On the probability of generating a primitive matrix

陈经纬

Joint work with Yong Feng, Yang Liu and Wenyuan Wu

arXiv:2105.05383

June 5, 2021 @ CM 2021

What is a primitive matrix?

Primitive vector $\boldsymbol{x} \in \mathbb{Z}^n$:

- Definition: $\boldsymbol{x} = d\boldsymbol{y}$ for $\boldsymbol{y} \in \mathbb{Z}^n$ and $d \in \mathbb{Z}$ implies $d = \pm 1$.
- Reiner '56: $\boldsymbol{x} \in \mathbb{Z}^n$ is primitive $\Longleftrightarrow$ $\boldsymbol{x}$ can be extended to an $n \times n$ **unimodular matrix** over $\mathbb{Z}$.

What is a primitive matrix?

Primitive vector $\boldsymbol{x} \in \mathbb{Z}^n$:

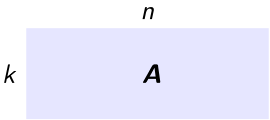
- Definition: $\boldsymbol{x} = d\boldsymbol{y}$ for $\boldsymbol{y} \in \mathbb{Z}^n$ and $d \in \mathbb{Z}$ implies $d = \pm 1$.
- Reiner '56: $\boldsymbol{x} \in \mathbb{Z}^n$ is primitive $\Longleftrightarrow$ $\boldsymbol{x}$ can be extended to an $n \times n$ **unimodular matrix** over $\mathbb{Z}$.

Primitive matrix $\boldsymbol{A} \in \mathbb{Z}^{k \times n}$ with $k \leq n$:

- Def.: $\boldsymbol{A}$ can be extended to an $n \times n$ unimodular matrix over $\mathbb{Z}$.

What is our problem?

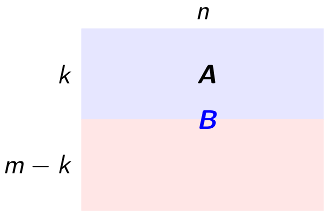
- For a given primitive matrix $\boldsymbol{A} \in \mathbb{Z}^{k \times n}$ with $\|\boldsymbol{A}\| = \max_{i,j} |a_{i,j}| \le \lambda$



What is our problem?

- For a given primitive matrix $\boldsymbol{A} \in \mathbb{Z}^{k\times n}$ with $\|\boldsymbol{A}\| = \max_{i,j} |a_{i,j}| \leq \lambda$
- Complete $\boldsymbol{A}$ to $\boldsymbol{B} \in \mathbb{Z}^{m\times n}$ with entries uniformly random from

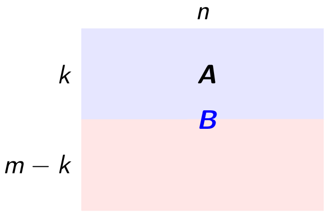
$$\Lambda := \mathbb{Z} \cap [0,\ \lambda).$$



What is our problem?

- For a given primitive matrix $\boldsymbol{A} \in \mathbb{Z}^{k \times n}$ with $\|\boldsymbol{A}\| = \max_{i,j} |a_{i,j}| \leq \lambda$
- Complete $\boldsymbol{A}$ to $\boldsymbol{B} \in \mathbb{Z}^{m \times n}$ with entries uniformly random from

$$\Lambda := \mathbb{Z} \cap [0,\ \lambda).$$



- **What is the probability** of that $\boldsymbol{B}$ is still primitive ?

Motivation

- Unimodular matrices has many applications.
  - lattice reduction, sigal compression, optimization, $\cdots$

Motivation

- Unimodular matrices has many applications.
  - lattice reduction, sigal compression, optimization, $\cdots$
- Unimodular matrix completion is classic.
  - Reiner '56, Cassels '71, Newman '72, $\cdots$

Motivation

- Unimodular matrices has many applications.
  - lattice reduction, sigal compression, optimization, $\cdots$
- Unimodular matrix completion is classic.
  - Reiner '56, Cassels '71, Newman '72, $\cdots$
- Unimodular matrix completion is still active.
  - Existence: Zhan '06, Fang '07, Duffner & Silva '17, $\cdots$
  - Polynomial matrices: Kalaimani, *et al*. '13, Zhou & Labahn '14, $\cdots$
  - Probability/density: Maze *et al*. '11, Fontein & Wocjan '14, $\cdots$

Motivation

- Unimodular matrices has many applications.
  - lattice reduction, sigal compression, optimization, $\cdots$
- Unimodular matrix completion is classic.
  - Reiner '56, Cassels '71, Newman '72, $\cdots$
- Unimodular matrix completion is still active.
  - Existence: Zhan '06, Fang '07, Duffner & Silva '17, $\cdots$
  - Polynomial matrices: Kalaimani, *et al*. '13, Zhou & Labahn '14, $\cdots$
  - Probability/density: Maze *et al*. '11, Fontein & Wocjan '14, $\cdots$
- How to effeciently complete a primitive matrix ?
  - Method: Choose elements uniformly at random from Λ.

Motivation

- Unimodular matrices has many applications.
  - lattice reduction, sigal compression, optimization, $\cdots$
- Unimodular matrix completion is classic.
  - Reiner '56, Cassels '71, Newman '72, $\cdots$
- Unimodular matrix completion is still active.
  - Existence: Zhan '06, Fang '07, Duffner & Silva '17, $\cdots$
  - Polynomial matrices: Kalaimani, *et al*. '13, Zhou & Labahn '14, $\cdots$
  - Probability/density: Maze *et al*. '11, Fontein & Wocjan '14, $\cdots$
- How to effeciently complete a primitive matrix ?
  - Method: Choose elements uniformly at random from Λ.
  - **Problem 1**: How many rows can we randomly choose ?

Motivation

- Unimodular matrices has many applications.
  - lattice reduction, sigal compression, optimization, $\cdots$
- Unimodular matrix completion is classic.
  - Reiner '56, Cassels '71, Newman '72, $\cdots$
- Unimodular matrix completion is still active.
  - Existence: Zhan '06, Fang '07, Duffner & Silva '17, $\cdots$
  - Polynomial matrices: Kalaimani, *et al*. '13, Zhou & Labahn '14, $\cdots$
  - Probability/density: Maze *et al*. '11, Fontein & Wocjan '14, $\cdots$
- How to effeciently complete a primitive matrix ?
  - Method: Choose elements uniformly at random from Λ.
  - **Problem 1**: How many rows can we randomly choose ?
  - **Problem 2**: What is the probability of success ?

Motivation

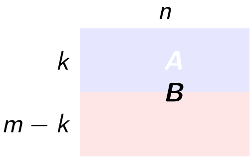
- Unimodular matrices has many applications.
  - lattice reduction, sigal compression, optimization, $\cdots$
- Unimodular matrix completion is classic.
  - Reiner '56, Cassels '71, Newman '72, $\cdots$
- Unimodular matrix completion is still active.
  - Existence: Zhan '06, Fang '07, Duffner & Silva '17, $\cdots$
  - Polynomial matrices: Kalaimani, *et al*. '13, Zhou & Labahn '14, $\cdots$
  - Probability/density: Maze *et al*. '11, Fontein & Wocjan '14, $\cdots$
- How to effeciently complete a primitive matrix ?
  - Method: Choose elements uniformly at random from Λ.
  - **Problem 1**: How many rows can we randomly choose ?
  - **Problem 2**: What is the probability of success ?
  - **Problem 3**: How fast is the algorithm ?

Our result on the probability

- A primitive matrix $\boldsymbol{A} \in \mathbb{Z}^{k \times n}$ with $\|\boldsymbol{A}\| \leq \lambda$
- An integer s with $0 \leq s \leq n - k - 2$
- $\boldsymbol{B} \in \mathbb{Z}^{(n-s-1) \times n}$: a completion of $\boldsymbol{A}$ with unif. rand. entries from Λ

Then the probability of that $\boldsymbol{B}$ is primitive is at least

$$1 - 4\left(\frac{2}{3}\right)^{s+1}\left(1 - \left(\frac{2}{3}\right)^{n-k-s-1}\right) - \frac{2(n-s-1)^2}{\lambda^{s+2}}\left(1 - \frac{1}{\lambda^{n-k-s-1}}\right).$$



$m = (n-1) - s$

Our result on the probability

- A primitive matrix $\boldsymbol{A} \in \mathbb{Z}^{k\times n}$ with $\|\boldsymbol{A}\| \leq \lambda$
- An integer s with $0 \leq s \leq n-k-2$
- $\boldsymbol{B} \in \mathbb{Z}^{(n-s-1)\times n}$: a completion of $\boldsymbol{A}$ with unif. rand. entries from Λ

Then the probability of that $\boldsymbol{B}$ is primitive is at least

$$1 - 4\left(\frac{2}{3}\right)^{s+1} \cancel{\left(1 - \left(\frac{2}{3}\right)^{n-k-s-1}\right)} - \frac{2(n-s-1)^2}{\lambda^{s+2}} \cancel{\left(1 - \frac{1}{\lambda^{n-k-s-1}}\right)}.$$

- The bound is almost independent of k.

Our result on the probability

- A primitive matrix $\boldsymbol{A} \in \mathbb{Z}^{k \times n}$ with $\|\boldsymbol{A}\| \le \lambda$
- An integer s with $0 \le s \le n-k-2$
- $\boldsymbol{B} \in \mathbb{Z}^{(n-s-1) \times n}$: a completion of $\boldsymbol{A}$ with unif. rand. entries from Λ

Then the probability of that $\boldsymbol{B}$ is primitive is at least

$$\mathbf{1 - 4\left(\frac{2}{3}\right)^{s+1}} \cancel{\left(1 - \left(\frac{2}{3}\right)^{n-k-s-1}\right)} - \cancel{\frac{2(n-s-1)^2}{\lambda^{s+2}}} \cancel{\left(1 - \frac{1}{\lambda^{n-k-s-1}}\right)}.$$

- The bound is almost independent of k.
- When λ is large, the bound could be even simpler.

Our result on the probability

- A primitive matrix $\boldsymbol{A} \in \mathbb{Z}^{k \times n}$ with $\|\boldsymbol{A}\| \leq \lambda$
- An integer s with $0 \leq s \leq n - k - 2$
- $\boldsymbol{B} \in \mathbb{Z}^{(n-s-1)\times n}$: a completion of $\boldsymbol{A}$ with unif. rand. entries from Λ

Then the probability of that $\boldsymbol{B}$ is primitive is at least

$$\mathbf{1 - 4\left(\frac{2}{3}\right)^{s+1}} \cancel{\left(1 - \left(\frac{2}{3}\right)^{n-k-s-1}\right)} - \cancel{\frac{2(n-s-1)^2}{\lambda^{s+2}}} \cancel{\left(1 - \frac{1}{\lambda^{n-k-s-1}}\right)}.$$

- The bound is almost independent of k.
- When λ is large, the bound could be even simpler.
- E.g., if $s = 3$, then the probability is ≥ 0.2.

Our result on the probability

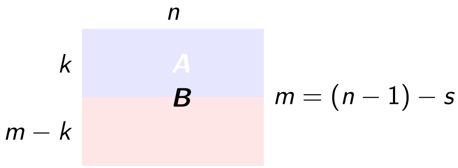
- A primitive matrix $\boldsymbol{A} \in \mathbb{Z}^{k \times n}$ with $\|\boldsymbol{A}\| \le \lambda$
- An integer s with $0 \le s \le n-k-2$
- $\boldsymbol{B} \in \mathbb{Z}^{(n-s-1) \times n}$: a completion of $\boldsymbol{A}$ with unif. rand. entries from Λ

Then the probability of that $\boldsymbol{B}$ is primitive is at least

$$\mathbf{1 - 4\left(\frac{2}{3}\right)^{s+1}} \cancel{\left(1-\left(\frac{2}{3}\right)^{n-k-s-1}\right)} - \cancel{\frac{2(n-s-1)^2}{\lambda^{s+2}}} \cancel{\left(1-\frac{1}{\lambda^{n-k-s-1}}\right)}.$$

- The bound is almost independent of k.
- When λ is large, the bound could be even simpler.
- E.g., if $s = 3$, then the probability is ≥ 0.2.
- The bound is **effective** only if $s \ge 3$!

Related work



- Maze, Rosenthal & Wagner '11: For $k = 0$, the natural density is

$$\prod_{j=s+2}^{n} \frac{1}{\zeta(j)} \quad (\lambda \to \infty),$$

  where $\zeta(\cdot)$ is the Riemann's zeta function.
- Fontein & Wocjan '14:
  - For $k \geq 2n+1$, a probability is rigorously proven.
  - For $n+1 \leq k < 2n+1$, a probability is conjectured.

Roadmap

1. **Proof of the result**

2. **Application to unimodular matrix completion**

Roadmap

1. **Proof of the result**

2. **Application to unimodular matrix completion**

The idea of the proof

For $i = k, \ \ldots, \ n-s-1$, define

$$\boldsymbol{A}_i = \begin{pmatrix} \boldsymbol{a}_1 \\ \boldsymbol{a}_2 \\ \vdots \\ \boldsymbol{a}_i \end{pmatrix} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & & \vdots \\ a_{i,1} & a_{i,2} & \cdots & a_{i,n} \end{pmatrix}.$$

Idea: Give an upper bound on the probability of the event that $\boldsymbol{A}_{n-s-1}$ is not primitive under the assumption that $\boldsymbol{A}_k$ is primitive.

Tool: If $\boldsymbol{A}_i$ is not primitive, then there must be at least one prime p such that $\mathrm{rank}(\boldsymbol{A}_i) \le i-1$ over $\mathbb{Z}_p$.

Some events and their probabilities

MDep_i: There exists at least one prime p s.t. $\mathrm{rank}(\boldsymbol{A}_i) \leq i - 1$ over $\mathbb{Z}_p$.

$\neg\mathrm{MDep}_i$: $\boldsymbol{A}_i$ is a primitive matrix.

Goal: Give an upper bound on $\Pr[\mathrm{MDep}_{n-s-1} | \neg\mathrm{MDep}_k]$.

Some events and their probabilities

MDep$_i$: There exists at least one prime p s.t. $\mathrm{rank}(\boldsymbol{A}_i) \leq i - 1$ over $\mathbb{Z}_p$.

$\neg$MDep$_i$: $\boldsymbol{A}_i$ is a primitive matrix.

Goal: Give an upper bound on $\Pr[\mathrm{MDep}_{n-s-1} | \neg\mathrm{MDep}_k]$.

$$\begin{aligned} & \Pr[\mathrm{MDep}_{n-s-1} | \neg\mathrm{MDep}_k] \\ \leq & \quad \cdots\cdots \\ \leq & \sum_{i=k+1}^{n-s-1} \Pr[\mathrm{MDep}_i \wedge \neg\mathrm{MDep}_{i-1}] \\ \leq & \sum_{i=k+1}^{n-s-1} \Pr[\mathrm{MDep}_i | \neg\mathrm{MDep}_{i-1}]. \end{aligned}$$

Bound $\Pr[\mathbf{MDep}_i | \neg \mathbf{MDep}_{i-1}]$

Let $\lambda \geq 2$ be an integer and $k+1 \leq i \leq n-3$.

Bound $\Pr[\mathbf{MDep}_i | \neg \mathbf{MDep}_{i-1}]$

Let $\lambda \geq 2$ be an integer and $k + 1 \leq i \leq n - 3$.

The case of $p < \lambda$

$$\Pr[\mathrm{MDep}_i | \neg \mathrm{MDep}_{i-1}] \leq \left(\frac{2}{3}\right)^{n-i+1} + \frac{3}{4}\left(\frac{1}{3}\right)^{n-i+1}.$$

Bound $\Pr[\mathbf{MDep}_i | \neg \mathbf{MDep}_{i-1}]$

Let $\lambda \geq 2$ be an integer and $k+1 \leq i \leq n-3$.

The case of $p < \lambda$

$$\Pr[\mathrm{MDep}_i | \neg \mathrm{MDep}_{i-1}] \leq \left(\frac{2}{3}\right)^{n-i+1} + \frac{3}{4}\left(\frac{1}{3}\right)^{n-i+1}.$$

The case of $p \geq \lambda$

$$\Pr[\mathrm{MDep}_i | \neg \mathrm{MDep}_{i-1}] \leq (i(1+\log_\lambda i)) \cdot \left(\frac{1}{\lambda}\right)^{n-i+1}.$$

Bound $\Pr[\mathbf{MDep}_i | \neg \mathbf{MDep}_{i-1}]$

Let $\lambda \geq 2$ be an integer and $k+1 \leq i \leq n-3$.

The case of $p < \lambda$

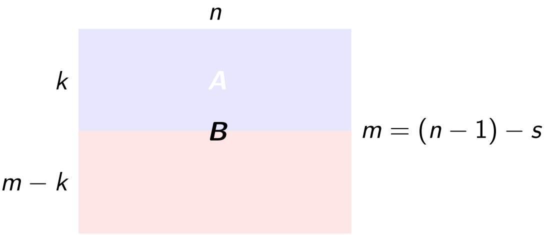
$$\Pr[\mathrm{MDep}_i | \neg \mathrm{MDep}_{i-1}] \leq \left(\frac{2}{3}\right)^{n-i+1} + \frac{3}{4}\left(\frac{1}{3}\right)^{n-i+1}.$$

The case of $p \geq \lambda$

$$\Pr[\mathrm{MDep}_i | \neg \mathrm{MDep}_{i-1}] \leq (i(1+\log_\lambda i)) \cdot \left(\frac{1}{\lambda}\right)^{n-i+1}.$$

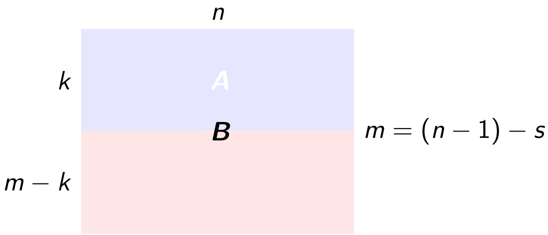
Remark. The analysis is adapted from Eberly, Giesbrecht & Villard (2000).

On the probability for $s = 0, 1, 2$



⚠ The bound is effective **only if** $s \geq 3$.

On the probability for $s = 0, 1, 2$



⚠ The bound is effective **only if** $s \geq 3$.

A heuristic based on an extensively experimental study:

A constant lower bound on the probability exists for $s = 0, 1, 2$ as well.

Roadmap

1. Proof of the result

2. **Application to unimodular matrix completion**

Hermite normal form

Non-singular matrix $\boldsymbol{H} \in \mathbb{Z}^{n\times n}$ is in Hermite normal form if

- $\boldsymbol{H}$ is upper triangular with non-negative entries,
- $h_{i,j} < h_{j,j}$.

$$\mathrm{HNF}(\boldsymbol{A}) = \begin{pmatrix} 1 & 0 & 0 & 10 & 260\,246\,748 \\ 0 & 1 & 0 & 2 & 292\,062\,707 \\ 0 & 0 & 1 & 7 & 244\,095\,302 \\ 0 & 0 & 0 & 14 & 342\,954\,195 \\ 0 & 0 & 0 & 0 & 344\,319\,363 \end{pmatrix}$$

Hermite normal form

Non-singular matrix $\boldsymbol{H} \in \mathbb{Z}^{n \times n}$ is in Hermite normal form if

- $\boldsymbol{H}$ is upper triangular with non-negative entries,
- $h_{i,j} < h_{j,j}$.

For any $\boldsymbol{A} \in \mathbb{Z}^{n \times n}$, there is a unique $\boldsymbol{H}$ in Hemite normal form, denoted by $\mathrm{HNF}(\boldsymbol{A})$, such that $\boldsymbol{H} = \boldsymbol{U}\boldsymbol{A}$ with $\boldsymbol{U}$ **unimodular**.

$$\mathrm{HNF}(\boldsymbol{A}) = \begin{pmatrix} 1 & 0 & 0 & 10 & 260\,246\,748 \\ 0 & 1 & 0 & 2 & 292\,062\,707 \\ 0 & 0 & 1 & 7 & 244\,095\,302 \\ 0 & 0 & 0 & 14 & 342\,954\,195 \\ 0 & 0 & 0 & 0 & 344\,319\,363 \end{pmatrix}$$

Hermite normal form

Non-singular matrix $\boldsymbol{H} \in \mathbb{Z}^{n\times n}$ is in Hermite normal form if

- $\boldsymbol{H}$ is upper triangular with non-negative entries,
- $h_{i,j} < h_{j,j}$.

For any $\boldsymbol{A} \in \mathbb{Z}^{n\times n}$, there is a unique $\boldsymbol{H}$ in Hemite normal form, denoted by $\mathrm{HNF}(\boldsymbol{A})$, such that $\boldsymbol{H} = \boldsymbol{U}\boldsymbol{A}$ with $\boldsymbol{U}$ **unimodular**.

$$\boldsymbol{A} = \begin{pmatrix} -66 & -65 & 20 & -90 & 30 \\ 55 & 5 & -7 & -21 & 62 \\ 68 & 66 & 16 & -56 & -79 \\ 13 & -41 & -62 & -50 & 28 \\ 26 & -36 & -34 & -8 & -71 \end{pmatrix} \quad \mathrm{HNF}(\boldsymbol{A}) = \begin{pmatrix} 1 & 0 & 0 & 10 & 260\,246\,748 \\ 0 & 1 & 0 & 2 & 292\,062\,707 \\ 0 & 0 & 1 & 7 & 244\,095\,302 \\ 0 & 0 & 0 & 14 & 342\,954\,195 \\ 0 & 0 & 0 & 0 & 344\,319\,363 \end{pmatrix}$$

Determinant reduction (Storjohann '03)

$$\boldsymbol{A} = \begin{pmatrix} -66 & -65 & 20 & -90 & 30 \\ 55 & 5 & -7 & -21 & 62 \\ 68 & 66 & 16 & -56 & -79 \\ 13 & -41 & -62 & -50 & 28 \\ 26 & -36 & -34 & -8 & -71 \end{pmatrix}$$

$$\mathrm{HNF}(\boldsymbol{A}) = \begin{pmatrix} 1 & 0 & 0 & 10 & 260\,246\,748 \\ 0 & 1 & 0 & 2 & 292\,062\,707 \\ 0 & 0 & 1 & 7 & 244\,095\,302 \\ 0 & 0 & 0 & 14 & 342\,954\,195 \\ 0 & 0 & 0 & 0 & 344\,319\,363 \end{pmatrix}$$

Determinant reduction (Storjohann '03)

$$\boldsymbol{A} = \begin{pmatrix} -66 & -65 & 20 & -90 & 30 \\ 55 & 5 & -7 & -21 & 62 \\ 68 & 66 & 16 & -56 & -79 \\ 13 & -41 & -62 & -50 & 28 \\ 26 & -36 & -34 & -8 & -71 \end{pmatrix} \quad \boldsymbol{B} = \begin{pmatrix} -66 & -65 & 20 & -90 & -14 \\ 55 & 5 & -7 & -21 & 2 \\ 68 & 66 & 16 & -56 & 17 \\ 13 & -41 & -62 & -50 & 4 \\ 26 & -36 & -34 & -8 & -4 \end{pmatrix}$$

$$\mathrm{HNF}(\boldsymbol{A}) = \begin{pmatrix} 1 & 0 & 0 & 10 & 260\,246\,748 \\ 0 & 1 & 0 & 2 & 292\,062\,707 \\ 0 & 0 & 1 & 7 & 244\,095\,302 \\ 0 & 0 & 0 & 14 & 342\,954\,195 \\ 0 & 0 & 0 & 0 & 344\,319\,363 \end{pmatrix}$$

Determinant reduction (Storjohann '03)

$$A = \begin{pmatrix} -66 & -65 & 20 & -90 & 30 \\ 55 & 5 & -7 & -21 & 62 \\ 68 & 66 & 16 & -56 & -79 \\ 13 & -41 & -62 & -50 & 28 \\ 26 & -36 & -34 & -8 & -71 \end{pmatrix} \quad B = \begin{pmatrix} -66 & -65 & 20 & -90 & -14 \\ 55 & 5 & -7 & -21 & 2 \\ 68 & 66 & 16 & -56 & 17 \\ 13 & -41 & -62 & -50 & 4 \\ 26 & -36 & -34 & -8 & -4 \end{pmatrix}$$

$$\mathrm{HNF}(A) = \begin{pmatrix} 1 & 0 & 0 & 10 & 260\,246\,748 \\ 0 & 1 & 0 & 2 & 292\,062\,707 \\ 0 & 0 & 1 & 7 & 244\,095\,302 \\ 0 & 0 & 0 & 14 & 342\,954\,195 \\ 0 & 0 & 0 & 0 & 344\,319\,363 \end{pmatrix} \qquad \mathrm{HNF}(B) = \begin{pmatrix} 1 & 0 & 0 & 10 & 0 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 1 & 7 & 0 \\ 0 & 0 & 0 & 14 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Determinant reduction (Storjohann '03)

Algorithm 1

Input: An integer matrix $\boldsymbol{A} \in \mathbb{Z}^{n\times n}$.

Output: A matrix $\boldsymbol{B} \in \mathbb{Z}^{n\times n}$, with $\boldsymbol{B}$ equal to $\boldsymbol{A}$ except for the last column, $\|\boldsymbol{B}\| \leq n^2\|\boldsymbol{A}\|$, and the last diagonal of HNF($\boldsymbol{B}$) equal to 1.

Proposition

Given an $n \times n$ integer matrix $\boldsymbol{A}$, Algorithm 1 is a correct Las Vegas algorithm and requires at most $O(n^{\omega+\varepsilon}\log^{1+\varepsilon}\|\boldsymbol{A}\|)$ bit operations.

Iterated determinant reduction (Storjohann '05)

$$\boldsymbol{B} = \begin{pmatrix} -66 & -65 & 20 & -90 & \color{red}{-14} \\ 55 & 5 & -7 & -21 & \color{red}{2} \\ 68 & 66 & 16 & -56 & \color{red}{17} \\ 13 & -41 & -62 & -50 & \color{red}{4} \\ 26 & -36 & -34 & -8 & \color{red}{-4} \end{pmatrix}$$

$$\mathrm{HNF}(\boldsymbol{B}) = \begin{pmatrix} 1 & 0 & 0 & 10 & \color{red}{0} \\ 0 & 1 & 0 & 2 & \color{red}{0} \\ 0 & 0 & 1 & 7 & \color{red}{0} \\ 0 & 0 & 0 & 14 & \color{red}{0} \\ 0 & 0 & 0 & 0 & \color{red}{1} \end{pmatrix}$$

Iterated determinant reduction (Storjohann '05)

$$\boldsymbol{B} = \begin{pmatrix} -66 & -65 & 20 & -90 & -14 \\ 55 & 5 & -7 & -21 & 2 \\ 68 & 66 & 16 & -56 & 17 \\ 13 & -41 & -62 & -50 & 4 \\ 26 & -36 & -34 & -8 & -4 \end{pmatrix} \quad \boldsymbol{BP} = \begin{pmatrix} -14 & -66 & -65 & 20 & -90 \\ 2 & 55 & 5 & -7 & -21 \\ 17 & 68 & 66 & 16 & -56 \\ 4 & 13 & -41 & -62 & -50 \\ -4 & 26 & -36 & -34 & -8 \end{pmatrix}$$

$$\mathrm{HNF}(\boldsymbol{B}) = \begin{pmatrix} 1 & 0 & 0 & 10 & 0 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 1 & 7 & 0 \\ 0 & 0 & 0 & 14 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Iterated determinant reduction (Storjohann '05)

$$\boldsymbol{B} = \begin{pmatrix} -66 & -65 & 20 & -90 & -14 \\ 55 & 5 & -7 & -21 & 2 \\ 68 & 66 & 16 & -56 & 17 \\ 13 & -41 & -62 & -50 & 4 \\ 26 & -36 & -34 & -8 & -4 \end{pmatrix} \quad \boldsymbol{BP} = \begin{pmatrix} -14 & -66 & -65 & 20 & -90 \\ 2 & 55 & 5 & -7 & -21 \\ 17 & 68 & 66 & 16 & -56 \\ 4 & 13 & -41 & -62 & -50 \\ -4 & 26 & -36 & -34 & -8 \end{pmatrix}$$

$$\mathrm{HNF}(\boldsymbol{B}) = \begin{pmatrix} 1 & 0 & 0 & 10 & 0 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 1 & 7 & 0 \\ 0 & 0 & 0 & 14 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad \mathrm{HNF}(\boldsymbol{BP}) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 10 \\ 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 7 \\ 0 & 0 & 0 & 0 & 14 \end{pmatrix}$$

Iterated determinant reduction (Storjohann '05)

$$\boldsymbol{BP} = \begin{pmatrix} -14 & -66 & -65 & 20 & -90 \\ 2 & 55 & 5 & -7 & -21 \\ 17 & 68 & 66 & 16 & -56 \\ 4 & 13 & -41 & -62 & -50 \\ -4 & 26 & -36 & -34 & -8 \end{pmatrix}$$

$$\mathrm{HNF}(\boldsymbol{BP}) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 10 \\ 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 7 \\ 0 & 0 & 0 & 0 & 14 \end{pmatrix}$$

Iterated determinant reduction (Storjohann '05)

$$
BP = \begin{pmatrix} -14 & -66 & -65 & 20 & -90 \\ 2 & 55 & 5 & -7 & -21 \\ 17 & 68 & 66 & 16 & -56 \\ 4 & 13 & -41 & -62 & -50 \\ -4 & 26 & -36 & -34 & -8 \end{pmatrix} \quad C = \begin{pmatrix} -14 & -66 & -65 & 20 & -20 \\ 2 & 55 & 5 & -7 & 12 \\ 17 & 68 & 66 & 16 & 31 \\ 4 & 13 & -41 & -62 & -21 \\ -4 & 26 & -36 & -34 & -9 \end{pmatrix}
$$

$$
\mathrm{HNF}(BP) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 10 \\ 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 7 \\ 0 & 0 & 0 & 0 & 14 \end{pmatrix} \qquad \mathrm{HNF}(C) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}
$$

Unimodular matrix completion

Theorem

Given a primitive matrix $\boldsymbol{A} \in \mathbb{Z}^{k \times n}$, there exists a Las Vegas algorithm that completes $\boldsymbol{A}$ to an $n \times n$ unimodular matrix $\boldsymbol{U}$ such that

$$\|\boldsymbol{U}\| \leq n^{O(1)} \|\boldsymbol{A}\|$$

in an expected number of

$$O(n^{\omega+\varepsilon} \log^{1+\varepsilon} \|\boldsymbol{A}\|)$$

bit operations.

- The standard method: $O((n-k) n^{\omega+\varepsilon} \log^{1+\varepsilon} \|\boldsymbol{A}\|)$.

Conclusion

Given a primitive $\boldsymbol{A} \in \mathbb{Z}^{k\times n}$, consider to complete $\boldsymbol{A}$ to an $(n-s-1)\times n$ matrix with uniformly random integers in $[0, \|\boldsymbol{A}\|)$.

- We present a rigorous proof of the probability for $3 \le s \le n-k-2$.
  - Previously, only the limit probability when $\lambda \to \infty$ is known for $k = 0$.

Conclusion

Given a primitive $\boldsymbol{A} \in \mathbb{Z}^{k\times n}$, consider to complete $\boldsymbol{A}$ to an $(n-s-1)\times n$ matrix with uniformly random integers in $[0, \|\boldsymbol{A}\|)$.

- We present a rigorous proof of the probability for $3 \leq s \leq n-k-2$.
  - Previously, only the limit probability when $\lambda \to \infty$ is known for $k = 0$.
- We propose a fast Las Vegas algorithm for unimodular matrix completion with expected bit-complexity bounded by $\widetilde{O}(n^{\omega} \log \|\boldsymbol{A}\|)$.

Conclusion

Given a primitive $\boldsymbol{A} \in \mathbb{Z}^{k \times n}$, consider to complete $\boldsymbol{A}$ to an $(n-s-1) \times n$ matrix with uniformly random integers in $[0, \|\boldsymbol{A}\|)$.

- We present a rigorous proof of the probability for $3 \leq s \leq n-k-2$.
  - Previously, only the limit probability when $\lambda \to \infty$ is known for $k = 0$.
- We propose a fast Las Vegas algorithm for unimodular matrix completion with expected bit-complexity bounded by $\widetilde{O}(n^{\omega} \log \|\boldsymbol{A}\|)$.

Open problems

- A rigorous proof for $0 \leq s \leq 2$?
- And for $-n-2 < s < -1$?
- Other distributions?

Conclusion

Given a primitive $\boldsymbol{A} \in \mathbb{Z}^{k \times n}$, consider to complete $\boldsymbol{A}$ to an $(n-s-1) \times n$ matrix with uniformly random integers in $[0, \|\boldsymbol{A}\|)$.

- We present a rigorous proof of the probability for $3 \leq s \leq n-k-2$.
  - Previously, only the limit probability when $\lambda \to \infty$ is known for $k = 0$.
- We propose a fast Las Vegas algorithm for unimodular matrix completion with expected bit-complexity bounded by $\widetilde{O}(n^{\omega} \log \|\boldsymbol{A}\|)$.

Open problems

- A rigorous proof for $0 \leq s \leq 2$?
- And for $-n-2 < s < -1$?
- Other distributions ?

THANKS