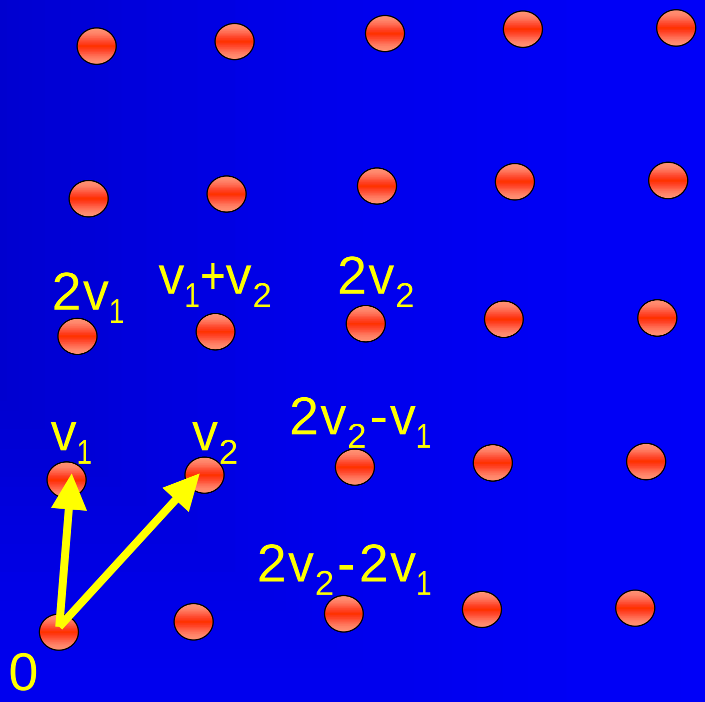
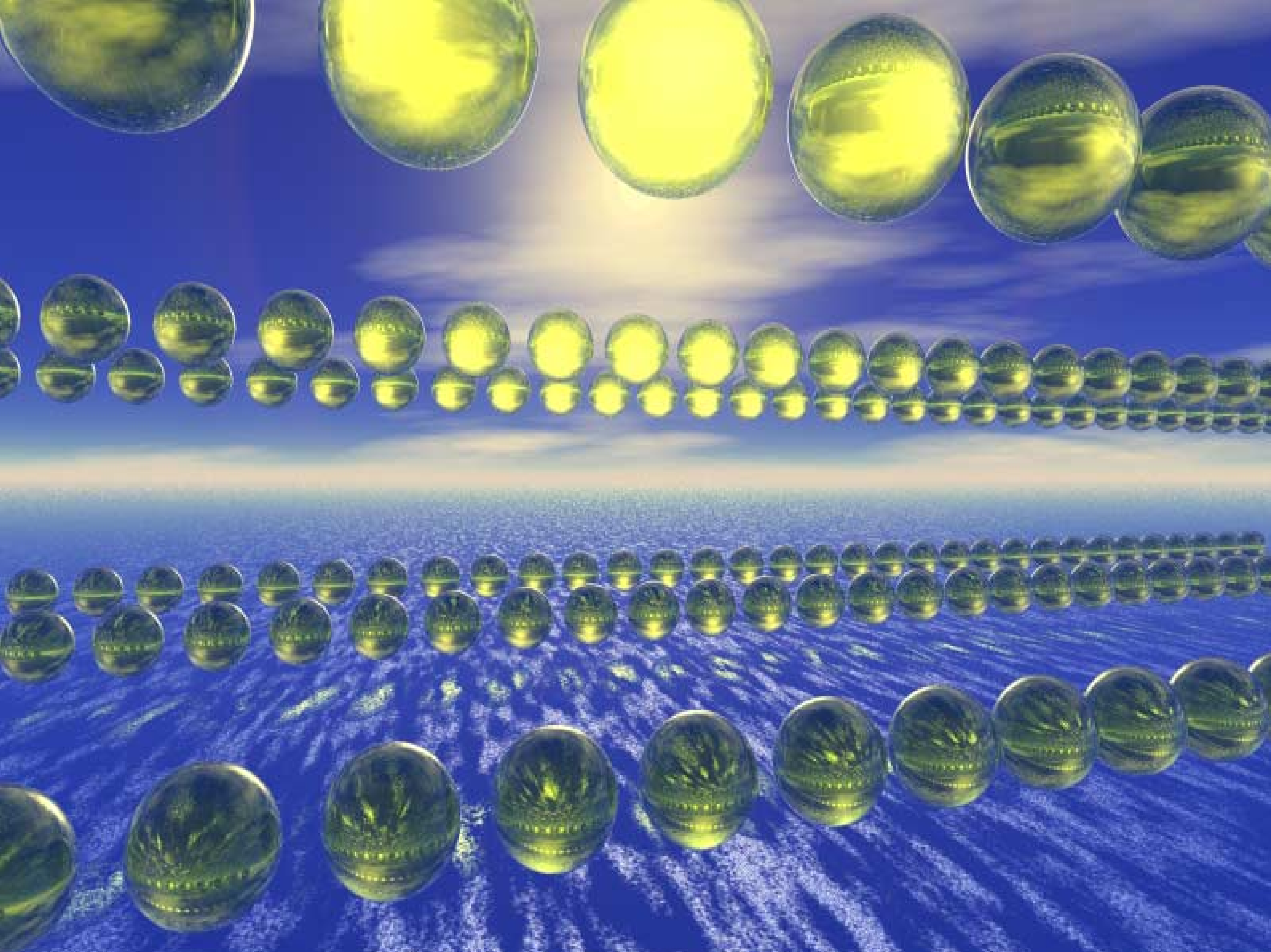
Quantum Computation and Lattice Problems

Oded Regev
Institute for Advanced Study

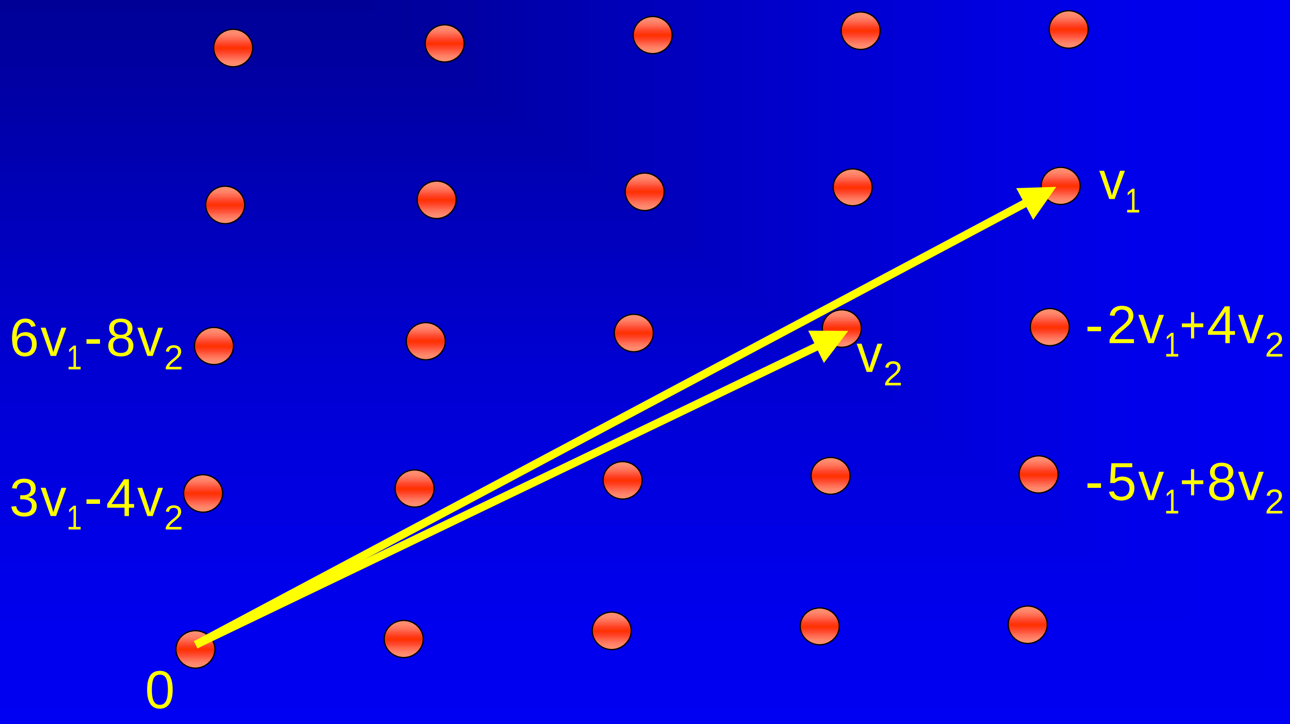
Lattices

- Basis: $v_1,\ldots,v_n$ vectors in R^n
- The lattice is $a_1v_1+\ldots+a_nv_n$ for all *integer* $a_1,\ldots,a_n$.
- What is the shortest vector ?



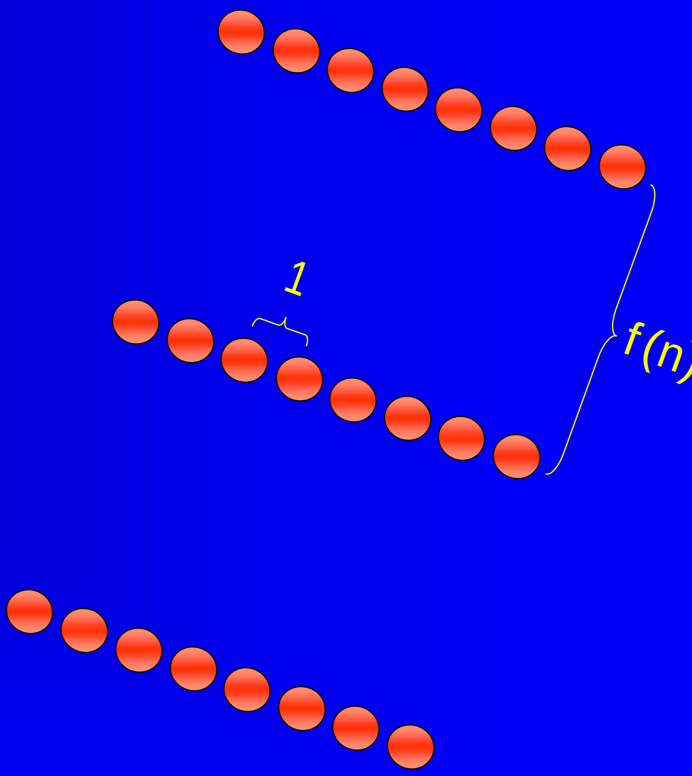


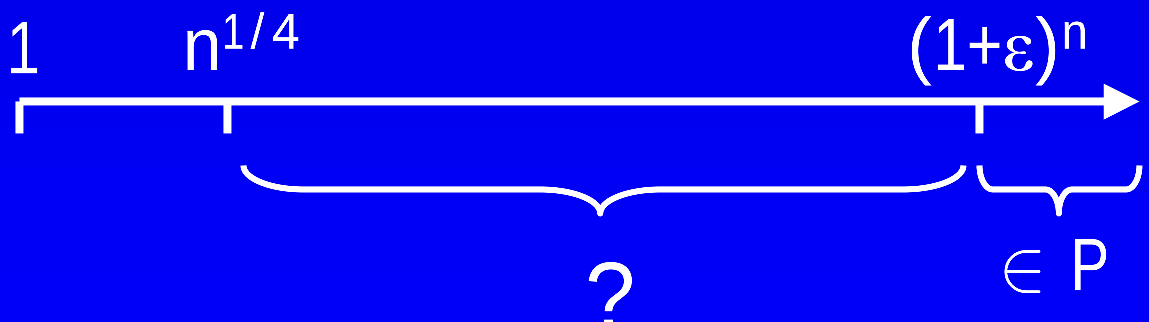
Lattices – not so easy



f(n)-unique-SVP (shortest vector problem)

- Promise: the shortest vector is shorter by a factor of f(n) than other non-parallel vectors
- Algorithm for $(1+\varepsilon)^n$-unique SVP [Schnorr87]
- $n^{1/4}$-unique-SVP not NP-hard [Cai,GoldreichGoldwasser98]





Lattices and Cryptography

- Standard cryptography
  - Based on ‘hardness’ of factoring, discrete log, or principal ideal problem
  - Solvable by quantum algorithms
- Lattice based cryptography [AjtaiDwork97]
  - Based on hardness of unique-SVP
  - Worst case hardness
  - Still not solvable by quantum algorithms

Results (1)

- Can we solve the unique-SVP with quantum algorithms ?
- Yes, but under the assumption that a solution exists to the dihedral HSP

Dihedral HSP → $n^{2.5}$-unique SVP

Hidden Subgroup Problem

- Major problem in quantum computation
- Given a function which is constant and distinct on cosets of $H \leq G$, find H

Symmetric group	Graph Isomorphism
Dihedral group	Lattices
Abelian groups	Factoring

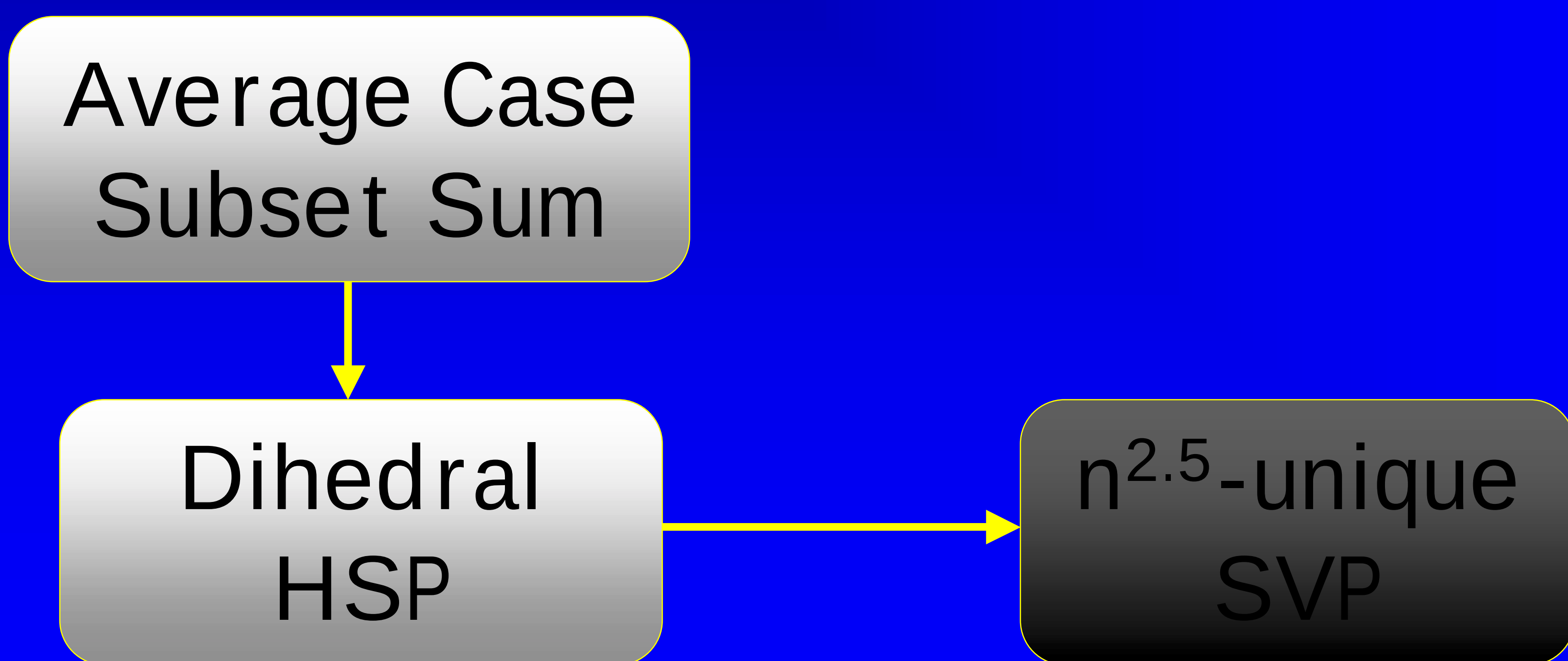
So, can we solve the dihedral HSP?

Dihedral HSP

- Ettinger and Høyer show how to solve dihedral HSP with only a polynomial number of measurements
- However, the running time of the algorithm is exponential...

Results (2)

- We solve the dihedral HSP with an average case subset-sum algorithm



Part I

or

Finding the Shortest Vector using Dihedral Cosets

Dihedral Coset Problem

- Given a black box that outputs a superposition of two numbers in {0,...,N-1} whose difference d modulo N is fixed, find d.
- Naïve solution: measure the result. The state collapses and we have no information about d!
- No known solution

Two Point Problem

- Given a black box that outputs two vectors in Z^n whose vector difference d is fixed, find d.

  e.g. $|4,9,1\rangle + |7,9,2\rangle$

  $|1,0,6\rangle + |4,0,7\rangle$

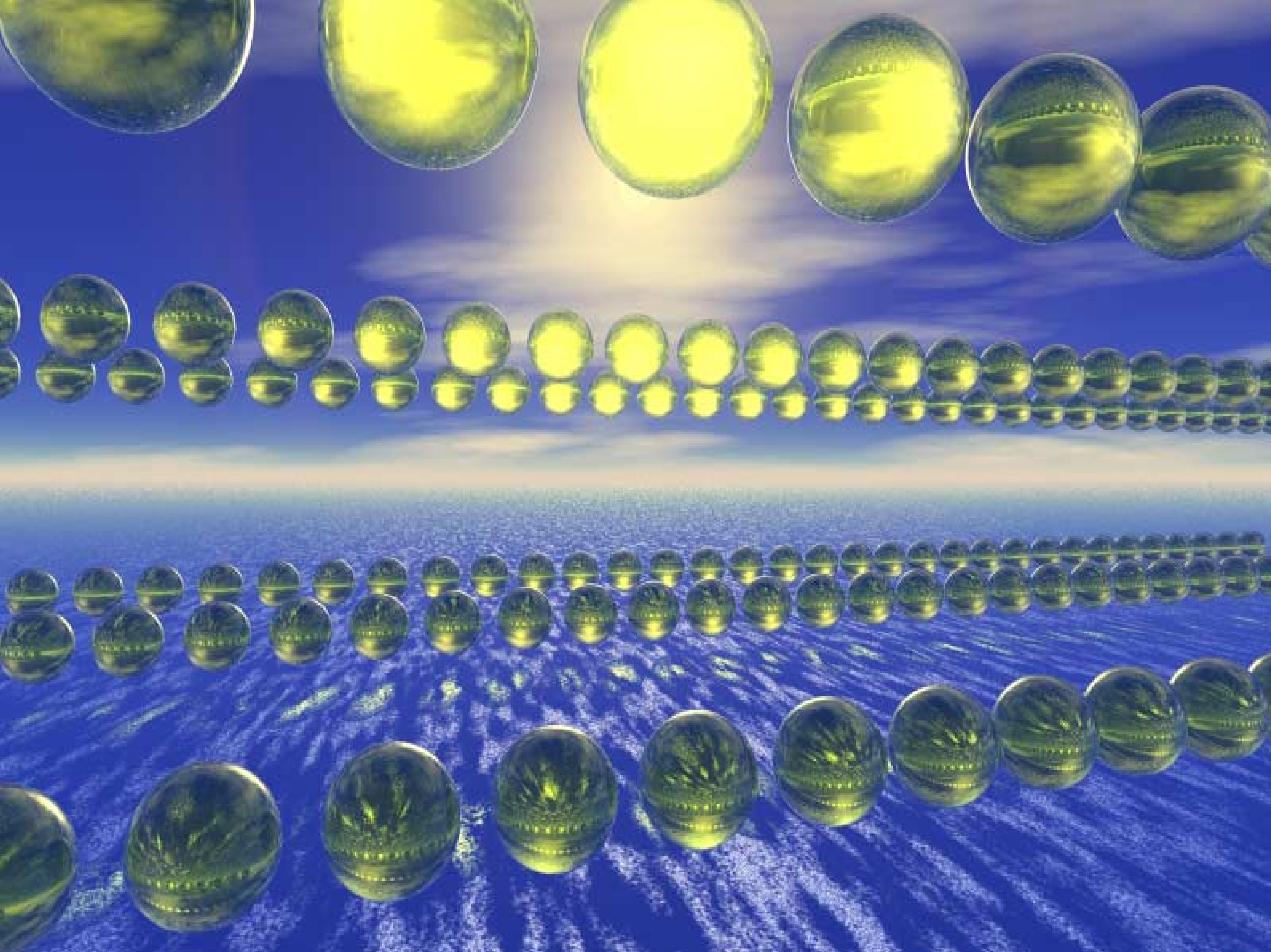
- Can be solved using a Dihedral Coset Algorithm:

  (1,3),(2,5) → 13,25 → 25-13=12 → (1,2)

  (4,0),(5,2) → 40,52 → 52-40=12 → (1,2)

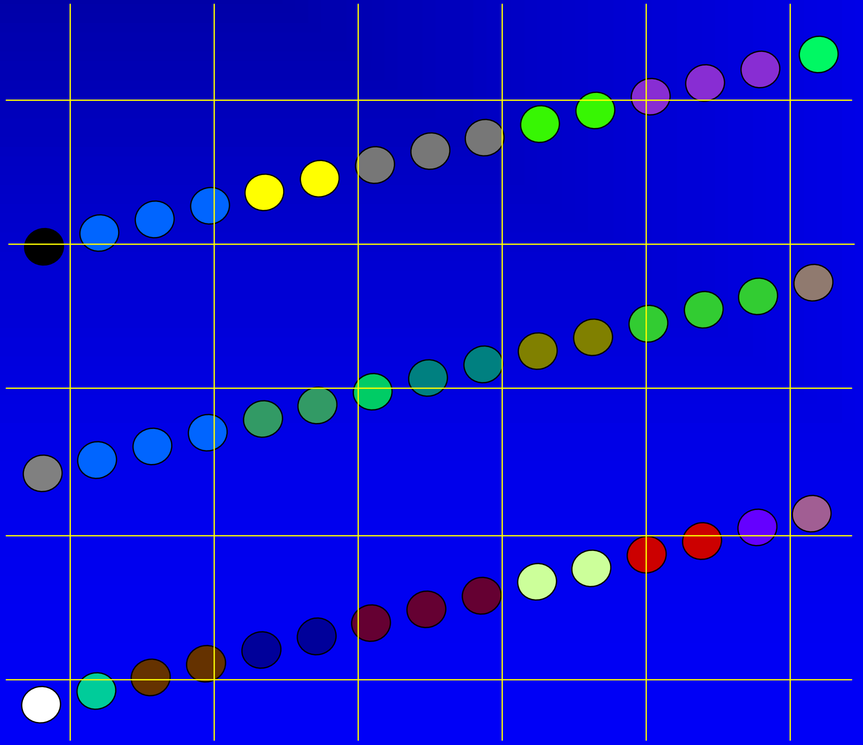
From 2PP to Lattices

- Assume we are given an algorithm for the two point problem
- We show a solution to the $n^3 \log^{0.5} n$-unique SVP by building the black box
- Idea: catch two points in a box !



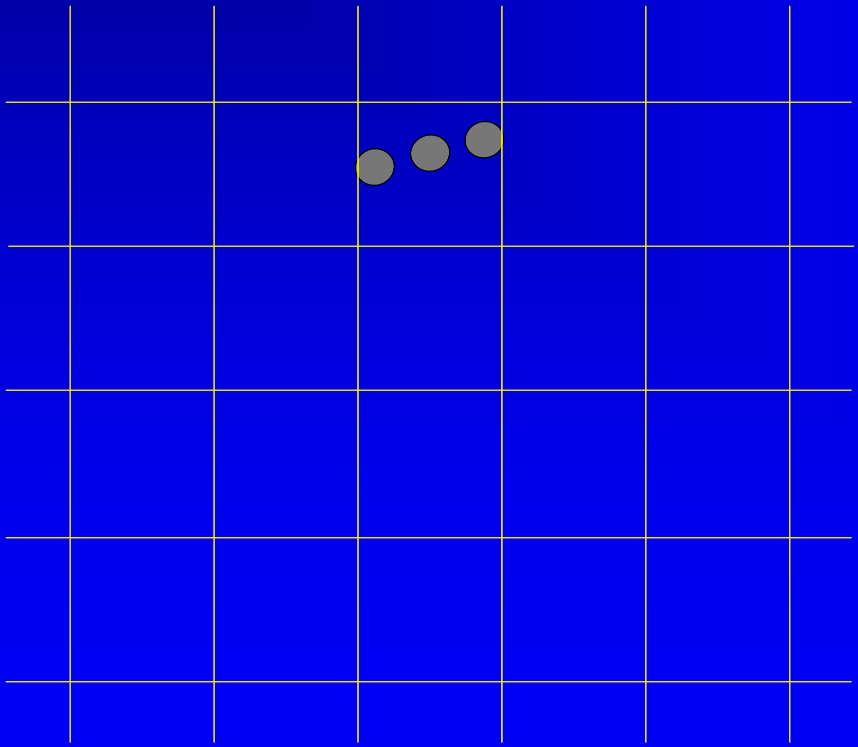
First Attempt

- Create a superposition of ‘all’ the lattice
- Partition the space into cubes and compute the location of each point
- Measure the result



First Attempt

- Not necessarily 2 points...



Spacing out the Lattice

- Shortest vector is an integer combination of the basis vectors:

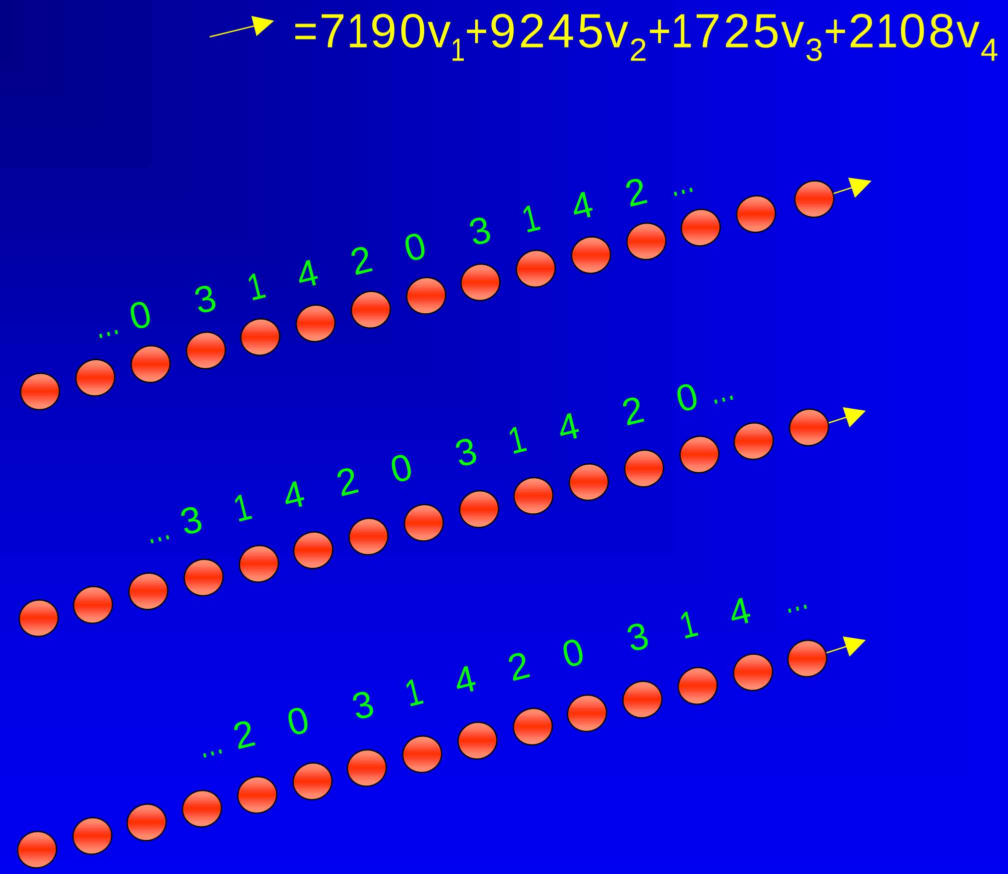
$$7190v_1+9245v_2+1725v_3+2108v_4$$

- Not all coefficients divisible by the prime p
- We can assume that we know which coefficient it is and its value modulo p which is denoted by m
- For example, p=5,a_4,m=3

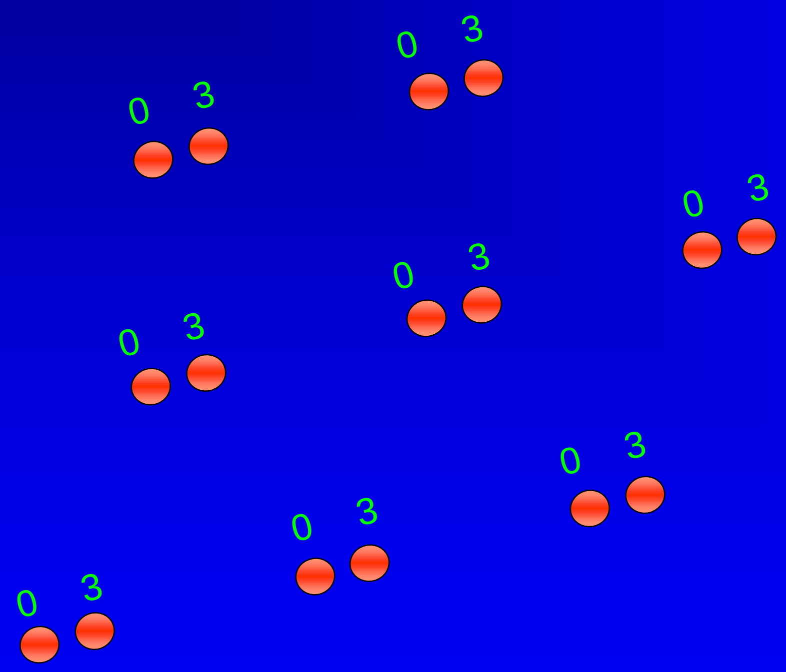
Spacing out the Lattice

p=5

m=3

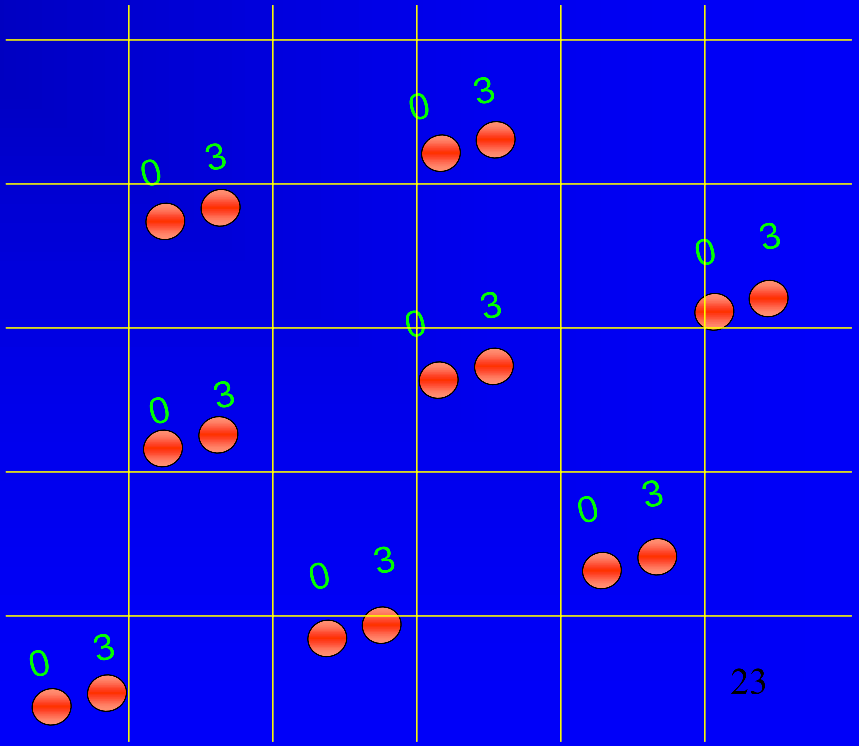


Spacing out the Lattice



Partitioning into Cubes

- Assume we have an estimate s on the length of the shortest vector
- Partition the space into cubes of side length ~ $(n^{2.5}\log^{1/2}n)s$



The Black Box

- Create the set of all the lattice points whose coefficient modulo p is 0 or m (e.g., 0,3)
- Compute the location of each point in a random rotation & translation of the grid of side length $(n^{2.5}\log^{0.5}n)$s
- Measure the result

Analysis

- The initial state is
  $$|p_1\rangle+|p_2\rangle+|p_3\rangle+|p_4\rangle+|p_5\rangle+|p_6\rangle$$
- After computing the locations:
  $|p_1,c_2\rangle+|p_2,c_1\rangle+|p_3,c_1\rangle+|p_4,c_3\rangle+|p_5,c_2\rangle+|p_6,c_3\rangle$
- After measuring the second register, say we got c_2:
  $|p_1,c_2\rangle+|p_5,c_2\rangle$
- The first register contains two points whose difference is fixed and equals to the shortest vector.
- Given this black box, the two point problem finds the shortest vector.

Analysis – error prob.

- Not more than two points
  - Because lattice is spaced out, and
  - Because $n^3\log^{1/2}n$-unique-SVP and cube side length is $n^{2.5}\log^{1/2}n$
- Prob. of one point is:
  - The projection of the shortest vector on each of the grid's axes is at most $(n^{-1/2}\log^{1/2}n)s$
  - Side length is $(n^{2.5}\log^{1/2}n)s$
  - Hence success probability is at least:

$$\left(1-\frac{1}{n^3}\right)^n \approx 1-\frac{1}{n^2}$$

  - Good enough because the space is 2^(n^2)

Part II

or

Solving Dihedral HSP using Subset Sum

Subset Sum Problem

- Given integers $a_1,\ldots,a_r,t,N$ find a subset of $\{a_1,\ldots,a_r\}$ that sums to t modulo N.
- We assume that there exists a routine S that solves a non-negligible part of the inputs
- We show how to solve the dihedral coset problem

Dihedral Coset Problem

- Given a black-box that outputs states of the form $|0,x\rangle+|1,x+d\rangle$ (both in $\{0,\ldots,N-1\}$) with fixed d**, find d**.
- We can add the first qubit in the lattice construction

Phase estimation

- By using the Hadamard transform we can estimate the phase difference between two *known* basis states:
- Given the state $e^{2\pi i\alpha}|a\rangle+e^{2\pi i\beta}|b\rangle \leftarrow$ where a and b are known, estimate $\beta-\alpha$

Finding d

- We describe a routine that estimates d
- Later, we will find d exactly by repeating the estimation process with 2d, 4d…

Black Box + Fourier

- Calling the black box returns the state $|0,x\rangle+|1,x+d\rangle$ on 1+logN qubits
- Apply the Fourier transform to the last logN qubits and the state is

$$\sum_{j=0}^{N-1} e^{2\pi i(jx/N)}\,|0,j\rangle+\sum_{j=0}^{N-1} e^{2\pi i(j(x+d)/N)}\,|1,j\rangle=$$

$$\sum_{j=0}^{N-1} e^{2\pi i(jx/N)}\left(|0\rangle+e^{2\pi i(jd/N)}\,|1\rangle\right)|j\rangle$$

Black Box + Fourier

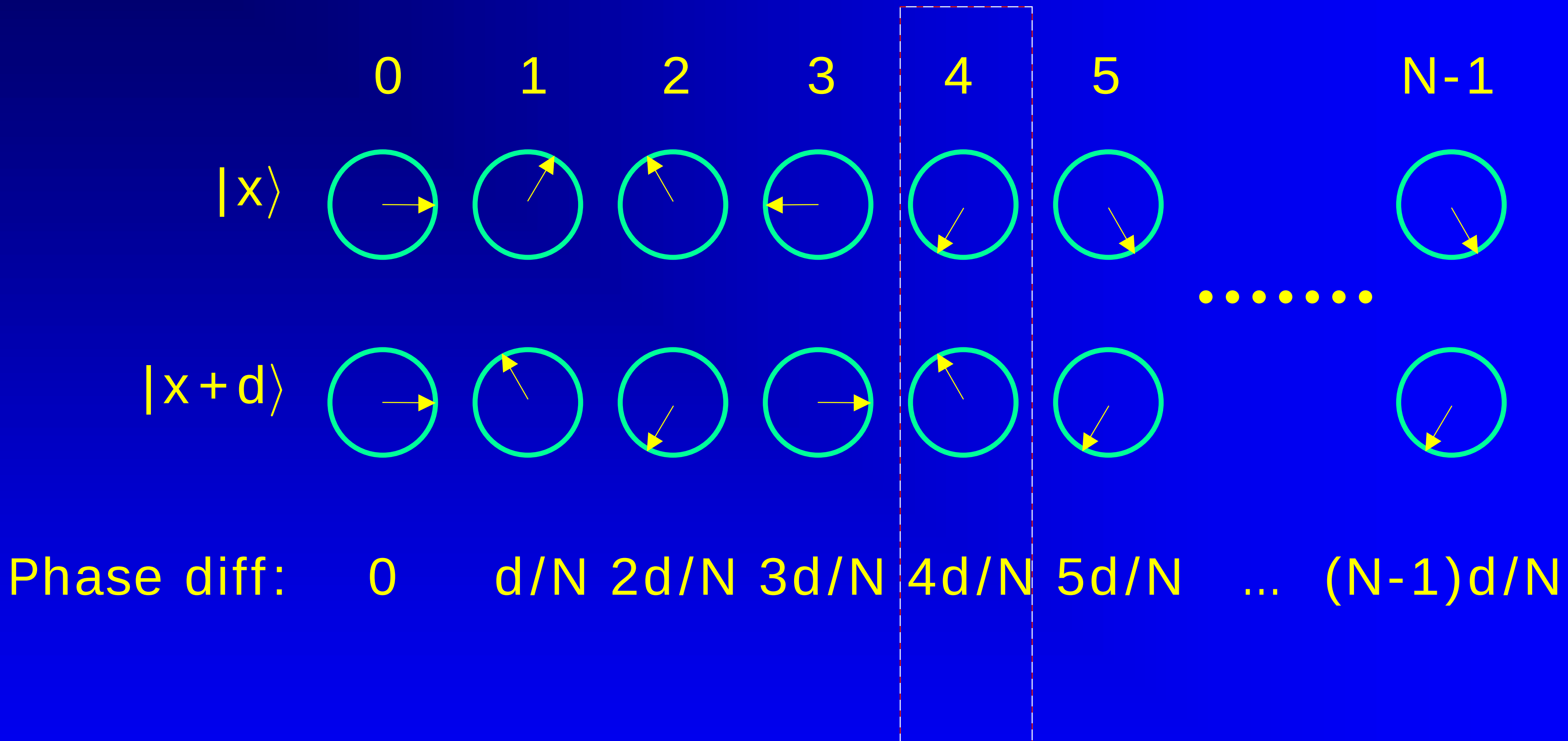
- Measure the second register
- We get a uniform value q between 0 and N-1 and the state collapses to:

$$e^{2\pi i(qx/N)}(|0\rangle + e^{2\pi i(qd/N)}|1\rangle)|q\rangle$$

or equivalently,

$$|0\rangle + e^{2\pi i(qd/N)}|1\rangle$$

Black Box + Fourier



Routine for estimating d

- So, by using the Fourier transform, we can create a phase difference of $2\pi(q \cdot d/N)$ for a *random* q in {0,...,N-1}.
- It would be nice if q=1...
- We repeat the process r=logN+c times and get a sequence $q_1,...,q_r$.

Routine for estimating d

- The state is,

$$\otimes_{j=1}^{r} |0\rangle + e^{2\pi i (q_j d / N)} |1\rangle$$

- This is a superposition of 2^r basis states
- Think of each basis state as a subset of $\{q_1,\ldots,q_r\}$.
- The phase of each subset is $2\pi(\Sigma q \cdot d/N)$
- So, instead of q=1, we'll try to find pairs whose phase is q and q+1

Routine for estimating d

- Assume r=4,N=10 and we got the random sequence $q_1=3, q_2=4, q_3=8, q_4=9$

$$(|0\rangle + e^{2\pi i(3d/10)}|1\rangle)(|0\rangle + e^{2\pi i(4d/10)}|1\rangle)(|0\rangle + e^{2\pi i(8d/10)}|1\rangle)(|0\rangle + e^{2\pi i(9d/10)}|1\rangle)$$

{3,4,8,9},Σ=4	{3,4,8},Σ=5	{3,4,9},Σ=6	{3,8,9},Σ=0
{4,8,9},Σ=1	{3,4},Σ=7	{3,9},Σ=2	{8,9},Σ=7
{3,8},Σ=1	{4,9},Σ=3	{4,8},Σ=2	{3},Σ=3
{4},Σ=4	{8},Σ=8	{9},Σ=9	{},Σ=0

S: 0→{}, 1→{4,8,9}, 2→X, 3→{3}, 4→{4},
5→{3,4,8}, 6→{3,4,9}, 7→X, 8→{8}, 9→{9}

Routine for estimating d

- We compute a color to each state
- A state is colored black if it is not returned by S

{3,4,8,9},Σ=4   {3,4,8},Σ=5   {3,4,9},Σ=6   {3,8,9},Σ=0

{4,8,9},Σ=1   {3,4},Σ=7   {3,9},Σ=2   {8,9},Σ=7

{3,8},Σ=1   {4,9},Σ=3   {4,8},Σ=2   {3},Σ=3

{4},Σ=4   {8},Σ=8   {9},Σ=9   {},Σ=0

S: 0→{}, 1→{4,8,9}, 2→X, 3→{3}, 4→{4},
5→{3,4,8}, 6→{3,4,9}, 7→X, 8→{8}, 9→{9}

Routine for estimating d

- The neighbor of i is i+1 if even and i-1 if odd
- A state is colored black if S doesn't answer about his neighbor

{3,4,8,9},Σ=4	{3,4,8},Σ=5	{3,4,9},Σ=6	{3,8,9},Σ=0
{4,8,9},Σ=1	{3,4},Σ=7	{3,9},Σ=2	{8,9},Σ=7
{3,8},Σ=1	{4,9},Σ=3	{4,8},Σ=2	{3},Σ=3
{4},Σ=4	{8},Σ=8	{9},Σ=9	{},Σ=0

S: 0→{}, 1→{4,8,9}, 2→X, 3→{3}, 4→{4},
5→{3,4,8}, 6→{3,4,9}, 7→X, 8→{8}, 9→{9}

Routine for estimating d

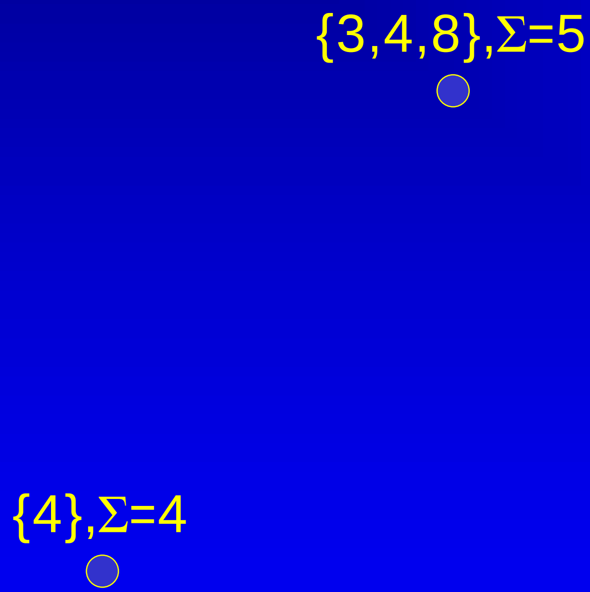
- Each remaining state is colored according to $\lfloor \Sigma/2 \rfloor$

{3,4,8,9},Σ=4	{3,4,8},Σ=5	{3,4,9},Σ=6	{3,8,9},Σ=0
{4,8,9},Σ=1	{3,4},Σ=7	{3,9},Σ=2	{8,9},Σ=7
{3,8},Σ=1	{4,9},Σ=3	{4,8},Σ=2	{3},Σ=3
{4},Σ=4	{8},Σ=8	{9},Σ=9	{},Σ=0

S: 0→{}, 1→{4,8,9}, 2→X, 3→{3}, 4→{4},
5→{3,4,8}, 6→{3,4,9}, 7→X, 8→{8}, 9→{9}

Routine for estimating d

- We measure one of the colors
- We estimate the phase difference between the two known states



S: 0→{}, 1→{4,8,9}, 2→X, 3→{3}, 4→{4}, 5→{3,4,8}, 6→{3,4,9}, 7→X, 8→{8}, 9→{9}

Finding d exactly

- The previous routine estimates d/N
- We repeat the routine but instead of pairing numbers with difference 1 we pair numbers with difference 2
- Then we get an estimate on 2d/N
- We continue with 4d/N, 8d/N,… until we find d exactly

Conclusion

- We described the first lattice-quantum connection
- We solved the shortest vector problem on $n^{2.5}$-unique lattices with the assumption that there exists a solution to the dihedral hidden subgroup problem
- We solved the dihedral hidden subgroup problem with the assumption that there exists an average case solution to the subset sum problem