Jet list decoding

D. J. Bernstein
University of Illinois at Chicago

Thanks to:

NSF
(1018836)

NIST
(60NANB10D263)

Cisco
(University Research Program)

<u>Interpolation</u>

Fix coprime $p_1, \ldots, p_n \in \mathbf{Z}_{>0}$.

Remainder repn of $t \in \mathbf{Z}$:
$\operatorname{ev} t = (t \bmod p_1, \ldots, t \bmod p_n)$.

Chinese remainder theorem:
$\operatorname{ev} t$ determines $t \bmod N$
where $N = p_1 \cdots p_n$.

Very fast computation:
If $0 \le t < N$ then

$$\frac{t}{N} = \left(\sum_i \frac{t q_i \bmod p_i}{p_i} \right) \bmod 1$$

where $q_i = (N/p_i)^{-1} \bmod p_i$.

Decoding

Fix $H < N$. Assume $0 \le t < H$.

Remainder repn is redundant.
Given any vector $v \approx \text{ev}\, t$
can reconstruct t.

Traditional definition of "$\approx$":
$\prod_{i: v_i \ne (\text{ev}\, t)_i} p_i \le \sqrt{N/H}$.
Surprisingly fast $v \mapsto t$ methods.

Proof that v determines t:
if $v \approx \text{ev}\, u$ and $v \approx \text{ev}\, t$ then
$\prod_{i: (\text{ev}\, u)_i \ne (\text{ev}\, t)_i} p_i \le N/H$ so
$\prod_{i: (\text{ev}\, u)_i = (\text{ev}\, t)_i} p_i \ge H$ but
$\prod_{i: (\text{ev}\, u)_i = (\text{ev}\, t)_i} p_i$ divides $t - u$.

List decoding

What if we know $|v - \mathrm{ev}\, t| \leq W$ where W is *above* $\sqrt{N/H}$?

Traditional answer: Give up.
No guarantee that t is unique.

Modern answer:
W determines a *list* of possibilities for t.
How quickly can we compute list?
How does speed degrade with W?

1957 Elias, 1958 Wozencraft:
bounds on list size,
but no fast algorithms.

Reed–Solomon decoding

Fix prime power q,
distinct $a_1, \ldots, a_n \in \mathbf{F}_q$.

Remainder repn of $t \in \mathbf{F}_q[x]$:
$\operatorname{ev} t = (t(a_1), \ldots, t(a_n))$.

Given any vector $v \approx \operatorname{ev} t$
can reconstruct t,
assuming $\deg t < h$.

Traditional "$\approx$":
$\#\{i : v_i \neq (\operatorname{ev} t)_i\} \leq (n - h)/2$.

List decoding:
compute list of possibilities for t
given larger bound on $|v - \operatorname{ev} t|$.

Jets

The algebra of 1-jets over $\mathbf{R}$
is the quotient ring $\mathbf{R}[\epsilon]/\epsilon^2$.

Analogous to the set of complex
numbers $\mathbf{C} = \mathbf{R}[i]/(i^2+1)$,
but $\epsilon^2 = 0$ while $i^2 = -1$.

Multiplication of jets:
$(a+b\epsilon)(c+d\epsilon) = ac+(ad+bc)\epsilon$.

Typical construction of a jet:
differentiable $f : \mathbf{R} \to \mathbf{R}$ induces
jet $f(x+\epsilon) = f(x) + f'(x)\epsilon$
for each $x \in \mathbf{R}$.
e.g. $\sin(x+\epsilon) = \sin x + (\cos x)\epsilon$.

Lattice-basis reduction

Define $L = (0, 24)\mathbf{Z} + (1, 17)\mathbf{Z}$
$= \{(b, 24a + 17b) : a, b \in \mathbf{Z}\}$.

What is the shortest
nonzero vector in L?

Lattice-basis reduction

Define $L = (0, 24)\mathbf{Z} + (1, 17)\mathbf{Z}$
$= \{(b, 24a + 17b) : a, b \in \mathbf{Z}\}$.

What is the shortest nonzero vector in L?

$L = (0, 24)\mathbf{Z} + (1, 17)\mathbf{Z}$

Lattice-basis reduction

Define $L = (0, 24)\mathbf{Z} + (1, 17)\mathbf{Z}$
$= \{(b, 24a + 17b) : a, b \in \mathbf{Z}\}$.

What is the shortest nonzero vector in L?

$$\begin{aligned} L &= (0, 24)\mathbf{Z} + (1, 17)\mathbf{Z} \\ &= (-1, 7)\mathbf{Z} + (1, 17)\mathbf{Z} \end{aligned}$$

Lattice-basis reduction

Define $L = (0,24)\mathbf{Z} + (1,17)\mathbf{Z}$
$= \{(b, 24a + 17b) : a, b \in \mathbf{Z}\}$.

What is the shortest
nonzero vector in L?

$$\begin{aligned} L &= (0,24)\mathbf{Z} + (1,17)\mathbf{Z} \\ &= (-1,7)\mathbf{Z} + (1,17)\mathbf{Z} \\ &= (-1,7)\mathbf{Z} + (3,3)\mathbf{Z} \end{aligned}$$

Lattice-basis reduction

Define $L = (0, 24)\mathbf{Z} + (1, 17)\mathbf{Z}$
$= \{(b, 24a + 17b) : a, b \in \mathbf{Z}\}$.

What is the shortest nonzero vector in L?

$$\begin{aligned} L &= (0, 24)\mathbf{Z} + (1, 17)\mathbf{Z} \\ &= (-1, 7)\mathbf{Z} + (1, 17)\mathbf{Z} \\ &= (-1, 7)\mathbf{Z} + (3, 3)\mathbf{Z} \\ &= (-4, 4)\mathbf{Z} + (3, 3)\mathbf{Z}. \end{aligned}$$

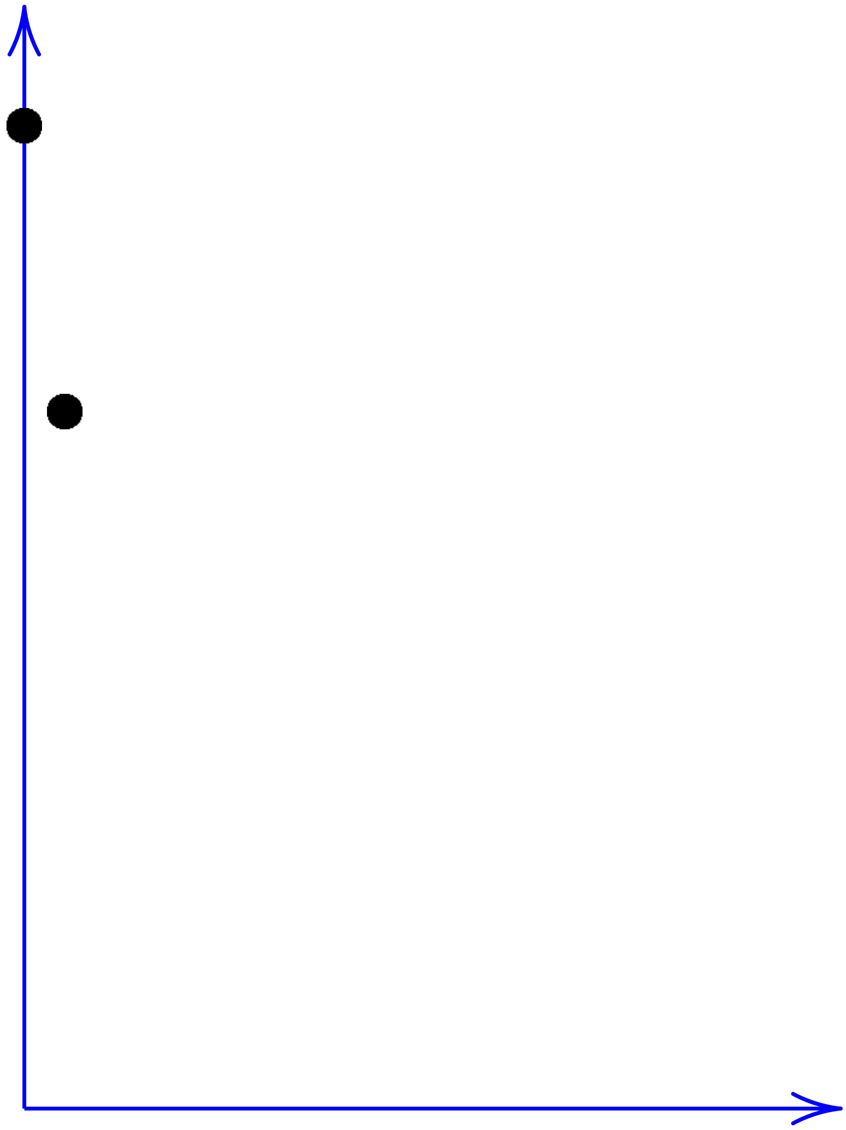
Lattice-basis reduction

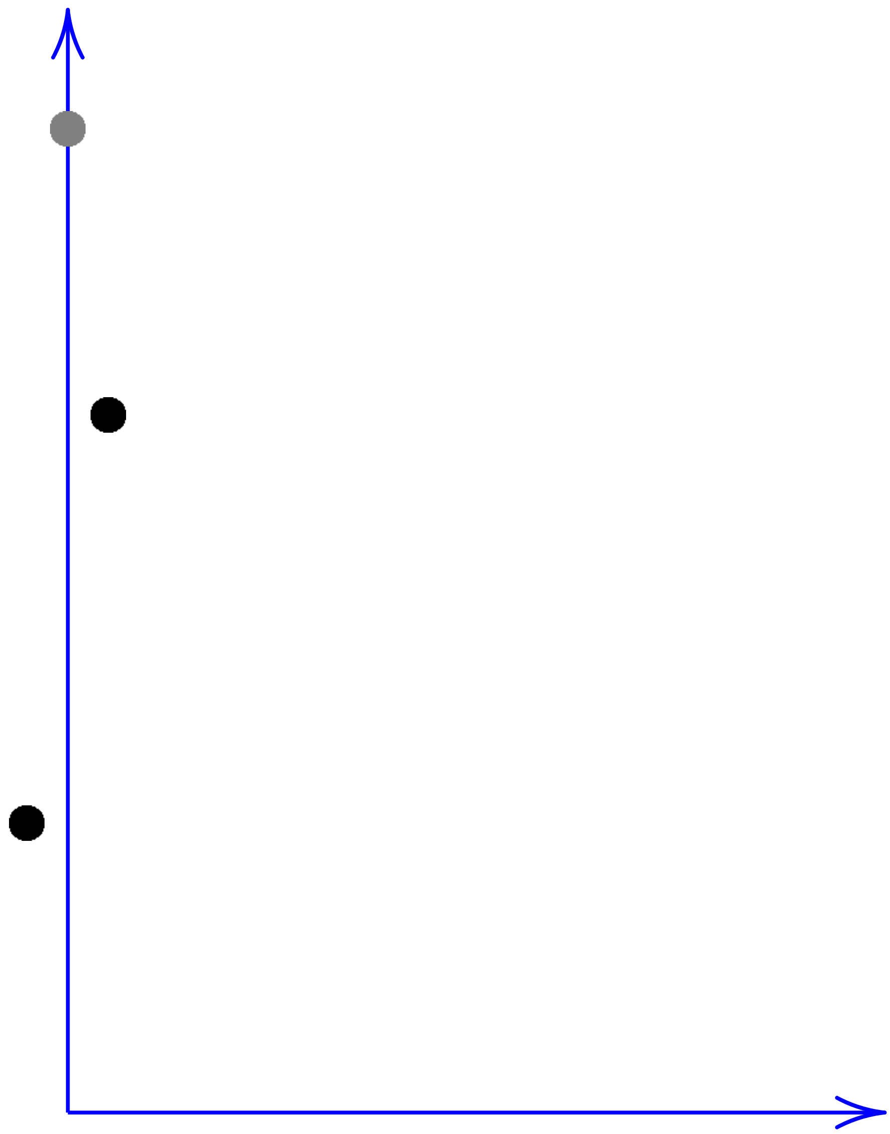
Define $L = (0, 24)\mathbf{Z} + (1, 17)\mathbf{Z}$
$= \{(b, 24a + 17b) : a, b \in \mathbf{Z}\}$.

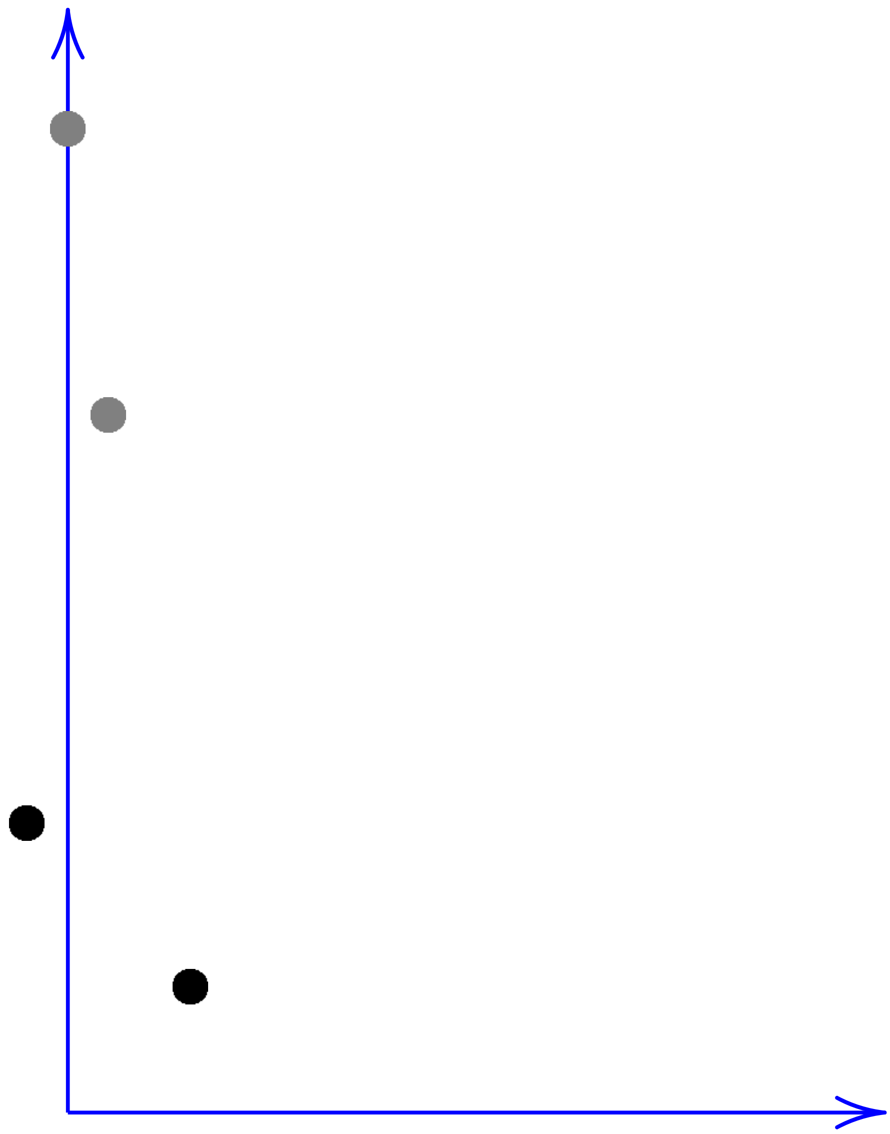
What is the shortest nonzero vector in L?

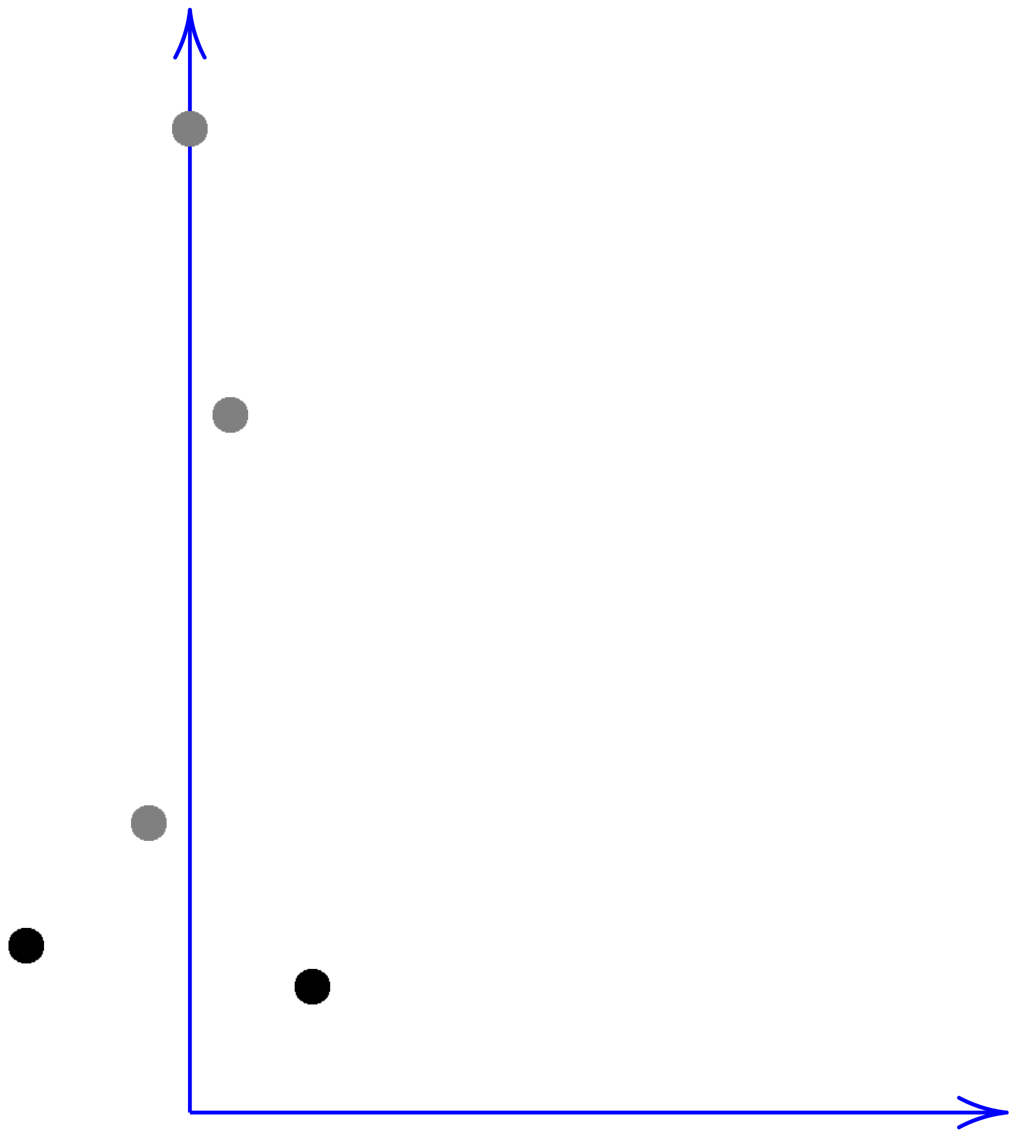
$$\begin{aligned} L &= (0, 24)\mathbf{Z} + (1, 17)\mathbf{Z} \\ &= (-1, 7)\mathbf{Z} + (1, 17)\mathbf{Z} \\ &= (-1, 7)\mathbf{Z} + (3, 3)\mathbf{Z} \\ &= (-4, 4)\mathbf{Z} + (3, 3)\mathbf{Z}. \end{aligned}$$

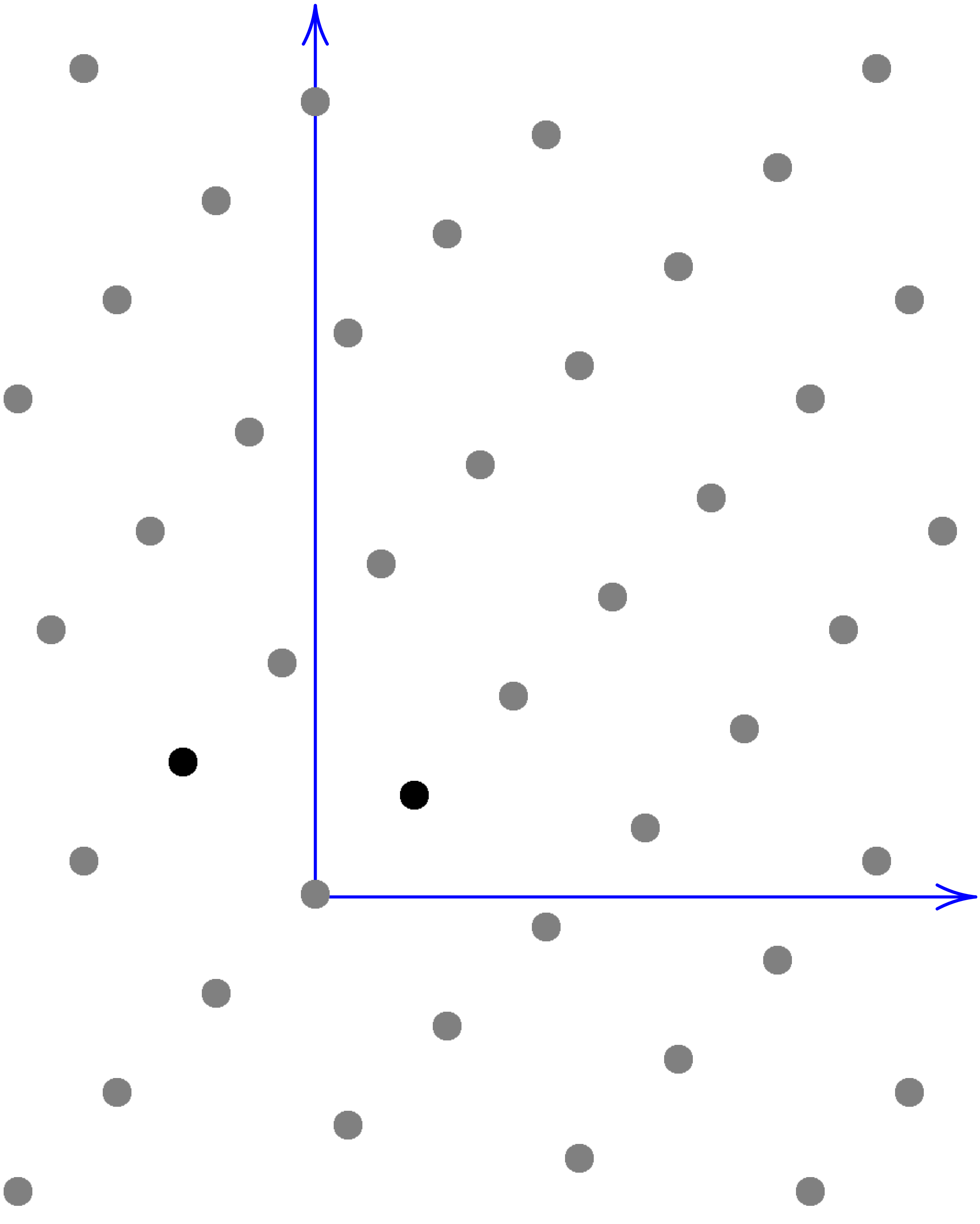
$(-4, 4), (3, 3)$ are orthogonal.
Shortest vectors in L are $(0, 0)$, $(3, 3)$, $(-3, -3)$.











Another example:
Define $L = (0, 25)\mathbf{Z} + (1, 17)\mathbf{Z}$.

What is the shortest
nonzero vector in L?

Another example:
Define $L = (0, 25)\mathbf{Z} + (1, 17)\mathbf{Z}$.

What is the shortest
nonzero vector in L?

$$L = (0, 25)\mathbf{Z} + (1, 17)\mathbf{Z}$$

Another example:

Define $L = (0, 25)\mathbf{Z} + (1, 17)\mathbf{Z}$.

What is the shortest nonzero vector in L?

$$\begin{aligned} L &= (0, 25)\mathbf{Z} + (1, 17)\mathbf{Z} \\ &= (-1, 8)\mathbf{Z} + (1, 17)\mathbf{Z} \end{aligned}$$

Another example:

Define $L = (0, 25)\mathbf{Z} + (1, 17)\mathbf{Z}$.

What is the shortest nonzero vector in L?

$$\begin{aligned} L &= (0, 25)\mathbf{Z} + (1, 17)\mathbf{Z} \\ &= (-1, 8)\mathbf{Z} + (1, 17)\mathbf{Z} \\ &= (-1, 8)\mathbf{Z} + (3, 1)\mathbf{Z}. \end{aligned}$$

Another example:

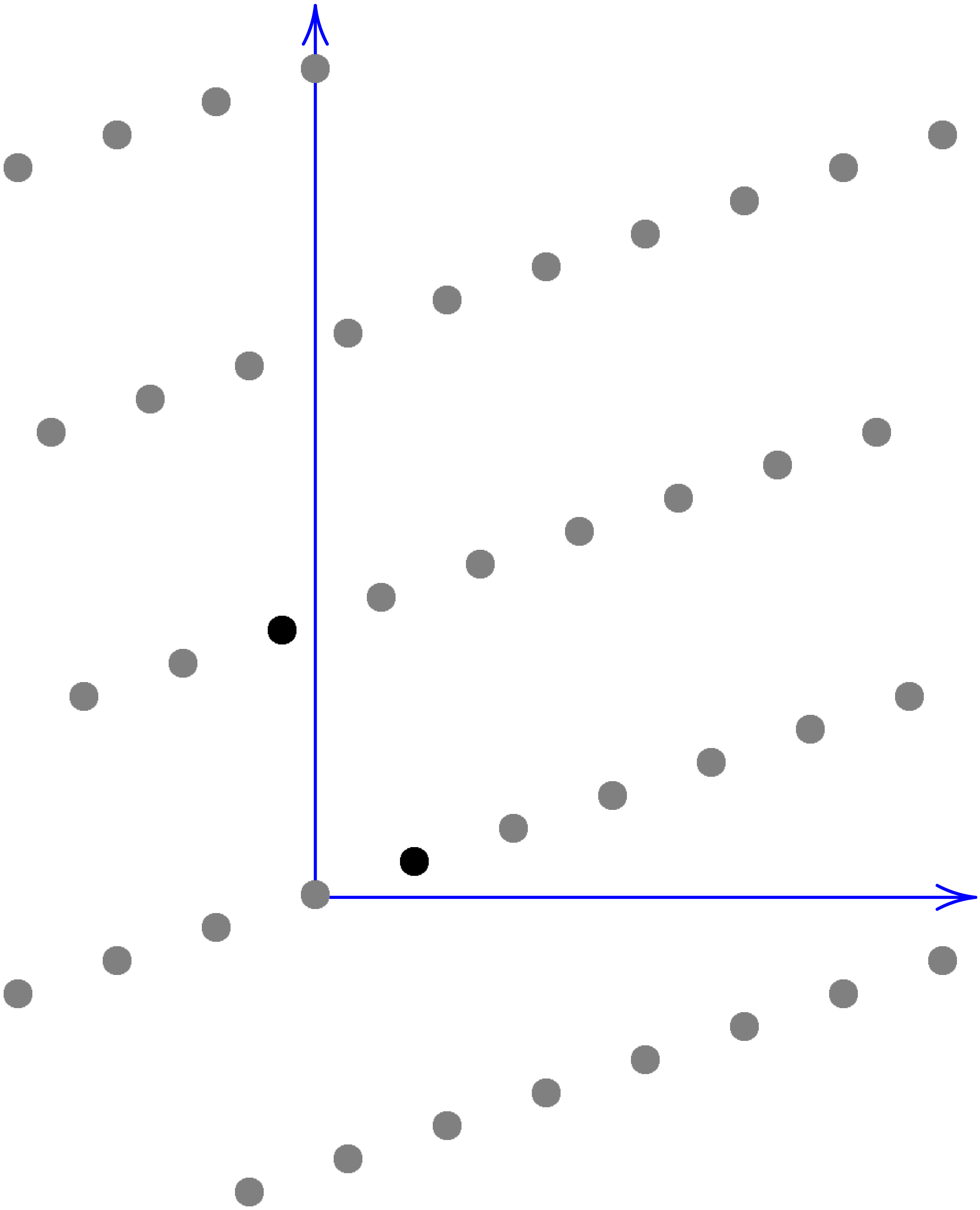
Define $L = (0,25)\mathbf{Z} + (1,17)\mathbf{Z}$.

What is the shortest nonzero vector in L?

$$\begin{aligned} L &= (0,25)\mathbf{Z} + (1,17)\mathbf{Z} \\ &= (-1,8)\mathbf{Z} + (1,17)\mathbf{Z} \\ &= (-1,8)\mathbf{Z} + (3,1)\mathbf{Z}. \end{aligned}$$

Nearly orthogonal.

Shortest vectors in L are $(0,0)$, $(3,1)$, $(-3,-1)$.



Polynomial lattices

Define $R = \mathbf{F}_2[x]$,
$r_0 = (101000)_x = x^5 + x^3 \in R$,
$r_1 = (10011)_x = x^4 + x + 1 \in R$,
$L = (0, r_0)R + (1, r_1)R$.

What is the shortest nonzero vector in L?

Polynomial lattices

Define $R = \mathbf{F}_2[x]$,
$r_0 = (101000)_x = x^5 + x^3 \in R$,
$r_1 = (10011)_x = x^4 + x + 1 \in R$,
$L = (0, r_0)R + (1, r_1)R$.

What is the shortest nonzero vector in L?

$L = (0, 101000)R + (1, 10011)R$

Polynomial lattices

Define $R = \mathbf{F}_2[x]$,
$r_0 = (101000)_x = x^5 + x^3 \in R$,
$r_1 = (10011)_x = x^4 + x + 1 \in R$,
$L = (0, r_0)R + (1, r_1)R$.

What is the shortest nonzero vector in L?

$$L = (0, 101000)R + (1, 10011)R$$
$$= (10, 1110)R + (1, 10011)R$$

Polynomial lattices

Define $R = \mathbf{F}_2[x]$,
$r_0 = (101000)_x = x^5 + x^3 \in R$,
$r_1 = (10011)_x = x^4 + x + 1 \in R$,
$L = (0, r_0)R + (1, r_1)R$.

What is the shortest nonzero vector in L?

$$\begin{aligned} L &= (0, 101000)R + (1, 10011)R \\ &= (10, 1110)R + (1, 10011)R \\ &= (10, 1110)R + (111, 1)R. \end{aligned}$$

Polynomial lattices

Define $R = \mathbf{F}_2[x]$,
$r_0 = (101000)_x = x^5 + x^3 \in R$,
$r_1 = (10011)_x = x^4 + x + 1 \in R$,
$L = (0, r_0)R + (1, r_1)R$.

What is the shortest nonzero vector in L?

$$\begin{aligned} L &= (0, 101000)R + (1, 10011)R \\ &= (10, 1110)R + (1, 10011)R \\ &= (10, 1110)R + (111, 1)R. \end{aligned}$$

$(111, 1)$: shortest nonzero vector.
$(10, 1110)$: shortest independent vector.

Degree of $(q, r) \in \mathbf{F}_2[x] \times \mathbf{F}_2[x]$ is defined as $\max\{\deg q, \deg r\}$.

Can use other metrics, or equivalently rescale L.

e.g. Define $L \subseteq \mathbf{F}_2[\sqrt{x}] \times \mathbf{F}_2[\sqrt{x}]$ as $(0, r_0\sqrt{x})R + (1, r_1\sqrt{x})R$.

Successive generators for L:
$(0, 101000\sqrt{x})$, degree 5.5.
$(1, 10011\sqrt{x})$, degree 4.5.
$(10, 1110\sqrt{x})$, degree 3.5.
$(111, 1\sqrt{x})$, degree 2.

Warning: Sometimes shortest independent vector is *after* shortest nonzero vector.

e.g. Define
$r_0 = 101000$, $r_1 = 10111$,
$L = (0, r_0\sqrt{x})R + (1, r_1\sqrt{x})R$.

Successive generators for L:
$(0, 101000\sqrt{x})$, degree 5.5.
$(1, 10111\sqrt{x})$, degree 4.5.
$(10, 110\sqrt{x})$, degree 2.5.
$(1101, 11\sqrt{x})$, degree 3.

For any $r_0, r_1 \in R = \mathbf{F}_q[x]$ with $\deg r_0 > \deg r_1$:

Euclid/Stevin computation:
Define $r_2 = r_0 \bmod r_1$,
$r_3 = r_1 \bmod r_2$, etc.

Extended: $q_0 = 0$; $q_1 = 1$;
$q_{i+2} = q_i - \lfloor r_i/r_{i+1} \rfloor q_{i+1}$.
Then $q_i r_1 \equiv r_i \pmod{r_0}$.

Lattice view: Have
$(0, r_0\sqrt{x})R + (1, r_1\sqrt{x})R =$
$(q_i, r_i\sqrt{x})R + (q_{i+1}, r_{i+1}\sqrt{x})R$.

Can continue until $r_{i+1} = 0$.
$\gcd\{r_0, r_1\} = r_i/\operatorname{leadcoeff} r_i$.

Reducing lattice basis for L is a "half gcd" computation, stopping halfway to the gcd.

$\deg r_i$ decreases; $\deg q_i$ increases; $\deg q_{i+1} + \deg r_i = \deg r_0$.

Say j is minimal with $\deg r_j\sqrt{x} \le (\deg r_0)/2$. Then $\deg q_j \le (\deg r_0)/2$ so $\deg(q_j, r_j\sqrt{x}) \le (\deg r_0)/2$. Shortest nonzero vector.

$(q_{j+\epsilon}, r_{j+\epsilon}\sqrt{x})$ has degree $\deg r_0\sqrt{x} - \deg(q_j, r_j\sqrt{x})$ for some $\epsilon \in \{-1, 1\}$. Shortest independent vector.

Proof of “shortest”:

Take any $(q, r\sqrt{x})$ in lattice.

$$(q, r\sqrt{x}) = u(q_j, r_j\sqrt{x}) \\ + v(q_{j+\epsilon}, r_{j+\epsilon}\sqrt{x})$$

for some $u, v \in R$.

$q_j r_{j+\epsilon} - q_{j+\epsilon} r_j = \pm r_0$
so $v = \pm(r q_j - q r_j)/r_0$
and $u = \pm(q r_{j+\epsilon} - r q_{j+\epsilon})/r_0$.

If $\deg(q, r\sqrt{x})$
$< \deg(q_{j+\epsilon}, r_{j+\epsilon}\sqrt{x})$
then $\deg v < 0$ so $v = 0$;
i.e., any vector in lattice
shorter than $(q_{j+\epsilon}, r_{j+\epsilon}\sqrt{x})$
is a multiple of $(q_j, r_j\sqrt{x})$.

Higher-rank lattices

If $M \in \mathbf{F}_q[x]^{\ell\times\ell}$ has $\det M \neq 0$ then the columns of M have a nonzero linear combination Q with $\deg Q \le (\deg\det M)/\ell$.

Can compute Q with similar speed to matrix mult.
(2003 Giorgi–Jeannerod–Villard
+ small fix from 2011 Bernstein)

$M \in \mathbf{Z}^{\ell\times\ell}$: loosen bound on Q.
(1982 Lenstra–Lenstra–Lovasz: polynomial time; . . . ;
2011 Novocin–Stehlé–Villard: almost as fast as $\mathbf{F}_q[x]$ case)

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 $\mathbf{Q}[y]$ define $g = Hy$ and $f = (A + Hy)/N$. 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 $\varphi \in \mathbf{Z} + \mathbf{Z}f + \mathbf{Z}fg \subset \mathbf{Q}[y]$. 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 $H < (A-H)/6N^{1/3}$:

$f = \cdots + Hy/N$,
$fg = \cdots + H^2y^2/N$,
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 $H < (A - H)/6N^{1/3}$:

$f = \cdots + Hy/N$,
$fg = \cdots + H^2y^2/N$,
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 $H < (A - H)/6N^{1/3}$:

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

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

$1, f(r), f(r)g(r) \in ((A+Hr)/N)\mathbf{Z}$
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 $g = Hy$ and $f = (A + BHy)/N$.
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 $g = Hy$ and $f = (A + BHy)/N$. Proceed as before.
Loses factor B^2 in det.

Much better approach: Define $g = Hy$ and $f = (UA + Hy)/N$, 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 $g = (H/J)y$; U as before; $f = (UA + (H/J)y)/N$.
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 $\leq 2H/JN^{2/3}$.

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

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 $A - H = N^\theta$.
$\#\{t \text{ possibilities searched}\} \approx N^{\theta^2}$.

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 $|t| \leq H$ and $\gcd\{A + t, N\} \geq N^\theta$.

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

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

1997 Sudan:

$\mathbf{F}_q[x]$ instead of $\mathbf{Z}$,

$N = (x - a_1) \cdots (x - a_n)$,

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 GS decoder":

Reconstruct $t \in \mathbf{F}_q[x]$ 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 $t \in \mathbf{F}_q[x]$ 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

$\gcd\{N, p(t)\} \geq N^\theta$:
$\#\{t$ 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 $t \in \{-H, \ldots, -1, 0, 1, \ldots, H\}$ 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 $\gcd\{\Delta, N_0^2\} \geq (N_0^2)^\theta$ where $\Delta = (A_0N_1 - A_1N_0)s + (B_0N_1 - B_1N_0)t$.

$\#\{(s,t) \text{ searched}\} \approx (N_0^2)^{\theta^2}$, assuming $\gcd\{N_0, B_0N_1\} = 1$.

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

Classical binary Goppa codes

Fix integers $n \geq 0$, $m \geq 1$;
distinct $a_1, \ldots, a_n \in \mathbf{F}_{2^m}$;
monic $g \in \mathbf{F}_{2^m}[x]$
with $g(a_1) \cdots g(a_n) \neq 0$.

The code: Define $\Gamma \subseteq \mathbf{F}_2^n$
as set of $(c_1, \ldots, c_n)$ with
$\sum_i c_i/(x - a_i) = 0$ in $\mathbf{F}_{2^m}[x]/g$.

$\min\{|c| : c \in \Gamma - \{0\}\} \geq \deg g + 1$;
$\lg \#\Gamma \geq n - m \deg g$.
Better bounds in the BCH case
$g = x^k$ and in many other cases.

Say we receive $v = c + e$.

Define $D, E \in \mathbf{F}_{2^m}[x]$ by

$D = \prod_{i:e_i \neq 0}(x - a_i)$ and

$E = \sum_i De_i/(x - a_i)$.

Say we receive $v = c + e$.

Define $D, E \in \mathbf{F}_{2^m}[x]$ by

$D = \prod_{i:e_i \neq 0}(x - a_i)$ and

$E = \sum_i De_i/(x - a_i)$.

Lift $\sum_i v_i/(x - a_i)$ from $\mathbf{F}_{2^m}[x]/g$ to $s \in \mathbf{F}_{2^m}[x]$ with $\deg s < \deg g$.

Find shortest nonzero $(q_j, r_j\sqrt{x})$ in the lattice $L = (0, g\sqrt{x})\mathbf{F}_{2^m}[x] + (1, s\sqrt{x})\mathbf{F}_{2^m}[x]$.

Say we receive $v = c + e$.

Define $D, E \in \mathbf{F}_{2^m}[x]$ by

$D = \prod_{i:e_i \neq 0}(x - a_i)$ and

$E = \sum_i De_i/(x - a_i)$.

Lift $\sum_i v_i/(x - a_i)$ from $\mathbf{F}_{2^m}[x]/g$ to $s \in \mathbf{F}_{2^m}[x]$ with $\deg s < \deg g$.

Find shortest nonzero $(q_j, r_j\sqrt{x})$ in the lattice $L = (0, g\sqrt{x})\mathbf{F}_{2^m}[x] + (1, s\sqrt{x})\mathbf{F}_{2^m}[x]$.

Fact: If $|e| \leq (\deg g)/2$ then $E/D = r_j/q_j$ so D is monic denominator of r_j/q_j.

Say we receive $v = c + e$.
Define $D, E \in \mathbf{F}_{2^m}[x]$ by
$D = \prod_{i:e_i \neq 0}(x - a_i)$ and
$E = \sum_i De_i/(x - a_i)$.

Lift $\sum_i v_i/(x - a_i)$ from $\mathbf{F}_{2^m}[x]/g$
to $s \in \mathbf{F}_{2^m}[x]$ with $\deg s < \deg g$.
Find shortest nonzero
$(q_j, r_j\sqrt{x})$ in the lattice $L =$
$(0, g\sqrt{x})\mathbf{F}_{2^m}[x] + (1, s\sqrt{x})\mathbf{F}_{2^m}[x]$.

Fact: If $|e| \leq (\deg g)/2$
then $E/D = r_j/q_j$ so
D is monic denominator of r_j/q_j.

$e_i = 0$ if $D(a_i) \neq 0$.
$e_i = E(a_i)/D'(a_i)$ if $D(a_i) = 0$.

Why does this work?

$\sum_i e_i/(x - a_i) = E/D$ and
$\sum_i c_i/(x - a_i) = 0$ in $\mathbf{F}_{2^m}[x]/g$
so $s = E/D$ in $\mathbf{F}_{2^m}[x]/g$
so $(D, E\sqrt{x}) \in L$.

Why does this work?

$\sum_i e_i/(x - a_i) = E/D$ and
$\sum_i c_i/(x - a_i) = 0$ in $\mathbf{F}_{2^m}[x]/g$
so $s = E/D$ in $\mathbf{F}_{2^m}[x]/g$
so $(D, E\sqrt{x}) \in L$.

$(D, E\sqrt{x})$ is a short vector:
$\deg(D, E\sqrt{x}) \le |e| \le (\deg g)/2$
$< \deg g + 1/2 - \deg(q_j, r_j\sqrt{x})$.

Why does this work?

$\sum_i e_i/(x - a_i) = E/D$ and
$\sum_i c_i/(x - a_i) = 0$ in $\mathbf{F}_{2^m}[x]/g$
so $s = E/D$ in $\mathbf{F}_{2^m}[x]/g$
so $(D, E\sqrt{x}) \in L$.

$(D, E\sqrt{x})$ is a short vector:
$\deg(D, E\sqrt{x}) \le |e| \le (\deg g)/2$
$< \deg g + 1/2 - \deg(q_j, r_j\sqrt{x})$.

Recall "shortest" proof:
$(D, E\sqrt{x}) \in (q_j, r_j\sqrt{x})\mathbf{F}_{2^m}[x]$,
so $E/D = r_j/q_j$. Done!

Euclid decoding: 1975 Sugiyama–Kasahara–Hirasawa–Namekawa.

List decoding for these codes

What if $|e| > (\deg g)/2$?

Find shortest nonzero $(D_0, E_0\sqrt{x})$
and independent $(D_1, E_1\sqrt{x})$ in
$(0, g\sqrt{x})\mathbf{F}_{2^m}[x] + (1, s\sqrt{x})\mathbf{F}_{2^m}[x]$,
with degrees $(\deg g)/2 - \delta$
and $(\deg g)/2 + 1/2 + \delta$
for some $\delta \in \{0, 1/2, 1, 3/2, \ldots\}$.

Know that $(D, E\sqrt{x}) =$
$u(D_0, E_0\sqrt{x}) + v(D_1, E_1\sqrt{x})$;
$v = \pm(ED_0 - DE_0)/g \in \mathbf{F}_{2^m}[x]$,
$u = \pm(DE_1 - ED_1)/g \in \mathbf{F}_{2^m}[x]$,
$\deg v \le |e| - (\deg g)/2 - 1/2 - \delta$,
$\deg u \le |e| - (\deg g)/2 + \delta$.

Critical facts about D:

- $D = uD_0 + vD_1$ with known D_0 and D_1, bounded u and v.
- D divides known $N = \prod_i (x - a_i)$.

Critical facts about D:

- $D = uD_0 + vD_1$ with known D_0 and D_1, bounded u and v.
- D divides known $N = \prod_i (x - a_i)$.

This is exactly the "linear combinations as divisors" problem! Solve with lattices.

Reach same $|e|$ as GS, but much smaller k.

(2007 Wu: dual of essentially this algorithm; see 2008 Bernstein for coprimality)

Jet list decoding

Recall $D = \prod_{i:e_i \neq 0}(x - a_i)$
and $E = \sum_i De_i/(x - a_i)$.

$e_i \in \{0, 1\}$
so $E = \sum_i D/(x - a_i) = D'$.

One consequence:
$\Gamma_2(g) = \Gamma_2(g^2)$ if g is squarefree.
This doubles $\deg g$, drastically
increasing # errors decoded.

But $\Gamma_2(g^2)$ decoders vary
in effectiveness and efficiency.

1968 Berlekamp decodes
$\deg g$ errors for $\Gamma_2(g^2)$.
1975 Patterson: same, faster.

1998 Guruswami–Sudan:
$\approx \deg g + (\deg g)^2/2n$ errors.
2007 Wu: same, faster;
the “rational” speedup.
2008 Bernstein: even faster;
“rational” + Patterson.

1968 Berlekamp decodes
$\deg g$ errors for $\Gamma_2(g^2)$.
1975 Patterson: same, faster.

1998 Guruswami–Sudan:
$\approx \deg g + (\deg g)^2/2n$ errors.
2007 Wu: same, faster;
the "rational" speedup.
2008 Bernstein: even faster;
"rational" + Patterson.

2001 Koetter–Vardy:
$\approx \deg g + (\deg g)^2/n$ errors.
Can "rational" algorithms
correct this many errors?

1968 Berlekamp decodes
$\deg g$ errors for $\Gamma_2(g^2)$.
1975 Patterson: same, faster.

1998 Guruswami–Sudan:
$\approx \deg g + (\deg g)^2/2n$ errors.
2007 Wu: same, faster;
the "rational" speedup.
2008 Bernstein: even faster;
"rational" + Patterson.

2001 Koetter–Vardy:
$\approx \deg g + (\deg g)^2/n$ errors.
Can "rational" algorithms
correct this many errors?
Yes! Jet list decoding.

Works for arbitrary $\Gamma_2(g)$.
Notation: $N, D, E, \ldots$ as before.

D divides N so the jet
$D(x+\epsilon) = D + \epsilon D' = D + \epsilon E$
divides $N(x+\epsilon) = N + \epsilon N'$.

$D + \epsilon E =$
$u(D_0 + \epsilon E_0) + v(D_1 + \epsilon E_1)$.

Apply the jet-divisors idea:
find large $\gcd\{N'D - NE, N^2\}$.

2007 Wu reaches same $|e|$
in one special case, BCH. Jet list
decoding is faster, more general.

Generalize $\mathbf{F}_2$ to $\mathbf{F}_q$: use
$\gcd\{(N'D)^{q-1} - (NE)^{q-1}, N^q\}$.