Computer Algebra
Lecture 7

James Davenport

University of Bath

11 September 2018

Diagrammatic illustration

Figure: Diagrammatic illustration of Many Small Prime gcd Algorithm

$$\begin{array}{ccc} \mathbf{Z}[x] & \overset{\text{gcd}}{\dashrightarrow} & \mathbf{Z}[x] \\ k\times\text{reduce}\downarrow & & \uparrow\text{interpret \& check} \\ \left.\begin{array}{ccc}\mathbf{Z}_{p_1}[x] & \xrightarrow{\text{gcd}} & \mathbf{Z}_{p_1}[x]\\ \vdots&\vdots&\vdots\\ \mathbf{Z}_{p_k}[x] & \xrightarrow{\text{gcd}} & \mathbf{Z}_{p_k}[x]\end{array}\right\} & \xrightarrow{\text{C.R.T.}} & \mathbf{Z}'_{p_1\cdots p_k}[x]\end{array}$$

$\mathbf{Z}'_{p_1\cdots p_k}[x]$ indicates that some of the p_i may have been rejected by the compatibility checks, so the product is over a subset of $p_1\cdots p_k$.

More generally

gcd could be almost any algorithm that works over the integers. But we always have these questions.

1. Are there "good" reductions from R?
2. How can we tell if R_i is good?
3. How many reductions should we take?
4. How do we combine?
5. How do we check the result?

For this gcd the answers are

1. Are there "good" reductions from R?

A All except (a) those that divide both leading coefficients; (b) those that divide a certain resultant

2. How can we tell if R_i is good?

A Type (a) immediately, Type (b) we can't — but given two different answers we know which is wrong

3. How many reductions should we take?

A The answer is given by the Landau–Mignotte Bounds, but these are often too pessimistic.

4. How do we combine?

A Chinese Remainder Theorem

5. How do we check the result?

A Lemma implies that, if G divides both, it *is* the g.c.d.

Another Application: linear equations over $\mathbf{Q}$

One problem is that, even if we have linear equations over $\mathbf{Z}$, unless the determinant is 1, the answers will be over $\mathbf{Q}$ rather than $\mathbf{Z}$. When we were looking for a g.c.d. with coefficients c: $|c| < M$, we needed $\prod p_i < 2M$. What happens over $\mathbf{Q}$?

procedure $\textsc{Farey}(y, N \in \mathbf{N})$

Output $n, d \in \mathbf{Z}$ such that $|n|, |d| < \sqrt{N/2}$ and $n/d \equiv y \pmod{N}$, or `failed` if none such exist.

$i := 1$; $a_0 := N$; $a_1 := y$; $a := 1$; $d := 1$; $b := c := 0$

▷ Loop invariant: $a_i = ay + bN$; $a_{i-1} = cy + dN$;

while $a_i > \sqrt{N/2}$ **do**

$a_{i+1} = \mathrm{rem}(a_{i-1}, a_i)$;

q_i :=the corresponding quotient: ▷ $a_{i+1} = a_{i-1} - q_i a_i$

$e := c - q_i a$; $e' := d - q_i b$; ▷ $a_{i+1} = ef + e'g$

$i := i + 1$;

$(c, d) = (a, b)$;

$(a, b) = (e, e')$

end while

if $|a| < \sqrt{N/2}$ and $\gcd(a, N) = 1$ **then return** (a_i, a)

else return `failed`

end if

end procedure

Comments

This is essentially the Euclidean algorithm on y, N; tracking the dependencies.

Correctness of this algorithm, i.e. the fact that the first $a_i < \sqrt{N/2}$ corresponds to the solution if it exists, is proved in [WGD82], using [HW79, Theorem 184].

The condition $\gcd(a, N) = 1$ was stressed by [CE95], without which we may return meaningless results, such as $(-2, 2)$, when trying to reconstruct $5 \pmod{12}$.

It is possible (not well written up!) to handle the case of reconstructing $\frac{c}{d}$ where $|c| < C$, $|d| < D$ (i.e. different bounds), as long as $N > 2CD$.

How big is the determinant $|M|$ of an $n \times n$ matrix M?

Notation

If $\mathbf{v}$ is a vector, then $||\mathbf{v}||_2$ (sometimes also written $|v|$) denotes the Euclidean norm *of $\mathbf{v}$, $\sqrt{\sum |v_i^2|}$.*

Proposition

If M is an $n \times n$ matrix with entries $\leq B$, $|M| \leq n!B^n$.

This is true because the determinant is the sum of $n!$ summands, each the product of n elements, therefore bounded by B^n.
This bound is frequently used, but we can do better.

Proposition

[Hadamard bound H_r] If M is an $n \times n$ matrix whose rows are the vectors $\mathbf{v}_i$, then $|M| \leq H_r = \prod ||\mathbf{v}_i||_2$, which in turn is $\leq n^{n/2}B^n$.

Much better if some rows are much larger than others.

There's also a column variant

Proposition

[Hadamard bound H_r] If M is an $n \times n$ matrix whose columns are the vectors $\mathbf{v}_i$, then $|M| \leq H_r = \prod ||\mathbf{v}_i||_2$, which in turn is $\leq n^{n/2} B^n$.

Much better if some columns are much larger than others.

Application to Linear Equations

Suppose we have $M.\mathbf{x} = \mathbf{a}$ (and assume $|M| \neq 0$). Then $x_i = \frac{D_i}{D}$ where $D = |M|$ and D_i is the determinant of the matrix replacing the i-th column of M by $\mathbf{a}$.
Hence we can choose lots of small primes and solve the linear equations (discarding those where the determinant is zero).
Choose a bound (probably using column version if $\mathbf{a}$ is bigger than M), and reconstruct.

Hence the questions

1. Are there "good" reductions from R?

A Yes, all primes with $|M| \neq 0 \pmod{p}$

2. How can we tell if R_i is good?

A $|M| \neq 0 \pmod{p}$, i.e. fairly upfront. Certainly before we reconstruct.

3. How many reductions should we take?

A given by the bounds

4. How do we combine?

A Farey reconstruction after C.R.T.

5. How do we check the result?

A We don't need to: all primes are good (as long as $|M| \neq 0 \pmod{p}$)

Are the bounds too great?

They certainly can be.
But [AM01] shows that, for random $n \times n$ matrices, $-\log_e(|M|/H) \approx \frac{n}{2}$, so the number of "wasted bits" $\approx \frac{3n}{4}$ *on average*.
What about early termination?

- Note that it's early termination by constancy of $\frac{p}{q}$ that matters: the integer will change!
- If we are reconstructing the whole of $\mathbf{x}$, then we can check the result. But this is a much bigger win when we are only reconstructing a few x_i, and then we have no check.

Diagrammatic illustration (2)

f is some finite algorithm of $+$, $-$, $*$, $/$ (and therefore tests for division by zero), producing a single result

Figure: Diagrammatic illustration of Many Small Prime f Algorithm

$$
\begin{array}{lcccc}
\mathbf{Z}[x] & \multicolumn{3}{c}{\overset{f_{\mathbf{Z}}}{\dashrightarrow}} & \mathbf{Z}[x] \\
k\times\text{reduce}\downarrow & & & & \begin{array}{c}\text{interpret} \\ \uparrow\text{\& check}\end{array} \\
\left.\begin{array}{ccc}
\mathbf{Z}_{p_1}[x] & \xrightarrow{f_{p_1}} & \mathbf{Z}_{p_1}[x] \\
\vdots & \vdots & \vdots \\
\mathbf{Z}_{p_k}[x] & \xrightarrow{f_{p_k}} & \mathbf{Z}_{p_k}[x]
\end{array}\right\} & & \xrightarrow{\text{C.R.T.}} & & \mathbf{Z}'_{p_1\cdots p_k}[x]
\end{array}
$$

$\mathbf{Z}'_{p_1\cdots p_k}[x]$ indicates that some of the p_i may have been rejected by the compatibility checks, so the product is over a subset of $p_1 \cdots p_k$.

Hence the questions

1. Are there "good" reductions from R?

A Yes. On a given input, f tests a finite set $z_1, \ldots, z_N$ for being zero. Therefore, any prime not dividing $\prod z_i$ is good.

N.B. Some primes dividing a z_i might still be good.

2. How can we tell if R_i is good?

A Good question.

3. How many reductions should we take?

A Good question.

4. How do we combine?

A C.R.T., possibly with Farey reconstruction.

5. How do we check the result?

A Good question.

Some primes dividing a z_i might still be good

Consider our g.c.d. example

$\mathbf{Z}$	(mod 5)
$x^8+x^6-3x^4-3x^3+8x^2+2x-5$	$x^8+x^6+2x^4+2x^3+3x^2+2x$
$3x^6+5x^4-4x^2-9x+21$	$3x^6+x^2+x+1$
$-15x^4+3x^2-9$	
$15795x^2+30375x-59535$	$4x^2+3$
$1254542875143750x$ -1654608338437500	x
$12593338[\ldots]7500$	3

The mod 5 calculation takes a different route but ends up with the "right" answer: constant.

So what about Gröbner bases [Arn03, IPS11]

1. Are there "good" reductions from R?

A Yes, by the "finite tests" rule

2. How can we tell if R_i is good?

A Good question. We can look at $\{\mathrm{lm}(g_i)\}$ for compatibility. But we don't have an equivalent of "larger degree is bad" rule from g.c.d.

3. How many reductions should we take?

A No useful bounds. Just wait for the answer (over $\mathbf{Q}$) to stabilise.

4. How do we combine?

A C.R.T. with Farey reconstruction to get a monic Gröbner base over $\mathbf{Q}$.

5. How do we check the result?

A Good question.

Bibliography I

J.A. Abbott and T. Mulders.
How Tight is Hadamard's Bound?
Experimental Math., 10:331–336, 2001.

E.A. Arnold.
Modular algorithms for computing Gröbner bases.
J. Symbolic Comp., 35:403–419, 2003.

G.E. Collins and M.J. Encarnación.
Efficient rational number reconstruction.
J. Symbolic Comp., 20:287–297, 1995.

G.H. Hardy and E.M. Wright.
An Introduction to the Theory of Numbers (5th. ed.).
Clarendon Press, 1979.

I. Idrees, G. Pfister, and S. Steidel.
Parallelization of Modular Algorithms.
J. Symbolic Comp., 46:672–684, 2011.

P.S. Wang, M.J.T. Guy, and J.H. Davenport.
p-adic Reconstruction of Rational Numbers.
SIGSAM Bulletin, 16(2):2–3, 1982.