Deterministic Truncation of Linear Matroids

DANIEL LOKSHTANOV, University of Bergen, Norway
PRANABENDU MISRA, University of Bergen, Norway
FAHAD PANOLAN, University of Bergen, Norway
SAKET SAURABH, Institute of Mathematical Sciences, India and University of Bergen, Norway

99

Let $M = (E, \mathcal{I})$ be a matroid of rank n. A *k-truncation* of M is a matroid $M' = (E, \mathcal{I}')$ such that for any $A \subseteq E$, $A \in \in I'$ if and only if $|A| \leq k$ and $A \in \mathcal{I}$. Given a linear representation, A, of M we consider the problem of finding a linear representation, A_k, of the k-truncation of M. A common way to compute A_k is to multiply the matrix A with a random $k \times n$ matrix, yielding a simple randomized algorithm. So a natural question is whether we can compute A_k *deterministically*. In this paper we settle this question for matrices over any field in which the field operations can be done efficiently. This includes any finite field and the field of rational numbers ($\mathbb{Q}$).

Our algorithms are based on the properties of the classical Wronskian determinant, and the folded Wronskian determinant, which was recently introduced by Guruswami and Kopparty [*FOCS 2013; COMBINATORICA 2016*], and Forbes and Shpilka [*STOC 2012*]. Our main conceptual contribution in this paper is to show that the Wronskian determinant can also be used to obtain a representation of the truncation of a linear matroid in deterministic polynomial time.

An important application of our result is a deterministic algorithm to compute Representative sets over linear matroids, which derandomizes a result of Fomin et. al. [*SODA 2014; J. ACM 2016*]. This result derandomizes several parameterized algorithms, including an algorithm for ℓ-Matroid Parity to which several problems, such as ℓ-Matroid Intersection, can be reduced to.

CCS Concepts: • **Mathematics of computing** → **Matroids and greedoids**; • **Theory of computation** → **Pseudorandomness and derandomization**;

Additional Key Words and Phrases: Matroid Truncation, Representative Sets, Matroid Parity, Wronskian Matrix

ACM Reference Format:
Daniel Lokshtanov, Pranabendu Misra, Fahad Panolan, and Saket Saurabh. 9999. Deterministic Truncation of Linear Matroids. *ACM Trans. Algor.* 9999, 44444, Article 99 (9999), 21 pages. https://doi.org/0000001.0000001

A preliminary version of this paper appeared in the proceedings of the 42nd International Colloquium on Automata, Languages, and Programming (ICALP 2015) [29].

Authors' addresses: Daniel Lokshtanov, University of Bergen, Bergen, Norway, daniello@ii.uib.no; Pranabendu Misra, University of Bergen, Bergen, Norway, Pranabendu.Misra@ii.uib.no; Fahad Panolan, University of Bergen, Bergen, Norway, Fahad.Panolan@ii.uib.no; Saket Saurabh, Institute of Mathematical Sciences, Chennai, India, University of Bergen, Bergen, Norway, saket@imsc.res.in.

1549-6325/9999/99-ART99 $15.00
https://doi.org/0000001.0000001

1 INTRODUCTION

A *rank k-truncation* of a $n \times m$ matrix M, is a $k \times m$ matrix M_k such that for every subset $I \subseteq \{1, \ldots, m\}$ of size at most k, the set of columns corresponding to I in M_k has rank $|I|$ if and only if the corresponding set of columns in M has rank $|I|$. We can think of finding a rank k-truncation of a matrix as a dimension reduction problem such that linear independence among all sets of columns of size at most k is preserved. This problem is a variant of the more general *dimensionality reduction* problem, which is a basic problem in many areas of computer science such as machine learning, data compression, information processing and others. In dimensionality reduction, we are given a collection of points (vectors) in a high dimensional space, and the objective is to map these points to points in a space of small dimension while preserving some property of the original collection of points. For an example, one could consider the problem of reducing the dimension of the space, while preserving the pairwise distance, for a given collection of points. Using the Johnson-Lindenstrauss Lemma this can be done approximately for any collection of m points, while reducing the dimension of the space to $\mathcal{O}(\log m)$ [6, 25]. In this work, we study dimensionality reduction under the constraint that linear independence of any sub-collection of size up to k of the given set of vectors is preserved. A motivation for this problem comes from *matroid theory* and its algorithmic applications. For a matroid $M = (E, \mathcal{I})$, a *k-truncation* of M is a matroid $M' = (E, \mathcal{I}')$ such that for any $A \subseteq E$, $A \in I'$ if and only if $|A| \leq k$ and $A \in \mathcal{I}$. Given a linear representation of a matroid $M = (E, \mathcal{I})$ of rank n over a ground set of size m (which has a representation matrix M of dimension $n \times m$), we want to find a linear representation of the k-truncation of the matroid M. In other words, we want to map the set of column vectors of M (which lie in a space of dimension n) to vectors in a space of dimension k such that, any set S of column vectors of M with $|S| \leq k$ are linearly independent if and only if the corresponding set of vectors in the k-dimensional vector space are linearly independent.

A common way to obtain a rank k-truncation of a matrix M, is to left-multiply M by a random matrix of dimension $k \times n$ (with entries from a field of an exponential size). Then using the Schwartz-Zippel Lemma one can show that, the product matrix is a k-truncation of the matrix M with high probability [31]. This raises a natural question of whether there is a deterministic algorithm for computing k-truncation of a matrix. In this paper we settle this question by giving a polynomial time deterministic algorithm to solve this problem. In particular we have the following theorem.

Theorem 1.1. *Let M be a $n \times m$ matrix over a field $\mathbb{F}$ of rank n. Given a number $k \leq n$, we can compute a matrix M_k over the field $\mathbb{F}(X)$ such that it is a representation of the k-truncation of M, in $\mathcal{O}(mnk)$ field operations over $\mathbb{F}$. Furthermore, given M_k, we can test whether a given set of ℓ columns in M_k are linearly independent in $\mathcal{O}(n^2k^3)$ field operations over $\mathbb{F}$.*

Observe that, using Theorem 1.1 we can obtain a deterministic truncation of a matrix over any field where the field operations can be done efficiently. This includes any finite field ($\mathbb{F}_{p^\ell}$) or field of rationals $\mathbb{Q}$. In particular our result implies that we can find deterministic truncation for important classes of matroids such as graphic matroids, co-graphic matroids, partition matroids and others. We note that for many fields, the k-truncation matrix can be represented over a finite degree extension of $\mathbb{F}$, which is useful in algorithmic applications.

A related notion is the *ℓ-elongation* of a matroid, where $\ell > \mathsf{rank}(M)$. It is defined as the matriod $M' = (E, \mathcal{I}')$ such that $S \subseteq E$ is a basis of M' if and only if, it contains a basis of M and $|S| = \ell$. Note that the rank of the matroid M' is ℓ. We have the following observation.

Observation 1 ([34], page 75). *Let M be a matroid of rank n over a ground set of size m. Let M^*, $T(M,k)$ and $E(M,\ell)$ denote the dual matroid, the k-truncation and the ℓ-elongation of the matroid M, respectively. Then $E(M,\ell) = \{T(M^*, m-\ell)\}^*$, i.e. the ℓ-elongation of M is the dual of the $(m-\ell)$-truncation of the dual of M.*

Now using the fact that, given a representation of a matroid, a representation of the dual matroid can be obtained in polynimial time, we obtain the following corollary.

Corollary 1.2. *Let M be a linear matroid of rank n, over a ground set of size m, which is representable over a field $\mathbb{F}$. Given a number $\ell \geq n$, we can compute a representation of the ℓ-elongation of M, over the field $\mathbb{F}(X)$ in polynomially many (in m, n, ℓ) field operations over $\mathbb{F}$.*

Tools and Techniques

The main tool used in this work, is the Wronskian determinant and its characterization of the linear independence of a set of polynomials. Given a polynomial $P_j(X)$ and a number ℓ, define $Y_j^\ell = (P_j(X), P_j^{(1)}(X), \ldots, P_j^{(\ell-1)}(X))^T$. Here, $P_j^{(i)}(X)$ is the i-th formal derivative of $P_j(X)$. Formally, the Wronskian matrix of a set of polynomials $P_1(X), \ldots, P_k(X)$ is defined as the $k \times k$ matrix $W(P_1, \ldots, P_k) = [Y_1^k, \ldots, Y_k^k]$. Recall that to get a k-truncation of a linear matroid, we need to map a set of vectors from $\mathbb{F}^n$ to $\mathbb{K}^k$ such that linear independence of any subset of the given vectors of size at most k is preserved. We associate with each vector, a polynomial whose coefficients are the entries of the vector. A known mathematical result states that a set of polynomials $P_1(X), \ldots, P_k(X) \in \mathbb{F}[X]$ are linearly independent over $\mathbb{F}$ if and only if the corresponding Wronskian determinant $\det(W(P_1, \ldots, P_k)) \not\equiv 0$ in $\mathbb{F}[X]$ [4, 19, 32]. However, this requires that the underlying field be $\mathbb{Q}$ (or $\mathbb{R}$, $\mathbb{C}$), or that it is a finite field whose characteristic is strictly larger than the maximum degree of $P_1(X), \ldots, P_k(X)$.

For fields of small characteristic, we use the notion of α-folded Wronskian, which was introduced by Guruswami and Kopparty [23, 24] in the context of subspace designs, with applications in coding theory. It was also implicitly present in the works of Forbes and Shpilka [14], who used it in reducing randomness for polynomial identity testing and related problems. Let $\mathbb{F}$ be a finite field and α be an element of $\mathbb{F}$. Given a polynomial $P_j(X) \in \mathbb{F}[X]$ and a number ℓ, define $Z_j^\ell = (P_j(X), P_j(\alpha X), \ldots, P_j(\alpha^{\ell-1}X))^T$. Formally, the α-folded Wronskian matrix of a family of polynomials $P_1(X), \ldots, P_k(X)$ is defined as the $k \times k$ matrix $W_\alpha(P_1, \ldots, P_k) = [Z_1^k, \ldots, Z_k^k]$. Let $P_1(X), \ldots, P_k(X)$ be a family of polynomials of degree at most $n-1$. From, the results of Forbes and Shpilka [14] one can derive that if α is an element of the field $\mathbb{F}$, of order at least n then $P_1(X), \ldots, P_k(X)$ are linearly independent over $\mathbb{F}$ if and only if the α-folded Wronskian determinant $\det(W_\alpha(P_1, \ldots, P_k)) \not\equiv 0$ in $\mathbb{F}[X]$.

Having introduced the tools, we continue to the description of our algorithm. Given a $n \times m$ matrix M over $\mathbb{F}$ and a positive integer k our algorithm for finding a k-truncation of M proceeds as follows. To a column C_i of M we associate a polynomial $P_i(X)$ whose coefficients are the entries of C_i. That is, if $C_i = (c_{1i}, \ldots, c_{ni})^T$ then $P_i(X) = \sum_{j=1}^n c_{ji}x^{j-1}$. If the characteristic of the field $\mathbb{F}$ is strictly larger than n or $\mathbb{F} = \mathbb{Q}$ then we return $M_k = [Y_1^k, \ldots, Y_m^k]$ as the required k-truncation of M. In other cases we first compute an $\alpha \in \mathbb{F}$ of order at least n and then return $M_k = [Z_1^k, \ldots, Z_m^k]$. We then use the properties of Wronskian determinant and α-folded Wronskian, to prove the correctness of our algorithm. Observe that when M is a representation of a linear matroid then M_k is a representation of its k-truncation. Further, each entry of M_k is a polynomial of degree at most $n-1$ in $\mathbb{F}[X]$. Thus, testing whether a set of columns of size at most k is independent, reduces to testing whether a determinant polynomial of degree at most $(n-1)k$ is identically zero or not. This is easily done by evaluating the determinant at $(n-1)k+1$ points in $\mathbb{F}$ and testing if it is zero at all those points.

Our main conceptual contribution in this paper is to show the connection between the Wronskian matrix and the truncation of a linear matroid, which can be used to obtain a representation of the truncation in deterministic polynomial time. These matrices are related to the notion of "rank extractors" which have important applications in polynomial identity testing and in the construction of randomness extractors [13, 14, 16, 17]. We believe that these and other related tools could be useful in obtaining other parameterized algorithms, apart from those mentioned in this paper. We note that, one can obtain a different construction of matrix truncation via an earlier result of Gabizon and Raz [17], which was used in construction of randomness extractors.

Applications

Matroid theory has found many algorithmic applications, starting from the characterization of greedy algorithms, to designing fixed parameter tractable (FPT) algorithms and kernelization algorithms. Recently the notion of *representative families* over linear matroids was used in designing fast FPT, as well as kernelization algorithm for several problems [10–12, 21, 26, 27, 31, 36]. Let us introduce this notion more formally. Let $M = (E, \mathcal{I})$ be a matroid and let $\mathcal{S} = \{S_1, \ldots, S_t\}$ be a p-family, i.e. a collection of subsets of E of size p. A subfamily $\widehat{\mathcal{S}} \subseteq \mathcal{S}$ is *q-representative* for $\mathcal{S}$ if for every set $Y \subseteq E$ of size at most q, if there is a set $X \in \mathcal{S}$ disjoint from Y with $X \cup Y \in \mathcal{I}$, then there is a set $\widehat{X} \in \widehat{\mathcal{S}}$ disjoint from Y and $\widehat{X} \cup Y \in \mathcal{I}$. In other words, if a set Y of size at most q can be extended to an independent set of size $|Y| + p$ by adding a subset from $\mathcal{S}$, then it also can be extended to an independent set of size $|Y| + p$ by adding a subset from $\widehat{\mathcal{S}}$ as well. The Two-Families Theorem of Bollobás [3] for extremal set systems and its generalization to subspaces of a vector space of Lovász [30] (see also [15]) imply that every family of sets of size p has a q-representative family with at most $\binom{p+q}{p}$ sets. Recently, Fomin et. al. [11] gave an efficient randomized algorithm to compute a representative family of size $\binom{p+q}{p}$ in a linear matroid of rank $n > p + q$. This algorithm starts by computing a randomized $(p + q)$-truncation of the given linear matroid and then computes a q-representative family over the truncated matroid deterministically. Therefore one of our motivations to study the k-truncation problem was to find an efficient deterministic computation of a representative family in a linear matroid. Formally, we have the following theorem.

THEOREM 1.3. *Let $M = (E, \mathcal{I})$ be a linear matroid of rank n and let $\mathcal{S}$ be a p-family of independent sets of size t. Let A be a $n \times |E|$ matrix representing M over a field $\mathbb{F}$, and let ω be the exponent of matrix multiplication. Then there are deterministic algorithms computing $\widehat{\mathcal{S}} \subseteq^q_{rep} \mathcal{S}$ as follows.*

(i) A family $\widehat{\mathcal{S}}$ of size $\binom{p+q}{p}$ in $\mathcal{O}\left(\binom{p+q}{p}^2 tp^3n^2 + t\binom{p+q}{q}^{\omega} np\right) + (n + |E|)^{\mathcal{O}(1)}$, operations over $\mathbb{F}$.

(ii) A family $\widehat{\mathcal{S}}$ of size $np\binom{p+q}{p}$ in $\mathcal{O}\left(\binom{p+q}{p} tp^3n^2 + t\binom{p+q}{q}^{\omega-1} (pn)^{\omega-1}\right) + (n + |E|)^{\mathcal{O}(1)}$ operations over $\mathbb{F}$.

Let us point out that the above algorithms offer a trade-off between the size of a representative set and the running time of the algorithm. As a corollary of the above theorem, we obtain a deterministic FPT algorithm for ℓ-MATROID PARITY, derandomizing the main algorithm of Marx [31]. This then derandomizes the algorithms for all the other problems in [31] as well. In particular this implies a deterministic FPT algorithm for ℓ-Matroid Intersection, certain packing problems and Feedback Edge Set with Budget Vectors. Using our results one can compute, in deterministic polynomial time, the k-truncation of graphic and co-graphic matroids, which has important applications in graph algorithms. Recently, the truncation of co-graphic matroid has been used to obtain deterministic parameterized algorithms, running in time $2^{\mathcal{O}(k)}n^{\mathcal{O}(1)}$ time, for problems where we need to delete k edges that keeps the graph connected and maintain certain parity conditions [22]. These problems include Undirected Eulerian Edge Deletion, Directed Eulerian Edge Deletion and Undirected Connected Odd Edge Deletion [5, 8, 9, 22].

2 PRELIMINARIES

In this section we give various definitions and notions which we make use of in the paper. We use the following notations: $[n] = \{1, \ldots, n\}$ and $\binom{[n]}{i} = \{X \mid X \subseteq [n],\ |X| = i\}$.

Fields, Polynomials, Vectors and Matrices

In this section we review some definitions and properties of fields that are required in this paper. We refer to any graduate textbook on algebra for more details. The number of elements in a field is called its *order*. For every prime number p and a positive integer ℓ, there exists a finite field of order p^ℓ. For a prime number p, the set $\{0, 1, \ldots, p-1\}$ with addition and multiplication modulo p forms a field, which we denote by $\mathbb{F}_p$. Let $\mathbb{F}$ be a finite field and then $\mathbb{F}[X]$ denotes the ring of polynomials in X over $\mathbb{F}$. For the ring $\mathbb{F}[X]$, we use $\mathbb{F}(X)$ to denote the *field of fractions* of $\mathbb{F}[X]$. We will use $\mathbb{F}[X]^{<n}$ to denote the set the polynomials in $\mathbb{F}[X]$ of degree $< n$. The *characteristic* of a field, denoted by $\mathrm{char}(\mathbb{F})$, is defined as least positive integer m such that $\sum_{i=1}^{m} 1 = 0$. For fields such as $\mathbb{R}$ where there is no such m, the characteristic is defined to be 0. For a finite field $\mathbb{F} = \mathbb{F}_{p^\ell}$, $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ is called the multiplicative group of $\mathbb{F}$. It is a cyclic group and has a generator $\alpha \in \mathbb{F}^*$, which is called a *primitive element* of $\mathbb{F}$. We say that an element $\beta \in \mathbb{F}$ has *order* r, if r is the least integer such that $\beta^r = 1$. Let us note that the order of any element is at most $|\mathbb{F}^*| = |\mathbb{F}| - 1$. A polynomial $P(X) \in \mathbb{F}[X]$ is called *irreducible* if it cannot expressed as a product of two other non-trivial polynomials in $\mathbb{F}[X]$. Let $P(X)$ be an irreducible polynomial in $\mathbb{F}[X]$ of degree ℓ. Then $\mathbb{K} = \mathbb{F}[X]/P(X) = \mathbb{F}[X](\text{mod } P(X))$ (i.e. the quotient ring of the ideal generated by $P(X)$), is also a field. It is of order $|\mathbb{F}|^\ell$ and characteristic of $\mathbb{K}$ is equal to the characteristic of $\mathbb{F}$. We note that the field $\mathbb{K}$ is well defined by specifying the irreducible polynomial $P(X)$. The field $\mathbb{K}$ is called a *field extension* of $\mathbb{F}$ of degree ℓ. All finite fields are obtained as extensions of prime fields, and for any prime p and positive integer ℓ there is exactly one finite field of order p^ℓ up to isomorphism.

Derivatives. Recall the definition of the formal derivative $\frac{d}{dx}$ of a function over $\mathbb{R}$. We denote the k-th formal derivative of a function f by $f^{(k)}$. We can extend this notion to finite fields. Let $\mathbb{F}$ be a finite field and let $\mathbb{F}[X]$ be the ring of polynomials in X over $\mathbb{F}$. Let $P \in \mathbb{F}[X]$ be a polynomial of degree $n-1$, i.e. $P = \sum_{i=0}^{n-1} a_i X^i$ where $a_i \in \mathbb{F}$. Then we define the *formal derivative* of as $P' = \sum_{i=1}^{n-1} i a_i X^{i-1}$. We can extend this definition to the k-th formal derivative of P as $P^{(k)} = (P^{(k-1)})'$. For a polynomial $P(X) \in \mathbb{F}[X]$, the i-th Hasse derivative $D^i(P)$ is defined as the coefficient of Z^i in $P(X+Z)$. Here, $P(X+Z) = \sum_{i=0}^{\infty} D^i(P(X))Z^i$. We note that Hasse derivatives differ from formal derivatives by a multiplicative factor. We refer to [7] and [20] for details.

Vector and Matrices. A vector v over a field $\mathbb{F}$ is an array of values from $\mathbb{F}$. A collection of vectors $\{v_1, v_2, \ldots, v_k\}$ are said to be linearly dependent if there exist values $a_1, a_2, \ldots, a_k$, not all zero, from $\mathbb{F}$ such that $\sum_{i=1}^{k} a_i v_i = 0$. Otherwise these vectors are called linearly independent. The matrix is said to have dimension $n \times m$ if it has n rows and m columns. For a matrix A (or a vector v), we denote its *transpose* by A^T (or v^T). Further, we use $\mathbf{C}(A)$ to denote the collection of column vectors of the matrix A. The rank of a matrix is the cardinality of the maximum sized collection of columns which are linearly independent. Equivalently, the rank of a matrix is the maximum number k such that there is a $k \times k$ submatrix whose determinant is non-zero. The determinant of a $n \times n$ matrix A is denoted by $\det(A)$. Throughout the paper we use ω to denote the matrix multiplication exponent. The current best known bound on $\omega < 2.373$ [18, 40].

Matroids

We review some definitions and properties of matroids. For a detailed introduction to matroids, we refer to the textbook of Oxley [35]. A pair $M = (E, \mathcal{I})$, where E is a ground set and $\mathcal{I}$ is a family of subsets (called independent sets) of E, is a *matroid* if it satisfies the following conditions: (I1) $\phi \in \mathcal{I}$. (I2) If $A' \subseteq A$ and $A \in \mathcal{I}$ then $A' \in \mathcal{I}$. (I3) If $A, B \in \mathcal{I}$ and $|A| < |B|$, then there is $e \in (B \setminus A)$ such that $A \cup \{e\} \in \mathcal{I}$. An inclusion-wise maximal set of $\mathcal{I}$ is called a *basis* of the matroid. Using axiom (I3) it is easy to show that all the bases of a matroid have the same size. This size is called the *rank* of the matroid M, and is denoted by $\mathsf{rank}(\mathrm{M})$. The dual of a matroid M is defined as the matroid $M^* = (E, \mathcal{I}^*)$, where $I' \subseteq E$ is a basis of M^* if and only if $I = E \setminus I'$ is a basis of M. Observe that $(M^*)^* = M$.

Let A be a matrix over an arbitrary field $\mathbb{F}$ and let E be the set of columns of A. For A, we define matroid $M = (E, \mathcal{I})$ as follows. A set $X \subseteq E$ is independent (that is $X \in \mathcal{I}$) if the corresponding columns are linearly independent over $\mathbb{F}$. The matroids that can be defined by such a construction are called *linear matroids*, and if a matroid can be defined by a matrix A over a field $\mathbb{F}$, then we say that the matroid is representable over $\mathbb{F}$. That is, a matroid $M = (E, \mathcal{I})$ of rank d is representable over a field $\mathbb{F}$ if there exist vectors in $\mathbb{F}^d$ corresponding to the elements such that linearly independent sets of vectors correspond to independent sets of the matroid. A matroid $M = (E, \mathcal{I})$ is called *representable* or *linear* if it is representable over some field $\mathbb{F}$. The dual matroid M^* of a linear matroid M is also linear and given a representation of M, a representation of M^* can be found in polynomial time.

Truncation of a Matroid. The *t-truncation* of a matroid $M = (E, \mathcal{I})$ is a matroid $M' = (E, \mathcal{I}')$ such that $S \subseteq E$ is independent in M' if and only if $|S| \leq t$ and S is independent in M.

3 DETERMINISTIC MATROID TRUNCATION

In this section we give the main result of this work. We start with an introduction to our tools and then we give two results that give rank k-truncation of the given matrix M.

Tools and Techniques

In this subsection we collect some known results, definitions and derive some new connections among them that will be central to our results.

Polynomials and Vectors. Let $\mathbb{F}$ be a field. The set of polynomials $P_1(X), P_2(X), \ldots, P_k(X)$ in $\mathbb{F}[X]$ are said to be *linearly independent* over $\mathbb{F}$ if there doesn't exist $a_1, a_2, \ldots, a_k \in \mathbb{F}$, not all zero such that $\sum_{i=1}^{k} a_i P_i(X) \equiv 0$. Otherwise they are said to be linearly dependent.

Definition 1. *Let $P(X)$ be a polynomial of degree at most $n-1$ in $\mathbb{F}[X]$. We define the vector v corresponding to the polynomial $P(X)$ as follows: $v[j] = c_j$ where $P(X) = \sum_{j=1}^{n} c_j x^{j-1}$. Similarly given a vector v of length n over $\mathbb{F}$, we define the polynomial $P(X)$ in $\mathbb{F}[X]$ corresponding to the vector v as follows: $P(X) = \sum_{j=1}^{n} v[j]x^{j-1}$.*

The next lemma will be key to several proofs later. The proof of this lemma follows easily from standard methods, and we include it for the sake of completeness.

Lemma 3.1. *Let $v_1, \ldots, v_k$ be vectors of length n over $\mathbb{F}$ and let $P_1(X), \ldots, P_k(X)$ be the corresponding polynomials respectively. Then $P_1(X), \ldots, P_k(X)$ are linearly independent over $\mathbb{F}$ if and only if $v_1, v_2, \ldots, v_k$ are linearly independent over $\mathbb{F}$.*

Proof. For $i \in \{1 \ldots k\}$, let $v_i = (c_{i1}, \ldots, c_{in})$ and let $P_i(X) = \sum_{j=1}^{n} c_{ij}x^{j-1}$ be the polynomial corresponding to v_i.

We first prove the forward direction of the proof. For a contradiction, assume that $v_1, \ldots, v_k$ are linearly dependent. Then there exists $a_1, \ldots, a_k \in \mathbb{F}$, not all zeros, such that $\sum_{i=1}^{k} a_i v_i = 0$. This implies that for each $j \in \{1, \ldots n\}$, $\sum_{i=1}^{k} a_i v_i[j] = 0$. Since $v_i[j] = c_{ij}$, we have $\sum_{i=1}^{k} a_i c_{ij} = 0$, which implies that $\sum_{i=1}^{k} a_i c_{ij} x^{j-1} = 0$. Summing over all these expressions we get $\sum_{i=1}^{k} a_i P_i(X) \equiv 0$, a contradiction. This completes the proof in the forward direction.

Next we prove the reverse direction of the lemma. To the contrary assume that $P_1(X), \ldots, P_k(X)$ are linearly dependent. Then there exists $a_1, \ldots, a_k \in \mathbb{F}$, not all zeros, such that $\sum_{i=1}^{k} a_i P_i(X) \equiv 0$. This implies that for each $j \in \{1, \ldots, n\}$, the coefficients of x^{j-1} satisfy $\sum_{i=1}^{k} a_i c_{ij} = 0$. Since c_{ij} is the j-th entry of the vector v_i for all i and j, we have $\sum_{i=1}^{k} a_i v_i = 0$. Thus the vectors $v_1, \ldots, v_k$ are linearly dependent, a contradiction to the given assumption. This completes the proof. $\square$

We will use this claim to view the column vectors of a matrix M over a field $\mathbb{F}$ as elements in the ring $\mathbb{F}[X]$ and in the field of fractions $\mathbb{F}(X)$. We shall then use properties of polynomials to deduce properties of these column vectors and vice versa.

The Wronskian determinant. Let $\mathbb{F}$ be a field with characteristic at least n. Consider a collection of polynomials $P_1(X), \ldots, P_k(X)$ from $\mathbb{F}[X]$ of degree at most $n-1$. We define the following matrix, called the *Wronskian*, of $P_1(X), \ldots, P_k(X)$ as follows.

$$W(P_1, \ldots, P_k) = \begin{pmatrix} P_1(X) & P_2(X) & \ldots & P_k(X) \\ P_1^{(1)}(X) & P_2^{(1)}(X) & \ldots & P_k^{(1)}(X) \\ \vdots & \vdots & \ddots & \vdots \\ P_1^{(k-1)}(X) & P_2^{(k-1)}(X) & \ldots & P_k^{(k-1)}(X) \end{pmatrix}_{k \times k}$$

Note that, the determinant of the above matrix actually yields a polynomial. For our purpose we will need the following well known result.

Theorem 3.2 ([4, 19, 32]). *Let $\mathbb{F}$ be a field and $P_1(X), \ldots, P_k(X)$ be a set of polynomials from $\mathbb{F}[X]^{<n}$ and let $\mathrm{char}(\mathbb{F}) > n$. Then $P_1(X), \ldots, P_k(X)$ are linearly independent over $\mathbb{F}$ if and only if the Wronskian determinant $\det(W(P_1, P_2, \ldots, P_k)) \not\equiv 0$ in $\mathbb{F}[X]$.*

The notion of Wronskian dates back to 1812 [32]. We refer to [4, 19] for some recent variations and proofs. The switch between usual derivatives and Hasse derivatives multiplies the Wronskian determinant by a constant, which is non-zero as long as $n < \text{char}(\mathbb{F})$, and thus this criterion works with both notions. Observe that the Wronskian determinant is a (univariate) polynomial of degree at most nk in $\mathbb{F}[X]$. Thus to test if such a polynomial (of degree d) is identically zero, we only need to evaluate it at $d+1$ arbitrary points of the field $\mathbb{F}$, and check if it is zero at all those points. Alternatively, if the order of the field $\mathbb{F}$ is small, we may also compute the coefficients of this polynomial.

The Folded Wronskian determinant. The above definition of Wronskian requires us to compute derivatives of degree $(n-1)$ polynomials. As noted earlier, they are well defined only if the underlying field has characteristic greater than or equal to n. However the matrix might be over a field of small characteristic. For these kind of fields, we have the notion of *Folded Wronskian* which was recently introduced by Guruswami and Kopparty in the context of subspace designs [23, 24].

Consider a collection of polynomials $P_1(X), \dots, P_k(X)$ from $\mathbb{F}[X]$ of degree at most $(n-1)$. Further, let $\mathbb{F}$ be of order at least $nk+1$, and α be an element of $\mathbb{F}^*$. We define the the *α-folded Wronskian*, of $P_1(X), \dots, P_k(X)$ as follows.

$$W_\alpha(P_1, \dots, P_k) = \begin{pmatrix} P_1(X) & P_2(X) & \dots & P_k(X) \\ P_1(\alpha X) & P_2(\alpha X) & \dots & P_k(\alpha X) \\ \vdots & \vdots & \ddots & \vdots \\ P_1(\alpha^{k-1}X) & P_2(\alpha^{k-1}X) & \dots & P_k(\alpha^{k-1}X) \end{pmatrix}_{k \times k}$$

As before, the determinant of this matrix is a polynomial of degree at most nk in $\mathbb{F}[X]$. The following theorem by Forbes and Shpilka [14] shows that the above determinant characterizes the linear independence of the collection of polynomials.

Theorem 3.3 ([14], Theorem 4.1). [1] *Let $1 \le k \le n$ and let M be a $n \times k$ matrix over $\mathbb{F}$ of rank k. Let $\mathbb{K}$ be an extension of $\mathbb{F}$ and let $g \in \mathbb{K}$ be an element of order $\ge n$. For $X \in \mathbb{K}$, define A_X to be a $k \times n$ matrix where $(A_X)_{i,j} = (g^{i-1}X)^{j-1}$. Then there are at most nk values of $X \in \mathbb{K}$ such that the rank of $A_X M$ is less than k.*

The following is a restatement of the above theorem in the language of this paper.

Theorem 3.4. [2] *Let $\mathbb{F}$ be a field with at least $nk+1$ elements, and let α be an element of $\mathbb{F}$ of order $\ge n$ and let $P_1(X), \dots, P_k(X)$ be a set of polynomials from $\mathbb{F}[X]^{<n}$. Then $P_1(X), \dots, P_k(X)$ are linearly independent over $\mathbb{F}$ if and only if the α-folded Wronskian determinant $\det(W_\alpha(P_1, \dots, P_k)) \not\equiv 0$ in $\mathbb{F}[X]$.*

Proof. The proof follows by observing the following. Let M_i be the column vector corresponding to the coefficients of P_i. And let A_X be the $k \times n$ matrix defined as, $(A_X)_{i,j} = (\alpha^{i-1}X)^{j-1}$. Then $W_i = A_X M_i = [P_i(X), P_i(\alpha X), \dots, P_i(\alpha^{k-1}X)]^T$. Thus if M were the $n \times k$ matrix with column vectors $\{M_i\}$, then $A_X M = W_\alpha(P_1, \dots, P_k)$ with $\{W_i\}$ as it's column vectors.

If $P_1, \dots, P_k$ are linearly independent, then M has rank k. We then apply Theorem 3.3 with $\mathbb{F} = \mathbb{K}$ and $g = \alpha$ to obtain that there is some value of X for which rank of the $k \times k$ matrix $A_X M$ has rank k. This means that the polynomial $\det(W_\alpha(P_1, \dots, P_k)) \not\equiv 0$. And,

[1] In [14], the matrix A is defined as $(A_X)_{i,j} = (g^i X)^j$. But the same proof also holds when we define $(A_X)_{i,j} = (g^{i-1}X)^{j-1}$ since the order of g is $\ge n$.

[2] Unaware of the results of [14], we had obtained a different proof of this theorem with a slightly weaker bound. We thank the anonymous reviewers for pointing out these results from literature. Our proof may be found in [28].

if $\{P_i\}$ were not linearly independent, then $\{W_i\}$ are also not linearly independent. Thus, $\det(W_\alpha(P_1, \ldots, P_k)) \equiv 0$. □

We must also note that the following lemma by Gabizon and Raz [17] can be used to obtain a different construction of matrix truncation. We omit the details.

LEMMA 3.5 ([17], LEMMA 6.1). *Let $1 \le k \le n$ and let M be a $n \times k$ matrix over $\mathbb{F}$ of rank k. For $X \in \mathbb{F}$, define A_X to be a $k \times n$ matrix where $(A_X)_{i,j} = X^{ij}$. Then there are at most $\le nk^2$ values of X such that the rank of $A_X M$ is less than k.*

Finding irreducible polynomials and elements of large order. Whenever we need to use folded Wronskians, we will also need to get hold of an element of large order of an appropriate field. We start by reviewing some known algorithms for finding irreducible polynomials over finite fields. Note that for a finite field of order p^ℓ, the field operations can be done in time $(\ell \log p)^{\mathcal{O}(1)}$. And for an infinite field, the field operations will require $(\log N)^{\mathcal{O}(1)}$ where N is the size of the largest value handled by the algorithm. Typically we will provide an upper bound on N when the need arises. A result by Shoup [37, Theorem 4.1]) allows us to find an irreducible polynomial of degree r over $\mathbb{F}_{p^\ell}$ in time polynomial in p, ℓ and d. Adleman and Lenstra [1, Theorem 2] gave an algorithm that allows us to compute an irreducible polynomial of degree at least r over a prime field $\mathbb{F}_p$ in time polynomial in $\log p$ and r.

LEMMA 3.6 ([1, 37]). (Finding Irreducible Polynomials)

(i) There is an algorithm such that given prime p and r it can compute an irreducible polynomial $f(X) \in \mathbb{F}_p[X]$ such that $r \le \deg(f) \le cr \log p$ in $(cr(\log p)^2)^c$ time, where c is a constant.

(ii) For $q = p^\ell$ and an integer r, we can compute an irreducible polynomial of $\mathbb{F}_q[X]$ of degree r in $\mathcal{O}(\sqrt{p}(\log p)^3 r^3 (\log r)^{\mathcal{O}(1)} + (\log p)^2 r^4 (\log r)^{\mathcal{O}(1)} + (\log p) r^4 (\log r)^{\mathcal{O}(1)} \ell^2 (\log \ell)^{\mathcal{O}(1)})$ time.

Next we consider a few algorithms for finding primitive elements in finite fields. For fields of large order but small characteristic, we have the following lemma from the results of Shparlinski [39] and also from the results of Shoup [38].

LEMMA 3.7 ([38, 39]). *Let $\mathbb{F} = \mathbb{F}_{p^\ell}$ be a finite field. Then we can compute a set $S \subset \mathbb{F}$ of size $\mathsf{poly}(p, \ell)$ containing a primitive element in time $\mathsf{poly}(p, \ell)$.* [3]

We use Lemma 3.7 to get the following result that allows us to find elements of sufficiently large order in a finite field of small size.

LEMMA 3.8. *Let $\mathbb{F} = \mathbb{F}_{p^\ell}$ be a finite field. Given an integer n such that $n < p^\ell$, we can compute an element of $\mathbb{F}$ of order at least n in $\mathsf{poly}(p, \ell, n)$ time.*

PROOF. We begin by applying Lemma 3.7 to the field $\mathbb{F}$ and obtain a set S of size $\mathsf{poly}(p, \ell)$. This takes time $\mathsf{poly}(p, \ell)$. Then for each element $\alpha \in S$ we compute the set $G_\alpha = \{\alpha^i \mid i = 1, 2, \ldots, n\}$. If for any α we have $|G_\alpha| \ge n$, i.e. the set contains n distinct elememts, then we return it as the required element of order at least n. Since the set S contains at least one primitive element of $\mathbb{F}$, we will find some α in this step. Note this step too takes $\mathsf{poly}(p, \ell, n)$ time. □

When given a small field, the following lemma allows us to increase the size of the field as well as find an element of large order in the bigger field.

[3]The term $\mathsf{poly}(x, y, z, \ldots)$ indicates a value that is bounded by a polynomial function in $x, y, z \ldots$.

Lemma 3.9. *Given a field $\mathbb{F} = \mathbb{F}_{p^\ell}$ and a number n such that $p^\ell < n$, we can find an extension $\mathbb{K}$ of $\mathbb{F}$ such that $n < |\mathbb{K}| < n^2$ and an element $\alpha \in \mathbb{K}$ of order at least n in time $n^{\mathcal{O}(1)}$.*

Proof. Let r be smallest number such that $p^{\ell r} > n$. But then $p^{\frac{\ell r}{2}} < n$. Therefore we have that $p^{\ell r} < n^2$. Next we find an extension $\mathbb{K}$ of $\mathbb{F}$ of degree r, by finding an irreducible polynomial $P(X) \in \mathbb{F}[X]$ of degree r using Lemma 3.6, in time polynomial in p, ℓ, r which is $n^{\mathcal{O}(1)}$. We then define the field $\mathbb{K}$ to be $\mathbb{F}[X]/P(X)$. Let us note that $\mathbb{K}$ is a field of order $p^{\ell r}$ since it is a degree r extension of the field $\mathbb{F}$ and $|\mathbb{F}| = p^\ell$. Then we can use Lemma 3.8 to compute an element of $\mathbb{K}$ of order at least n. Since $|\mathbb{K}| < n^2$, this can be done in time $n^{\mathcal{O}(1)}$. This completes the proof of this lemma. □

Deterministic Truncation of Matrices

In this subsection we look at algorithms for computing k-truncation of matrices. We consider matrices over the set of rational numbers $\mathbb{Q}$ or over some finite field $\mathbb{F}$. Therefore, we are given as input a matrix M of rank n over a field $\mathbb{F}$. Let p be the characteristic of the field $\mathbb{F}$ and N denote the size of the input in bits. The following theorem gives us an algorithm to compute the truncation of a matrix using the classical wronskian, over an appropriate field. We shall refer to this as the *classical wronskian method of truncation*.

Lemma 3.10. *Let M be a $n \times m$ matrix of rank n over a field $\mathbb{F}$, where $\mathbb{F}$ is either $\mathbb{Q}$ or $\mathrm{char}(\mathbb{F}) > n$. Then we can compute a $k \times m$ matrix M_k of rank k over the field $\mathbb{F}(X)$ which is a k-truncation of the matrix M in $\mathcal{O}(mnk)$ field operations over $\mathbb{F}$.*

Proof. Let $\mathbb{F}[X]$ be the ring of polynomials in X over $\mathbb{F}$ and let $\mathbb{F}(X)$ be the corresponding field of fractions. Let $C_1, \ldots, C_m$ denote the columns of M. Observe that we have a polynomial $P_i(X)$ corresponding to the column C_i of degree at most $n-1$, and by Lemma 3.1 we have that $C_{i_1}, \ldots, C_{i_\ell}$ are linearly independent over $\mathbb{F}$ if and only if $P_{i_1}(X), \ldots, P_{i_\ell}(X)$ are linearly independent over $\mathbb{F}$. Further note that P_i lies in $\mathbb{F}[X]$ and thus also in $\mathbb{F}(X)$. Let D_i be the vector $(P_i(X), P_i^{(1)}(X), \ldots, P_i^{(k-1)}(X))$ of length k with entries from $\mathbb{F}[X]$ (and also in $\mathbb{F}(X)$). Note that the entries of D_i are polynomials of degree at most $n-1$. Let us define the matrix M_k to be the $(k \times m)$ matrix whose columns are D_i^T, and note that M_k is a matrix with entries from $\mathbb{F}[X]$. We will show that indeed M_k is a desired k-truncation of the matrix M .

Let $I \subseteq \{1, \ldots, m\}$ such that $|I| = \ell \leq k$. Let $C_{i_1}, \ldots, C_{i_\ell}$ be a linearly independent set of columns of the matrix M over $\mathbb{F}$, where $I = \{i_1, \ldots, i_\ell\}$. We will show that the columns $D_{i_1}^T, \ldots, D_{i_\ell}^T$ are linearly independent in M_k over $\mathbb{F}(X)$. Consider the $k \times \ell$ matrix M_I whose column are the vectors $D_{i_1}^T, \ldots, D_{i_\ell}^T$. We shall show that M_I has rank ℓ by showing that there is a $\ell \times \ell$ submatrix whose determinant is a non-zero polynomial. Let $P_{i_1}(X), \ldots, P_{i_\ell}(X)$ be the polynomials corresponding to the vectors $C_{i_1}, \ldots, C_{i_\ell}$. By Lemma 3.1 we have that $P_{i_1}(X), \ldots, P_{i_\ell}(X)$ are linearly independent over $\mathbb{F}$. Then by Theorem 3.2, the $(\ell \times \ell)$ matrix formed by the column vectors $(P_{i_j}(X), P_{i_j}^{(1)}(X), \ldots, P_{i_j}^{(\ell-1)}(X))^T$, $i_j \in I$, is a non-zero determinant in $\mathbb{F}[X]$. But note that this matrix is a submatrix of M_I. Therefore M_I has rank ℓ in $\mathbb{F}(X)$. Therefore the vectors $D_{i_1}^T, \ldots, D_{i_\ell}^T$ are linearly independent in $\mathbb{F}(X)$. This completes the proof of the forward direction.

Let $I \subseteq \{1, \ldots, m\}$ such that $|I| = \ell \leq k$ and let $D_{i_1}^T, \ldots, D_{i_\ell}^T$ be linearly independent in M_k over $\mathbb{F}(X)$, where $I = \{i_1, \ldots, i_\ell\}$. We will show that the corresponding set of columns $C_{i_1}, \ldots, C_{i_\ell}$ are also linearly independent over $\mathbb{F}$. For a contradiction assume that $C_{i_1}, \ldots, C_{i_\ell}$ are linearly *dependent* over $\mathbb{F}$. Let $P_{i_1}(X), \ldots, P_{i_\ell}(X)$ be the polynomials in

$\mathbb{F}[X]$ corresponding to these vectors. Then by Lemma 3.1 we have that $P_{i_1}(X), \ldots, P_{i_\ell}(X)$ are linearly dependent over $\mathbb{F}$. So there is a tuple $a_{i_1}, \ldots, a_{i_\ell}$ of values of $\mathbb{F}$ such that $\sum_{j=1}^{\ell} a_{i_j} P_{i_j}(X) = 0$. Therefore, for any $d \in \{1, \ldots, \ell-1\}$, we have that $\sum_{j=1}^{\ell} a_{i_j} P_{i_j}^{(d)}(X) = 0$. Now consider the column vectors $D_{i_1}^T, \ldots, D_{i_\ell}^T$ of M_k corresponding to $C_{i_1}, \ldots, C_{i_\ell}$. Note that $\mathbb{F}$ is a subfield of $\mathbb{F}(X)$ and by the above, we have that $\sum_{j=1}^{\ell} a_{i_j} D_{i_j} = 0$. Thus $D_{i_1}^T, \ldots, D_{i_\ell}^T$ are linearly dependent in M_k over $\mathbb{F}(X)$, a contradiction to our assumption.

Thus we have shown that for any $\{i_1, \ldots, i_\ell\} \subseteq \{1, \ldots, m\}$ such that $\ell \leq k$, $C_{i_1}, \ldots, C_{i_\ell}$ are linearly independent over $\mathbb{F}$ if and only if $D_{i_1}, \ldots, D_{i_\ell}$ are linearly independent over $\mathbb{F}(X)$. To estimate the running time, observe that for each C_i we can compute D_i in $\mathcal{O}(kn)$ field operations and thus we can compute M_k in $\mathcal{O}(mnk)$ field operations. This completes the proof of this lemma. $\square$

Lemma 3.10 is useful in obtaining k-truncation of matrices whose entries are either from the field of large characteristic or from $\mathbb{Q}$. The following lemma allows us to find truncations in fields of small characteristic which have large order. The proof of this lemma is similar to the proof of Lemma 3.10. However, we will require an element of high order of such a field to compute the truncation. Therefore, we demand a lower bound on the size of the field as we need an element of certain order. We will later see how to remove this requirement from the statement of the next lemma.

Lemma 3.11. *Let $\mathbb{F}$ be a finite field with at least $nk+1$ elements, and let α be an element of $\mathbb{F}$ of order at least n. Let M be a $n \times m$ matrix of rank n over a field $\mathbb{F}$. Then we can compute a $(k \times m)$ matrix M_k of rank k over the field $\mathbb{F}(X)$ which is a k-truncation of the matrix M in $\mathcal{O}(mnk)$ field operations over $\mathbb{F}$.*

Proof. Let $\mathbb{F}[X]$ be the ring of polynomials in X over $\mathbb{F}$ and let $\mathbb{F}(X)$ be the corresponding field of fractions. Let $C_1, \ldots, C_m$ denote the columns of M. Observe that we have a polynomial $P_i(X)$ corresponding to the column C_i of degree at most $n-1$, and by Lemma 3.1 we have that $C_{i_1}, \ldots, C_{i_\ell}$ are linearly independent over $\mathbb{F}$ if and only if $P_{i_1}(X), \ldots, P_{i_\ell}(X)$ are linearly independent over $\mathbb{F}$. Further note that $P_i(X)$ lies in $\mathbb{F}[X]$ (and also in $\mathbb{F}(X)$).

Let D_i be the vector $(P_i(X), P_i(\alpha X), \ldots, P_i(\alpha^{k-1}X))$. Observe that the entries of D_i are polynomials of degree at most $n-1$ and are elements of $\mathbb{F}[X]$. Let us define the matrix M_k to be the $(k \times m)$ matrix whose columns are the vectors D_i^T, and note that M_k is a matrix with entries from $\mathbb{F}[X] \subseteq \mathbb{F}(X)$. We will show that M_k is a desired k-truncation of the matrix M .

Let $I \subseteq \{1, \ldots, m\}$ such that $|I| = \ell \leq k$. Let $C_{i_1}, \ldots, C_{i_\ell}$ be a linearly independent set of columns of the matrix M over $\mathbb{F}$, where $I = \{i_1, \ldots, i_\ell\}$. We will show that $D_{i_1}^T, \ldots, D_{i_\ell}^T$ are linearly independent in M_k over $\mathbb{F}(X)$. Consider the $k \times \ell$ matrix M_I whose columns are the vectors $D_{i_1}^T, \ldots, D_{i_\ell}^T$. We shall show that M_I has rank ℓ by showing that there is a $\ell \times \ell$ submatrix whose determinant is a non-zero polynomial. Let $P_{i_1}(X), \ldots, P_{i_\ell}(X)$ be the polynomials corresponding to the vectors $C_{i_1}, \ldots, C_{i_\ell}$. By Lemma 3.1 we have that $P_{i_1}(X), \ldots, P_{i_\ell}(X)$ are linearly independent over $\mathbb{F}$. Then by Theorem 3.4, the $(\ell \times \ell)$ matrix formed by the column vectors $(P_{i_j}(X), P_{i_j}(\alpha X), \ldots, P_{i_j}(\alpha^{(\ell-1)}X))^T$, $i_j \in I$, is a non-zero determinant in $\mathbb{F}[X]$. But note that this matrix is a submatrix of M_I. Therefore M_I has rank ℓ in $\mathbb{F}(X)$. Therefore the vectors $D_{i_1}, \ldots, D_{i_\ell}$ are linearly independent in $\mathbb{F}(X)$. This completes the proof of the forward direction.

Let $I \subseteq \{1, \ldots, m\}$ such that $|I| = \ell \leq k$ and let $D_{i_1}^T, \ldots, D_{i_\ell}^T$ be linearly independent in M_k over $\mathbb{F}(X)$, where $I = \{i_1, \ldots, i_\ell\}$. We will show that the corresponding set of columns $C_{i_1}, \ldots, C_{i_\ell}$ are also linearly independent over $\mathbb{F}$. For a contradiction assume that

$C_{i_1}, \ldots, C_{i_\ell}$ are linearly *dependent* over $\mathbb{F}$. Let $P_{i_1}(X), \ldots, P_{i_\ell}(X)$ be the polynomials in $\mathbb{F}[X]$ corresponding to these vectors. Then by Lemma 3.1 we have that $P_{i_1}(X), \ldots, P_{i_\ell}(X)$ are linearly dependent over $\mathbb{F}$. So there is a tuple $a_{i_1}, \ldots, a_{i_\ell}$ of values of $\mathbb{F}$ such that $\sum_{j=1}^{\ell} a_{i_j} P_{i_j}(X) = 0$. Therefore, for any $d \in \{1, \ldots, \ell-1\}$, we have that $\sum_{j=1}^{\ell} a_{i_j} P_{i_j}(\alpha^d X) = 0$. Now let $D_{i_1}^T, \ldots, D_{i_\ell}^T$ be the column vectors of M_k corresponding to $C_{i_1}, \ldots, C_{i_\ell}$. Note that $\mathbb{F}$ is a subfield of $\mathbb{F}(X)$ and by the above, we have that $\sum_{j=1}^{\ell} a_{i_j} D_{i_j} = 0$. Thus $D_{i_1}^T, \ldots, D_{i_\ell}^T$ are linearly dependent in M_k over $\mathbb{F}(X)$, a contradiction to our assumption.

Thus we have shown that for any $\{i_1, \ldots, i_\ell\} \subseteq \{1, \ldots, m\}$ such that $\ell \leq k$, $C_{i_1}, \ldots, C_{i_\ell}$ are linearly independent over $\mathbb{F}$ if and only if $D_{i_1}, \ldots, D_{i_\ell}$ are linearly independent over $\mathbb{F}(X)$. To estimate the running time, observe that for each C_i we can compute D_i in $\mathcal{O}(kn)$ field operations and thus we can compute M_k in $\mathcal{O}(mnk)$ field operations. This completes the proof of this lemma. ☐

In Lemma 3.11 we require that the field $\mathbb{F}$ contain at least $nk+1$ elements, and further α be an element of order at least n. We can ensure these requirements by preprocessing the input before invoking the Lemma 3.11. Formally, we have the following lemma.

LEMMA 3.12. *Let M be a $n \times m$ matrix of rank n over a field $\mathbb{F}$, and of rank n. Let $\mathbb{F} = \mathbb{F}_{p^\ell}$ where $p < n$, and let $n' \geq n$ be an integer. Then in time polynomial in m, n', p and ℓ, we can find an extension field $\mathbb{K}$ of order at least $n'+1$ and an element $\alpha \in \mathbb{K}$ of order at least n', such that M is a matrix over $\mathbb{K}$ with the same linear independence relationships between it's columns as before.*

PROOF. We distinguish two cases by comparing the values of p^ℓ and n.

Case 1: $p^\ell \leq n'+1$ In this case we use Lemma 3.9 to obtain an extension $\mathbb{K}$ of $\mathbb{F}$ of size at most $(n'+1)^2$, and an element $\alpha \in \mathbb{K}$ of order at least n' in polynomial time.

Case 2: $p^\ell > n'+1$ In this case we set $\mathbb{K} = \mathbb{F}$ and use Lemma 3.8 to find an element of order at least n', in time $\mathsf{poly}(p, \ell, n')$.

Observe that $\mathbb{F}$ is a subfield of $\mathbb{K}$ and M is also a matrix over $\mathbb{K}$. Thus, any collection of linearly dependent columns over $\mathbb{F}$ continue to be linearly dependent over $\mathbb{K}$. Similarly, any collection of linearly independent columns continue to be linearly independent. This completes the proof of this lemma. ☐

Next we show a result that allows us to find basis of matrices with entries from $\mathbb{F}[X]$.

LEMMA 3.13. *Let M be a $m \times t$ matrix with entries from $\mathbb{F}[X]^{<n}$ and let $m \leq t$. Let $w : \mathbf{C}(M) \to \mathbb{R}^+$ be a weight function. Then we can compute minimum weight column basis of M in $\mathcal{O}(m^2n^2t + m^\omega nt)$ field operations over $\mathbb{F}$*

PROOF. Let $S \subseteq \mathbb{F}^*$ be a set of size $(n-1)m+1$ and for every $\alpha \in S$, let $M(\alpha)$ be the matrix obtained by substituting α for X in the polynomials in matrix M. Now we compute the minimum weight column basis $C(\alpha)$ in $M(\alpha)$ for all $\alpha \in S$. Let $\ell = \max\{|C(\alpha)| \mid \alpha \in S\}$. Among all the column basis of size ℓ, let $C(\zeta)$ be a minimum weighted column basis for some $\zeta \in S$. Let C' be the columns in M corresponding to $C(\zeta)$. We will prove that C' is a minimum weighted column basis of M. Towards this we start with the following claim.

CLAIM 1. *The rank of M is the maximum of the rank of matrices $M(\alpha)$, $\alpha \in S$.*

PROOF. Let $r \leq m$ be the rank of M. Thus, we know that there exists a submatrix $W$of M of dimension $r \times r$ such that $\det(W)$ is a non-zero polynomial. The degree of the polynomial $\det(W(X)) \leq (n-1) \times r \leq (n-1)m$. Thus, we know that it has at-most $(n-1)m$ roots.

Hence, when we evaluate $\det(W(X))$ on set S of size more than $(n-1)m$, there exists at least one element in S, say β, such that $\det(W(\beta)) \neq 0$. Thus, the rank of M is upper bounded by the rank of $M(\beta)$ and hence upper bounded by the maximum of the rank of matrices $M(\alpha)$, $\alpha \in S$.

As before let $r \leq \ell$ be the rank of M. Let α be an arbitrary element of S. Observe that for any submatrix Z of dimension $r' \times r'$, $r' > r$ we have that $\det(Z(X)) \equiv 0$. Thus, for any α, the determinant of the corresponding submatrix of $M(\alpha)$ is also 0. This implies that for any α, the rank of $M(\alpha)$ is at most r. This completes the proof. $\square$

Claim 1 implies that $\ell = \max\{|C(\alpha)| \mid \alpha \in S\}$ is equal to the rank of M. Our next claim is following.

Claim 2. *For any $\alpha \in S$, and $C \subseteq \mathbf{C}(M(\alpha))$, if C is linearly independent in $M(\alpha)$ then C is also linearly independent in M.*

The proof follows from the arguments similar to the ones used in proving reverse direction of Claim 1. Let $r \leq m$ be the rank of M and let C^* be a minimum weight column basis of M. Thus, we know that there exists a submatrix W of M of dimension $r \times r$ such that $\det(W)$ is a non-zero polynomial. The degree of the polynomial $\det(W(X)) \leq (n-1) \times r \leq (n-1)m$. Thus, we know that it has at most $(n-1)r$ roots. Hence, when we evaluate $\det(W(X))$ on set S of size more than $(n-1)r$, there exists at least one element in S, say β, such that $\det(W(\beta)) \neq 0$ and the set of columns C^* is linearly independent in $M(\beta)$. Using Claim 2 and the fact that C^* is linearly independent in both $M(\beta)$ and M, we can conclude that C^* is a column basis for $M(\beta)$. Since $|C'| = |C^*|$, $w(C') \leq w(C^*)$, C' is indeed a minimum weighted column basis of M.

We can obtain any $M(\alpha)$ with at most $\mathcal{O}(nmt)$ field operations in $\mathbb{F}$. Furthermore, we can compute minimum weight column basis of $M(\alpha)$ in $\mathcal{O}(tm^{\omega-1})$ field operations [2]. Hence the total number of field operations over $\mathbb{F}$ is bounded by $\mathcal{O}(m^2n^2t + m^{\omega}nt)$. $\square$ $\square$

Finally, we combine Lemma 3.10, Lemma 3.12 and Lemma 3.11 to obtain the following theorem.

Theorem 3.14 (Theorem 1.1, restated). *Let M be a $n \times m$ matrix over $\mathbb{F}$ of rank n. Given a number $k \leq n$, we can compute a matrix M_k over the field $\mathbb{F}(X)$ such that it is a representation of the k-truncation of M, in $\mathcal{O}(mnk)$ field operations over $\mathbb{F}$. Furthermore, given M_k, we can test whether a given set of ℓ columns in M_k are linearly independent in $\mathcal{O}(n^2k^3)$ field operations over $\mathbb{F}$.*

Proof. Let $p = \text{char}(\mathbb{F})$. We first consider the case when $p = 0$ or $p > n$. In this case we apply Lemma 3.10 to obtain a matrix M_k over $\mathbb{F}(X)$ which is a k-truncation of M. Next, we consider the case when $\mathbb{F}$ is a finite field and the characteristic of $\mathbb{F}$ is at most n, i.e. $p \leq n$. First apply Lemma 3.12 to ensure that the order of the field $\mathbb{F}$ is at least $nk+1$ and to obtain an element of order at least n in the field $\mathbb{F}$. Of course by doing this, we have gone to an extension of $\mathbb{K}$ of $\mathbb{F}$ of size at least $nk+1$. However, for brevity of presentation we will assume that the input is given over such an extension. We then apply Lemma 3.11 to obtain a matrix M_k over $\mathbb{F}(X)$ which is a representation of the k-truncation of the matrix M. This completes the description of M_k.

Let $I \subseteq \{1, \ldots, m\}$ such that $|I| = \ell \leq k$. Let $D_{i_1}, \ldots, D_{i_\ell}$ be a set of columns of the matrix M_k over $\mathbb{F}$, where $I = \{i_1, \ldots, i_\ell\}$. Furthermore, by M_I we denote the $k \times \ell$ submatrix of M_k containing the columns $D_{i_1}, \ldots, D_{i_\ell}$. To test whether these columns are linearly independent, we can apply Lemma 3.13 on M_I^T and see the size of column basis of M_I^T is ℓ or not. This takes time $\mathcal{O}(\ell^2 n^2 k + \ell^\omega nk) = \mathcal{O}(n^2k^3)$ field operations in $\mathbb{F}$. $\square$

Observe that, using Theorem 1.1 we can obtain a deterministic truncation of a matrix over any field where the field operations can be done efficiently. This includes any finite field ($\mathbb{F}_{p^\ell}$) and field of rationals $\mathbb{Q}$.

Representing the truncation over a finite field. In Theorem 3.14, the representation M_k is over the field $\mathbb{F}(X)$. However, in some cases this matrix can also be viewed as a representation over a finite extension of $\mathbb{F}$ of sufficiently large degree, which is useful for algorithmic applications. That is, if $\mathbb{F} = \mathbb{F}_{p^\ell}$ is a finite field then M_k will be a matrix over $\mathbb{F}_{p^{\ell'}}$ where $\ell' \geq nk\ell$. Formally, we have the following corollary.

THEOREM 3.15. *Let M be a $n \times m$ matrix over $\mathbb{F}$ of rank n, $k \leq n$ be a positive integer and N be the size of the input matrix. If $\mathbb{F} = \mathbb{F}_p$ be a prime field or $\mathbb{F} = \mathbb{F}_{p^\ell}$ where $p = N^{\mathcal{O}(1)}$, then in polynomial time we can find a k-truncation M_k of M over a finite extension $\mathbb{K}$ of $\mathbb{F}$ where $\mathbb{K} = \mathbb{F}_{p^{nk\ell}}$.*

PROOF. Let M_k be the matrix returned by Theorem 3.14. Next we show how we can view the entries in M_k over a finite extension of $\mathbb{F}$. Consider any extension $\mathbb{K}$ of $\mathbb{F}$ of degree $r \geq nk$. Thus $\mathbb{K} = \frac{\mathbb{F}[X]}{r(X)}$, where $r(X)$ is a irreducible polynomial in $\mathbb{F}[X]$ of degree r. Recall that each entry of M_k is a polynomial in $\mathbb{F}[X]$ of degree at most $n-1$ and therefore they are present in $\mathbb{K}$. Further the determinant of any $k \times k$ submatrix of M_k is identically zero in $\mathbb{K}$ if and only if it is identically zero in $\mathbb{F}(X)$. This follows from the fact that the determinant is a polynomial of degree at most $(n-1)k$ and therefore is also present in $\mathbb{K}$. Thus M_k is a representation over $\mathbb{K}$.

To specify the field $\mathbb{K}$ we need to compute the irreducible polynomial $r(X)$. If $\mathbb{F}$ is a prime field, i.e. $\mathbb{F} = \mathbb{F}_p$, then we can compute the polynomial $r(X)$ using the first part of Lemma 3.6. And if $p = N^{\mathcal{O}(1)}$ we can use the second part of Lemma 3.6 to compute $r(X)$. Thus we have a well defined k-truncation of M over the finite field $\mathbb{K} = \frac{\mathbb{F}[X]}{r(X)}$. Furthermore, if degree of $r(X)$ is nk then $\mathbb{K}$ is isomorphic to $\mathbb{F}_{p^{nk\ell}}$. This completes the proof of this theorem. $\square$

4 DETERMINISTIC COMPUTATION OF REPRESENTATIVE FAMILIES

In this section we give deterministic algorithms to compute representative families of a linear matroid, given its representation matrix. We start with the definition of a *q-representative family.*

*Definition 4.1 (q-**Representative Family**).* Given a matroid $M = (E, \mathcal{I})$ and a family $\mathcal{S}$ of subsets of E, we say that a subfamily $\widehat{\mathcal{S}} \subseteq \mathcal{S}$ is *q-representative* for $\mathcal{S}$ if the following holds: for every set $Y \subseteq E$ of size at most q, if there is a set $X \in \mathcal{S}$ disjoint from Y with $X \cup Y \in \mathcal{I}$, then there is a set $\widehat{X} \in \widehat{\mathcal{S}}$ disjoint from Y with $\widehat{X} \cup Y \in \mathcal{I}$. If $\hat{\mathcal{S}} \subseteq \mathcal{S}$ is q-representative for $\mathcal{S}$ we write $\widehat{\mathcal{S}} \subseteq_{rep}^{q} \mathcal{S}$.

In other words if some independent set in $\mathcal{S}$ can be extended to a larger independent set by q new elements, then there is a set in $\widehat{\mathcal{S}}$ that can be extended by the same q elements. We say that a family $\mathcal{S} = \{S_1, \ldots, S_t\}$ of sets is a *p-family* if each set in $\mathcal{S}$ is of size p. In [11] the following theorem is proved.

THEOREM 4.2 ([11]). *Let $M = (E, \mathcal{I})$ be a linear matroid and let $\mathcal{S} = \{S_1, \ldots, S_t\}$ be a p-family of independent sets. Then there exists $\hat{\mathcal{S}} \subseteq_{rep}^{q} \mathcal{S}$ of size $\binom{p+q}{p}$. Furthermore, given a* *representation A_M of M over a field $\mathbb{F}$, there is a randomized algorithm computing $\widehat{\mathcal{S}} \subseteq^q_{rep} \mathcal{S}$ in $\mathcal{O}\left(\binom{p+q}{p} tp^{\omega} + t\binom{p+q}{q}^{\omega-1}\right)$ operations over $\mathbb{F}$.*

Let $p+q=k$. Fomin et al. [11, Theorem 3.7] first give a deterministic algorithm for computing q-representative of a p-family of independent sets if the rank of the corresponding matroid is $p+q$. To prove Theorem 4.2 one first computes the representation matrix of a k-truncation of $M=(E,\mathcal{I})$. This step returns a representation of a k-truncation of $M=(E,\mathcal{I})$ with a high probability. Given this matrix, one applies [11, Theorem 3.7] and arrives at Theorem 4.2. In this section we design a deterministic algorithm for computing q-representative even if the underlying linear matroid has unbounded rank, using deterministic truncation of linear matroids.

Observe that the representation given by Theorem 3.14 is over $\mathbb{F}(X)$. For the purpose of computing q-representative of a p-family of independent sets we need to find a set of linearly independent columns over a matrix with entries from $\mathbb{F}[X]$. However, deterministic algorithms to compute basis of matrices over $\mathbb{F}[X]$ is not as fast as compared to the algorithms where we do not need to do symbolic computation. We start with a lemma that allows us to find a spanning set of columns of a matrix over $\mathbb{F}[X]$ quickly; though the size of the set returned by the algorithm given by the lemma could be slightly larger than the basis of the given matrix.

Definition 2. *Let $W=\{v_1,\ldots,v_m\}$ be a set of vectors over $\mathbb{F}$ and $w: W \to \mathbb{R}^+$. We say that $S \subseteq W$ is a* spanning set*, if every $v \in W$ can be written as linear combination of vectors in S with coefficients from $\mathbb{F}$. We say that S is a* nice spanning set *of W, if S is a spanning set and for any $z \in W$ if $z=\sum_{v\in S} \lambda_v v$, and $0 \neq \lambda_v \in \mathbb{F}$ then we have $w(v) \leq w(z)$.*

The following lemma enables us to find a small size spanning set of vectors over $\mathbb{F}(X)$.

Lemma 4.3. *Let $\mathbb{F}$ be a field and let $M \in \mathbb{F}[X]^{m\times t}$ be a matrix over $\mathbb{F}[X]^{<n}$ and let $w: \mathbf{C}(M) \to \mathbb{R}^+$ be a weight function. Then we can find a nice spanning set S of $\mathbf{C}(M)$ of size at most nm with at most $\mathcal{O}(t(nm)^{\omega-1})$ field operations over $\mathbb{F}$.*

Proof. The main idea is to do a “gaussian elimination” in M, but only over the subfield $\mathbb{F}$ of $\mathbb{F}(X)$. Let C_i be a column of the matrix M. It is a vector of length m over $\mathbb{F}[X]^{<n}$ and it's entries are polynomials $P_{ji}(X)$, where $j \in \{1,\ldots,m\}$. Observe that $P_{ji}(X)$ is a polynomial of degree $n-1$ with coefficients from $\mathbb{F}$. Let v_{ji} denote the vector of length n corresponding to the polynomial $P_{ji}(X)$. Consider the column vector v_i formed by concatenating each v_{ji} in order from $j=1$ to m. That is, $v_i=(v_{1i},\ldots,v_{mi})^T$. This vector has length nm and has entries from $\mathbb{F}$. Let N be the matrix where columns correspond to column vectors v_i. Note that N is a matrix over $\mathbb{F}$ of dimension $nm \times t$ and the time taken to compute N is $\mathcal{O}(tnm)$. For each column v_i of N we define it's weight to be $w(C_i)$. We now compute a minimum weight set of column vectors S', which spans N over the field $\mathbb{F}$. Observe that $|S'| \leq nm$ and time taken to compute it is $\mathcal{O}(t(nm)^{\omega-1})$ [2]. Let S be the set of column vectors in M corresponding to the column vectors in S'. We return S as a nice spanning set of column vectors in M.

Now we show the correctness of the above algorithm. We first show that S is a spanning set of M. Let $v_1,\ldots,v_{|S|}$ be the set of vectors in S and let v_d be some column vector in N. Then $v_d=\sum_{i=1}^{|S|} a_i v_i$ where $a_i \in \mathbb{F}$. In particular for any $j \in \{1,\ldots,m\}$ we have $v_{jd}=\sum_{i=1}^{|S|} a_i v_{ji}$. Let $C_1,\ldots,C_{|S|}$ be the column vectors corresponding to $v_1,\ldots,v_{|S|}$ and let C_d be the column vector corresponding to v_d. We claim that $C_d = \sum_{i=1}^{|S|} a_i C_i$. Consider the j-the entry of the column vector C and of $C_1, \ldots, C_{|S|}$. Towards our claim we need to show that $P_{jd}(X) = \sum_{i=1}^{|S|} a_i P_{ji}(X)$. But since v_{dj} and $\{v_{ij} \mid j \in \{1, \ldots, m\}\}$ are the collection of vectors corresponding to $P_{jd}(X)$ and $\{P_{ji}(X) \mid j \in \{1, \ldots, m\}\}$, the claim follows.

Next we show that S is indeed a nice spanning set. Since S is a spanning set of M we have that any column $C_d = \sum_{C_i \in S} \lambda_i C_i$, $\lambda_i \in \mathbb{F}$. Let $C_j \in S$ be such that $\lambda_j \neq 0$ and $w(C_j) > w(C_d)$. Let v_d and v_j be the vectors corresponding to C_d and C_j respectively. We have that $v_d = \sum_{v_i \in S} \lambda_i v_i$, which implies $v_j = \lambda_j^{-1} v_d - \sum_{v_i \in S, v_i \neq v_j} \lambda_j^{-1} \lambda_i v_i$. But this implies that $S^* = (S \setminus \{v_j\}) \cup \{v_d\}$ is a spanning set of N, and $w(S^*) < w(S)$, which is a contradiction. Thus we have that for every column vector $C \in M$ if $C = \sum_{C_i \in S} \lambda_i C_i$ and $0 \neq \lambda_i \in \mathbb{F}$, then $w(C_i) \leq w(C)$. This completes the proof. ☐

The main theorem of this section is as follows.

Theorem 4.4 (Theorem 1.3, restated). *Let $M = (E, \mathcal{I})$ be a linear matroid of rank n and let $\mathcal{S} = \{S_1, \ldots, S_t\}$ be a p-family of independent sets. Let A be a $n \times |E|$ matrix representing M over a field $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_{p^\ell}$ or $\mathbb{F}$ is $\mathbb{Q}$. Then there are deterministic algorithms computing $\widehat{\mathcal{S}} \subseteq^q_{rep} \mathcal{S}$ as follows.*

(i) A family $\widehat{\mathcal{S}}$ of size $\binom{p+q}{p}$ in $\mathcal{O}\left(\binom{p+q}{p}^2 tp^3n^2 + t\binom{p+q}{q}^\omega np\right) + (n+|E|)^{\mathcal{O}(1)}$, operations over $\mathbb{F}$.

(ii) A family $\widehat{\mathcal{S}}$ of size $np\binom{p+q}{p}$ in $\mathcal{O}\left(\binom{p+q}{p} tp^3n^2 + t\binom{p+q}{q}^{\omega-1}(pn)^{\omega-1}\right) + (n+|E|)^{\mathcal{O}(1)}$ operations over $\mathbb{F}$.

Proof. Let $p + q = k$ and $|E| = m$. We start by finding k-truncation of A, say A_k, over $\mathbb{F}[X] \subseteq \mathbb{F}(X)$ using Theorem 3.14. We can find A_k with at most $(n+m)^{\mathcal{O}(1)}$ operations over $\mathbb{F}$. Given the matrix A_k we follow the proof of [11, Theorem 3.7]. For a set $S \in \mathcal{S}$ and $I \in \binom{[k]}{p}$, we define $s[I] = \det(A_k[I, S])$. We also define the following.

$$\vec{s_i} = (s_i[I])_{I \in \binom{[k]}{p}}$$

Thus the entries of the vector $\vec{s_i}$ are the values of $\det(A_k[I, S_i])$, where I runs through all the p sized subsets of rows of A_k. Let $H_{\mathcal{S}} = (\vec{s}_1, \ldots, \vec{s}_t)$ be the $\binom{k}{p} \times t$ matrix obtained by taking $\vec{s_i}$ as columns. Observe that each entry in A_k is in $\mathbb{F}[X]^{<n}$. Thus, the determinant polynomial corresponding to any $p \times p$ submatrix of A_k has degree at most pn. As we can find determinant of a $p \times p$ matrix over $\mathbb{F}[X]^{<n}$ in time $\mathcal{O}(p^3n^2)$ [33]. Thus, we can obtain $H_{\mathcal{S}}$ in time $\mathcal{O}(t\binom{p+q}{p}p^3n^2)$.

Let W be a spanning set of columns for $\mathbf{C}(H_{\mathcal{S}})$. We define $\widehat{W} = \{S_\alpha \mid \vec{s}_\alpha \in W\}$ as the corresponding subfamily of $\mathcal{S}$. The proof of [11, Theorem 3.7] implies that if W is a spanning set of columns for $\mathbf{C}(H_{\mathcal{S}})$ then the corresponding $\widehat{W}$ is the required q-representative family for $\mathcal{S}$. That is, $\widehat{W} \subseteq^q_{rep} \mathcal{S}$. We get the desired running time by either using Lemma 3.13 to compute a basis of size $\binom{p+q}{p}$ for $H_{\mathcal{S}}$ or by using Lemma 4.3 to compute a spanning set of size $np\binom{p+q}{p}$ of $\mathbf{C}(H_{\mathcal{S}})$. This completes the proof. ☐

In fact one can prove Theorem 4.4 for a "weighted notion of representative family". This requires the notion of a nice spanning set. It is presented in the following section.

Weighted representative families of linear matroids. In this section we give deterministic algorithms for the weighted version of representative families of a linear matroid. It is useful in solving problems where we are looking for objects of maximum or minimum weight. We refer to [11, Theorem 3.7] for further discussions. Given a non-negative weight function $w : E \to \mathbb{R}^+$ and $A \subseteq E$, we define $w(A) = \sum_{a \in A} w(a)$, a weighted version of q-representative families is defined as follows.

Definition 3 (**Min/Max q-Representative Family**). *Given a matroid $M = (E, \mathcal{I})$, a family $\mathcal{S}$ of subsets of E and a non-negative weight function $w : \mathcal{S} \to \mathbb{R}^+$, we say that a subfamily $\widehat{\mathcal{S}} \subseteq \mathcal{S}$ is* min q-representative *(*max q-representative*) for $\mathcal{S}$ if the following holds: for every set $Y \subseteq E$ of size at most q, if there is a set $X \in \mathcal{S}$ disjoint from Y with $X \cup Y \in \mathcal{I}$, then there is a set $\widehat{X} \in \widehat{\mathcal{S}}$ disjoint from Y with*

(i) $\widehat{X} \cup Y \in \mathcal{I}$; and

(ii) $w(\widehat{X}) \leq w(X)$ $(w(\widehat{X}) \geq w(X))$.

We use $\widehat{\mathcal{S}} \subseteq^q_{minrep} \mathcal{S}$ ($\widehat{\mathcal{S}} \subseteq^q_{maxrep} \mathcal{S}$) to denote a min q-representative (max q-representative) family for $\mathcal{S}$.

For our proof we also need the following well-known generalized Laplace expansion of determinants. For a matrix $A = (a_{ij})$, the row set and the column set are denoted by $\mathbf{R}(A)$ and $\mathbf{C}(A)$ respectively. For $I \subseteq \mathbf{R}(A)$ and $J \subseteq \mathbf{C}(A)$, $A[I, J] = \big(a_{ij} \mid i \in I,\ j \in J\big)$ means the submatrix (or minor) of A with the row set I and the column set J. For $I \subseteq [n]$ let $\bar{I} = [n] \setminus I$ and $\sum I = \sum_{i \in I} i$.

Proposition 4.5 (Generalized Laplace expansion). *For an $n \times n$ matrix A and $J \subseteq \mathbf{C}(A) = [n]$, it holds that*

$$\det(A) = \sum_{I \subseteq [n], |I| = |J|} (-1)^{\sum I + \sum J} \det(A[I, J]]) \det(A[\bar{I}, \bar{J}])$$

We refer to [34, Proposition 2.1.3] for a proof of the above identity. We always assume that the number of rows in the representation matrix A_M of M over a field $\mathbb{F}$ is equal to $\mathsf{rank}(M)$=$\mathsf{rank}(A_M)$. Otherwise, using Gaussian elimination we can obtain a matrix of the desired kind in polynomial time. See [31, Proposition 3.1] for details. The main theorem in this section is as follows.

Theorem 4.6. *Let $M = (E, \mathcal{I})$ be a linear matroid of rank n and let $\mathcal{S} = \{S_1, \dots, S_t\}$ be a p-family of independent sets. Let $w : \mathcal{S} \to \mathbb{R}^+$ is a non-negative weight function on $\mathcal{S}$. Let A be a $n \times |E|$ matrix representing M over a field $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_{p^\ell}$ or $\mathbb{F}$ is $\mathbb{Q}$. Then there are deterministic algorithms computing $\widehat{\mathcal{S}} \subseteq^q_{minrep} \mathcal{S}$ as follows.*

(i) A family $\widehat{\mathcal{S}}$ of size $\binom{p+q}{p}$ in $\mathcal{O}\left(\binom{p+q}{p}^2 tp^3n^2 + t\binom{p+q}{q}^\omega np\right) + (n + |E|)^{\mathcal{O}(1)}$, operations over $\mathbb{F}$.

(ii) A family $\widehat{\mathcal{S}}$ of size $np\binom{p+q}{p}$ in $\mathcal{O}\left(\binom{p+q}{p} tp^3n^2 + t\binom{p+q}{q}^{\omega-1}(pn)^{\omega-1}\right) + (n + |E|)^{\mathcal{O}(1)}$ operations over $\mathbb{F}$.

Proof. Let $p + q = k$ and $|E| = m$. We start by finding k-truncation of A, say A_k, over $\mathbb{F}[X] \subseteq \mathbb{F}(X)$ using Theorem 3.14. We can find A_k with at most $(n + m)^{\mathcal{O}(1)}$ operations over $\mathbb{F}$. Given the matrix A_k we follow the proof of [11, Theorem 3.7]. For a set $S \in \mathcal{S}$ and $I \in \binom{[k]}{p}$, we define $s[I] = \det(A_k[I, S])$. We also define the following.

$$\vec{s_i} = (s_i[I])_{I \in \binom{[k]}{p}}$$

Thus the entries of the vector $\vec{s}_i$ are the values of $\det(A_k[I, S_i])$, where I runs through all the p sized subsets of rows of A_k. Let $H_{\mathcal{S}} = (\vec{s}_1, \ldots, \vec{s}_t)$ be the $\binom{k}{p} \times t$ matrix obtained by taking $\vec{s}_i$ as columns. Observe that each entry in A_k is in $\mathbb{F}[X]^{<n}$. Thus, the determinant polynomial corresponding to any $p \times p$ submatrix of A_k has degree at most pn. It is well known that we can find determinant of a $p \times p$ matrix over $\mathbb{F}[X]^{<n}$ in time $\mathcal{O}(p^3n^2)$ [33]. Thus, we can obtain $H_{\mathcal{S}}$ in time $\mathcal{O}(t\binom{p+q}{p}p^3n^2)$.

Now we define a weight function $w' : \mathbf{C}(H_{\mathcal{S}}) \to \mathbb{R}^+$ on the set of columns of $H_{\mathcal{S}}$. For the column $\vec{s}_i$ corresponding to $S_i \in \mathcal{S}$, we define $w'(\vec{s}_i) = w(S_i)$. Let W be a spanning set of columns for $\mathbf{C}(H_{\mathcal{S}})$. We define $\widehat{\mathcal{S}} = \{S_\alpha \mid \vec{s}_\alpha \in W\}$ as the corresponding subfamily of $\mathcal{S}$. Now we claim that if W is a nice spanning set of columns for $\mathbf{C}(H_{\mathcal{S}})$ or minimum weight column basis of $\mathbf{C}(H_{\mathcal{S}})$, then the corresponding $\widehat{\mathcal{S}}$ is the required min q-representative family for $\mathcal{S}$. That is, $\widehat{\mathcal{S}} \subseteq^q_{minrep} \mathcal{S}$. Observe that, if W is a minimum weight column basis of $\mathbf{C}(H_{\mathcal{S}})$, then the claim follows from the proof of [11, Theorem 3.7].

Now we show that if W is a nice spanning set of columns for $\mathbf{C}(H_{\mathcal{S}})$, then $\widehat{\mathcal{S}} \subseteq^q_{minrep} \mathcal{S}$. Let $S_\beta \in \mathcal{S}$ such that $S_\beta \notin \widehat{\mathcal{S}}$. We show that if there is a set $Y \subseteq E$ of size at most q such that $S_\beta \cap Y = \emptyset$ and $S_\beta \cup Y \in \mathcal{I}$, then there exists a set $\widehat{S}_\beta \in \widehat{\mathcal{S}}$ disjoint from Y with $\widehat{S}_\beta \cup Y \in \mathcal{I}$ and $w(\widehat{S}_\beta) \leq w(S_\beta)$. Let us first consider the case $|Y| = q$. Since $S_\beta \cap Y = \emptyset$ we have that $|S_\beta \cup Y| = p + q = k$. Furthermore, since $S_\beta \cup Y \in \mathcal{I}$, we have that the columns corresponding to $S_\beta \cup Y$ in M are linearly independent over $\mathbb{F}(X)$; that is, $\det(A_k[\mathbf{R}(A_k), S_\beta \cup Y]) \not\equiv 0$. Recall that, $\vec{s}_\beta = (s_\beta[I])_{I \in \binom{[k]}{p}}$, where $s_\beta[I] = \det(A_k[I, S_\beta])$. Similarly we define $y[L] = \det(A_k[L, Y])$ and $\vec{y} = (y[L])_{L \in \binom{[k]}{q}}$.

In the following, let $\sum J$ denote $\sum_{j \in S_\beta} j$. Then we define.

$$\gamma(\vec{s}_\beta, \vec{y}) = \sum_{I \in \binom{[k]}{p}} (-1)^{\sum I + \sum J} s_\beta[I] \cdot y[\bar{I}]$$

Since $\binom{k}{p} = \binom{k}{k-p} = \binom{k}{q}$ the above formula is well defined. Observe that by Proposition 4.5, we have that $\gamma(\vec{s}_\beta, \vec{q}) = \det(A_k[\mathbf{R}(A_k), S_\beta \cup Y]) \not\equiv 0$. We also know that $\vec{s}_\beta$ can be written as a linear combination of vectors in $W = \{\vec{s}_1, \vec{s}_2, \ldots, \vec{s}_\ell\}$. That is, $\vec{s}_\beta = \sum_{i=1}^{\ell} \lambda_i \vec{s}_i$, $\lambda_i \in \mathbb{F}$ and for some i, $\lambda_i \neq 0$. Thus,

$$\begin{aligned}
\gamma(\vec{s}_\beta, \vec{y}) &= \sum_I (-1)^{\sum I + \sum J} s_\beta[I] \cdot y[\bar{I}] \\
&= \sum_I (-1)^{\sum I + \sum J} \left(\sum_{i=1}^{\ell} \lambda_i s_i[I] \right) y[\bar{I}] \\
&= \sum_{i=1}^{\ell} \lambda_i \left(\sum_I (-1)^{\sum I + \sum J} s_i[I] y[\bar{I}] \right) \\
&= \sum_{i=1}^{\ell} \lambda_i \det(A_k[\mathbf{R}(A_k), S_i \cup Y]) \quad \text{(by Proposition 4.5)}
\end{aligned}$$

Define the following.

$$\mathsf{sup}(S_\beta) = \left\{ S_i \;\middle|\; S_i \in \widehat{\mathcal{S}},\ \lambda_i \det(A_k[\mathbf{R}(A_k), S_i \cup Y])) \not\equiv 0 \right\}$$

Since $\gamma(\vec{s}_\beta, \vec{y}) \neq 0$, we have that $(\sum_{i=1}^{\ell} \lambda_i \det(A_k[\mathbf{R}(A_k), S_i \cup Y])) \not\equiv 0$ and thus $\mathsf{sup}(S_\beta) \neq \emptyset$. Observe that for all $S \in \mathsf{sup}(S_\beta)$ we have that $\det(A_k[\mathbf{R}(A_k), S \cup Y]) \not\equiv 0$ and thus $S \cup Y \in \mathcal{I}$. Since W is a nice spanning set, If $\vec{s}_\beta = \sum_{i=1}^{\ell} \lambda_i \vec{s}_i$ and $0 \neq \lambda_i \in \mathbb{F}$, then $w(\vec{s}_\beta) \geq w(\vec{s}_i)$. Thus $w(\widehat{S}) \leq w(S)$ for all $S \in \mathsf{sup}(S_\beta)$. Thus $\widehat{S}$ is a min q-representative of S.

Suppose that $|Y| = q' < q$. Since M is a matroid of rank $k = p + q$, there exists a superset $Y' \in \mathcal{I}$ of Y of size q such that $S_\beta \cap Y' = \emptyset$ and $S_\beta \cup Y' \in \mathcal{I}$. This implies that there exists a set $\widehat{S} \in \widehat{\mathcal{S}}$ such that $\det(A_k[\mathbf{R}(A_k), \widehat{S} \cup Y']) \not\equiv 0$. Thus the columns corresponding to $\widehat{S} \cup Y$ are linearly independent.

Thus, if W is a minimum weight column basis of $\mathbf{C}(H_{\mathcal{S}})$ or a nice spanning set of columns for $\mathbf{C}(H_{\mathcal{S}})$ then the corresponding $\widehat{\mathcal{S}}$ is a min q-representative family for $\mathcal{S}$. By applying Lemma 3.13 to compute a basis of size $\binom{p+q}{p}$ for $H_{\mathcal{S}}$, we get min q-representative family for $\mathcal{S}$ of size $\binom{p+q}{p}$ in $\mathcal{O}\big(\binom{p+q}{p}^2 tp^3n^2 + t\binom{p+q}{q}^{\omega} np\big) + (n + |E|)^{\mathcal{O}(1)}$ operations over $\mathbb{F}$. By applying Lemma 4.3 to compute a nice spanning set of size $np\binom{p+q}{p}$ of $\mathbf{C}(H_{\mathcal{S}})$, we get min q-representative family for $\mathcal{S}$ of size $np\binom{p+q}{p}$ in $\mathcal{O}\left(\binom{p+q}{p} tp^3n^2 + t\binom{p+q}{q}^{\omega-1}(pn)^{\omega-1}\right) + (n + |E|)^{\mathcal{O}(1)}$ operations over $\mathbb{F}$. This completes the proof. ◻

4.1 Applications

Marx [31] gave algorithms for several problems based on matroid optimization. The main theorem in [31] is Theorem 1.1 on which most applications of [31] are based. This theorem gives a randomized FPT algorithm for the ℓ-Matroid Parity problem.

ℓ-Matroid Parity	**Parameter:** k, ℓ

Input: Let $M = (E, \mathcal{I})$ be a linear matroid where the ground set is partitioned into blocks of size ℓ and let A_M be a linear representation M.
Question: is there an independent set that is the union of k blocks ?

The proof of the theorem uses an algorithm to find representative sets as a black box. Applying our algorithm (Theorem 4.4 of this paper) instead gives a deterministic version of Theorem 1.1 of [31].

Proposition 4.7. *Let $M = (E, \mathcal{I})$ be a linear matroid where the ground set is partitioned into blocks of size ℓ. Given a linear representation A_M of M, it can be determined in $\mathcal{O}(2^{\omega k \ell}||A_M||^{\mathcal{O}(1)})$ time whether there is an independent set that is the union of k blocks. ($||A_M||$ denotes the length of A_M in the input.)*

We mention an application from [31] which we believe could be useful to obtain single exponential time parameterized and exact algorithms.

ℓ-Matroid Intersection	**Parameter:** k

Input: Let $M_1 = (E, \mathcal{I}_1), \ldots, M_1 = (E, \mathcal{I}_\ell)$ be matroids on the same ground set E given by their representations $A_{M_1}, \ldots, A_{M_\ell}$ over the same field $\mathbb{F}$ and a positive integer k.
Question: Does there exist k element set that is independent in each M_i ($X \in \mathcal{I}_1 \cap \ldots \cap \mathcal{I}_\ell$)?

By using Proposition 4.7 instead, we get the following result.

Proposition 4.8. *ℓ-Matroid Intersection can be solved in $\mathcal{O}(2^{\omega k \ell}||A_M||^{\mathcal{O}(1)})$ time.*

5 CONCLUSION

In this paper we give the first deterministic algorithm to compute a k-truncation of linear matroid. Our algorithms were based on the properties of the Wronskian determinant and the α-folded Wronskian determinant. We also show how these can be used to compute representative families over any linear matroid deterministically. We conclude with a few related open problems.

- Our algorithm produces a representation of the truncation over the ring $\mathbb{F}[X]$ when the input field is $\mathbb{F}$. However when $\mathbb{F}$ is large enough, then one can obtain a randomized representation of the truncation over $\mathbb{F}$ itself. It is an interesting problem to compute the representation over $\mathbb{F}$ deterministically. One should note that, even verifying if a given matrix is a truncation of another matrix seems to be a difficult problem.
- Finding a deterministic representation of Transversal matroids and Gammoids, remains interesting open problem in Matroid Theory. A solution to this problem will lead to a deterministic kernelization algorithm for several important graph problems in Parameterized Complexity [26, 27].

ACKNOWLEDGMENTS

We sincerely thank all the anonymous reviewers for their insightful comments and suggestions and for pointing out the results of Forbes and Shpilka [14], and Gabizon and Raz [17] to us, which we were unaware of.

Daniel Lokshtanov was supported by the Bergen Research Foundation and the University of Bergen through project “BeHard” and by the European Research Council through ERC Starting Grant Agreement no. 715744) (PaPaAlg). Fahad Panolan was supported by the European Research Council through ERC Grant Agreement no. 267959. Pranabendu Misra and Saket Saurabh are supported by the European Research Council through ERC Starting Grant Agreement no. 306992 (PARAPPROX).

REFERENCES

[1] Leonard M. Adleman and Hendrik W. Lenstra Jr. 1986. Finding Irreducible Polynomials over Finite Fields. In *STOC*. 350–355.

[2] Hans L. Bodlaender, Marek Cygan, Stefan Kratsch, and Jesper Nederlof. 2013. Deterministic Single Exponential Time Algorithms for Connectivity Problems Parameterized by Treewidth. In *ICALP*, Vol. 7965. 196–207.

[3] B. Bollobás. 1965. On generalized graphs. *Acta Math. Acad. Sci. Hungar* 16 (1965), 447–452.

[4] Alin Bostan and Philippe Dumas. 2010. Wronskians and linear independence. *The American Mathematical Monthly* 117, 8 (2010), 722–727.

[5] Marek Cygan, Dániel Marx, Marcin Pilipczuk, Michal Pilipczuk, and Ildikó Schlotter. 2014. Parameterized Complexity of Eulerian Deletion Problems. *Algorithmica* 68, 1 (2014), 41–61.

[6] Sanjoy Dasgupta and Anupam Gupta. 2003. An elementary proof of a theorem of Johnson and Lindenstrauss. *Random Struct. Algorithms* 22, 1 (2003), 60–65.

[7] Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan. 2009. Extensions to the method of multiplicities, with applications to Kakeya sets and mergers. In *FOCS*. IEEE, 181–190.

[8] Fedor V. Fomin and Petr A. Golovach. 2013. Long Circuits and Large Euler Subgraphs. In *ESA*, Vol. 8125. 493–504.

[9] Fedor V. Fomin and Petr A. Golovach. 2014. Parameterized complexity of connected even/odd subgraph problems. *J. Comput. Syst. Sci.* 80, 1 (2014), 157–179.

[10] Fedor V. Fomin, Daniel Lokshtanov, Fahad Panolan, and Saket Saurabh. 2014. Representative Sets of Product Families. In *ESA*. 443–454.

[11] Fedor V. Fomin, Daniel Lokshtanov, Fahad Panolan, and Saket Saurabh. 2016. Efficient Computation of Representative Families with Applications in Parameterized and Exact Algorithms. *J. ACM* 63, 4 (2016).

[12] Fedor V. Fomin, Daniel Lokshtanov, and Saket Saurabh. 2014. Efficient Computation of Representative Sets with Applications in Parameterized and Exact Algorithms. In *SODA*. 142–151.

[13] Michael A. Forbes, Ramprasad Saptharishi, and Amir Shpilka. 2014. Hitting sets for multilinear read-once algebraic branching programs, in any order. In *STOC*. 867–875.

[14] Michael A Forbes and Amir Shpilka. 2012. On identity testing of tensors, low-rank recovery and compressed sensing. In *STOC*. ACM, 163–172.

[15] P. Frankl. 1982. An extremal problem for two families of sets. *European J. Combin.* 3, 2 (1982), 125–127.

[16] Ariel Gabizon. 2011. *Deterministic Extraction from Weak Random Sources*. Springer. i–xi, 1–148 pages.

[17] Ariel Gabizon and Ran Raz. 2008. Deterministic extractors for affine sources over large fields. *Combinatorica* 28, 4 (2008), 415–440.

[18] François Le Gall. 2014. Powers of tensors and fast matrix multiplication. In *ISSAC*. 296–303.

[19] Arnaldo Garcia and Jose Felipe Voloch. 1987. Wronskians and linear independence in fields of prime characteristic. *Manuscripta Mathematica* 59, 4 (1987), 457–469.

[20] David Goldschmidt. 2003. *Algebraic functions and projective curves*. Vol. 215. Springer.

[21] Prachi Goyal, Neeldhara Misra, and Fahad Panolan. 2013. Faster Deterministic Algorithms for r-Dimensional Matching Using Representative Sets. In *FSTTCS*. 237–248.

[22] Prachi Goyal, Pranabendu Misra, Fahad Panolan, Geevarghese Philip, and Saket Saurabh. 2015. Finding Even Subgraphs Even Faster. In *FSTTCS*. 434–447.

[23] Venkatesan Guruswami and Swastik Kopparty. 2013. Explicit Subspace Designs. In *FOCS*. 608–617.

[24] Venkatesan Guruswami and Swastik Kopparty. 2016. Explicit subspace designs. *Combinatorica* 36, 2 (2016), 161–185.

[25] William B. Johnson and Joram Lindenstrauss. 1984. Extensions of Lipschitz mappings into a Hilbert space. In *Conference in modern analysis and probability, 1982)*. Contemp. Math., Vol. 26. Amer. Math. Soc., 189–206.

[26] Stefan Kratsch and Magnus Wahlström. 2012. Compression via matroids: a randomized polynomial kernel for odd cycle transversal. In *SODA*. SIAM, 94–103.

[27] Stefan Kratsch and Magnus Wahlström. 2012. Representative Sets and Irrelevant Vertices: New Tools for Kernelization. In *FOCS*. IEEE, 450–459.

[28] Daniel Lokshtanov, Pranabendu Misra, Fahad Panolan, and Saket Saurabh. 2014. Deterministic Truncation of Linear Matroids. *CoRR* abs/1404.4506 (2014).

[29] Daniel Lokshtanov, Pranabendu Misra, Fahad Panolan, and Saket Saurabh. 2015. Deterministic Truncation of Linear Matroids. In *ICALP*. 922–934.

[30] L. Lovász. 1977. Flats in matroids and geometric graphs.. In *In Combinatorial surveys (Proc. Sixth British Combinatorial Conf., Royal Holloway Coll., Egham)*. Academic Press, London, 45–86.

[31] Dániel Marx. 2009. A parameterized view on matroid optimization problems. *Theor. Comput. Sci.* 410, 44 (2009), 4471–4479.

[32] Thomas Muir. 1882. *A Treatise on the Theory of Determinants*. Dover Publications.

[33] Thom Mulders and Arne Storjohann. 2003. On lattice reduction for polynomial matrices. *J. Symb. Comput.* 35, 4 (2003), 377–401.

[34] Kazuo Murota. 2000. *Matrices and matroids for systems analysis*. Vol. 20. Springer.

[35] James G Oxley. 2006. *Matroid theory*. Vol. 3. Oxford University Press.

[36] Hadas Shachnai and Meirav Zehavi. 2014. Representative Families: A Unified Tradeoff-Based Approach. In *ESA*. 786–797.

[37] Victor Shoup. 1988. New Algorithms for Finding Irreducible Polynomials over Finite Fields. In *FOCS*. 283–290.

[38] Victor Shoup. 1990. Searching for Primitive Roots in Finite Fields. In *STOC*. 546–554.

[39] Igor Evgen'evich Shparlinski. 1990. On primitive elements in finite fields and on elliptic curves. *Matematicheskii Sbornik* 181, 9 (1990), 1196–1206.

[40] Virginia Vassilevska Williams. 2012. Multiplying matrices faster than Coppersmith-Winograd. In *STOC*. 887–898.