$\mathrm{GapSVP}_{\sqrt{n}}$ and $\mathrm{GapCVP}_{\sqrt{n}}$ are in $\mathrm{NP} \cap \mathrm{coNP}$

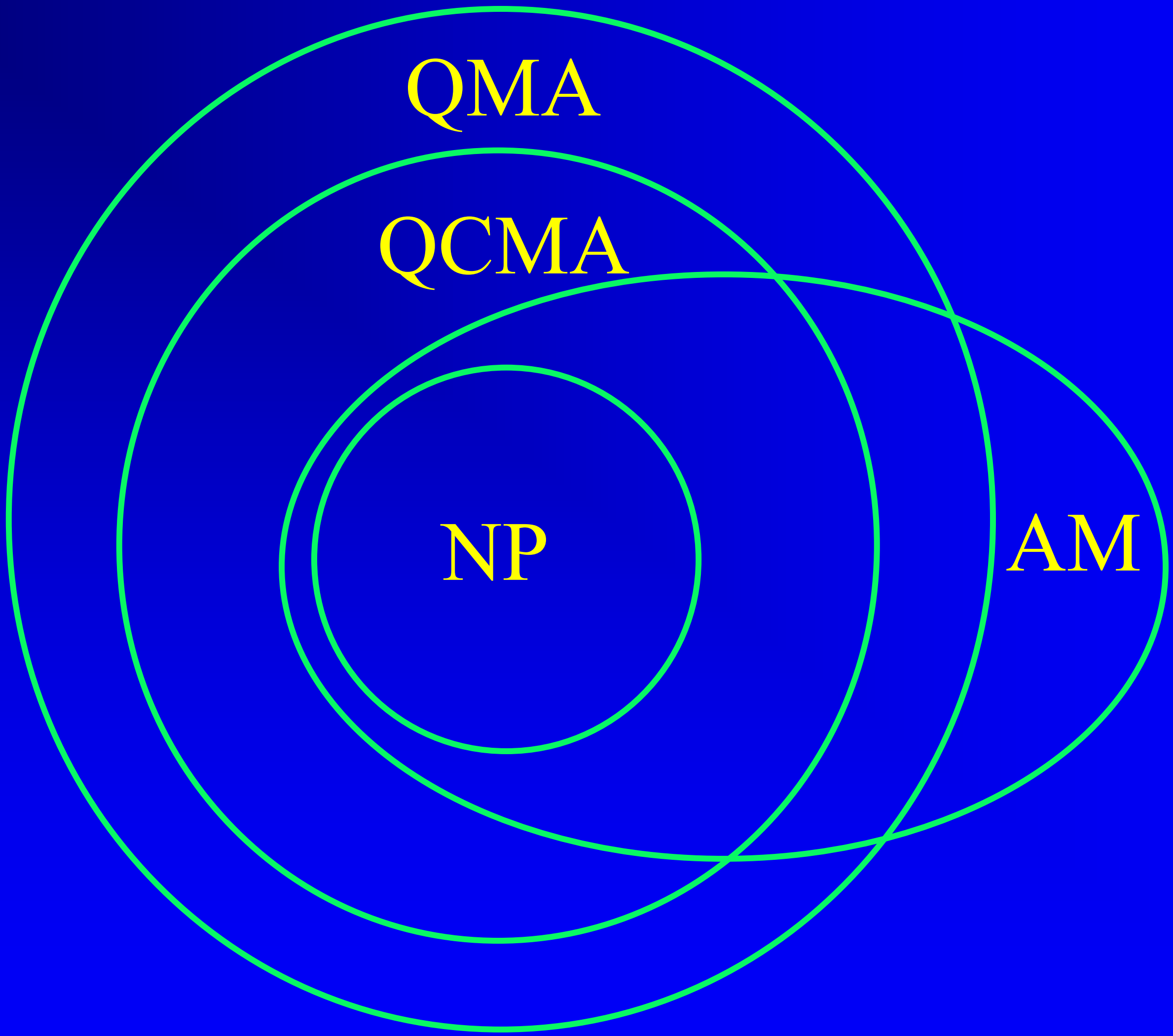
Dorit Aharonov

Oded Regev

NP, QCMA and QMA

- A language Λ2NP if 9 classical deterministic verifier V such that
  - 8 x 2 Λ 9 w, V accepts x,w
  - 8 x ∉ Λ 8 w, V rejects x,w
- A language Λ2QCMA if 9 quantum verifier V such that
  - 8 x 2 Λ 9 w, V accepts x,w w.p. > $\frac{3}{4}$
  - 8 x ∉ Λ 8 w, V accepts x,w w.p. < $\frac{1}{4}$
- A language Λ2QMA if 9 quantum verifier V such that
  - 8 x 2 Λ 9 |ηi, V accepts x,η w.p. > $\frac{3}{4}$
  - 8 x ∉ Λ 8 |ηi, V accepts x,η w.p. < $\frac{1}{4}$

NP, QCMA and QMA



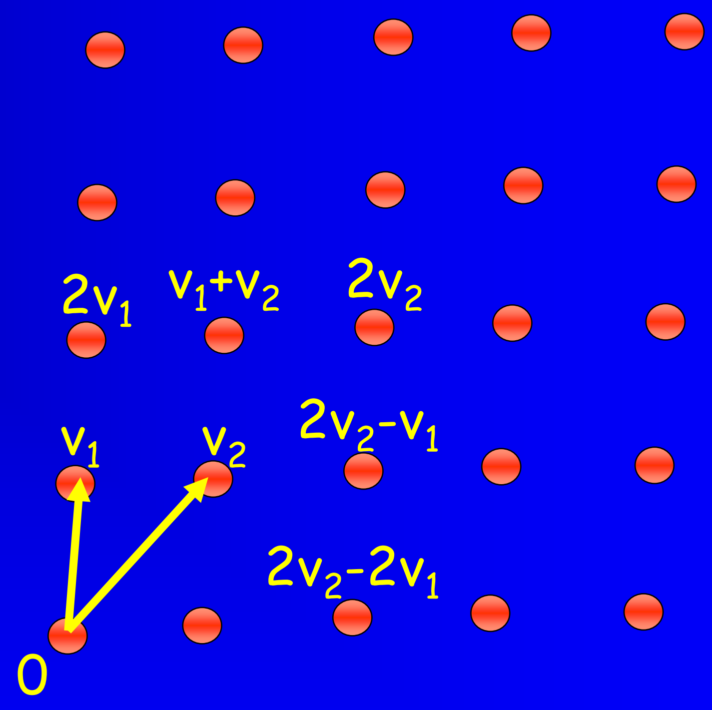
Lattices

- Basis:

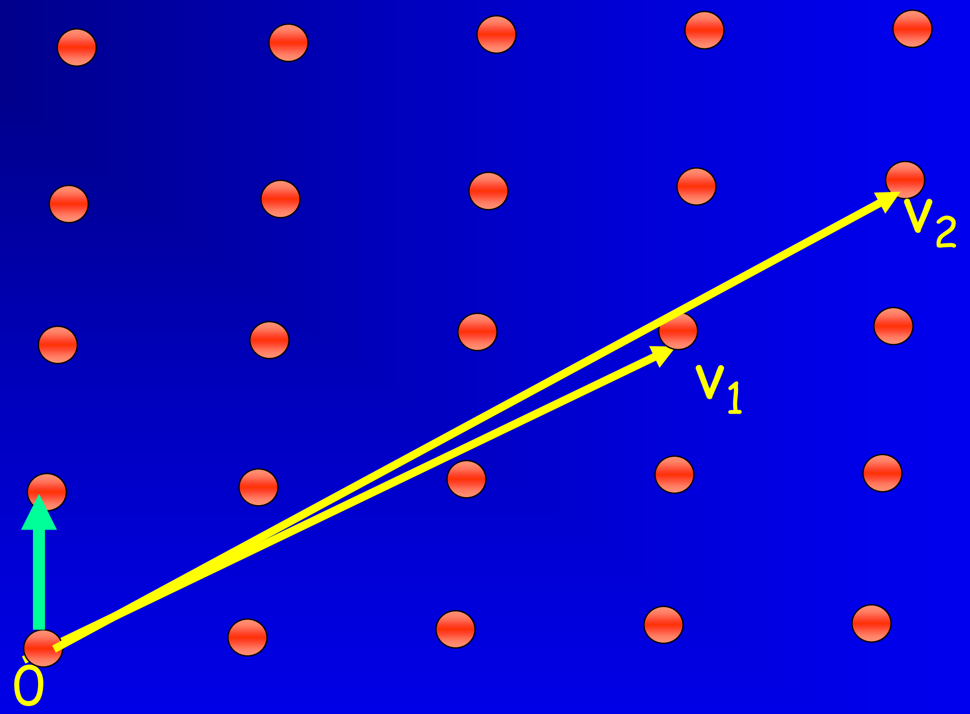
  $v_1,\ldots,v_n$ vectors in R^n

- The lattice is

  $L=\{a_1v_1+\ldots+a_nv_n \mid a_i \text{ integers}\}$

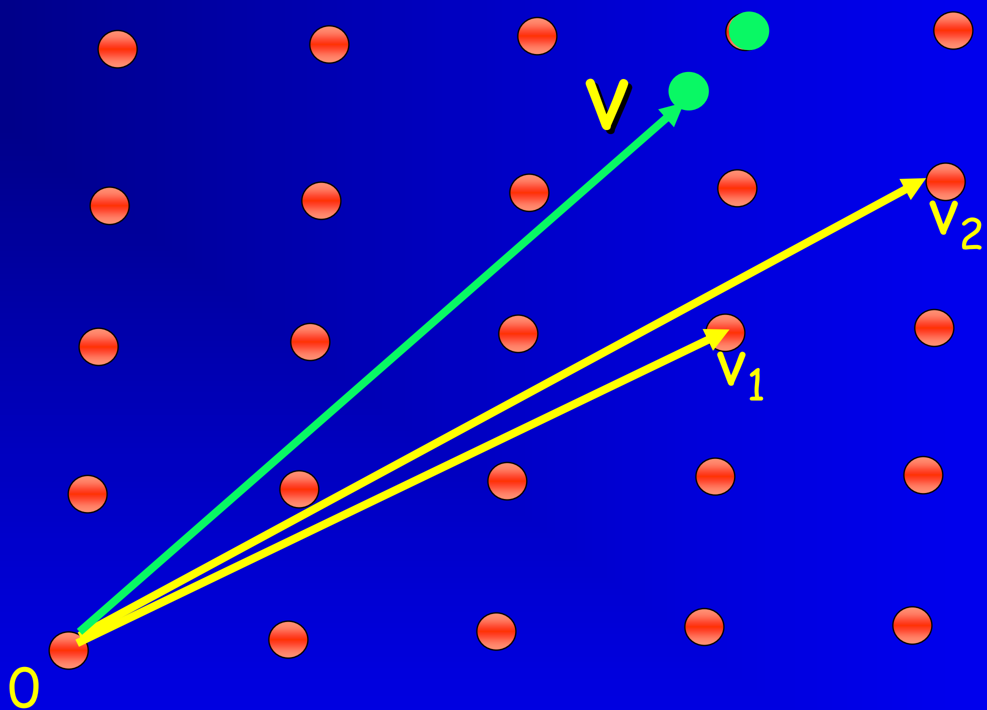


Shortest Vector Problem (SVP)



- GapSVP$_\beta$: Given a lattice, decide if the length of the shortest vector is:
  - YES: less than 1
  - NO: more than β

Closest Vector Problem (CVP)



- $GapCVP_\beta$: Given a lattice and a point v, decide if the distance of v from the lattice is:
  - YES: less than 1
  - NO: more than β

- $GapSVP_\beta$ is easier than $GapCVP_\beta$ [GoldreichMicciancioSafraSeifert99]

The Importance of Lattices

- Lattice problems are believed to be very hard classically
- They are used in strong cryptosystems [AjtaiDwork97,Regev03]
- Some connections are known to the dihedral hidden subgroup problem [Regev02]

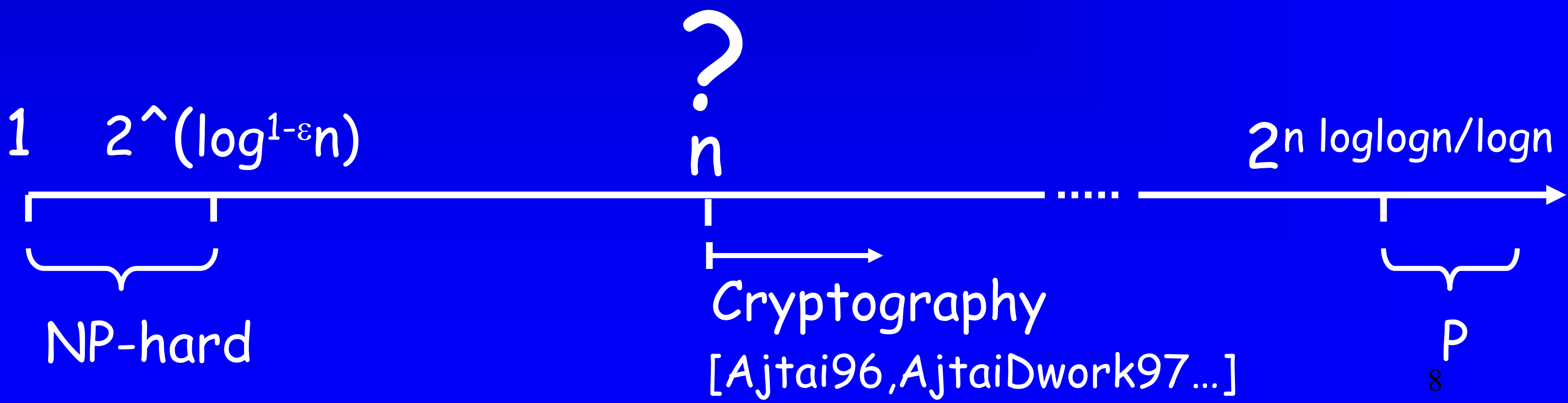
- Major open problem:

  find quantum algorithms for lattices

Known Results

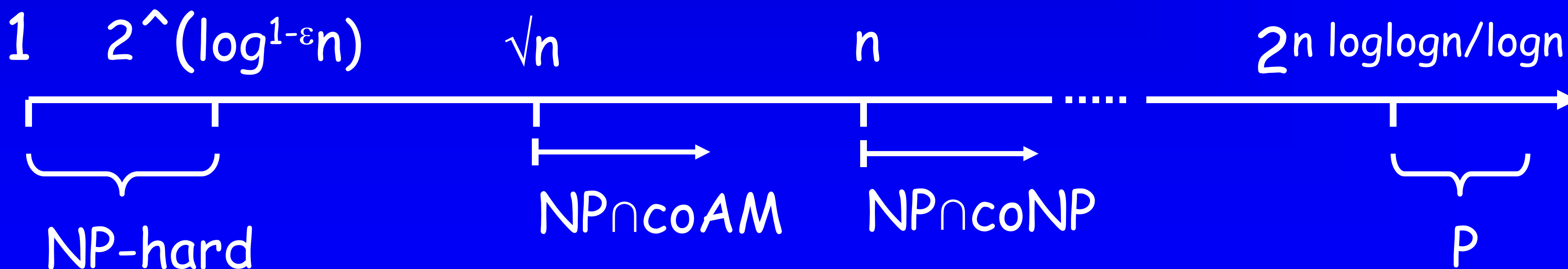
- Polytime algorithms for gap $2^{n \log\log n/\log n}$ [LLL82,Schnorr87,AjtaiKumarSivakumar02]

- NP-hardness is known for:
  - GapCVP: $2^{(\log^{1-\varepsilon} n)}$ [DinurKindlerSafra03]
  - GapSVP: $\sqrt{2}$ [Micciancio98]



Known Results
Limits on Inapproximability

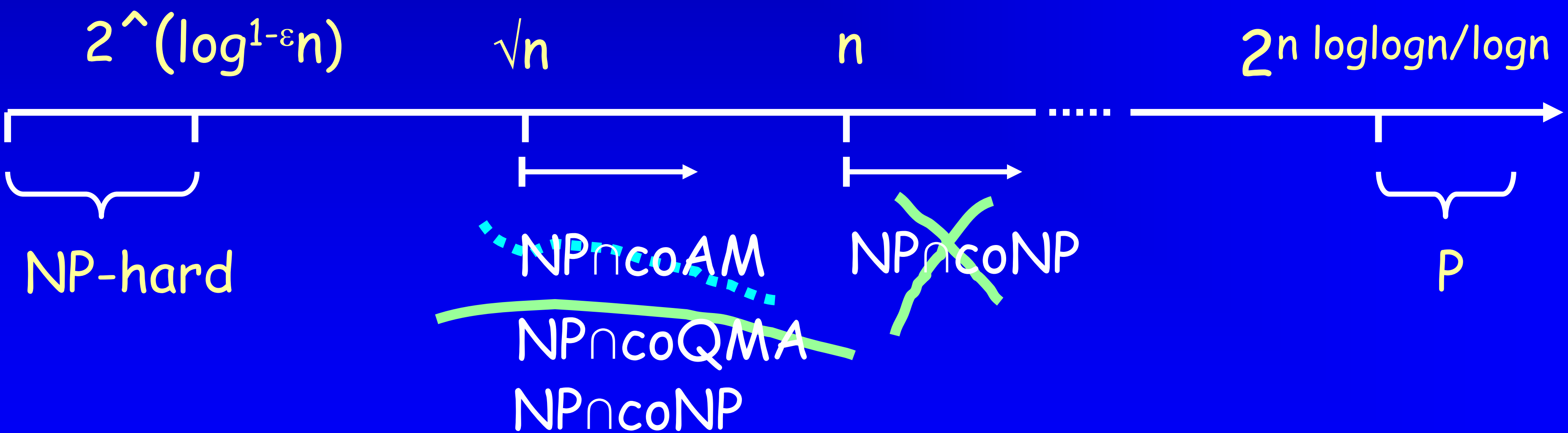
- GapCVP_{n} 2 NP∩coNP [LagariasLenstraSchnorr90, Banaszczyk93]
- $\mathrm{GapCVP}_{\sqrt{n}}$ 2 NP∩coAM [GoldreichGoldwasser98]



New Results
Limits on Inapproximability

GapSVP$_{\sqrt{n}}$ 2 NP∩coQMA [AharonovRegev03]

GapCVP$_{\sqrt{n}}$ 2 NP∩coNP [AharonovRegev04]



From Quantum to Classical

- ☹ One less problem in QMA
- ☺ This is another quantum inspired result (e.g., [Kerenidis-deWolf03,Aaronson04])
- The proof is entirely classical and is in fact simpler than the original quantum proof

Outline

- Part 1: How to dequantize QMA
- Part 2: $\mathrm{GapCVP}_{\sqrt{n}}$ 2 $\mathrm{NP} \cap \mathrm{coNP}$

Part 1:

Dequantizing

$\text{coGapSVP}_{\sqrt{n}}$ 2 QMA [AR03]

$$\Downarrow$$

$\text{coGapCVP}_{\sqrt{n}}$ 2 NP [AR04]

QMA (again)

- A language Λ2QMA if 9 quantum verifier V such that
  - 8 x 2 Λ 9 |ηi, V accepts x,η w.p. > ¾
  - 8 x ∉ Λ 8 |ηi, V accepts x,η w.p. < ¼
- Equivalently,
  - 8 x 2 Λ 9 |ηi,

$$\langle\eta|\Pi' V_x^\dagger \Pi V_x \Pi'|\eta\rangle > 3/4$$

  - 8 x ∉ Λ 8 |ηi,

$$\langle\eta|\Pi' V_x^\dagger \Pi V_x \Pi'|\eta\rangle < 1/4$$

Dequantizing QMA Verifiers

- Notice that
$$\Pi' V_x^\dagger \Pi V_x \Pi' = \Pi'^\dagger V_x^\dagger \Pi^\dagger \Pi V_x \Pi'$$
is positive semidefinite and hence the maximum of $\langle\eta|\Pi' V_x^\dagger \Pi V_x \Pi'|\eta\rangle$ is obtained when $|\eta$i is an eigenvector
- Let $|\eta_{x,1}$i,…,$|\eta_{x,N}$i be all the eigenvectors of V_x
- Therefore, an equivalent definition is,
  - 8 x 2 Λ 9 i $\langle\eta_{x,i}|\Pi' V_x^\dagger \Pi V_x \Pi'|\eta_{x,i}\rangle > 3/4$
  - 8 x $\notin$ Λ 8 i $\langle\eta_{x,i}|\Pi' V_x^\dagger \Pi V_x \Pi'|\eta_{x,i}\rangle < 1/4$
- Hence, if $|\eta_{x,i}$i can be generated efficiently from x,i then the language is in QCMA

Dequantizing [AR03]

- [AR03] showed that coGapSVP$_{\sqrt{n}}$ 2 QMA
- A witness to the [AR03] verifier is of the form

$$|\alpha_1\rangle \otimes \ldots \otimes |\alpha_k\rangle$$

where
$$\alpha_i = \sum_{x \in \mathbb{R}^n} f_i(x)|x\rangle$$

- The tests performed are all 'shift tests'
- An easy analysis shows that the eigenvectors are given by tensor of Fourier vectors, i.e., by

$$|\alpha_1\rangle \otimes \ldots \otimes |\alpha_k\rangle$$

where
$$\alpha_i = \sum_{x \in \mathbb{R}^n} e^{2\pi i \langle x, v_i \rangle}|x\rangle$$

for some $v_1,\ldots,v_k$

Dequantizing [AR03]

- Since Fourier vectors are easy to generate by the quantum Fourier transform, we immediately obtain that coGapSVP$_{\sqrt{n}}$ 2 QCMA
- It turns out that the resulting QCMA verifier can be implemented by a deterministic classical circuit and hence we obtain coGapSVP$_{\sqrt{n}}$ 2 NP
- Moreover, we can simplify the proof and even strengthen it to

coGapCVP$_{\sqrt{n}}$ 2 NP [AR04]

Part 2:

coGapCVP$_{\sqrt{n}}$ in NP

Our Goal

Given:

- Lattice L (by $v_1, v_2, \ldots, v_n$)
- Point v

We want:

A witness for the fact that v is far from L

Overview

Step 1: Define f

- Its value depends on the distance from L:
  - Almost zero if distance > $\sqrt{n}$
  - More than zero if distance < $\sqrt{\log}$

Step 2: Encode f

Show that the function f has a short description

CVPP approximation algorithm

Step 3: Verify f

Verify that the function is non-negligible close to L

Step 1:

Define f

The function f

Consider the Gaussian:

$$e^{-\pi|x|^2}$$

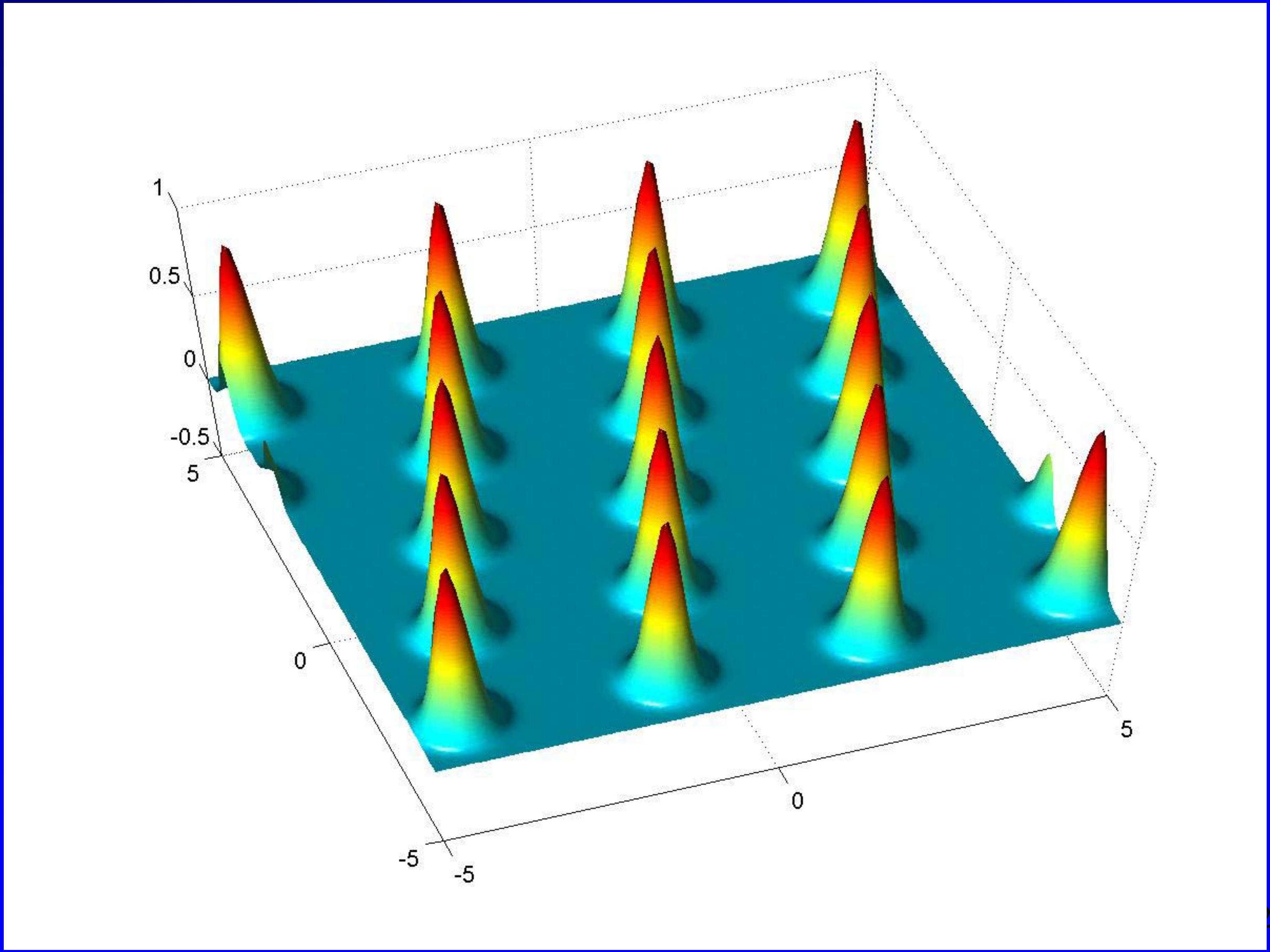
Periodize over L:

$$g(x) = \sum_{y \in L} e^{-\pi|x-y|^2}$$

Normalize by g(0):

$$\boxed{f(x) = \frac{g(x)}{g(0)}}$$

The function f



f distinguishes between far and close vectors

(a) $d(x,L) \geq \sqrt{n}$ → $f(x) \leq 2^{-\Omega(n)}$

(b) $d(x,L) \leq \sqrt{\log n}$ → $f(x) > n^{-5}$

Proof: (a) Banaszczyk93 (simple for one Gaussian)

(b) Not too difficult

Step 2:

Encode f

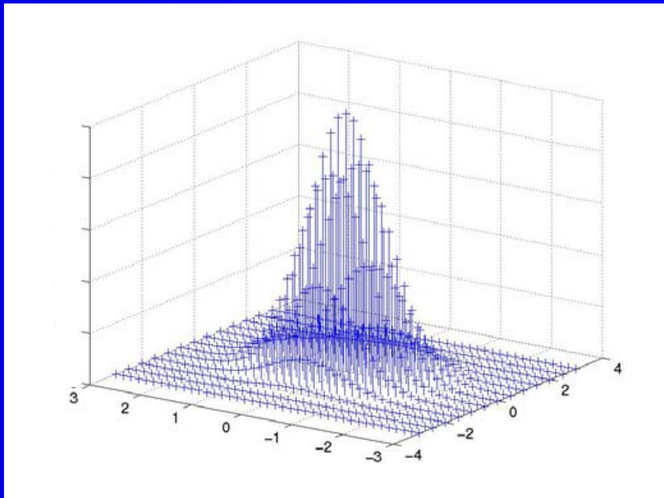
The function f (again)

$$g(x) = \sum_{y \in L} e^{-\pi |x-y|^2}$$

$$f(x) = \frac{g(x)}{g(0)}$$

Let's consider its Fourier transform !

$\hat{f}$ is a probability measure



Claim: $\hat{f}$ is a probability measure on L^*

$$L^* = \{ w \mid \langle w, x \rangle \in Z \quad \forall x \in L \}$$

Proof: g is a convolution of a Gaussian and δ_L

$$\hat{g}(w) = \widehat{e^{-\pi|x|^2}} \cdot \hat{\delta}_L = \begin{cases} e^{-\pi|w|^2} & w \in L^* \\ 0 & o.w. \end{cases}$$

$$\hat{f}(w) = \frac{\hat{g}(w)}{g(0)} = \frac{e^{-\pi|w|^2}}{\sum_{z \in L^*} e^{-\pi|z|^2}}$$

f is an expectation

$$f(x) = \sum_{w \in L^*} \hat{f}(w) e^{2\pi i \langle x, w \rangle}$$

$$= E_{w \in \hat{f}} \left(e^{2\pi i \langle x, w \rangle} \right)$$

In fact, it is an expectation of a real variable between -1 and 1:

$$f(x) = E_{w \in \hat{f}} \left(\cos(2\pi \langle x, w \rangle) \right)$$

Chernoff!

Encoding f

$$f(x) = E_{w \in \hat{f}} \cos(2\pi \langle x, w \rangle)$$

Pick $W=(w_1,w_2,\ldots,w_N)$ with N=poly(n) according to the $\hat{f}$ distribution on L*

$$f_W(x) = \frac{1}{N}\sum_{j=1}^{N} \cos(2\pi \langle x, w_j \rangle)$$

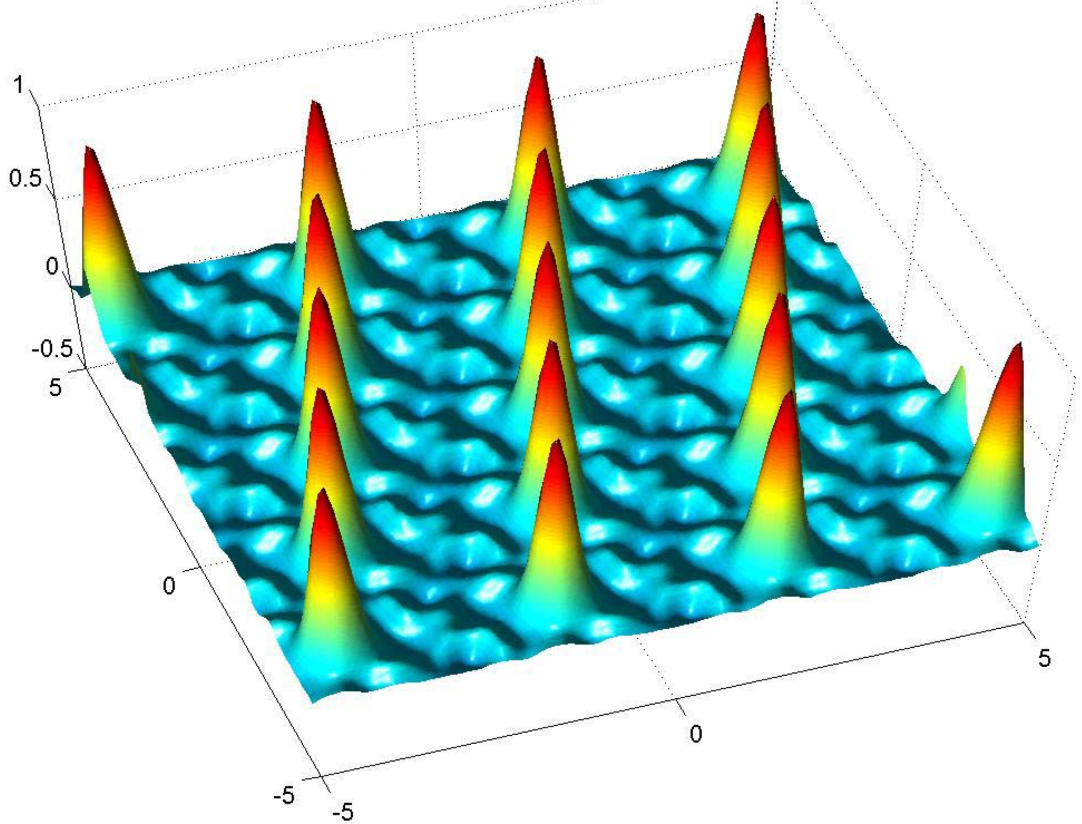
$f(x) \approx f_W(x)$ (Chernoff)

This is true even pointwise!

The Approximating Function

$$f_W(x) = \frac{1}{N}\sum_{j=1}^{N}\cos(2\pi\langle x, w_j\rangle)$$

with N=1000 dual vectors



This concludes Step 2: Encode f

The encoding is a list W of vectors in L*

$f_W(x) \approx f(x)$

Interlude: CVPP

GapCVPP

Solve GapCVP on a preprocessed lattice (allowed infinite computational power, but before seeing v)

Algorithm for GapCVPP:

Prepare the function f_W in advance;

When given v, calculate $f_W(v)$.

→ Algorithm for $\text{GapCVPP}_{\sqrt{(n/\log n)}}$, improving the GapCVPP_n of [Regev03]

Back to coGapCVP$_{\sqrt{n}}$ in NP

The input is L and v

The witness is a list of vectors

$W = (w_1, \ldots, w_N)$

$$f_W(x) = \frac{1}{N}\sum_{j=1}^{N} \cos(2\pi\langle x, w_j\rangle)$$

Verify that f_W is non-negligible near L

Step 3:

Verify f_w

The Verifier (First Attempt)

Accepts iff

1. $f_W(v) < n^{-10}$, and
2. $f_W(x) > n^{-5}$ for all x within distance 0.01 ~~$\sqrt{\log n}$~~ from L

- Completeness and soundness would follow
- But: how to check (2) ?
  - First check that f_W is periodic over L (true if W in L^*)
  - Then check that $>n^{-5}$ around origin

- We don't know how to do this for distance $\sqrt{\log n}$
- We do this for distance 0.01

The Verifier (Second Attempt)

Accepts iff

1. $f_W(v) < n^{-10}$, and
2. $w_1,\dots,w_N \in L^*$, and
3. $\forall x \in \Re^n, \forall u, \left|\frac{\partial^2 f_W(x)}{\partial^2 x_u}\right| \leq 100$

2 implies that f_W is periodic on L:

$$\forall x \in \Re^n, \forall y \in L, f_W(x+y) = \tfrac{1}{N}\sum_{j=1}^{N}\cos(2\pi\langle x+y, w_j\rangle)$$

$$= \tfrac{1}{N}\sum_{j=1}^{N}\cos(2\pi\langle x, w_j\rangle + \cancel{2\pi\langle y, w_j\rangle}) = f_W(x)$$

The Verifier (Second Attempt)

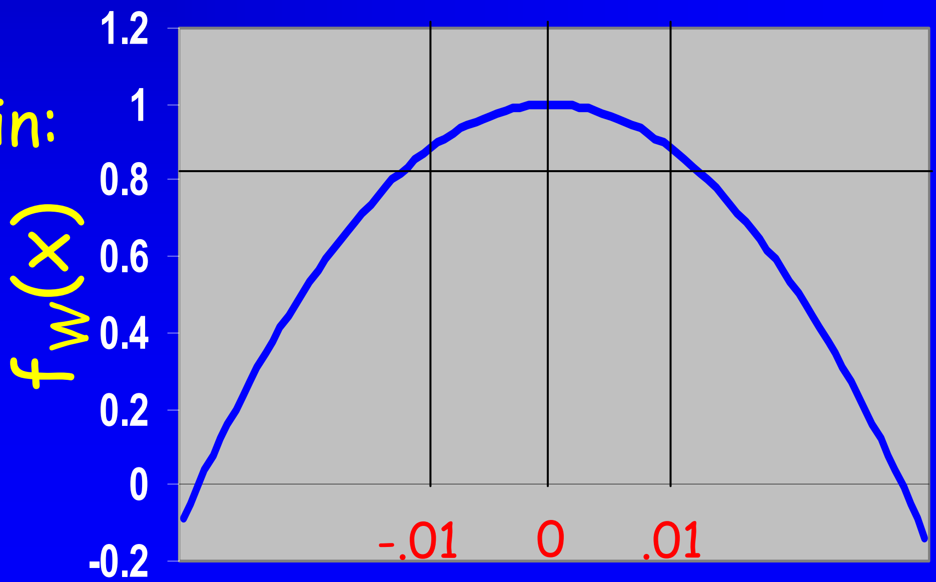
Accepts iff

1. $f_W(v) < n^{-10}$, and
2. $w_1,\ldots,w_N \in L^*$, and
3. $\forall x \in \Re^n, \forall u, \left|\frac{\partial^2 f_W(x)}{\partial^2 x_u}\right| \leq 100$

3 implies that f_W is at least .8 within distance .01 of the origin:

$$f_W(0) = 1$$

$$\frac{\partial f_W}{\partial x_u}(0) = 0$$



The Final Verifier

Accepts iff

1. $f_W(v) < n^{-10}$, and
2. $w_1,\ldots,w_N \in L^*$, and
3. $\|WW^T\| < N$ where $W = \left(\begin{pmatrix} \\ w_1 \\ \\ \end{pmatrix} \begin{pmatrix} \\ w_2 \\ \\ \end{pmatrix} \cdots\cdots \begin{pmatrix} \\ w_N \\ \\ \end{pmatrix} \right)$

3 checks that in any direction the w's are not too long:

$$\left\|WW^T\right\| = \max_{|u|=1} uWW^T u^T = \max_{|u|=1} \sum_{j=1}^{N} \langle u, w_j \rangle^2$$

The Final Verifier

Accepts iff

1. $f_W(v) < n^{-10}$, and
2. $w_1,\dots,w_N \in L^*$, and
3. $||WW^T||<N$ where $W = \left(\begin{pmatrix} \\ w_1 \\ \\ \end{pmatrix} \begin{pmatrix} \\ w_2 \\ \\ \end{pmatrix} \dots\dots \begin{pmatrix} \\ w_N \\ \\ \end{pmatrix} \right)$

$$\frac{\partial^2 f_W(x)}{\partial^2 x_u} = \frac{-4\pi^2}{N} \sum_{j=1}^{N} \langle w_j, u\rangle^2 \cos(2\pi \langle w_j, x\rangle)$$

$$\left| \frac{\partial^2 f_W(x)}{\partial^2 x_u} \right| \le \frac{4\pi^2}{N} \sum_{j=1}^{N} \langle w_j, u\rangle^2 = \frac{4\pi^2}{N} uWW^T u^T \le \frac{4\pi^2}{N} \left\| WW^T \right\| \le 100$$

Conclusion

- Main result: $\mathrm{GapCVP}_{\sqrt{n}}$ 2 $\mathrm{NP} \cap \mathrm{coNP}$
- An algorithm for $\mathrm{GapCVPP}_{\sqrt{(n/\log n)}}$

Open Problems

- Can the containment in NP∩coNP be improved to $\sqrt{(n/\log n)}$ or even below?
- Can similar ideas work for problems such as Graph Isomorphism ?
- Other 'quantum inspired' results ?
- Find a sub-exponential time quantum algorithm for lattice problems
- Find a polynomial time quantum algorithm for solving GapSVP with sub-exponential gaps