Vector Rational Number Reconstruction

Curtis Bright

August 20, 2009

Modular Arithmetic

- Recall the notion of congruence modulo M: If integers a and b share the same remainder upon division by M, we write

$$a \equiv b \pmod{M}.$$

- The set of integers reduced modulo M may be thought of as the set

$$\mathbb{Z}_M = \{0, 1, 2, \ldots, M-1\}.$$

- We can do computations within $\mathbb{Z}_M$. We can define addition, subtraction, multiplication, and (sometimes) even division.

Modular 'Division'

- The multiplicative inverse of an $r \in \mathbb{Z}_M$, denoted r^{-1}, exists if and only if r and M are coprime (share no common factors).
- Given r, how can we compute r^{-1}? Need to solve for x in:

$$rx \equiv 1 \pmod{M}$$

- The classic *Extended Euclidean Algorithm* can find integers s, t such that:

$$sr + tM = 1$$

- For example, if $r = 17 \in \mathbb{Z}_{25}$:

$$3 \cdot 17 - 2 \cdot 25 = 1$$

$$3 \cdot 17 \equiv 1 \pmod{25}$$

$$3 \equiv 17^{-1} \pmod{25}$$

  So $17^{-1} = 3$ in $\mathbb{Z}_{25}$.

Rational Number *Deconstruction*

- How can we reduce a rational number modulo M?
- Say $a \in \mathbb{Q}$ has the lowest-terms representation $a = \frac{n}{d}$.
- Assuming d and M are coprime, d^{-1} exists and we say that

$$a \equiv n \cdot d^{-1} \pmod{M}.$$

- For example, the rational number $\frac{5}{17}$ reduces to 15 in $\mathbb{Z}_{25}$:

$$\frac{5}{17} \equiv 5 \cdot 17^{-1} \equiv 5 \cdot 3 \equiv 15 \pmod{25}$$

Rational Number Reconstruction

- Can we go the other way? That is, for some given $r \in \mathbb{Z}_M$, can we find an $a = \frac{n}{d} \in \mathbb{Q}$ such that $r \equiv \frac{n}{d} \pmod{M}$?
- One complication: a is not unique...

$$15 \equiv \tfrac{5}{2} \equiv \tfrac{10}{9} \equiv \tfrac{15}{1} \equiv \tfrac{20}{3} \pmod{25}$$

- However, if we restrict $|n|$ and $|d|$ to be relatively small compared to M we can guarantee uniqueness.

Reconstruction Uniqueness

- Say we require solutions to satisfy $|n| \leq N$ and $|d| \leq D$.
- Then if $M > 2ND$ then there is at most one $a \in \mathbb{Q}$ with $a = \frac{n}{d}$ such that

$$\frac{n}{d} \equiv r \pmod{M}$$

for every $r \in \mathbb{Z}_M$.

An Application

- Consider the problem of solving a linear system exactly.
- Given a nonsingular matrix $\boldsymbol{A} \in \mathbb{Z}^{k \times k}$ and a vector $\boldsymbol{b} \in \mathbb{Z}^k$, find the vector $\boldsymbol{x} \in \mathbb{Q}^k$ such that

$$\boldsymbol{A}\boldsymbol{x} = \boldsymbol{b}.$$

- Solving via Gaussian elimination may suffer from coefficient growth.
- Idea: This wouldn't be a problem if we could do all computations modulo M.

Finding $\boldsymbol{x} = \boldsymbol{A}^{-1}\boldsymbol{b}$

- Do Gaussian elimination modulo M to find $\boldsymbol{A}^{-1} \pmod{M}$ and $\boldsymbol{A}^{-1}\boldsymbol{b} \pmod{M}$, then use rational reconstruction to recover $\boldsymbol{x}$.
- Caveat: The denominators of $\boldsymbol{x}$ divide $\det(\boldsymbol{A})$, so we would need M to be coprime with $\det(\boldsymbol{A})$ for $\boldsymbol{x} \pmod{M}$ to exist.
- Can choose N and D (bounds on numerators and denominators of $\boldsymbol{x}$) based on Cramer's rule.
- We need to ensure $M > 2ND$ and M coprime to $\det(\boldsymbol{A})$.
- Note: Actually more efficient to compute $\boldsymbol{A}^{-1} \pmod{p}$ (for some small prime p), and use this to calculate $\boldsymbol{A}^{-1}\boldsymbol{b} \pmod{p^i}$ for some $p^i > 2ND$.

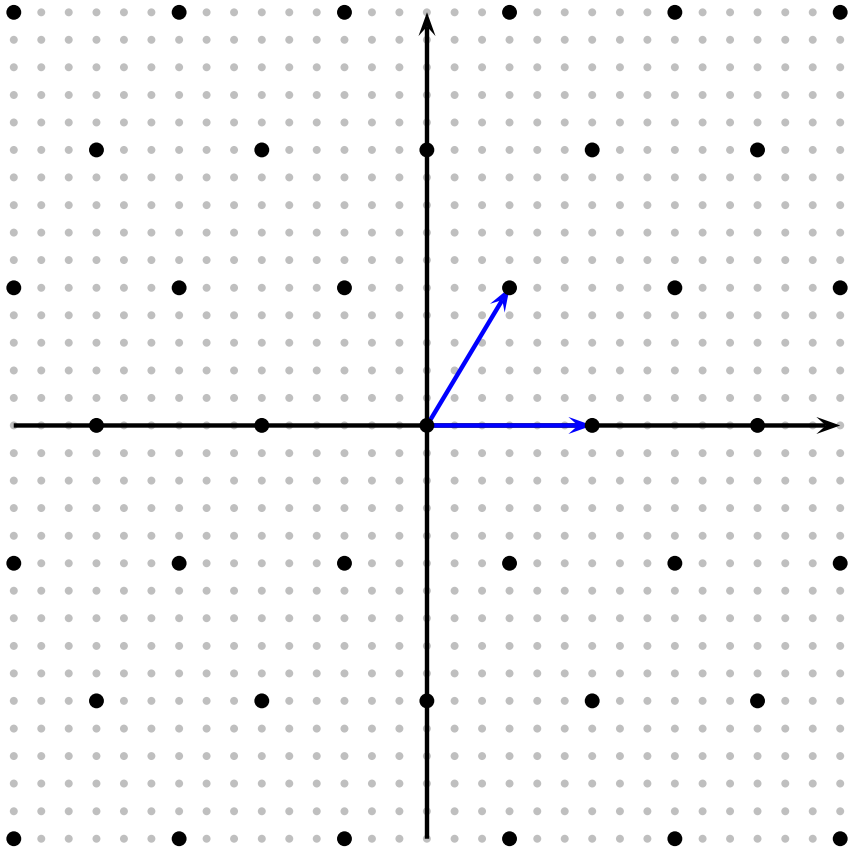
Vector Rational Number Reconstruction

- We could use rational reconstruction on each entry of $\boldsymbol{x}$ (mod M), but this ignores the knowledge of a common denominator.
- Given an integer vector $\boldsymbol{a} \in \mathbb{Z}_M^k$ and a size bound N, the vector rational number reconstruction problem is to solve

$$d\boldsymbol{a} \equiv \boldsymbol{n} \pmod{M}, \qquad \|[\, d \mid \boldsymbol{n}\,]\| \leq N$$

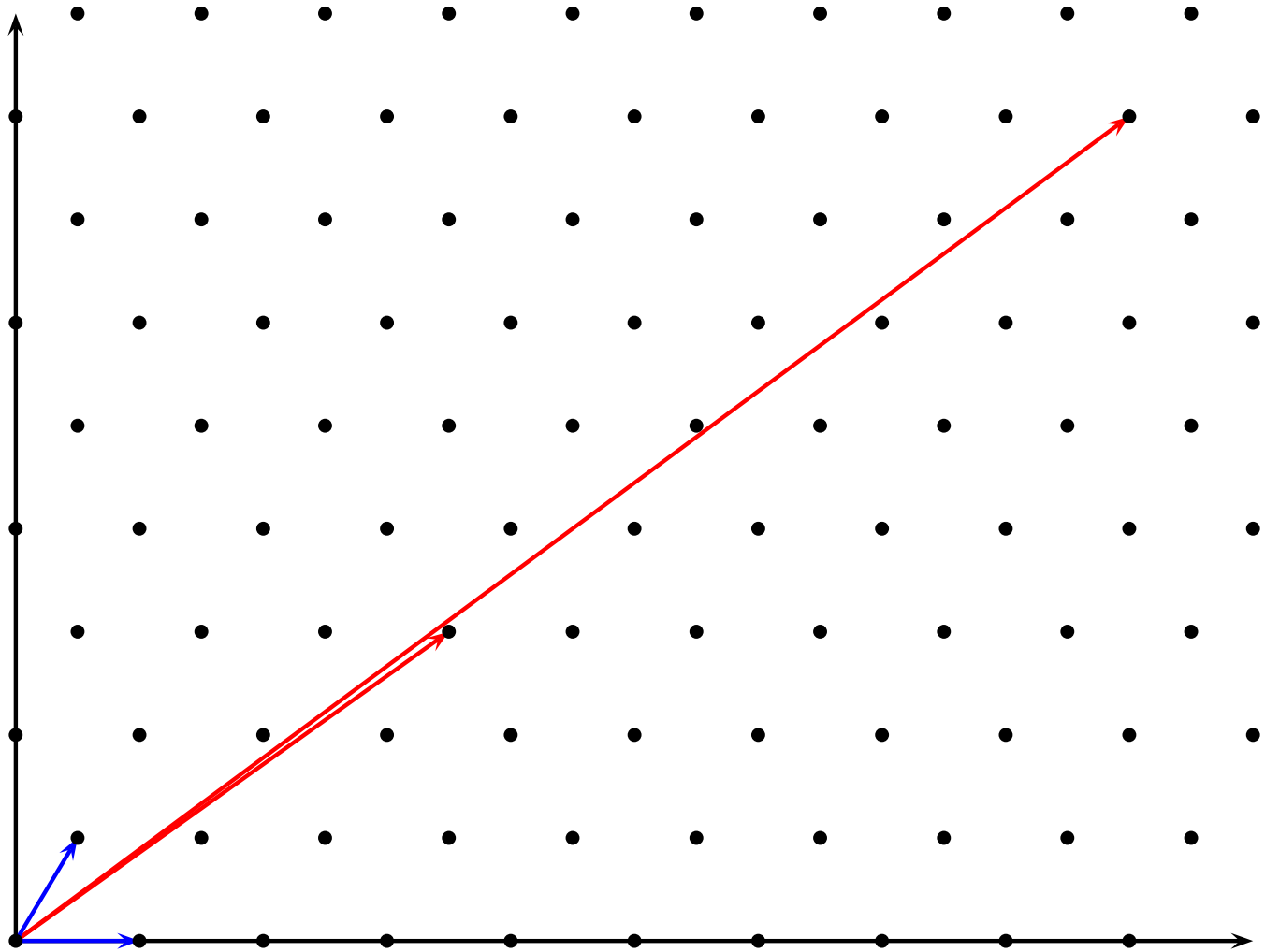
for $\boldsymbol{n} \in \mathbb{Z}^k$ and $d \in \mathbb{Z}$.

Lattices



- This is the lattice generated by $\boldsymbol{b}_1 = \begin{bmatrix} 3 & 5 \end{bmatrix}$ and $\boldsymbol{b}_2 = \begin{bmatrix} 6 & 0 \end{bmatrix}$ in $\mathbb{Z}^2$.
- $\{\boldsymbol{b}_1, \boldsymbol{b}_2\}$ is a *basis* of the lattice.

Good and Bad Bases



Lattice Basis Reduction

- *Lattice reduction* is the process of finding 'good' bases for lattices.
- That is: bases with short and approximately orthogonal basis vectors.
- The *LLL Algorithm* (1982) finds reasonably good bases in polynomial time in the lattice dimension.

Using Lattices for Rational Reconstruction

- Consider the lattice generated by the rows of the matrix

$$\begin{bmatrix} 0 & M \\ 1 & x \end{bmatrix}.$$

- If $\begin{bmatrix} d & n \end{bmatrix}$ is an arbitrary element of this lattice, then

$$dx \equiv n \pmod{M}.$$

- If d is coprime to M then $\frac{n}{d}$ is a rational reconstruction of x.
- If n and d are sufficiently small then this is the *unique* short reconstruction.

- Similarly, consider the lattice generated by the rows of the matrix

$$\begin{bmatrix} & & & & M \\ & & & \iddots & \\ & & M & & \\ & M & & & \\ 1 & x_1 & x_2 & \cdots & x_k \end{bmatrix}.$$

- Every element of this lattice $\left[\, d \mid n_1 \mid n_2 \mid \cdots \mid n_k \,\right]$ satisfies

$$d\boldsymbol{x} \equiv \boldsymbol{n} \pmod{M}.$$

- Finding a short vector in this lattice solves the vector rational reconstruction problem.

Conclusion

- We can run the LLL Algorithm on this lattice to find a short vector, but this is much too expensive.
- The full lattice has dimension $k+1$, but because of its special form it is possible to run LLL on sublattices of dimension $c+1$ instead (for c a small constant).
- For linear system solving with $M = p^i$ (i.e., i lifting steps),
  - Usual elementwise reconstruction requires $i \approx 2 \log N$.
  - The lattice technique requires $i \approx (1 + \frac{1}{c}) \log N$.