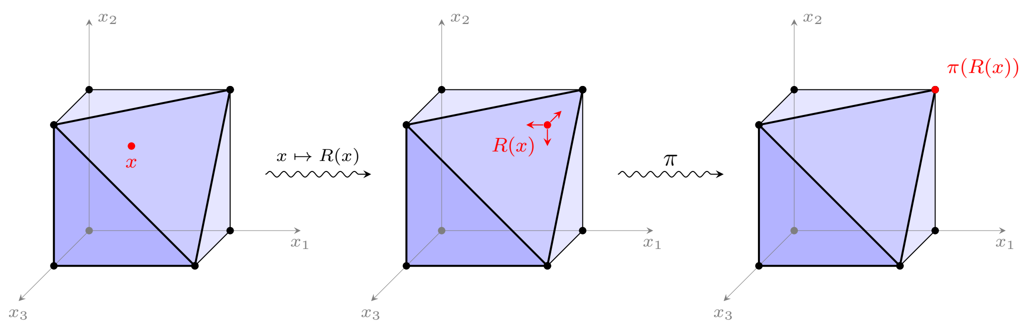
$$\pi : 2^E \mapsto \mathcal{I}$$
$$\pi(A) = A \quad \text{for any } A \neq \{e_1, e_2, e_3\}$$
$$\pi(\{e_1, e_2, e_3\}) = \begin{cases} \{e_1, e_2\} & \text{with probability } 1/3 \\ \{e_1, e_3\} & \text{with probability } 1/3 \\ \{e_2, e_3\} & \text{with probability } 1/3. \end{cases}$$

In words, if $R(x)$ happens to round to $\{e_1, e_2, e_3\}$, then we remove one element with uniform probability. We now want to prove this CR scheme is c-balanced for some c. The goal is thus to find a scalar $c \in [0,1]$ such that $\mathbb{P}[e \in \pi(R(x)) \mid e \in R(x)] \geq c$ for any $e \in \text{supp}(x)$. It turns out that $c = 2/3$ works in this case.

Proposition 1.1. *Algorithm 1.1 is a* $2/3$*-balanced CR scheme for the graphic matroid polytope of* K_3.



(a) One run of Algorithm 1.1 on the graph K_3.



(b) One run of Algorithm 1.1 on $P_{\mathcal{I}}$.

Figure 2: Two different ways to visualize a run of the CR scheme described by Algorithm 1.1.

Proof. Instead of directly trying to compute $\mathbb{P}[e \in \pi(R(x)) \mid e \in R(x)]$, we will work with the complement $\mathbb{P}[e \notin \pi(R(x)) \mid e \in R(x)]$ and try to upper bound this quantity. This will be the strategy used to prove the balancedness of every CR scheme in this thesis.
Suppose $x_1 > 0$. We use the total probability law on the events $\{R(x) = E\}$ and $\{R(x) \neq E\}$ to compute the desired probability:

$$\begin{aligned}\mathbb{P}\big[e_1 \notin \pi(R(x) \mid e_1 \in R(x)\big] &= \mathbb{P}\big[e_1 \notin \pi(R(x)), R(x) = E \mid e_1 \in R(x)\big] \\ &\quad + \mathbb{P}\big[e_1 \notin \pi(R(x)), R(x) \neq E \mid e_1 \in R(x)\big] \\ &= \mathbb{P}\big[e_1 \notin \pi(R(x)) \mid R(x) = E\big]\, \mathbb{P}\big[R(x) = E \mid e_1 \in R(x)\big] \\ &\quad + \mathbb{P}[e_1 \notin \pi(R(x)) \mid R(x) \neq E, e_1 \in R(x)]\, \mathbb{P}\big[R(x) \neq E \mid e_1 \in R(x)\big] \\ &= \mathbb{P}\big[e_1 \notin \pi(R(x)) \mid R(x) = E\big]\, \mathbb{P}\big[e_2 \in R(x), e_3 \in R(x)\big] = \frac{1}{3}\, x_2 x_3.\end{aligned}$$

By doing these exact same steps again, we get three exact probabilities.

- $\mathbb{P}\big[e_1 \notin \pi(R(x) \mid e_1 \in R(x)\big] = \frac{1}{3}\, x_2 x_3$ for every $x \in P_{\mathcal{I}}$ with $x_1 > 0$.
- $\mathbb{P}\big[e_2 \notin \pi(R(x) \mid e_2 \in R(x)\big] = \frac{1}{3}\, x_1 x_3$ for every $x \in P_{\mathcal{I}}$ with $x_2 > 0$.
- $\mathbb{P}\big[e_3 \notin \pi(R(x) \mid e_3 \in R(x)\big] = \frac{1}{3}\, x_1 x_2$ for every $x \in P_{\mathcal{I}}$ with $x_3 > 0$.

Since $x_1, x_2, x_3 \leq 1$ by (1.6), we get that for every $x \in P_{\mathcal{I}}$,

$$\mathbb{P}\big[e \notin \pi(R(x) \mid e \in R(x)\big] \leq \frac{1}{3} \qquad \forall e \in \operatorname{supp}(x).$$

Our desired result therefore follows:

$$\mathbb{P}\big[e \in \pi(R(x) \mid e \in R(x)\big] \geq 1 - \frac{1}{3} = \frac{2}{3} \qquad \forall e \in \operatorname{supp}(x).$$

□

A natural question is then the following. *Can we find a CR scheme with a higher balancedness than 2/3? If so, what is the best that we can do?* The answer is that we can indeed do better, and the best we can achieve is $23/27 \approx 0.85$. Here is a CR scheme that achieves that.

Algorithm 1.2. For every $x \in P_{\mathcal{I}}$,

$$\begin{aligned}
&\pi_x : 2^E \mapsto \mathcal{I}\\
&\pi_x(A) = A \quad \text{for any } A \neq \{e_1, e_2, e_3\}\\
&\pi_x(\{e_1, e_2, e_3\}) = \begin{cases} \{e_1, e_2\} & \text{with probability } x_3/(x_1 + x_2 + x_3)\\ \{e_1, e_3\} & \text{with probability } x_2/(x_1 + x_2 + x_3)\\ \{e_2, e_3\} & \text{with probability } x_1/(x_1 + x_2 + x_3)\end{cases}
\end{aligned}$$

Proposition 1.2. *Algorithm 1.2 is a 23/27-balanced CR scheme for the graphic matroid polytope of K_3. Moreover, this balancedness is optimal, i.e. there does not exist a c-balanced CR scheme for the graphic matroid polytope of K_3 satisfying $c > 23/27$.*

Notice that Algorithm 1.2 is not oblivious anymore, i.e. it does depend on the input point $x \in P_{\mathcal{I}}$. Proposition 1.2 will be a special case of the first result that we will present in this thesis. Indeed, we will provide an optimal CR scheme for any matroid with pairwise disjoint circuits.

1.5 Known results and our contributions

In this thesis, we are interested in designing contention resolution schemes for different classes of matroids. A CR scheme with a balancedness of $1-(1-1/n)^n$ is provided for the uniform matroid of rank 1 in [7] and [8]. Moreover, it is shown that this is *optimal*, which means that no c-balanced CR scheme exists for the uniform matroid of rank 1 with $c > 1-(1-1/n)^n$. A result proved in [5] shows that there exists in fact a $1-(1-1/n)^n$-balanced CR scheme for any general matroid. This existence proof can then be turned into an efficient algorithm with a balancedness of $1 - 1/e \approx 0.63$. It is also argued in that same paper that this is (asymptotically) optimal, since $1-(1-1/n)^n$ converges to $1 - 1/e$ as n gets large and one cannot do better than $1 - (1 - 1/n)^n$ for the uniform matroid of rank one, as previously mentioned. However, this algorithm uses random sampling and lacks simplicity, which is why another simpler CR scheme with a worse balancedness was also presented.

There has been work done in getting CR schemes for different types of independence families (see [2], [11]), or by having the elements of the random set $R(x)$ arrive in an online fashion (see [1], [9], [14]).

However, to the best of our knowledge, not much work has been done in the direction of finding subclasses of matroids where the $1-1/e$ balancedness factor can be improved. This is the problem tackled in this thesis, where we consider three different types of matroids and provide simple CR schemes achieving a strictly better balancedness factor than $1 - 1/e$. Moreover, we also show that the achieved balancedness factors are optimal.

Our first result is an optimal monotone CR scheme for matroids with pairwise disjoint circuits. The balancedness of this scheme is of $1 - \frac{1}{g}\,(1 - \frac{1}{g})^{g-1}$, where g is the girth, or length of a shortest circuit of the matroid. Note that $1 - \frac{1}{g}\,(1 - \frac{1}{g})^{g-1} \geq 0.75$ for any $g \geq 2$, which is already much higher than $1 - 1/e \approx 0.63$.

The second and main result of this thesis is an optimal monotone CR scheme for the uniform matroid of rank k on n elements, where the balancedness is of $c(k,n) := 1 - \binom{n}{k}\left(1 - \frac{k}{n}\right)^{n+1-k}\left(\frac{k}{n}\right)^{k}$. This generalizes the previous result of $1 - (1 - 1/n)^n$ for the rank one case by plugging in $k = 1$. Moreover, for a fixed value of k, $c(k,n) \xrightarrow{n\to\infty} 1 - e^{-k}k^k/k!$, which also generalizes the asymptotical $1 - 1/e$ balancedness for $k = 1$. Finally, even in that case, our scheme is in a sense simpler than the one provided in [7] and [8], since our algorithm simply consists of assigning a probability to each base contained in the input set and picking one base according to that probability distribution.

Finally, the above CR scheme for uniform matroids naturally generalizes to partition matroids. If we denote by $c(k,n)$ the optimal balancedness for the uniform matroid U_n^k, then the balancedness we get for a partition matroid with blocks D_i and capacities d_i is $\min_i c(d_i, |D_i|)$. Again, we also prove that this is optimal.

2 An optimal monotone contention resolution scheme for matroids with pairwise disjoint circuits

2.1 The CR Scheme

We provide in this section an optimal monotone CR Scheme for any matroid with pairwise disjoint circuits. We are given a point $x \in P_{\mathcal{I}}$ and a subset $A \subset \text{supp}(x)$. The CR scheme checks one by one whether each circuit is completely contained inside the set A. When a circuit is completely included, the algorithm removes one element from it randomly, where the probability depends on the input point $x \in P_{\mathcal{I}}$. The framework is the following:

- $N = \{e_1, .., e_n\}$ is the ground set.
- $\mathcal{M} = (N, \mathcal{I})$ is a matroid with circuits $\{C_1, ..., C_k\}$ where $C_i \cap C_j = \emptyset$ for every $i \neq j \in \{1, ..., k\}$.
- $P_{\mathcal{I}} = \{x \in \mathbb{R}^N_{\geq 0} \mid x(A) \leq r(A) \quad \forall A \subset N\} = \left\{x \in [0,1]^N \mid x(C_i) \leq |C_i| - 1 \quad \forall i \in \{1, ..., k\}\right\}$ is the corresponding matroid polytope.

We may assume without loss of generality that the matroid does not have loops, i.e. the girth of $\mathcal{M}$ satisfies $g \geq 2$. Indeed, if an element $e \in N$ is a loop, it is a one element dependent set and $r(\{e\}) = 0$. It follows that any point $x \in P_{\mathcal{I}}$ satisfies $x_e = 0$ and that the random set $R(x)$ will never contain the element $\{e\}$ in the first place.

Algorithm 2.1 (CR scheme π for $P_{\mathcal{I}}$)**.** We are given a point $x \in P_{\mathcal{I}}$ and a set $A \subset \text{supp}(x)$.

- For each circuit C_i, check whether C_i is completely included in A, i.e. check whether $C_i \subset A$ for each $i \in \{1, \ldots, k\}$.
- If $C_i \subset A$, remove one element $e \in C_i$ randomly with probability $x(e)/x(C_i)$.

Remark. We here use a standard notation that we have already used before, which is that for any $A \subset N, x(A) := \sum_{e \in A} x(e)$.

Theorem 2.1. *The CR scheme described in Algorithm 2.1 for a matroid with pairwise disjoint circuits has a balancedness of*

$$c = 1 - \frac{1}{g}\left(1 - \frac{1}{g}\right)^{g-1},$$

where g is the girth of the matroid $\mathcal{M}$.

Remark. This balancedness is actually *optimal*. That is, no CR scheme can achieve a higher balancedness for this type of matroids. We prove that in the next section.

Notice that c is always greater than $(1 - 1/e) \approx 0.63$, which is the balancedness of the CR scheme provided for an arbitrary matroid in [5]. The worst case here is $3/4 = 0.75$, which corresponds to

g	2	3	4	5	6	10
c	0.75	0.85	0.89	0.92	0.93	0.96

Table 1: Numerical values for the balancedness of the CR scheme described in Algorithm 2.1

$g = 2$. Indeed, the balancedness grows as g increases, since

$$x \to 1 - \frac{1}{x}\left(1 - \frac{1}{x}\right)^{x-1}$$

is a strictly increasing function for $x \geq 2$. This is illustrated in Table 1.

Let us now move on to the proof of Theorem 2.1. We will first need the following lemma.

Lemma 2.1. *Let $\mathcal{M} = (N, \mathcal{I})$ be a matroid and let $x \in P_{\mathcal{I}}$. Let C be a circuit of the matroid with $x(C) > 0$. Then:*

$$\frac{\prod_{e \in C} x(e)}{x(C)} \leq \frac{1}{|C|}\left(1 - \frac{1}{|C|}\right)^{|C|-1} \leq \frac{1}{g}\left(1 - \frac{1}{g}\right)^{g-1}$$

where g is the girth of the matroid.

Proof of Lemma 2.1. The proof is a consequence of the arithmetic-geometric mean inequality and of the constraint of the matroid polytope corresponding to the circuit C: $x(C) \leq |C| - 1$. We set $m := |C|$ for simplicity. As a reminder, the arithmetic-geometric mean inequality states:

$$\prod_{e \in C} x(e) \leq \left(\frac{\sum_{e \in C} x(e)}{|C|}\right)^{|C|} = \frac{x(C)^m}{m^m}.$$

Hence,

$$\frac{\prod_{e \in C} x(e)}{x(C)} \leq \frac{x(C)^m}{m^m\, x(C)} = \frac{x(C)^{m-1}}{m\, m^{m-1}} \leq \frac{(m-1)^{m-1}}{m\, m^{m-1}} = \frac{1}{m}\left(1 - \frac{1}{m}\right)^{m-1} \leq \frac{1}{g}\left(1 - \frac{1}{g}\right)^{g-1}.$$

The first inequality follows from the arithmetic-geometric mean inequality, the second one from the constraint $x(C) \leq |C| - 1$ of $P_{\mathcal{I}}$ and the last one from the fact that $g \leq m$. □

We are now ready to prove Theorem 2.1.

Proof of Theorem 2.1. Since the circuits are by definition the minimal (inclusion-wise) dependent sets of the matroid, removing one element from them gives an independent set. Since the circuits are all pairwise disjoint, the algorithm removes one element from each of the circuits completely contained in A, hence returning an independent set which is a subset of A.

Let's compute the balancedness of the scheme. We are given a point $x \in P_{\mathcal{I}}$ and a random set $R(x) \subset N$ where each element $e_i \in N$ is included with probability $x(e_i)$ independently.

Let $e \in \text{supp}(x)$ and suppose $R(x)$ contains e. If e does not lie in any circuit of the matroid $\mathcal{M}$, then Algorithm 2.1 will always keep that element. Hence:

$$\mathbb{P}\big[e \in \pi_x(R(x)) \mid e \in R(x)\big] = 1.$$

We can thus suppose that there exists a unique $i \in \{1, ..., k\}$ such that $e \in C_i$.
If $C_i \not\subset \text{supp}(x)$, then C_i will never be completely included in $R(x)$ and Algorithm 2.1 will thus always keep the element e. Our desired probability is equal to one again:

$$\mathbb{P}\big[e \in \pi_x(R(x)) \mid e \in R(x)\big] = 1.$$

Hence, we can assume that $C_i \subset \text{supp}(x)$. We condition on the event $\{C_i \subset R(x)\}$ to compute the desired probability.

$$\begin{aligned}
\mathbb{P}\big[e \notin \pi_x(R(x)) \mid e \in R(x)\big] &= \mathbb{P}\big[e \notin \pi_x(R(x)) \mid e \in R(x), C_i \subset R(x)\big]\ \mathbb{P}\big[C_i \subset R(x) \mid e \in R(x)\big] \\
&\quad + \mathbb{P}\big[e \notin \pi_x(R(x)) \mid e \in R(x), C_i \not\subset R(x)\big]\ \mathbb{P}\big[C_i \not\subset R(x) \mid e \in R(x)\big] \\
&= \mathbb{P}\big[e \notin \pi_x(R(x)) \mid C_i \subset R(x)\big]\ \mathbb{P}\big[C_i \subset R(x) \mid e \in R(x)\big] \\
&= x(e)/x(C_i) \prod_{f \in C_i \setminus e} x(f) \\
&= \left(\prod_{e \in C_i} x(e)\right) \Big/ x(C_i) \\
&\leq \frac{1}{g}\left(1 - \frac{1}{g}\right)^{g-1},
\end{aligned}$$

where the inequality follows from Lemma 2.1. We therefore get the desired result by taking the complement:

$$\mathbb{P}\big[e \in \pi_x(R(x)) \mid e \in R(x)\big] \geq 1 - \frac{1}{g}\left(1 - \frac{1}{g}\right)^{g-1}.$$

□

2.2 Optimality

We provide in this section a hardness result about the balancedness of a contention resolution schemes for any matroid. The bound that we find takes into account the girth g of the matroid, i.e. the circuit of shortest length. In particular, we show that the balancedness of any CR scheme for any matroid cannot be higher than $1 - 1/g\,(1 - 1/g)^{g-1}$. This also shows us that Algorithm 2.1 is an *optimal* CR scheme for matroids with pairwise disjoint circuits.

Theorem 2.2. *Let $\mathcal{M} = (N, \mathcal{I})$ be a matroid with girth g. There does not exist a c-balanced CR scheme for $\mathcal{M}$ with $c > 1 - \frac{1}{g}\left(1 - \frac{1}{g}\right)^{g-1}$.*

The proof for Theorem 2.2 generalizes the idea of the proof of a similar statement for uniform matroids of rank one given in [5].

Proof. We let $N = \{e_1, \dots, e_n\}$ be our ground set and C a shortest circuit of the matroid. Without loss of generality, we may reorder the elements of the ground set so that $C = \{e_1, \dots, e_k\}$ where we denote by k the cardinality, or length of that circuit. Hence $k = g$, where g is the girth of the matroid.

We fix the following point in the matroid polytope:

$$x(e) = \begin{cases} (k-1)/k & \text{if } e \in C. \\ 0 & \text{if } e \notin C. \end{cases} \tag{2.1}$$

Notice that $x \in P_{\mathcal{I}} = \{x \in \mathbb{R}^N_{\geq 0} \mid x(A) \leq r(A) \quad \forall A \subset N\}$. Indeed, for any $A \subsetneq C$,

$$x(A) = \frac{k-1}{k}|A| < |A| = r(A),$$

since any strict subset of a circuit is independent. Moreover,

$$x(C) = k - 1 = r(C).$$

Since the values of x are zero everywhere outside the circuit C, it is clear that all the other constraints of the matroid polytope are satisfied as well.

Let π be any c-balanced CR scheme for $\mathcal{M}$, and let $R(x) \subset N$ be a random set satisfying $\mathbb{P}[e \in R(x)] = x(e)$ for every $e \in N$ independently. We denote by $I := \pi_x(R(x))$ the independent set returned by this CR scheme. Notice that since I is always a subset of $R(x)$, we get that

$$\mathbb{E}\left[|I|\right] \leq \mathbb{E}\left[r(R(x))\right]. \tag{2.2}$$

Moreover, due to our choice of the point x in (2.1) and the definition of a c-balanced CR scheme,

$$\mathbb{E}\left[|I|\right] = \mathbb{E}\left[\sum_{e \in N} \mathbf{1}_{\{e \in I\}}\right] = \sum_{e \in N} \mathbb{P}[e \in I] \geq \sum_{e \in N} c\, x(e) = \sum_{e \in C} c\, x(e) = (k-1)c. \tag{2.3}$$

We thus get the following upper bound for the balancedness factor by combining (2.2) and (2.3):

$$c \leq \frac{\mathbb{E}\big[r(R(x))\big]}{k-1}. \tag{2.4}$$

Let's now compute the expected rank by using the following facts:

- Since $\text{supp}(x) = C$, we get that $r(R(x))$ can only take values in $\{0, \ldots, k-1\}$.
- $\mathbb{P}[r(R(x)) = i] = \mathbb{P}[|R(x)| = i] = \binom{k}{i} \left(\frac{k-1}{k}\right)^i \left(\frac{1}{k}\right)^{k-i}$ for any $i \in \{0, \ldots, k-2\}$.
- $\mathbb{P}[r(R(x)) = k-1] = \mathbb{P}[|R(x)| = k-1] + \mathbb{P}[|R(x)| = k] = \binom{k}{k-1} \left(\frac{k-1}{k}\right)^{k-1} \left(\frac{1}{k}\right) + \left(\frac{k-1}{k}\right)^k$.

Then,

$$\begin{aligned}
\mathbb{E}\big[r(R(x))\big] &= \sum_{i=0}^{k-1} i\, \mathbb{P}[r(R(x)) = i] \\
&= \sum_{i=1}^{k-1} i \binom{k}{i} \left(\frac{k-1}{k}\right)^{i} \left(\frac{1}{k}\right)^{k-i} + (k-1)\left(\frac{k-1}{k}\right)^{k} \\
&= \frac{1}{k^k} \sum_{i=1}^{k-1} i \binom{k}{i} (k-1)^i + \frac{(k-1)^{k+1}}{k^k} \\
&= \frac{1}{k^k}\Big((k-1)k^k - k(k-1)^k\Big) + \frac{(k-1)^{k+1}}{k^k} \\
&= k - 1 - \frac{k(k-1)^k}{k^k} + \frac{(k-1)^{k+1}}{k^k} \\
&= (k-1)\left(1 - \frac{k(k-1)^{k-1}}{k^k} + \frac{(k-1)^k}{k^k}\right) \\
&= (k-1)\left(1 - \frac{1}{k}\left(\frac{k-1}{k}\right)^{k-1}\right) \\
&= (k-1)\left(1 - \frac{1}{k}\left(1 - \frac{1}{k}\right)^{k-1}\right)
\end{aligned} \tag{2.5}$$

where we have used the equality $\sum_{i=1}^{k-1} i \binom{k}{i} (k-1)^i = (k-1)k^k - k(k-1)^k$ from the third to the fourth line. This is an easy consequence of the binomial formula by taking the derivative on both sides.

By plugging the above into (2.4) and remembering that $k = g$, where g is the girth of the matroid $\mathcal{M} = (N, \mathcal{I})$, we finally get:

$$c \leq 1 - \frac{1}{g}\left(1 - \frac{1}{g}\right)^{g-1}.$$

□

2.3 Monotonicity

We prove in this subsection that the CR scheme provided in Algorithm 2.1 is monotone.

Theorem 2.3. *Algorithm 2.1 is a monotone CR scheme for any matroid $\mathcal{M}$ with disjoint circuits, i.e. for any $x \in P_{\mathcal{I}}$ and any $e \in A \subset B \subset supp(x)$,*

$$\mathbb{P}[e \in \pi_x(A)] \geq \mathbb{P}[e \in \pi_x(B)].$$

Proof. Let $x \in P_{\mathcal{I}}$. If e does not lie in any circuit of the matroid, then π_x will always keep that element (c.f. Algorithm 2.1). This means that $\mathbb{P}[e \in \pi_x(A)] = 1$ and the theorem trivially holds. We thus suppose that e is contained in a unique circuit C_i for some $i \in \{1, \dots, k\}$. If C_i is not completely contained in A, then again Algorithm 2.1 will always keep the element e, and therefore $\mathbb{P}[e \in \pi_x(A)] = 1$. Finally, if $e \in C_i \subset A$, we also have that $C_i \subset B$, which means that

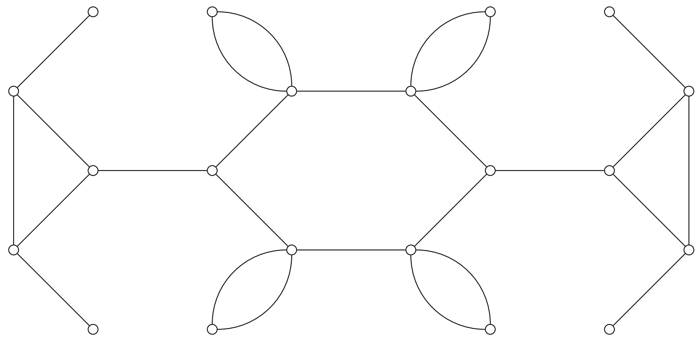


Figure 3: An example of a cactus graph

$$\mathbb{P}[e \in \pi_x(A)] = \mathbb{P}[e \in \pi_x(B)] = 1 - \frac{x(e)}{x(C_i)},$$

and the theorem holds in that case as well. □

2.4 Applications to graphic matroids

A direct and straightforward application of Theorem 2.1 is to the graphic matroid of graphs with pairwise disjoint cycles (where by disjoint we mean the edge sets of those cycles). Equivalently, these are graphs where each edge lies in at most one cycle. It turns out that such a definition already exists for connected graphs.

Definition 2.1. A connected graph G is a *cactus graph* if each edge of G lies in at most one cycle. Equivalently, the cycles of the connected graph have disjoint edge sets.

Remark. The name *cactus graph* was originally introduced in [10]. They were previously also named *Husimi trees* in [12].

Therefore, the graphs G for which we can apply Algorithm 2.1 / Theorem 2.1 are disjoint union of cacti.

Corollary (Corollary of Theorem 2.1)**.** *Let G be a disjoint union of cacti. Then Algorithm 2.1 is a c-balanced CR scheme for the graphic matroid polytope of G with*

$$c = 1 - \frac{1}{g}\left(1 - \frac{1}{g}\right)^{g-1},$$

where g is the girth of G.

It turns out that there is a broad class of graphs which satisfy that property. Indeed, any simple graph without even cycles is a disjoint union of cacti.

Proposition 2.1 ([18])**.** *Let $G = (V, E)$ be a simple graph without even cycles. Then each edge lies in at most one cycle.*

We provide a detailed proof which was first found in the online reference [18].

Proof. Suppose for contradiction that there exists an edge $e \in E$ that is contained in two distinct cycles C_1 and C_2. We split the proof into two cases.

Case 1: Suppose C_1 and C_2 intersect in one common path. Denote the common path of C_1 and C_2 by P and its endpoints by u and v.

- If P has even length, then the path $C_1 \backslash P$ from v to u must have odd length, since C_1 has odd length. Likewise, the path $C_2 \backslash P$ from v to u must have odd length. We can then construct a new cycle $C_3 := (C_1 \backslash P) \cup (C_2 \backslash P)$ of even length, which is a contradiction.
- If P has odd length, then the path $C_1 \backslash P$ from v to u must have even length, since C_1 has odd length. Likewise, the path $C_2 \backslash P$ from v to u must have even length. We can then construct a new cycle $C_3 := (C_1 \backslash P) \cup (C_2 \backslash P)$ of even length, which is a contradiction.

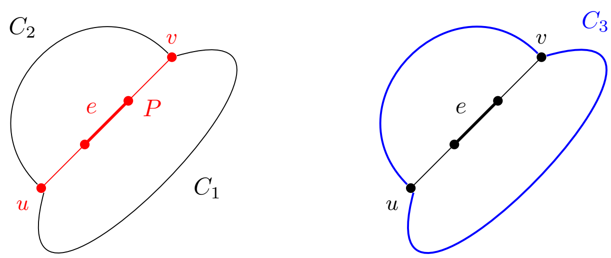


Figure 4: Illustration of the first case of the proof of Theorem 2.1

Case 2: Suppose C_1 and C_2 intersect in at least two disjoint common paths. Let P_1 and P_2 be two disjoint consecutive common paths of $C_1 \cap C_2$. Let a be the last vertex of P_1 and let b the first vertex of P_2. We construct a new cycle C_3 the following way: we follow the cycle C_1 from a to b (we call this path Q_1), and then follow C_2 from b to a (we call this path Q_2). Then, since C_3 must have odd length by assumption, $Q_1 \subset C_1$ and $Q_2 \subset C_2$ must have different parities. But then $C_1 - Q_1 + Q_2$ (we modify C_1 by replacing Q_1 by Q_2) is a cycle of even length, which is a contradiction.

□

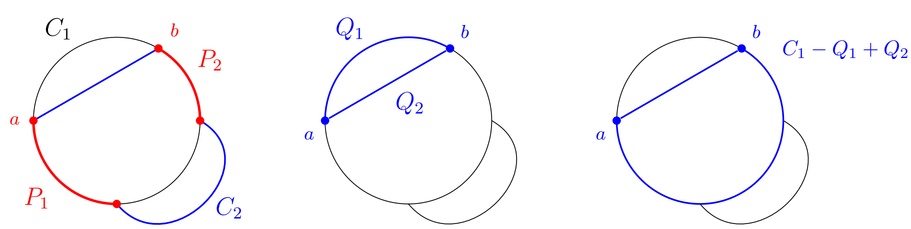


Figure 5: Illustration of the second case of the proof of Theorem 2.1

This allows us to have another corollary of Theorem 2.1.

Corollary (Corollary of Theorem 2.1)**.** *Let G be a simple graph without even cycles. Then there exists a c-balanced CR scheme for the graphic matroid polytope of G satisfying $c \geq 23/27 \approx 0.85$.*

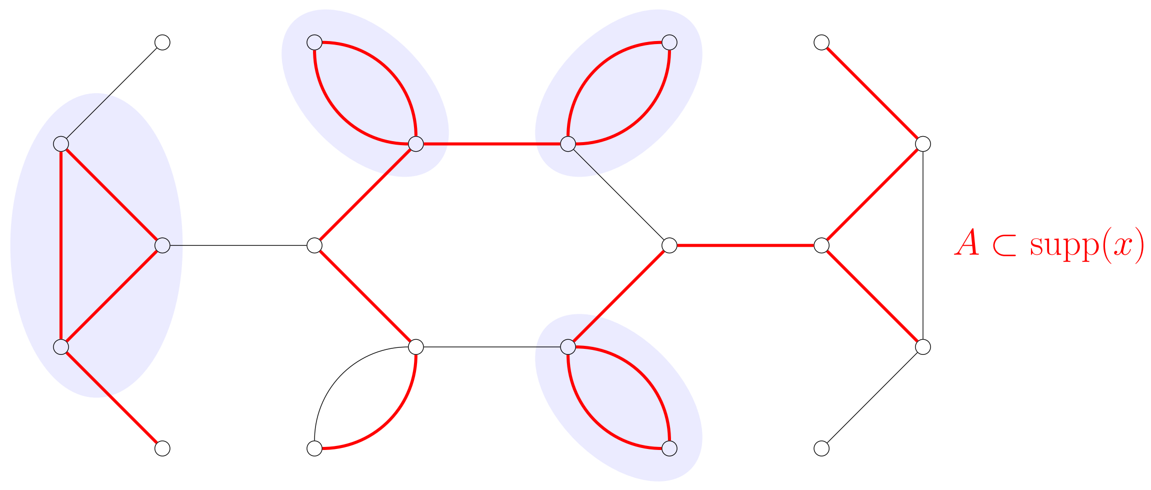
Proof. By Theorem 2.1, G is a disjoint union of cacti. By the previous corollary, Algorithm 2.1 is a c-balanced CR scheme for the graphic matroid of that graph with

$$c = 1 - \frac{1}{g}\left(1 - \frac{1}{g}\right)^{g-1}.$$

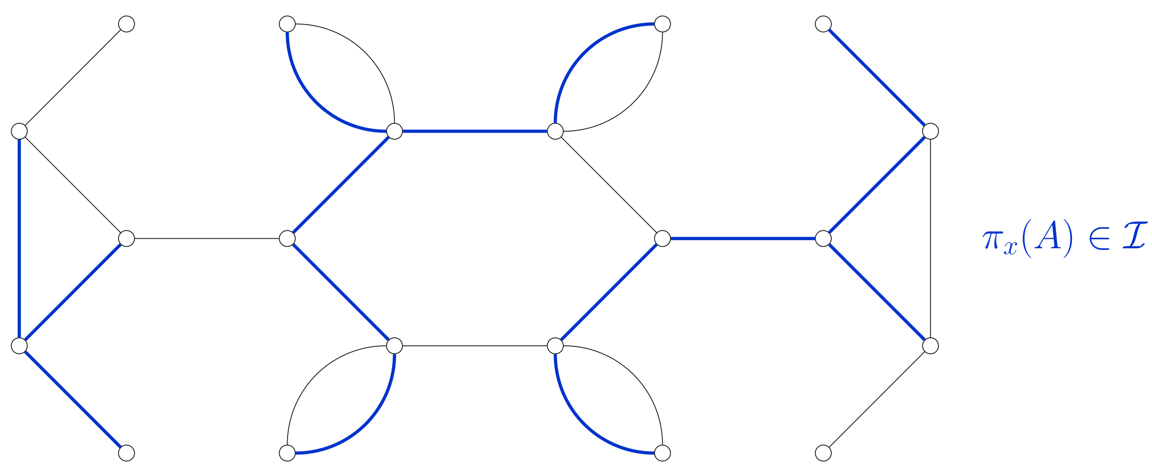
Since G is a simple graph, it cannot have any parallel edges, which means that $g \geq 3$. In particular,

$$c \geq 1 - \frac{1}{3}\left(1 - \frac{1}{3}\right)^{3-1} = 23/27.$$

□



(a) The input set $A \subset \text{supp}(x)$. The cycles that need to be broken by Algorithm 2.1 are shaded in blue.



(b) The output of Algorithm 2.1, which is independent (acyclic) set $\pi_x(A) \in \mathcal{I}$

.

Figure 6: An example run of Algorithm 2.1 applied to the graphic matroid of a cactus graph.

3 An optimal monotone contention resolution scheme for uniform matroids

We consider in this section the problem of designing an optimal CR scheme for any uniform matroid. To the best of our knowledge, this was only done so far for the uniform matroid of rank one (that we denote by U_n^1) in [7] and [8]. For a ground set of size n, a CR scheme with a balancedness of $1-(1-1/n)^n$ was given and it was shown in [5] that this was optimal, i.e. no c-balanced CR scheme for the uniform matroid of rank one can satisfy $c > 1-(1-1/n)^n$.

Our contribution is an optimal CR scheme for the uniform matroid of rank k on n elements (that we denote by U_n^k) which has a balancedness factor of $c(k,n) := 1 - \binom{n}{k}\left(1-\frac{k}{n}\right)^{n+1-k}\left(\frac{k}{n}\right)^k$. It is clear that this generalizes the previous result for the uniform matroid of rank 1 by setting $k=1$. Moreover, as mentioned before, this factor is optimal, thus no c-balanced CR scheme for U_n^k can satisfy $c > 1 - \binom{n}{k}\left(1-\frac{k}{n}\right)^{n+1-k}\left(\frac{k}{n}\right)^k$. For a fixed k, this satisfies $c(k,n) \xrightarrow{n\to\infty} 1 - e^{-k}k^k/k!$, which also generalizes the $(1-1/e)$ asymptotically optimal balancedness for the rank one case. In addition, even when considering the case $k=1$, our CR scheme is in a sense simpler than the one presented in [7] and [8], even though both CR schemes are $(1-(1-1/n)^n)$ -balanced, since we are in that case simply assigning a probability to each element of the input set and picking an element according to that probability distribution.

3.1 The CR scheme for U_n^k

Let us describe the framework for the uniform matroid $U_n^k = (N,\mathcal{I})$. We assume throughout this whole section that $n \geq 2$ and that $k \in \{1,\dots,n-1\}$.

- $N = \{1,\dots,n\}$ is the ground set.
- $\mathcal{I} = \{A \subset N \mid |A| \leq k\}$ are the independent sets.
- $P_{\mathcal{I}} = \{x \in \mathbb{R}^N_{\geq 0} \mid x(A) \leq r(A) \quad \forall A \subset N\} = \{x \in [0,1]^N \mid x_1 + \dots + x_n \leq k\}$ is the matroid polytope.

Let's now describe the CR scheme. For any point $x \in P_{\mathcal{I}}$, we let $R(x)$ be the random set satisfying $\mathbb{P}[i \in R(x)] = x_i$ independently for each coordinate. If the size of $R(x)$ is at most k, then $R(x)$ is already an independent set and the CR scheme returns that. If however $|R(x)| > k$, then the CR scheme returns a random subset of k elements by making the probabilities of each subset of k elements depend linearly on the x-coordinates of the original point $x \in P_{\mathcal{I}}$.

Let us define what these probabilities are. We first fix an arbitrary $x \in P_{\mathcal{I}}$. For any set $A \subset \text{supp}(x)$ with $|A| > k$ and any subset $B \subset A$ of size k, we define:

$$q_A(B) := \frac{1}{\binom{|A|}{|B|}}\Big(1 + \bar{x}(A\setminus B) - \bar{x}(B)\Big) \tag{3.1}$$

where we use the following convenient notation:

$$\bar{x}(A) := \frac{1}{|A|}x(A) = \frac{1}{|A|}\sum_{i\in A} x_i.$$

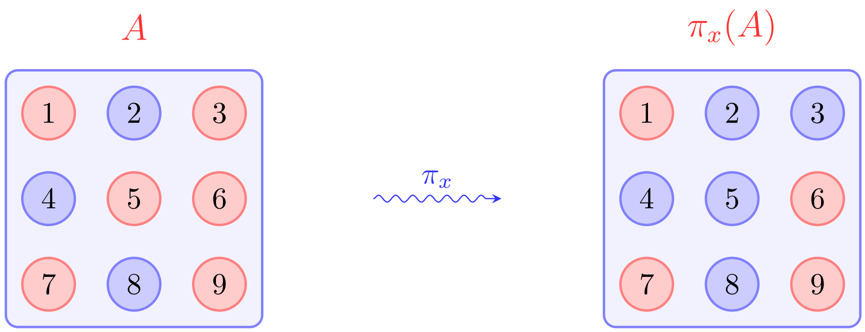


Figure 7: An example run of Algorithm 3.1 with $n = 9$ and $k = 4$

We are now ready to define the following randomized CR scheme π for U_n^k.

Algorithm 3.1 (CR scheme π for U_n^k)**.** We are given a point $x \in P_{\mathcal{I}}$ and a set $A \subset \text{supp}(x)$.

- If $|A| \leq k$, then $\pi_x(A) = A$
- If $|A| > k$, then for every $B \subset A$ with $|B| = k, \pi_x(A) = B$ with probability $q_A(B)$.

Let us first prove that this CR scheme is well-defined, i.e. q_A is a valid probability distribution.

Lemma 3.1. *The above procedure π is a well-defined CR scheme, i.e. $\forall x \in P_{\mathcal{I}}, A \subset \text{supp}(x)$*

$$q_A(B) \geq 0, \sum_{B \subset A, |B|=k} q_A(B) = 1.$$

Proof. Since $\bar{x}(A \setminus B) \in [0, 1]$ and $\bar{x}(B) \in [0, 1]$, it directly follows from the definition (3.1) that

$$q_A(B) \geq 0.$$

In order to prove the second claim, we will need the equality

$$\sum_{B \subset A, |B|=k} x(B) = \binom{|A| - 1}{k - 1} x(A) \tag{3.2}$$

that we derive the following way:

$$\begin{aligned} \sum_{B \subset A, |B|=k} x(B) &= \sum_{B \subset A, |B|=k} \sum_{i \in A} x_i \mathbf{1}_{\{i \in B\}} = \sum_{i \in A} x_i \sum_{B \subset A, |B|=k} \mathbf{1}_{\{i \in B\}} \\ &= \sum_{i \in A} x_i \, |\{B \subset A \mid |B| = k, i \in B\}| = \binom{|A| - 1}{k - 1} x(A). \end{aligned}$$

Hence,

$$\begin{aligned}
\sum_{B\subset A,|B|=k} q_A(B) &= \sum_{B\subset A,|B|=k} \frac{1}{\binom{|A|}{k}} \left(1 + \frac{x(A\setminus B)}{|A|-k} - \frac{x(B)}{k}\right) \\
&= 1 + \frac{1}{\binom{|A|}{k}} \sum_{B\subset A,|B|=k} \left(\frac{x(A)}{|A|-k} - \frac{x(B)}{|A|-k} - \frac{x(B)}{k}\right) \\
&= 1 + \frac{1}{\binom{|A|}{k}} \sum_{B\subset A,|B|=k} \left(\frac{x(A)}{|A|-k} - \frac{|A|\, x(B)}{k\,(|A|-k)}\right) \\
&= 1 + \frac{1}{\binom{|A|}{k}\left(|A|-k\right)} \sum_{B\subset A,|B|=k} \left(x(A) - \frac{|A|}{k} x(B)\right) \\
&= 1 + \frac{1}{\binom{|A|}{k}\left(|A|-k\right)} \left(\binom{|A|}{k} x(A) - \binom{|A|}{k} x(A)\right) = 1
\end{aligned}$$

□

Here is the main theorem of this section.

Theorem 3.1. *Algorithm 3.1 is a c-balanced CR scheme for the uniform matroid of rank k on n elements (denoted by U_n^k), where:*

$$c = 1 - \binom{n}{k} \left(1 - \frac{k}{n}\right)^{n+1-k} \left(\frac{k}{n}\right)^k.$$

Since we use the expression on the right hand side of the previous equation very often throughout this section, we denote it by:

$$c(k,n) := 1 - \binom{n}{k} \left(1 - \frac{k}{n}\right)^{n+1-k} \left(\frac{k}{n}\right)^k. \tag{3.3}$$

A few important remarks:

- for $k = 1$, we get $c(k,n) = 1 - (1 - 1/n)^n$, which indeed reproduces the optimal balancedness for U_n^1 provided in [7] and [8]. This converges to $1 - 1/e \approx 0.63$ when n gets large.
- for $k = n - 1$, we get $c(k,n) = 1 - \frac{1}{n}\left(1 - \frac{1}{n}\right)^{n-1}$. Notice that $U_n^{n-1} = \mathcal{M}_{C_n}$, where $\mathcal{M}_{C_n}$ is the graphic matroid of the cycle graph. The result from Section 2: "An optimal monotone CR scheme for matroids with pairwise disjoint circuits" coincides with the one here. This converges to 1 as n tends to infinity.
- An efficient CR scheme for an arbitrary matroid was provided in [5] with a balancedness of $1 - 1/e \approx 0.63$. In our case, $c(k,n) > 1 - 1/e$ for any k and n. This is illustrated in Table 2.

Proposition 3.1. *For a fixed k, the limit of $c(k,n)$ as n tends to infinity is*

$$\lim_{n\to\infty} c(k,n) = 1 - e^{-k}\, \frac{k^k}{k!}.$$

$n \setminus k$	1	2	3	4	9	99	999
2	0.75						
3	0.704	0.852					
4	0.684	0.813	0.895				
5	0.672	0.793	0.862	0.918			
10	0.651	0.759	0.813	0.850	0.961		
100	0.633	0.732	0.779	0.810	0.874	0.996	
1000	0.632	0.730	0.776	0.809	0.869	0.962	0.999

Table 2: Numerical values for the balancedness $c(k, n)$ of Theorem 3.1

Proof. We will need Stirling's approximation, which states that:

$$n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n \tag{3.4}$$

which means that these two quantities are asymptotic, i.e. their ratio tends to 1 if we tend n to infinity. By (3.4), we get

$$\frac{n!}{(n-k)!} \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n \frac{1}{\sqrt{2\pi(n-k)}} \left(\frac{e}{n-k}\right)^{n-k} = e^{-k} \frac{n^n}{(n-k)^{n-k}} \sqrt{\frac{n}{n-k}}. \tag{3.5}$$

Hence,

$$\begin{aligned} 1 - c(k, n) &= \binom{n}{k} \left(1 - \frac{k}{n}\right)^{n+1-k} \left(\frac{k}{n}\right)^k \\ &= \frac{k^k}{k!} \frac{n!}{(n-k)!} \frac{(n-k)^{n+1-k}}{n^{n+1}} \\ &\sim e^{-k} \frac{k^k}{k!} \frac{n-k}{n} \sqrt{\frac{n}{n-k}} \\ &= e^{-k} \frac{k^k}{k!} \sqrt{\frac{n-k}{n}} \\ &\sim e^{-k} \frac{k^k}{k!}, \end{aligned}$$

where we have used (3.5) from the second to the third line. □

3.2 Outline of the proof of Theorem 3.1

We give in this subsection an outline of the proof of Theorem 3.1. Throughout this whole section on uniform matroids, we fix an arbitrary $e \in N$. In order to prove Theorem 3.1, we need to show that for every $x \in P_{\mathcal{I}}$ with $x_e > 0$:

$$\mathbb{P}[e \in \pi_x(R(x)) \mid e \in R(x)] \geq c(k, n).$$

This is equivalent to showing that for every $x \in P_{\mathcal{I}}$ with $x_e > 0$:

$$\mathbb{P}[e \notin \pi_x(R(x)) \mid e \in R(x)] \leq 1 - c(k,n). \tag{3.6}$$

We now fix a few key definitions/notations.

Notation 1. For any $B \subset A \subset N$,

$$p_A(B) := \mathbb{P}[R_A(x) = B] = \prod_{i \in B} x_i \prod_{i \in A \setminus B} (1 - x_i).$$

where $R_A(x)$ is the random set obtained by rounding each coordinate of $x|_A$ in the reduced ground set A to one independently with probability x_i.

Remark. Of course, $p_N(B) = \mathbb{P}[R(x) = B]$. We do not write the dependence on $x \in P_{\mathcal{I}}$ for simplicity of notation.

Notation 2. We will mainly work on the set $N \setminus \{e\}$. For this reason, we define:

$$S := N \setminus \{e\}.$$

Of course, this means that $|S| = n - 1$, which is something that we will use very often. These two notations allow us to rewrite the probability in (3.6) in a more convenient form. Indeed, for any $x \in P_{\mathcal{I}}$ satisfying $x_e > 0$,

$$\begin{aligned}
\mathbb{P}\Big[e \notin \pi_x(R(x)) \mid e \in R(x)\Big] &= \sum_{A \subset S} \mathbb{P}[e \notin \pi_x(R(x)) \mid R_S(x) = A, e \in R(x)]\, \mathbb{P}[R_S(x) = A \mid e \in R(x)] \\
&= \sum_{A \subset S, |A| \geq k} \mathbb{P}\Big[e \notin \pi_x(R(x)) \mid R(x) = A \cup e\Big]\, p_S(A) \\
&= \sum_{A \subset S, |A| \geq k} p_S(A) \sum_{B \subset A, |B| = k} q_{A \cup e}(B).
\end{aligned}$$

The obtained expression is a multivariable function of the variables $x_1, \ldots, x_n$, since $p_S(A)$ and $q_{A\cup e}(B)$ depend on those variables as well. We give it the following notation.

Notation 3.

$$G(x) := \sum_{A \subset S, |A| \geq k} p_S(A) \sum_{B \subset A, |B| = k} q_{A \cup e}(B). \tag{3.7}$$

It turns out that for proving Theorem 3.1, it is enough to show the following.

Theorem 3.2. *Let $G(x)$ and $c(k,n)$ be as defined above. Then the following maximization problem satisfies*

$$\max_{x \in P_{\mathcal{I}}} G(x) = 1 - c(k,n)$$

and the maximum is attained at the point

$$(x_1, \ldots, x_n) = (k/n, \ldots, k/n) \in P_{\mathcal{I}}.$$

Proof that Theorem 3.2 implies Theorem 3.1. Indeed, Theorem 3.2 implies that for every $x \in P_{\mathcal{I}}$,

$$G(x) \leq 1 - c(k,n)$$

with equality holding if $x = (k/n, \dots, k/n)$. In particular, for any $x \in P_{\mathcal{I}}$ satisfying $x_e > 0$, we get:

$$G(x) = \mathbb{P}\Big[e \notin \pi_x(R(x)) \mid e \in R(x)\Big] \leq 1 - c(k,n),$$

which is what we needed to prove Theorem 3.1 by (3.6). □

Notice that for the conditional probability to be well defined, we need the assumption that $x_e > 0$. However, in our case, $G(x)$ is simply a multivariable function of the n variables $x_1, \dots, x_n$ and is thus also defined when $x_e = 0$. We may therefore forget the conditional probability and simply treat Theorem 3.2 as a multivariable maximization problem over a bounded domain. We now state the outline of the proof.

1. We first maximize $G(x)$ over the variable x_e. We then get an expression depending only on the x-variables in S. This is done in Section 3.3.
2. We then maximize the expression obtained in the first part over the unit hypercube $[0,1]^S$. This is done in Section 3.4.
3. Finally, we will combine the first two parts to show that the maximum in Theorem 3.2 is attained at the point $x_i = k/n$ for every $i \in N$. This is done in Section 3.5.

3.3 Maximizing over the variable x_e

The matroid polytope of U_n^k is

$$P_{\mathcal{I}} = \{x \in [0,1]^N \mid x(N) \leq k\}.$$

We define a new polytope by removing the constraint $x_e \leq 1$ from $P_{\mathcal{I}}$:

$$\widetilde{P}_{\mathcal{I}} := \{x \in \mathbb{R}^N_{\geq 0} \mid x(N) \leq k \text{ and } x_i \leq 1 \quad \forall i \in S\}. \tag{3.8}$$

Clearly, $P_{\mathcal{I}} \subset \widetilde{P}_{\mathcal{I}}$. Here is the main result of this subsection.

Lemma 3.2. *For every $x \in \widetilde{P}_{\mathcal{I}}$,*

$$G(x) \leq \sum_{A \subset S, |A| = k} p_S(A)\Big(1 - \bar{x}(A)\Big). \tag{3.9}$$

Moreover, equality holds when $x_e = k - x(S)$.

Remark. In other words, we consider the maximization problem $\max\{G(x) \mid x \in \widetilde{P}_{\mathcal{I}}\}$ and maximize $G(x)$ over the variable x_e while keeping all the other variables (x_i for every $i \in S$) fixed to get an expression depending only on the x-variables in S.

Proof.

$$\begin{aligned}
G(x) &= \sum_{A\subset S,|A|\geq k} p_S(A) \sum_{B\subset A,|B|=k} q_{A\cup e}(B) \\
&= \sum_{A\subset S,|A|\geq k} p_S(A) \sum_{B\subset A,|B|=k} \frac{1}{\binom{|A|+1}{k}} \Big(1+\,\bar{x}\Big((A\setminus B)\cup e\Big) - \bar{x}(B)\Big) \\
&= \sum_{A\subset S,|A|\geq k} p_S(A) \frac{1}{\binom{|A|+1}{k}} \sum_{B\subset A,|B|=k} \left(1+\,\frac{x(A\setminus B)+x_e}{|A|-k+1} - \frac{x(B)}{k}\right). \qquad (3.10)
\end{aligned}$$

We now maximize this expression with respect to the variable x_e over $\widetilde{P}_{\mathcal{I}}$ while keeping all the other variables fixed. Since this is a linear function of x_e and the coefficient of x_e is positive, the maximal value will be $x_e = k - x(S)$ in order to satisfy the constraint $x(N) \leq k$. Note that this was the reason for the definition of $\widetilde{P}_{\mathcal{I}}$, since $k - x(S)$ might not necessarily be smaller than 1. We thus plug-in $x_e = k - x(S)$ in (3.10) and write an inequality to emphasize that the derivation holds for any $x \in \widetilde{P}_{\mathcal{I}}$.

$$\begin{aligned}
(3.10) &\leq \sum_{A\subset S,|A|\geq k} p_S(A) \frac{1}{\binom{|A|+1}{k}} \sum_{B\subset A,|B|=k} \left(1+\,\frac{x(A\setminus B)+k-x(S)}{|A|-k+1} - \frac{x(B)}{k}\right) \\
&= \sum_{A\subset S,|A|\geq k} p_S(A) \frac{1}{\binom{|A|+1}{k}} \sum_{B\subset A,|B|=k} \left(1+\,\frac{k-x(S\setminus A)-x(B)}{|A|-k+1} - \frac{x(B)}{k}\right) \\
&= \sum_{A\subset S,|A|\geq k} p_S(A) \frac{1}{\binom{|A|+1}{k}} \sum_{B\subset A,|B|=k} \left(1+\frac{k}{|A|-k+1} - \frac{x(S\setminus A)}{|A|-k+1} - \left(\frac{1}{|A|-k+1}+\frac{1}{k}\right)x(B)\right) \\
&= \sum_{A\subset S,|A|\geq k} p_S(A) \frac{1}{\binom{|A|+1}{k}} \sum_{B\subset A,|B|=k} \left(\frac{|A|+1}{|A|-k+1} - \frac{x(S\setminus A)}{|A|-k+1} - \frac{|A|+1}{k(|A|-k+1)}x(B)\right). \qquad (3.11)
\end{aligned}$$

Notice the only part which depends on B in the last summation is $x(B)$. By using Equation (3.2) and noticing that $\sum_{B\subset A,|B|=k} 1 = \binom{|A|}{k}$, we get

$$\begin{aligned}
(3.11) &= \sum_{A\subset S,|A|\geq k} p_S(A) \frac{1}{\binom{|A|+1}{k}} \frac{1}{|A|-k+1} \left(\binom{|A|}{k}(|A|+1) - \binom{|A|}{k}x(S\setminus A) - \frac{|A|+1}{k}\binom{|A|-1}{k-1}x(A)\right) \\
&= \sum_{A\subset S,|A|\geq k} p_S(A) \frac{1}{\binom{|A|+1}{k}} \frac{1}{|A|-k+1} \binom{|A|}{k} \left(|A|+1-x(S\setminus A) - \frac{|A|+1}{|A|}x(A)\right) \\
&= \sum_{A\subset S,|A|\geq k} p_S(A)\, \frac{|A|-k+1}{|A|+1} \frac{1}{|A|-k+1} \left(|A|+1-x(S\setminus A) - \frac{|A|+1}{|A|}x(A)\right) \\
&= \sum_{A\subset S,|A|\geq k} \frac{p_S(A)}{|A|+1} \left(|A|+1-x(S\setminus A) - \frac{|A|+1}{|A|}x(A)\right) \\
&= \sum_{A\subset S,|A|\geq k} p_S(A) \left(1-\frac{x(S\setminus A)}{|A|+1} - \frac{x(A)}{|A|}\right). \qquad (3.12)
\end{aligned}$$

Now, note that by definition of the term $p_S(A)$, we have

$$x_i\, p_S(A) = (1 - x_i)\, p_S(A \cup i) \quad \text{for any } i \in S \setminus A. \tag{3.13}$$

We compute the middle term in (3.12) by plugging in (3.13) and the change of variable $B := A \cup i$.

$$\begin{aligned}
\sum_{A \subset S, |A| \geq k} \frac{1}{|A|+1} p_S(A)\, x(S \setminus A) &= \sum_{A \subset S, |A| \geq k} \sum_{i \in S} \frac{1}{|A|+1}\, x_i\, p_S(A)\, \mathbf{1}_{\{i \notin A\}} \\
&= \sum_{i \in S} \sum_{A \subset S, |A| \geq k} \frac{1}{|A|+1}\, (1 - x_i)\, p_S(A \cup i)\, \mathbf{1}_{\{i \notin A\}} \\
&= \sum_{i \in S} \sum_{B \subset S, |B| \geq k+1} \frac{1}{|B|}\, (1 - x_i)\, p_S(B)\, \mathbf{1}_{\{i \in B\}} \\
&= \sum_{B \subset S, |B| \geq k+1} \frac{1}{|B|}\, p_S(B) \sum_{i \in S} \mathbf{1}_{\{i \in B\}} - \sum_{B \subset S, |B| \geq k+1} \frac{1}{|B|}\, p_S(B) \sum_{i \in S} x_i \mathbf{1}_{\{i \in B\}} \\
&= \sum_{B \subset S, |B| \geq k+1} p_S(B) - \sum_{B \subset S, |B| \geq k+1} \frac{p_S(B)}{|B|}\, x(B) \\
&= \sum_{B \subset S, |B| \geq k+1} p_S(B) \left(1 - \frac{x(B)}{|B|}\right) \\
&= \sum_{A \subset S, |A| \geq k+1} p_S(A) \left(1 - \frac{x(A)}{|A|}\right).
\end{aligned} \tag{3.14}$$

We finally plug-in (3.14) into (3.12) and use $\sum_{A \subset S, |A| \geq k} = \sum_{A \subset S, |A| \geq k+1} + \sum_{A \subset S, |A| = k}$ to get

$$(3.12) = \sum_{A \subset S, |A| = k} p_S(A) \left(1 - \frac{x(A)}{|A|}\right) = \sum_{A \subset S, |A| = k} p_S(A) \Big(1 - \bar{x}(A)\Big).$$

Notice that the only place where we used an inequality was from (3.10) to (3.11). Hence equality holds when $x_e = k - x(S)$. $\square$

3.4 Maximizing $h_S^k : [0,1]^S \mapsto \mathbb{R}$

We now turn our attention in this section into maximizing the right-hand side expression in Lemma 3.2 over the unit hypercube $[0,1]^S$:

$$\sum_{\substack{A \subset S \\ |A| = k}} p_S(A)(1 - \bar{x}(A)). \tag{3.15}$$

It turns out it is more convenient to work with the following function.

$$h_S^k(x) := \sum_{\substack{A \subset S \\ |A| = k}} p_S(A)(k - x(A)). \tag{3.16}$$

Expression (3.16) is simply expression (3.15) multiplied by k. Hence, maximizing one or the other is equivalent: the optimal solution will be the same, whereas the optimal function value will be multiplied by a factor of k.

Let us give a few reminders to make this subsection self-complete.

- We assume that $n \geq 2$ and $k \in \{1, \ldots, n-1\}$.
- $S := N \backslash \{e\}$ is the set we obtain by removing the fixed element $e \in N$ from the original ground set $N = \{1, \ldots, n\}$. We may without loss of generality assume here that $S = \{1, \ldots, n-1\}$.
- $p_S(A) := \prod_{i \in A} x_i \prod_{i \in S \backslash A}(1 - x_i)$ for every $A \subset S$. This quantity implicitly depends on the point $x \in [0,1]^S$.
- $c(k,n) := 1 - \binom{n}{k} \left(1 - \frac{k}{n}\right)^{n+1-k} \left(\frac{k}{n}\right)^k$ is the balancedness we are trying to show for the CR scheme described in Algorithm 3.1.

Theorem 3.3. *Let $n \geq 2$ and $k \in \{1, \ldots, n-1\}$. In particular, $|S| = n - 1 \geq 1$. Then,*

$$h_S^k(x) = \sum_{\substack{A \subset S \\ |A| = k}} p_S(A)(k - x(A)) \tag{3.17}$$

attains its maximum over the unit hypercube $[0,1]^S$ at the point $(k/n, \ldots, k/n)$ with value

$$h_S^k\Big(k/n, \ldots, k/n\Big) = k \binom{n}{k} \left(1 - \frac{k}{n}\right)^{n+1-k} \left(\frac{k}{n}\right)^k = k\Big(1 - c(k,n)\Big). \tag{3.18}$$

For simplicity, we denote this maximum by:

$$\alpha(k,n) := k \binom{n}{k} \left(1 - \frac{k}{n}\right)^{n+1-k} \left(\frac{k}{n}\right)^k. \tag{3.19}$$

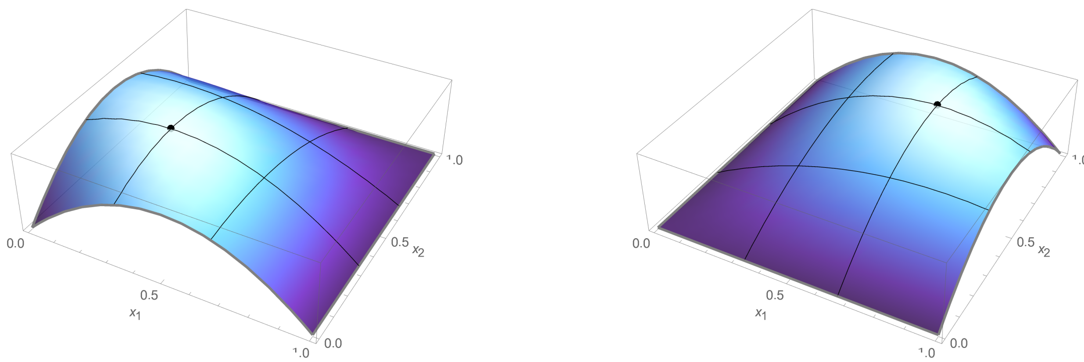
Notice that $h_S^0(x) = h_S^n(x) = 0$ for any $x \in [0,1]^S$. The theorem thus holds for $k = 0$ and $k = n$ as well. Moreover, the function $h_S^k(x)$ also satisfies an interesting duality property: $h_S^k(x) = h_S^{n-k}(1 - x)$.

Let us state the outline of the proof of Theorem 3.3.

1. We first prove a proposition stating that this function has a unique local maximum in the interior of $[0,1]^S$ at the point $(k/n, \ldots, k/n)$.
2. We then show by induction on n that any point in the boundary of $[0,1]^S$ has a lower function value than $h_S^k(k/n, \ldots, k/n)$.

Proposition 3.2. *For any $k \in \{1, \ldots, n-1\}, h_S^k(x)$ has a unique extremum in the interior of the unit hypercube $[0,1]^S$ at the point $(k/n, \ldots, k/n)$. Moreover, that point is a local maximum.*

We need the following lemma in order to prove Proposition 3.2.



(a) $S = \{1, 2\}, k = 1$ (b) $S = \{1, 2\}, k = 2$

Figure 8: Plot of $h^k_S(x)$ for $S = \{1, 2\}$. The maximum is attained at $x_1 = x_2 = 1/3$ in (a) and at $x_1 = x_2 = 2/3$ in (b).

Lemma 3.3. *The following holds for any* $x \in [0, 1]^S$*:*

$$h^k_S(x) = \sum_{i=0}^{k-1} Q^i_S(x) \big(x(S) - i\big) \tag{3.20}$$

where

$$Q^k_S(x) := \sum_{A \subset S, |A|=k} p_S(A). \tag{3.21}$$

Remark. This formula actually holds for h^k_A for any $A \subset N$ and we will use it again in Section 3.6 for $A = N$.

Proof of Lemma 3.3. Notice that for $i \in A$, $p_S(A)\,(1 - x_i) = p_S(A \setminus i)\, x_i$. Then

$$\begin{aligned}
h^k_S(x) &= \sum_{\substack{A \subset S \\ |A|=k}} p_S(A) \sum_{i \in A} (1 - x_i) = \sum_{\substack{A \subset S \\ |A|=k}} \sum_{i \in S} p_S(A)(1 - x_i)\mathbf{1}_{\{i \in A\}} \\
&= \sum_{i \in S} \sum_{\substack{A \subset S \\ |A|=k}} x_i\, p_S(A \setminus i)\, \mathbf{1}_{\{i \in A\}} = \sum_{i \in S} \sum_{\substack{B \subset S \setminus i \\ |B|=k-1}} x_i\, p_S(B) \\
&= \sum_{i \in S} x_i \sum_{\substack{A \subset S \setminus i \\ |A|=k-1}} p_S(A) = \sum_{i \in S} x_i \left(\sum_{\substack{A \subset S \\ |A|=k-1}} p_S(A) - \sum_{\substack{A \subset S \\ |A|=k-1}} p_S(A)\mathbf{1}_{\{i \in A\}} \right) \\
&= x(S) Q^{k-1}_S(x) - \sum_{\substack{A \subset S \\ |A|=k-1}} p_S(A) x(A).
\end{aligned} \tag{3.22}$$

Notice that by definition of $h_S^k(x)$ we have

$$
\begin{aligned}
h_S^{k-1}(x) &= \sum_{\substack{A\subset S\\|A|=k-1}} p_S(A)(k-1-x(A)) = (k-1)\sum_{\substack{A\subset S\\|A|=k-1}} p_S(A) - \sum_{\substack{A\subset S\\|A|=k-1}} p_S(A)x(A)\\
&= (k-1)\,Q_S^{k-1}(x) - \sum_{\substack{A\subset S\\|A|=k-1}} p_S(A)x(A).
\end{aligned}
\tag{3.23}
$$

Substracting (3.23) from (3.22) we get

$$
h_S^k(x) - h_S^{k-1}(x) = Q_S^{k-1}(x)\Big(x(S)-(k-1)\Big). \tag{3.24}
$$

We can rewrite this recursive formula as

$$
h_S^{i+1}(x) - h_S^{i}(x) = Q_S^{i}(x)\Big(x(S)-i\Big). \tag{3.25}
$$

By summing both sides from 0 to $k-1$ and noticing that $h_S^0(x)=0$, we get the desired result. □

We are now able to prove Proposition 3.2.

Proof of Proposition 3.2. Let $k \in \{1,\dots,n-1\}$. To find the extrema of $h_S^k : [0,1]^S \mapsto \mathbb{R}$, we want to solve $\nabla h_S^k(x) = 0$. We thus first need to find

$$
\frac{\partial h_S^k(x)}{\partial x_i} \quad \text{for every } i \in S. \tag{3.26}
$$

Notice that:

- For a set $A \subset S$ such that $i \in A$,

$$
\begin{aligned}
\frac{\partial}{\partial x_i} p_S(A)(k-x(A)) &= (k-x(A))\prod_{j\in A\setminus i} x_j \prod_{j\in S\setminus A}(1-x_j) - p_S(A)\\
&= (k-x(A))\prod_{j\in A\setminus i} x_j \prod_{j\in S\setminus A}(1-x_j) - x_i\prod_{j\in A\setminus i} x_j \prod_{j\in S\setminus A}(1-x_j)\\
&= (k-x(A))\,p_{S\setminus i}(A\setminus i) - x_i\,p_{S\setminus i}(A\setminus i)\\
&= p_{S\setminus i}(A\setminus i)\Big(k - x(A\setminus i) - 2x_i\Big).
\end{aligned}
\tag{3.27}
$$

- For a set $A \subset S$ such that $i \notin A$,

$$
\begin{aligned}
\frac{\partial}{\partial x_i} p_S(A)(k-x(A)) &= -(k-x(A))\prod_{j\in A} x_j \prod_{j\in (S\setminus A)\setminus i}(1-x_j)\\
&= -p_{S\setminus i}(A)\Big(k-x(A)\Big).
\end{aligned}
\tag{3.28}
$$

We are now able to compute (3.26):

$$
\begin{aligned}
\frac{\partial h_S^k(x)}{\partial x_i} &= \frac{\partial}{\partial x_i} \sum_{\substack{A\subset S\\|A|=k}} p_S(A)(k - x(A)) \\
&= \sum_{\substack{A\subset S\\|A|=k\\i\in A}} \frac{\partial}{\partial x_i} p_S(A)(k - x(A)) + \sum_{\substack{A\subset S\\|A|=k\\i\notin A}} \frac{\partial}{\partial x_i} p_S(A)(k - x(A)) \\
&= \sum_{\substack{A\subset S\\|A|=k\\i\in A}} p_{S\setminus i}(A\setminus i)\Big(k - x(A\setminus i) - 2x_i\Big) - \sum_{\substack{A\subset S\\|A|=k\\i\notin A}} p_{S\setminus i}(A)\Big(k - x(A)\Big) \\
&= \sum_{\substack{B\subset S\setminus i\\|B|=k-1}} p_{S\setminus i}(B)\Big(k - x(B) - 2x_i\Big) - \sum_{\substack{A\subset S\setminus i\\|A|=k}} p_{S\setminus i}(A)\Big(k - x(A)\Big) \\
&= \sum_{\substack{A\subset S\setminus i\\|A|=k-1}} p_{S\setminus i}(A)\Big(k - 1 - x(A) + 1 - 2x_i\Big) - h_{S\setminus i}^k(x) \\
&= \sum_{\substack{A\subset S\setminus i\\|A|=k-1}} p_{S\setminus i}(A)\Big(k - 1 - x(A)\Big) + (1-2x_i) \sum_{\substack{A\subset S\setminus i\\|A|=k-1}} p_{S\setminus i}(A) - h_{S\setminus i}^k(x) \\
&= (1-2x_i) Q_{S\setminus i}^{k-1}(x) - \Big(h_{S\setminus i}^k(x) - h_{S\setminus i}^{k-1}(x)\Big) \\
&= (1-2x_i) Q_{S\setminus i}^{k-1}(x) - Q_{S\setminus i}^{k-1}(x)\Big(x(S\setminus i) - (k-1)\Big) \\
&= Q_{S\setminus i}^{k-1}(x)\Big(k - x(S) - x_i\Big) \qquad (3.29)
\end{aligned}
$$

where we use (3.25) (or equivalently Lemma 3.3) in the second to last line.

We now set

$$\nabla h_S^k(x) = 0.$$

By (3.29), this is equivalent to

$$Q_{S\setminus i}^{k-1}(x)\Big(k - x(S) - x_i\Big) = 0 \quad \forall i \in S. \qquad (3.30)$$

Notice that

$$
\begin{aligned}
Q_{S\setminus i}^{k-1}(x) = 0 \iff \sum_{\substack{A\subset S\setminus i\\|A|=k-1}} p_{S\setminus i}(A) = 0 &\iff p_{S\setminus i}(A) = 0 \quad \forall A \subset S\setminus i, |A| = k-1 \\
&\iff \prod_{j\in A} x_j \prod_{j\in (S\setminus i)\setminus A} (1-x_j) = 0 \quad \forall A \subset S, |A| = k-1.
\end{aligned}
$$

We can see this implies that such a solution lies on the boundary of $[0,1]^S$, since there exists an index $j \in S$ such that $x_j = 0$ or $x_j = 1$. Since we are focusing on extrema in the interior, we may disregard that solution. Hence, by (3.30),

$$x_i = k - x(S) \quad \forall i \in S.$$

By setting $x_i = t$ for every $i \in S$, we get

$$t = k - (n-1)t \iff t = k/n \iff x_i = k/n \quad \forall i \in S.$$

Therefore, $h_S^k(x)$ has a unique extremum in the interior of $[0,1]^S$ at the point $(k/n, \ldots, k/n)$.

It is left to prove that this point is a local maximum. We do that by computing the Hessian matrix $H(x)$ and showing that $H(k/n, \ldots, k/n)$ is negative definite. Note that $H(x)$ is a $(n-1) \times (n-1)$ matrix defined by:

$$H(x)_{i,j} = \frac{\partial^2 h_S^k(x)}{\partial x_i \partial x_j}.$$

By Lemma A.1 and Lemma A.2, which can be found in the Appendix, we are able to compute the Hessian:

$$\frac{\partial^2 h_S^k}{\partial x_i^2}(k/n, \ldots, k/n) = -2\binom{n-2}{k-1}\left(\frac{k}{n}\right)^{k-1}\left(\frac{n-k}{n}\right)^{n-k-1} \qquad \forall i \in S \tag{3.31}$$

and

$$\frac{\partial^2 h_S^k}{\partial x_i \partial x_j}(k/n, \ldots, k/n) = -\binom{n-2}{k-1}\left(\frac{k}{n}\right)^{k-1}\left(\frac{n-k}{n}\right)^{n-k-1} \qquad \text{for } i \neq j \tag{3.32}$$

Therefore,

$$H(k/n, \ldots, k/n) = -c\begin{pmatrix} 2 & 1 & 1 & \ldots & 1 \\ 1 & 2 & 1 & \ldots & 1 \\ \vdots & & & & \vdots \\ 1 & 1 & 1 & \ldots & 2 \end{pmatrix} =: -c\, A \tag{3.33}$$

where

$$c := \binom{n-2}{k-1}\left(\frac{k}{n}\right)^{k-1}\left(\frac{n-k}{n}\right)^{n-k-1} > 0.$$

Our goal is to show that $H(k/n, \ldots, k/n) \in \mathbb{R}^{(n-1)\times(n-1)}$ is negative-definite. Notice that λ is an eigenvalue of $H(k/n, \ldots, k/n)$ with corresponding eigenvector $v \in \mathbb{R}^{n-1}$ if and only if $-\lambda/c$ is an eigenvalue of A with the same eigenvector $v \in \mathbb{R}^{n-1}$. It is thus enough to show that A is positive-definite, i.e. all the eigenvalues of A are positive.

Notice that $A = I_{n-1} + J_{n-1}$, where I_{n-1} and J_{n-1} are respectively the identity matrix and the all-ones matrix of size $(n-1) \times (n-1)$. In particular, we may rewrite this as

$$A = I_{n-1} + e\, e^T \tag{3.34}$$

where $e \in \mathbb{R}^{n-1}$ is the all-ones vector.

Let μ be an eigenvalue of A with corresponding eigenvector v. Then

$$\begin{aligned} Av = \mu v &\iff v + (e^T v)e = \mu v \\ &\iff (e^T v)e = (\mu - 1)v. \end{aligned}$$

- If $\mu = 1$, the corresponding eigenspace is $\{v \in \mathbb{R}^{n-1} \mid e^T v = 0\}$. This eigenspace is a hyperplane of dimension $n-2$, which means that there exists $n-2$ linearly independent eigenvectors corresponding to the eigenvalue $\mu = 1$.
- If $\mu \neq 1$, then we see that e and v are collinear, which means that e is an eigenvector corresponding to μ. We compute the value of μ:

$$Ae = \mu e \iff e + (e^T e)e = \mu e \iff e + (n-1)e = \mu e \iff \mu = n.$$

Hence, the spectrum of A is equal to $\{1, n\}$, where the multiplicity of the eigenvalue 1 is $n-2$, whereas the multiplicity of the eigenvalue n is 1. We have therefore just proven that A is positive-definite, which, by (3.33), implies that $H(k/n, \ldots, k/n)$ is negative-definite and concludes the proof. □

We need one more lemma before being able to prove Theorem 3.3. Recall that

$$\alpha(k,n) = k \binom{n}{k} \left(1 - \frac{k}{n}\right)^{n+1-k} \left(\frac{k}{n}\right)^k.$$

Lemma 3.4. *The following holds for any $n \geq 2$ and $k \in \{1, \ldots, n-1\}$:*

$$\alpha(k,n) > \alpha(k-1, n-1) \tag{3.35}$$
$$\alpha(k,n) > \alpha(k, n-1) \tag{3.36}$$

Proof of Lemma 3.4. First, notice that the function $g(x) := \left(\frac{x-1}{x}\right)^x$ is strictly increasing for $x \geq 1$. Indeed, by using the strict inequality $\log(1+x) < x$ for any $x > 0$, we see that the derivative of $\log(g(x))$ is strictly positive:

$$\begin{aligned}\frac{d}{dx}\log(g(x)) &= \frac{d}{dx} x \log\left(\frac{x-1}{x}\right) = \log\left(\frac{x-1}{x}\right) + x \frac{x}{x-1}\frac{1}{x^2} = \log\left(\frac{x-1}{x}\right) + \frac{1}{x-1} \\ &= \frac{1}{x-1} - \log\left(\frac{x}{x-1}\right) = \frac{1}{x-1} - \log\left(1 + \frac{1}{x-1}\right) > 0.\end{aligned}$$

We first prove (3.35). If $k = 1$, then $\alpha(k-1, n-1) = 0$ and the statement clearly holds. We may thus assume $k > 1$. Then,

$$\begin{aligned}\frac{\alpha(k,n)}{\alpha(k-1,n-1)} &= \frac{k}{k-1} \frac{\binom{n}{k}}{\binom{n-1}{k-1}} \left(\frac{n-k}{n}\right)^{n+1-k} \left(\frac{k}{n}\right)^k \left(\frac{n-1}{n-k}\right)^{n+1-k} \left(\frac{n-1}{k-1}\right)^{k-1} \\ &= \frac{k}{k-1} \frac{n}{k} \frac{k^k (n-1)^n}{n^{n+1}(k-1)^{k-1}} \\ &= \left(\frac{n-1}{n}\right)^n \left(\frac{k}{k-1}\right)^k \\ &= \frac{g(n)}{g(k)} > 1.\end{aligned}$$

We now prove (3.36). If $k = n-1$, then $\alpha(k, n-1) = 0$ and the statement clearly holds. We may thus assume $k < n-1$. Then,

$$\begin{aligned}
\frac{\alpha(k,n)}{\alpha(k,n-1)} &= \frac{\binom{n}{k}}{\binom{n-1}{k}} \left(\frac{n-k}{n}\right)^{n+1-k} \left(\frac{k}{n}\right)^{k} \left(\frac{n-1}{n-1-k}\right)^{n-k} \left(\frac{n-1}{k}\right)^{k} \\
&= \frac{n}{n-k} \frac{(n-k)^{n+1-k}}{n^{n+1}} \frac{(n-1)^{n}}{(n-1-k)^{n-k}} \\
&= \left(\frac{n-1}{n}\right)^{n} \left(\frac{n-k}{n-k-1}\right)^{n-k} \\
&= \frac{g(n)}{g(n-k)} > 1.
\end{aligned}$$

□

We are now ready to prove Theorem 3.3.

Proof of Theorem 3.3. We prove the statement by induction on $n \geq 2$. The base case corresponds to $n = 2$ and $k = 1$. In this case, we get $S = \{1\}$ and

$$h_S^k(x) = x_1(1 - x_1).$$

It is easy to see that this is a parabola which attains its maximum at the point $x_1 = 1/2$ over the unit interval $[0, 1]$. Moreover the function value at that point is $1/4 = \alpha(1, 2)$.

We now prove the induction step. Let $n \geq 3$ and $k \in \{1, \ldots, n-1\}$, and assume by induction hypothesis that the statement holds for any $2 \leq n' < n$ and $k \in \{1, 2, \ldots, n'-1\}$.

By Proposition 3.2, $h_S^k(x)$ has a unique extremum (in particular a local maximum) in the interior of $[0, 1]^S$ at the point $(k/n, \ldots, k/n)$. We first show that the function $h_S^k(x)$ evaluated at that point is indeed equal to $\alpha(k, n)$.

$$\begin{aligned}
h_S^k(k/n, \ldots, k/n) &= \binom{n-1}{k} \left(\frac{k}{n}\right)^{k} \left(1 - \frac{k}{n}\right)^{n-1-k} \left(k - k\frac{k}{n}\right) \\
&= k\binom{n-1}{k} \left(\frac{k}{n}\right)^{k} \left(1 - \frac{k}{n}\right)^{n-k} \\
&= k\frac{n-k}{n}\binom{n}{k} \left(\frac{k}{n}\right)^{k} \left(1 - \frac{k}{n}\right)^{n-k} \\
&= \alpha(k, n).
\end{aligned} \tag{3.37}$$

The only thing left to prove is that any point on the boundary of $[0, 1]^S$ has a lower function value than $\alpha(k, n)$. A point $x \in [0, 1]^S$ lies on the boundary if there exists $i \in S$ such that $x_i = 0$ or $x_i = 1$.

- Suppose there exists $i \in S$ such that $x_i = 0$. For any set $A \subset S$ containing i, we get $p_S(A) = 0$. Hence:

  $$h_S^k(x) = \sum_{A \subset S, |A| = k} p_S(A)(k - x(A)) = \sum_{A \subset S \setminus i, |A| = k} p_{S \setminus i}(A)(k - x(A)) = h_{S \setminus i}^k(x).$$

  If $k = n - 1$, then $h_{S \setminus i}^k(x) = 0$. We then clearly get $h_S^k(x) = h_{S \setminus i}^k(x) = 0 < \alpha(k, n)$.

  If $k < n - 1$, then by induction hypothesis and Lemma 3.4,

  $$h_S^k(x) = h_{S \setminus i}^k(x) \leq \alpha(k, n-1) < \alpha(k, n).$$

- Suppose there exists $i \in S$ such that $x_i = 1$. For any set $A \subset S$ not containing i, we get $p_S(A) = 0$. Hence:

$$
\begin{aligned}
h_S^k(x) &= \sum_{A \subset S, |A|=k} p_S(A)(k - x(A)) = \sum_{\substack{A \subset S \\ |A|=k \\ i \in A}} p_S(A)(k - x(A)) \\
&= \sum_{\substack{A \subset S \\ |A|=k \\ i \in A}} p_{S\setminus i}(A \setminus i)(k - 1 - x(A \setminus i)) = \sum_{\substack{A \subset S\setminus i \\ |A|=k-1}} p_{S\setminus i}(A)(k - 1 - x(A)) \\
&= h_{S\setminus i}^{k-1}(x).
\end{aligned}
$$

If $k = 1$, then $h_{S\setminus i}^{k-1}(x) = 0$. We then clearly get $h_S^k(x) = h_{S\setminus i}^{k-1}(x) = 0 < \alpha(k, n)$.

If $k > 1$, then by induction hypothesis and Lemma 3.4,

$$h_S^k(x) = h_{S\setminus i}^{k-1}(x) \leq \alpha(k-1, n-1) < \alpha(k, n).$$

□

3.5 Proof of Theorem 3.1

We now have all the pieces in order to prove Theorem 3.2 and, therefore, Theorem 3.1. Indeed, the two main building blocks for this proof are Lemma 3.2 and Theorem 3.3. Let us restate the main theorems for convenience.

Theorem (Theorem 3.1)**.** *Algorithm 3.1 is a c-balanced CR scheme for the uniform matroid of rank k on n elements (denoted by U_n^k), where:*

$$c = 1 - \binom{n}{k} \left(1 - \frac{k}{n}\right)^{n+1-k} \left(\frac{k}{n}\right)^k =: c(k, n). \tag{3.38}$$

We have already argued in Section 3.2 that proving Theorem 3.2 would imply Theorem 3.1.

Theorem (Theorem 3.2)**.** *The following maximization problem satisfies*

$$\max_{x \in P_{\mathcal{I}}} G(x) = \binom{n}{k} \left(1 - \frac{k}{n}\right)^{n+1-k} \left(\frac{k}{n}\right)^k = 1 - c(k, n) \tag{3.39}$$

and the maximum is attained at the point

$$(x_1, \ldots, x_n) = (k/n, \ldots, k/n) \in P_{\mathcal{I}}.$$

Proof of Theorem 3.2. By Lemma 3.2, we get that for any $x \in P_{\mathcal{I}}$ (since $P_{\mathcal{I}} \subset \widetilde{P}_{\mathcal{I}}$),

$$G(x) \leq \sum_{\substack{A \subset S \\ |A|=k}} p_S(A)(1 - \bar{x}(A)). \tag{3.40}$$

Moreover, for every $x \in P_{\mathcal{I}}$ satisfying $x_e = k - x(S)$, equality holds in (3.40).

By Theorem 3.3, we get that for any $x \in P_{\mathcal{I}}$,

$$\sum_{\substack{A \subset S \\ |A|=k}} p_S(A)(1 - \bar{x}(A)) \leq 1 - c(k,n). \tag{3.41}$$

Equality holds in (3.41) if $x_i = k/n$ for every $i \in S$. This holds because the above expression does not depend on x_e, and the projection of the polytope $P_{\mathcal{I}}$ to the S coordinates is included in the unit hypercube $[0,1]^S$.

Therefore, by combining (3.40) and (3.41), we get that for every $x \in P_{\mathcal{I}}$:

$$G(x) \leq 1 - c(k,n).$$

Moreover, for the point $x_i = k/n$ for every $i \in N$, equality holds:

$$G(k/n, \ldots, k/n) = 1 - c(k,n).$$

Indeed, (3.40) holds with equality because $x_e = k - x(S)$ is satisfied (since $k - x(S) = k - (n-1)k/n = k/n$) and (3.41) also holds with equality because $x_i = k/n$ for every $i \in S$. ☐

3.6 Optimality

We prove in this section that Algorithm 3.1 is actually *optimal* for U_n^k.

Theorem 3.4. *There does not exist a c-balanced CR scheme for the uniform matroid of rank k on n elements (denoted by U_n^k) satisfying:*

$$c > 1 - \binom{n}{k} \left(1 - \frac{k}{n}\right)^{n+1-k} \left(\frac{k}{n}\right)^k.$$

The proof uses a similar argument to the one used for U_n^1 in [5]. It relies on computing the value $\mathbb{E}\big[r(R(x))\big]$, i.e. the expected rank of the random set $R(x)$. However, for general values of $k > 1$, the argument becomes more involved than the one presented in [5] for U_n^1. The proof we present surprisingly uses Lemma 3.3.

Corollary (of Lemma 3.3)**.** *Let $x \in P_{\mathcal{I}}$ be the point $x_i = k/n \quad \forall i \in N$. Then,*

$$h_N^k(x) = \sum_{i=0}^{k-1} Q_N^i(x)(k-i). \tag{3.42}$$

Proof of Theorem 3.4. We let π be an arbitrary c-balanced CR scheme for U_n^k, and we fix the point

$$x_i = \frac{k}{n} \quad \text{for every } i \in N.$$

Clearly, $x \in P_{\mathcal{I}} = \{x \in [0,1]^N \mid x_1 + \cdots + x_n \leq k\}$. We let $R(x)$ be the random set satisfying $\mathbb{P}[i \in R(x)] = x_i$ for each i independently, and denote by $I := \pi_x(R(x))$ the set returned by the CR scheme π. By definition of a CR scheme,

$$\mathbb{E}[|I|] \leq \mathbb{E}\big[r(R(x))\big]$$

and

$$\mathbb{E}[|I|] = \sum_{i \in N} \mathbb{P}[i \in I] \geq \sum_{i \in N} c\, x_i = \frac{nck}{n} = ck.$$

We therefore get the following upper bound for c:

$$c \leq \frac{\mathbb{E}\big[r(R(x))\big]}{k}. \tag{3.43}$$

Moreover, recall that

$$\mathbb{P}[|R(x)| = i] = \sum_{\substack{A \subset N \\ |A| = i}} p_N(A) = Q_N^i(x). \tag{3.44}$$

Using (3.42) and (3.44), we get

$$\begin{aligned}
\mathbb{E}[r(R(x))] &= \sum_{i=0}^{k} i\, \mathbb{P}[r(R(x)) = i] = \sum_{i=0}^{k-1} i\, \mathbb{P}\big[|R(x)| = i\big] + k\, \mathbb{P}\big[|R(x)| \geq k\big] \\
&= \sum_{i=0}^{k-1} i\, \mathbb{P}\big[|R(x)| = i\big] + k\, \Big(1 - \mathbb{P}\big[|R(x)| \leq k-1\big]\Big) \\
&= k + \sum_{i=0}^{k-1} i\, \mathbb{P}\big[|R(x)| = i\big] - k \sum_{i=0}^{k-1} \mathbb{P}\big[|R(x)| = i\big] \\
&= k - \sum_{i=0}^{k-1} (k-i) Q_N^i(x) && \text{by (3.44)} \\
&= k - h_N^k(x) && \text{by (3.42)} \\
&= k - \sum_{A \subset N, |A| = k} p_N(A)(k - x(A)) \\
&= k - \sum_{A \subset N, |A| = k} \left(\frac{k}{n}\right)^k \left(1 - \frac{k}{n}\right)^{n-k} \left(k - k\frac{k}{n}\right) \\
&= k \left(1 - \binom{n}{k} \left(1 - \frac{k}{n}\right)^{n+1-k} \left(\frac{k}{n}\right)^k\right).
\end{aligned}$$

Plugging the obtained formula into (3.43) leads to the desired result: an arbitrary c-balanced CR scheme for U_n^k has to satisfy

$$c \leq 1 - \binom{n}{k} \left(1 - \frac{k}{n}\right)^{n+1-k} \left(\frac{k}{n}\right)^k.$$

□

3.7 Monotonicity

We prove in this subsection that Algorithm 3.1 is a monotone CR scheme. As a reminder, this is an important property for a CR scheme to have in order to be able to use it in an approximation algorithm for the constrained submodular maximization problem.

Theorem 3.5. *Algorithm 3.1 is a monotone CR scheme for U_n^k, i.e. for every $x \in P_{\mathcal{I}}$ and $e \in A \subset B \subset supp(x)$,*

$$\mathbb{P}[e \in \pi_x(A)] \geq \mathbb{P}[e \in \pi_x(B)].$$

We start by giving an explicit formula for the probabilities above.

Lemma 3.5. *The following holds for any $e \in A$ and $|A| > k$:*

$$\mathbb{P}[e \in \pi_x(A)] = \frac{k - x_e}{|A|} + \frac{x(A \setminus e)}{|A|(|A|-1)}.$$

Proof.

$$\begin{aligned}
\mathbb{P}[e \in \pi_x(A)] &= \sum_{\substack{B \subset A \\ |B|=k \\ e \in B}} q_A(B) = \sum_{\substack{B \subset A \setminus e \\ |B|=k-1}} q_A(B \cup e) \\
&= \sum_{\substack{B \subset A \setminus e \\ |B|=k-1}} \frac{1}{\binom{|A|}{k}} \left(1 + \frac{x(A \setminus e) - x(B)}{|A|-k} - \frac{x(B) + x_e}{k}\right) \\
&= \sum_{\substack{B \subset A \setminus e \\ |B|=k-1}} \frac{1}{\binom{|A|}{k}} \left(1 - \frac{x_e}{k} + \frac{x(A \setminus e)}{|A|-k} - x(B)\left(\frac{1}{|A|-k} + \frac{1}{k}\right)\right) \\
&= \sum_{\substack{B \subset A \setminus e \\ |B|=k-1}} \frac{1}{\binom{|A|}{k}} \left(\frac{k - x_e}{k} + \frac{x(A \setminus e)}{|A|-k} - x(B)\frac{|A|}{k(|A|-k)}\right). \qquad (3.45)
\end{aligned}$$

We now use Equation (3.2) in a slightly modified form:

$$\sum_{\substack{B \subset A \setminus e \\ |B|=k-1}} x(B) = \binom{|A|-2}{k-2} x(A \setminus e). \qquad (3.46)$$

The only part in the sum (3.45) that depends on B is the last term with $x(B)$. Hence, by plugging-in (3.46) into (3.45), we get:

$$\binom{|A|}{k}\mathbb{P}[e \in \pi_x(A)] = \binom{|A|-1}{k-1}\left(\frac{k - x_e}{k}\right) + \binom{|A|-1}{k-1}\frac{x(A \setminus e)}{|A|-k} - \binom{|A|-2}{k-2}\frac{|A|}{k(|A|-k)} x(A \setminus e). \qquad (3.47)$$

We now use the formula

$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$$

to remove all the binomial coefficients from (3.47). We thus get:

$$\begin{aligned}
\frac{|A|}{k}\mathbb{P}[e \in \pi_x(A)] &= \frac{k - x_e}{k} + \frac{x(A \setminus e)}{|A| - k} - \frac{k-1}{|A|-1}\frac{|A|}{k(|A|-k)}x(A \setminus e) \\
&= \frac{k - x_e}{k} + \frac{x(A \setminus e)}{|A| - k}\left(1 - \frac{|A|(k-1)}{(|A|-1)k}\right) \\
&= \frac{k - x_e}{k} + \frac{x(A \setminus e)}{k(|A| - 1)}.
\end{aligned}$$

This implies the desired result:

$$\mathbb{P}[e \in \pi_x(A)] = \frac{k - x_e}{|A|} + \frac{x(A \setminus e)}{|A|(|A| - 1)}.$$

□

We can now prove Theorem 3.5.

Proof of Theorem 3.5. Let $A \subset N$ and $e \in A$. If $|A| \leq k$, then

$$\mathbb{P}[e \in \pi_x(A)] = 1$$

and the theorem trivially holds. We therefore suppose that $|A| > k$. In order to prove the theorem, it is clearly enough to show that for any $f \notin A$,

$$\mathbb{P}[e \in \pi_x(A)] \geq \mathbb{P}[e \in \pi_x(A \cup f)]. \tag{3.48}$$

We show the difference of those two terms is greater than 0 by using Lemma 3.5 for both terms:

$$\begin{aligned}
\mathbb{P}[e \in \pi_x(A)] - \mathbb{P}[e \in \pi_x(A \cup f)] &= \frac{k - x_e}{|A|} + \frac{x(A \setminus e)}{|A|(|A| - 1)} - \frac{k - x_e}{|A| + 1} - \frac{x(A \setminus e) + x_f}{(|A| + 1)|A|} \\
&= \frac{k - x_e}{|A|} - \frac{k - x_e}{|A| + 1} - \frac{x_f}{(|A| + 1)|A|} + x(A \setminus e)\left(\frac{1}{|A|(|A| - 1)} - \frac{1}{(|A| + 1)|A|}\right) \\
&= \frac{(|A| + 1)(k - x_e) - |A|(k - x_e) - x_f}{|A|(|A| + 1)} + \frac{2x(A \setminus e)}{(|A|^2 - 1)|A|} \\
&= \frac{k - x_e - x_f}{|A|(|A| + 1)} + \frac{2x(A \setminus e)}{(|A|^2 - 1)|A|} \\
&\geq 0.
\end{aligned}$$

The last inequality holds because since $x \in P_{\mathcal{I}} = \{x \in [0, 1]^N \mid x(N) \leq k\}$, we have

$$x_e + x_f \leq k,$$

and all the other terms are positive. We have thus shown (3.48) which is enough to prove the theorem.

□

4 An optimal monotone contention resolution scheme for partition matroids

4.1 The CR scheme

The CR scheme for uniform matroids defined in Algorithm 3.1 can be naturally extended to a CR scheme for *partition matroids*. This is not surprising since partition matroids can be seen as a direct sum of uniform matroids.

We define the framework for a partition matroid $\mathcal{M} = (N, \mathcal{I})$.

- $N = \{1, \dots, n\}$ is the ground set and it admits the partition $N = D_1 \sqcup \cdots \sqcup D_k$. Moreover, each set D_i (called a *block* of the partition matroid) has an associated integer $d_i \in \mathbb{Z}_{\geq 0}$, called the *capacity* of the block.
- $\mathcal{I} = \Big\{ A \subset N \mid |A \cap D_i| \leq d_i \quad \forall i \in \{1, \dots, k\} \Big\}$ are the independent sets.
- $P_{\mathcal{I}} = \Big\{ x \in [0,1]^N \mid x(D_i) \leq d_i \quad \forall i \in \{1, \dots, k\} \Big\}$ is the matroid polytope.

Notice that, for every i, the restriction of the partition matroid to a subset D_i is a uniform matroid, i.e.

$$\mathcal{M}|_{D_i} = U(d_i, |D_i|) \qquad \forall i \in \{1, \dots, k\} \tag{4.1}$$

where $U(k,n) := U_n^k$ is the uniform matroid of rank k on n elements.

We fix the following convenient notations:

- $P_{\mathcal{I}}^{(i)} = \{ y \in [0,1]^{D_i} \mid y(D_i) \leq d_i \}$ is the matroid polytope of the uniform matroid $\mathcal{M}|_{D_i}$. Notice that $P_{\mathcal{I}}^{(i)}$ is the canonical projection of $P_{\mathcal{I}}$ onto the D_i coordinates.
- For any $x \in P_{\mathcal{I}}$, we denote by $x^{(i)} := x|_{D_i}$ the restriction of x to the D_i coordinates. Notice then that $x^{(i)} \in P_{\mathcal{I}}^{(i)}$.

We remind the following definitions that we already used for uniform matroids. For any $B \subset A \subset N$,

$$q_A(B) := \frac{1}{\binom{|A|}{|B|}} \Big(1 + \bar{x}(A \setminus B) - \bar{x}(B) \Big) \tag{4.2}$$

and

$$p_A(B) := \prod_{i \in B} x_i \prod_{i \in A \setminus B} (1 - x_i) = \mathbb{P}[R_A(x) = B], \tag{4.3}$$

where $R_A(x)$ is the random set obtained by rounding each coordinate of $x|_A$ to 1 with probability x_i. In other words, $R_A(x) = R(x) \cap A$. Of course, $R_N(x)$ is simply equal to the standard $R(x)$.

We denote by

$$c(k,n) := 1 - \binom{n}{k} \left(1 - \frac{k}{n}\right)^{n+1-k} \left(\frac{k}{n}\right)^k \tag{4.4}$$

the optimal balancedness for U_n^k, the uniform matroid of rank k on n elements.

The main result of this section is the following.

Algorithm 4.1 CR Scheme π for partition matroids

Input: A point $x \in P_{\mathcal{I}}$ and a set $A \subset \text{supp}(x)$
Output: An independent set $I \in \mathcal{I}$ such that $I \subset A$.

$I \leftarrow \emptyset$
for $i \in \{1, ..., k\}$ **do**
  Set $A_i \leftarrow A \cap D_i$
  if $|A_i| \leq d_i$ **then**
    $I \leftarrow I \cup A_i$
  else
    Pick any $B \subset A_i$ of size $|B| = d_i$ with probability $q_{A_i}(B)$
    $I \leftarrow I \cup B$
return I

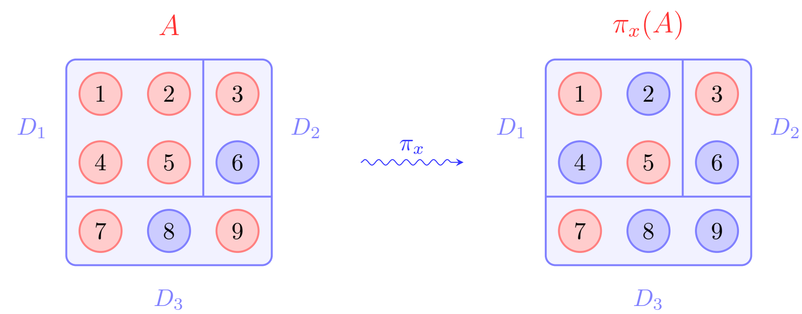


Figure 9: An example run of the CR scheme with $d_1 = 2, d_2 = 1, d_3 = 1$

Theorem 4.1. *Algorithm 4.1 is a c-balanced CR scheme for the partition matroid $\mathcal{M} = (N, \mathcal{I})$, where*

$$c = \min_{i \in \{1,...,k\}} c(d_i, |D_i|)$$

Proof. Let $e \in N$. We need to show that for every $x \in P_{\mathcal{I}}$ with $x_e > 0$,

$$\mathbb{P}[e \in \pi_x(R(x)) \mid e \in R(x)] \geq \min_{i \in \{1,...,k\}} c(d_i, |D_i|).$$

This is equivalent to showing that for every $x \in P_{\mathcal{I}}$ with $x_e > 0$,

$$\mathbb{P}[e \notin \pi_x(R(x)) \mid e \in R(x)] \leq \max_{i \in \{1,...,k\}} \binom{|D_i|}{d_i} \left(1 - \frac{d_i}{|D_i|}\right)^{|D_i|+1-d_i} \left(\frac{d_i}{|D_i|}\right)^{d_i}. \tag{4.5}$$

Since all the D_i's form a partition of N, we let $j \in \{1, \ldots, k\}$ be the unique index such that $e \in D_j$. We compute:

$$
\begin{aligned}
\mathbb{P}[e \notin \pi_x(R(x)) \mid e \in R(x)] &= \frac{1}{x_e}\mathbb{P}[e \notin \pi_x(R(x)),\ e \in R(x),\ |R_{D_j}(x)| > d_j] \\
&= \frac{1}{x_e}\mathbb{P}[e \notin \pi_x(R(x)), e \in R_{D_j}(x), |R_{D_j}(x)| > d_j] \\
&= \frac{1}{x_e} \sum_{\substack{A \subset D_j \setminus e \\ |A| \geq d_j}} \mathbb{P}[e \notin \pi_x(R(x)),\ R_{D_j}(x) = A \cup e] \\
&= \frac{1}{x_e} \sum_{\substack{A \subset D_j \setminus e \\ |A| \geq d_j}} \mathbb{P}[e \notin \pi_x(R(x)) \mid R_{D_j}(x) = A \cup e]\ \mathbb{P}[R_{D_j}(x) = A \cup e] \\
&= \sum_{\substack{A \subset D_j \setminus e \\ |A| \geq d_j}} \frac{p_{D_j}(A \cup e)}{x_e}\ \mathbb{P}[e \notin \pi_x(R(x)) \mid R_{D_j}(x) = A \cup e] \\
&= \sum_{\substack{A \subset D_j \setminus e \\ |A| \geq d_j}} p_{D_j \setminus e}(A) \sum_{\substack{B \subset A \\ |B| = d_j}} q_{A \cup e}(B) = G(x). \qquad (4.6)
\end{aligned}
$$

Note that this is exactly the function $G(x)$ that we defined for uniform matroids in (3.7). The only difference being that our uniform matroid is now on the ground set D_j (instead of N) and of rank d_j (instead of k). We do not explicitly write down the dependence on the ground set and the rank in the definition of $G(x)$ for simplicity of notation. Moreover, notice that expression (4.6) only depends on the x-variables in D_j. Hence, because of Theorem 3.2, we get:

$$
\max\{G(x) \mid x \in P_{\mathcal{I}}\} = \max\{G(x) \mid x \in P_{\mathcal{I}}^{(j)}\} = \binom{|D_j|}{d_j} \left(1 - \frac{d_j}{|D_j|}\right)^{|D_j|+1-d_j} \left(\frac{d_j}{|D_j|}\right)^{d_j} \qquad (4.7)
$$

We therefore get the desired result: for any $x \in P_{\mathcal{I}}$ and $e \in \mathrm{supp}(x)$,

$$
\mathbb{P}[e \notin \pi_x(R(x)) \mid e \in R(x)] \leq \max_{i \in \{1,\dots,k\}} \binom{|D_i|}{d_i} \left(1 - \frac{d_i}{|D_i|}\right)^{|D_i|+1-d_i} \left(\frac{d_i}{|D_i|}\right)^{d_i}
$$

which is indeed what we wanted to show in (4.5).

□

4.2 Optimality

We now show that this factor is *optimal*. Again, this follows naturally from the proof of the uniform matroid case.

Theorem 4.2. *There does not exist a c-balanced CR scheme for the partition matroid $\mathcal{M}$ satisfying:*

$$
c > \min_{i \in \{1,\dots,k\}} c(d_i, |D_i|)
$$

Proof. Let π be an arbitrary c-balanced CR scheme for the partition matroid $\mathcal{M}$. We take $j \in \text{argmin}_{\{i\in 1,\ldots,k\}} c(d_i, |D_i|)$ and define the point $x \in P_{\mathcal{I}}$ by

$$x_e = \begin{cases} d_j/|D_j| & \text{if } e \in D_j. \\ 0 & \text{otherwise.} \end{cases}$$

As usual, we let $R(x)$ be the random set obtained by rounding independently each coordinate of x to one with probability x_e. Moreover, we denote by $I := \pi_x(R(x))$ the independent set returned by the CR scheme π. We have

$$c\, d_j = \sum_{e\in D_j} c\, x_e = \sum_{e\in N} c\, x_e \le \sum_{e\in N} \mathbb{P}[e \in I] = \mathbb{E}[|I|] \le \mathbb{E}[r(R(x))]. \tag{4.8}$$

Moreover, notice that by our choice of the point $x \in P_{\mathcal{I}}$, we have

$$\mathbb{E}[r(R(x))] = \mathbb{E}\Big[r\big(R_{D_j}(x^{(j)})\big)\Big].$$

Hence, by Theorem 3.4, we get that

$$\mathbb{E}[r(R(x))] = d_j \left(1 - \binom{|D_j|}{d_j} \left(1 - \frac{d_j}{|D_j|}\right)^{|D_j|+1-d_j} \left(\frac{d_j}{|D_j|}\right)^{d_j}\right). \tag{4.9}$$

Plugging, (4.9) into (4.8), we obtain the desired result:

$$c \le c(d_j, |D_j|) = \min_{i\in\{1,\ldots,k\}} c(d_i, |D_i|).$$

□

4.3 Monotonicity

We prove in this subsection that the CR scheme for partition matroids is monotone. Once again, this follows from the result about monotonicity for uniform matroids: Theorem 3.5.

Theorem 4.3. *Algorithm 4.1 is a monotone CR scheme for the partition matroid $\mathcal{M}$, i.e. for every $x \in P_{\mathcal{I}}$ and $e \in A \subset B \subset supp(x)$,*

$$\mathbb{P}[e \in \pi_x(A)] \ge \mathbb{P}[e \in \pi_x(B)].$$

Proof. We let $x \in P_{\mathcal{I}}$, let $e \in A \subset B$ and let $j \in \{1, \ldots, k\}$ be the unique index such that $e \in D_j$. We denote in this proof the CR scheme applied to the partition matroid $\mathcal{M}$ (Algorithm 4.1) by π_x. Moreover, we denote the CR scheme applied to the uniform matroid of rank d_j on the ground set D_j (Algorithm 3.1) by ρ_x.

We denote $A_j := A \cap D_j$ and $B_j := B \cap D_j$. By construction of both algorithms, it is clear that

$$\mathbb{P}[e \in \pi_x(A)] = \mathbb{P}[e \in \rho_x(A_j)]$$

and

$$\mathbb{P}[e \in \pi_x(B)] = \mathbb{P}[e \in \rho_x(B_j)].$$

Moreover, since $A_j \subset B_j$, by Theorem 3.5:

$$\mathbb{P}[e \in \rho_x(A_j)] \geq \mathbb{P}[e \in \rho_x(B_j)],$$

which implies the desired result by the previous two equalities:

$$\mathbb{P}[e \in \pi_x(A)] \geq \mathbb{P}[e \in \pi_x(B)].$$

□

5 Conclusion and outlook

To sum up, we have in this thesis looked at the problem of designing contention resolution schemes for different matroids. The goal was to try to improve the balancedness of $1-1/e$ provided for a general matroid in [5]. We have managed to do that for three cases: matroids with disjoint circuits, uniform matroids and partition matroids.

We provide in Section 2 an optimal monotone CR scheme for matroids with disjoint circuits with a balancedness factor of $1-\frac{1}{g}(1-\frac{1}{g})^{g-1}$. The idea of the algorithm is quite simple: we check which cycles are completely included in the random set $R(x)$. For these cycles, we remove one element randomly from each of them with a probability that depends on the input point $x \in P_{\mathcal{I}}$. The proof for the balancedness is a consequence of the arithmetic-geometric mean inequality. We then prove optimality of this balancedness, as well as monotonicity of the scheme. We also discuss a couple of interesting applications to graphic matroids.

In Section 3, we design an optimal monotone CR scheme for any uniform matroid of rank k on n elements. The balancedness of this scheme is $1-\binom{n}{k}\left(1-\frac{k}{n}\right)^{n+1-k}\left(\frac{k}{n}\right)^{k} := c(k,n)$, which generalizes the known optimal balancedness for the uniform matroid of rank one of $1-(1-1/n)^n$. Asymptotically, $c(k,n) \xrightarrow{n\to\infty} 1-e^{-k}k^k/k!$, which also generalizes the asymptotic $1-1/e$ for $k=1$. The idea is again quite simple: we simply check whether the random set $R(x)$ has more than k elements and keep k of those randomly with a probability which depends on the input point $x \in P_{\mathcal{I}}$. The proof of the balancedness is non-trivial and the main idea consists of looking at the complement probability $\mathbb{P}[e \notin \pi_x(R(x)) \mid e \in R(x)]$, rewriting it as a function of n variables, and maximizing this multivariable function over the uniform matroid polytope $P_{\mathcal{I}}$. We first maximize over the variable x_e while keeping all the other variables fixed. We then get an expression of $n-1$ variables and maximize that by simply finding the unique extremum (which is a local maximum) in the interior of the domain, and finally checking that any point in the boundary has a lower function value than that point. We also provide a proof of optimality for the balancedness which surprisingly uses a result that we found during the second step of the maximization problem discussed above. Finally, we also show the CR scheme is monotone.

In Section 4, we show that we can generalize the CR scheme we constructed for uniform matroids to partition matroids. The arguments all follow quite naturally and the balancedness is of $\min_i c(d_i, |D_i|)$, where the D_i's are the blocks of the partition matroid with each D_i having capacity d_i. The scheme turns out to be optimal and monotone in this case as well.

The idea of designing CR schemes by assigning a certain probability depending on the input point $x \in P_{\mathcal{I}}$ to every independent subset of the input set is the central idea of every CR scheme in this thesis. It might be possible to use that idea to design other CR schemes for different matroids, or even different independence families. All the proofs of optimality also follow the same basic principle and a generalization ot that argument to other matroids might be something doable as well.

References

[1] S. Alaei. “Bayesian combinatorial auctions. Expanding single buyer mechanisms to many buyers”. In: *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011* (2011).

[2] S. Bruggmann and R. Zenklusen. “An optimal monotone contention resolution scheme for bipartite matchings via a polyhedral viewpoint”. In: *Mathematical Programming* (2020).

[3] G. Calinescu et al. “Maximizing a monotone submodular function subject to a matroid constraint”. In: *SIAM Journal on Computing* (2011).

[4] G. Calinescu et al. “Maximizing a submodular set function subject to a matroid constraint”. In: *Proceedings of the 12th IPCO Conference* (2007).

[5] C. Chekuri, J. Vondrák, and R. Zenklusen. “Submodular Function Maximization via the Multilinear Relaxation and Contention Resolution Schemes”. In: *SIAM Journal on Computing* (2014).

[6] J. Edmonds. “Submodular functions, matroids, and certain polyhedra”. In: *Combinatorial Structures and Their Applications, Gordon and Breach, New York* (1970).

[7] U. Feige and J. Vondrak. “Appoximation Algorithms for allocation problems: Improving the factor of 1-1/e”. In: *47th Annual IEEE Symposium on Foundations of Computer Science* (2006).

[8] U. Feige and J. Vondrak. “The Submodular Welfare Problem with Demand Queries”. In: *Theory of Computing* (2010).

[9] M. Feldman, O. Svensson, and R. Zenklusen. “Online Contention Resolution Schemes”. In: *SIAM Symposium on Discrete Algorithms* (2016).

[10] D. Geller and B. Manvel. “Reconstruction of Cacti”. In: *Canadian Journal of Mathematics* (1969).

[11] G. Guruganesh and E. Lee. “Understanding the correlation gap for matchings”. In: *Proceedings of the 37th Annual IARCS Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS)* (2017).

[12] F. Harary and G. E. Uhlenbeck. “On the Number of Husimi Trees, I”. In: *Proceedings of the National Academy of Sciences of the United States of America* (1953).

[13] F. Harary and D. Welsh. “Matroids Versus Graphs”. In: *The Many Facets of Graph Theory* (1969).

[14] E. Lee and S. Singla. “Optimal Online Contention Resolution Schemes via Ex-Ante Prophet Inequalities”. In: *26th Annual European Symposium on Algorithms, ESA 2018* (2018).

[15] B. Lehmann, D. Lehmann, and N. Nisan. “Combinatorial auctions with decreasing marginal utilities”. In: *Games and Economic Behavior* (2006).

[16] B. Mirzasoleiman et al. “Distributed submodular maximization: Identifying representative elements in massive data”. In: *Proceedings of the 26th International Conference on Neural Information Processing Systems (NIPS)* (2013).

[17] A. Schrijver. *Combinatorial Optimization: Polyhedra and Efficiency*. 2003.

[18] StackExchange. *A graph with no even cycles has each edge in at most one cycle*. 2015. URL: https://math.stackexchange.com/questions/413288/graph-with-no-even-cycles-has-each-edge-in-at-most-one-cycle.

[19] K. Wei, R. Iyer, and J. Bilmes. "Fast multi-stage submodular maximization". In: *Proceedings of the 31st International Conference on Machine Learning (ICML)* (2014).

A Appendix

We give here the computations (Lemma A.1 and Lemma A.2) that allow us to compute the Hessian matrix

$$H(x)_{i,j} = \frac{\partial^2 h_S^k(x)}{\partial x_i \partial x_j}.$$

at the point $(k/n, \dots, k/n)$ of the function

$$h_S^k(x) = \sum_{\substack{A \subset S \\ |A|=k}} p_S(A)(k - x(A)).$$

These two results were used for the proof of Proposition 3.2.

Note that we have already computed in (3.29) that

$$\frac{\partial h_S^k(x)}{\partial x_i} = Q_{S \setminus i}^{k-1}(x)\Big(k - x(S) - x_i\Big) \qquad \forall i \in S. \tag{A.1}$$

where

$$Q_S^k(x) := \sum_{A \subset S, |A|=k} p_S(A).$$

A useful and straightforward computation is the following:

$$Q_S^l(k/n, \dots, k/n) = \binom{n-1}{l} \left(\frac{k}{n}\right)^l \left(\frac{n-k}{n}\right)^{n-1-l}. \tag{A.2}$$

Lemma A.1. *The diagonal terms of the Hessian matrix at the point $(k/n, \dots, k/n)$ satisfy:*

$$\frac{\partial^2 h_S^k}{\partial x_i^2}(k/n, \dots, k/n) = -2\binom{n-2}{k-1} \left(\frac{k}{n}\right)^{k-1} \left(\frac{n-k}{n}\right)^{n-k-1} \qquad \forall i \in S.$$

Proof. Since the term $Q_{S \setminus i}^{k-1}(x)$ in (A.1) does not depend on x_i, we easily derive:

$$\frac{\partial^2 h_S^k(x)}{\partial x_i^2} = -2\, Q_{S \setminus i}^{k-1}(x) \qquad \forall i \in S. \tag{A.3}$$

Therefore, by (A.2), evaluating expression (A.3) at the point $(k/n, \dots, k/n)$ gives us:

$$\frac{\partial^2 h_S^k}{\partial x_i^2}(k/n, \dots, k/n) = -2\binom{n-2}{k-1} \left(\frac{k}{n}\right)^{k-1} \left(\frac{n-k}{n}\right)^{n-k-1} \qquad \forall i \in S.$$

□

Lemma A.2. *The non-diagonal terms of the Hessian matrix at the point $(k/n, \dots, k/n)$ satisfy:*

$$\frac{\partial^2 h_S^k}{\partial x_i \partial x_j}(k/n, \dots, k/n) = -\binom{n-2}{k-1} \left(\frac{k}{n}\right)^{k-1} \left(\frac{n-k}{n}\right)^{n-k-1} \qquad \text{for } i \neq j \tag{A.4}$$

Proof. We first show that

$$Q^{k-1}_{S\setminus i}(x) = x_j\, Q^{k-2}_{S\setminus i,j}(x) + (1-x_j)\, Q^{k-1}_{S\setminus i,j}(x). \tag{A.5}$$

Indeed,

$$\begin{aligned}
Q^{k-1}_{S\setminus i}(x) &= \sum_{\substack{A\subset S\setminus i\\ |A|=k-1}} p_{S\setminus i}(A)\\
&= \sum_{\substack{A\subset S\setminus i\\ |A|=k-1\\ j\in A}} p_{S\setminus i}(A) + \sum_{\substack{A\subset S\setminus i\\ |A|=k-1\\ j\notin A}} p_{S\setminus i}(A)\\
&= x_j \sum_{\substack{A\subset S\setminus i\\ |A|=k-1\\ j\in A}} p_{S\setminus i}(A\setminus j) + (1-x_j) \sum_{\substack{A\subset S\setminus i\\ |A|=k-1\\ j\notin A}} p_{S\setminus i,j}(A)\\
&= x_j \sum_{\substack{B\subset S\setminus i,j\\ |B|=k-2}} p_{S\setminus i,j}(B) + (1-x_j) \sum_{\substack{A\subset S\setminus i,j\\ |A|=k-1}} p_{S\setminus i,j}(A)\\
&= x_j\, Q^{k-2}_{S\setminus i,j}(x) + (1-x_j)\, Q^{k-1}_{S\setminus i,j}(x).
\end{aligned}$$

We can therefore compute the non-diagonal terms of $H(x)$ by (A.1) and (A.5). For $i \neq j$,

$$\begin{aligned}
\frac{\partial^2 h^k_S(x)}{\partial x_j \partial x_i} &= \Big(Q^{k-2}_{S\setminus i,j}(x) - Q^{k-1}_{S\setminus i,j}(x)\Big)(k - x(S) - x_i) - Q^{k-1}_{S\setminus i}(x)\\
&= \Big(Q^{k-2}_{S\setminus i,j}(x) - Q^{k-1}_{S\setminus i,j}(x)\Big)(k - x(S) - x_i) - x_j\, Q^{k-2}_{S\setminus i,j}(x) - (1-x_j)\, Q^{k-1}_{S\setminus i,j}(x)\\
&= Q^{k-2}_{S\setminus i,j}(x)\Big(k - x(S) - x_i - x_j\Big) - Q^{k-1}_{S\setminus i,j}(x)\Big(k + 1 - x(S) - x_i - x_j\Big).
\end{aligned}$$

We can now evaluate the last expression at the point $(k/n, \ldots, k/n)$ with (A.2):

$$\begin{aligned}
\frac{\partial^2 h^k_S}{\partial x_i^2}(k/n,\ldots,k/n) &= -\binom{n-3}{k-2}\left(\frac{k}{n}\right)^{k-1}\left(\frac{n-k}{n}\right)^{n-k-1} - \binom{n-3}{k-1}\left(\frac{k}{n}\right)^{k-1}\left(\frac{n-k}{n}\right)^{n-k-1}\\
&= -\left(\frac{k}{n}\right)^{k-1}\left(\frac{n-k}{n}\right)^{n-k-1}\left(\binom{n-3}{k-2} + \binom{n-3}{k-1}\right)\\
&= -\binom{n-2}{k-1}\left(\frac{k}{n}\right)^{k-1}\left(\frac{n-k}{n}\right)^{n-k-1}.
\end{aligned}$$

□