Lattice Compression of Polynomial Matrices

by

Chao Li

A thesis
presented to the University of Waterloo
in fulfilment of the
thesis requirement for the degree of
Master of Mathematics
in
Computer Science

Waterloo, Ontario, Canada, 2007

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

Chao Li

I understand that my thesis may be made electronically available to the public.

Chao Li

Abstract

This thesis investigates lattice compression of polynomial matrices over finite fields. For an $m \times n$ matrix, the goal of lattice compression is to find an $m \times (m+k)$ matrix, for some relatively small k, such that the lattice span of two matrices are equivalent. For any $m \times n$ polynomial matrix with degree bound d, it can be compressed by multiplying by a random $n \times (m+k)$ matrix B with degree bound s. In this thesis, we prove that there is a positive probability that $\mathcal{L}(A) = \mathcal{L}(AB)$ with $k(s+1) = \Theta(\log md)$. This is shown to hold even when $s = 0$ (i.e., where B is a matrix of constants). We also design a competitive probabilistic lattice compression algorithm of the Las Vegas type that has a positive probability of success on any input and requires $O\tilde{}(nm^{\theta-1}\mathsf{B}(d))$ field operations.

Acknowledgments

I gratefully appreciate my supervisors Prof. Arne Storjohann and Prof. Mark Giesbercht who helped me and guide me in both academic and daily life during my two years' life in Waterloo. I would like to greatly acknowledge Prof. George Labahn and Prof. Kevin Hare for reading this thesis. Thanks Mr. Reinhold Burger, Mr. Wei Zhou and all other group members in symbolic computation group. I appreciate all my friends in Waterloo.

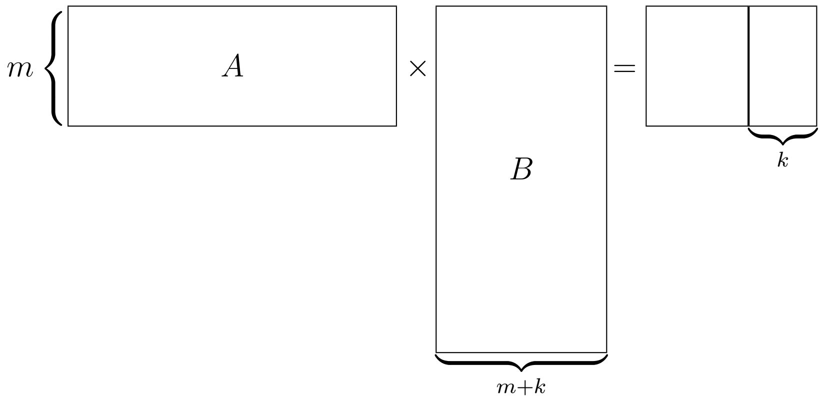
I especially thanks my parents for their cares and support and thanks to Shizhe with her love, which greatly encouraged me in those years.

Contents

Chapter 1

Introduction

Let K be a finite field and A be an $m \times n$ matrix with rank m over the univariate polynomial ring $\mathsf{K}[x]$. The m-dimensional lattice $\mathcal{L}(A)$ is defined to be the set of all $\mathsf{K}[x]$-linear combination of the columns of A. *Lattice Compression* is a way to construct a new generating set for $\mathcal{L}(A)$ with fewer columns; we randomly choose a matrix $B \in \mathsf{K}[x]^{n \times (m+k)}$ for a some integer k and then compute AB. If B is well-chosen, we could have $\mathcal{L}(A) = \mathcal{L}(AB)$ and $m + k < n$. In this case, we say that the compression is successful.



For example, when $m = 1$ the matrix A is a row vector and the lattice compression is equivalent to finding $k + 1$ random linear combinations of the entries of A whose greatest common divisor is equal to the gcd of all n entries of A. For example

$$[x^2+2x+3, x, x-3, 3x^2-1]\begin{bmatrix} 1 & 2 \\ 2 & -3 \\ x-1 & 2x-3 \\ 3 & 3x+2 \end{bmatrix} = [-2x^2-2x+2, -3x^3+2x^2-2],$$

is a successful compression on $\mathbb{Z}_7[x]$. For $m > 1$, an example input matrix over $\mathbb{Z}_7[x]$ is

$$A = \begin{bmatrix} 2-x & -2-x & -3-x & -2-x & 3-x & -2-x & -2+2x & 1 \\ -x & x & -2+2x & -1+3x & 1-2x & -1+x & 3+3x & 3 \\ 1+2x & -3+x & 1-2x & -3+3x & 2-x & -1+3x & -2+2x & 3 \\ 2-2x & 2-2x & 3x & -3-2x & 2+x & 2-3x & -2-x & -2x \end{bmatrix} \in \mathsf{K}[x]^{4\times 8}.$$

Consider the compression matrix

$$B = \begin{bmatrix} 0 & 2 & 1 & -1 & 2 \\ -3 & 2 & 1 & -1 & -1 \\ 0 & -1 & 1 & 3 & -2 \\ 0 & 0 & 3 & -2 & 0 \\ -1 & -3 & 1 & 0 & 1 \\ 2 & 0 & 2 & 3 & 1 \\ -1 & -3 & -2 & -1 & -3 \\ 3 & -2 & 3 & 1 & 3 \end{bmatrix} \in \mathsf{K}^{8\times 5}.$$

In this case the lattice compression is again successful. The compressed matrix

$$AB = \begin{bmatrix} -3 & -2+x & -3+x & -1+3x & 1 \\ 3-2x & -2+2x & -3-2x & 0 & -3-3x \\ 2+2x & 3-2x & 3-3x & -1-x & -2+3x \\ -2+x & 1 & -2-2x & 3 & -2+x \end{bmatrix} \in \mathsf{K}[x]^{4\times 5}$$

satisfies $\mathcal{L}(AB) = \mathcal{L}(A)$. In the example above, we chose B directly from K and the number of extra columns k to be exactly one. This suggests a series of questions: can we find a matrix B over K and with only one extra column under any circumstance, with a positive probability of success? If not, can we always keep a small k or even $k = 1$ with B generated from low degree polynomials over $\mathsf{K}[x]$? Or, how large will k need to be if we insist on choosing the entries of B randomly from K? Moreover, we are also interested in the relationship between the size of the field K and the probability of making a successful compression.

Lattice Compression is particularly useful in reducing the size of input matrices when an algorithm concerns properties of matrices that are invariant under unimodular column transformations. Thus it can be applied in linear system solving and computation of column standard forms, such as Hermite form, Smith form and column reduced form. We will show its detailed applications later in this chapter.

1.1 Main results

In this thesis we present a thorough discussion of lattice compression when A is over $\mathsf{K}[x]$, and the entries of B are chosen uniformly and randomly from K or polynomials in $\mathsf{K}[x]$ with a degree bound s. Let d denote the degree bound of the entries in A, and recall that k is the number of extra columns in the compressed matrix. Our approach shows that we can always get a positive probability of successful lattice compression as long as $k(s + 1) \in \Omega(\log md)$, where $\Omega(f)$ means asymptotic lower bounded by f [see Knuth, 1997, pp. 111]. More precisely, let $q = \#\mathsf{K}$ be the size of the finite field. Our study gives a lower bound on the probability of successful compression in different cases with respect to q, m, k, d and s:

- For a finite field K with size $q = \#\mathsf{K} > 2(md+5)$, we can choose the entries of B randomly and uniformly from K (that is, $s = 0$) and keep $k = 1$, exactly as we have shown in the example above, and still have a positive probability of successful lattice compression larger than 1/2. More precisely, the probability of success is larger than $1 - (md + 5)/q$.
- In order to draw the entries of B directly from K, which means $s = 0$, we show that is sufficient to have $k \in \Omega(\log md)$. More precisely we show that $k \geq 2\lceil \log_q md \rceil + 9$ is sufficient to get a positive probability of successful lattice compression. The probability of failure decreases exponentially with increasing of k. When $t = 2\lceil \log_q md \rceil + 6$, the probability of failure will be less than $(1/q)^{\lfloor (k-t)/3 \rfloor}$.

- In general, to get a positive probability of success, q, m, k, d and s should satisfy the following inequality:

$$k(s+1) \geq \left(2\log_q md + 3\left(1+\log_q 300\right)\right).$$

The probability of failure can be bounded in terms of k: it is less than $(1/q)^k + 2(1/q)^{k+1} + (1/q)^{2k} + 0.01$, for $q > 2$ or $k > 2$.

- Notice the probability mentioned above in the general case will larger than 1 for $q = 2$ and $k = 1$. We analyze the probability in the special case that $q = 2 \wedge k \leq 2$, and prove the probability of failure is less than $2(\frac{1}{2})^k - \frac{3}{4}(\frac{1}{4})^k + 0.01$.

1.2 Comparison with previous work

Storjohann and Labahn [1995] analyzed the $k = 1$ case of lattice compression. Based on an idea of Kaltofen et al. [1990], they choose the entries of a random matrix B from a subset of a finite field K. Storjohann and Labahn [1995] prove that the compression is successful if the entries in the random matrix B are not roots of a multivariate polynomial with degree bounded by m^2d, where d is the degree bound of A. According to the Schwartz-Zippel lemma [Schwartz, 1980], to keep the probability of failure smaller than ϵ, the desired size of the sample set K should be greater than or equal to $2\lceil m^2d/\epsilon\rceil$. If the finite field isn't large enough, Storjohann and Labahn mentioned that we can work over an extension of K. In this thesis, our approach shows that if the size of finite field is larger than or equal to $\lceil(md+5)/\epsilon\rceil$, we can keep $k = 1$ and generate the entries of B randomly and uniformly from K to get a probability of failure smaller than ϵ. More generally, for finite fields with small size (e.g. $q = 2$), we can get a positive probability of success by generating a random matrix B over $\mathsf{K}[x]$ rather than some field extension of K. If we insist on choosing the entries of B directly from K, our approach shows we only need to increase k by a small (logarithmic) amount.

Another case, where $m = 1$ and $k = 1$, is that of finding GCDs of polynomials and is studied by Conflitti [2003]. Instead of relying on the Schwartz-Zippel lemma, he constructed B with random polynomials with degree $\Theta(\log d)$ and considered the number of irreducible polynomials over the finite field that can divide the two polynomials after compression. Here $\Theta(f)$ means asymptotically tight bounded by f [see Knuth, 1997, pp. 111]. Our result generalizes this into any k and m with the same order of required degree bound.

Lattice compression over other principal ideal domains has been studied as well. An analysis for the integer case when $k = 1$ and $m = 1$ case is given by Cooperman et al. [1999] and von zur Gathen and Shparlinski [2004]. The detailed study for arbitrary k and m over the integer domain is given by Chen and Storjohann [2005].

1.3 Applications

An important application of this work is to under-determined linear system solving. Given a rectangular matrix A with more columns than rows over $\mathsf{K}[x]$, we wish to compute a solution u in $\mathsf{K}[x]$ to the linear system $Au = b$ or determine that no such u exists. Using lattice compression we can reduce this problem to solving an almost square system. If $\mathcal{L}(AB) = \mathcal{L}(A)$, the compressed system $(AB)v = b$ will have a solution over $\mathsf{K}[x]$ if and only if $Au = b$ has a solution. If v is a solution to the compressed system, then $u = Bv$ will be a solution to the original system.

Lattice compression can also be used with the algorithms which compute invariants of $\mathcal{L}(A)$, such as the Hermite form, the Smith form and a column reduced form. Since the best known algorithms for these normal forms require a square or almost square input matrix, we can use AB instead of A, so that the input matrix is almost square with only k extra columns. For this application it is desirable to have a compression with k as small as possible.

In particular, many algorithms for computing canonical forms require the input matrix to be non-singular, such as the Smith form algorithm in Storjohann [2002] and the column reduced form algorithm in Giorgi et al. [2003]. We present an algorithm in Chapter 7, based on the determinant reduction algorithm in Storjohann [2002] to transform AB, which has a dimension $m \times (m + k)$, to a non-singular matrix $\tilde{A}$ such that

$$\tilde{A} = \begin{bmatrix} AB \\ * \end{bmatrix} \in \mathsf{K}[x]^{(m+k)\times(m+k)},$$

with $\deg \tilde{A} \leq \deg AB$. Moreover, the Hermite column basis of $\tilde{A}$ is

$$\begin{bmatrix} H_{AB} & 0 \\ 0 & I_k \end{bmatrix} \in \mathsf{K}[x]^{(m+k)\times(m+k)},$$

where $H_{AB} \in \mathsf{K}[x]^{m\times m}$ is exactly the Hermite column basis of AB. Then we can compute the Smith form, Hermite form or column reduced form of the original matrix A from the square non-singular matrix $\tilde{A}$.

1.4 Outline

In Chapter 2 we present some mathematical foundations and characterize a successful lattice compression. In Chapter 3 we recall some probability bounds that a partially randomized matrix will have full row rank. Chapter 4 separates the problem into several parts and bounds the probability of failure for each part. Then Chapter 5 gives a detailed discussion in different cases and bounds the probability that $\mathcal{L}(A) \neq \mathcal{L}(AB)$. We prove some supplementary theorems in Chapter 6. Finally, in Chapter 7, we show how to verify the correctness of a compression and present a Las Vegas compression algorithm.

Chapter 2

Mathematical foundations

In this chapter we will recall some mathematical properties of matrices over fields. We follow the discussion from Mulders and Storjohann [2004] and Chen and Storjohann [2005]. Consider the situation when A is an $m \times n$ matrix over a field F with rank m. Since F is a field and A has full row rank, the lattice $\mathcal{L}(A)$ is the entire m-dimensional vector space over F^m, and for any $n \times (m+k)$ matrix B over F, $\mathcal{L}(A) = \mathcal{L}(AB)$ if and only if AB has full rank m over F. Instead of checking the rank of AB directly, we rely on the following lemma:

Lemma 2.1 (Mulders and Storjohann, 2004, Lemma 15)**.** *Let $A \in \mathsf{F}^{m\times n}$ have rank m and $N \in \mathsf{F}^{n\times(n-m)}$ be a right nullspace basis of A. For any matrix $B \in \mathsf{F}^{n\times(m+k)}$, $rank(AB) = rank([N|B]) - (n-m)$.*

Now consider extending Lemma 2.1 to the univariate polynomial ring $\mathsf{K}[x]$ over a finite field K. Use $\mathsf{K}(x)$ to denote the field of fractions of $\mathsf{K}[x]$ and for any irreducible polynomial $p \in \mathsf{K}[x]$, let $\mathsf{K}[x]/(p)$ be the residue class ring modulo p. From the definition of a lattice, we know for two matrices X and Y over $\mathsf{K}(x)$, that $\mathcal{L}(X) = \mathcal{L}(Y)$ over $\mathsf{K}(x)$ if and only if $X = YU$ for some invertible matrix U over $\mathsf{K}(x)$. Similarly, if X and Y are over $\mathsf{K}[x]$, $\mathcal{L}(X) = \mathcal{L}(Y)$ over $\mathsf{K}[x]$ if and only if $X = YU$ for some unimodular matrix U over $\mathsf{K}[x]$. Recall that a unimodular matrix over $\mathsf{K}[x]$ is one whose determinant is a non-zero element of K. Such matrices are exactly those which are invertible over $\mathsf{K}[x]$. When $X = YU$ for unimodular U, we say X and Y are *right equivalent* and denote this by $X \equiv_R Y$. Similarly, we say X and Y are *left equivalent* if $X = UY$ for a unimodular U or equivalently X^T and Y^T are right equivalent. We denote left equivalence by $X \equiv_L Y$. Here we show an example in which $A \equiv_R AB_1$ over $\mathbb{Z}_{11}[x]$ and $A \equiv_R AB_2$ over $\mathbb{Z}_{11}(x)$ only:

$$A = \begin{bmatrix} -5-5\,x & -3-3\,x & 3+3\,x \\ -4+x & 4+5\,x & -1-5\,x \\ 2\,x & -3-5\,x & 3+5\,x \end{bmatrix},$$

$$B_1 = \begin{bmatrix} 5 & 0 & -1 \\ 3-4\,x & 4 & 2+3\,x \\ 5\,x-1 & -2\,x & -5+x \end{bmatrix}, \quad \det(B_1) = -5,$$

$$AB_1 \cdot \begin{bmatrix} 5\,x+4+x^2 & 4\,x & -3 \\ 4+x+5\,x^2 & 3-2\,x & -4 \\ 3\,x-3+5\,x^2 & -2\,x & -4 \end{bmatrix} = A;$$

$$B_2 = \begin{bmatrix} 1+5\,x & -2\,x+1 & -3-3\,x \\ 4+5\,x & 5-2\,x & 4-3\,x \\ 1-x & 5-4\,x & 4+5\,x \end{bmatrix}, \quad \det(B_2) = -2x-2,$$

$$AB_2 \cdot \begin{bmatrix} -\frac{2x}{x+1} & \frac{4}{x+1} & \frac{-4+x}{x+1} \\ \frac{-5-4\,x}{x+1} & \frac{2+4\,x}{x+1} & \frac{-3}{x+1} \\ \frac{-2+3\,x}{x+1} & \frac{2+x}{x+1} & \frac{5-2\,x}{x+1} \end{bmatrix} = A.$$

Noticing that B_1 is unimodular over $\mathbb{Z}_{11}[x]$ and B_2 isn't, we know $AB_1 \equiv_R A$ and $AB_2 \not\equiv_R A$ over $\mathbb{Z}_{11}[x]$.

Definition 2.2 (Chen and Storjohann, 2005, Definition 2)**.** *Let $A \in \mathsf{K}[x]^{m\times n}$ have full row rank m. A matrix $N \in \mathsf{K}[x]^{n\times(n-m)}$ such that $\mathcal{L}(N) = \{x \in \mathsf{K}[x]^n \mid Ax = 0\}$ is called a right kernel of A.*

For any matrix $A \in \mathsf{K}[x]^{m\times n}$ consider a lower triangular matrix H over $\mathsf{K}[x]$ such that $A \equiv_R H$. One such such choice for H is the Hermite normal form of A.

Definition 2.3. *A matrix $H \in \mathsf{K}[x]^{m\times n}$ $(m < n)$ of full rank is said be in Hermite normal form if it has the form $[\tilde{H}\ 0]$, where $\tilde{H} \in \mathsf{K}[x]^{m\times m}$ is a nonsingular, lower triangular matrix in which each row has a unique monic entry with highest degree* *located on the main diagonal of $\tilde{H}$. If $A \equiv_R \tilde{H}$ then $\tilde{H}$ is the unique* Hermite *Column basis of A.*

We will use H_A to denote the Hermite column basis of A. Then the matrix $\bar{A} = H_A^{-1}A$ has entries from $\mathsf{K}[x]$ and $\bar{A} \equiv_R I_m$. Here is an example over $\mathbb{Z}_7[x]$:

$$A = \begin{bmatrix} 3+3\,x & 3+2\,x & -3\,x \\ 2+2\,x & 2-x^2 & 3-x-x^2 \\ -2+3\,x & 2-3\,x+3\,x^2 & 3\,x+3\,x^2 \end{bmatrix},$$

$$H_A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1+x & 0 \\ 2+2\,x & 1+2\,x-x^2 & x^3+3\,x+3 \end{bmatrix},$$

$$\bar{A} = H_A^{-1}A = \begin{bmatrix} 3+3\,x & 3+2\,x & -3\,x \\ -1 & -1-x & 3-x \\ 0 & -1 & -1 \end{bmatrix},$$

$$\bar{A} \cdot \begin{bmatrix} 2 & -2-x & 1+x^2 \\ 3 & 2+2\,x & -1+2\,x-2\,x^2 \\ -3 & -2-2\,x & 2\,x^2-2\,x \end{bmatrix} = I.$$

Lemma 2.4. *Let $X \in \mathsf{K}[x]^{m\times n}$ with $m \le n$. Then $X \equiv_R I_m$ if and only if X* mod *$p \in (\mathsf{K}[x]/(p))^{m\times n}$ has full row rank over $\mathsf{K}[x]/(p)$ for all irreducible polynomials $p \in \mathsf{K}[x]$.*

Proof. If $X \equiv_R I_m$ over $\mathsf{K}[x]$, then $X \equiv_R I_m$ over $\mathsf{K}[x]/(p)$ for all irreducible polynomials $p \in \mathsf{K}[x]$. Thus $X \bmod p$ has full rank over $\mathsf{K}[x]/(p)$ for all irreducible polynomials $p \in \mathsf{K}[x]$.

Now let's consider the other direction. Let U be a unimodular matrix over $\mathsf{K}[x]$ such that $XU = [H|0]$ where $H \in \mathsf{K}[x]^{m\times m}$ is the Hermite column basis of X.

Since U is nonsingular, $\text{rank}(X) = \text{rank}([H|0]) = \text{rank}(H)$ over $\mathsf{K}[x]$. Moveover, since U is unimodular, $U \bmod p$ is nonsingular over $\mathsf{K}[x]/(p)$ for any prime $p \in \mathsf{K}[x]$ and $\text{rank}(X \bmod p) = \text{rank}(H \bmod p)$ over $\mathsf{K}[x]/(p)$ for an irreducible $p \in \mathsf{K}[x]$.

Therefore, if $X \not\equiv_R I_m$, and we have $H \neq I_m$, which means $\deg(\det(H)) > 1$. Thus, there exists a prime $p \in \mathsf{K}[x]$ such that p divides $\det(H)$, which means $H \bmod p$ doesn't have full rank over $\mathsf{K}[x]/(p)$, a contradiction. $\square$

Using Lemma 2.4, Chen and Storjohann [2005] proved a theorem that shows when $AB \equiv_R A$ when they are over a principal ideal domain.

Theorem 2.5 (Chen and Storjohann, 2005, Theorem 4)**.** *Let $A \in \mathsf{K}[x]^{m\times n}$ with rank m. Let $N \in \mathsf{K}[x]^{n\times(n-m)}$ be a right kernel for A. For any matrix $B \in \mathsf{K}[x]^{n\times(m+k)}$, $AB \equiv_R A$ if and only if $[N|B] \equiv_R I_n$.*

Corollary 2.6 (Chen and Storjohann, 2005, Corollary 5)**.** *There exist a nonzero minor M of AB with the property that for all primes $p \in \mathsf{K}[x]$ not dividing M, the rank of $[N|B] \bmod p$ over $\mathsf{K}[x]/(p)$ does not decrease compared to the rank of $[N|B]$ over $\mathsf{K}[x]$.*

Chapter 3

The rank of a random matrix

Theorem 2.5 shows that $AB \equiv_R A$ if and only if $[N|B] \equiv_R I_n$, where $N \in \mathsf{K}[x]^{n\times(n-m)}$ is the right kernel of $A \in \mathsf{K}[x]^{m\times n}$. This means that to check whether the compression is successful, we can consider the rank of the partially random matrix $[N|B]$. For the fully random matrix, there's a well known result: let F be a field, and let $D \in \mathsf{F}^{n\times(n+k)}$ be a random matrix whose entries are chosen randomly and uniformly from F. The probability P such that the matrix D has full row rank is

$$P = \prod_{i=k+1}^{n+k} \left(1 - \left(\frac{1}{\#\mathsf{F}}\right)^i\right).$$

In general, if the matrix is a partially random matrix with the form $[C|D]$ where the entries of D are chosen randomly and uniformly from a finite subset U of F, Mulders and Storjohann [2004] gives a similar lower bound of the probability P such that matrix $[C|D]$ has full row rank.

Lemma 3.1 (Mulders and Storjohann, 2004, Lemma 13)**.** *Let $C \in \mathsf{F}^{n\times m_1}$ and rank$(C) = n - r$. Let $D \in \mathsf{F}^{n\times(r+k)}$ be a random matrix whose entries are chosen randomly and uniformly from a finite set $U \subseteq \mathsf{F}$. The probability P that the matrix $[C|D]$ has full row rank satisfies*

$$P \geq \prod_{i=k+1}^{r+k} \left(1 - \left(\frac{1}{\#U}\right)^i\right).$$

Notice that in Lemma 3.1, r denotes the minimum number of columns that D should have required to make the matrix $[C|D]$ full row rank. Since $D \in F^{n\times(r+k)}$, we say that the partially random matrix $[C|D]$ is k *extra columns*. In this thesis, we need a lower bound on P that is independent of r. We can raise the upper bound of the product in Lemma 3.1 up to ∞. Then we have a general lower bound

$$P > \prod_{i=k+1}^{\infty} \left(1 - \left(\frac{1}{\#U}\right)^i\right), \tag{3.1}$$

valid for all r. This gives the following theorem.

Theorem 3.2. *Let $C \in \mathsf{F}^{n\times m_1}$ with rank$(C) = n-r$. Let $D \in \mathsf{F}^{n\times(r+k)}$ be a random matrix whose entries are chosen randomly and uniformly from a finite set $U \subseteq \mathsf{F}$. The probability P that the matrix $[C|D]$ has full row rank satisfies*

$$P > \prod_{i=k+1}^{\infty} \left(1 - \left(\frac{1}{\#U}\right)^i\right). \tag{3.2}$$

For $s \geq 0$, we denote by $\mathsf{K}_s[x]$ the subset of $\mathsf{K}[x]$ consisting of all the polynomials in $\mathsf{K}[x]$ with the degree less than or equal to s. Applying Theorem 3.2 to the fraction field $\mathsf{K}(x)$ and letting $U = \mathsf{K}_s[x] \subset \mathsf{K}(x)$, we get the following theorem immediately from Theorem 3.2.

Theorem 3.3. *Let $C \in \mathsf{K}[x]^{n\times m_1}$ with rank$(C) = n-r$. Let $D \in \mathsf{K}[x]^{n\times(r+k)}$ have entries chosen randomly and uniformly from $\mathsf{K}_s[x]$. Then the probability P that $[C|D]$ will have a full row rank over $\mathsf{K}(x)$ satisfies*

$$P > \prod_{i=k+1}^{\infty} \left(1 - \left(\frac{1}{q^{s+1}}\right)^i\right). \tag{3.3}$$

For any irreducible polynomial $p \in \mathsf{K}[x]$, we can apply Theorem 3.2 on the residue field $\mathsf{K}[x]/(p)$. When the degree of p is at least $s+1$, we can still let $U = \mathsf{K}_s[x] \subseteq \mathsf{K}[x]/(p)$ as in Theorem 3.3. If the degree of p is less than or equal to s, consider the modular mapping ϕ from $\mathsf{K}_s[x]$ to $\mathsf{K}[x]/(p)$. For each polynomial f in $\mathsf{K}[x]/(p)$, its set of preimages in $\mathsf{K}_s[x]$ is

$$\phi^{-1}(f) = \{g \cdot p + f \,|\, \deg(g) + \deg(p) \leq s\}, \tag{3.4}$$

so that each polynomial in $\mathsf{K}[x]/(p)$ has $q^{s-\deg(p)+1}$ preimages in $\mathsf{K}_s[x]$. Therefore, if entries of matrix D are chosen randomly and uniformly from $\mathsf{K}_s[x]$, entries of $D \bmod p$ are randomly and uniformly chosen from $\mathsf{K}[x]/(p)$. This gives the following theorem.

Theorem 3.4. *Let $C \in \mathsf{K}[x]^{n\times m_1}$ with rank($C \bmod p$) $= n - r$ over $\mathsf{K}[x]/(p)$. Let $D \in \mathsf{K}_s[x]^{n\times(r+k)}$ have entries chosen uniformly from polynomials in $\mathsf{K}_s[x]$. Then the probability P that $[C|D] \bmod p$ will have a full row rank over $\mathsf{K}[x]/(p)$ satisfies*

$$P \geq \prod_{i=k+1}^{\infty}\left(1-\left(\frac{1}{q^{\delta}}\right)^{i}\right), \tag{3.5}$$

where $\delta = \min\{\deg(p), s+1\}$.

To approximate the probabilities, for $0 < x \leq 1/2$, $s, t > 0$, $u \geq 0$, we have

$$\begin{aligned}\prod_{i=s}^{\infty}(1-x^i) &= (1-x^s)\prod_{i=s+1}^{\infty}(1-x^i)\\ &\leq (1-x^s)\left(1-\sum_{i=s+1}^{\infty}x^i\right)\\ &= (1-x^s)\left(1-\frac{x^{s+1}}{1-x}\right)\\ &\leq (1-x^s)(1-2x^{s+1}).\end{aligned} \tag{3.6}$$

Lemma 3.5. *Let $0 < x \leq 1/2$, $s, t > 0$, and $u \geq 0$. Then*

$$\prod_{i=s}^{\infty}(1-x^i) \leq (1-x^s)(1-2x^{s+1}).$$

Since $q \geq 2$, then $0 < 1/q \leq 1/2$ always holds. Since we also need to bound from above the probability that $[C|D]$ doesn't have a full row rank, we can give a further approximation

$$1-(1-2x^{s+1})(1-x^s) = x^s + 2x^{s+1} - 2x^{2s+1} < (1+2x)x^s. \tag{3.7}$$

Applying (3.7), we derive the following corollary from Theorem 3.3 and 3.4.

Corollary 3.6. *Let $C \in \mathsf{K}[x]^{n\times m_1}$, rank($C$) $= n - r$. Let $D \in \mathsf{K}[x]^{n\times(r+k)}$ with the entries chosen uniformly from polynomials in $\mathsf{K}_s[x]$. Then the probability $\bar{P}$ that $[C|D]$ will not have a full row rank over $\mathsf{K}(x)$ satisfies*

$$\bar{P} < \left(1+\frac{2}{q^{s+1}}\right)\left(\frac{1}{q}\right)^{(s+1)(k+1)}. \tag{3.8}$$

Corollary 3.7. *Let $C \in \mathsf{K}[x]^{n \times m_1}$ with rank$(C \bmod p) = n - r$ over $\mathsf{K}[x]/(p)$. Let $D \in \mathsf{K}_s[x]^{n \times (r+k)}$ have entries chosen uniformly from polynomials in $\mathsf{K}_s[x]$. Then the probability $\bar{P}$ that $[C|D] \bmod p$ will not have full row rank over $\mathsf{K}[x]/(p)$ satisfies*

$$\bar{P} < \left(1 + \frac{2}{q^{\delta}}\right)\left(\frac{1}{q}\right)^{\delta(k+1)}, \tag{3.9}$$

where $\delta = \min\{\deg(p), s+1\}$.

Chapter 4

The probability that $AB \not\equiv_R A$

Recall that the Theorem 2.5 shows that $AB \in \mathsf{K}[x]^{m\times(m+k)}$ satisfies $AB \equiv_R A$ if and only if $[N|B] \in \mathsf{K}[x]^{n\times(n+k)}$ satisfies $[N|B] \equiv_R I_n$. Instead of considering the probability that $AB \not\equiv_R A$ we consider the probability that $[N|B] \not\equiv_R I$. Let **P** denote the event that $[N|B] \not\equiv_R I$, which means there exists at least one irreducible polynomial $p \in \mathsf{K}[x]$ such that $[N|B] \bmod p \in (\mathsf{K}[x]/(p))^{n\times(n+k)}$ has rank strictly less than n over $\mathsf{K}[x]/(p)$. Recall the entries of B are randomly and uniformly chosen from $\mathsf{K}_s[x]$. To bound the probability of event **P** we define the following events:

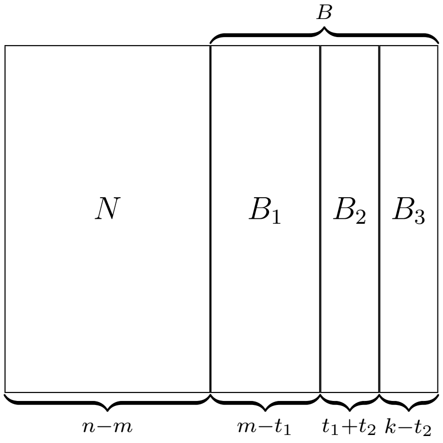
- Event **L**: there exist at least one irreducible polynomial p with degree larger than s such that $[N|B] \bmod p \in (\mathsf{K}[x]/(p))^{n\times(n+k)}$ has rank strictly less than n over $\mathsf{K}[x]/(p)$.
- Event **S**: there exist at least one irreducible polynomial p with degree less than or equal to s such that $[N|B] \bmod p \in (\mathsf{K}[x]/(p))^{n\times(n+k)}$ has rank strictly less than n over $\mathsf{K}[x]/(p)$.

Then the event **P** is equivalent to event $\mathbf{L} \vee \mathbf{S}$ (that is, L "or" S). Thus we know that

$$P(\mathbf{P}) = P(\mathbf{L} \vee \mathbf{S}) \leq P(\mathbf{L}) + P(\mathbf{S}).$$

Following the method in Chen and Storjohann [2005],we split the matrix B as $[B_1|B_2|B_3]$ with $m - t_1$, $t_1 + t_2$, $k - t_2$ columns, respectively. The parameters t_1, t_2 are non-negative integers with $t_1 + t_2 \leq k$. We will specify the values of t_1, t_2 later.

The split of B is shown as follows:



We define two other events:

- Event $\mathbf{L}_1$: there exist at least one irreducible polynomial p with degree strictly higher than s such that $[N|B_1] \bmod p \in (\mathsf{K}[x]/(p))^{n\times(n-t_1)}$ has rank at most $n-t_1-2$ over $\mathsf{K}[x]/(p)$.
- Event $\mathbf{L}_2$: The matrix $[N|B_1|B_2] \in \mathsf{K}[x]^{n\times(n+t_2)}$ doesn't have full row rank n over $\mathsf{K}(x)$.

According to the rules of probability, we have

$$\begin{aligned} P(\mathbf{P}) &\le P(\mathbf{L}) + P(\mathbf{S}) \\ &\le P(\mathbf{L}_1) + P(\mathbf{L}_2) + P[\mathbf{L}|\neg(\mathbf{L}_1 \vee \mathbf{L}_2)] + P(\mathbf{S}). \end{aligned}$$

In Section 4.1, 4.2, 4.3 and 4.4, we will use Corollary 3.6 and Corollary 3.7 to evaluate the probabilities of event $P(\mathbf{L}_2)$, $P[\mathbf{L}|\neg(\mathbf{L}_1 \vee \mathbf{L}_2)]$, $P(\mathbf{L}_1)$ and $P(\mathbf{S})$, respectively.

4.1 Upper bound for $P(\mathbf{L}_2)$

In this case $[B_1|B_2] \in \mathsf{K}[x]^{n\times(m+t_2)}$ is the random part of the partially random matrix $[N|B_1|B_2] \in \mathsf{K}[x]^{n\times(n+t_2)}$ with $\operatorname{rank}(N) = n-m$. Therefore the matrix $[N|B_1|B_2]$ has t_2 extra columns and Corollary 3.6 gives

$$P(\mathbf{L}_2) \;<\; \left(1+\frac{2}{q^{s+1}}\right)\left(\frac{1}{q}\right)^{(s+1)(t_2+1)}. \tag{4.1}$$

4.2 Upper bound for $P[\mathbf{L}|\neg(\mathbf{L}_1 \vee \mathbf{L}_2)]$

Since event $\mathbf{L}_1$ isn't satisfied, $[N|B_1] \in \mathsf{K}[x]^{n\times(n-t_1)}$ has rank at least $n - t_1 - 1$ over $\mathsf{K}[x]/(p)$ for all irreducible polynomials $p \in \mathsf{K}[x]$ with degree at least $s+1$. Let $\bar{P}_p$ be the probability that the partially random matrix $[N|B_1|B_3] \bmod p \in (\mathsf{K}[x]/(p))^{n\times(n+k-t_1-t_2)}$ does not have full row rank n over $\mathsf{K}[x]/(p)$, conditional on $\mathbf{L}_1$ not being satisfied. Taking $B_3 \in \mathsf{K}[x]^{n\times(k-t_2)}$ as the random part, Corollary 3.7 yields

$$\bar{P}_p \;<\; \left(1+\frac{2}{q^{s+1}}\right)\left(\frac{1}{q}\right)^{(s+1)(k-t_1-t_2)}. \tag{4.2}$$

According to the assumption that event $\mathbf{L}_2$ isn't satisfied, by Corollary 2.6 there exists a nonzero minor M of $A[B_1|B_2]$ such that for all irreducible polynomials p not dividing M, $A[B_1|B_2] \bmod p$ has full rank n. Let $\Gamma(D,s)$ denote the maximum number of distinct irreducible divisors with degree strictly larger than s of a polynomial in $\mathsf{K}_D[x]$. Since the degree of M is at most $m(d+s)$, considering (4.2) gives

$$\begin{aligned}
P[\mathbf{L}|\neg(\mathbf{L}_1 \vee \mathbf{L}_2)] \;&\leq\; \sum_{p|M,\,\deg(p)>s} P_p \\
&<\; \sum_{p|M,\deg(p)>s} \left(1+\frac{2}{q^{s+1}}\right)\left(\frac{1}{q}\right)^{(s+1)(k-t_1-t_2)} \\
&\leq\; \Gamma(m(d+s),s)\left(1+\frac{2}{q^{s+1}}\right)\left(\frac{1}{q}\right)^{(s+1)(k-t_1-t_2)}.
\end{aligned} \tag{4.3}$$

4.3 Upper bound for $P(\mathbf{L}_1)$

Following Eberly et al. [2000], we define events for $i = n-m, n-m+1, \ldots, n-1, n$. Let Dep_i denote the event that the first i columns of $[N|B_1]$ don't have full column rank. If Dep_{i-1} is not satisfied then there exist $i-1$ rows of $[N|B_1]$ such that the first $i-1$ columns of $[N|B_1]$ on those $i-1$ rows are a basis of $\mathsf{K}[x]^{i-1}$. Since any elementary column operation on the first $i-1$ columns of $[N|B_1]$ doesn't change the span of the first $i-1$ columns, we can assume the first $i-1$ columns of $[N|B_1]$

is in reduced column echelon form over $\mathsf{K}(x)$

$$[N|B_1] = \left[\begin{array}{c|c} \overbrace{\begin{matrix} 1 & 0 & 0 & 0 & \dots & 0 \\ * & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 & \dots & 0 \\ * & * & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ * & * & * & * & \dots & * \end{matrix}}^{i-1} & \begin{matrix} * & * & * \\ * & * & * \\ * & * & * \\ * & * & * \\ * & * & * \\ * & * & * \end{matrix} \end{array}\right].$$

Let $j_1, \dots, j_{i-1}$ be those rows whose i-th entry is 1 and all other entries are zero. When randomly generating the i-th column, first we pick the entries in the row $j_1 \dots, j_{i-1}$ of the i-th column, and then choose the rest of the entries on the i-th column uniformly and randomly from $\mathsf{K}_s[x]$. Considering the diagram above, we know once the entries in row $j_1 \dots, j_{i-1}$ are fixed of the i-th column, there's at most one choice for the other entries of the i-th column over $\mathsf{K}[x]$ such that those first i columns does not have a full column rank. So the probability that the first i columns do not have a full column rank is no more than $(1/q)^{(s+1)(n-i+1)}$. This gives

$$P[\mathrm{Dep}_i|\neg\mathrm{Dep}_{i-1}] \leq \left(\frac{1}{q}\right)^{(s+1)(n-i+1)}. \tag{4.4}$$

For an irreducible polynomial p with degree larger than s, let $\mathrm{MDep}_i^{(p)}$ denote the event that the first i columns of $[N|B_1] \bmod p \in (\mathsf{K}[x]/(p))^{n\times i}$ have a column rank at most $i-2$ over $\mathsf{K}[x]/(p)$. Let MDep_i denote the event that the first i columns of $[N|B_1] \bmod p$ have a column rank at most $i-2$ over $\mathsf{K}[x]/(p)$ for at least one irreducible polynomial p with degree larger than s. If MDep_{i-1} is not satisfied, it means the first $i-1$ columns of $[N|B_1] \bmod p$ has rank either $i-1$ or $i-2$ for any irreducible polynomial p with degree larger than s. If $[N|B_1] \bmod p$ has full column rank $i-1$ over $\mathsf{K}[x]/(p)$, then $\mathrm{MDep}_i^{(p)}$ can't be satisfied. Otherwise, if the first $i-1$ columns of $[N|B_1] \bmod p$ has rank $i-2$ over $\mathsf{K}[x]/(p)$, which means $\mathrm{MDep}_i^{(p)}$ is satisfied if and only if the i-th column of $[N|B_1] \bmod p$ is in the span of first $i-1$ columns of $[N|B_1] \bmod p$ over $\mathsf{K}[x]/(p)$. Thus we can use similar analysis with the event $\mathrm{Dep}_i|\neg\mathrm{Dep}_{i-1}$ on the field $\mathsf{K}(x)$, and the probability that the first i columns of $[N|B_1] \bmod p$ have rank $i-2$ over $\mathsf{K}[x]/(p)$ is less than or equal to

$(1/q)^{(s+1)(n-i+2)}$. In general, we have

$$P[\mathrm{MDep}_i^{(p)} | \neg \mathrm{MDep}_{i-1}] \le \left(\frac{1}{q}\right)^{(s+1)(n-i+2)}. \tag{4.5}$$

If Dep_{i-1} isn't satisfied, then according to Lemma 2.6, there exists a nonzero minor M_i of dimension $i-1$ of the first $i-1$ columns of AB_i such that for all irreducible polynomials p not dividing M_i, the first $i-1$ columns of $[N|B_1]$ have full column rank over $\mathsf{K}[x]/(p)$. Summing (4.5) over all the divisors of M_i with degree higher than s gives

$$\begin{aligned} P[\mathrm{MDep}_i | \neg(\mathrm{Dep}_{i-1} \vee \mathrm{MDep}_{i-1})] &\le \sum_{p|M_i, \deg p > s} P[\mathrm{MDep}_i^{(p)} | \neg(\mathrm{Dep}_{i-1} \vee \mathrm{MDep}_{i-1})] \\ &\le \sum_{p|M_i, \deg p > s} \left(\frac{1}{q}\right)^{(s+1)(n-i+2)} \\ &\le \Gamma(m(d+s), s) \left(\frac{1}{q}\right)^{(s+1)(n-i+2)}. \end{aligned} \tag{4.6}$$

From (4.4) and (4.6), we have

$$\begin{aligned} &P[\mathrm{Dep}_i \vee \mathrm{MDep}_i | \neg(\mathrm{Dep}_{i-1} \vee \mathrm{MDep}_{i-1})] \\ &\quad\le P[\mathrm{Dep}_i | \neg(\mathrm{Dep}_{i-1} \vee \mathrm{MDep}_{i-1})] + P[\mathrm{MDep}_i | \neg(\mathrm{Dep}_{i-1} \vee \mathrm{MDep}_{i-1})] \\ &\quad\le \left(1 + \Gamma(m(d+s), s) \left(\frac{1}{q}\right)^{s+1}\right) \left(\frac{1}{q}\right)^{(s+1)(n-i+1)}. \end{aligned} \tag{4.7}$$

Notice the event MDep_{n-t_1} is event $\mathbf{L}_1$. To estimate the $P(\mathbf{L}_1)$ we need the following lemma.

Lemma 4.1. *Let $E_0, E_1, \ldots, E_l$ be a series of events, such that $P(E_0) = 0$. Then:*

$$P(E_l) \le \sum_{i=1}^{l} P(E_i | E_{i-1}).$$

Proof. For any $1 \le i \le l$, we have

$$\begin{aligned} P(E_i) &= P((E_i \wedge E_{i-1}) \vee (E_i \wedge \neg E_{i-1})) \\ &\le P(E_i \wedge E_{i-1}) + P(E_i \wedge \neg E_{i-1}) \\ &\le P(E_{i-1}) + P(E_i | \neg E_{i-1}). \end{aligned}$$

Thus we know $P(E_i) - P(E_{i-1}) \leq P(E_i|\neg E_{i-1})$. Summing from $i = 1$ to l, we have

$$P(E_l) - P(E_0) = \sum_{i=1}^{l}(P(E_i) - P(E_{i-1})) \leq \sum_{i=1}^{l} P(E_i|E_{i-1}).$$

Notice that $P(E_0) = 0$ to finish the proof. □

Since $N \equiv_L I_{n-m}$, we know that $P[\text{Dep}_{n-m}] = P[\text{MDep}_{n-m}] = 0$. Therefore, according to Lemma 4.1 and (4.7), we can bound the probability of event $\mathbf{L}_1$ as follows.

$$\begin{aligned}
P(\mathbf{L}_1) &= P[\text{MDep}_{n-t_1}] \\
&\leq P[\text{Dep}_{n-t_1} \vee \text{MDep}_{n-t_1}] \\
&\leq \sum_{i=n-m+1}^{n-t_1} P[(\text{Dep}_i \vee \text{MDep}_i|\neg(\text{Dep}_{i-1} \vee \text{MDep}_{i-1}))] \\
&\leq \sum_{i=n-m+1}^{n-t_1} \left(1 + \Gamma(m(d+s), s)\left(\frac{1}{q}\right)^{s+1}\right)\left(\frac{1}{q}\right)^{(s+1)(n-i+1)} \\
&\leq \sum_{i=t_1+1}^{\infty} \left(1 + \Gamma(m(d+s), s)\left(\frac{1}{q}\right)^{s+1}\right)\left(\frac{1}{q}\right)^{(s+1)i} \\
&\leq \left(1 + \Gamma(m(d+s), s)\left(\frac{1}{q}\right)^{s+1}\right)\left(1 + \frac{2}{q^{s+1}}\right)\left(\frac{1}{q}\right)^{(s+1)(t_1+1)}. \qquad (4.8)
\end{aligned}$$

4.4 An upper bound for $P(\mathbf{S})$

According to Corollary 3.7, for an irreducible polynomial p with degree less than or equal to s, we know the probability P_p that $[N|B] \in (\mathsf{K}[x]/(p))^{n\times(n+k)}$ doesn't have a full row rank over $\mathsf{K}/(p)$ satisfies

$$P_p < \left(1 + \frac{2}{q^{\deg(p)}}\right)\left(\frac{1}{q}\right)^{\deg(p)(k+1)}. \qquad (4.9)$$

Use $N_q(n)$ to denote the number of irreducible polynomials with degree n in finite field $\mathbf{F}_q[x]$. Summing (4.9) over all irreducible polynomials with degree less than or equal to s gives

$$\begin{aligned} P(\mathbf{S}) &\leq \sum_{i=1}^{s} N_q(i) P_p \\ &\leq \sum_{i=1}^{s} N_q(i) \left(1 + \frac{2}{q^i}\right) \left(\frac{1}{q}\right)^{i(k+1)} \\ &\leq \sum_{i=1}^{\infty} N_q(i) \left(1 + \frac{2}{q^i}\right) \left(\frac{1}{q}\right)^{i(k+1)} . \end{aligned} \tag{4.10}$$

Chapter 5

The probability that $AB \not\equiv_R A$ in different cases

Now we present concrete upper bounds for the probability that $AB \not\equiv_R A$ in different cases. Recall that $\mathbf{P}$ denotes the event that $AB \not\equiv_R A$ and we separate event $\mathbf{P}$ into two events. $\mathbf{L}$ denotes the event that $AB \not\equiv_R A$ over $\mathsf{K}[x]/(p)$ for at least one irreducible polynomial p with $\deg P > s$. $\mathbf{S}$ denotes the event that $AB \not\equiv_R A$ over $\mathsf{K}[x]/(p)$ for at least one irreducible polynomial p with $\deg \mathbf{P} \leq s$. Therefore

$$P(\mathbf{P}) \leq P(\mathbf{L}) + P(\mathbf{S}).$$

In Section 5.1 we consider the special case $s = 0$, which means the entries of B are chosen randomly and uniformly from the finite field K. In this case $P(\mathbf{S}) = 0$ and it will suffice to bound $P(\mathbf{L})$. We present an upper bound of the minimum k required in this case to guarantee a positive probability that $AB \equiv_R A$.

We analyze the case $s > 0$ in Section 5.2, 5.3 and 5.4. The bound on the probability of event $\mathbf{S}$ is discussed in Section 5.2. Since this general bound on $P(\mathbf{S})$ doesn't work well when $q = 2 \wedge k \leq 2$, we further analyze this special case in Section 5.3. The relationship between $P(\mathbf{L})$, s and k are presented in Section 5.4.

We summarize all the probabilities for those different cases in Section 5.5.

5.1 Special case: $s = 0$

For $s = 0$ we know that $P(\mathbf{S}) = 0$. Equation (4.1), (4.3) and (4.8) with $s = 0$ become:

$$\begin{aligned} P(\mathbf{L}_1|s=0) &< \left(1+\frac{2}{q}\right)\left(1+\frac{\Gamma(md,0)}{q}\right)\left(\frac{1}{q}\right)^{t_1+1}, & (5.1)\\ P(\mathbf{L}_2|s=0) &< \left(1+\frac{2}{q}\right)\left(\frac{1}{q}\right)^{t_2+1}, & (5.2)\\ P[(\mathbf{L}|\neg(\mathbf{L}_1 \vee \mathbf{L}_2))|s=0] &< \Gamma(md,0)\left(1+\frac{2}{q}\right)\left(\frac{1}{q}\right)^{k-t_1-t_2}. & (5.3)\end{aligned}$$

To make $P(\mathbf{L}_1|s=0) + P(\mathbf{L}_2|s=0) + P[(\mathbf{L}|\neg(\mathbf{L}_1 \vee \mathbf{L}_2))|s=0] < 1$, we assign t_1, t_2, k as follows:

$$t_1 = \left\lceil \log_q \Gamma(md,0) \right\rceil + C_1, \quad t_2 = C_2, \quad k - t_1 - t_2 = \left\lceil \log_q \Gamma(md,0) \right\rceil + C_3.$$

Here, C_1, C_2 and C_3 depend on q:

q	2	3	4	≥ 5
C_1	2	1	0	0
C_2	1	0	0	0
C_3	3	2	2	1

(5.4)

Thus, since in this special case

$$P(\mathbf{P}|s=0) \leq P(\mathbf{L}_1|s=0) + P(\mathbf{L}_2|s=0) + P[(\mathbf{L}|\neg(\mathbf{L}_1 \vee \mathbf{L}_2))|s=0],$$

there exists a positive probability such that AB has full row rank when $k \geq t$, where

$$t = 2\left\lceil \log_q \Gamma(md,0) \right\rceil + 6.$$

Lemma 5.1. *$\Gamma(m(d+s),s) \leq md$.*

We will leave the proof of this Lemma to Chapter 6. From the lemma, we know that $\Gamma(md,0) \leq md$. Moreover, the analysis on the function Γ will imply that $\Gamma(md,0) \in \Omega(md/\log_q md)$. Since the term with order $O(\log\log md)$ doesn't improve the value of t much, we can use md instead of $\Gamma(md)$. Let

$$t_1 = \left\lceil \frac{k-t-1}{3} \right\rceil + \left\lceil \log_q md \right\rceil + 2,\ t_2 = \left\lceil \frac{k-t}{3} \right\rceil + 1, \text{ and } t = 2\left\lceil \log_q md \right\rceil + 6.$$

Then the probability of success is no less than $1 - (1/q)^{\lfloor (k-t)/3 \rfloor}$.

Moreover, if $q \geq md + 5$, let $t_1 = t_2 = 0$, $k = 1$ in (5.1), (5.2) and (5.3). Summing those equations give

$$\begin{aligned} P(\mathbf{P}|s=0) &\leq P(\mathbf{L}_1|s=0) + P(\mathbf{L}_2|s=0) + P[(\mathbf{L}|\neg(\mathbf{L}_1 \vee \mathbf{L}_2))|s=0] \\ &\leq \frac{(q+2)((md+2)q+md)}{q^3} \\ &< \frac{md+5}{q} - \frac{9}{q^2} < 1. \end{aligned}$$

Thus, if $q \geq md + 5$, we can keep $k = 1$ and obtain a positive probability that $AB \equiv_R A$.

5.2 Computation of $P(\mathrm{S})$ in the general case

It's well known that the number $N_q(n)$ of irreducible polynomials with degree n over finite field $\mathbf{F}_q$ satisfies the following theorem:

Lemma 5.2. *(Theorem 3.25 in Lidl and Niederreiter [1983]) The number $N_q(n)$ of monic irreducible polynomials in $\mathbf{F}_q[x]$ of degree n is given by*

$$N_q(n) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d = \frac{1}{n}\sum_{d|n} \mu(d) q^{\frac{n}{d}}, \tag{5.5}$$

where $\mu(n)$ is the Moebius function on $\mathbb{N}$ defined as

$$\mu(n) = \begin{cases} 1 & \textit{if } n = 1; \\ (-1)^k & \textit{if } n \textit{ is the product of } k \textit{ distinct primes;} \\ 0 & \textit{if } n \textit{ is divisible by the square of a prime.} \end{cases}$$

Lemma 5.3. *$N_q(n) \leq \frac{1}{n} q^n$.*

The proof of Lemma 5.3 is very easy and is deferred until Chapter 6. From

Lemma 5.2 and Lemma 5.3, we know

$$\begin{aligned}
\sum_{i=1}^{\infty} N_q(i)\left(\frac{1}{q}\right)^{i(k+1)} &= N_q(1)\left(\frac{1}{q}\right)^{(k+1)} + N_q(2)\left(\frac{1}{q}\right)^{2(k+1)} \\
&\quad + N_q(3)\left(\frac{1}{q}\right)^{3(k+1)} + \sum_{i=4}^{\infty} N_q(i)\left(\frac{1}{q}\right)^{i(k+1)} \\
&< \left(\frac{1}{q}\right)^{k} + \frac{1}{2}(q^2-q)\left(\frac{1}{q}\right)^{2(k+1)} \\
&\quad + \frac{1}{3}(q^3-q)\left(\frac{1}{q}\right)^{3(k+1)} + \sum_{i=4}^{\infty}\frac{1}{i}\left(\frac{1}{q}\right)^{ik} \\
&< \left(\frac{1}{q}\right)^{k} + \frac{1}{2}\left(\frac{1}{q}\right)^{2k} - \frac{1}{2}\left(\frac{1}{q}\right)^{3k} + \frac{1}{3}\left(\frac{1}{q}\right)^{3k} \\
&\quad - \frac{1}{3}\left(\frac{1}{q}\right)^{5k} + \frac{1}{4}\left(\frac{1}{q}\right)^{4k} + \frac{1}{5}\sum_{i=5}^{\infty}\left(\frac{1}{q}\right)^{ik} \\
&\leq \left(\frac{1}{q}\right)^{k} + \frac{1}{2}\left(\frac{1}{q}\right)^{2k} - \frac{1}{2}\left(\frac{1}{q}\right)^{3k} + \frac{1}{3}\left(\frac{1}{q}\right)^{3k} \\
&\quad - \frac{1}{3}\left(\frac{1}{q}\right)^{5k} + \frac{1}{4}\left(\frac{1}{q}\right)^{4k} + \frac{2}{5}\left(\frac{1}{q}\right)^{5k} \\
&< \left(\frac{1}{q}\right)^{k} + \frac{1}{2}\left(\frac{1}{q}\right)^{2k}. \qquad (5.6)
\end{aligned}$$

Substituting (5.6) into (4.10) we can give an upper bound on $P(\mathbf{S})$ directly.

$$\begin{aligned}
P(\mathbf{S}) &\leq \sum_{i=1}^{\infty} N_q(i)\left(1+\frac{2}{q^i}\right)\left(\frac{1}{q}\right)^{i(k+1)} \\
&< \left(\frac{1}{q}\right)^{k} + 2\left(\frac{1}{q}\right)^{k+1} + \frac{1}{2}\left(\frac{1}{q}\right)^{2k} + \left(\frac{1}{q}\right)^{2(k+1)} \\
&< \left(\frac{1}{q}\right)^{k} + 2\left(\frac{1}{q}\right)^{k+1} + \left(\frac{1}{q}\right)^{2k}. \qquad (5.7)
\end{aligned}$$

5.3 Special case: $P(\mathbf{S}|q = 2 \wedge k \leq 2)$

When $q = 2$, the bound on $P(\mathbf{S})$ given by (5.7) is too large, even larger than 1 for $k = 1$. Since the observation of (4.10) implies that the first terms of sum is fairly large for small q and k and they dominate the primary part of the sum, we apply some other techniques to compute those probabilities.

Based on Theorem 3.4 we consider the rank of $[C|D]$ over more than one residue field.

Theorem 5.4. *Let $p_1, \ldots, p_t$ be irreducible polynomials over $\mathsf{K}[x]$. Let $C \in \mathsf{K}[x]^{n\times(n-m)}$ with rank($C \bmod p_i) = n-m$ over $\mathsf{K}[x]/(p_i)$ for all $1 \le i \le t$. Let $D \in \mathsf{K}[x]^{n\times(m+k)}$ have entries chosen uniformly from polynomials in $\mathsf{K}[x]$ whose degrees are no more than s, where $s+1 \ge \sum_{i=1}^{t} \deg(p_i)$. Then the probability P that $[C|D] \bmod p_i$ will have a full rank over $\mathsf{K}[x]/(p_i)$ for all $1 \le i \le t$ is*

$$P > \prod_{i=1}^{t} \prod_{j=k+1}^{\infty} \left(1 - \left(\frac{1}{q^{\deg(p_i)}}\right)^{j}\right). \tag{5.8}$$

Proof. Let $p = \prod_{i=1}^{t} p_t$ and $d = \sum_{i=1}^{t} \deg(p_i) = \deg(p)$. Since $s+1 > d$, consider the mapping:

$$\begin{array}{rcl} \phi_p : \mathsf{K}_s[x] & \mapsto & \mathsf{K}_{d-1}[x], \\ f & \mapsto & f \bmod p. \end{array}$$

Since each image of this mapping have the same number of preimages and for any matrix $M \in \mathsf{K}_s[x]$, its rank over $\mathsf{K}[x]/(p_i)$ is exactly the same with the rank of $M \bmod p$ over the same residue field. Thus we can only consider the probability P in case that $s = p-1$.

Let ϕ_i be the modular mapping from $\mathsf{K}_{d-1}[x]$ to $\mathsf{K}[x]/(p_i)$. According to the Chinese Remainder Theorem, for a set of polynomials $f_1, f_2, \ldots, f_t$ such that $f_i \in \mathsf{K}[x]/(p_i)$, there exists an unique polynomial $f \in \mathsf{K}_{d-1}[x]$ such that $f \bmod p_i = f_i$, $i \le i \le t$. Use ψ to denote this reconstruction. Then ψ and $\phi_1 \times \phi_2 \times \ldots \times \phi_t$ present an isomorphic between $\mathsf{K}[x]/(p_1) \times \mathsf{K}[x]/(p_2) \times \ldots \times \mathsf{K}[x]/(p_t)$ and $\mathsf{K}_{d-1}[x]$. Since the rank of a matrix $M \in \mathsf{K}_{d-1}[x]$ over $\mathsf{K}/(p_i)$ is only related on its image under ϕ_i, we know the probability that M has full rank over $\mathsf{K}/(p_1), \mathsf{K}/(p_2), \ldots, \mathsf{K}/(p_t)$ are independent. Thus the probability P that $[C|D] \bmod p_i$ will have a full rank over $\mathsf{K}[x]/(p_i)$ for any $1 \le i \le t$ is the product of the probabilities that $[C|D] \bmod p_i$ will have a full rank over $\mathsf{K}[x]/(p_i)$ over each i. Then

$$P > \prod_{i=1}^{t} \prod_{j=k+1}^{\infty} \left(1 - \left(\frac{1}{q^{\deg(p_i)}}\right)^{j}\right).$$

□

According to Theorem 5.4 we can consider three irreducible polynomials with lowest degree together in this case. We know $N_2(1) = 2$, $N_2(2) = 1$. Then we should keep $s \geq 3$ for $q = 2$. Then we compute $P(\mathbf{S})$. When $q = 2$, using the approximation Lemma 3.5 and the upper bound for $N_2(i)$ in Lemma 5.3 gives

$$\begin{aligned}
P(\mathbf{S}|q = 2 \wedge k \leq 2) &\leq 1 - \prod_{i=k+1}^{\infty} \left(1 - \frac{1}{2^i}\right)^2 \left(1 - \frac{1}{4^i}\right) + \sum_{i=3}^{s} N_2(i) P_p \\
&\leq 1 - \prod_{i=k+1}^{\infty} \left(1 - \frac{1}{2^i}\right)^2 \left(1 - \frac{1}{4^i}\right) \\
&\quad + \sum_{i=3}^{\infty} N_2(i) \left(1 + \frac{1}{2^{i-1}}\right) \left(\frac{1}{2}\right)^{i(k+1)}. \qquad (5.9)
\end{aligned}$$

According to Lemmas 5.2 and 5.3, consider $k \geq 1$ and we have

$$\begin{aligned}
\sum_{i=3}^{\infty} N_2(i) \left(\frac{1}{2}\right)^{i(k+1)} &= N_2(3) \left(\frac{1}{2}\right)^{3(k+1)} + N_2(4) \left(\frac{1}{2}\right)^{4(k+1)} + \sum_{i=5}^{\infty} N_2(i) \left(\frac{1}{2}\right)^{i(k+1)} \\
&\leq \frac{1}{3}(2^3 - 2) \left(\frac{1}{2}\right)^{3(k+1)} + \frac{1}{4}(2^4 - 2) \left(\frac{1}{2}\right)^{4(k+1)} + \sum_{i=5}^{\infty} \frac{1}{i} \left(\frac{1}{2}\right)^{ik} \\
&< \frac{1}{3} \left(\frac{1}{2}\right)^{3k} - \frac{1}{3} \left(\frac{1}{2}\right)^{5k} + \frac{1}{4} \left(\frac{1}{2}\right)^{4k} \\
&\quad - \frac{1}{4} \left(\frac{1}{2}\right)^{6k} + \frac{1}{5} \left(\frac{1}{2}\right)^{5k} + \frac{1}{6} \sum_{i=6}^{\infty} \left(\frac{1}{2}\right)^{ik} \\
&\leq \frac{1}{3} \left(\frac{1}{2}\right)^{3k} - \frac{1}{3} \left(\frac{1}{2}\right)^{5k} + \frac{1}{4} \left(\frac{1}{2}\right)^{4k} \\
&\quad - \frac{1}{4} \left(\frac{1}{2}\right)^{6k} + \frac{1}{5} \left(\frac{1}{2}\right)^{5k} + \frac{1}{3} \left(\frac{1}{2}\right)^{6k} \\
&< \frac{1}{3} \left(\frac{1}{2}\right)^{3k} + \frac{1}{4} \left(\frac{1}{2}\right)^{4k}. \qquad (5.10)
\end{aligned}$$

Substituting (5.10) into (5.9) and recalling the approximation given by Lemma 3.5, we have

$$\begin{aligned}
P(\mathbf{S}|q=2\wedge k\leq 2) &\leq 1-\prod_{i=k+1}^{\infty}\left(1-\frac{1}{2^i}\right)^2\left(1-\frac{1}{4^i}\right)+\sum_{i=3}^{\infty}N_2(i)\left(1+\frac{1}{2^{i-1}}\right)\left(\frac{1}{2}\right)^{i(k+1)} \\
&< 1-\left(1-\left(\frac{1}{2}\right)^{k+1}\right)^4\left(1-\left(\frac{1}{4}\right)^{k+1}\right)\left(1-2\left(\frac{1}{4}\right)^{k+2}\right) \\
&\quad +\frac{1}{3}\left(\frac{1}{2}\right)^{3k}+\frac{1}{4}\left(\frac{1}{2}\right)^{4k}+\frac{2}{3}\left(\frac{1}{2}\right)^{3(k+1)}+\frac{1}{2}\left(\frac{1}{2}\right)^{4(k+1)} \\
&< 2\left(\frac{1}{2}\right)^k-\frac{3}{4}\left(\frac{1}{4}\right)^k. \qquad (5.11)
\end{aligned}$$

Substituting $k = 1, 2$ into (5.11) gives

k	1	2
$P(\mathbf{S}\|q=2\wedge k\leq 2)$	0.813	0.453

(5.12)

5.4 Computation of $P(\mathbf{L})$

According to (4.1), (4.3) and (4.8), we know $P(\mathbf{L})$ can be as small as possible with a large enough s. Let C be the desired upper bound on $P(\mathbf{L})$. Consider (4.1) (4.3) and (4.8):

$$\begin{aligned}
P(\mathbf{L}_1) &< \left(1+\frac{2}{q^{s+1}}\right)\left(1+\frac{\Gamma(m(d+s),s)}{q^{s+1}}\right)\left(\frac{1}{q}\right)^{(s+1)(t_1+1)}\leq\frac{C}{3}, \\
P(\mathbf{L}_2) &< \left(1+\frac{2}{q^{s+1}}\right)\left(\frac{1}{q}\right)^{(s+1)(t_2+1)}\leq\frac{C}{3}, \\
P[\mathbf{L}|\neg(\mathbf{L}_1\vee\mathbf{L}_2)] &< \Gamma(m(d+s),s)\left(1+\frac{2}{q^{s+1}}\right)\left(\frac{1}{q}\right)^{(s+1)(k-t_1-t_2)}\leq\frac{C}{3}.
\end{aligned}$$

Thus we can set s to satisfy the following inequalities:

$$\begin{aligned}
t_1 &\geq \left\lceil\frac{1}{s+1}\left(\log_q\left(1+\frac{2}{q^{s+1}}\right)+\log_q\left(1+\frac{\Gamma(m(d+s),s)}{q^{s+1}}\right)+\log_q\frac{3}{C}\right)\right\rceil-1, \\
t_2 &\geq \left\lceil\frac{1}{s+1}\left(\log_q\left(1+\frac{2}{q^{s+1}}\right)+\log_q\frac{3}{C}\right)\right\rceil-1, \\
k-t_1-t_2 &\geq \left\lceil\frac{1}{s+1}\left(\log_q\Gamma(m(d+s),s)+\log_q\left(1+\frac{2}{q^{s+1}}\right)+\log_q\frac{3}{C}\right)\right\rceil.
\end{aligned}$$

Summing the above equations gives

$$k(s+1) \geq 2\log_q \Gamma(m(d+s),s) + 3\left(1+\log_q \frac{3}{C}\right). \tag{5.13}$$

Using a similar analysis with the case $s=0$ we know that we can use md to take the place of $\Gamma(m(d+s),s)$. Then (5.13) becomes

$$k(s+1) \geq 2\log_q md + 3\left(1+\log_q \frac{3}{C}\right), \tag{5.14}$$

for any $0 < C \leq 1$. In particular, for $q=2$ and $k \leq 2$, (5.14) shows that s should be at least 3 in order to use the technique in Section 5.3 in this special case.

5.5 Results

According to the sections above, to simplify the inequality (5.14) and the expression of $P(\mathbf{L})$, let the constant $C = 0.01$. Recall that K is a finite field with $\#\mathsf{K} = q$, $A \in \mathsf{K}[x]^{m\times n}$ with degree bound d, and $B \in \mathsf{K}[x]^{n\times(m+k)}$ with degree bound s. $\mathbf{P}$ denotes the event that $AB \not\equiv_R A$. The relationship between the probability of the event $\mathbf{P}$ and the parameters m, d, q, k and s can be presented in the following theorem.

Theorem 5.5. *The probability of event* $\mathbf{P}$ *satisfies the following:*

1. *If the entries of* B *are chosen from* K *(that is,* $s=0$*), then*

$$P(\mathbf{P}|s=0) \leq \left(\frac{1}{q}\right)^{\left\lfloor \frac{k-t}{3}\right\rfloor}, \tag{5.15}$$

where $t = 2\lceil \log_q md\rceil + 6$.

2. *If* k *is fixed and the entries of* B *are chosen from* $\mathsf{K}_s[x]$ *with* $s \geq s_0$*, then*

$$P(\mathbf{P}|s\geq s_0) \leq \left(\frac{1}{q}\right)^{k} + 2\left(\frac{1}{q}\right)^{k+1} + \left(\frac{1}{q}\right)^{2k} + 0.01, \tag{5.16}$$

where $s_0 = \left\lfloor \frac{1}{k}\left(2\log_q md + 3\left(1+\log_q 300\right)\right)\right\rfloor$.

3. *In particular, as a special case of part 2, if $q = 2$, $k \leq 2$ and $s \geq s_0^*$, then*

$$P(\mathbf{P}|q = 2 \wedge k \leq 2 \wedge s \geq s_0^*) \leq 2\left(\frac{1}{2}\right)^k - \frac{3}{4}\left(\frac{1}{4}\right)^k + 0.01, \tag{5.17}$$

where $s_0^* = \left\lfloor \frac{1}{k}\left(2\log_2 md + 28\right)\right\rfloor$.

4. *if we keep only one extra column and draw entries of B from K (that is, $s = 0 \wedge k = 1$),*

$$P(\mathbf{P}|s = 0 \wedge k = 1) < \frac{md + 5}{q} - \frac{9}{q^2}. \tag{5.18}$$

Chapter 6

The bounds and approximations for $N_q(n)$ and $\Gamma(D, s)$

In this section we will discuss the properties of $N_q(n)$ and $\Gamma(D, s)$. In the process, we will also prove Lemmas 5.1 and 5.3.

Recall that $N_q(n)$ denotes the number of irreducible polynomials with degree n over finite field F_q and $\Gamma(D, s)$ denote the maximum number of distinct irreducible divisors with degree strictly larger than s of a polynomial with degree D. First we present an upper bound on $\Gamma(D, s)$. Consider the case that a polynomial with degree D gets maximum number of distinct divisors, in which this polynomial should be the multiple of all irreducible of polynomials with degree $s + 1$, $s + 2$, $\ldots$ until the degree of their product is larger than D. According to the definition of $\Gamma(D, s)$, the number of irreducible divisors of such polynomial is an upper bound on $\Gamma(D, s)$.

Definition 6.1. *For a non-negative integer D, let $\gamma(D, s)$ be an integer such that*

$$\sum_{i=s+1}^{\gamma(D,s)} iN_q(i) \leq D < \sum_{i=s+1}^{\gamma(D,s)+1} iN_q(i). \tag{6.1}$$

Theorem 6.2. *For a non-negative integer D, we have the following upper bound on $\Gamma(D, s)$:*

$$\Gamma(D, s) \leq \sum_{i=s+1}^{\gamma(D,s)} N_q(i) + \left\lfloor \frac{1}{\gamma(D, s) + 1} \left(D - \sum_{i=s+1}^{\gamma(D,s)} iN_q(i) \right) \right\rfloor .$$

According to the definition of $\gamma(D,s)$, and using n_0 to denote $\gamma(D,s)$, we have

$$\Gamma(D,s) \; < \; \sum_{i=s+1}^{n_0+1} N_q(i). \tag{6.2}$$

Suppose $n = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_t^{\alpha_t}$ is the complete factorization of integer n, and $q_1 < q_2 < \dots < q_t$ are primes. If $n = q_1^{\alpha_1}$ then

$$nN_q(n) = q^n - q^{\frac{n}{q_1}}. \tag{6.3}$$

Otherwise, since the value of Moebius function is in $\{-1, 0, 1\}$,

$$\begin{aligned} nN_q(n) &= \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d && (6.4)\\ &\le q^n - q^{\frac{n}{q_1}} - q^{\frac{n}{q_2}} + \sum_{i=1}^{\frac{n}{q_1 q_2}} q^i && (6.5)\\ &< q^n - q^{\frac{n}{q_1}} - q^{\frac{n}{q_2}} + q^{\frac{n}{q_1 q_2}+1} \\ &\le q^n - q^{\frac{n}{q_1}}, && (6.6) \end{aligned}$$

According to the definition of μ, the largest $d < n$ to make $\mu(n/d) = 1$ is $n/(q_1 q_2)$. Discarding all $d|n$, $d < n/q_2$ with $\mu(n/d) = -1$, and assuming that for all $d < n/(q_1 q_2)$, $\mu(n/d) = 1$ in (6.4), we maximize the sum and derive (6.5). Now observe

$$\begin{aligned} nN_q(n) &= \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d && (6.7)\\ &\ge q^n - q^{\frac{n}{q_1}} - \sum_{i=1}^{\frac{n}{q_2}} q^i && (6.8)\\ &> q^n - q^{\frac{n}{q_1}} - q^{\frac{n}{q_2}+1} \\ &\ge q^n - 2q^{\frac{n}{q_1}} \\ &\ge q^n - q^{\frac{n}{q_1}+1}. \end{aligned}$$

As above, since the largest $d < n/q_1$ to make $\mu(n/d) = -1$ is n/q_2, discard all $d|n$, $d < n/q_1$ with $\mu(n/d) = 1$, and assume for all $d < n/q_2$, that $\mu(n/d) = -1$ in (6.7). Then we can obtain (6.8).

For $n \ge 3$, $n/q_1 + 1 \le n - 1$. Let

$$\underline{N_q}(n) \; = \; \begin{cases} N_q(n) & n = 1, 2, \\ \frac{1}{n}\left(q^n - q^{n-1}\right) & n \ge 3, \end{cases} \tag{6.9}$$

$$\overline{N_q}(n) \; = \; \frac{1}{n}\left(q^n - q\right). \tag{6.10}$$

Then we have

$$\underline{N_q}(n) \le N_q(n) \le \frac{1}{n}\left(q^n - q^{\frac{n}{q_1}}\right) \le \overline{N_q}(n). \tag{6.11}$$

This equation gives the proof of Lemma 5.3. Moreover, since

$$\sum_{i=s+1}^{n} i\overline{N_q}(i) = \frac{q^{n+1}-q^{s+1}}{q-1} - (n-s)q < q^{n+1} - q^s \le \sum_{i=s+1}^{n+1} i\underline{N_q}(i),$$

we have

$$\sum_{i=s+1}^{n_0} iN_q(i) \le \sum_{i=s+1}^{n_0} i\overline{N_q}(i) < \sum_{i=s+1}^{n_0+1} i\underline{N_q}(i) \le \sum_{i=s+1}^{n_0+1} iN_q(i). \tag{6.12}$$

It follows that

$$\left\lfloor \log_q(D+q^s) \right\rfloor - 1 \le n_0 = \gamma(D,s) \le \left\lfloor \log_q(D+q^s) \right\rfloor. \tag{6.13}$$

Meanwhile, we give some approximation of $\Gamma(D,s)$:

$$\begin{aligned}
\Gamma(D,s) \;&\ge\; \sum_{i=s+1}^{n_0} N_q(i) + \frac{1}{n_0+1}\left(D - \sum_{i=s+1}^{n_0} iN_q(i)\right) - 1 \\
&=\; \sum_{i=s+1}^{n_0} N_q(i)\left(1 - \frac{i}{n_0+1}\right) + \frac{D}{n_0+1} - 1 \\
&\ge\; \frac{D}{n_0+1} - 1 & (6.14)\\
&\ge\; \frac{D}{\left\lfloor \log_q(D+q^s) \right\rfloor + 1} - 1. & (6.15)
\end{aligned}$$

Equation (6.15) shows that $\Gamma(D,s)$ is on the order of $\Omega(D/\log D)$. Moreover, according to the definition of $\Gamma(D,s)$, we know:

$$\Gamma(D,s) \le \frac{D}{s+1}.$$

When $D = m(d+s)$, we have:

$$\Gamma(m(d+s),s) \le \frac{m(d+s)}{s+1} = m\left(d - \frac{d-1}{s+1}s\right) \le md. \tag{6.16}$$

Thus Lemma 5.1 has been proved.

Chapter 7

Verification and complexity analysis

In this chapter, we analyze the complexity of computing a lattice compression AB and give an algorithm to verify the correctness of the compression (that is, verify that $AB \equiv_R A$). We discuss the cost of the Monte Carlo lattice compression algorithm in Section 7.1. Recall we mention many algorithms require square input matrices in Chapter 1. In Section 7.2, we give an algorithm to convert a rectangular matrix into a square one. In Section 7.3, we present a method to verify the correctness of compressions and design a Las Vegas lattice compression algorithm.

To give cost estimates, we use the following notations. Let $\mathsf{M}(d)$ denote the required number of field operations for the multiplications of polynomials over $\mathsf{K}[x]$ with degree bound d. Let $\mathsf{B}(d)$ denote the required number of field operations for polynomial gcd-related computations between polynomials over $\mathsf{K}[x]$ with degree bound d. Let θ, $2 < \theta \leq 3$, be such that the multiplication of two $n \times n$ matrices takes $O(n^{\theta})$ field operations. Here we always assume that $\mathsf{B}(d) = \mathsf{M}(d) \log d$ and $\mathsf{B}(n) = O(n^{\theta - 1})$.

7.1 The cost of the Monte Carlo compression algorithm

Theorem 5.5 gives a straightforward Monte Carlo Compression algorithm as follows.

Algorithm 7.1 Monte-Carlo Compression Algorithm: MCComp(A, k)

```
Input: $A \in \mathsf{K}[x]^{m \times n}$ with full row rank, $\deg A \le d$, $k \ge 1$.
Output: $AB \in \mathsf{K}[x]^{m \times (m+k)}$.
1: if $k \ge 2\lceil \log_q md \rceil + 9$ then
2:     $s := 0$
3: else
4:     $s := \lfloor \frac{1}{k}(2\log_q md + 3(1 + \log_q 300)) \rfloor$
5: end if
6: Generate a random matrix $B \in \mathsf{K}[x]^{n \times (m+k)}$, whose entries are chosen uniformly
   from $\mathsf{K}_s[x]$.
7: return $AB$.
```

The following table gives upper bounds on the probability that Algorithm 7.1 returns a incorrect lattice compression with respect to k.

	$k \ge 2\lceil \log_q md \rceil + 9$	$q = 2 \wedge k \le 2$	$q > 2 \vee k > 2$
probability of failure	$\left(\frac{1}{q}\right)^{\left\lfloor \frac{k-t}{3} \right\rfloor}$[1]	$2\left(\frac{1}{2}\right)^k - \frac{3}{4}\left(\frac{1}{4}\right)^k + 0.01$	$\left(\frac{1}{q}\right)^k + 2\left(\frac{1}{q}\right)^{k+1} + \left(\frac{1}{q}\right)^{2k} + 0.01$

(7.1)

The cost of computing the matrix multiplication in line 7 determines the cost of Algorithm 7.1. When $s \in O(1)$, the cost of the multiplication is $O(nm^{\theta-2}(m + \log d)\mathsf{M}(d))$ field operations. When $s \in \Theta(\log md)$, the cost of the multiplication is $O(nm^{\theta-1}\mathsf{M}(d + \log m))$ field operations. Thus we have the following theorem.

Theorem 7.1. *The Cost of the Monte Carlo Compression Algorithm 7.1 is:*

- $O(nm^{\theta-2}(m + \log d)\mathsf{M}(d))$ *field operations, if* $s \in O(1)$.
- $O(nm^{\theta-1}\mathsf{M}(d + \log m))$ *field operations, if* $s \in \Theta(\log md)$.

7.2 Convert rectangular matrix into square matrix

Recall from Chapter 1 that many algorithms require square input matrices. Since the output of lattice compression is still a rectangular matrix, we present a method to generate a square matrix from a rectangular one in this section.

[1] Here $t = 2\lceil \log_q md \rceil + 6$.

For a matrix $C \in \mathsf{K}[x]^{m\times(m+k)}$ with full row rank m, we are going to construct a nonsingular matrix $\tilde{C} \in \mathsf{K}[x]^{(m+k)\times(m+k)}$ with the form of

$$\tilde{C} = \left[\begin{array}{c} C \\ \hline * \end{array}\right] \in \mathsf{K}[x]^{(m+k)\times(m+k)},$$

such that $\deg(\tilde{C}) \leq \deg(C)$ and it has the Hermite column basis

$$H_{\tilde{C}} = \left[\begin{array}{c|c} H_C & 0 \\ \hline 0 & I_k \end{array}\right] \in \mathsf{K}[x]^{(m+k)\times(m+k)},$$

where H_C is the Hermite column basis of C.

In order to compute $\tilde{C}$, we rely on the determinant reduction algorithm in Storjohann [2002]. This algorithm can transform a nonsingular square matrix D into $\tilde{D}$ with $\tilde{D}$ equal to D except the last row, $\deg(\tilde{D}) \leq \deg(D)$, and the last diagonal entry of $\tilde{D}$ in the Hermite column basis of $\tilde{D}$ equal to 1. Here is an example of determinant reduction over $\mathbb{Z}_7[x]$. The rectangular matrix

$$C = \begin{bmatrix} 3x^2 - x + 2 & 3x & 3x \\ x^2 + 3x + 3 & 3x^2 - 2x & 3x^2 - 3x \end{bmatrix},$$

with its Hermite column basis

$$H_C = \begin{bmatrix} 1 & 0 \\ -2 & x \end{bmatrix}.$$

Attach matrix C with a row vector and covert it into a square matrix D. Before the reduction, the matrix D and its Hermite column basis H_D are:

$$\begin{aligned} D &= \begin{bmatrix} 3x^2 - x + 2 & 3x & 3x \\ x^2 + 3x + 3 & 3x^2 - 2x & 3x^2 - 3x \\ -2x^2 + x - 1 & 3x^2 + x & 3x^2 - 2 \end{bmatrix}, \\ H_D &= \begin{bmatrix} 1 & 0 & 0 \\ -2 & x & 0 \\ -x + 3 & x + 2 & x^2 + x + 2 \end{bmatrix}. \end{aligned}$$

After the reduction, we have a new matrix $\tilde{D}$ and its Hermite column basis $H_{\tilde{D}}$ are:

$$\begin{aligned} \tilde{D} &= \begin{bmatrix} 3x^2 - x + 2 & 3x & 3x \\ x^2 + 3x + 3 & 3x^2 - 2x & 3x^2 - 3x \\ 3x & 3x & 3x - 1 \end{bmatrix}, \\ H_{\tilde{D}} &= \begin{bmatrix} 1 & 0 & 0 \\ -2 & x & 0 \\ 0 & 0 & 1 \end{bmatrix}. \end{aligned}$$

Storjohann [2002] also mentions that the determinant reduction for more than one row can be accomplished with single row determinant reductions and permutations. Thus if we have a nonsingular $(m+k) \times (m+k)$ matrix with the form of

$$\left[\begin{array}{c} C \\ \hline * \end{array}\right] \in \mathsf{K}[x]^{(m+k)\times(m+k)},$$

we can apply the determinant reduction algorithm to this matrix and obtain the desired matrix $\tilde{C}$. Let $\tilde{X} \in \mathsf{K}[x]$ be an irreducible polynomial such that $\operatorname{rank}(C \bmod \tilde{X}) = m$ over $\mathsf{K}[x]/(\tilde{X})$. Without loss of generality, suppose the first m columns have full rank m over $\mathsf{K}[x]/(\tilde{X})$, then the matrix

$$\left[\begin{array}{cc} \multicolumn{2}{c}{C} \\ \hline 0 & I_k \end{array}\right] \in \mathsf{K}[x]^{(m+k)\times(m+k)}$$

has full rank over $\mathsf{K}[x]$.

The cost of line 1 in Algorithm 7.2 is same with the cost of Gaussian elimination of an $m \times (m+k)$ matrix over $\mathsf{K}[x]/(\tilde{X})$, which costs $O((m+k)m^{\theta-1}\mathsf{B}(\deg \tilde{X}))$ field operations. The determinant reduction in line 4 of Algorithm 7.2 consists of k single row determinant reduction. According to Storjohann, 2002, Propsition 38, we know the cost of one single row determinant reduction is $O((m+k)^\theta \log(m+k)\mathsf{B}(\deg \tilde{X} + \deg C))$ field operations. This gives the following.

Theorem 7.2. *The cost of Algorithm 7.2 is* $O((m+k)m^{\theta-1}\mathsf{B}(\deg \tilde{X}) + k(m+k)^\theta \log(m+k)\mathsf{B}(\deg \tilde{X} + \deg C))$.

Algorithm 7.2 Convert a rectangular matrix into a square one: SQconv$(C, \tilde{X})$

```
Input: $C \in \mathsf{K}[x]^{m\times(m+k)}$, rank$(C) = m$ over $\mathsf{K}[x]$. $\tilde{X} \in \mathsf{K}[x]$ is an irreducible
    polynomial such rank$(C \bmod \tilde{X}) = m$ over $\mathsf{K}[x]/(\tilde{X})$.
Output: $\tilde{C} \in \mathsf{K}[x]^{(m+k)\times(m+k)}$ such that $H_{\tilde{C}} = \begin{bmatrix} H_C & 0 \\ 0 & I_k \end{bmatrix}$.
1: Use LSP decomposition [Ibarra et al., 1982] to compute the permutation
    $P \in \mathsf{K}[x]^{(m+k)\times(m+k)}$ such that the first $m$ columns of $CP$ have full rank over
    $\mathsf{K}[x]/(\tilde{X})$.
2: Let
    $$C^* = \left[\begin{array}{c} CP \\ \hline 0 \quad I_k \end{array}\right] P^{-1}$$
3: Apply $k$-rows determinant reduction algorithm to $C^*$. Let $\tilde{C}$ be its result.
4: return $\tilde{C}$.
```

7.3 Correctness verification and Las Vegas compression algorithm

We now consider how to verify the correctness of a compression. We know that $AB \equiv_R A$ if and only if $H_A = H_{AB}$, where H_A and H_{AB} are Hermite column basis of A and AB, respectively. Therefore, we can verify the correctness by computing and comparing H_A and H_{AB}. However, computing the Hermite column basis of A using the fastest known algorithm of Storjohann [2000] will cost $O(nm^{\theta-1}\mathsf{B}(md))$ field operations. Comparing it with the cost in Theorem 7.1, we know that computing H_A is almost m times as costly as computing AB. In this section, we present an alternative method to verify the correctness.

Apply Algorithm 7.2 to the compressed matrix AB and we can get an $(m+k)\times(m+k)$ nonsingular matrix $\tilde{A}$ with the form of

$$\tilde{A} = \left[\begin{array}{c} AB \\ \hline * \end{array}\right],$$

such that it has the Hermite column basis

$$H_{\tilde{A}} = \left[\begin{array}{c|c} H_{AB} & 0 \\ \hline 0 & I_k \end{array}\right],$$

The following lemma provides a method to verify the correctness of a compression.

Lemma 7.3. *$AB \equiv_R A$ if and only if $\tilde{A}^{-1}\left[\begin{array}{c} A \\ \hline 0 \end{array}\right] \in \mathsf{K}[x]^{(m+k)\times n}$.*

Proof. Let $U_{\tilde{A}}$ be the unimodular transform matrix such that $\tilde{A}U_{\tilde{A}} = H_{\tilde{A}}$. Then

$$\tilde{A}^{-1}\left[\begin{array}{c} A \\ \hline 0 \end{array}\right] = U_{\tilde{A}}H_{\tilde{A}}^{-1}\left[\begin{array}{c} A \\ \hline 0 \end{array}\right] = U_{\tilde{A}}\left[\begin{array}{c|c} H_{AB}^{-1} & 0 \\ \hline 0 & I_k \end{array}\right]\left[\begin{array}{c} A \\ \hline 0 \end{array}\right] = U_{\tilde{A}}\left[\begin{array}{c} H_{AB}^{-1}A \\ \hline 0 \end{array}\right].$$

Here H_{AB} is the Hermite column basis of AB. Notice that $\tilde{A}^{-1}\left[\begin{array}{c} A \\ \hline 0 \end{array}\right]$ is over $\mathsf{K}[x]$ if and only if $H_{AB}^{-1}A$ is over $\mathsf{K}[x]$. Since $\mathcal{L}(AB) \subseteq \mathcal{L}(A)$, $H_{AB}^{-1}A$ is over $\mathsf{K}[x]$ if and only if $H_A = H_{AB}$. □

Using the integrality certification algorithm in Storjohann [2002], which will tell us whether $\tilde{A}^{-1}A$ is over $\mathsf{K}[x]$, we can verify the correctness of the compression. The cost of integrality certification is $O(\log(m+k)nm^{\theta-1}\mathsf{B}(d+s))$ field operations, which is only logarithmic times as much as the lattice compression.

Our Las Vegas lattice compression algorithm has three stages.

1. Choose an random irreducible $\tilde{X} \in \mathsf{K}[x]$ such that $\operatorname{rank}(A \bmod \tilde{X}) = m$. Return fail if $\operatorname{rank}(A \bmod \tilde{X}) < m$.
2. Compute the lattice compression AB.
3. Verify that $AB \equiv_R A$. Return AB if $AB \equiv_R A$, otherwise return fail.

The Algorithm 7.2 requires an irreducible polynomial $\tilde{X}$ such that $\tilde{X} \perp \det H_{AB}$ for its input matrix AB. The integrality certification algorithm also needs such an $\tilde{X}$ with respect to matrix $\tilde{A}$. Since the Hermite column basis of $\tilde{A}$ is the same as the Hermite column basis of AB except for the last k columns, and the last k diagonal entries in the Hermite column basis of $\tilde{A}$ are equal to one. We know $\det \tilde{A}$ is an associate of $\det H_{AB}$ and the compression is successful if and only if $H_A = H_{AB}$. Thus we only need to find an irreducible $\tilde{X}$ such that $\tilde{X} \perp \det H_A$. Since $\det H_A \leq md$, if the finite field K is large enough with $q > 8md$, we can randomly draw a polynomial $\tilde{X}$ in K with degree 1 and the probability that $\operatorname{rank}(A) < m$ over $\mathsf{K}[x]/(\tilde{X})$ is $md/q < 1/8$.

When $q \leq 8md$, we generate $\tilde{X}$ randomly and uniformly in all the irreducible polynomials with degree t for some integer t. According to (6.9), we know that the total number of such polynomials is $N_q(t) \geq (q^t - q^{t-1})/t \geq q^t/2t$, and that the number of irreducible divisors of $\det \mathcal{L}(A)$ is no more than md/t. Thus we know the probability P such that $\text{rank}(A) < m$ over $\mathsf{K}[x]/(\tilde{X})$ satisfies

$$P \leq \frac{md}{t} \cdot \frac{2t}{q^t} = \frac{2md}{q^t}.$$

If $t = \lceil \log_q md \rceil + 4$, the probability that $\text{rank}(A) < m$ over $\mathsf{K}[x]/(\tilde{X})$ is smaller than or equal to $1/8$. The detail version of the Las Vegas compression algorithm is presented in Algorithm 7.3.

First we compute the probability of failure of Algorithm 7.3. According to the construction of $\tilde{X}$, we know the probability that $\tilde{X}$ is a divisor of $\det \mathcal{L}(A)$ is less than or equal to $1/8$. Thus the probability of returning failed in line 7 of Algorithm 7.3 is bounded by $1/8$.

Lines 16 and 20 of Algorithm 7.3 are the verification of correctness of the compression. Thus they fail if and only if the compression isn't successful, and the probability that Algorithm 7.3 fails in Line 16 or 20 is the same as the probability of failure in (7.1), which shows that the probability that the compression fails is less than 0.823. Thus we have the following theorem.

Theorem 7.4. *The probability that Algorithm 7.3 returns "fail" is less than* 0.95[1].

In the end, we analysis the complexity of Algorithm 7.3. The algorithm in Shoup [1994] showed that the cost of generating a random irreducible polynomial with degree bound d over a finite field with size q is $O((d^2 \log d + d \log q) \log d \log \log d)$ field operations. In this paper, we always consider q as constant, so that this cost should be $O(d^2 (\log d)^2 \log \log d)$. The cost of rank checking in line 16 of Algorithm 7.3 is same with cost of line 1 of Algorithm 7.2. According to Storjohann [2002], the integrality certification in line 19 takes $O(\log(m+k) n (m+k)^{\theta-1} \mathsf{B}(d+s))$ field operations. Observing of the costs above, recalling the cost of compression in Theorem 7.1 and the cost of Algorithm 7.2 in Theorem 7.2, we discuss the complexity of our Algorithm 7.3 in two cases.

- When $k \in O(1)$, according to (5.14), we have $s \in \Theta(\log md)$. Theorem 7.1 shows the cost of lattice compression is $O(nm^{\theta-1}\mathsf{M}(d+\log m))$ field operations. Theorem 7.2 gives the cost of Algorithm 7.2 in line 18 as $O(nm^{\theta-1}\mathsf{B}(d+\log m))$ field operations, and the integral certificate in line 19 takes $O((\log m) nm^{\theta-1}\mathsf{B}(d+\log m))$ field operations. Thus the total cost of Algorithm 7.3 is $O((\log m) nm^{\theta-1}\mathsf{B}(d+\log m))$ field operations.

[1] This is the probability in the worst case that $q = 2 \wedge k = 1$. The probability of failure will decrease exponentially with the increase of k.

Algorithm 7.3 Las Vegas Compression Algorithm: LVComp(A, k)

```
Input: $A \in \mathsf{K}[x]^{m\times n}$ with full row rank, $\deg A \leq d$. $k \geq 1$
Output: $AB \in \mathsf{K}[x]^{m\times(m+k)}$ such that $\mathcal{L}(A) = \mathcal{L}(AB)$, or fail.
[Stage 1. Randomly Generate $\tilde{X}$]
if $q > 8md$ then
    Randomly and uniformly choose an irreducible polynomial in $\mathsf{K}_1[x]$ as $\tilde{X}$.
else $\{q \leq 8md\}$
    Randomly and uniformly choose an irreducible polynomial with degree
    $\lceil \log_q md \rceil + 4$ as $\tilde{X}$.
end if
[Stage 2. Compute Lattice Compression $AB$]
if $rank(A \bmod \tilde{X}) < m$ over $\mathsf{K}[x]/(\tilde{X})$ then
    return fail
end if
if $k \geq 2\lceil \log_q md \rceil + 9$ then
    $s := 0$
else
    $s := \lfloor \frac{1}{k}(2\log_q md + 3(1 + \log_q 300)) \rfloor$
end if
Generate a random matrix $B \in \mathsf{K}[x]^{n\times(m+k)}$, whose entries are chosen uniformly
from $\mathsf{K}_s[x]$. Compute $AB$.
[Stage 3. Verify that $AB \equiv_R A$]
if $rank(AB \bmod \tilde{X}) < m$ over $\mathsf{K}[x]/(\tilde{X})$ then
    return fail
end if
SQconv$(AB, \tilde{X})$
Use integrality certification to know whether $\tilde{A}^{-1}\left[\begin{array}{c} A \\ \hline 0 \end{array}\right]$ is over $\mathsf{K}[x]$. if the
integrality certification returns fail then
return fail
end if
return $AB$.
```

- When $k \in \Theta(\log md)$, $s \in O(1)$. According to Theorem 7.1 the cost of lattice compression is $O(nm^{\theta-2}(m+\log d)\mathsf{M}(d))$ field operations. The cost of Algorithm 7.2 in line 23 given by Theorem 7.2 is $O((\log md)^2(m+\log d)^{\theta}\mathsf{B}(d))$ field operations. The integral certificate in line 24 takes $O((\log md)n(m+\log d)^{\theta-1}\mathsf{B}(d))$ field operations. Therefore, the total cost of Algorithm 7.3 is $O((\log md)n(m+\log d)^{\theta-1}\mathsf{B}(d)+(\log md)^2(m+\log d)^{\theta}\mathsf{B}(d))$ field operations.

Theorem 7.5. *The cost of Algorithm 7.3 is:*

- $O((\log m)nm^{\theta-1}\mathsf{B}(d+\log m))$ *field operations if* $k \in O(1)$.
- $O((\log md)n(m+\log d)^{\theta-1}\mathsf{B}(d)+(\log md)^2(m+\log d)^{\theta}\mathsf{B}(d))$ *field operations if* $k \in \Theta(\log md)$.

Ignoring logarithmic factors, the cost estimate in Theorem 7.5 becomes $O\tilde{}(nm^{\theta-1}\mathsf{B}(d))$ field operations.

Chapter 8

Conclusion

We have studied lattice compression over the polynomial ring of finite fields. For a finite field K with size q and an $m \times n$ matrix A over $\mathsf{K}[x]$ with degree bound d, we compress A with a $n \times (m+k)$ matrix B whose entries are randomly and uniformly chosen from $\mathsf{K}[x]$ with degree bound s. Our main contribution is the analysis of the probability that $AB \equiv_R A$ with respect to m, d, q, k, and present the proper degree bound s in different cases. We show that there is a positive probability to get a successful compression even if $s = 0$ as long as $k \in \Omega(\log_q md)$. In general, we can always guarantee a positive probability of successful compression by keeping $k(s+1) \in \Omega(\log_q md)$. Particularly, if the field k has enough entries, we can keep $s = 0$ and $k = 1$ to get a positive probability of success.

The lattice compression can be implemented with either Monte Carlo or Las Vegas randomized algorithm. The Monte Carlo algorithm can be used in some applications where the correctness verification isn't required such as linear system solving. For those applications in which the correctness of the compression must be guaranteed, we design a competitive Las Vegas compression algorithm with a positive probability of success and cost of $O\tilde{}(nm^{\theta-1}\mathsf{B}(d))$ field operations.

Though in our discussion, we assume A to be a matrix with full row rank, it can be generalized to singular matrices as well. If $\text{rank}(A) = r$, the results in Section 5.5 still work even with each occurrence of m replaced with r. Moreover, the algorithm could as well be modified to compress a singular matrix A with its rank r given by the input. We can pick $r \times n$ minor $\bar{A}$ of A with full row rank during the LSP decomposition in line 1 of Algorithm 7.3, find a compression matrix for $\bar{A}$ and then generate the correspond compression matrix for A.

The further study in lattice compression lays on the case in which A is a sparse matrix. Since probability in (3.1) and the analysis in Section 4.3 do not hold in this case, we need to find some other methods to compute the probability or use different way to generate the random matrix B.

Bibliography

Z. Chen and A. Storjohann. A BLAS based C library for exact linear algebra on integer matrices. In M. Kauers, editor, *Proc. Int'l. Symp. on Symbolic and Algebraic Computation: ISSAC '05*, pages 92–99. ACM Press, New York, 2005.

A. Conflitti. On computation of the greatest common divisor of several polynomials over a finite field. *Finite Field Appl.*, 9:423–431, 2003.

G. Cooperman, S. Feisel, J. von zur Gathen, and G. Havas. GCD of many integers (Extended Abstract). In *Proceedings of the Fifth International Computing and Combinatorics Conference, Tokyo, 1999, Lecture Notes in Computer Science*, volume 1627, pages 310–317, Berlin, 1999. Springer-Verlag.

W. Eberly, M. Giesbrecht, and G. Villard. Computing the determinant and Smith form of an integer matrix. In *Proc. 31st Ann. IEEE Symp. Foundations of Computer Science*, pages 675–685, 2000.

J. von zur Gathen and I. E. Shparlinski. GCD of random linear forms. In *Algorithms and Computation: 15th International Symposium, ISAAC 2004*, LNCS 3341, pages 464–469. Springer Verlag, 2004.

P. Giorgi, C.-P. Jeannerod, and G. Villard. On the complexity of polynomial matrix computations. In R. Sendra, editor, *Proc. Int'l. Symp. on Symbolic and Algebraic Computation: ISSAC '03*, pages 135–142. ACM Press, New York, 2003.

O. Ibarra, S. Moran, and R. Hui. A generalization of the fast LUP matrix decomposition algorithm and applications. *Journal of Algorithms*, 3:45–56, 1982.

E. Kaltofen, M. S. Krishnamoorthy, and B. D. Saunders. Parallel algorithms for matrix normal forms. *Linear Algebra and its Applications*, 136:189–208, 1990.

Donald E. Knuth. *Art of Computer Programming, Volume 1: Fundamental Algorithms (3rd Edition).* Addison-Wesley Professional, November 1997.

R. Lidl and H. Niederreiter. *Finite Fields.* Addison-Wesley, 1983.

T. Mulders and A. Storjohann. Certified dense linear system solving. *Journal of Symbolic Computation*, 37(4):485–510, 2004.

J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27:701–717, 1980.

V. Shoup. Fast construction of irreducible polynomials over finite fields. *Journal of Symbolic Computation*, 17:371–391, 1994.

A. Storjohann. *Algorithms for Matrix Canonical Forms.* PhD thesis, Swiss Federal Institute of Technology, ETH–Zurich, 2000.

A. Storjohann. High–order lifting. Extended Abstract. In T. Mora, editor, *Proc. Int'l. Symp. on Symbolic and Algebraic Computation: ISSAC '02*, pages 246–254. ACM Press, New York, 2002.

A. Storjohann and G. Labahn. Preconditioning of rectangular polynomial matrices for efficient Hermite normal form computation. In A. H. M. Levelt, editor, *Proc. Int'l. Symp. on Symbolic and Algebraic Computation: ISSAC '95*, pages 119–125. ACM Press, New York, 1995.