Motivation and applications of LLL

HATS lightning talk

April 25, 2020

Lattices

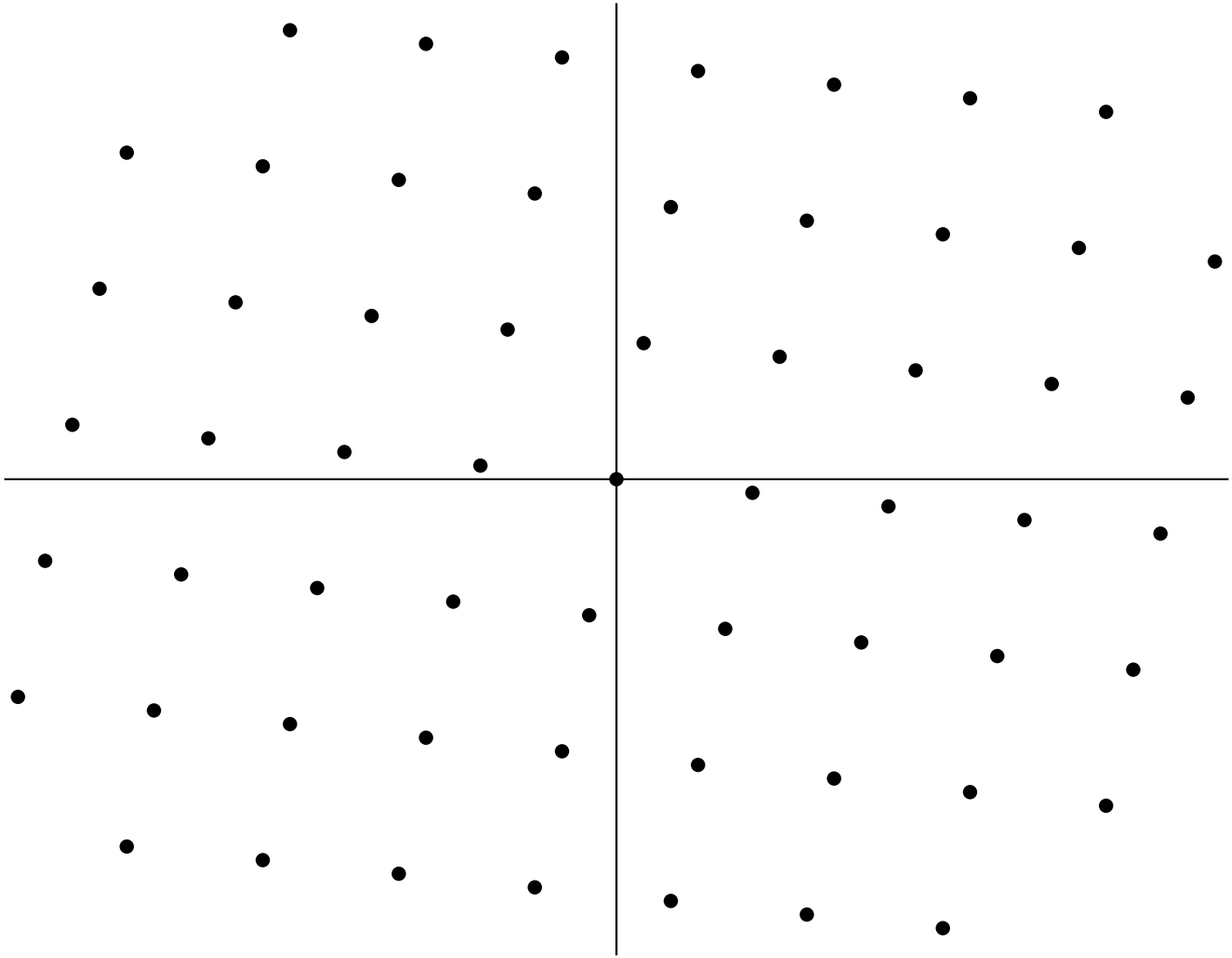
Let $\mathbf{b}_i$ be some vectors, the lattice generated by $\mathbf{b}_i$ is $\sum_i \mathbb{Z}\mathbf{b}_i$, containing elements like

$$1\mathbf{b}_1 + 4\mathbf{b}_2 - 3\mathbf{b}_3$$

$$-\mathbf{b}_2 + 2\mathbf{b}_3$$

$$\mathbf{b}_1$$

Lattice in $\mathbb{R}^2$



Euclidean algorithm

The Euclidean algorithm returns the gcd of a, b

while $b \neq 0$ **do**
  if $|a| > |b|$ **then**
    $a, b \leftarrow b, a$
  end if
  $d \leftarrow \frac{b}{a}$
  $b \leftarrow b - \lfloor d \rceil\, a$
end while
return a

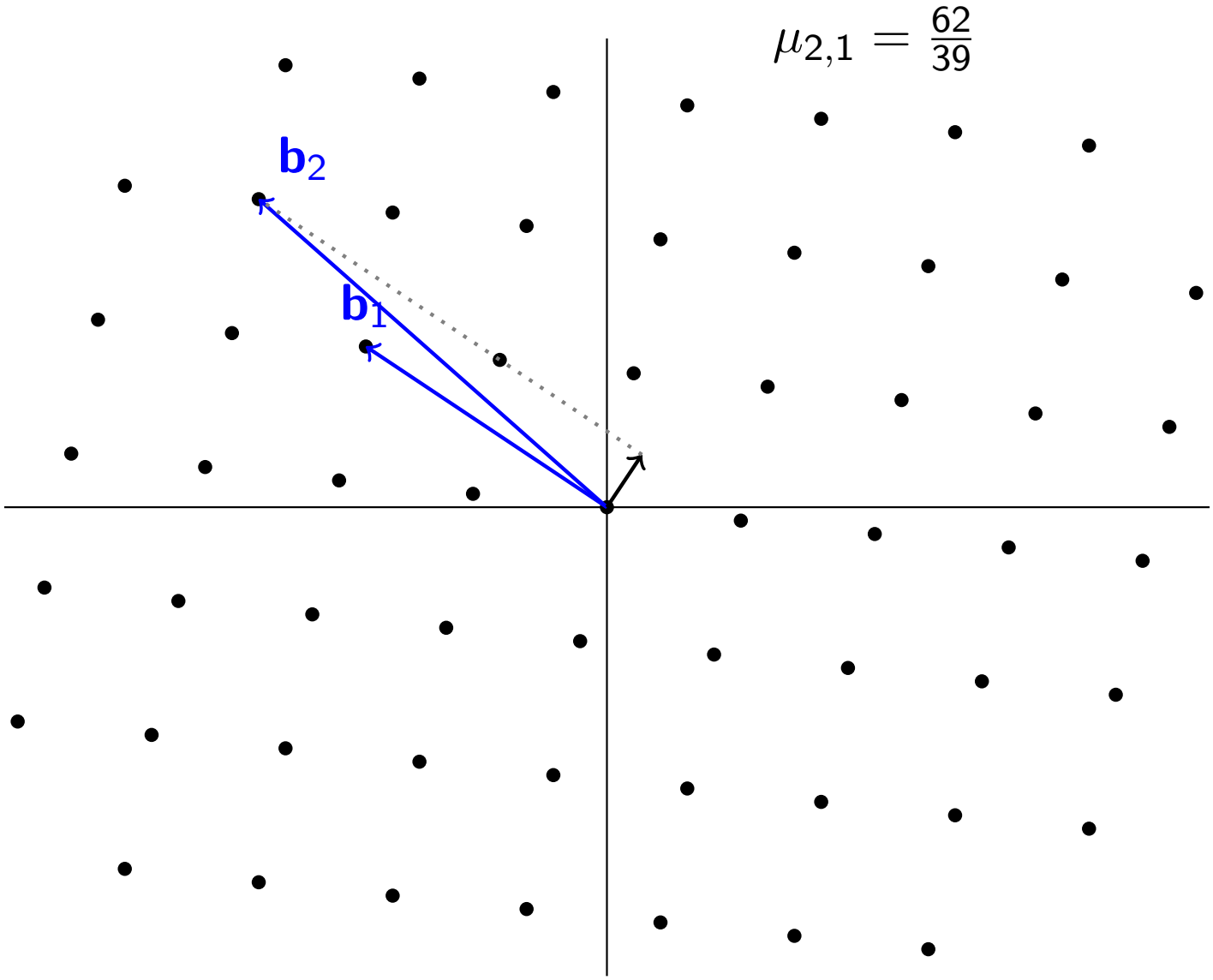
a, b is just a lattice in $\mathbb{R}^1$ and $\gcd(a, b)$ is it's reduced lattice

Gaussian Lattice Reduction

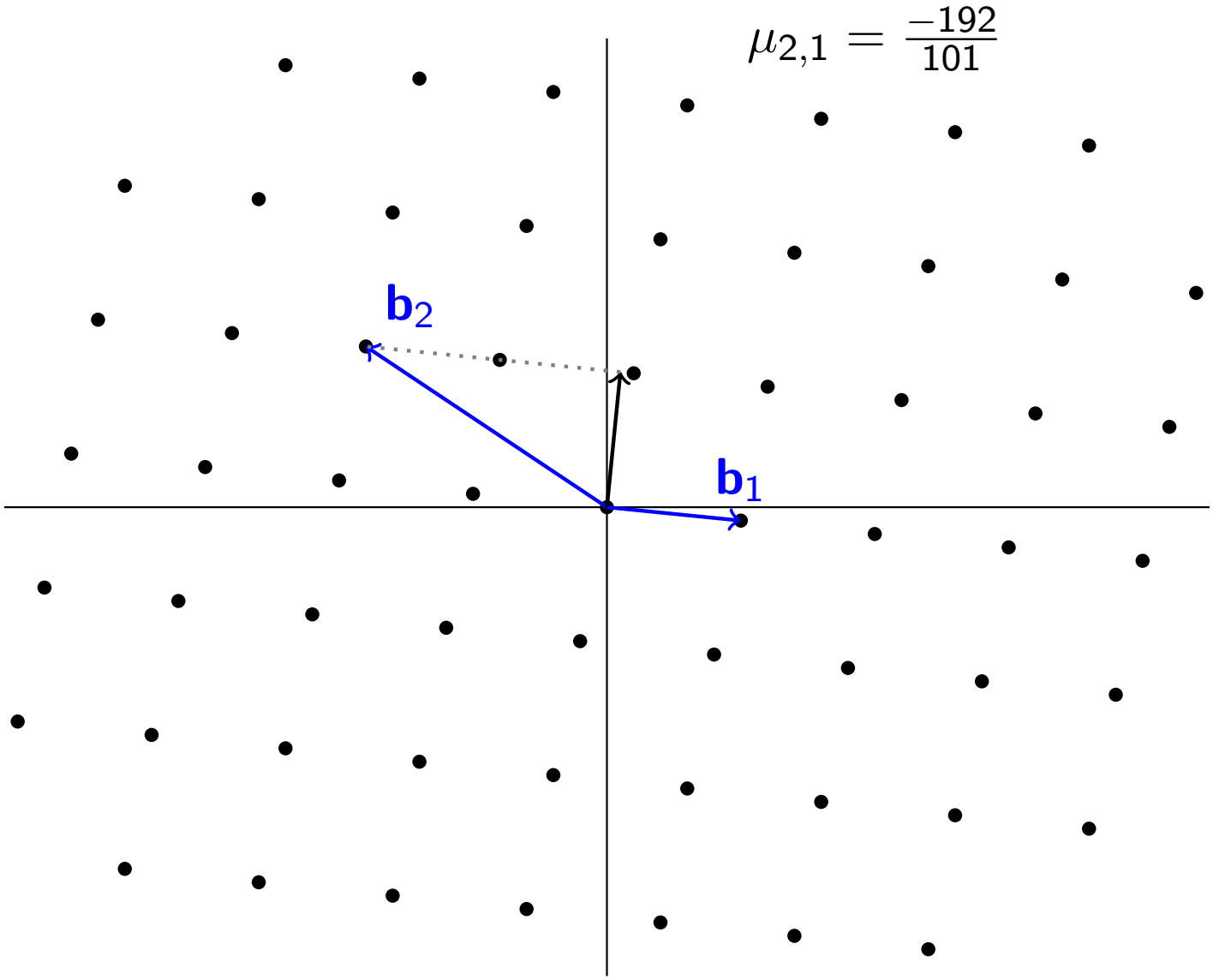
Let $\mathbf{b}_1, \mathbf{b}_2$ be a basis.

while $\lfloor \mu_{2,1} \rceil \neq 0$ **do**
  if $||\mathbf{b}_1|| > ||\mathbf{b}_2||$ **then**
    $\mathbf{b}_1, \mathbf{b}_2 \leftarrow \mathbf{b}_2, \mathbf{b}_1$
  end if
  $\mu_{2,1} \leftarrow \frac{(\mathbf{b}_2, \mathbf{b}_1)}{||b_1||^2}$
  $\mathbf{b}_2 \leftarrow \mathbf{b}_2 - \lfloor \mu_{2,1} \rceil \mathbf{b}_1$
end while
return $\mathbf{b}_1, \mathbf{b}_2$

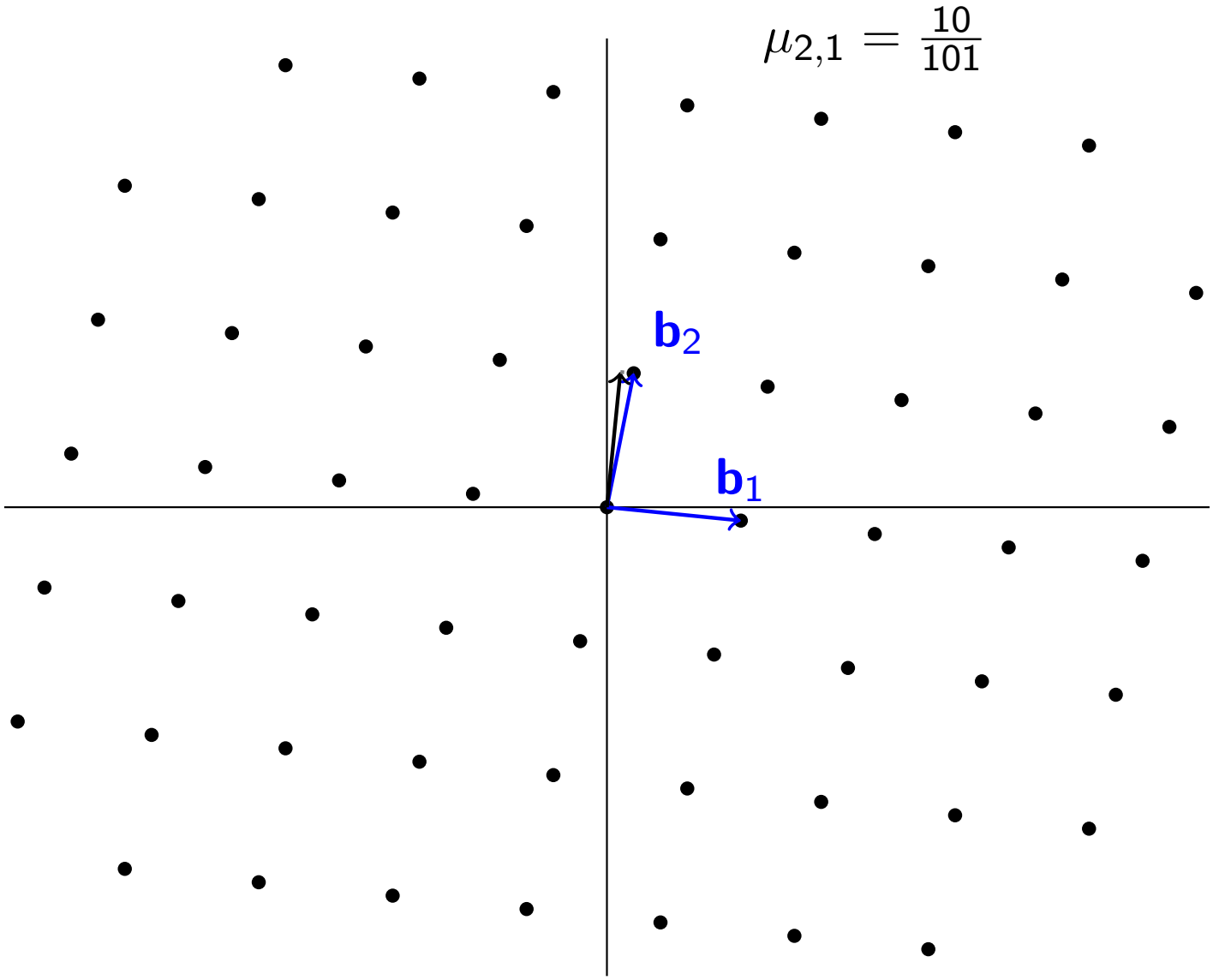
Example



Example



Example



Gram-Schmidt

For some vectors $\mathbf{b}_i \in \mathbb{R}^n$, define the orthogonal vectors $\mathbf{b}_i^*$ as

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \frac{\left(\mathbf{b}_i, \mathbf{b}_j^*\right)}{\left|\left|\mathbf{b}_j^*\right|\right|^2} \mathbf{b}_j^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{j,i} \mathbf{b}_j^*$$

with $\mu_{i,j} = \frac{\left(\mathbf{b}_i, \mathbf{b}_j^*\right)}{\left|\left|\mathbf{b}_j^*\right|\right|^2}$

Then the space generated by b_i and b_i^* are the same. Typically we normalize the vectors but for lattice reduction purposes this is not done.

LLL-reduced

For some basis $\mathbf{b}_i$, let $\mathbf{b}_i^*$ be the Gram-Schmidt orthogonalized basis. Then the basis is LLL-reduced for $\delta \in \left(\frac{1}{4}, 1\right)$ iff:

1. Size reduced: $j < i, \mu_{i,j} \leq \frac{1}{2}$
2. Lovász condition: $\left(\delta - \mu_{i+1,i}^2\right) ||\mathbf{b}_i^*||^2 \leq \left|\left|\mathbf{b}_{i+1}^*\right|\right|^2$

The Lovász condition in some sense is ensuring that the vectors are 'sufficiently' orthogonal. Note that the bound given by these are just theoretical, it is common for these to be overestimations.

LLL algorithm

$i \leftarrow 2$
while $i < n$ **do**
  for $j = i-1, i-2, ..., 1$ **do**
    if $|\mu_{i,j}| > \frac{1}{2}$ **then**
      $\mathbf{b}_i \leftarrow \mathbf{b}_i - \lfloor \mu_{i,j} \rceil \, \mathbf{b}_j$
    end if
  end for
  if $\left(\delta - \mu_{i,i-1}^2\right) \left|\left|\mathbf{b}_{i-1}^*\right|\right|^2 \leq ||\mathbf{b}_i^*||^2$ **then**
    $i \leftarrow i + 1$
  else
    $i \leftarrow \max(i-1, 2)$
    $\mathbf{b}_{i-1}, \mathbf{b}_i \leftarrow \mathbf{b}_i, \mathbf{b}_{i-1}$
  end if
end while

Applications

1. Rational approximation
2. Algebraic number approximation
3. Small roots

Rational approximation

To find a rational approximation of x, let B be a big number.

$$\begin{pmatrix} 1 & 0 & xB \\ 0 & 1 & -B \end{pmatrix}$$

Then the smallest vector of the LLL reduced matrix is of the form (a, b, k) where $0 \approx \frac{k}{B} = a - bx$, hence $x \approx \frac{b}{a}$

Algebraic number approximation

A algebraic number is a root to a polynomial with integer coefficients.
To find a algebraic approximation of x, let B be a big number and n be the degree of a polynomial.

$$\begin{pmatrix} 1 & 0 & \dots & 0 & B \\ 0 & 1 & \dots & 0 & xB \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & x^n B \end{pmatrix}$$

Then the smallest vector of the LLL reduced matrix is of the form $(f_0, f_1, \dots, f_n, k)$ with k small and x is approximately the root of $\sum f_i y^i$

Howgrave Graham

Let $f(x)$ be some univariate polynomial with n monomials. For some modulus M and bound B:
$f(x_0) = 0 \pmod{M}$, $x_0 < B$ and $|f(x)| < M$ for all $0 < x < B$ implies $f(x_0) = 0$ over $\mathbb{Z}$.
$f(x_0) = 0 \pmod{B}$ and $||f(Bx)||_2 < \frac{B}{\sqrt{n}}$ implies $f(x_0) = 0$ over $\mathbb{Z}$.

Coppersmith algorithm

If $x_0 < B$ and $f(x_0) \pmod N = 0$ for some polynomial $f(x) = \sum_{i=0}^{n} f_i x^i$ with $f_n = 1$, then construct the lattice

$$\begin{pmatrix} N & 0 & 0 & \dots & 0 & 0 \\ 0 & NB & 0 & \dots & 0 & 0 \\ 0 & 0 & NB^2 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & NB^{n-1} & 0 \\ f_0 & f_1 B & f_2 B^2 & \dots & f_{n-1} B^{n-1} & f_n B^n \end{pmatrix}$$

If $\mathbf{v}$ is the shortest vector after LLL, then $g(x) = \sum_{i=0}^{n} v_i x^i$ possibly a root $\frac{x_0}{B}$ over the reals.

Motivation and applications of LLL

HATS lightning talk

April 25, 2020