

HARD LATTICE PROBLEMS

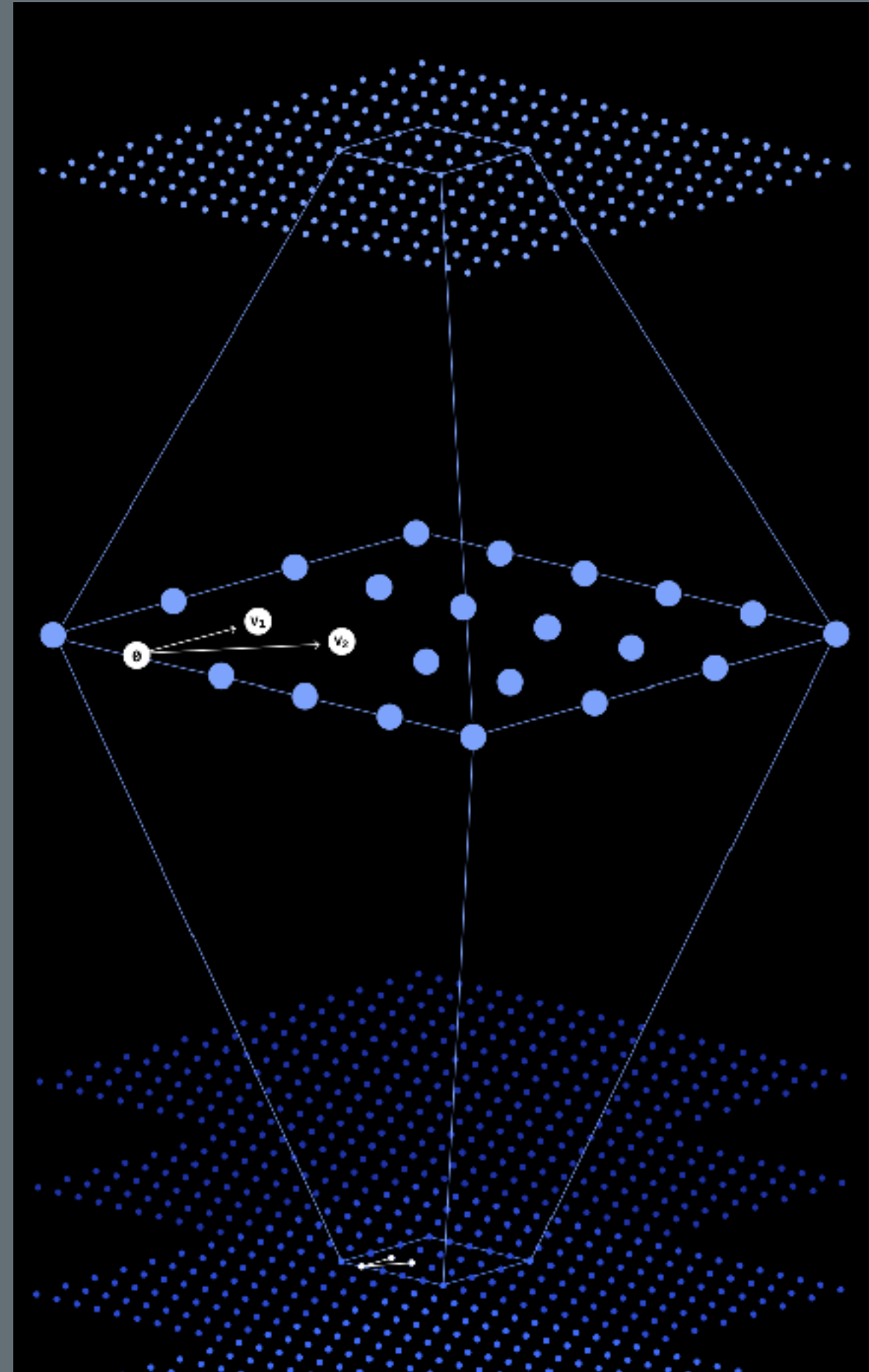
PHONG NGUYEN

<http://www.di.ens.fr/~pnguyen>

October 2026



LATTICE PROBLEMS



LATTICE ALGORITHMS

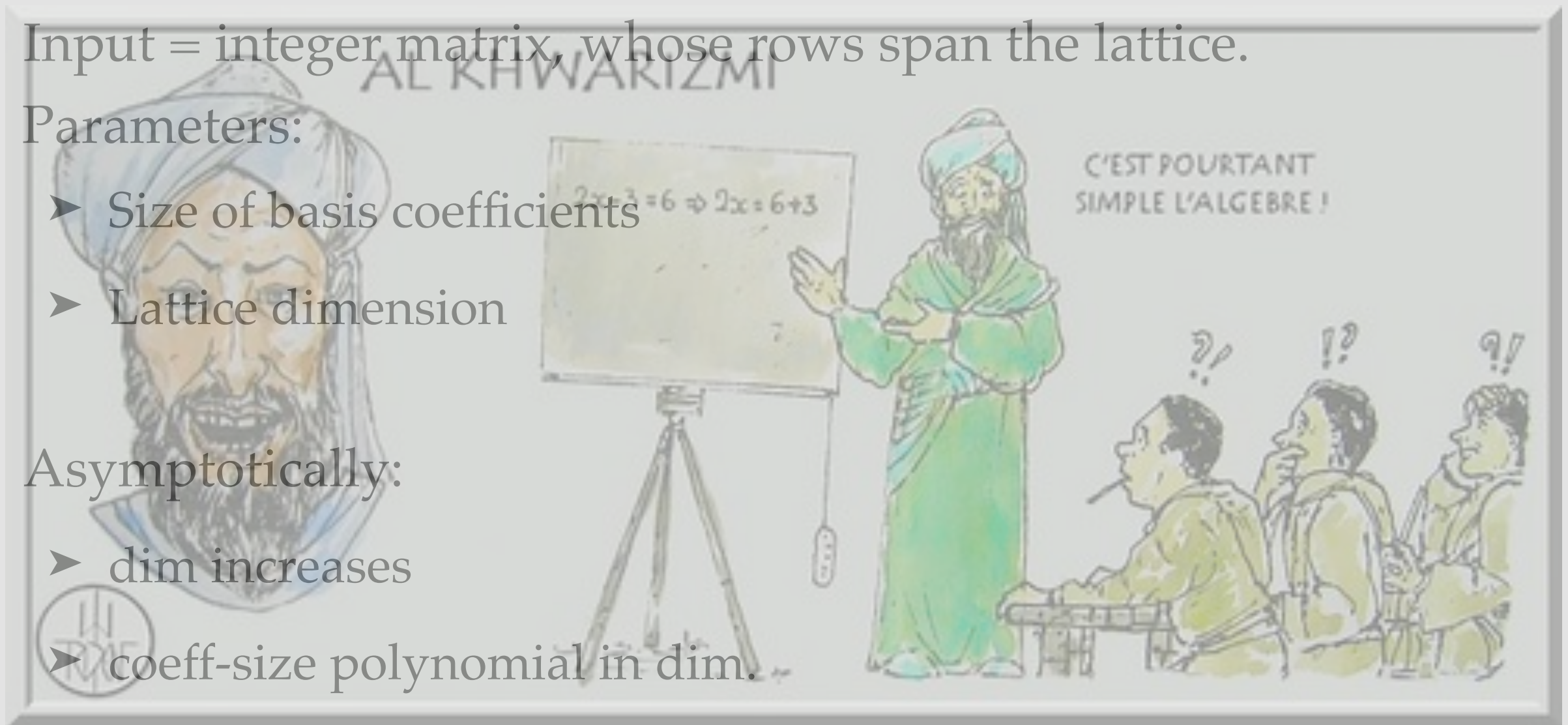
- Input = integer matrix, whose rows span the lattice.

Parameters:

- Size of basis coefficients
- Lattice dimension

- Asymptotically:

- dim increases
- coeff-size polynomial in dim.

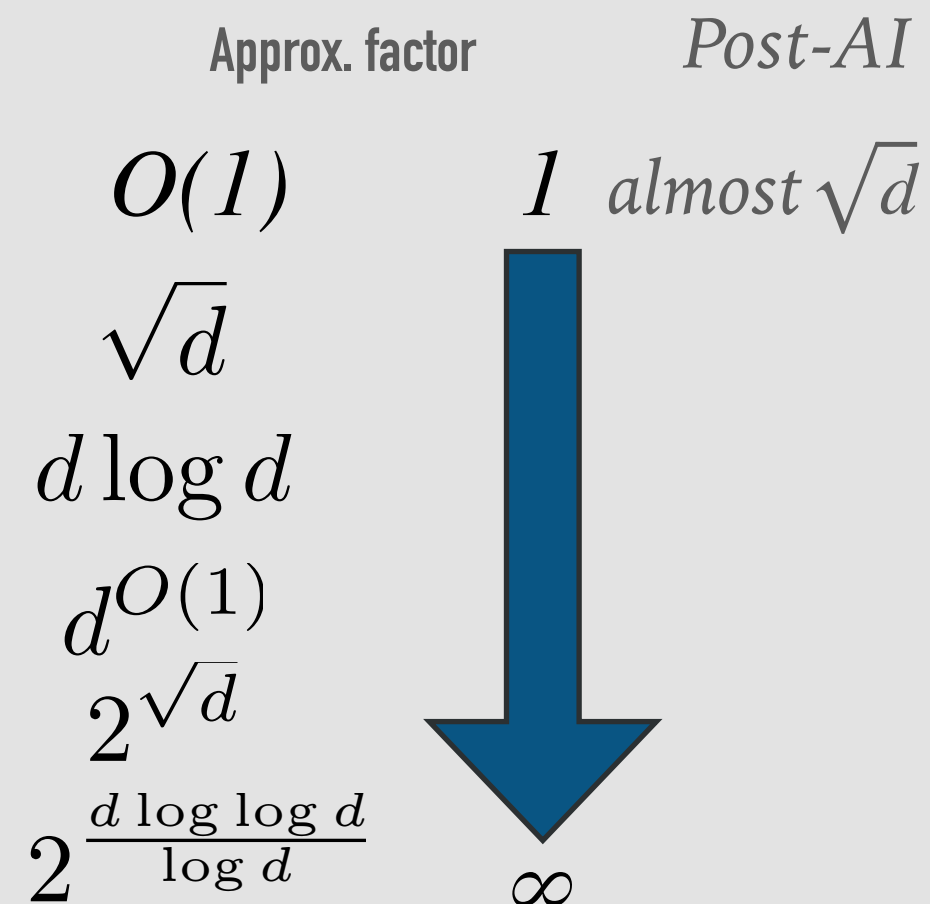


HARD LATTICE PROBLEMS

- Since 1996, lattices are very trendy in classical and quantum complexity theory.

- Depending on the dimension d :

- **exp-time** algorithms and NP-hardness
- non NP-hardness ($\text{NP} \cap \text{co-NP}$)
- worst-case / average-case reduction
- cryptography
- **subexp-time** algorithms
- **poly-time** algorithms



WHAT HAPPENED IN AUGUST?



Chris Peikert
@ChrisPeikert



WOW!! 🤯

Among many jaw-dropping results, this proves NP-hardness of the Closest Vector and Nearest Codeword Problems for *polynomial* approximation factors, for the first time ever, and via a totally new approach (Reed-Solomon techniques). Amazing!



Chris Peikert
@ChrisPeikert



2/ Strangely, Astra didn't optimize the polynomial approx factor!

1min with GPT-5.6 suggests that n^c -CVP is hard for **any $c < 1/14$ ** (not just $c=1/400$), simply by tightening up the bookkeeping.

(Recall that $c=1/2$ is a fundamental barrier, where n^c -CVP is in $NP \setminus coNP$.)



Mira ✓
@_Mira__Mira_



x.com/_Mira__Mira_/...

I got it up to $1/2$. Your comment about it being completely unoptimized inspired me to give it a try.



Mira ✓ @_Mira__Mira_ · Aug 9

Replying to @_Mira__Mira_
github.com/Mira-acc/cvp

"This repository contains the Lean 4 formalization of NP-hardness of integer-target GapCVP with approximation factor N^c for every fixed real constant $0 < c < 1/2$..."



Mira ✓
@_Mira__Mira_

Joined February 2023 >



Mira ✓ @_Mira__Mira_ · Oct 2



@grok Generate an image of Mira Future World Ruler and the establishment of Miratopia, Grand Capital City of the Miran Empire.

HARD LATTICE PROBLEMS

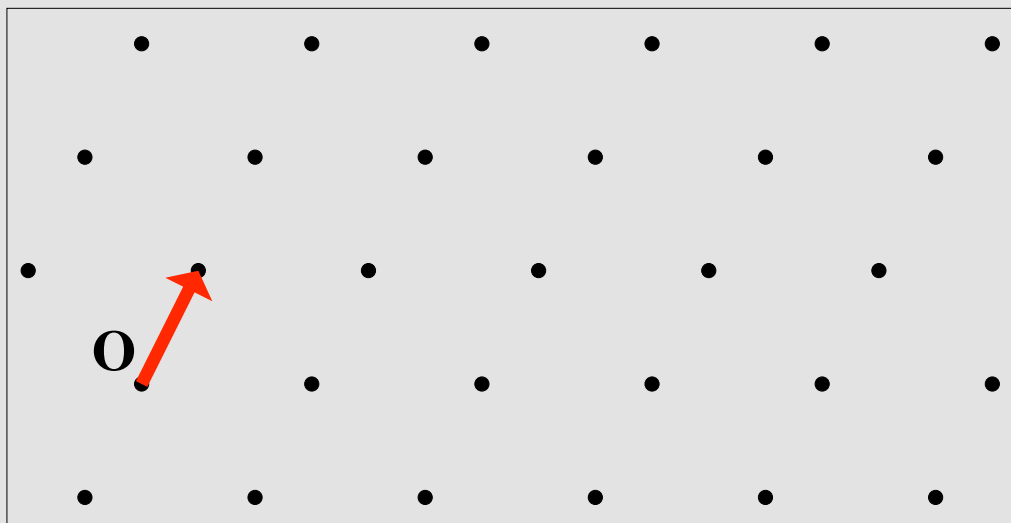
- Input: a lattice L and an n -dim ball C .
- Output: decide if $L \cap C$ is non-trivial, and find a point when applicable. Easy if $L = \mathbb{Z}^n$.
- Two settings
 - Approx: $L \cap C$ has **many points**.
Ex: SIS and ISIS.
 - Unique: **only one non-trivial point**.
Ex: BDD.

THE SHORTEST VECTOR PROBLEM



THE SHORTEST VECTOR PROBLEM (SVP)

- Input: a basis of a d -dim lattice L .
- Output: nonzero $v \in L$ minimizing $\|v\|$ i.e. $\|v\| = \lambda_1(L)$



2	0	0	0	0
0	2	0	0	0
0	0	2	0	0
0	0	0	2	0
1	1	1	1	1

THE SHORTEST VECTOR PROBLEM (SVP): DECISIONAL VARIANT

- Input: a basis of a d -dim lattice L and a rational number r
- Output: is there $v \in L$ such that $\|v\| \leq r$, i.e. is $\lambda_1(L) \leq r$?

THE SHORTEST VECTOR PROBLEM (SVP): OPTIMIZATION VARIANT

- Input: a basis of a d -dim lattice L and a rational number r
- Output: the integer $\lambda_1(L)^2$

EXERCISE

- Show that given an oracle for Decisional-SVP, one can solve Optimization-SVP and SVP in polynomial time.
- Lagrange's algorithm shows how to solve rank-2 SVP in polynomial time : we will see it soon.

RELAXING SVP

- Input: a basis of a d -dim lattice L .
- Output: nonzero $v \in L$ such that:

➤ **Approximate-SVP:** $\|v\| \leq f(d) \lambda_1(L)$ [relative]



➤ **Hermite-SVP:** $\|v\| \leq g(d) \text{vol}(L)^{1/d}$ [absolute]

GAP-SVP

- Input: a basis of a d -dim lattice L and rational number r and gap γ
- Output: decide if $\lambda_1(L) \leq r$ or $\lambda_1(L) \geq \gamma r$ (we are promised to be in either situation)

LATTICE CHALLENGES

WILMINGTON, MA (PRWEB) FEBRUARY 05, 2015

Security
understa
security a
users of

Access to

The Chal
paramete
consists
a few mo

The prize
solution
chosen f
conferen

latticechallenge.org/svp-challenge/halloffame.php



SVP CHALLENGE

HALL OF FAME

Position	Dimension	Euclidean Norm	Seed	Contestant	Solution	Algorithm	Subm. Date	Approx. Factor
1	210	3808	0	Jintai Ding, Ziyu Zhao	vec	Sieving	2026-01-1	1.04497
2	200	3723	0	Ziyu Zhao, Jintai Ding	vec	Sieving	2025-03-4	1.04865
3	192	3595	0	Shi Bai, Yuanmi Chen, Jiangxia Ge, Yituo He, Xiangxue Li, Chao Sun, Yu Yu	vec	Sieving	2026-09-17	1.03159
4	190	3613	0	Yao Sun and Shuai Chang	vec	Sieving	2024-07-21	1.04237
5	188	3582	0	Leizhang Wang, Lin Wang, Baocang Wang, Geng Wang, Huiwen Jia	vec	Sieving	2025-03-12	1.03823

THE SVP CHALLENGE

- Each SVP challenge gives an $n \times n$ lower-triangular basis

$$\begin{pmatrix} p & 0 & & \dots & 0 \\ a_1 & 1 & \ddots & & \vdots \\ a_2 & 0 & 1 & \ddots & \\ \vdots & \vdots & \ddots & \ddots & 0 \\ a_{n-1} & 0 & \dots & 0 & 1 \end{pmatrix}$$

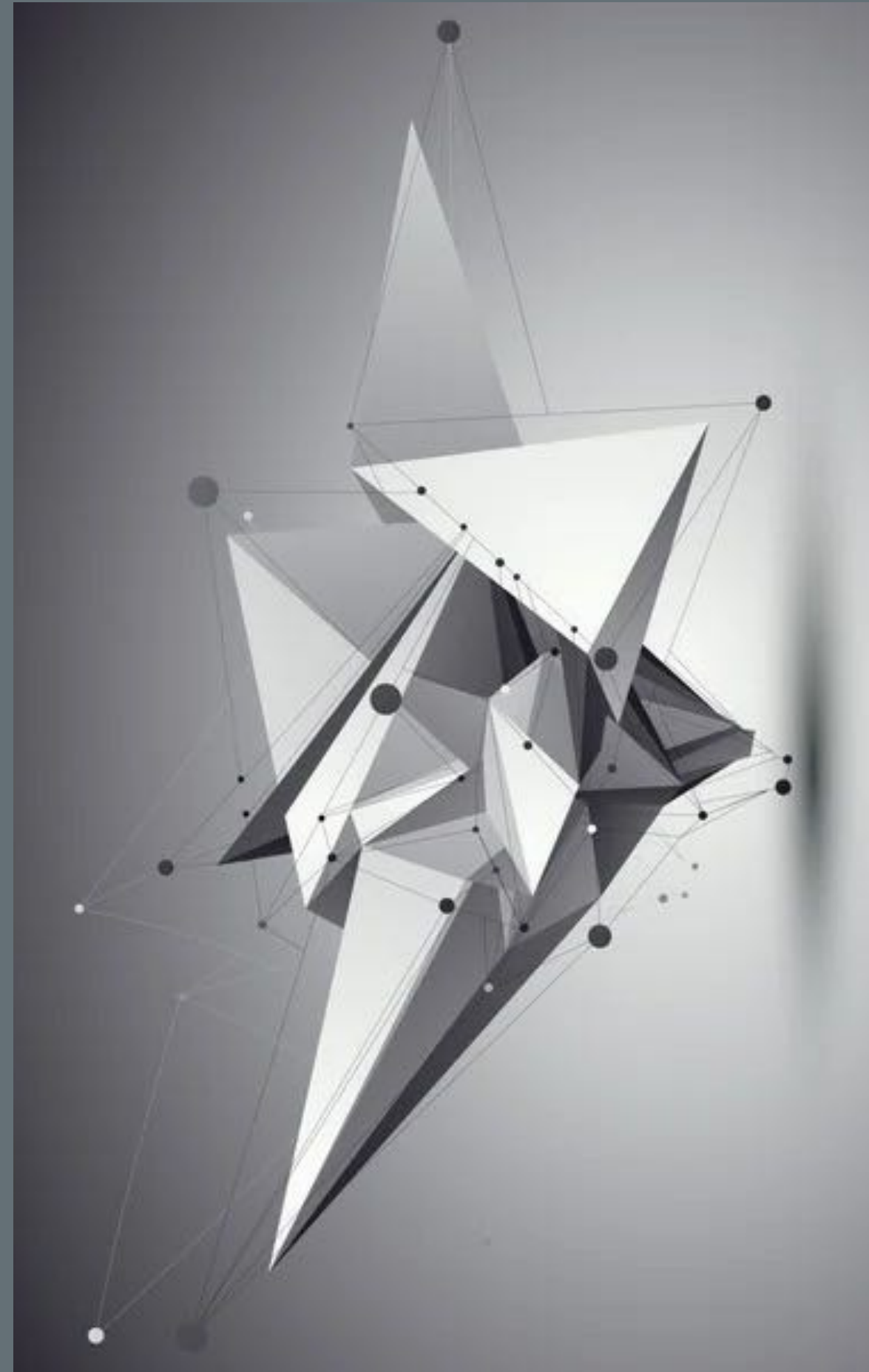
- p is a $10n$ -bit prime, $0 \leq a_i < p$
- What is the rank and covolume of this lattice?

- The lattice is the set of $(x_0, x_1, \dots, x_{n-1}) \in \mathbb{Z}^n$ such that $x_0 - \sum_{i=1}^{n-1} x_i a_i \equiv 0 \pmod{p}$

- The challenge asks to find a non-zero lattice vector of norm

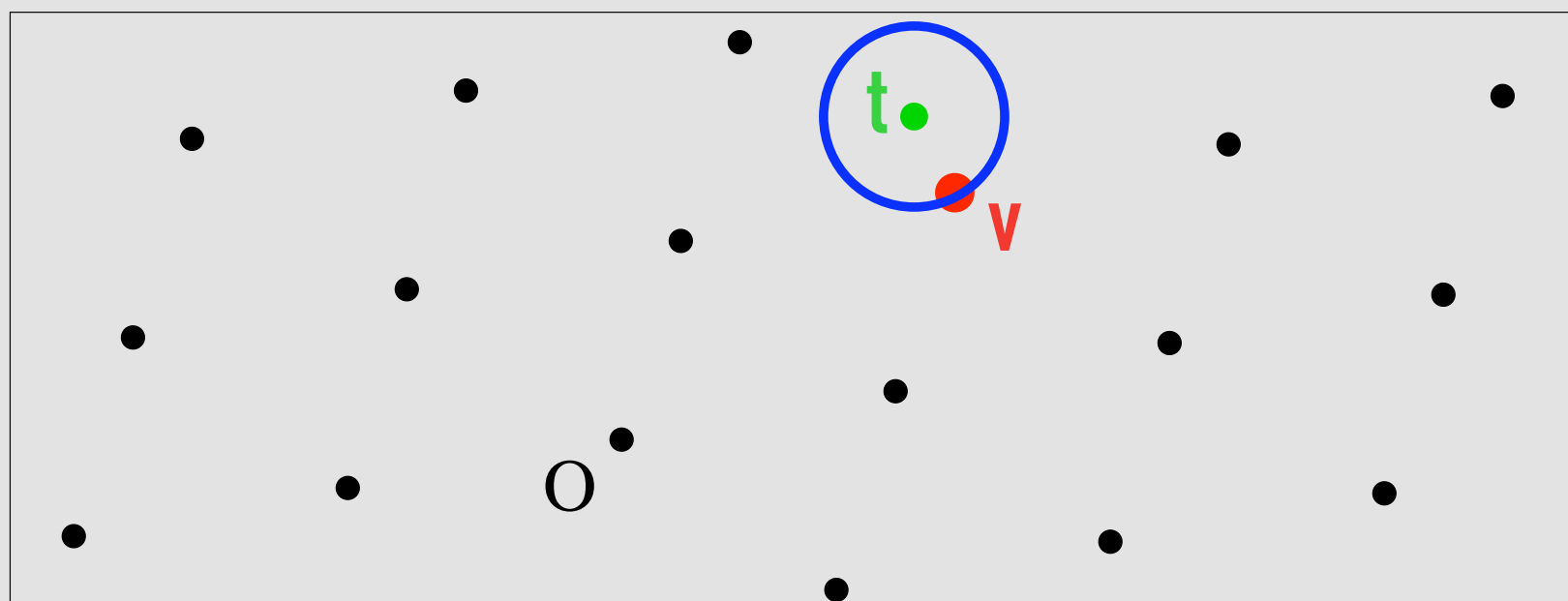
$$1.05 \times \frac{\Gamma(n/2 + 1)^{1/n}}{\sqrt{\pi}} \times p^{1/n} \approx 1.05 \sqrt{\frac{n}{2\pi e}} p^{1/n}$$

THE CLOSEST VECTOR PROBLEM



THE CLOSEST VECTOR PROBLEM (CVP)

- Input: a basis of a lattice L of dim d , and a target vector t .
- Output: $\mathbf{v} \in L$ minimizing $\|\mathbf{v} - t\|$, i.e. finding a shortest vector in the coset $t + L$.



- **BDD (bounded distance decoding)**: special case when t is very close to L .

EXERCISES

- Solve CVP for rank-1 lattices.
- CVP is NP-hard.
- SVP is not harder than CVP: if one can solve exact CVP, one can solve exact SVP.

COVERING RADIUS

- $\mu(L)$ is the largest distance $\text{dist}(x, L)$ where x runs over $\text{span}(L)$:
why is it reached for some x ?
 - Show that $\mu(L) \geq \lambda_1(L)/2$ and even $\mu(L) \geq \lambda_n(L)/2$.
 - Show that $\mu(L) \leq \sum_i \lambda_i(L)/2$

A FEW REDUCTIONS



DECISION-CVP IS NP-COMPLETE

- Subset sum: given integers $a_1, \dots, a_n$ and s , decide if $s = \sum_{i=1}^n x_i a_i$ where $x_i \in \{0,1\}$.

- Consider L spanned by $\begin{pmatrix} a_1 & 2 & 0 & \dots & 0 \\ a_2 & 0 & 2 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ a_n & 0 & \dots & 0 & 2 \end{pmatrix}$ and $\vec{t} = (s \quad 1 \quad \dots \quad 1)$

- Ask if $\text{dist}(\vec{t}, L) \leq \sqrt{n}$

SVP IS NOT HARDER THAN CVP

- Input: a basis $(\vec{b}_1, \dots, \vec{b}_n)$ of L
- Output: $\sum_{i=1}^n x_i \vec{b}_i$ of minimal non-zero norm
- For any solution, one of the x_i 's is odd: $x_i = 2y_i + 1$
- Then $\sum_{j \neq i} x_j \vec{b}_j + 2y_i \vec{b}_i \in L(\vec{b}_1, \dots, \vec{b}_{i-1}, 2\vec{b}_i, \vec{b}_{i+1}, \dots, \vec{b}_n)$ (sublattice of L) is a closest vector to $-\vec{b}_i$
- By calling n times a CVP-oracle, we solve SVP.

SEARCH-TO-DECISION CVP

- Input: a basis $(\vec{b}_1, \dots, \vec{b}_n)$ of L and a target $\vec{t}$
- Output: $\sum_{i=1}^n x_i \vec{b}_i$ minimizing $\| \sum_{i=1}^n x_i \vec{b}_i - \vec{t} \|$
- We can compute $\text{dist}(\vec{t}', L')$ for any $(\vec{t}', L')$.
- Let the sublattice $L_i = L(\vec{b}_1, \dots, \vec{b}_{i-1}, 2\vec{b}_i, \vec{b}_{i+1}, \dots, \vec{b}_n)$
- Check if $\text{dist}(\vec{t}, L) = \text{dist}(\vec{t}, L_1)$
 - Yes: There is a solution s.t. x_1 is even. We replace L by L_1 .
 - No: all solutions have odd x_1 , so we want to minimize $\|x_1(2\vec{b}_1) + \sum_{i=2}^n x_i \vec{b}_i - (\vec{t} + \vec{b}_1)\|$, so we replace $(\vec{t}, L)$ by $(\vec{t} + \vec{b}_1, L_1)$
- By iterating, we obtain the full x_1 of one solution: we know we have removed all the bits of x_1 if $\text{dist}(\vec{t}, L) = \text{dist}(\vec{t}, L(\vec{b}_2, \dots, \vec{b}_n))$
- Now, replace $\vec{t}$ by $\vec{t} - x_1 \vec{b}_1$ and L by $L(\vec{b}_2, \dots, \vec{b}_n)$: this decreased the rank, and we can iterate.

DIMENSION TWO



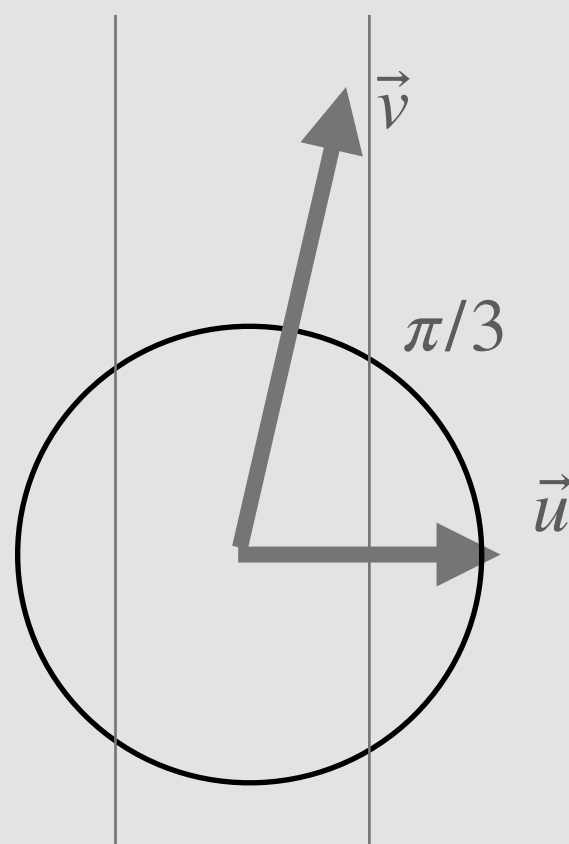
LAGRANGE'S REDUCTION (1773)

1. Lagrange reduction.

(**)

Let L be a two-rank lattice. A basis $(\vec{u}, \vec{v})$ of L is *Lagrange-reduced* if $\|\vec{u}\| \leq \|\vec{v}\|$ and $|\langle \vec{u}, \vec{v} \rangle| \leq \|\vec{u}\|^2/2$. Show that :

1. If $(\vec{u}, \vec{v})$ is reduced, then $\|\vec{u}\| = \lambda_1(L) \leq (4/3)^{1/4} \text{vol}(L)^{1/2}$ and $\|\vec{v}\| = \lambda_2(L)$.
 2. There exists a reduced basis $(\vec{u}, \vec{v})$ of L .
 3. There exists a lattice L such that $\lambda_1(L) = (4/3)^{1/4} \text{vol}(L)^{1/2}$.
-



LAGRANGE'S ALGORITHM

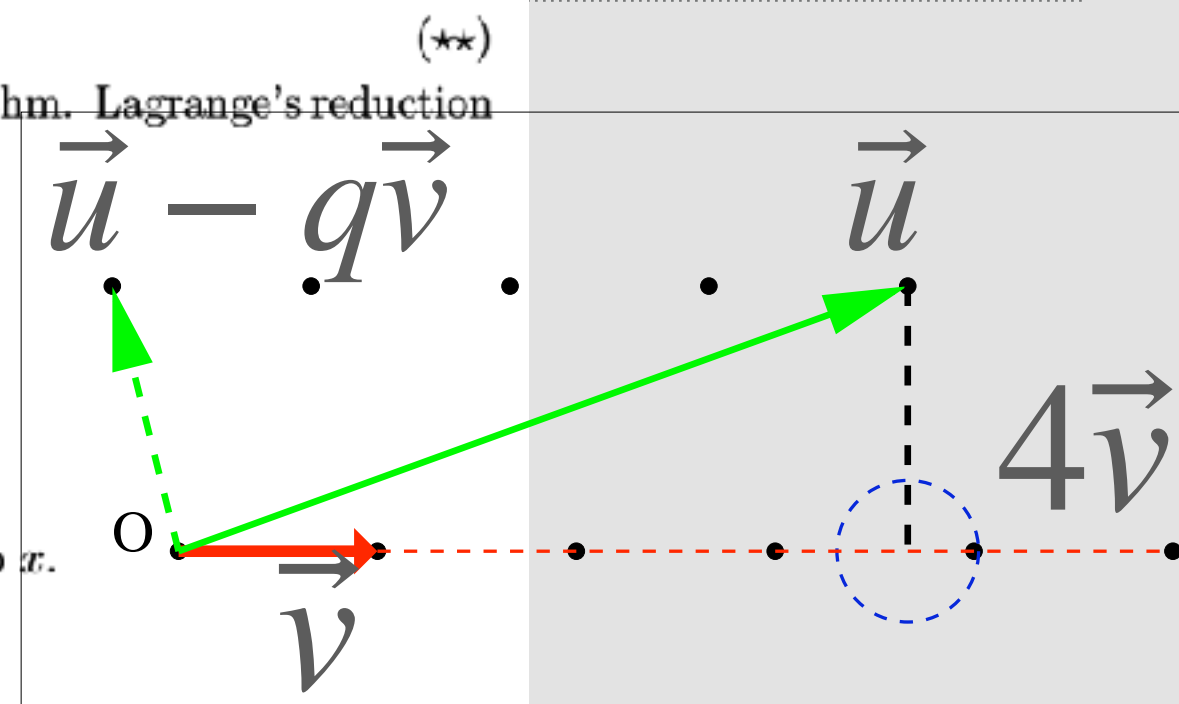
2. Lagrange's Algorithm.

In 1773, Lagrange published the following two-dimensional reduction algorithm. Lagrange's reduction algorithm.

Input: a basis $(\vec{u}, \vec{v})$ of a two-rank lattice L .

Output: a Lagrange-reduced basis of L .

- 1: **if** $\|\vec{u}\| < \|\vec{v}\|$ **then**
- 2: swap $\vec{u}$ and $\vec{v}$
- 3: **end if**
- 4: **repeat**
- 5: $\vec{r} \leftarrow \vec{u} - q\vec{v}$ where $q = \left\lfloor \frac{\langle \vec{u}, \vec{v} \rangle}{\|\vec{v}\|^2} \right\rfloor$ and $\lfloor x \rfloor$ denotes an integer closest to x .
- 6: $\vec{u} \leftarrow \vec{v}$
- 7: $\vec{v} \leftarrow \vec{r}$
- 8: **until** $\|\vec{u}\| \leq \|\vec{v}\|$
- 9: **Output** $(\vec{u}, \vec{v})$.



1. Consider Line 5 of Algorithm : show that this choice of $q \in \mathbb{Z}$ minimizes $\|\vec{u} - q\vec{v}\|$.
2. Show that Lagrange's algorithm terminates, i.e. that the repeat/until loop is not infinite, and that the output basis is Lagrange-reduced.
3. Consider the integer q of Step 5. Show that :
 - if $q = 0$, then this must be the last iteration of the loop.
 - if $|q| = 1$, then this must be either the first or last iteration of the loop.
4. Show that the number τ of iterations of the repeat/until loop is bounded by : $\tau = O(1 + \log B - \log \lambda_1(L))$ where B denotes the maximal Euclidean norm of the input basis vectors $\vec{u}$ and $\vec{v}$.
5. Show that when $L \subseteq \mathbb{Z}^n$, the bit-complexity of Lagrange's algorithm is polynomial in $\log B$.

KEY ARGUMENTS

- If $q=0$, then the basis is reduced by definition.
- If it is not the last iteration then $\|\vec{u} - q\vec{v}\| < \|\vec{v}\| < \|\vec{u}\|$.
 - If $|q|=1$, then $\|\vec{u} - q\vec{v}\| = \|\vec{v} - q\vec{u}\|$ so $\|\vec{v} - q\vec{u}\| < \|\vec{v}\|$ which means that $\vec{v}$ could be shortened by $\vec{u}$. This can only happen at the first iteration.
- Except maybe the first and last iteration, we always have $|q| \geq 2$.
 - Then $\mu = \frac{\langle \vec{u}, \vec{v} \rangle}{\|\vec{v}\|^2}$ satisfies $|\mu| \geq 3/2$.
 - But $\mu\vec{v}$ is the projection of $\vec{u}$ over $\text{span}(\vec{v})$ so $\|\vec{u}\|^2 \geq \|\mu\vec{v}\|^2 \geq \frac{9}{4}\|\vec{v}\|^2$
therefore $\|\vec{v}\|^2 \leq \frac{4}{9}\|\vec{u}\|^2$: the norms decrease geometrically!

RANDOM INSTANCES



RANDOM INSTANCES

- Which distributions of integer lattices (SVP and CVP) and target (CVP/BDD)?
- A full-rank integer lattice $L \subseteq \mathbb{Z}^m$ defines a finite Abelian group $\mathbb{Z}^m/L$. Two different lattices can define the same quotient.
- Can we fix a quotient, then generate a random lattice with that quotient? Is it hard to find short vectors in such a random lattice?

THE SIS PROBLEM (1996): SMALL INTEGER SOLUTIONS



Miklós Ajtai

- Let $(G, +)$ be a finite Abelian group: $G = (\mathbb{Z} / q\mathbb{Z})^n$ in [A]. View G as a $\mathbb{Z}$ -module.
- Pick $g_1, \dots, g_m$ uniformly at random from G .
- Goal: Find short $(\mathbf{x}_1, \dots, \mathbf{x}_m) \in \mathbb{Z}^m$ s.t. $\sum_i \mathbf{x}_i g_i = 0$,
e.g. $\|\mathbf{x}\| \leq \sqrt{m}(\#G)^{1/m}$.
- This is essentially finding a short vector in a (uniform) **random lattice** of $L_m(G) = \{ \text{lattices } L \subseteq \mathbb{Z}^m \text{ s.t. } \mathbb{Z}^m / L \sim G \}$.

EX: CYCLIC G

- Let $G = \mathbf{Z} / q\mathbf{Z}$
 - Pick $g_1, \dots, g_m$ uniformly at random mod q .
 - Goal: Find short $\mathbf{x} = (\mathbf{x}_1, \dots, \mathbf{x}_m) \in \mathbf{Z}^m$ s.t. $\sum_i \mathbf{x}_i g_i \equiv 0 \pmod{q}$.
- This is finding a short lattice vector for random lattices L such that $\mathbf{Z}^m / L \sim \mathbf{Z} / q\mathbf{Z}$.

SIS AND LWE

2444	2471	2498	1900	27	54	81	108	135	162	189	216
2470	2497	1899	1901	53	80	107	134	161	188	215	242
2496	1898	1925	1927	79	103	133	160	187	214	241	268
1897	1924	1926	1953	105	132	159	186	213	240	267	294
1923	1950	1952	1979	131	158	185	212	239	266	293	320
1949	1951	1978	2005	157	184	211	238	265	292	319	346
1975	1977	2004	2031	183	210	237	264	291	318	345	372
1976	2003	2030	2057	209	233	263	290	317	344	371	398
2002	2029	2056	2083	235	262	289	316	343	370	397	424
2028	2055	2082	2109	261	288	315	342	369	396	423	450
2054	2081	2108	2135	287	314	341	368	395	422	449	451
2080	2107	2134	2161	2188	340	367	394	421	448	475	477
2106	2133	2160	2187	339	363	393	420	447	474	476	503
2132	2159	2186	2213	365	392	419	446	473	500	502	529
2158	2185	2212	2239	391	418	445	472	499	501	528	555
2184	2211	2238	2265	417	444	471	498	525	527	554	581
2210	2237	2264	2291	443	470	497	524	526	553	580	607
2236	2263	2290	2317	469	493	523	550	552	579	606	8
2262	2289	2316	2343	495	522	549	551	578	605	7	34
2288	2315	2342	2369	521	548	575	577	604	8	33	60
2314	2341	2368	2395	547	574	576	603	5	32	59	86
2340	2367	2394	2421	573	600	602	4	31	58	85	112
2366	2393	2420	2447	599	601	3	30	57	84	111	138
2392	2419	2446	2473	625	2	29	56	83	110	137	164
543	570	597	624	1876	1903	1930	1957	1984	2011	2038	2065
569	596	623	25	1902	1929	1956	1983	2010	2037	2064	2091
595	622	24	26	1928	1955	1982	2009	2036	2063	2090	2117
621	23	50	52	1954	1981	2008	2035	2062	2089	2116	2143
22	49	51	78	1980	2007	2034	2061	2088	2115	2142	2169
48	75	77	104	2006	2033	2060	2087	2114	2141	2168	2195
74	76	103	130	2032	2059	2086	2113	2140	2167	2194	2221
100	102	129	156	2058	2085	2112	2139	2166	2193	2220	2247
101	128	155	182	2084	2111	2138	2165	2192	2219	2246	2273
127	154	181	208	2110	2137	2164	2191	2218	2245	2272	2299
153	180	207	234	2136	2163	2190	2217	2244	2271	2298	2325
179	206	233	260	2162	2189	2216	2243	2270	2297	2324	2352
205	232	259	286	313	2215	2242	2269	2296	2323	2350	2352
231	258	285	312	2214	2241	2268	2295	2322	2349	2351	2378
257	284	311	338	2240	2267	2294	2321	2348	2375	2377	2404
283	310	337	364	2266	2293	2320	2347	2374	2376	2403	2430
309	336	363	390	2292	2319	2346	2373	2400	2402	2429	2456
335	362	389	416	2318	2345	2372	2399	2401	2428	2455	2482
361	388	415	442	2344	2371	2398	2425	2427	2454	2481	1883
387	414	441	468	2370	2397	2424	2426	2453	2480	1882	1909
413	440	467	494	2396	2423	2450	2452	2479	1881	1908	1935
439	466	493	520	2422	2449	2451	2478	1880	1907	1934	1961
465	492	519	546	2448	2475	2477	1879	1906	1933	1960	1987
491	518	545	572	2474	2476	1878	1905	1932	1959	1986	2013
517	544	571	598	2500	1877	1904	1931	1958	1985	2012	2039

WORST-CASE TO AVERAGE-CASE REDUCTION

- [Ajtai96]: If one can efficiently solve SIS for $G=(\mathbb{Z}/q_n\mathbb{Z})^n$ on the average, then one can efficiently find short vectors in every n -dim lattice.
- [GINX16]: This can be generalized to any sequence (G_n) of finite abelian groups, provided that $\#G_n$ is sufficiently large $\geq n^{\Omega(\max(n, \text{rank}(G)))}$ and m too. Ex: $(\mathbb{Z}/2\mathbb{Z})^n$ is not.

Generating Hard Instances of Lattice Problems

Extended abstract

M. Ajtai

IBM Almaden Research Center

650 Harry Road, San Jose, CA, 95120

e-mail: ajtai@almaden.ibm.com

ABSTRACT. We give a random class of lattices in $\mathbb{Z}^n$ so that, if there is a probabilistic polynomial time algorithm which finds a short vector in a random lattice with a probability of at least $\frac{1}{2}$ then there is also a probabilistic polynomial time algorithm which solves the following three lattice problems in every lattice in $\mathbb{Z}^n$ with a probability exponentially close to one. (1) Find the length of a shortest nonzero vector in an n -dimensional lattice, approximately, up to a polynomial factor. (2) Find the shortest nonzero vector in an n -dimensional lattice L where the shortest vector v is unique in the sense that any other vector whose length is at most $n^c\|v\|$ is parallel to v , where c is a sufficiently large absolute constant. (3) Find a basis $b_1, \dots, b_n$ in the n -dimensional lattice L whose length, defined as $\max_{i=1}^n \|b_i\|$, is the smallest possible up to a polynomial factor.

THE SIS ONE-WAY FUNCTION

- Let $(G, +)$ be a finite Abelian group
- Pick $g_1, \dots, g_m$ uniformly at random from G .
- Let f : short $(\mathbf{x}_1, \dots, \mathbf{x}_m) \in \mathbb{Z}^m \mapsto \sum_i \mathbf{x}_i g_i \in G$.
 - f is many-to-one.
 - Given $h = \sum_i \mathbf{y}_i g_i \in G$, finding a short $(\mathbf{x}_1, \dots, \mathbf{x}_m) \in \mathbb{Z}^m$ s.t. $h = \sum_i \mathbf{x}_i g_i \in G$ is as hard as SIS.

DUALITY

- Remember the SIS lattice:
 - $g_1, \dots, g_m$ in some finite Abelian group $(G, +)$
 - $L = \{\mathbf{x} = (\mathbf{x}_1, \dots, \mathbf{x}_m) \in \mathbb{Z}^m \text{ s.t. } \sum_i \mathbf{x}_i g_i = 0\}$
- The **dual lattice** of L is related to the dual group $G^\times$ of (additive) characters of G : morphisms from G to $\mathbf{T} = \mathbf{R} / \mathbf{Z}$
 - $L^\times = \{(\mathbf{y}_1, \dots, \mathbf{y}_m) \in \mathbf{R}^m \text{ s.t. for some } s \in G^\times, \text{ for all } i \mathbf{y}_i \equiv s(g_i) \pmod{1}\}$

WHY?

- Let $\mathbf{x} \in L$: $\mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}^m$ s.t. $\sum_i x_i g_i = 0$
- For any character s in $G^\times$, we have $s(\sum_i x_i g_i) = 0$ in $T = \mathbb{R} / \mathbb{Z}$ so $\sum_i x_i s(g_i) = 0$
- Hence, for any $(y_1, \dots, y_m) \in \mathbb{R}^m$ s.t. for all i $y_i \equiv s(g_i) \pmod{1}$, we have
$$\sum_{i=1}^m x_i y_i \in \mathbb{Z} \text{ so } (y_1, \dots, y_m) \in L^\times$$
- Reciprocally if $\sum_{i=1}^m x_i y_i \in \mathbb{Z}$ whenever $\sum_i x_i g_i = 0$, there is s in $G^\times$ s.t.
 $y_i \equiv s(g_i) \pmod{1}$ for all i . This defines s over the subgroup generated by the g_i 's: if $\sum_{i=1}^m a_i g_i = \sum_{i=1}^m b_i g_i$ then $s(\sum_{i=1}^m a_i g_i) = s(\sum_{i=1}^m b_i g_i)$ because
$$\sum_{i=1}^m (a_i - b_i) g_i = 0 \text{ implies that } \sum_{i=1}^m (a_i - b_i) y_i \in \mathbb{Z}$$

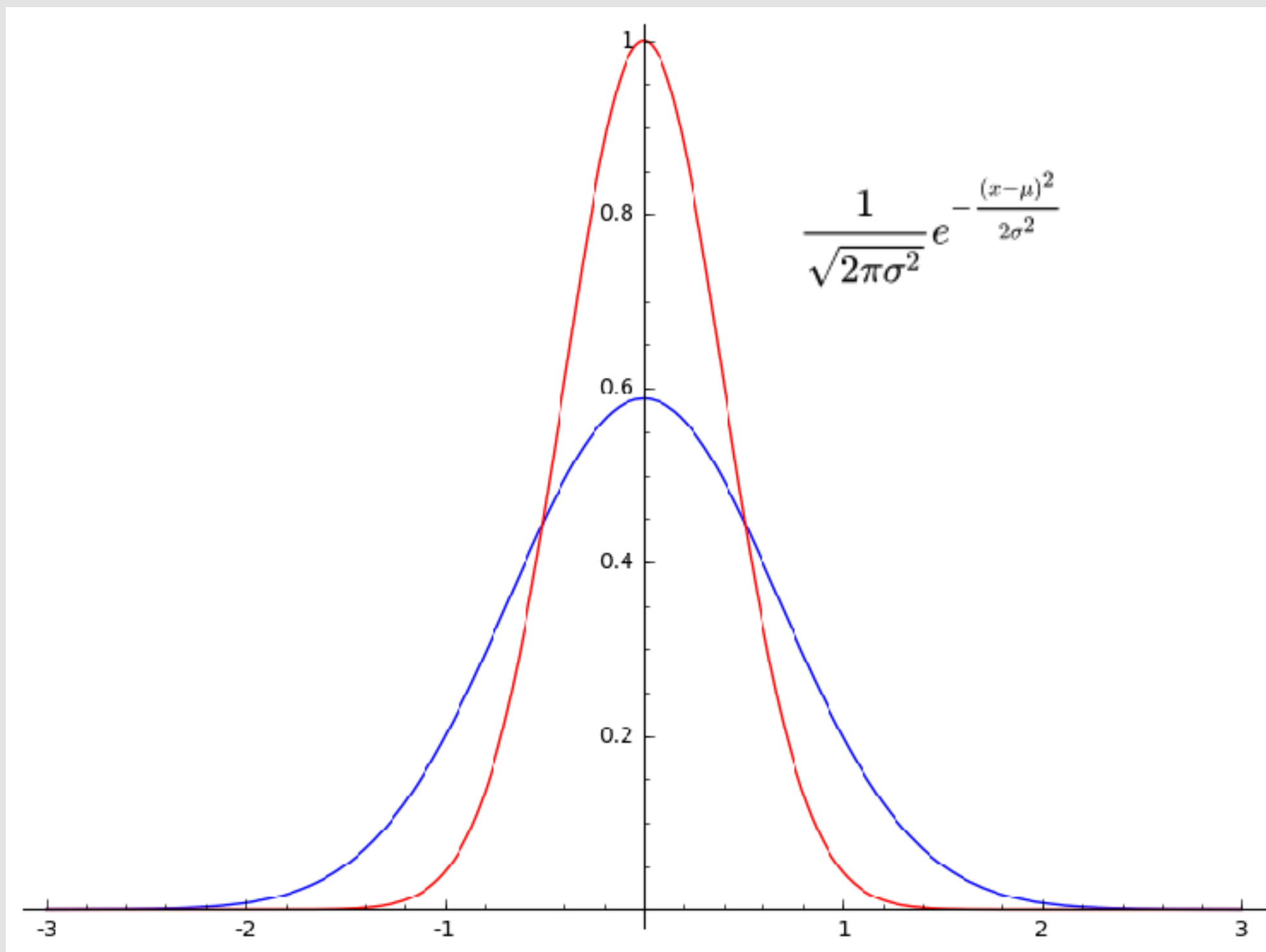
THE LWE PROBLEM: LEARNING (A CHARACTER) WITH ERRORS



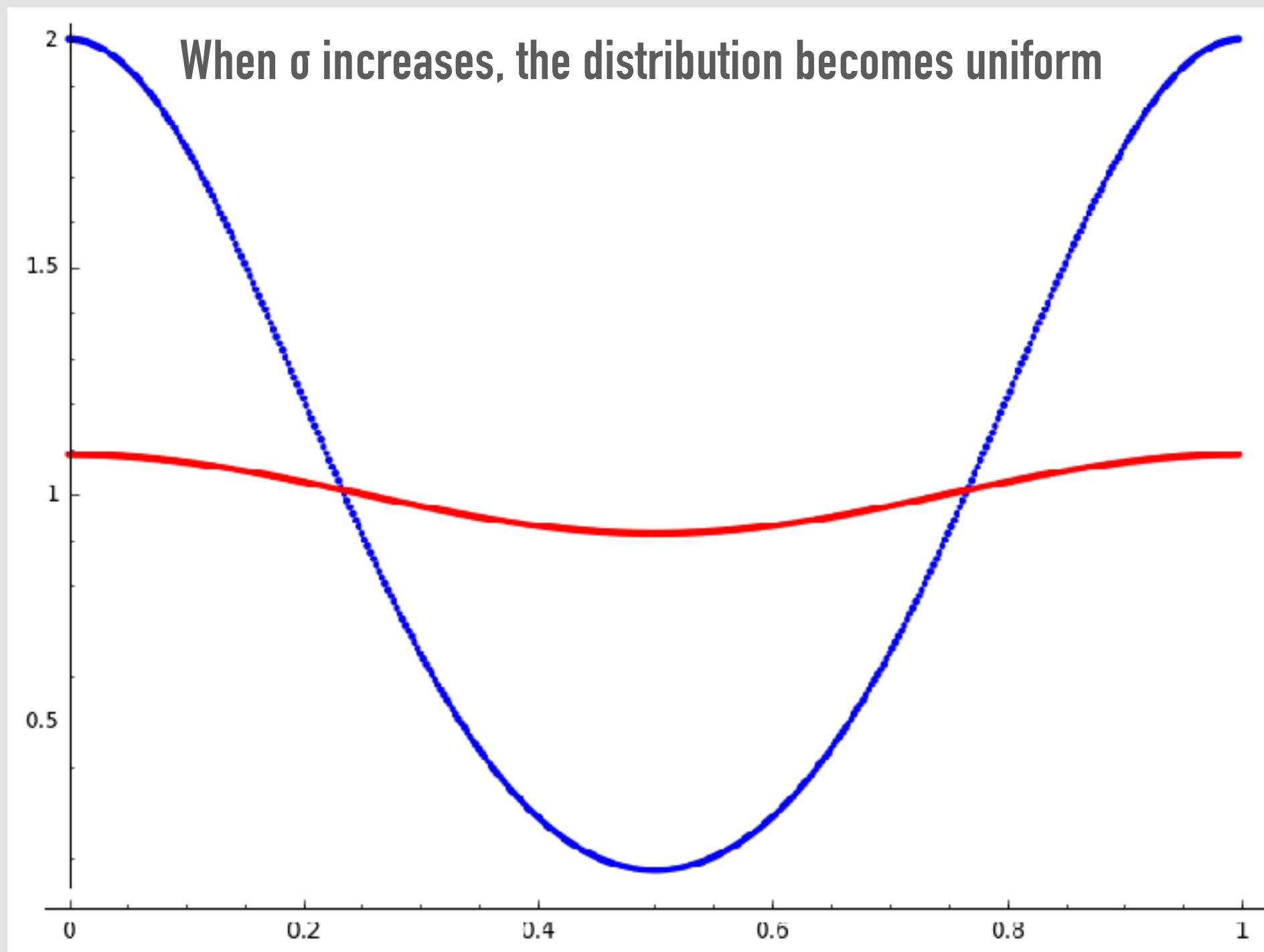
Oded Regev

- Let $(G, +)$ be any finite Abelian group e.g. $G = (\mathbb{Z}/p\mathbb{Z})^n$.
- Pick $g_1, \dots, g_m$ uniformly at random from G .
- Pick a random **character** s in $G^\times$.
- Goal: recover s given $g_1, \dots, g_m$ and **noisy** approximations of $s(g_1), \dots, s(g_m)$. Ex: Gaussian noise.

GAUSSIAN NOISE OVER R



GAUSSIAN NOISE OVER R/Z



EX: CYCLIC G

- Let $G = \mathbb{Z} / q\mathbb{Z}$
- Pick $g_1, \dots, g_m$ uniformly at random mod q .
- Goal: recover $s \in \mathbb{Z}$ given $g_1, \dots, g_m$ and randomized approximations of $sg_1 \bmod q, \dots, sg_m \bmod q$.
- This is exactly a randomized variant of Boneh-Venkatesan's **Hidden Number Problem** from CRYPTO '96.

HARDNESS OF LWE

- [Regev05]: If one can efficiently solve LWE for $G=(\mathbb{Z} / q_n \mathbb{Z})^n$ on the average, then one can **quantum**-efficiently find short vectors in **every n-dim** lattice.
- [GINX16]: This can be generalized to any sequence (G_n) of finite abelian groups, provided that **$\#G_n$ is sufficiently large**.