Jet list decoding

D. J. Bernstein
University of Illinois at Chicago

Thanks to: Cisco
University Research Program

And thanks to: NIST
grant 60NANB10D263

Divisors in intervals

Classic problem: Find all divisors of N in $[A - H, A + H]$, given positive integers N, A, H with $A > H$.

Reformulation: In $\mathbf{Q}[x]$ define $g = Hx$ and $f = (A + Hx)/N$. Want all $r \in \mathbf{Q}$ with $|r| \le 1$, $g(r) \in \mathbf{Z}$, numerator$(f(r)) = 1$.

Classic solution for many cases: Find small nonzero polynomial $\varphi \in \mathbf{Z} + \mathbf{Z}f + \mathbf{Z}fg \subset \mathbf{Q}[x]$. For each rational root r of φ, check whether $A + Hr$ divides N.

Understanding this solution for $H < (A - H)/6N^{1/3}$:

Understanding this solution
for $H < (A - H)/6N^{1/3}$:

$f = \cdots + Hx/N$,
$fg = \cdots + H^2x^2/N$,
so $\det(1, f, fg) = H^3/N^2$.
Lattice-basis reduction finds
φ with coeffs $\leq 2H/N^{2/3}$.

Understanding this solution
for $H < (A - H)/6N^{1/3}$:

$f = \cdots + Hx/N$,
$fg = \cdots + H^2x^2/N$,
so $\det(1, f, fg) = H^3/N^2$.
Lattice-basis reduction finds
φ with coeffs $\le 2H/N^{2/3}$.

Take divisor of N in $[A{-}H, A{+}H]$.
Write as $A + Hr$; $r \in \mathbf{Q}$, $|r| \le 1$.
Then $|\varphi(r)| \le 6H/N^{2/3}$.

Understanding this solution for $H < (A - H)/6N^{1/3}$:

$f = \cdots + Hx/N$,
$fg = \cdots + H^2x^2/N$,
so $\det(1, f, fg) = H^3/N^2$.
Lattice-basis reduction finds φ with coeffs $\le 2H/N^{2/3}$.

Take divisor of N in $[A-H, A+H]$.
Write as $A + Hr$; $r \in \mathbf{Q}$, $|r| \le 1$.
Then $|\varphi(r)| \le 6H/N^{2/3}$.

$1, f(r), f(r)g(r) \in ((A+Hr)/N)\mathbf{Z}$
so $\varphi(r) \in ((A + Hr)/N)\mathbf{Z}$.
But $(A + Hr)/N > 6H/N^{2/3}$
so $\varphi(r)$ must be 0.

Classic generalization: Find all divisors of N in $\{A - BH, \ldots, A - B, A, A + B, \ldots, A + BH\}$, given positive integers N, A, B, H with $A > BH$.

Mediocre approach: Define $g = Hx$ and $f = (A + BHx)/N$.
Proceed as before.
Loses factor B^2 in det.

Classic generalization: Find all divisors of N in $\{A - BH, \ldots, A - B, A, A + B, \ldots, A + BH\}$, given positive integers N, A, B, H with $A > BH$.

Mediocre approach: Define $g = Hx$ and $f = (A + BHx)/N$.
Proceed as before.
Loses factor B^2 in det.

Much better approach: Define $g = Hx$ and $f = (UA + Hx)/N$, assuming $U \in \mathbf{Z}$, $UB - 1 \in N\mathbf{Z}$.
If $Hr \in \mathbf{Z}$ and $A + BHr$ divides N then $f(r) \in ((A + BHr)/N)\mathbf{Z}$.

Linear combinations as divisors

Further generalization: Find all divisors $As + Bt$ of N with $1 \le s \le J$; $|t| \le H$; $\gcd\{s, t\} = 1$.

Generalization of classic solution:

Define $g = (H/J)x$; U as before; $f = (UA + (H/J)x)/N$.
As before find small nonzero $\varphi \in \mathbf{Z} + \mathbf{Z}f + \mathbf{Z}fg$.

Write each rational root of φ as Jt/Hs with $\gcd\{s, t\} = 1$, $s > 0$.
Check whether $As + Bt$ divides N with $s \le J$ and $|t| \le H$.

Understanding this solution for $HJ < (A - BH)/6N^{1/3}$:

$\det(1, f, fg) = H^3/J^3N^2$. Lattice-basis reduction finds φ with coeffs $\le 2H/JN^{2/3}$.

If $1 \le s \le J$ and $|t| \le H$ and $r = Jt/Hs$ then $\left|s^2\varphi(r)\right| = \left|\varphi_0 s^2 + \varphi_1 stJ/H + \varphi_2 t^2J^2/H^2\right| \le 3(2H/JN^{2/3})J^2 = 6HJ/N^{2/3}$.

If also $As + Bt$ divides N then $sf(r) = (UAs + t)/N \in ((As + Bt)/N)\mathbf{Z}$ and $sg(r) \in \mathbf{Z}$ so $s^2\varphi(r) \in ((As + Bt)/N)\mathbf{Z}$.

1984 Lenstra: $A + Bt$ algorithm, for proving primality.

1986 Rivest–Shamir: $A + t$, for attacking constrained RSA.

Many subsequent generalizations.

2003 Bernstein: projective view, but only affine applications.

Projective applications:
2007 Wu, 2008 Bernstein
(including this $As + Bt$ algorithm),
2009 Castagnos–Joux–
Laguillaumie–Nguyen.

Higher multiplicities

Generalization of $A + t$ algorithm:

Choose a multiplicity k
and a lattice dimension ℓ.

Find small nonzero $\varphi \in$
$\mathbf{Z} + \mathbf{Z}f + \mathbf{Z}f^2 + \cdots + \mathbf{Z}f^k$
$+\mathbf{Z}f^k g + \mathbf{Z}f^k g^2 + \cdots + \mathbf{Z}f^k g^{\ell-k-1}$.

det $=$
$(H/N)^{\ell(\ell-1)/2} N^{(\ell-k)(\ell-k-1)/2}$
so $|\varphi| \le$
$\cdots (H/N)^{(\ell-1)/2} N^{(\ell-k)(\ell-k-1)/2\ell}$.

But $\varphi(r) \in (\text{divisor}/N)^k \mathbf{Z}$.

Optimize: large ℓ with $k \approx \theta\ell$
if $A - H = N^{\theta}$.
$\#\{t$ possibilities searched$\} \approx N^{\theta^2}$.

Same for $A + Bt$ etc.

1996 Coppersmith:
$A + t$ with multiplicities; N^{θ^2};
various generalizations.
But algorithm was slower:
identified lattice via dual.

1997 Howgrave-Graham:
this algorithm; skip dualization;
simply write down f^k etc.

The gcd tweak

Minor tweak: Find all $A + t$ with $|t| \le H$ and $\gcd\{A + t, N\} \ge N^\theta$.

These t's include previous t's: if $A + t$ divides N and $A + t \ge N^\theta$ then $\gcd\{A + t, N\} \ge N^\theta$.

Solution: Compute the same φ from the same lattice as before. For each rational root r of φ, check $\gcd\{A + Hr, N\} \ge N^\theta$.

1997 Sudan:
$\mathbf{F}_q[z]$ instead of $\mathbf{Z}$,
$N = (z - a_1) \cdots (z - a_n)$,
multiplicity 1, dual algorithm,
for list decoding.

1999 Guruswami–Sudan:
same with high multiplicity.

1999 Goldreich–Ron–Sudan:
$\mathbf{Z}$, multiplicity 1, dual.

2000 Boneh:
$\mathbf{Z}$, high multiplicity.

The list-decoding application:

Given $t \bmod p_1, \ldots, t \bmod p_n$
for distinct primes $p_1, \ldots, p_n$,
can interpolate $t \bmod N$
where $N = p_1 p_2 \cdots p_n$.

Given same *with some errors*,
interpolation produces A where
all the other primes divide $t - A$;
i.e., $\gcd\{t - A, N\}$ is large.

Can find all t
in interval of length $\approx N^{\theta^2}$
with $\gcd\{t - A, N\} \geq N^{\theta}$.

RS and GRS codes—
"the GS decoder":

Reconstruct $t \in \mathbf{F}_q[z]$ given
$(t(a_1), \ldots, t(a_n)) +$ errors;
distinct $a_1, \ldots, a_n \in \mathbf{F}_q$;
$\#$errors $< (1-\theta)n$;
$\deg t \le \theta^2 n$.

Reconstruct $t \in \mathbf{F}_q[z]$ given
$(\beta_1 t(a_1), \ldots, \beta_n t(a_n)) +$ errors;
distinct $a_1, \ldots, a_n \in \mathbf{F}_q$;
nonzero $\beta_1, \ldots, \beta_n \in \mathbf{F}_q$;
$\#$errors $< (1-\theta)n$;
$\deg t \le \theta^2 n$.

Higher-degree polynomials

$\gcd\{N, p(t)\} \ge N^\theta$:
$\#\{t$ possibilities searched$\}$
$\approx N^{\theta^2/d}$ if p monic, $\deg p = d$.

1988 Håstad: $\theta = 1$, $k = 1$.

1989 Vallée–Girault–Toffin:
$\theta = 1$, $k = 1$, dual.

1996 Coppersmith:
$\theta = 1$, high multiplicity, dual.

1997 Howgrave-Graham:
$\theta = 1$, high multiplicity.

2000 Boneh:
any θ, high multiplicity.

Gaussian divisors in intervals

New (?) problem: Find all
$t \in \{-H, \dots, -1, 0, 1, \dots, H\}$
with $A_0 + t + A_1 i$ dividing $N_0 + N_1 i$
in $\mathbf{Z}[i]/(i^2 + 1)$; assume $A_0 > H$.

One approach: Take norms.
$(A_0 + t)^2 + A_1^2$ divides $N_0^2 + N_1^2$.
Use standard degree-2 algorithm.
Works for $H \approx (N_0^2 + N_1^2)^{\theta^2/2}$
if $(A_0 - H)^2 + A_1^2 = (N_0^2 + N_1^2)^{\theta}$.

Worse: Find divisor of $N_0^2 + N_1^2$
in $[(A_0 - H)^2 + A_1^2, (A_0 + H)^2 + A_1^2]$,
using degree-1 algorithm.
Works for $A_0 H \approx (N_0^2 + N_1^2)^{\theta^2}$.

Another approach:
lattice-basis reduction over $\mathbf{Z}[i]$.
Works, but searches $t \in \mathbf{Z}[i]$,
again wasting time.

Another approach:
lattice-basis reduction over $\mathbf{Z}[i]$.
Works, but searches $t \in \mathbf{Z}[i]$,
again wasting time.

Better approach:
$(A_0 + t)^2 + A_1^2$ divides
$(A_0 + t - A_1 i)(N_0 + N_1 i)$
so it divides $(A_0 + t)N_1 - A_1 N_0$.
Also divides $N_0^2 + N_1^2$.

$$\gcd\left\{(A_0 + t)N_1 - A_1 N_0, N_0^2 + N_1^2\right\}$$
$$\geq (N_0^2 + N_1^2)^\theta.$$

Works for $H \approx (N_0^2 + N_1^2)^{\theta^2}$,
assuming $\gcd\{N_0, N_1\} = 1$.

Jet divisors

Easily generalize:
$A_0 s + B_0 t$, other algebras, etc.
My main interest today:
the "1-jet" algebra $\mathbf{Z}[\epsilon]/\epsilon^2$.

To search for small $(s,t) \in \mathbf{Z} \times \mathbf{Z}$
with $(A_0 + A_1\epsilon)s + (B_0 + B_1\epsilon)t$
dividing $N_0 + N_1\epsilon$ in $\mathbf{Z}[\epsilon]/\epsilon^2$: use
$\gcd\{\Delta, N_0^2\} \ge (N_0^2)^\theta$ where $\Delta =$
$(A_0 N_1 - A_1 N_0)s + (B_0 N_1 - B_1 N_0)t$.

$\#\{(s,t) \text{ searched}\} \approx (N_0^2)^{\theta^2}$,
assuming $\gcd\{N_0, B_0 N_1\} = 1$.

Searching for $A_0 s + B_0 t$ dividing
N_0 would search only $N_0^{\theta^2}$.

Classical binary Goppa codes

Fix $q \in \{2, 4, 8, 16, \ldots\}$.
Fix distinct $a_1, \ldots, a_n \in \mathbf{F}_q$.
Fix monic $D \in \mathbf{F}_q[z]$
coprime to $N = \prod_i (z - a_i)$.

Define $\Gamma = \Gamma_2(a_1, \ldots, a_n, D)$ as
$$\Big\{(c_1, \ldots, c_n) \in \mathbf{F}_2^n : \sum_i c_i/(z - a_i) = 0 \text{ in } \mathbf{F}_q[z]/D\Big\}.$$

$\lg \#\Gamma \geq n - (\lg q) \deg D$.

If D is squarefree then
min distance of $\Gamma \geq 2 \deg D + 1$.
Proof: $e = \prod_{i:c_i=1}(z - a_i)$ has
D dividing Ne'/e, hence e'; so
D^2 divides e', so $\deg e' \geq 2 \deg D$.

If $C \in \mathbf{F}_q[z]$ has
$\deg C < n - \deg D$ and
$c_i = C(a_i)D(a_i)/N'(a_i) \in \mathbf{F}_2$
for all i then $(c_1, \ldots, c_n) \in \Gamma$
since $C D = \sum_i c_i N/(z - a_i)$.

All elements of Γ arise this way.

If $\#\text{errors} < (1 - \theta)n$ and
$n - \deg D - 1 = \theta^2 n$, i.e.,
$\#\text{errors} < n - \sqrt{n(n - \deg D - 1)}$:
can use the GS decoder.

If $C \in \mathbf{F}_q[z]$ has
$\deg C < n - \deg D$ and
$c_i = C(a_i)D(a_i)/N'(a_i) \in \mathbf{F}_2$
for all i then $(c_1, \ldots, c_n) \in \Gamma$
since $C D = \sum_i c_i N/(z - a_i)$.

All elements of Γ arise this way.

If $\#$errors $< (1 - \theta)n$ and
$n - \deg D - 1 = \theta^2 n$, i.e.,
$\#$errors $< n - \sqrt{n(n - \deg D - 1)}$:
can use the GS decoder.

2000 Koetter–Vardy:
This is not optimal;
can decode many more errors!

“The KV decoder”:

Polynomial-time algorithm for #errors $< (1-\theta)n/2$ and $n/2 - \deg D - 1 = \theta^2 n/2$, i.e., #errors $< n/2 - \sqrt{(n/2)((n/2) - \deg D - 1)}$.

Exploits fact that errors are required to be in $\mathbf{F}_2$.

2011 Bernstein “Simplified high-speed high-distance list decoding for alternant codes”: adaptation of Howgrave-Graham idea to KV.

If D is squarefree then
$\Gamma_2(\ldots, D) = \Gamma_2(\ldots, D^2)$.
(1970 Goppa?; different, more general, proof: 1975 Sugiyama–Kasahara–Hirasawa–Namekawa)

Allows decoding even more errors.

If #errors $\leq \deg D$: can use naive decoders for $\Gamma_2(\ldots, D^2)$.

If #errors $< n - \sqrt{n(n - 2\deg D - 1)}$: can use GS etc. for $\Gamma_2(\ldots, D^2)$.

If #errors $< n/2 - \sqrt{(n/2)((n/2) - 2\deg D - 1)}$: can use KV etc. for $\Gamma_2(\ldots, D^2)$.

A different approach

1975 Patterson:

Assume D irreducible.

Given $(w_1, \ldots, w_n) \in \mathbf{F}_2^n - \Gamma$,
compute $s \in \mathbf{F}_q[z]/D$ with
$1/(s^2 + z) = \sum_i w_i/(z - a_i)$.

Find shortest nonzero $(\alpha_0, \beta_0\sqrt{z})$
in $(D, 0)\mathbf{F}_q[z] + (s, \sqrt{z})\mathbf{F}_q[z]$.

Compute $e_0 = \alpha_0^2 + \beta_0^2 z$.

If #errors $\leq \deg D$ then
the errors are the roots of e_0.

Why this works:

Say errors are $(e_1, \ldots, e_n)$:
i.e. $(w_1, \ldots) - (e_1, \ldots) \in \Gamma$
and $\#\{i : e_i = 1\} \le \deg D$.

Write $e = \prod_{i:e_i=1}(z - a_i)$
as $\alpha^2 + \beta^2 z$. Then
$\beta^2/(\alpha^2{+}\beta^2 z) = e'/e = 1/(s^2{+}z)$
in $\mathbf{F}_q[z]/D$ so $(\alpha, \beta\sqrt{z}) \in$
$(D, 0)\mathbf{F}_q[z] + (s, \sqrt{z})\mathbf{F}_q[z]$.

$\det = D\sqrt{z}$; $\left|(\alpha, \beta\sqrt{z})\right|^2 \le |D|$;
so $(\alpha, \beta\sqrt{z})$ is multiple
of shortest nonzero vector.

$\gcd\{\alpha, \beta\} = 1$ so mult is const.

What if #errors $> \deg D$?

2008 Bernstein:

Find short
$(\alpha_0, \beta_0\sqrt{z})$, $(\alpha_1, \beta_1\sqrt{z})$
generating the same lattice.

Then $(\alpha, \beta\sqrt{z}) =$
$c_0(\alpha_0, \beta_0\sqrt{z}) + c_1(\alpha_1, \beta_1\sqrt{z})$
for some c_0, c_1
so $e = e_0 c_0^2 + e_1 c_1^2$.
Tweak e_1 so $\gcd\{e_1, N\} = 1$.

Find e by finding small linear combination of e_0, e_1 dividing N.

This algorithm decodes
same #errors as
GS applied to $\Gamma_2(\ldots, D^2)$,
and has a big advantage:
much smaller lattice rank.

See also 2007 Wu:
Reed–Solomon decoder
with same advantage.

KV applied to $\Gamma_2(\ldots, D^2)$
decodes many more errors
but loses this advantage.
Is this tradeoff required?

New, jet list decoding:

Search for divisors of jet
$N + N'\epsilon \in \mathbf{F}_q[z][\epsilon]/\epsilon^2$
as $\mathbf{F}_q[z]$-linear combinations of
$e_0 + e'_0\epsilon$, $e_1 + e'_1\epsilon$.

In particular find desired
$e + e'\epsilon =$
$(e_0 + e'_0\epsilon)c_0^2 + (e_1 + e'_1\epsilon)c_1^2$.

#errors should match D^2 KV,
using much smaller lattice rank!