Vector Rational Number Reconstruction

Curtis Bright
(joint work with Arne Storjohann)

University of Waterloo

June 9, 2011

Rational Number Reconstruction

- Given an integer residue $r \pmod{M}$, find a rational number a/b such that $r \equiv a/b \pmod{M}$.
- Would like the solution a/b to be unique, so we require the solution pair (a, b) be small:

$$|a| \leq T, \quad 0 < b \leq T$$

  for a given bound T.
- If $M > 2T^2$ then the solution (if any) is unique.

Example

- The reconstruction of $-106641 \pmod{2000003}$ with target bound $T = 1000$:

$$-106641 \equiv \frac{-995}{994} \pmod{2000003}.$$

Motivation

- Consider the problem of linear system solving:

$$\begin{bmatrix} -97 & -69 & 2 \\ -38 & 69 & -88 \\ -36 & -15 & 99 \end{bmatrix} \boldsymbol{x} = \begin{bmatrix} -86 \\ 50 \\ -94 \end{bmatrix} \implies \boldsymbol{x} = \begin{bmatrix} \frac{691692}{1006629} \\ \frac{263002}{1006629} \\ \frac{-664416}{1006629} \end{bmatrix}.$$

- Using Hensel lifting, we compute

$$\boldsymbol{x} \equiv \begin{bmatrix} 8835469671548 \\ 3425840105938 \\ 1711762724896 \end{bmatrix} \pmod{10^{13}},$$

and then find $\boldsymbol{x}$ using *entrywise* rational number reconstruction.

- Goal: perform less lifting, e.g.,

$$\boldsymbol{x} \equiv \begin{bmatrix} 469671548 \\ 840105938 \\ 762724896 \end{bmatrix} \pmod{10^{9}},$$

and then find $\boldsymbol{x}$ using *vector* rational number reconstruction.

Rational Number Reconstruction: The Vector Version

- Given a vector $\boldsymbol{r} \in \mathbb{Z}^n$ of images modulo M and a target length T, find a vector $\boldsymbol{a}/b \in \mathbb{Q}^n$ such that

$$\boldsymbol{r} \equiv \boldsymbol{a}/b \pmod{M}, \quad 0 < \left\| \left[\, b \,\middle|\, \boldsymbol{a} \,\right] \right\|_2 \leq T.$$

- As in the scalar case, $M > 2T^2$ implies solution uniqueness, but often we still have uniqueness for smaller M.

Example

- Find a vector of size at most $T = 1000$ which gives a reconstruction of

$$\left[\; -11431 \quad 5719 \quad -16455 \;\right] \bmod 40009.$$

- Unique solution: $\left[\; 33/231 \quad 792/231 \quad -250/231 \;\right]$, even though $M < 2T^2$.
- The length of $\left[\; 231 \;\middle|\; 33 \quad 792 \quad -250 \;\right]$ is shorter than T.

The Obvious Approach

- Use scalar rational number reconstruction on each of the n coordinates.
- In general this requires $M > 2T^2$, even if in fact uniqueness holds for smaller M.

Example

- In an attempt to reconstruct $\begin{bmatrix} -11431 & 5719 & -16455 \end{bmatrix}$, Maple's `iratrecon` finds the following:

$$\begin{aligned} -11431 &\equiv 1/7 &&\equiv 124/868 &&\pmod{40009} \\ 5719 &\equiv 24/7 &&\equiv 2976/868 &&\pmod{40009} \\ -16455 &\equiv 39/124 &&\equiv 273/868 &&\pmod{40009} \end{aligned}$$

- The length of $\left[\begin{array}{c|ccc} 868 & 124 & 2976 & 273 \end{array}\right]$ is larger than our target length of $T = 1000$.

The Lattice Approach

- Find vectors with length shorter than T in the lattice $\mathcal{L}$ generated by the rows of the matrix

$$\boldsymbol{L} = \begin{bmatrix} & & & M \\ & & \iddots & \\ & M & & \\ 1 & r_1 & \cdots & r_n \end{bmatrix} \in \mathbb{Z}^{(n+1)\times(n+1)}.$$

- Short vectors in $\mathcal{L}$ have the general form $\left[\, b \,\middle|\, b\boldsymbol{r} \bmod M \,\right]$, and note that $\boldsymbol{a} = b\boldsymbol{r} \bmod M$.

Example

- From our previous example, $\mathcal{L}$ would be generated by

$$\boldsymbol{L} = \begin{bmatrix} & & & 40009 \\ & & 40009 & \\ & 40009 & & \\ 1 & -11431 & 5719 & -16455 \end{bmatrix}.$$

Continued Example

- The LLL lattice basis reduction algorithm can be used to find short vectors in lattices.

$$\mathrm{LLL}(\boldsymbol{L}) = \begin{bmatrix} 231 & 33 & 792 & -250 \\ 175 & 25 & 600 & 1023 \\ 4610 & -5057 & -1341 & -486 \\ -5974 & -6569 & 2380 & 57 \end{bmatrix}$$

- However, when n is large the LLL algorithm is much too costly to run, and its ability to find short vectors is hindered.

Gradual Sublattice Reduction

- Work on the basis $\boldsymbol{L}$ *gradually*, by iteratively reducing bases of truncated sublattices of $\mathcal{L}$.
- References:
  - A. Novocin, PhD Thesis, 2008
  - M. van Hoeij, A. Novocin, LATIN 2010

Example: Gradual Sublattice Reduction

- LLL-reduce the lower-left 2×2 submatrix of $\boldsymbol{L}$:

$$\begin{bmatrix} 0 & 40009 \\ 1 & -11431 \end{bmatrix} \xrightarrow{\text{LLL}} \begin{bmatrix} -7 & -1 \\ 802 & -5601 \end{bmatrix}.$$

  Now, any vector which includes the last row must be longer than T, so the last row is discarded.

- Add a column and row and LLL-reduce:

$$\begin{bmatrix} 0 & 0 & 40009 \\ -7 & -1 & -40033 \end{bmatrix} \xrightarrow{\text{LLL}} \begin{bmatrix} -7 & -1 & -24 \\ -10738 & -1534 & 3193 \end{bmatrix}$$

  Once again, the last row may be discarded.

- Add a column and row and LLL-reduce:

$$\begin{bmatrix} 0 & 0 & 0 & 40009 \\ -7 & -1 & -24 & 115185 \end{bmatrix} \xrightarrow{\text{LLL}} \begin{bmatrix} -231 & -33 & -792 & 250 \\ 175 & 25 & 600 & 1023 \end{bmatrix}$$

  Once again, the last row may be discarded.

A Gradual Sublattice Reduction Invariant

- Let c be a small integer constant such that

$$M > 2^{(c+1)/2} T^{1+1/c}.$$

- For example, with $c = 5$ we require $M > 8T^{6/5}$.
- The gradual sublattice reduction procedure just described never has to reduce lattices of row dimension more than $c + 1$.

Basic Cost Analysis

- The algorithm just demonstrated requires $O(n^2 (\log M)^3)$ bit operations, but both of these factors can be improved upon.

Optimization 1

- Problem: As the gradual sublattice reduction proceeds, the column dimension of the work bases increases up to n.

$$\begin{bmatrix} 518 & 74 & 1776 & -1773 & -4186 & 210 & -3285 \\ 119 & 17 & 408 & 2296 & 1201 & -10765 & -214 \\ -994 & -142 & -3408 & -7411 & -618 & 2841 & 4141 \end{bmatrix}$$

- Only store the first column. All short vectors in the lattice have the form $\left[\, b \,\middle|\, b\boldsymbol{r} \bmod M \,\right]$.
- Reconstruct the entries at the conclusion of the algorithm, for example:

$$518 \cdot r_1 = -5921258 \equiv 74 \pmod{M}.$$

- The running of LLL only requires the quantities in the Gramian matrix $\boldsymbol{L}\boldsymbol{L}^{\mathrm{T}}$, not the vector entries themselves.

Optimization 2

- The running time of LLL variants with respect to the bitlength of the vector entries has been improved in recent years.
- References:
  - P. Q. Nguyen, D. Stehlé, SIAM Journal on Computing 2009.
  - I. Morel, D. Stehlé, G. Villard, ISSAC 2009.
  - A. Novocin, D. Stehlé, G. Villard, STOC 2011.
- We employ the L^2 algorithm to achieve a $O(n(\log M)^2)$ bit operation cost.

Conclusion: Scalar vs. Vector Reconstruction

- Using p-adic lifting, we reconstruct the solution $\boldsymbol{x}$ from its image $\boldsymbol{x} \bmod M$, where $M = p^k$ for large enough k.
- Let T be the maximum of the magnitudes of the denominator and numerators of $\boldsymbol{x}$.

$$\begin{array}{ll} \text{scalar reconstruction requires:} & M \in \Omega(T^2) \\ \text{vector reconstruction requires:} & M \in \Omega((\sqrt{n}T)^{1+1/c}) \end{array}$$

- The number of bits in M required to solve n dimensional linear systems with ± 1 entries:

n	Scalar RatRecon	VecRecon $c = 5$
200	1061	642
400	2398	1444
800	5349	3215
1600	11806	7090