Reductions between short vector problems and simultaneous approximation

ANTS 2020

Daniel Martin

July 7, 2020

University of Colorado, Boulder

Lattice problems

Our goal is to reduce the first problem to the second:

Short vector problem (approx-SVP)

For $M \in \mathrm{M}_n(\mathbb{Z})$ and $\alpha \geq 1$, find $\mathbf{q_0} \in \mathbb{Z}^n$ with $0 \neq \|M\mathbf{q}_0\| \leq \alpha \min_{\mathbf{q}}^{\times} \|M\mathbf{q}\|$.

Simultaneous approximation problem

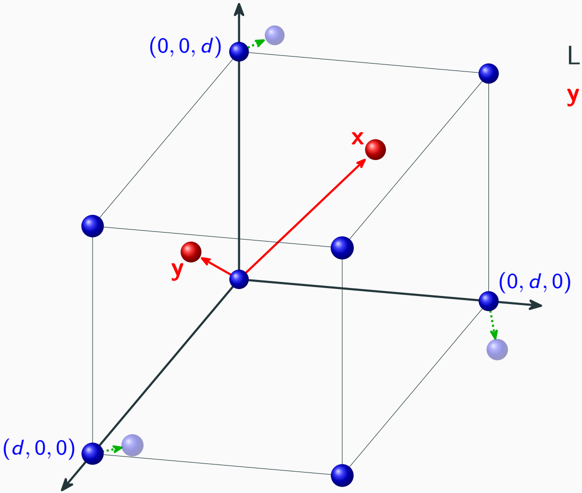
For $\mathbf{x} \in \mathbb{Q}^n$ and $\alpha' \geq 1$, find $q_0 \in \mathbb{Z}$ with $0 \neq \|\{q_0\mathbf{x}\}\| \leq \alpha' \min_q^{\times} \|\{q\mathbf{x}\}\|$.

Alternatively, we could ask that $q_0 \leq \alpha' N$ and $\|\{q_0\mathbf{x}\}\| \leq \alpha' \min_{q \leq N} \|\{q\mathbf{x}\}\|$.

Under a fixed ℓ_p-norm, the reduction is gap-preserving ($\alpha = \alpha'$). It requires $O(n^4 \log mn)$ operations on integers of length $O(n^4 \log mn)$, where m is the maximum input integer magnitude.

The goal

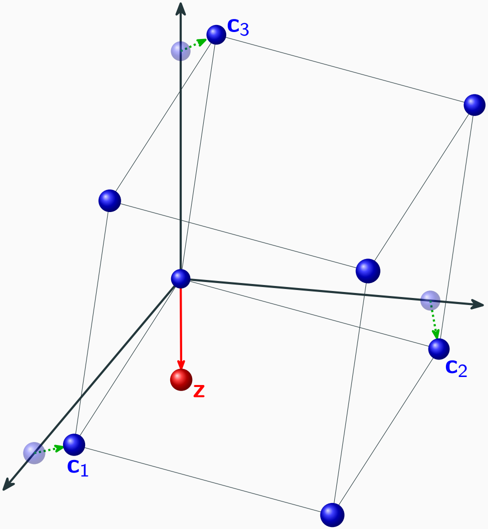
For short vector problems, we typically have lattices of this form:



Lattice generated by $\mathbf{x}$, $\mathbf{y}$, and $d\mathbb{Z}^3$.

The goal

For short vector problems, we typically have lattices of this form:



Lattice generated by $\mathbf{x}$, $\mathbf{y}$, and $d\mathbb{Z}^3$.

Another generating set is $\{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{z}\}$.

Do simultaneous approximation on the vector $[\mathbf{c}_1\,\mathbf{c}_2\,\mathbf{c}_3]^{-1}\mathbf{z}$.

Since $[\mathbf{c}_1\,\mathbf{c}_2\,\mathbf{c}_3]$ is nearly scaled orthonormal, it preserves shortness.

The goal

So the desired setup is

$$\underbrace{\begin{matrix}\text{scaled}\\ \text{orthonormal}\\ \text{sublattice}\end{matrix} + \begin{matrix}\text{small}\\ \text{lattice}\\ \text{vectors}\end{matrix}}_{n \text{ vectors}}, \qquad \begin{matrix}\text{extra}\\ \text{lattice}\\ \text{vector}\end{matrix}.$$

Let M be the input matrix (column vectors). Using a multiple of $\det M\,\mathbb{Z}^n$ as the sublattice, this becomes

$$M(c \operatorname{adj} M) \;+\; MA, \qquad M\mathbf{b},$$

where $A \in \mathrm{M}_n(\mathbb{Z})$, $\mathbf{b} \in \mathbb{Z}^n$, and $c \in \mathbb{Z}$. The goals are

1. the columns of $c \operatorname{adj} M + A$ and $\mathbf{b}$ generate $\mathbb{Z}^n$
2. MA is small relative to $c \det M$ (do 1, then make c bigger)

The goal

For 1, we'll make sure that replacing the last column of $c \operatorname{adj} M + A$ with $\mathbf{b}$ gives a matrix with determinant 1.

By Cramer's rule, we want the last entry in

$$\operatorname{adj}(c \operatorname{adj} M + A)\mathbf{b}$$

to be 1. We can choose A and c so that

$$\operatorname{adj}(c \operatorname{adj} M + A)\mathbf{b} = \begin{bmatrix} * & * & \cdots & * \\ \vdots & \vdots & & \vdots \\ * & * & \cdots & * \\ \color{red}{*} & \color{red}{*} & \cdots & * \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} * \\ * \\ \vdots \\ * \\ \color{red}{1} \end{bmatrix}.$$

coprime

Then b_1 and b_2 can be Bézout coefficients.

Finding A

Suppose we have the following value of $c \operatorname{adj} M$ (here $c = 1$).

$$\begin{bmatrix} 2 & -1 & 1 & -1 \\ \color{red}{4} & \color{red}{1} & \color{red}{5} & -5 \\ \color{red}{4} & \color{red}{1} & \color{red}{-1} & 1 \\ \color{red}{2} & \color{red}{-1} & \color{red}{1} & -7 \end{bmatrix}$$

determinant: -36

$$\begin{bmatrix} \color{red}{2} & \color{red}{-1} & \color{red}{1} & -1 \\ 4 & 1 & 5 & -5 \\ \color{red}{4} & \color{red}{1} & \color{red}{-1} & 1 \\ \color{red}{2} & \color{red}{-1} & \color{red}{1} & -7 \end{bmatrix}$$

determinant: 0

Finding A

Suppose we have the following value of $c \operatorname{adj} M$ (here $c = 1$).

$$\begin{bmatrix} 2 & -1 & 1 & -1 \\ 4 & 1 & 5 & -5 \\ 4 & 1 & -1 & 1 \\ 2 & -1 & 1+x & -7 \end{bmatrix}$$

determinant: $-36 + 0x$

$$\begin{bmatrix} 2 & -1 & 1 & -1 \\ 4 & 1 & 5 & -5 \\ 4 & 1 & -1 & 1 \\ 2 & -1 & 1+x & -7 \end{bmatrix}$$

determinant: $0 + 6x$

Finding A

Suppose we have the following value of $c \operatorname{adj} M$ (here $c = 1$).

$$\begin{bmatrix} 2 & -1 & 1 & -1 \\ \color{red}{4} & \color{red}{1} & 5 & -5 \\ \color{red}{4} & \color{red}{1} & -1 & 1 \\ 2 & -1 & 1+x & -7 \end{bmatrix}$$

determinant: 0

$$\begin{bmatrix} \color{red}{2} & \color{red}{-1} & 1 & -1 \\ 4 & 1 & 5 & -5 \\ \color{red}{4} & \color{red}{1} & -1 & 1 \\ 2 & -1 & 1+x & -7 \end{bmatrix}$$

determinant: 6

Finding A

Suppose we have the following value of $c \operatorname{adj} M$ (here $c = 1$).

$$\begin{bmatrix} 2 & -1 & 1 & -1 \\ \color{red}{4} & \color{red}{1} & 5 & -5 \\ \color{red}{4} & \color{red}{1+y} & -1 & 1 \\ 2 & -1 & 1+x & -7 \end{bmatrix}$$

determinant: $0 + 4y$

$$\begin{bmatrix} \color{red}{2} & \color{red}{-1} & 1 & -1 \\ 4 & 1 & 5 & -5 \\ \color{red}{4} & \color{red}{1+y} & -1 & 1 \\ 2 & -1 & 1+x & -7 \end{bmatrix}$$

determinant: $6 + 2y$

Finding A

Suppose we have the following value of $c \operatorname{adj} M$ (here $c = 1$).

$$\begin{bmatrix} 2 & -1 & 1 & -1 \\ \color{red}{4} & 1 & 5 & -5 \\ 4 & 1+y & -1 & 1 \\ 2 & -1 & 1+x & -7 \end{bmatrix}$$

determinant: 4

$$\begin{bmatrix} \color{red}{2} & -1 & 1 & -1 \\ 4 & 1 & 5 & -5 \\ 4 & 1+y & -1 & 1 \\ 2 & -1 & 1+x & -7 \end{bmatrix}$$

determinant: 2

Finding A

Suppose we have the following value of $c \operatorname{adj} M$ (here $c = 1$).

$$\begin{bmatrix} 2 & -1 & 1 & -1 \\ \color{red}{4+1} & 1 & 5 & -5 \\ 4 & 1+y & -1 & 1 \\ 2 & -1 & 1+x & -7 \end{bmatrix}$$

determinant: 5

$$\begin{bmatrix} \color{red}{2} & -1 & 1 & -1 \\ 4+1 & 1 & 5 & -5 \\ 4 & 1+y & -1 & 1 \\ 2 & -1 & 1+x & -7 \end{bmatrix}$$

determinant: 2

Finding A

Suppose we have the following value of $c \operatorname{adj} M$ (here $c = 1$).

$$\begin{bmatrix} 2 & -1 & 1 & -1 \\ \color{red}{4+1} & \color{red}{1} & 5 & -5 \\ \color{red}{4} & \color{red}{1+y} & -1 & 1 \\ 2 & -1 & 1+x & -7 \end{bmatrix} \qquad \begin{bmatrix} \color{red}{2} & \color{red}{-1} & 1 & -1 \\ 4+1 & 1 & 5 & -5 \\ \color{red}{4} & \color{red}{1+y} & -1 & 1 \\ 2 & -1 & 1+x & -7 \end{bmatrix}$$

determinant: $1 + 5y$ determinant: $6 + 2y$

Finding A

Suppose we have the following value of $c \operatorname{adj} M$ (here $c = 1$).

$$\begin{bmatrix} 2 & -1 & 1 & -1 \\ 4+1 & 1 & 5 & -5 \\ 4 & 1+0 & -1 & 1 \\ 2 & -1 & 1+x & -7 \end{bmatrix}$$

determinant: 1

$$\begin{bmatrix} 2 & -1 & 1 & -1 \\ 4+1 & 1 & 5 & -5 \\ 4 & 1+0 & -1 & 1 \\ 2 & -1 & 1+x & -7 \end{bmatrix}$$

determinant: 6

Finding A

Suppose we have the following value of $c \operatorname{adj} M$ (here $c = 1$).

$$\begin{bmatrix} 2 & -1 & 1 & -1 \\ 4+1 & 1 & 5 & -5 \\ 4 & 1+0 & -1 & 1 \\ 2 & -1 & 1+x & -7 \end{bmatrix}$$

determinant: $-36 + 1x$

$$\begin{bmatrix} 2 & -1 & 1 & -1 \\ 4+1 & 1 & 5 & -5 \\ 4 & 1+0 & -1 & 1 \\ 2 & -1 & 1+x & -7 \end{bmatrix}$$

determinant: $0 + 6x$

Finding A

Suppose we have the following value of $c\,\mathrm{adj}\,M$ (here $c = 1$).

$$\begin{bmatrix} 2 & -1 & 1 & -1 \\ 4+1 & 1 & 5 & -5 \\ 4 & 1+0 & -1 & 1 \\ 2 & -1 & 1+1 & -7 \end{bmatrix} \qquad \begin{bmatrix} 2 & -1 & 1 & -1 \\ 4+1 & 1 & 5 & -5 \\ 4 & 1+0 & -1 & 1 \\ 2 & -1 & 1+1 & -7 \end{bmatrix}$$

determinant: -35

determinant: 6

This gives

$$\mathrm{adj}(c\,\mathrm{adj}\,M + A)\mathbf{b} = \begin{bmatrix} 30 & 0 & 30 & 0 \\ -125 & 30 & 25 & 0 \\ 30 & 36 & -42 & -36 \\ 35 & 6 & -7 & -36 \end{bmatrix} \begin{bmatrix} -1 \\ 6 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} -30 \\ 305 \\ 180 \\ 1 \end{bmatrix}.$$

Changing to simultaneous approximation

The columns of

$$M\operatorname{adj}(c\operatorname{adj}M + A) = \begin{bmatrix} 6 & 0 & 0 & 0 \\ 1 & 6 & 0 & 0 \\ 1 & 0 & 5 & 0 \\ 0 & 0 & -1 & 6 \end{bmatrix} \qquad \text{and} \qquad M\mathbf{b} = \begin{bmatrix} -1 \\ 10 \\ 5 \\ -1 \end{bmatrix}$$

generate the same lattice as the columns of M. The matrix above is roughly scaled orthonormal, so do simultaneous approximation on

$$\begin{bmatrix} 6 & 0 & 0 & 0 \\ 1 & 6 & 0 & 0 \\ 1 & 0 & 5 & 0 \\ 0 & 0 & -1 & 6 \end{bmatrix}^{-1} \begin{bmatrix} -1 \\ 10 \\ 5 \\ -1 \end{bmatrix} = \begin{bmatrix} -1/6 \\ 61/36 \\ 31/30 \\ 1/180 \end{bmatrix}.$$

Avoiding Jacobsthal

For a pair of integers r, s, the previous algorithm finds a small t so that r and $s + t$ are coprime.

The maximum "smallest t" needed as s varies is called *Jacobsthal's function*, $J(r)$. We know

$$J(r) < 2\omega(r)^{2+2e\log\omega(r)} \qquad \text{(Stevens)},$$

$$J(r) \ll (\omega(r)\log\omega(r))^2 \qquad \text{(Iwaniec)},$$

where ω counts distinct prime factors.

These bounds make for difficult worst-case analysis, so leave "c" a variable. Then $r(c)$ and $s(c)$ are polynomials. And if $r(c) \neq 0$ there are at most $\deg r(c)$ integers t for which $r(c)$ and $s(c) + t$ are not coprime over $\mathbb{Q}(c)$.

This is the version presented in the paper.

References

M. Agrawal. Simultaneous Diophantine approximation and short lattice vectors. https://www.youtube.com/watch?v=7SGCXbim6Ug, 2019.

W. Chen and J. Meng. An improved lower bound for approximating Shortest Integer Relation in ℓ_∞-norm. *Information Processing Letters*, 101(4):174–179, 2007.

H. Iwaniec. On the problem of Jacobsthal. *Demonstratio Mathematica*, 11(1):225–232, 1978.

J. Lagarias. The computational complexity of simultaneous Diophantine approximation problems. *SIAM Journal on Computing*, 14(1):196–209, 1985.

H. Stevens. On Jacobsthal's $g(n)$-function. *Mathematische Annalen*, 226(1):95–97, 1977.