SIAM J. DISCRETE MATH.
Vol. 33, No. 3, pp. 1277–1296

RANK VERTEX COVER AS A NATURAL PROBLEM FOR ALGEBRAIC COMPRESSION*

SYED M. MEESUM†, FAHAD PANOLAN‡, SAKET SAURABH§, AND MEIRAV ZEHAVI¶

Abstract. The question of the existence of a polynomial kernelization of the VERTEX COVER ABOVE LP problem was a long-standing, notorious open problem in parameterized complexity. Some years ago, the breakthrough work by Kratsch and Wahlström on representative sets finally answered this question in the affirmative [FOCS 2012]. In this paper, we present an alternative, *algebraic compression* of the VERTEX COVER ABOVE LP problem into the RANK VERTEX COVER problem. Here, the input consists of a graph G, a parameter k, and a bijection between $V(G)$ and the set of columns of a representation of a matroid M, and the objective is to find a vertex cover whose rank is upper bounded by k.

Key words. kernelization, algebraic compression, vertex cover, odd cycle transversal

AMS subject classifications. 05C85, 68R10

DOI. 10.1137/17M1154370

1. Introduction.

The field of parameterized complexity concerns the study of *parameterized problems*, where each problem instance is associated with a *parameter* k that is a nonnegative integer. Given a parameterized problem of interest, which is generally computationally hard, the first, most basic question that arises asks whether the problem at hand is *fixed-parameter tractable (FPT)*. Here, a problem Π is said to be FPT if it is solvable in time $f(k)\cdot|X|^{\mathcal{O}(1)}$, where f is an arbitrary function that depends *only* on k and $|X|$ is the size of the input instance. In other words, the notion of FPT signifies that it is not necessary for the combinatorial explosion in the running time of an algorithm for Π to depend on the input size, but it can be confined to the parameter k. Having established that a problem is FPT, the second, most basic question that follows asks whether the problem also admits a *polynomial kernel*. A concept closely related to kernelization is one of *polynomial compression*. Here, a problem Π is said to admit a polynomial compression if there exists a problem $\widehat{\Pi}$ and a polynomial-time algorithm such that given an instance (X,k) of Π, the algorithm outputs an equivalent instance $(\widehat{X},\widehat{k})$ of $\widehat{\Pi}$, where $|\widehat{X}| = \widehat{k}^{\mathcal{O}(1)}$ and $\widehat{k} \leq k$. Roughly speaking, compression is a mathematical concept that aims to analyze preprocessing procedures in a formal, rigorous manner. We note that in case $\Pi = \widehat{\Pi}$, the problem is further said to admit a *polynomial kernelization*, and the output $(\widehat{X},\widehat{k})$ is called a *kernel*.

The VERTEX COVER problem is (arguably) the most well-studied problem in parameterized complexity [12, 9]. Given a graph H and a parameter k, this problem asks whether H admits a vertex cover of size at most k. Over the years, a notable number of algorithms have been developed for the VERTEX COVER problem [4, 2, 13, 27, 7, 5, 8]. Currently, the best-known algorithm solves this problem in the remarkable time $1.2738^k \cdot n^{\mathcal{O}(1)}$ [8]. While it is not known whether the constant

*Received by the editors October 30, 2017; accepted for publication (in revised form) April 22, 2019; published electronically July 23, 2019.
https://doi.org/10.1137/17M1154370
Funding: Supported by Parameterized Approximation, ERC Starting Grant 306992, and Rigorous Theory of Preprocessing, ERC Advanced Investigator Grant 267959.

†Institute of Computer Science, University of Wrocław, Poland (meesum.syed@gmail.com).
‡Department of Informatics, University of Bergen, Norway (fahad.panolan@ii.uib.no).
§The Institute of Mathematical Sciences, HBNI, Chennai, India (saket@imsc.res.in).
¶Ben-Gurion University of the Negev, Beer-Sheva, Israel (meiravze@bgu.ac.il).

1.2738 is "close" to optimal, it is known that unless the exponential time hypothesis fails, Vertex Cover cannot be solved in time $2^{o(k)} \cdot n^{\mathcal{O}(1)}$ [18]. On the other hand, in the context of kernelization, the picture is clear in the following sense: It is known that Vertex Cover admits a kernel with $\mathcal{O}(k^2)$ vertices and edges [4], but unless NP $\subseteq$ co-NP/poly, it does not admit a kernel with $\mathcal{O}(k^{2-\epsilon})$ edges [11] for any $\epsilon > 0$. We remark that it is also known that Vertex Cover admits a kernel not only of size $\mathcal{O}(k^2)$ but also with only $2k$ vertices [7, 22], and it is conjectured that this bound might be essentially tight [6].

It has become widely accepted that Vertex Cover is one of the most natural test beds for the development of new techniques and tools in parameterized complexity. Unfortunately, the vertex cover number of a graph is generally large—in fact, it is often linear in the size of the entire vertex set of the graph [12, 9]. Therefore, alternative parameterizations, known as *above-guarantee parameterizations*, have been proposed. The two most well known such parameterizations are based on the observation that the vertex cover number of a graph H is at least as large as the *fractional vertex cover number* of H, which in turn is at least as large as the maximum size of a matching of H. Here, the fractional vertex cover number of H is the solution to the linear program that minimizes $\sum_{v \in V(H)} x_v$ subject to the constraints $x_u + x_v \geq 1$ for all $\{u, v\} \in E(H)$ and $x_v \geq 0$ for all $v \in V(H)$. Accordingly, given a graph H and a parameter k, the Vertex Cover Above MM problem asks whether H admits a vertex cover of size at most $\mu(H) + k$, where $\mu(H)$ is the maximum size of a matching of H, and the Vertex Cover Above LP problem asks whether H admits a vertex cover of size at most $\ell(H) + k$, where $\ell(H)$ is the fractional vertex cover number of H.

On the one hand, several parameterized algorithms for these two problems have been developed in the last decade [30, 29, 10, 26, 23]. Currently, the best-known algorithm for Vertex Cover Above LP, which is also the best-known algorithm for Vertex Cover Above MM, runs in time $2.3146^k \cdot n^{\mathcal{O}(1)}$ [23]. On the other hand, the question of the existence of polynomial kernelizations of these two problems was a long-standing, notorious open problem in parameterized complexity. Five years ago, the breakthrough work by Kratsch and Wahlström [21] on representative sets finally answered this question in the affirmative. To date, the kernelizations by Kratsch and Wahlström have remained the only known (randomized) polynomial compressions of Vertex Cover Above MM and Vertex Cover Above LP. Note that since $\ell(H)$ is necessarily at least as large as $\mu(H)$, a polynomial compression of Vertex Cover Above LP also doubles as a polynomial compression of Vertex Cover Above MM. We also remark that several central problems in parameterized complexity, such as the Odd Cycle Transversal problem, are known to admit parameter-preserving reductions to Vertex Cover Above LP [23]. Hence, the significance of a polynomial compression of Vertex Cover Above LP also stems from the observation that it simultaneously serves as a polynomial compression of additional well-known problems and can therefore potentially establish the target problem as a natural candidate to express compressed problem instances.

Recently, a higher above-guarantee parameterization of Vertex Cover, resulting in the Vertex Cover Above Lovász-Plummer, has been introduced by Garg and Philip [14]. Here, given a graph H and a parameter k, the objective is to determine whether H admits a vertex cover of size at most $(2\ell(H) - \mu(H)) + k$. Garg and Philip [14] showed that this problem is solvable in time $3^k \cdot n^{\mathcal{O}(1)}$, and Kratsch [20] showed that it admits a (randomized) kernelization that results in a large yet polynomial kernel. We remark that above-guarantee parameterizations can very easily reach bars beyond which the problem at hand is no longer FPT. For example, Gutin et

al. [16] showed that the parameterization of Vertex Cover above $m/\Delta(H)$, where $\Delta(H)$ is the maximum degree of a vertex in H and m is the number of edges in H, results in a problem that is not FPT (unless FPT=W[1]).

Our results and methods. In this paper, we present an alternative, *algebraic compression* of the Vertex Cover Above LP problem into the Rank Vertex Cover problem. We remark that Rank Vertex Cover was originally introduced by Lovász [24] as a tool for the examination of critical graphs. Given a graph H, a parameter ℓ, and a bijection between $V(H)$ and the set of columns of a representation of a matroid M, the objective of Rank Vertex Cover is to find a vertex cover of H whose rank, which is defined by the set of columns corresponding to its vertices, is upper bounded by ℓ. Note that formal definitions of the terms used in the definition of Rank Vertex Cover can be found in section 2.

We obtain a (randomized) polynomial compression of size $\mathcal{O}(k^7 + k^{4.5} \log \frac{1}{\varepsilon})$, where ε is the probability of failure and $k = \ell - \mu(H)$. Here, by failure we mean that we output an instance of Rank Vertex Cover which is not equivalent to the input instance. Our work makes use of properties of linear spaces and matroids and also relies on elementary probability theory. One of the main challenges it overcomes is the conversion of the methods of Lovász [24] into a procedure that works over rationals with reasonably small binary encoding.

2. Preliminaries. We use $\mathbb{N}$ to denote the set of natural numbers. For any $n \in \mathbb{N}$, we use $[n]$ as a shorthand for $\{1, 2, \ldots, n\}$. In this paper, the notation $\mathbb{F}$ will refer either to a finite field of prime size or to the field $\mathbb{R}$ of real numbers. Accordingly, $\mathbb{F}^n$ is an n-dimensional linear space over the field $\mathbb{F}$, where a vector $v \in \mathbb{F}^n$ is a tuple of n elements from the field $\mathbb{F}$. Here, the vector v is implicitly assumed to be represented as a column vector, unless stated otherwise. A finite set of vectors S over the field $\mathbb{F}$ is said to be *linearly independent* if the only solution to the equation $\sum_{v \in S} \lambda_v v = 0$, where it holds that $\lambda_v \in \mathbb{F}$ for all $v \in S$, is the one that assigns zero to all of the scalars λ_v. A set S that is not linearly independent is said to be *linearly dependent*. The *span* of a set of vectors S, denoted by $\overline{S}$ (or span(S)), is the set $\{\sum_{v \in S} \alpha_v v : \alpha_v \in \mathbb{F}\}$, defined over the linear space $\mathbb{F}^n$.

For a graph G, we use $V(G)$ and $E(G)$ to denote the vertex set and the edge set of G, respectively. We treat the edge set of an *undirected graph* G as a family of subsets of size 2 of $V(G)$, i.e., $E(G) \subseteq \binom{V(G)}{2}$. An *independent set* in a graph G is a set of vertices X such that for all $u, v \in X$, it holds that $\{u, v\} \notin E(G)$. For a graph G and a vertex $v \in V(G)$, we use $G \setminus v$ to denote the graph obtained from G after deleting v and the edges incident with v.

2.1. Matroids.

Definition 2.1. *A* matroid X *is a pair* $(U, \mathcal{I})$*, where* U *is a set of elements and* $\mathcal{I}$ *is a set of subsets of* U*, with the following properties:* (i) $\emptyset \in \mathcal{I}$*;* (ii) *if* $I_1 \subset I_2$ *and* $I_2 \in \mathcal{I}$*, then* $I_1 \in \mathcal{I}$*; and* (iii) *if* $I_1, I_2 \in \mathcal{I}$ *and* $|I_1| < |I_2|$*, then there is* $x \in (I_2 \setminus I_1)$ *such that* $I_1 \cup \{x\} \in \mathcal{I}$*.*

A set $I' \in \mathcal{I}$ is said to be *independent*; otherwise, it is said to be *dependent*. A set $B \in \mathcal{I}$ is a *basis* if no superset of B is independent. For example, $U_{t,n} = ([n], \{I : I \subseteq [n], |I| \leq t\})$ forms a matroid known as a *uniform matroid*. For a matroid $X = (U, \mathcal{I})$, we use $E(X), \mathcal{I}(X)$, and $\mathcal{B}(X)$ to denote the ground set U of X, the set of independent sets $\mathcal{I}$ of X, and the set of bases of X, respectively. Here, we are mainly interested in *linear matroids*, which are defined as follows. Given a matroid $X = (U, \mathcal{I})$, a matrix M having $|U|$ columns is said to *represent* X if (i) the columns of M are in bijection

with the elements in U and (ii) a set $A \subseteq U$ is independent in X if and only if the columns corresponding to A in M are linearly independent. Accordingly, a matroid is a linear matroid if it has a representation over some field. For simplicity, we use the same symbol to refer to a matroid M and its representation. For a matrix M and some subset B of columns of M, we let $M[\star, B]$ denote the submatrix of M that is obtained from M by deleting all columns not in B. The submatrix of M over a subset of rows R and a subset of columns B is denoted using $M[R, B]$. We define the Rank Vertex Cover problem using a representable matroid as follows.

Rank Vertex Cover
Input: A graph H, an integer ℓ, and a bijection ϕ between $V(H)$ and the set of columns of a representation of a matroid M.
Output: Is there a vertex cover $S \subseteq V(H)$ of H such that $\text{rank}(\{\phi(s) : s \in S\}) \leq \ell$?

In the paper we would be working with the above-guarantee parameter k, where $k = \ell - \mu(H)$. We proceed by stating several basic definitions related to matroids that are central to our work. For this purpose, let $X = (U, \mathcal{I})$ be a matroid. An element $x \in U$ is called a *loop* if $\{x\} \notin \mathcal{I}$; equivalently, it does not belong to any independent set of X. If X is a linear matroid, then loops correspond to zero column vectors in its representation. An element $x \in U$ is called a *co-loop* if it occurs in every basis of X. Note that for a linear matroid X, an element x is a co-loop if and only if it is linearly independent from any subset of $U \setminus \{x\}$. Observe that for any co-loop x and $A \in \mathcal{I}$, we have $A \cup \{x\} \in \mathcal{I}$. For a subset $A \subseteq U$, the *rank* of A is defined as the maximum size of an independent subset of A, that is, $\text{rank}_X(A) := \max_{I' \subseteq A}\{|I'| : I' \in \mathcal{I}\}$. We remove the subscript of $\text{rank}_X(A)$ if the matroid is clear from the context. The rank of a matroid is defined to be the rank of the set U.

The *rank function* of X is the function $\text{rank} : 2^U \to \mathbb{N}$ that assigns $\text{rank}(A)$ to each subset $A \subseteq U$. Note that this function satisfies the following properties:

1. $0 \leq \text{rank}(A) \leq |A|$;
2. if $A \subseteq B$, then $\text{rank}(A) \leq \text{rank}(B)$;
3. $\text{rank}(A \cup B) + \text{rank}(A \cap B) \leq \text{rank}(A) + \text{rank}(B)$.

A set F such that $\emptyset \subseteq F \subseteq U$ is a *flat* if $\text{rank}(F \cup \{x\}) > \text{rank}(F)$ for all $x \notin F$. Let $\mathcal{F}$ be the set of all flats of the matroid X. For any subset A of U, the closure $\overline{A}$ is defined as $\overline{A} = \bigcap_{F \in \mathcal{F}}\{F : A \subseteq F\}$. It can be seen that the closure of a set is the flat of minimum rank containing it. We list out some useful properties of flats and the closure operation as follows:

1. For any flat F, we have $F = \overline{F}$.
2. For any two flats X, Y, we have that $X \cap Y$ is also a flat.
3. For any set $S \subseteq U$, we have $\text{rank}(S) = \text{rank}(\overline{S})$.

For a linear matroid the analogue of closure operation is the operation of span. To denote the span of a set in a matroid M, we would use the notation span_M and remove the subscript if the matroid is clear from the context. In this paper, for a linear matroid both these notions have been used interchangeably. Flats in a linear matroid are the subspaces of the column space of the representation matrix. Any matroid always contains two flats trivially if it has a nonzero matrix representation, namely, the flat containing the zero vector and the column space of the representation. We next define the notion of general position on a flat for a linear matroid.

Definition 2.2 (general position on a flat in a linear matroid). *Let F be a flat of a linear matroid X. An element $x \in F$ is said to be in* general position on F *if for any flat F' of X, if x is contained in* $\text{span}(F' \setminus \{x\})$*, then $F \subseteq F'$.*

The notion of general position is related to the independent sets of a linear matroid as follows.

LEMMA 2.3. *Given a linear matroid M, a flat F of M, and a vector $x \in F$. If for all $I \in \mathcal{I}(M)$ such that $F \not\subseteq \overline{I}$ we have $I \cup \{x\} \in \mathcal{I}(M)$, then x is in general position on F.*

Proof. We prove the contrapositive. Assume that x is not in general position on F. Using Definition 2.2, we see that there exists a flat F' with $x \in \overline{F' \setminus \{x\}}$ such that F' does not contain F. In particular, F is not spanned by any subset of F'. Let I be a maximal independent set contained in $F' \setminus \{x\}$. Clearly, I does not span F, but $I \cup \{x\}$ is a dependent set. ∎

Observation 1. If a vector x is in general position on a flat F with $\text{rank}(F) \geq 1$, in a linear matroid, then x is nonzero.

Proof. Assume that $x = \vec{0}$. As F has rank at least one, we get that the representation matrix M is nonzero. So, M has $F' = \{\vec{0}\}$ as a flat such that $F \not\subseteq F'$, but $x \in \text{span}(F' \setminus \{x\}) = \text{span}(\emptyset) = \{\vec{0}\}$. Therefore, we get a contradiction. ∎

Deletion and contraction. The deletion of an element u from X results in a matroid X', denoted by $X \setminus u$, with ground set $E(X') = E(X) \setminus \{u\}$ and set of independent sets $\mathcal{I}(X') = \{I \ : \ I \in \mathcal{I}(X), u \notin I\}$. The contraction of a nonloop element u from X results in a matroid X', denoted by X/u, with ground set $E(X') = E(X) \setminus \{u\}$ and set of independent sets $\mathcal{I}(X') = \{I \setminus \{u\} \ : \ u \in I \text{ and } I \in \mathcal{I}(X)\}$. The basis sets in a matroid and its contraction satisfy the following.

Observation 2. A set B is a basis in X/u if and only if $B \cup \{u\}$ is a basis in X.

When we are considering two matroids X and X/u, then for any subset $T \subseteq E(X) \setminus \{u\}$, $\overline{T}$ represents the closure of T with respect to the matroid X.

A matroid can also be represented by a ground set and a rank function, and for our purposes, it is sometimes convenient to employ such a representation. That is, we also use a pair (U, r) to specify a matroid, where U is the ground set and r is rank function. Now, we prove several lemmas regarding operations on matroids, which are used later in the paper.

Observation 3. Let X be a matroid, $u \in E(X)$ be a nonloop element, and v be a co-loop in X. Then v is a co-loop in X/u. Moreover, $\text{rank}(X/u) = \text{rank}(X) - 1$.

Proof. If B is a basis in X/u, then $B \cup \{u\}$ is a basis in X by Observation 2. As v is a co-loop in X, $v \in B \cup \{u\}$, which implies that $v \in B$. Hence, v is a co-loop in X/u. ∎

Given a matrix (or a linear matroid) A and a column $v \in A$, by moving the column vector v to some vector u, we refer to the operation of replacing v in A by a vector u.

LEMMA 2.4. *Let $X = (U, \mathcal{I})$ be a linear matroid, $W \subseteq U$, and let $u, v \notin W$ be two elements in X with v a co-loop in X. Let X' be the matroid obtained by replacing u with any vector in* $\text{span}(W)$. *Then v is also a co-loop in X'.*

Proof. Let u' denote the vector in the span of W which replaced u. Notice that the only modification performed with respect to the vectors of X is the update of u to u'. Suppose, by way of contradiction, that v is not a co-loop in X'. Then there exists a set of elements $S \subseteq E(X')$, where $v \notin S$, whose span contains v. If $u' \notin S$,

then $S \subseteq U$, which implies that v was not a co-loop in X. Since this results in a contradiction, we have that $u' \in S$. As u' is in the span of W, v must be in the span of $(W \cup S) \setminus \{u'\}$. Since $(W \cup S) \setminus \{u'\} \subseteq U$ and $v \notin (W \cup S) \setminus \{u'\}$, we have thus reached a contradiction. ∎

We remark that Lemma 2.4 also holds in the special case when vector u is moved to a general position on the flat spanned by W.

In general, the rank of any set in the contracted matroid is given by the following.

LEMMA 2.5 (see [15, Proposition 3.9]). *Let v be an element in a matroid $X = (U, \mathcal{I})$, which is not a loop in X. Let $T \subseteq U$ such that $v \notin T$. Then* $\text{rank}_{X/v}(T) = \text{rank}_X(T \cup v) - 1$.

The next lemma follows from the above.

LEMMA 2.6. *Let v be an element in a matroid $X = (U, \mathcal{I})$, which is not a loop in X. Let T be a subset of U such that $v \in \overline{T}$. Then* $\text{rank}_{X/v}(T \setminus \{v\}) = \text{rank}_X(T) - 1$.

The lemma above can be rephrased as follows: If T is a set of elements in a matroid $X = (U, \mathcal{I})$ such that an element $v \in U$ is contained in the span of T, then the rank of $T \setminus \{v\}$ in the contracted matroid X/v is smaller by 1 than the rank of T in X. The span of sets in a contracted matroid are given by the following.

LEMMA 2.7 (see [28, Proposition 3.1.12]). *For any matroid X, let $T \subset E(X)$ and $A \subseteq E(X) \setminus T$. Then* $\text{span}_{X/T}(A) = \text{span}_X(A \cup T) \setminus T$.

3. Compression. Our objective is to give a polynomial compression of VERTEX COVER ABOVE LP. More precisely, we develop a polynomial-time randomized algorithm that, given an instance of VERTEX COVER ABOVE LP with parameter k and $\varepsilon > 0$ with probability at least $1 - \varepsilon$, outputs an equivalent instance of RANK VERTEX COVER whose size is bounded by a polynomial in k and ε. It is known that there is a parameter-preserving reduction from VERTEX COVER ABOVE LP to VERTEX COVER ABOVE MM such that the parameter of the output instance is linear in the parameter of the original instance [21]. Thus, in order to give a polynomial compression of VERTEX COVER ABOVE LP to RANK VERTEX COVER where the size of the output instance is bounded by $\mathcal{O}(k^7 + k^{4.5} \log \frac{1}{\varepsilon})$, it is enough to give a polynomial compression of VERTEX COVER ABOVE MM to RANK VERTEX COVER with the same bound on the size of the output instance. For a graph H, we use $\mu(H)$ and $\beta(H)$ to denote the maximum size of a matching and the vertex cover number of H, respectively. Let (G, k) be an instance of VERTEX COVER ABOVE MM. Let $n = |V(G)|$ and I_n denote the $n \times n$ identity matrix. That is, I_n is a representation of $U_{n,n}$. Notice that (G, k) is a YES-instance of VERTEX COVER ABOVE MM if and only if $(G, I_n, \mu(G) + k)$ with any arbitrary bijection between $V(G)$ and columns of I_n, is a YES-instance of RANK VERTEX COVER.

In summary, to give the desired polynomial compression of VERTEX COVER ABOVE LP, it is enough to give a polynomial compression of instances of the form $(G, I_n, \mu(G) + k)$ of RANK VERTEX COVER where the size of the output instance is bounded by $\mathcal{O}(k^7 + k^{4.5} \log \frac{1}{\varepsilon})$. Here, the parameter is k. For instances of RANK VERTEX COVER, we assume that the columns of the matrix are labeled by the vertices in $V(G)$ in a manner corresponding to a bijection between the input graph and columns of the input matrix. As discussed above, we again stress that now our objective is to give a polynomial compression of an instance of the form $(G, I_n, \mu(G) + k)$ of RANK VERTEX COVER to RANK VERTEX COVER, which can now roughly be thought of as a polynomial kernelization. We achieve the compression in two steps:

1. In the first step, given $(G, M = I_n, \mu(G) + k)$, in polynomial time we either conclude that $(G, I_n, \mu(G)+k)$ is a YES-instance of RANK VERTEX COVER or (with high probability of success) output an equivalent instance (G_1, M_1, ℓ) of RANK VERTEX COVER where the number of rows in M_1 and hence $\text{rank}(M_1)$ is upper bounded by $\mathcal{O}(k^{3/2})$. Moreover, we also bound the bits required for each entry in the matrix to be $\tilde{\mathcal{O}}(k^{5/2} + \log(1/\varepsilon))$ This step is explained in section 3.2. Notice that after this step, the graph G_1 need not be bounded by $k^{\mathcal{O}(1)}$.
2. In the second step, we work with the output (G_1, M_1, ℓ) of the first step, and in polynomial time we reduce the number of vertices and edges in the graph G_1 (and hence the number of columns in the matrix M_1). That is, output of this step is an equivalent instance (G_2, M_2, ℓ), where the size of G_2 is bounded by $\mathcal{O}(k^3)$. This step is explained in section 3.3.

Throughout the compression algorithm, we work with RANK VERTEX COVER. Notice that the input of RANK VERTEX COVER consists of a graph G, an integer ℓ, and a linear representation M of a matroid with a bijection between $V(G)$ and the set of columns of M. In the compression algorithm, we use operations that modify the graph G and the matrix M simultaneously. To employ these "simultaneous operations" conveniently, we define (in section 3.1) the notion of a *graph-matroid pair*. We note that the definition of a graph-matroid pair is the same as a pregeometry defined in [24], and various lemmas from [24] which we use here are adapted to this definition. We also define deletion and contraction operations on a graph-matroid pair and state some properties of these operations.

3.1. Graph-matroid pairs. We start with the definition of a graph-matroid pair.

DEFINITION 3.1. *A pair (H, M), where H is a graph and M is a matroid over the ground set $V(H)$, is called a* graph-matroid pair.

Notice that there is natural bijection between $V(H)$ and $E(M)$, which is the identity map. Now, we define deletion and contraction operations on graph-matroid pairs.

DEFINITION 3.2. *Let $P = (H, M)$ be a graph-matroid pair, and let $u \in V(H)$. The* deletion *of u from P, denoted by $P \setminus u$, results in the graph-matroid pair $(H \setminus u, M \setminus u)$. If u is not a loop in M, then the* contraction *of u in P, denoted by P/u, results in the graph-matroid pair $(H \setminus u, M/u)$. For an edge $e \in E(H)$, $P \setminus e$ represents the pair $(H \setminus e, M)$.*

We remark that matroid deletion and contraction can be done in time polynomial in the size of ground set for a linear matroid. For details, we refer the reader to [15, 28].

DEFINITION 3.3. *Given a graph-matroid pair $P = (H, M)$, the vertex cover number of P is defined as $\tau(P) = \min\{\text{rank}_M(S) : S \text{ is a vertex cover of } H\}$.*

For example, if M is an identity matrix (where each element is a co-loop), then $\tau(P)$ is the vertex cover number of H. Moreover, if we let M be the uniform matroid $U_{t,n}$ such that t is at least the size of the vertex cover number of H, then $\tau(P)$ again equals the vertex cover number of H.

Let $P = (H, M)$ be a graph-matroid pair, where M is a linear matroid. Recall that M is also used to refer to a given linear representation of the matroid. For the sake of clarity, we use v_M to refer explicitly to the column vector associated with a vertex $v \in V(H)$. When it is clear from context, we use v and v_M interchangeably.

LEMMA 3.4 (see [24, Proposition 4.2]). *Let $P = (H, M)$ be a graph-matroid pair and $v \in V(H)$ such that the vector v_M is a co-loop in M, where M is a linear matroid. Let $P' = (H, M')$ be the graph-matroid pair obtained by moving v_M to a vector $v_{M'}$ such that in the matroid M', $v_{M'}$ is in general position on a flat containing the neighbors of v, $N_H(v)$. Then $\tau(P') = \tau(P)$.*

Proof. Note that the operation in the statement of the lemma does not change the graph H. The only change occurs in the matroid, where we map a co-loop v_M to a vector lying in the span of its neighbors. It is clear that such an operation does not increase the rank of any vertex cover. Indeed, given a vertex cover T of H, in case it excludes v, the rank of T is the same in both M and M', and otherwise, since v_M is a co-loop, the rank of T cannot increase when M is modified by replacing v_M with *any* other vector. Thus, $\tau(P') \leq \tau(P)$.

For the other inequality, let T be the set of vectors corresponding to a minimum rank vertex cover of the graph H in the graph-matroid pair P' (where we have replaced the vector v_M by the vector $v_{M'}$). In what follows, note that as we are working with linear matroids, the closure operation is the linear span. We have the following two cases:

Case 1: $v_{M'} \notin T$. In this case, T has the same rank in M as it has in M'. Thus, $\tau(P') = \text{rank}_{M'}(T) = \text{rank}_M(T) \geq \tau(P)$.

Case 2: $v_{M'} \in T$. Here, we have two subcases:

- If $v_{M'} \notin \overline{T \setminus \{v_{M'}\}}$, then note that $\tau(P') = \text{rank}_{M'}(T) = \text{rank}_{M'}(T \setminus \{v_{M'}\}) + 1 = \text{rank}_M((T \setminus \{v_{M'}\}) \cup \{v_M\}) \geq \tau(G)$. The third equality follows because v_M is a co-loop.
- If $v_{M'} \in \overline{T \setminus \{v_{M'}\}}$, then as $v_{M'}$ is in general position on a flat containing its neighbors, by definition this means that all of the neighbors of $v_{M'}$ are also present in $\overline{T \setminus \{v_{M'}\}}$. Since v_M and $v_{M'}$ have the same neighbors, as the graph H has not been modified, all of the neighbors of v_M belong to $\overline{T \setminus \{v_{M'}\}}$. Thus, $\overline{T \setminus \{v_{M'}\}}$ is a vertex cover of H. Therefore, $\tau(P') = \text{rank}_{M'}(T) = \text{rank}_{M'}(\overline{T}) = \text{rank}_{M'}(\overline{T \setminus \{v_{M'}\}}) = \text{rank}_M(\overline{T \setminus \{v_{M'}\}}) \geq \tau(P)$. The second equality crucially relies on the observation that the rank of a set is equal to the rank of the span of the set.

This completes the proof of the lemma. ∎

LEMMA 3.5 (see [24, Proposition 4.3]). *Let $P = (H, M)$ be a graph-matroid pair, and let v be a vertex of H such that v is not a loop and v is contained in the flat spanned by its neighbors. Let $P' = P/v$. Then $\tau(P') = \tau(P) - 1$.*

Proof. Recall that the contraction of a vertex v in P results in the graph-matroid pair $P' = (H', M') = (H \setminus v, M/v_M)$; i.e., the vertex is deleted from the graph and contracted in the matroid.

We first prove that $\tau(P) \leq \tau(P')+1$. Let T be a minimum rank vertex cover in P', i.e., $\text{rank}_{M'}(T) = \tau(P')$. Let W be a maximum sized independent set in $\mathcal{I}(M')$ contained in T. Then, by the definition of contraction, $W \cup \{v\}$ is a maximum sized independent set in $\mathcal{I}(M)$ contained in $T \cup \{v\}$. Moreover, $T \cup \{v\}$ is a vertex cover in H, and therefore we get that $\tau(P) \leq \text{rank}_M(T \cup \{v\}) = |W \cup \{v\}| = \text{rank}_{M'}(T)+1 = \tau(P')+1$.

Now we prove that $\tau(P') \leq \tau(P) - 1$. Assume that T is a minimum rank vertex cover of P. In case $v \notin T$, it holds that all the neighbors of v must belong in T to cover edges incident to v. By our assumption, v is in the span of its neighbors in M. Therefore, in any case, v necessarily belongs to the span of T. Note that $T \setminus \{v\}$ is a vertex cover of H'. By Lemma 2.6, we have that $\tau(P) = \text{rank}_M(T) = \text{rank}_{M'}(T \setminus \{v\}) + 1 \geq \tau(P') + 1$. This completes the proof. ∎

3.2. Rank reduction. In this section we explain the first step of our compression algorithm. Formally, we want to solve the following problem.

RANK REDUCTION
Input: An instance $(G, M = I_n, \mu(G) + k)$ of RANK VERTEX COVER, where $n = |V(G)|$.
Output: An equivalent instance (G', M', ℓ) such that the number of rows in M' is at most $\mathcal{O}(k^{3/2})$.

Here, we give a randomized polynomial-time algorithm for RANK REDUCTION. More precisely, along with the input of RANK REDUCTION, we are given an error bound $\varepsilon > 0$, and the objective is to output a "small" equivalent instance with probability at least $1 - \varepsilon$. We begin by stating the well-known crown decomposition, which is used as a reduction rule.

DEFINITION 3.6 (crown decomposition). *A* crown decomposition *of a graph G is a partitioning of $V(G)$ into three parts C, H, and R such that the following hold:*

- *C and H are nonempty.*
- *C is an independent set.*
- *There are no edges between vertices of C and R. That is, H separates C and R.*
- *Let E' be the set of edges between vertices of C and H. Then E' contains a matching of size $|H|$.*

Using the decomposition above, we get the following reduction rule. For correctness, we refer the reader to [9, section 2.3].

REDUCTION RULE 1 (crown reduction). *For an instance (P, ℓ) of* RANK VERTEX COVER *with $P = (G, I_{|V(G)|})$, if G has a crown decomposition (C, H, R), then return $(P' = P \setminus (H \cup C), \ell' = \ell - |H|)$.*

If a graph G has a crown decomposition (C, H, R), then there is an optimum vertex cover containing H. Any maximum matching of G can be modified to give another maximum matching of G which matches every vertex of H to some vertex in C; this gives us $\mu(G - (H \cup C)) \geq \mu(G) - |H|$. Therefore, for the output instance (P', ℓ') in Reduction Rule 1, $\ell' - \mu(G') \leq \ell - \mu(G)$, where $G' = G - (H \cup C)$. There exists a polynomial-time algorithm which produces an induced subgraph of the input graph G such that the crown reduction is not applicable on it; we refer the reader to [31, section 4, Theorem 6] for details. We call a graph *crown reduced* if crown reduction is not applicable to it. The rule above is applied to exhaustion once before any of the rules described below are applied. Next, we state a reduction rule that reduces the rank by 2.

REDUCTION RULE 2 (vertex deletion). *Let (P, ℓ) be an instance of* RANK VERTEX COVER*, where $P = (G, M)$ is a graph-matroid pair. Let $v \in V(G)$ be a vertex such that v_M is a co-loop in M and the flat spanned by its neighbors $N_G(v)$ is nonzero. Let M_1 be the matrix obtained after moving v_M to a vector v_{M_1} which is in general position on the flat spanned by $N_G(v)$ in the matroid M_1. Let $P_1 = (G, M_1)$, and let $P' = P_1 / v_{M_1}$. Then output $(P', \ell - 1)$.*

LEMMA 3.7. *Reduction Rule* 2 *is safe.*

Proof. We need to show that (P, ℓ) is a YES-instance if and only if $(P', \ell - 1)$ is a YES-instance, which follows from Lemmas 3.4 and 3.5. ∎

LEMMA 3.8. *Let (P, ℓ) be an instance of* RANK VERTEX COVER*, where $P = (G, M)$ is a graph-matroid pair. Let $(P', \ell - 1)$ be the output of Reduction Rule* 2*, where $P' = (G', M')$. Then* $\mathrm{rank}(M') = \mathrm{rank}(M) - 2$.

Proof. In Reduction Rule 2, we move a co-loop v_M of M to a vector v_{M_1}, obtaining a matrix M_1. If Reduction Rule 2 is applicable, the rank of flat spanned by neighbors of v_M has rank at least 1. So, by Observation 1, v_{M_1} is not a loop in M_1. As $M' = M_1/v_{M_1}$, by Observation 3, we get $\mathrm{rank}(M') = \mathrm{rank}(M_1) - 1 = \mathrm{rank}(M) - 2$. ∎

Now, we will explain how to apply Reduction Rule 2 efficiently. Later we will explain (Lemma 3.22) how to keep the bit length of each entry in the matrix bounded by a polynomial in k.

We first elaborate the effect of contracting one element on the size of representing matrix. To contract an element e in a matroid M, we perform row reduction such that there is exactly one nonzero entry in the column corresponding to e in M. If row r is the one containing the only nonzero entry in column e in M, then the contracted matroid is represented by the matrix obtained from M by deleting row r and column e from it. We can do this step in a straightforward manner; it is similar to one step of Gaussian elimination for row reduction of a matrix. We first fix a nonzero row element of e as a pivot. Suppose, without loss of generality, that the first element e_1 of e is nonzero. Next, to make any other row element e_j in column e equal to zero, we multiply the jth row of M by e_1 and subtract from it the product of the first row of M with e_j. Hence, we get the following observation.

Observation 4. Let e be a nonloop element in a linear matroid M with integer entries. If each entry in the representation M has an absolute value at most m, then there is a polynomial-time computable representation of M/e over integers with each entry at most $2m^2$ in absolute value.

LEMMA 3.9. *Let M be a linear matroid of rank r represented over integers with $|E(M)| = n$, and let $p \geq 2^n$ be an integer. Then Reduction Rule* 2 *can be applied in polynomial time with success probability at least $1 - \frac{2^n}{p}$. If the longest entry in the matrix M has an absolute value m, then the longest entry in the output matrix is at most $2(mnp)^2$ in absolute value after applying Reduction Rule* 2*. Moreover, the output matrix is over integers.*[1]

Proof. Suppose Reduction Rule 2 is applied to a co-loop v. We first show how to find a vector in general position which replaces the co-loop v. Let F be the set of columns in M corresponding to $N_G(v)$. Using formal indeterminates $x = \{x_h : h \in F\}$, obtain a vector $g(x) = \sum_{h \in F} x_h h$. Suppose the values of the indeterminates have been fixed to some numbers x^* such that for any independent set $I \in \mathcal{I}(M)$ which does not span F, $I \cup \{g(x^*)\}$ is also independent. Using Lemma 2.3, we see that $g(x^*)$ is in general position on $\overline{F}$.

Let I be an independent set which does not span F. We need to select x in such a way that $D_{R,I}(x) = \det(M[R, I \cup \{g(x)\}])$ is not identically zero for some R. First of all, note that there is a choice of R for which the polynomial $D_{R,I}(x)$ is not identically zero and has total degree 1. This is so because $D_{R,I}(x) = \sum_{h \in F} x_h \det(M[R, I \cup \{h\}])$; if it is identically zero for every R, then $\forall h \in F$ we have $\det(M[R, I \cup \{h\}]) = 0$, implying that every element $h \in F$ is spanned by I. Thus, this case does not arise due to the choice of I. Let us fix this choice of rows to be R for the rest of the proof. If we choose $x \in [p]^{|F|}$ uniformly at random, for some number p, then the probability

[1] We remark that we are unaware of a procedure to derandomize the application of Reduction Rule 2.

that $D_{R,I}(x) = 0$ is at most $\frac{1}{p}$ by the Schwartz–Zippel lemma. The number of independent sets in M which do not span F is at most 2^n. Applying the union bound, the probability that $D_{R,I}(x) = 0$ for some $I \in \mathcal{I}(M)$ is at most $\frac{2^n}{p}$. Therefore, the success probability is at least $1 - \frac{2^n}{p}$.

Suppose each entry in M has absolute value at most m. The procedure of finding a point in general position takes polynomial time, and the longest entry in the column which replaces v has absolute value at most mnp, as at most n of the columns are added together after multiplying them by a factor of at most p. Combining the previous statement with Observation 4 gives us the claimed entry sizes and the running time. ∎

In the very first application of Reduction Rule 2 (when the input matrix is I_n), the lemma above tells us that the numbers may become $\mathcal{O}(n^2p^2)$. On applying the rule again and again, the bit length of entries could become exponential due to Gaussian elimination performed for contracting the elements in the matroid. The combined effect of contracting several elements can make the numbers very large. To circumvent this, suppose we are given a linear matroid $(U, \mathcal{I})$ of *low* rank and where the ground set U is *small*, along with a representation matrix M over the field $\mathbb{R}$. We show that for a randomly chosen *small* prime q, the matrix M mod q, obtained by replacing each entry of M by its remainder on division by q, is also a linear representation of M (see Lemma 3.13). To prove this result, we first observe that for any number n, the number of distinct prime factors is bounded by $\mathcal{O}(\log n)$.

Observation 5. The number of distinct prime factors of any number n is at most $log_2 n$.

The well-known prime number theorem implies the following.

PROPOSITION 3.10. *There is a constant c such that the number of distinct prime numbers smaller than or equal to n, denoted by $\pi(n)$, is at least $c\frac{n}{\log n}$.*

Moreover, we can generate a prime number in polynomial time with a good success probability as shown by the following.

PROPOSITION 3.11 (folklore). *Given a number N and a real number $\zeta \in (0, 1]$, there is a randomized polynomial-time algorithm which generates a prime number at most N uniformly at random with failure probability less than ζ.*

Proof. The probability that a randomly generated number less than N is a prime is at least $\frac{\pi(N)}{N} \geq \frac{c}{\log N}$ by Proposition 3.10. To decrease the probability of failure to less than ζ, we generate at most $\mathcal{O}(\log \frac{1}{\zeta} \log N)$ random numbers and test each of them for primality using the AKS algorithm [1]. If one of the generated numbers is a prime, we return it; otherwise, we return failure after exhausting the allowed number of trials. ∎

In what follows, we also need the following general lemma about linear matroids.

LEMMA 3.12 (see [15]). *Let M be an $a \times b$ matrix representing some matroid. If M' is a matrix consisting of a row basis of M, then M' represents the same matroid as M.*

Assume that a given matroid representation M has size $r' \times s$, but the rank of the matroid is some integer $r < r'$. By Lemma 3.12, we can simply keep a row basis of the representation matrix and discard the other rows to get a representation matrix of size $r \times s$. A row basis can be easily identified by row reducing the matrix M into a matrix M_{rred} in polynomial time [3] and then keeping the rows in M which

correspond to nonzero rows in M_{rred}. Note that this operation does not increase the size of new representation of M.

We also state the following inequality to be used in the next lemma.

Observation 6. For $a, b \in \mathbb{R}$ with $a \geq 0$ and $b \geq 1$, we have $a + b \leq 2(a+1)b$.

LEMMA 3.13. *Let $X = (U, \mathcal{I})$ be a rank r linear matroid representable by an $r \times n$ matrix M over $\mathbb{R}$ with each entry an integer between $-\frac{n^{c'n}}{\delta}$ and $\frac{n^{c'n}}{\delta}$ for some constants c' and δ, where $\delta \in (0,1]$. For every $\varepsilon \in (0,1]$, there is a number $c \in \mathcal{O}(1+\log\frac{1}{\varepsilon})$ such that for a prime number q chosen uniformly at random from the set of prime numbers smaller than or equal to $c\frac{n^{2r+3}(n\log n+\log(1/\delta))^2}{\varepsilon}$, the matrix $M_q = M \mod q$ over $\mathbb{R}$ represents the matroid X with probability at least $1-\frac{\varepsilon}{n}$.*

Proof. To prove that M_q is a representation of X (with high probability), it is enough to show that for any basis $B \in \mathcal{B}(X)$, the corresponding columns in M_q are linearly independent. For this purpose, consider some basis $B \in \mathcal{B}(X)$. Since B is an independent set in M, we have that the determinant of the square matrix $M[\star, B]$, denoted by $\det(M[\star, B])$, is nonzero. The determinant of $M_q[\star, B]$ is equal to $\det(M[\star, B]) \mod q$. Let $a = \det(M[\star, B])$, and let $b = a \mod q$. The value of b is equal to zero only if q is a prime factor of a. Since the absolute value of each entry in M is at most $n^{c'n}(1/\delta)$, the absolute value of a is upper bounded by $r!n^{c'nr}(1/\delta)^r$. By Observation 5, the number of prime factors of a is at most $\log(r!)+c'nr\log n+r\log\frac{1}{\delta}$. As the rank of X is r, the number of bases in X is at most n^r. Hence, the cardinality of the set

$$F = \{z : z \text{ is a prime factor of } \det(M[\star, B]) \text{ for some } B \in \mathcal{B}(X)\}$$

is at most $n^r \cdot (\log(r!) + c'nr\log n + r\log(1/\delta)) \leq c_1 n^{r+1}(n\log n + \log(1/\delta))$ for some constant c_1.

By Proposition 3.10, there is a constant c_2 such that the number of prime numbers less than or equal to $c\frac{n^{2r+3}(n\log n+\log(1/\delta))^2}{\varepsilon}$ is at least

$$t = c_2 c \frac{n^{2r+3}(n\log n + \log(1/\delta))^2}{\varepsilon \log(c\frac{n^{2r+3}(n\log n+\log(1/\delta))^2}{\varepsilon})}.$$

The probability that M_q is not a representation of X (denote it by $M_q \not\equiv M$) is

$$\begin{aligned}
\Pr[M_q \not\equiv M] = \Pr[q \in F] &\leq \frac{|F|}{t} \\
&\leq \frac{c_1}{c_2 c} \cdot \frac{\log(c\frac{n^{2r+3}(n\log n+\log(1/\delta))^2}{\varepsilon})}{n^{r+1}(n\log n + \log(1/\delta))} \cdot \frac{\varepsilon}{n} \\
&= \frac{c_1}{c_2 c} \cdot \frac{\log(c\frac{nv_{n,\delta,r}^2}{\varepsilon})}{v_{n,\delta,r}} \cdot \frac{\varepsilon}{n} \qquad \text{where } v_{n,\delta,r} = n^{r+1}(n\log n + \log(1/\delta)) \\
&\leq \frac{2c_1(1+\log\frac{1}{\varepsilon})}{c_2 c} \cdot \frac{\log(cnv_{n,\delta,r}^2)}{v_{n,\delta,r}} \cdot \frac{\varepsilon}{n} \qquad \text{using Observation 6.}
\end{aligned}$$

For any $\varepsilon \in (0,1]$ and $r \geq 0$, there is a number $c \in \mathcal{O}(1+\log\frac{1}{\varepsilon})$ such that the above probability is at most $\frac{\varepsilon}{2n}$. To complete the proof, we use Proposition 3.11 to generate a prime number of required size with failure probability at most $\frac{\varepsilon}{2n}$. If the algorithm in Proposition 3.11 fails to return a prime, then we output a small fixed matrix and exit. The overall failure probability is at most $\frac{\varepsilon}{n}$. This completes the proof of the lemma. ∎

By combining Lemmas 3.9, 3.12, and 3.13, we can apply Reduction Rule 2 such that each entry in the output representation matrix has bounded value.

LEMMA 3.14. *Given $\varepsilon \in (0,1]$, Reduction Rule 2 can be applied in polynomial time with success probability at least $1-\frac{\varepsilon}{n}$. Moreover, each entry in the output representation matrix of rank r is at most $c\frac{n^{2r+3}(n\log n+\log(1/\varepsilon^8))^2}{\varepsilon}$, where $c \in \mathcal{O}(1+\log\frac{1}{\varepsilon})$.*

Proof. Let M be the input representation matrix. The proof is by induction on the steps performed for Reduction Rule 2. Each *step* consists of an application of Lemma 3.9, Lemma 3.12, and then Lemma 3.13 in order. The invariant at the end of the steps is that the absolute values of matrix entries are bounded by the value of q as given in Lemma 3.13 for $\delta = \varepsilon^8$. Before the application of first step, the matrix consists of I_n; therefore, the sizes are bounded as claimed. Let $\epsilon' = \varepsilon/(2n)$. We apply Lemma 3.9 with $p = \lceil \frac{2^n}{\epsilon'} \rceil$ to a co-loop. Let M' be the output representation matrix of Lemma 3.9. By Lemma 3.9, Reduction Rule 2 succeeds with probability at least $1-\epsilon'$, and the absolute values of individual entries are at most

$$\begin{aligned}
2(qnp)^2 &\le q^2\frac{1}{\varepsilon^2}n^4 2^{2n+5} \quad \text{using } p \le \frac{2^{n+2}n}{\varepsilon} \\
&\le c^2\frac{2^{2n+5}n^{4r+10}(n\log n+\log(1/\varepsilon^8))^4}{\varepsilon^4} \\
&\le c^2\frac{2^{2n+6}n^{4r+18}(1+8\log(1/\varepsilon))^4}{\varepsilon^4} \quad \text{using Observation 6 and } \log n \le n \\
&\le \frac{(1+\log(1/\varepsilon))^4}{\varepsilon^4}n^{c'n} \quad \text{for some constant } c' \\
&\le \frac{n^{c'n}}{\varepsilon^8} \quad \text{using } 1+\log\frac{1}{\varepsilon} \le \frac{1}{\varepsilon}.
\end{aligned}$$

So, the invariant holds, and if there is a co-loop, we can apply Lemma 3.13 for Reduction Rule 2 again, as we have the bit sizes in the required form. ∎

We would like to apply Reduction Rule 2 as many times as possible in order to obtain a "good" bound on the rank of the matroid. However, for this purpose, after applying Reduction Rule 2 with respect to some co-loop of the matroid, (i) some other co-loops need to remain co-loops, and (ii) Reduction Rule 2 should be applicable on them. To achieve the first goal, instead of applying Reduction Rule 2 arbitrarily, we choose vectors v_M whose vertices belong to a predetermined independent set of the graph. To understand the advantage behind a more careful choice of the vectors v_M, suppose that we are given an independent set U in the graph G such that every vertex in it is a co-loop in the matroid. Then, after we apply Reduction Rule 2 with one of the vertices in U, it holds that every other vertex in U is still a co-loop (by Lemma 2.4 and Observation 3).

To achieve the second goal stated above, we need to ensure that neighborhoods of remaining co-loops are nonzero. This property is not true for all graphs. For example, in a complete bipartite graph $G = (A \cup B, E)$, with partite sets A and B satisfying $|A| > |B|$, we cannot apply Reduction Rule 2 on all the elements in A, as the rank of B will become zero before all the elements have been processed. We next show that the second goal is achievable in our case, as our graph is crown reduced.

LEMMA 3.15. *For a matroid $X = (U, \mathcal{I})$, let $C \subseteq U$ and $A, B \subseteq U \setminus C$. If $\text{span}_X(A) \subseteq \text{span}_X(B)$, then $\text{span}_{X/C}(A) \subseteq \text{span}_{X/C}(B)$.*

Proof. It suffices to prove the lemma for one element $c \in C$; the general statement follows from induction on $|C|$. Let $A' \subseteq A$ be a basis of A in $X/\{c\}$. By Observation 2, $A' \cup \{c\}$ is independent in X. From the statement of the lemma, we get $A' \subseteq \text{span}_X(B)$. By Lemma 2.7, we have $\text{span}_{X/\{c\}}(B) = \text{span}_X(B \cup \{c\}) \setminus \{c\}$; therefore, A' is contained in $\text{span}_{X/\{c\}}(B)$. ∎

It is possible to compute all the points in general position on their neighborhood before any matroid contraction. Next we show that matroid contraction does not affect the status of a point in general position.

LEMMA 3.16. *For $P = (G, M)$, let $u, v \in G$ be two distinct vertices. If u, v are in general position on $N_G(u)$ and $N_G(v)$, respectively, in M, then u is in general position on $N_G(u)$ in $M/\{v\}$.*

Proof. Suppose u is not in general position on $\text{span}_{M/\{v\}}(N(u))$; then there exists $F \subseteq E(M) \setminus \{u, v\}$ such that $u \in \text{span}_{M/\{v\}}(F)$ and $\text{span}_{M/\{v\}}(N_G(u)) \not\subseteq \text{span}_{M/\{v\}}(F)$. Since $\text{span}_{M/\{v\}}(F) = \text{span}_M(F \cup \{v\}) \setminus \{v\}$ (by Lemma 2.7), we get $u \in \text{span}_M(F \cup \{v\}) \setminus \{v\}$, which implies that $u \in \text{span}_M(F \cup \{v\})$. Similarly, by Lemma 2.7 and $\text{span}_{M/\{v\}}(N_G(u)) \not\subseteq \text{span}_{M/\{v\}}(F)$, we also have that (i) $\text{span}_M(N_G(u) \cup \{v\}) \setminus \{v\} \not\subseteq \text{span}_M(F \cup \{v\}) \setminus \{v\}$. In what follows, we show that $\text{span}_M(F \cup \{v\})$ is a flat for which u fails the general position condition. We have already proved that $u \in \text{span}_M(F \cup \{v\})$. From the statement (i), we have $\text{span}_M(N_G(u) \cup \{v\}) \not\subseteq \text{span}_M(F \cup \{v\})$. If $\text{span}_M(N_G(u)) \subseteq \text{span}_M(F \cup \{v\})$, then we have $\text{span}_M(N_G(u) \cup \{v\}) \subseteq \text{span}_M(F \cup \{v\})$. Therefore, it must be the case that $\text{span}_M(N_G(u)) \not\subseteq \text{span}_M(F \cup \{v\})$. This contradicts the assumption that u is in general position on $N_G(u)$ in M. ∎

LEMMA 3.17. *Let (P, ℓ) with $P = (G, M)$ be an instance of* RANK VERTEX COVER*, and let S be any independent set of G. If G is* crown reduced*, then Reduction Rule* 2 *is applicable on every $s \in S$.*

Proof. The matroid before any contraction is $M = I_n$. Let $D \subseteq S$ be an ordered sequence of elements such that the rank of $J \subseteq V(G) \setminus S$ becomes zero after application of Reduction Rule 2 on the elements of D. If there is some other element $s \in S \setminus D$ with $N_G(s) \subseteq J$, then we would not be able to apply Reduction Rule 2 on it. To simplify the discussion, we assume that elements in D refer to corresponding points in the flat of their neighborhoods; moreover, the points in general position can all be computed initially before any matroid contraction by Lemma 3.16. Due to commutativity of matroid contraction, the order of contraction of elements in D does not affect the final matroid. Therefore, any permutation of elements in D will result in the same final matroid upon contraction. Let $C = \{c_1, c_2, \ldots, c_p\} \subseteq D$ be a *shortest* length subsequence which results in rank of a subset of $V(G) \setminus S$ becoming zero upon contraction. Let $H \subseteq V(G) \setminus S$ be the *largest* cardinality set whose rank became zero after the contraction of C. Given a permutation Π of $\{1, \ldots, p\}$, let M_i denote the matroid obtained after contraction of the elements in C indexed by the first i indices in $\Pi(\{1, \ldots, p\})$, and let rank_i and span_i denote the rank and span in M_i, respectively.

Claim 3.18. *For any $c_i \in C$, if there exists a permutation Π of C such that $\text{rank}_{\Pi(i)}(H) = \text{rank}_{\Pi(i)-1}(H) - 1$, then $N_G(c_i) \subseteq H$.*

Proof. Assume $N_G(c_i) \not\subseteq H$, and let $j = \Pi(i)$. As $\text{rank}_j(H) = \text{rank}_{j-1}(H) - 1$, we have $c_i \in \text{span}_{j-1}(H)$ by Lemma 2.5. Also, as c_i is in general position on $\text{span}_{j-1}(N_G(c_i))$ in M_{j-1}, we have $\text{span}_{j-1}(N_G(c_i)) \subseteq \text{span}_{j-1}(H)$. By Lemma 3.15,

$\text{span}_p(N_G(c_i)) \subseteq \text{span}_p(H)$, which implies that $N_G(c_i) \cup H$ is a larger cardinality set with rank equal to zero in M_p, a contradiction to our choice of H. ∎

Claim 3.19. $N(C) \subseteq H$.

Proof. For any $c_i \in C$, pick a Π with $\Pi(i) = p$. If c_i does not change the rank of H in this order, then $C \setminus \{c_i\}$ is a shorter sequence. Hence, Claim 3.18 gives us $N_G(c_i) \subseteq H$. ∎

Clearly, C does not have any edges to vertices in $V(G) \setminus (C \cup H)$. Therefore, there cannot be any matching from H to C of size $|H|$, as G is crown reduced. Consider the bipartite graph B with bipartition $H \uplus C$ and $E(B)$ is the set of edges in G between C and H. By Hall's theorem, there is a nonempty set $H^* \subseteq H$ such that $|H^*| > |N_B(H^*)|$. Let $C^* = N_B(H^*)$. We first contract the elements in $C \setminus C^*$. These do not decrease the rank of the set H^* upon contraction due to Lemma 2.4 and Observation 3 along with the fact that $N_B(C \setminus C^*) \cap H^* = \emptyset$; in particular, elements of H^* remain co-loops. By Lemma 2.5, the rank of H^* after contraction by C^* is at least $|H^*| - |N_B(H^*)| > 0$. This is not possible, as H^* is a subset of a rank zero set H in the matroid $M_p = M/C$. ∎

In order to find a large independent set (in order to apply Reduction Rule 2 many times), we use the following two known algorithmic results about Vertex Cover Above MM.

Lemma 3.20 (see [23]). *There is a* $2.3146^k \cdot n^{\mathcal{O}(1)}$*-time deterministic algorithm for* Vertex Cover Above MM.

Recall that for a graph G, we let $\beta(G)$ denote the vertex cover number of G.

Lemma 3.21 (see [25]). *For any* $\epsilon > 0$*, there is a randomized polynomial-time approximation algorithm that, given a graph* G*, outputs a vertex cover of* G *of cardinality at most* $\mu(G) + \mathcal{O}(\sqrt{\log n})(\beta(G) - \mu(G))$ *with probability at least* $1 - \epsilon$.

We are now ready to give the main lemma of this subsection.

Lemma 3.22. *There is a polynomial-time randomized algorithm that, given an instance* $(G, M = I_n, \mu(G) + k)$ *of* Rank Vertex Cover *and* $\hat{\varepsilon} > 0$ *with probability at least* $1 - \hat{\varepsilon}$*, outputs an equivalent instance* (G', M', ℓ) *of* Rank Vertex Cover *such that* ℓ *and the number of rows in* M' *are both at most* $\mathcal{O}(k^{3/2})$*. Here,* M' *is an integer matrix over the field* $\mathbb{R}$*, where each entry is* $\mathcal{O}(k^{5/2} + \log(1/\hat{\varepsilon}))$ *bits long.*

Proof. On the input instance, apply crown reduction exhaustively. Recall that $n = |V(G)|$. If $k \leq \log n$, then we use Lemma 3.20 to solve the problem in polynomial time. Next, we assume that $\log n < k$. Let $\delta = \hat{\varepsilon}/2$.

Now, by Lemma 3.21, we know that there exists an algorithm which in polynomial time outputs a vertex cover of G of cardinality at most $\mu(G) + \mathcal{O}(\sqrt{\log n})(\beta(G) - \mu(G))$ with probability at least $1 - \delta$, where c' is some constant. Run this algorithm on G. If the algorithm signals failure or outputs a vertex cover Y of G such that $|Y| > \mu(G) + c'\sqrt{\log n} \cdot k$, then output an arbitrary constant-sized No-instance of Rank Vertex Cover (the probability of this happening despite the input instance being a Yes-instance is at most δ). Therefore, we can assume that $|Y| \leq \mu(G) + c'\sqrt{\log n} \cdot k \leq \mu(G) + c' \cdot k^{3/2}$; let $S = V(G) \setminus Y$. Since Y is a vertex cover of G, we have that S is an independent set of G. Clearly, $|S| \geq n - (\mu(G) + c' \cdot k^{3/2})$. Since $M = I_n$, all the elements of M, including the ones in S, are co-loops in M. Now, we apply Reduction

Rule 2 with the elements of S (one by one). By Lemma 2.4 and Observation 3, after each application of Reduction Rule 2, the remaining elements in S are still coloops. In particular, Reduction Rule 2 is applied $|S|$ times. Let (G', M', ℓ) be the instance obtained after these $|S|$ applications of Reduction Rule 2 using Lemma 3.14 (substituting $\varepsilon = \delta$ in Lemma 3.14).

By Lemmas 3.8 and 3.17, application of Reduction Rule 2 reduces the rank by 2 for each vertex in S. Hence,

$$\begin{aligned}\operatorname{rank}(M') &= \operatorname{rank}(M) - 2|S| \\ &\leq n - 2\left(n - (\mu(G) + c' \cdot k^{3/2})\right) \\ &= -n + 2\mu(G) + 2c' \cdot k^{3/2} \leq 2c' \cdot k^{3/2} \qquad \text{(because } 2\mu(G) \leq n\text{)}.\end{aligned}$$

During each application of Reduction Rule 2, by Lemma 3.12, we can assume that the number of rows in the representation matrix is exactly same as the rank of the matrix. Now, we return (G', M', ℓ) as the output. Notice that the number of rows in M' is at most $\mathcal{O}(k^{3/2})$. By Lemma 3.5, the rank of vertex cover falls by $|S|$. Therefore, $\ell = \mu(G) + k - |S| \leq k + c' \cdot k^{3/2}$.

Now, we analyze the probability of success. As finding the approximate vertex cover Y using Lemma 3.21 fails with probability at most $\delta = \frac{\hat{\varepsilon}}{2}$, in order to get the required success probability of $1 - \hat{\varepsilon}$, $|S|$ applications of Reduction Rule 2 should succeed with probability at least $1 - \frac{\hat{\varepsilon}}{2}$. We suppose that the matrix $M = I_n$ is over the field $\mathbb{R}$. Recall that the instance (G', M', ℓ) is obtained after $|S|$ applications of Reduction Rule 2. The failure probability of each application of Reduction Rule 2 is at most $\frac{\delta}{n}$. Hence, by union bound, the probability of failure in at least one application of Reduction Rule 2 is at most δ. Hence, the total probability of success is at least $1 - (\delta + \delta) = 1 - \hat{\varepsilon}$. By Lemma 3.14, each entry in the output representation matrix is at most $c\frac{n^{2r+3}(n \log n + 8 \log(2/\hat{\varepsilon}))^2}{\hat{\varepsilon}/2}$. Hence, the number of bits required to represent an entry in M' is at most $\mathcal{O}(r \log n + \log(2/\hat{\varepsilon})) = \mathcal{O}(k^{5/2} + \log(1/\hat{\varepsilon}))$. ∎

The rank reduction of the input matroid reduces the number of rows to a function of parameter, but the number of vertices and the number of columns in the matroid is $|V(G')| = n - |S| \leq \mu(G) + c' \cdot k^{3/2}$. This is not sufficient for a compression. The next section shows how to reduce the number of edges to a function of k using the matroid.

3.3. Graph reduction. In the previous subsection, we have seen how to reduce the number of rows in the matroid. In this subsection, we move to the second step of our compression algorithm, that is, to reduce the size of the graph. The value of k in the following is the same as in the previous sections; it is the above-guarantee parameter. Formally, we want to solve the following problem.

Graph Reduction
Input: An instance (G', M, ℓ) of Rank Vertex Cover such that ℓ and the number of rows in M are both at most $\mathcal{O}(k^{\frac{3}{2}})$.
Output: An equivalent instance (G'', M', ℓ) such that $\lvert V(G'')\rvert, \lvert E(G'')\rvert \leq \mathcal{O}(k^3)$.

Here, we give an algorithm to reduce the number of edges in the graph. Having reduced the number of edges, we also obtain the desired bound on the number of vertices (as isolated vertices are discarded). Towards this, we first give some definitions and notations. In this section, we use $\mathbb{F}$ to denote either a finite field or $\mathbb{R}$.

DEFINITION 3.23 (symmetric square). *For a set of column vectors S over a field $\mathbb{F}$, the* symmetric square*, denoted by $S^{(2)}$, is defined as $S^{(2)} = \{uv^T + vu^T : u, v \in S\}$, where the operation is matrix multiplication. The elements of $S^{(2)}$ are matrices. We can define the rank function $r^{(2)} : 2^{S^{(2)}} \to \mathbb{N}$ by treating the matrices as "long" vectors over the field $\mathbb{F}$.*

With a rank function $r^{(2)}$, the pair $(S^{(2)}, r^{(2)})$ forms a matroid. For details we refer the reader to [24].

The *dot product* of two column vectors $a, b \in \mathbb{F}^n$ is the scalar $a^T b$ and is denoted by $\langle a, b\rangle$. Two properties of dot product are (i) $\langle a, b\rangle = \langle b, a\rangle$ and (ii) $\langle a, b + c\rangle = \langle a, b\rangle + \langle a, c\rangle$.

DEFINITION 3.24. *Given a vector space $\mathbb{F}^d$ and a subspace F of $\mathbb{F}^d$, the* orthogonal space *of F is defined as $F^\perp = \{x \in \mathbb{F}^d \ : \ \langle y, x\rangle = 0$ for all $y \in F\}$.*

To avoid confusion later, we state the following observation, which follows from the fact that the dot product of two column vectors v and w is equal to the scalar $v^T w$.

Observation 7. Let u, v, w be three column vectors. Then $uv^T w = \langle v, w\rangle u$.

DEFINITION 3.25 (2-tuples meeting a flat). *For a flat F in a linear matroid S (here S is a set of vectors), the* set of 2-tuples meeting *F is defined as $F_2 := \{uv^T + vu^T \ : \ v \in F, u \in S\}$.*

For the sake of completeness, we prove the following lemmas using elementary techniques from linear algebra.

LEMMA 3.26 (see [24, Proposition 2.8]). *For any flat F in a linear matroid S with rank function r, it holds that F_2 (the set of 2-tuples meeting F) forms a flat in the matroid $(S^{(2)}, r^{(2)})$.*

Proof. Suppose, by way of contradiction, that F_2 is not a flat. Then there exist $a, b \in S$ such that $e = ab^T + ba^T \in S^{(2)}$ is not in F_2 and

$$r^{(2)}(F_2 \cup \{e\}) = r^{(2)}(F_2).$$

As e lies in the span of F_2, there exist scalars λ_{uv} such that

$$ab^T + ba^T = \sum_{u \in F, v \in S} \lambda_{uv}(uv^T + vu^T). \tag{3.1}$$

Note that neither a nor b belongs to F because if at least one of them belongs to F, then e lies in F_2 (by the definition of F_2). Therefore, $F \neq S$, and it is a proper subspace of S, which implies that $F^\perp$ is nonempty (follows from Proposition 13.2 in [19]). Pick an element $x \in F^\perp$. By right multiplying the column matrix x with the terms in (3.1), we get

$$\begin{aligned} ab^T x + ba^T x &= \sum_{u \in F, v \in S} \lambda_{uv}(uv^T x + vu^T x) \\ \langle b, x\rangle a + \langle a, x\rangle b &= \sum_{u \in F, v \in S} \lambda_{uv}\langle v, x\rangle u + \langle u, x\rangle v \\ &= \sum_{u \in F, v \in S} \lambda_{uv}\langle v, x\rangle u. \end{aligned} \tag{3.2}$$

The second equality follows from Observation 7, and the third equality follows from the fact that $\langle u, x\rangle = 0$ (because $u \in F$ and $x \in F^\perp$). Now, by taking dot

product with x, from (3.2), we have that

$$2\langle a,x\rangle\langle b,x\rangle = \sum_{u\in F, v\in S} \lambda_{uv}\langle v,x\rangle\langle u,x\rangle = 0. \tag{3.3}$$

The last equality follows from the fact that $\langle u,x\rangle = 0$. As the choice of x was arbitrary, (3.2) and (3.3) hold for all $x \in F^{\perp}$.

By (3.3), for all $x \in F^{\perp}$, at least one of $\langle b,x\rangle$ or $\langle a,x\rangle$ is zero. If exactly one of $\langle b,x\rangle$ or $\langle a,x\rangle$ is zero for some $x \in F^{\perp}$, then at least one of a or b is a linear combination of vectors from F (by (3.2)), and hence it belongs to F, which is a contradiction (recall that we have argued that both a and b do not belong to the flat F). Now, consider the case where both $\langle b,x\rangle$ and $\langle a,x\rangle$ are zero for all $x \in F^{\perp}$. Then both a and b belong to $F^{\perp\perp}$. Since $F^{\perp\perp} = F$ (in the case F is a finite dimensional vector space defined over a finite field, see [17, Theorem 7.5]), again we have reached a contradiction. ∎

For a graph-matroid pair $P = (H, M)$ (here, M represents a set of vectors), define $\mathcal{E}(P) \subseteq M^{(2)}$ as $\mathcal{E}(P) = \{uv^T + vu^T : \{u,v\} \in E(H)\}$. Note that $\mathcal{E}(P)$ forms a matroid with the same rank function as the one of $M^{(2)}$. Moreover, the elements of $\mathcal{E}(P)$ are in correspondence with the edges of H. For simplicity, we refer to an element of $\mathcal{E}(P)$ as an edge. Using Lemma 3.26, we prove the following lemma.

LEMMA 3.27 (see [24, Proposition 4.7]). *Let $P = (H, M)$ be a graph-matroid pair, and let $r^{(2)}$ be the rank function of $\mathcal{E}(P)$. For an edge e that is not a co-loop in $(\mathcal{E}(P), r^{(2)})$, it holds that $\tau(P \setminus e) = \tau(P)$.*

Proof. The deletion of edges cannot increase the vertex cover number; thus, $\tau(P \setminus e) \leq \tau(P)$. Next, we show that it also holds that $\tau(P \setminus e) \geq \tau(P)$.

Let T be a vertex cover of $H \setminus e$. Notice that $\overline{T}$ is a flat in M. Denote $e = \{u, v\}$ and $F = \overline{T}$. If at least one of u or v lies in F, then F is a vertex cover of H, and hence $\tau(P \setminus e) \geq \tau(P)$. Hence, to conclude the proof, it is sufficient to show that at least one of u or v lies in F. Suppose, by way of contradiction, that $u, v \notin F$. Then the edge $e = uv^T + vu^T$ does not belong to F_2 (the set of 2-tuples meeting F). By Lemma 3.26, we have that F_2 is a flat in $(M^{(2)}, r^{(2)})$. Since F is a vertex cover of $H \setminus e$, by the definition of F_2 and $\mathcal{E}(P)$, we have that $\mathcal{E}(P) \setminus \{e\} \subseteq F_2$. Recall that e is not a co-loop in $(\mathcal{E}(P), r^{(2)})$. This implies that e belongs to the closure of $\mathcal{E}(P) \setminus \{e\}$, and hence it belongs to its superset F_2. We have thus reached a contradiction. This completes the proof. ∎

Using Lemma 3.27, we get the following bound on the number of edges analogously to Theorem 4.6 in [24].

LEMMA 3.28. *Let (H, M, ℓ) be an instance of* RANK VERTEX COVER *and $r = \mathrm{rank}(M)$. Applying the reduction given by Lemma 3.27 on (H, M) exhaustively results in a graph with at most $\binom{r+1}{2}$ edges.*

Proof. Let $\{v_1, \ldots, v_r\}$ be a column basis of M. By construction, any element in $S^{(2)}$ can be written as a linear combination of elements in $B^{(2)} = \{v_i v_j^T + v_j v_i^T : i, j \in [r]\}$. The set $B^{(2)}$ contains $r + \binom{r}{2} = \binom{r+1}{2}$ elements. Therefore, the rank of the matroid $(\mathcal{E}(P), r^{(2)})$ is at most $\binom{r+1}{2}$.

The reduction given by Lemma 3.27 deletes any edge that is not a co-loop in this matroid. In other words, once the reduction can no longer be applied, every edge is a co-loop in the matroid $(\mathcal{E}(P), r^{(2)})$, and hence the graph has at most $\binom{r+1}{2}$ edges. ∎

Lemma 3.28 bounds the number of edges of the graph. To bound the number of vertices in the graph, we apply the following simple reduction rule.

REDUCTION RULE 3. *Let* (G, M, ℓ) *be an instance of* RANK VERTEX COVER. *For any* $v \in V(G)$ *of degree* 0 *in* G, *output* $(G \setminus v, M \setminus v, \ell)$.

Reduction Rule 3 and Lemma 3.28 lead us to the main result of this subsection.

COROLLARY 3.29. *There is a polynomial-time algorithm which, given an instance* (G', M', ℓ) *of* RANK VERTEX COVER *such that the number of rows in* M *is at most* $\mathcal{O}(k^{\frac{3}{2}})$, *outputs an equivalent instance* (G'', M'', ℓ) *such that* $|V(G'')|, |E(G'')| = \mathcal{O}(k^3)$. *Here,* M'' *is a restriction of* M'.

By combining the corollary above with Lemma 3.22, we get the following result.

THEOREM 3.30. *There is a polynomial-time randomized algorithm that, given an instance* $(G, M = I_n, \mu(G) + k)$ *of* RANK VERTEX COVER *and* $\varepsilon > 0$ *with probability at least* $1 - \varepsilon$, *outputs an equivalent instance* (G', M', ℓ) *of* RANK VERTEX COVER *such that* ℓ *and the number of rows in* M' *are both at most* $\mathcal{O}(k^{3/2})$. *Moreover,* M' *is an integer matrix over the field* $\mathbb{R}$ *containing* $\mathcal{O}(k^7 + k^{4.5} \log \frac{1}{\varepsilon})$ *bits, and* G' *has at most* $\mathcal{O}(k^3)$ *vertices and edges.*

Theorem 3.30 also gives us a polynomial compression of size $\mathcal{O}(k^7 + k^{4.5} \log \frac{1}{\varepsilon})$ for VERTEX COVER ABOVE LP.

4. Conclusion. In this paper, we presented a (randomized) polynomial compression of the VERTEX COVER ABOVE LP problem into the algebraic RANK VERTEX COVER problem. With probability at least $1 - \varepsilon$, the output instance is equivalent to the original instance, and it is of bit length $\mathcal{O}(k^7 + k^{4.5} \log \frac{1}{\varepsilon})$. Here, the probability ε is part of the input. Recall that having our polynomial compression at hand, one also obtains polynomial compressions of additional well-known problems, such as the ODD CYCLE TRANSVERSAL problem, into the RANK VERTEX COVER problem.

Finally, we note that we do not know how to derandomize our polynomial compression, and it is also not known how to derandomize the polynomial kernelization by Kratsch and Wahlström [21]. Thus, to conclude our paper, we would like to pose the following intriguing open problem: Does there exist a deterministic polynomial compression of the VERTEX COVER ABOVE LP problem?

REFERENCES

[1] M. AGRAWAL, N. KAYAL, AND N. SAXENA, *Primes is in P*, Ann. Math., (2004), pp. 781–793.

[2] R. BALASUBRAMANIAN, M. R. FELLOWS, AND V. RAMAN, *An improved fixed-parameter algorithm for vertex cover*, Inform. Process. Lett., 65 (1998), pp. 163–168.

[3] E. H. BAREISS, *Sylvester's identity and multistep integer-preserving Gaussian elimination*, Math. Comp., 22 (1968), pp. 565–578.

[4] J. F. BUSS AND J. GOLDSMITH, *Nondeterminism within P*, SIAM J. Comput., 22 (1993), pp. 560–572, https://doi.org/10.1137/0222038.

[5] L. S. CHANDRAN AND F. GRANDONI, *Refined memorization for vertex cover*, Inform. Process. Lett., 93 (2005), pp. 125–131.

[6] J. CHEN, H. FERNAU, I. A. KANJ, AND G. XIA, *Parametric duality and kernelization: Lower bounds and upper bounds on kernel size*, SIAM J. Comput., 37 (2007), pp. 1077–1106, https://doi.org/10.1137/050646354.

[7] J. CHEN, I. A. KANJ, AND W. JIA, *Vertex cover: Further observations and further improvements*, J. Algorithms, 41 (2001), pp. 280–301, https://doi.org/10.1006/jagm.2001.1186.

[8] J. CHEN, I. A. KANJ, AND G. XIA, *Improved upper bounds for vertex cover*, Theoret. Comput. Sci., 411 (2010), pp. 3736–3756.

[9] M. CYGAN, F. V. FOMIN, L. KOWALIK, D. LOKSHTANOV, D. MARX, M. PILIPCZUK, M. PILIPCZUK, AND S. SAURABH, *Parameterized Algorithms*, Springer, Berlin, 2015.

[10] M. Cygan, M. Pilipczuk, M. Pilipczuk, and J. O. Wojtaszczyk, *On multiway cut parameterized above lower bounds*, ACM Trans. Comput. Theory, 5 (2013), p. 3, https://doi.org/10.1145/2462896.2462899.

[11] H. Dell and D. Van Melkebeek, *Satisfiability allows no nontrivial sparsification unless the polynomial-time hierarchy collapses*, J. ACM, 61 (2014), p. 23.

[12] R. G. Downey and M. R. Fellows, *Fundamentals of Parameterized Complexity*, Texts Comput. Sci., Springer, Cham, Switzerland, 2013.

[13] R. G. Downey, M. R. Fellows, and U. Stege, *Parameterized complexity: A framework for systematically confronting computational intractability*, in Contemporary Trends in Discrete Mathematics: From DIMACS and DIMATIA to the Future, Vol. 49, 1999, pp. 49–99.

[14] S. Garg and G. Philip, *Raising the bar for vertex cover: Fixed-parameter tractability above a higher guarantee*, in Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016, SIAM, Philadelphia, 2016, pp. 1152–1166, https://doi.org/10.1137/1.9781611974331.ch80.

[15] G. Gordon and J. McNulty, *Matroids: A Geometric Introduction*, Cambridge University Press, Cambridge, 2012, https://doi.org/10.1017/CBO9781139049443.

[16] G. Gutin, E. J. Kim, M. Lampis, and V. Mitsou, *Vertex cover problem parameterized above and below tight bounds*, Theory Comput. Syst., 48 (2011), pp. 402–410.

[17] R. Hill, *A First Course in Coding Theory*, Oxford Applied Linguistics, Clarendon Press, Oxford, 1986, https://books.google.co.in/books?id=UTxjBX9lKoMC.

[18] R. Impagliazzo, R. Paturi, and F. Zane, *Which problems have strongly exponential complexity?*, J. Comput. Sys. Sci., 63 (2001), pp. 512–530.

[19] S. Jukna, *Extremal combinatorics: With applications in computer science*, Texts Theoret. Comput. Sci. EATCS Ser., Springer, Berlin, 2011, https://books.google.co.in/books?id=NV3Y8vjWo8kC.

[20] S. Kratsch, *A randomized polynomial kernelization for vertex cover with a smaller parameter*, in 24th Annual European Symposium on Algorithms, ESA 2016, Aarhuss, Denmark, 2016, pp. 59:1–59:17, https://doi.org/10.4230/LIPIcs.ESA.2016.59.

[21] S. Kratsch and M. Wahlström, *Representative sets and irrelevant vertices: New tools for kernelization*, in IEEE 53rd Annual Symposium on Foundations of Computer Science (FOCS-12), T. Roughgarden ed., IEEE Computer Society, Los Alamitos, CA, 2012, pp. 450–459.

[22] M. Lampis, *A kernel of order* $2k - c \log k$ *for vertex cover*, Inform. Process. Lett., 111 (2011), pp. 1089–1091.

[23] D. Lokshtanov, N. Narayanaswamy, V. Raman, M. Ramanujan, and S. Saurabh, *Faster parameterized algorithms using linear programming*, ACM Trans. Algorithms, 11 (2014), p. 15.

[24] L. Lovász, *Flats in matroids and geometric graphs*, Combinatorial Surveys, (1977), pp. 45–86.

[25] S. Mishra, V. Raman, S. Saurabh, S. Sikdar, and C. R. Subramanian, *The complexity of König subgraph problems and above-guarantee vertex cover*, Algorithmica, 61 (2011), pp. 857–881, https://doi.org/10.1007/s00453-010-9412-2.

[26] N. Narayanaswamy, V. Raman, M. Ramanujan, and S. Saurabh, *LP can be a cure for parameterized problems*, in STACS'12 (29th Symposium on Theoretical Aspects of Computer Science), Vol. 14, LIPIcs, 2012, pp. 338–349.

[27] R. Niedermeier and P. Rossmanith, *Upper bounds for vertex cover further improved*, in Annual Symposium on Theoretical Aspects of Computer Science, Springer, Berlin, 1999, pp. 561–570.

[28] J. G. Oxley, *Matroid Theory*, Oxford Graduate Texts in Mathematics, Oxford University Press, New York, 2006.

[29] V. Raman, M. Ramanujan, and S. Saurabh, *Paths, flowers and vertex cover*, in European Symposium on Algorithms, Springer, Berlin, 2011, pp. 382–393.

[30] I. Razgon and B. O'Sullivan, *Almost* 2*-SAT is fixed-parameter tractable*, J. Comput. Sys. Sci., 75 (2009), pp. 435–450.

[31] F. N. Abu-Khzam, M. A. Langston, and W. H. Suters, *Fast, effective vertex cover kernelization: a tale of two algorithms*, 3rd ACS/IEEE International Conference on Computer Systems and Applications, 2005, IEEE, Piscataway, NJ, 2005.