Solving the inverse Gram problem over commutative matrix $*$-algebras over $\mathbb{Z}$ using lattice methods

Assaf Goldberger

Hadamard 2025, May 27 2025

The inverse Gram Problem over $\mathbb{Z}$

- In the following, let $S \subset \mathbb{C}$ be a subset, and $R \subseteq \mathbb{C}$ be a subring, both closed under complex conjugation.
- The Inverse Gram Problem (IGP) over S, R is the following:

Definition (Inverse Gram Problem)

Given a symmetric, positive semidefinite matrix $M \in M_n(R)$, find a matrix $X \in M_n(S)$ such that

$$XX^* = M.$$

The inverse Gram Problem over $\mathbb{Z}$

- In the following, let $S \subset \mathbb{C}$ be a subset, and $R \subseteq \mathbb{C}$ be a subring, both closed under complex conjugation.
- The Inverse Gram Problem (IGP) over S, R is the following:

Definition (Inverse Gram Problem)

Given a symmetric, positive semidefinite matrix $M \in M_n(R)$, find a matrix $X \in M_n(S)$ such that

$$XX^* = M.$$

Typical instances are:

- $S, R = \mathbb{C}$; (Standard Linear algebra)
- $S, R = \mathbb{Q}$; (Hasse-Minkowski Theorem, Not constructive)
- $S, R = \mathbb{Z}$; (More difficult)
- $S = \{0, \pm 1\}, R = \mathbb{Z}$. (Combinatorial probelms)

Special cases

Some special cases in mathematical research are:

- Hadamard matrices $H(n)$: $S = \{\pm 1\}$, $XX^* = nI$.

Special cases

Some special cases in mathematical research are:

- Hadamard matrices $H(n)$: $S = \{\pm 1\}$, $XX^* = nI$.
- Weighing matrices $W(n, m)$: $S = \{-1, 0, 1\}$, $XX^* = mI$.

Special cases

Some special cases in mathematical research are:

- Hadamard matrices $H(n)$: $S = \{\pm 1\}$, $XX^* = nI$.
- Weighing matrices $W(n, m)$: $S = \{-1, 0, 1\}$, $XX^* = mI$.
- Combinatorial designs, $SBIBD(v, k, \lambda)$: $S = \{0, 1\}$, $XX^\top = (k - \lambda)I + \lambda J$ (J the all 1's matrix).

Special cases

Some special cases in mathematical research are:

- Hadamard matrices $H(n)$: $S = \{\pm 1\}$, $XX^* = nI$.
- Weighing matrices $W(n, m)$: $S = \{-1, 0, 1\}$, $XX^* = mI$.
- Combinatorial designs, $SBIBD(v, k, \lambda)$: $S = \{0, 1\}$, $XX^\top = (k - \lambda)I + \lambda J$ (J the all 1's matrix).
- Difference sets: $S = \{0, 1\}$, $DD^\top = aI + bJ$. (Here D must be of a special structure, such as circulant, or be some other group type matrix).

Structured Inverse Gram Problems

In many papers, people study the equation $XX^* = M$, imposing various structures on X. Examples are:

- Circulant matrices
- Circulant core matrices, one and two core
- Group-Developed matrices
- Cocyclic matrices
- Doubling constructions.
- Legendre Pairs.
- Williamson and Goethhals-Seidel matrices.

Matrix $*$-algebras

All of the structured examples above except Goethhals-Seidel are matrix $*$-algebras.

Definition

An integral matrix $*$-algebra is a subset $\mathcal{A} \subseteq M_n(\mathbb{Z})$ closed under matrix addition, multiplication and transposition.

Matrix $*$-algebras

All of the structured examples above except Goethhals-Seidel are matrix $*$-algebras.

Definition

An integral matrix $*$-algebra is a subset $\mathcal{A} \subseteq M_n(\mathbb{Z})$ closed under matrix addition, multiplication and transposition.

- If $\mathcal{A}$ is an integral matrix $*$-algebra, and F is a field of charactristic 0 stable under complex-conjugation, it is known that $\mathcal{A}_F := \mathcal{A} \otimes F$ is semisimple.

Matrix $*$-algebras

All of the structured examples above except Goethhals-Seidel are matrix $*$-algebras.

Definition

An integral matrix $*$-algebra is a subset $\mathcal{A} \subseteq M_n(\mathbb{Z})$ closed under matrix addition, multiplication and transposition.

- If $\mathcal{A}$ is an integral matrix $*$-algebra, and F is a field of charactristic 0 stable under complex-conjugation, it is known that $\mathcal{A}_F := \mathcal{A} \otimes F$ is semisimple.

In this case, the Artin-Wedderburn theorem states that

$$\mathcal{A}_F \cong \bigoplus_i M_{n_i}(D_i),$$

where D_i are division algebras with center F. The isomorphism respects the $*$

Examples of the Artin-Wedderburn decomposition

Let $\zeta_n := \exp(2\pi i/n)$. Some examples of Artin-Wedderburn are

- The circulant $n \times n$ algebra:

$$\mathcal{A}_{\mathbb{Q}} = \bigoplus_{d|n} \mathbb{Q}(\zeta_d); \qquad \mathcal{A}_{\mathbb{C}} \cong \mathbb{C}^n \text{ (DFT)}.$$

Examples of the Artin-Wedderburn decomposition

Let $\zeta_n := \exp(2\pi i/n)$. Some examples of Artin-Wedderburn are

- The circulant $n \times n$ algebra:

$$\mathcal{A}_{\mathbb{Q}} = \bigoplus_{d|n} \mathbb{Q}(\zeta_d); \qquad \mathcal{A}_{\mathbb{C}} \cong \mathbb{C}^n \text{ (DFT)}.$$

- The dihedral group-algebra $\mathbb{Z}[D_n]$ (n odd):

$$\mathcal{A}_{\mathbb{Q}} \cong \bigoplus_{1<d|n} M_2(\mathbb{Q}(\zeta_d)^+) \oplus \mathbb{Q}^2; \qquad \mathcal{A}_{\mathbb{C}} \cong M_2(\mathbb{C})^{(n-1)/2} \oplus \mathbb{C}^2.$$

Examples of the Artin-Wedderburn decomposition

Let $\zeta_n := \exp(2\pi i/n)$. Some examples of Artin-Wedderburn are

- The circulant $n \times n$ algebra:

$$\mathcal{A}_{\mathbb{Q}} = \bigoplus_{d|n} \mathbb{Q}(\zeta_d); \qquad \mathcal{A}_{\mathbb{C}} \cong \mathbb{C}^n \text{ (DFT)}.$$

- The dihedral group-algebra $\mathbb{Z}[D_n]$ (n odd):

$$\mathcal{A}_{\mathbb{Q}} \cong \bigoplus_{1<d|n} M_2(\mathbb{Q}(\zeta_d)^+) \oplus \mathbb{Q}^2; \qquad \mathcal{A}_{\mathbb{C}} \cong M_2(\mathbb{C})^{(n-1)/2} \oplus \mathbb{C}^2.$$

- The one-circulant-core algebra:

$$\mathcal{A}_{\mathbb{Q}} \cong \bigoplus_{1<d|n} \mathbb{Q}(\zeta_d) \oplus M_2(\mathbb{Q}); \qquad \mathcal{A}_{\mathbb{C}} \cong \mathbb{C}^{n-1} \oplus M_2(\mathbb{C}).$$

Finding solutions over $\mathbb{Z}$

Main objective

Solve the equation $XX^* = M$ over an integral $*$-algebra $\mathcal{A}$.

Finding solutions over $\mathbb{Z}$

Main objective

Solve the equation $XX^* = M$ over an integral $*$-algebra $\mathcal{A}$.

Let $\mathcal{A}_{\mathbb{Q}} = \bigoplus_i \mathcal{A}_{\mathbb{Q},i}$ be the A-W decomposition, and $e_i \in \mathcal{A}_{\mathbb{Q}}$ be the idempotents.

- Solving over $\mathcal{A}_{\mathbb{Q}}$ can be done componentwise. Any choice of solutions $X_i \in \mathcal{A}_{\mathbb{Q},i}$ combine to a solution $X \in \mathcal{A}$.

Finding solutions over $\mathbb{Z}$

Main objective

Solve the equation $XX^* = M$ over an integral $*$-algebra $\mathcal{A}$.

Let $\mathcal{A}_\mathbb{Q} = \bigoplus_i \mathcal{A}_{\mathbb{Q},i}$ be the A-W decomposition, and $e_i \in \mathcal{A}_\mathbb{Q}$ be the idempotents.

- Solving over $\mathcal{A}_\mathbb{Q}$ can be done componentwise. Any choice of solutions $X_i \in \mathcal{A}_{\mathbb{Q},i}$ combine to a solution $X \in \mathcal{A}$.
- This is not true for $\mathcal{A}$. A tuple of solutions $X_i \in e_i\mathcal{A}$, does not usually combine to a solution in $X \in \mathcal{A}$.
- The map

$$\mathcal{A} \to \bigoplus_i e_i\mathcal{A}$$

is injective, but not surjective. Its image is of finite index.

Objectives of this talk

- We will show how to search a commutative integral matrix $*$-algebra in a practical way.
- We will explain how to solve general (=unstructured) gram problems over $\mathbb{Z}$ using the determinant-lattice method, under "generic conditions".
- For commutative $\mathcal{A}$ we will mention the field-descent-method, which suffers from the principal ideal problem.
- We will propose an amalgamation of the previous two methods to give a practical solution (but of worse asymptotic complexity).

Examples of common commutative $*$-algebras

Some examples of common commutative $*$-algebras are:

- Circulant matrices
- Negacyclic matrices
- Commutative group developed matrices
- Commutative Bose-Mesner algebras
- Legendre Pairs (A, B) where both A, B are circulant symmetric

The determinant-lattice method (AG and Y.Strassler)

We outline the lattice reduction method to solve general Gram problems $XX^\top = M$ over $\mathbb{Z}$. There are two main steps:

- Determinant reduction.
- Lattice reduction.

The determinant-lattice method (AG and Y.Strassler)

We outline the lattice reduction method to solve general Gram problems $XX^\top = M$ over $\mathbb{Z}$. There are two main steps:

- Determinant reduction.
- Lattice reduction.

- Determinant reduction reduces to an equation $ZZ^\top = H$, where $\det H = 1$.
- Lattice reduction finds $Z \in M_n(\mathbb{Z})$.

The determinant-lattice method (AG and Y.Strassler)

We outline the lattice reduction method to solve general Gram problems $XX^\top = M$ over $\mathbb{Z}$. There are two main steps:

- Determinant reduction.
- Lattice reduction.

- Determinant reduction reduces to an equation $ZZ^\top = H$, where $\det H = 1$.
- Lattice reduction finds $Z \in M_n(\mathbb{Z})$.

Necessary condition

Need to check that M is positive semidefinite and $\det M$ is a perfect square.

Determinant reduction

Let p be a prime power dividing $\det M$. We go prime by prime.

1. We know that also $p | \det X$. Let's try to guess a vector v with

$$vX \equiv 0 \mod p.$$

Determinant reduction

Let p be a prime power dividing $\det M$. We go prime by prime.

1. We know that also $p | \det X$. Let's try to guess a vector v with
$$vX \equiv 0 \mod p.$$
2. We do not know X, but we know that $vM \equiv 0 \mod p$.

Determinant reduction

Let p be a prime power dividing $\det M$. We go prime by prime.

1. We know that also $p | \det X$. Let's try to guess a vector v with

$$vX \equiv 0 \mod p.$$

2. We do not know X, but we know that $vM \equiv 0 \mod p$.
3. But suppose that $p^2 \nmid \sqrt{\det M}$. 'Generically' we expect that v will be unique (up to a scalar).

Determinant reduction

Let p be a prime power dividing $\det M$. We go prime by prime.

1. We know that also $p | \det X$. Let's try to guess a vector v with

$$vX \equiv 0 \mod p.$$

2. We do not know X, but we know that $vM \equiv 0 \mod p$.
3. But suppose that $p^2 \nmid \sqrt{\det M}$. 'Generically' we expect that v will be unique (up to a scalar).
4. WLOG $v = [1, x_2, \ldots, x_n]$. The matrix

$$P_p = \begin{pmatrix} 1/p & x_2/p & \cdots & x_n/p \\ & 1 & \cdots & 0 \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

Determinat reduction

- Modify $X_1 = P_p X$ and $M_1 = P_p M P_p^\top$.
- We should check that $M_1 \in M_n(\mathbb{Z})$. If yes, we are reduced to

$$X_1 X_1^\top = M_1, \quad \text{with} \quad \det M_1 = \frac{1}{p^2} \det M.$$

- Otherwise, stop or branch (try another v if exists).
- Repeat with $M \leftarrow M_1$ for the next prime. Finish if $\det M = 1$.

Lattice reduction

Definition

A lattice is a free abelian group

$$L = \mathbb{Z}b_1 \oplus \cdots \oplus \mathbb{Z}b_n$$

together with a Euclidean metric $\langle , \rangle$.

- Lattice reduction tries to find a *good basis*.
- There are several notions of good bases, e.g. LLL-reduced, HKZ, and Minkowski.
- In a good basis, the vectors are short and approximately orthogonal.

Lattice reduction

Known algorithms of lattice reduction are

- Approximate algorithms.
  - LLL algorithm. Approximately short vectors, polynomial time in n.
  - BKZ - like LLL, slower but of better quality. polynomial time in n.
- Exact algorithms
  - AKS and Sieving methods: Finding the shortest vectors, hueristic complexity $O(2^{0.3n})$.

Lattice reduction

Known algorithms of lattice reduction are

- Approximate algorithms.
  - LLL algorithm. Approximately short vectors, polynomial time in n.
  - BKZ - like LLL, slower but of better quality. polynomial time in n.
- Exact algorithms
  - AKS and Sieving methods: Finding the shortest vectors, hueristic complexity $O(2^{0.3n})$.

Definition

A lattice L is cubical if it has a basis for which $\langle b_i, b_j \rangle = \delta_{i,j}$. L is called unimodular if the metric is given by $\langle x, y \rangle := xMy^\top$, for PSD $M \in M_n(\mathbb{Z})$ with $\det M = 1$.

Facts on cubic lattices

- If L is cubical, then applying exact lattice reduction reveals the cubical basis.
- The basis transformation matrix X is a solution to $XX^\top = M$.
- The cubical basis is unique up to a permutation and signs.
- Experimental observation: In dimension $n \leq 75$, LLL finds the cubical basis.
- In dimension ≤ 120, BKZ (window size=10) extends this behavior.

Corollary

The solution over $\mathbb{Z}$ to $XX^\top = M$ for unimodular M is unique up to permutations and signs of the columns.

Generic equations

Definition

The equation $XX^\top = M$ is called generic if $\sqrt{\det M}$ is squarefree and the elementary divisors of M are all 1 except for the last one.

Generic equations

Definition

The equation $XX^\top = M$ is called generic if $\sqrt{\det M}$ is squarefree and the elementary divisors of M are all 1 except for the last one.

Theorem (AG and Strassler)

(a) *If $M \in M_n(\mathbb{Z})$ is generic, then the gram equation $XX^\top = M$ has at most one integral solution, up to permutations and signs on the columns of X.*

(b) *There exists an algorithm that outputs a solution X with hueristic complexity $O(2^{0.3n} poly(log||M||))$.*

Generic equations

Definition

The equation $XX^\top = M$ is called generic if $\sqrt{\det M}$ is squarefree and the elementary divisors of M are all 1 except for the last one.

Theorem (AG and Strassler)

(a) *If $M \in M_n(\mathbb{Z})$ is generic, then the gram equation $XX^\top = M$ has at most one integral solution, up to permutations and signs on the columns of X.*

(b) *There exists an algorithm that outputs a solution X with hueristic complexity $O(2^{0.3n} poly(log||M||))$.*

Using LLL or BKZ, generic gram equations are solved in minutes on size ≤ 120, using desktop computers.

Non-generic equations

- The Hadamard problem (and other design problems) is very non-generic.
- Determinant reduction heavily branches for such problems. As a byproduct, there can be many solutions.
- Many branches eventually turn out to be non-cubical when on passing to lattice reduction.
- We will see that on commutative $*$-algebras, branching is greatly reduced.

The Field-Descent Method (B. Schmidt)

- The field-descent method is an algebraic method for solving a Gram equation $XX^* = M$ over integral matrix (or abstract) commutative $*$-algebras.
- The method is outlined as follows:
  - The rational algebra is a product of fields:

$$\mathcal{A}_{\mathbb{Q}} \cong \bigoplus K_i.$$

  - We solve the problem separately over each integer ring $\mathcal{O}_{K_i}$.
  - The solutions combine to a rational solution in $\mathcal{A}_{\mathbb{Q}}$. But all integral solutions are in that list.

Special case: Circulant matrices and cyclotomic fields

- As a special case, let $\mathcal{A}$ be the $*$-algebra of $n \times n$ integral circulant matrices.
- We have

$$\mathcal{A}_{\mathbb{Q}} \cong \bigoplus_{d|n} \mathbb{Q}(\zeta_d).$$

- Need to solve equations $xx^* = m$ in each $\mathbb{Z}[\zeta_d]$. We use algebraic number theory.

Step 1 : Solve for ideals. Write if possible

$$(m) = \prod \mathfrak{M}_i^{e_i} \cdot \mathfrak{M}^{*}{}_i^{e_i}.$$

- Is $\prod \mathfrak{M}_i^{e_i}$ principal?
  - If yes, find a generator (ξ).
  - If no, try another ideal factorization (distributing conugate ideals on both sides).

Circulant matrices -continued

- In $(\xi) = \prod \mathfrak{M}_i^{e_i}$, we have $\xi\xi^* = m \cdot u$; $u \in \mathbb{Z}[\zeta_d]^\times$ is a unit.
- We are reduced to a unit equation $vv^* = u$. Can be solved by computing a unit basis (the Dirichlet unit theorem).

Circulant matrices -continued

- In $(\xi) = \prod \mathfrak{M}_i^{e_i}$, we have $\xi\xi^* = m \cdot u$; $u \in \mathbb{Z}[\zeta_d]^\times$ is a unit.
- We are reduced to a unit equation $vv^* = u$. Can be solved by computing a unit basis (the Dirichlet unit theorem).
- Pros and Cons:
  - Pro: Ideal factorization is easy (modulo integer factorization).
  - Pro: Utilizes algebraic number theory. Many insights.
  - Con: Finding generators for principal ideals is hard.
  - Con: Computing a basis for the units is hard.
  - Con: Most combined solutions over all $\mathbb{Z}[\zeta_d]$ are not integral.
- Solving a Gram equation for $n \approx 100$ is not practical.
- The method generalizes to commutative integral $*$-algebras.

The Lattice Algebraic Descent Method

- We propose a new method, called the lattice algebraic descent method (LAM).
- It is designed to search commutative integral $*$-algebras.
- It is an amalgamation of the field descent method + the lattice-determinant method.
- Treats $\mathcal{A}$ as a whole, not by components.
- Using LLL or BKZ, dimension $n \approx 100$ becomes practical.

Algebraic geometry - Affine schemes

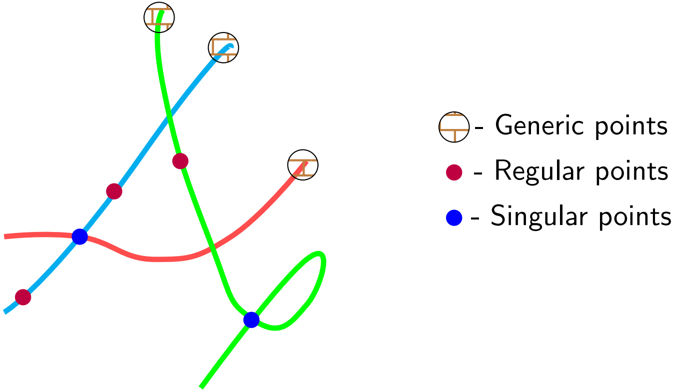
Definition

For a commutative algebra $\mathcal{A}$, let

$$Spec(\mathcal{A}) := \{\text{Prime ideals of } \mathcal{A}\}.$$

- It has a topology (the Zariski topology).
- Has geometric features like:
  - Connected components;
  - Irreducible components;
  - Dimension;
  - Intersections and multiplicity; tangent intersection;
  - Singular and regular points, nodes;

The affine scheme $Spec(\mathcal{A})$



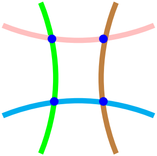
For $\mathcal{A} \otimes \mathbb{Q}$, only generic points remain.

Example: Circulant matrices of order 6

$Spec(\mathcal{C}_6)$

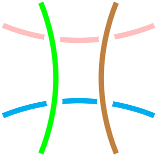
$Spec(\bigoplus_{d|6} \mathbb{Z}[\zeta_d])$

$Spec(\mathbb{Z}[\zeta_6])$



$Spec(\mathbb{Z}[1])$

$Spec(\mathbb{Z}[-1])$ $Spec(\mathbb{Z}[\zeta_3])$



Determinant reduction in ALM

- Consider a Gram equation $XX^* = M$ over a commutative $\mathcal{A}$.
- Let $p|\det(M)$. Then $p|\det(A)$. Since X, X^* commute,

$$\ker(M \mod p) \supseteq \ker(X \mod p) + \ker(X^* \mod p).$$

Hence there is branching

Determinant reduction in ALM

- Consider a Gram equation $XX^* = M$ over a commutative $\mathcal{A}$.
- Let $p|\det(M)$. Then $p|\det(A)$. Since X, X^* commute,

$$\ker(M \bmod p) \supseteq \ker(X \bmod p) + \ker(X^* \bmod p).$$

Hence there is branching

Fortunately, branching is in 1:1 correspondence with ideal factorizations $M\mathcal{A} = I \cdot I^*$.

Theorem (Ideal factorization)

For matrix $*$-algebras, Any ideal $I \triangleleft \mathcal{A}$ factors as

$$I = \prod_{\mathfrak{P}_i \text{ regular}} \mathfrak{P}_i^{e_i} \cdot \prod_{\mathfrak{Q}_i \text{ singular}} \widehat{\mathfrak{Q}_i},$$

where $\widehat{\mathfrak{Q}_i}$ are $\mathfrak{Q}_i$-primary. Morever, both products are stable under the $*$.

Using ideal factorization as a guide

- The primes of $\mathcal{A}$ dividing $M\mathcal{A}$ come in conjugate pairs, or are self-conjugate.
- If $\mathfrak{P}$ is a regular prime ideal dividing M, sitting above p, and assuming $\mathfrak{P}|X$, we can tell what is $\ker(X \bmod p)$:

Using ideal factorization as a guide

- The primes of $\mathcal{A}$ dividing $M\mathcal{A}$ come in conjugate pairs, or are self-conjugate.
- If $\mathfrak{P}$ is a regular prime ideal dividing M, sitting above p, and assuming $\mathfrak{P}|X$, we can tell what is $\ker(X \bmod p)$:
  - Compute a $\mathbb{Z}$-basis for $\mathfrak{P}$.
  - Write all basis element as matrices: $B_1, \dots, B_n$.
  - We have

$$\bigcap_i \ker B_i \subseteq \ker(X \mod p).$$

- Factorizations of $M\mathcal{A}$ are in 1:1 correspondence with branches.

- Factorizations of $M\mathcal{A}$ are in 1:1 correspondence with branches.
- The factorization and primary factors can be computed locally (i.e. in the p-adic completion).

- Factorizations of $M\mathcal{A}$ are in 1:1 correspondence with branches.
- The factorization and primary factors can be computed locally (i.e. in the p-adic completion).
- Given a factorization, it is desirable to work with the full p-primary part before moving on to the next prime.

- Factorizations of $M\mathcal{A}$ are in 1:1 correspondence with branches.
- The factorization and primary factors can be computed locally (i.e. in the p-adic completion).
- Given a factorization, it is desirable to work with the full p-primary part before moving on to the next prime.
- Singular primes and primaries are more difficult to analyze, but are tractible.

- Factorizations of $M\mathcal{A}$ are in 1:1 correspondence with branches.
- The factorization and primary factors can be computed locally (i.e. in the p-adic completion).
- Given a factorization, it is desirable to work with the full p-primary part before moving on to the next prime.
- Singular primes and primaries are more difficult to analyze, but are tractible.
- We conclude with the lattice reduction as usual.

ALM - final comments

- The ALM uses ideal factorization, but determinant reduction kicks us away from $\mathcal{A}$.

ALM - final comments

- The ALM uses ideal factorization, but determinant reduction kicks us away from $\mathcal{A}$.
- Passing from a rational prime p to the next rational prime q requires extra care, since we are no longer in $\mathcal{A}$.

ALM - final comments

- The ALM uses ideal factorization, but determinant reduction kicks us away from $\mathcal{A}$.
- Passing from a rational prime p to the next rational prime q requires extra care, since we are no longer in $\mathcal{A}$.
- The final solution after lattice reduction may not be in $\mathcal{A}$. We still have the freedom to use permutations and signs.

ALM - final comments

- The ALM uses ideal factorization, but determinant reduction kicks us away from $\mathcal{A}$.
- Passing from a rational prime p to the next rational prime q requires extra care, since we are no longer in $\mathcal{A}$.
- The final solution after lattice reduction may not be in $\mathcal{A}$. We still have the freedom to use permutations and signs.
- After permuting and signing, the solution still may not be in $\mathcal{A}$.

ALM - final comments

- The ALM uses ideal factorization, but determinant reduction kicks us away from $\mathcal{A}$.
- Passing from a rational prime p to the next rational prime q requires extra care, since we are no longer in $\mathcal{A}$.
- The final solution after lattice reduction may not be in $\mathcal{A}$. We still have the freedom to use permutations and signs.
- After permuting and signing, the solution still may not be in $\mathcal{A}$.
- In the cases of group-development, or when $\mathcal{A}$ is defined by a symmetry group, the solution will eventually belong to $\mathcal{A}$, provided we chose the branching according to ideals.

QUESTIONS?