Hallgren's Quantum Algorithm for Pell's Equation

Pradeep Sarvepalli

pradeep@cs.tamu.edu

Department of Computer Science,

Texas A&M University

Outline

- Pell's equation
- Classical method for solving Pell's equation
- Reformulating the Pell's equation in number theoretic terms
- Overview of Hallgren's quantum algorithm
- Hallgren's algorithm
  - Algebraic background
  - Quantum period finding algorithm
  - Classical post processing
  - Putting all the pieces together

Outline - cont'd

- Applications
  - Class group of a quadratic field
  - Principal ideal problem
- Generalizations
  - Unit group of a finite extension of $\mathbb{Q}$
  - Class group of a finite extension of $\mathbb{Q}$
  - Principal ideal problem
- References
  - "Notes on Hallgren's efficient quantum algorithm for solving Pell's equation" by Richard Jozsa
  - "Polynomial time quantum algorithms for Pell's equation and principal ideal problem" by Sean Hallgren

Pell's Equation

- Goal is to find finding integral and positive solutions to the following equation

$$x^2 - dy^2 = 1$$

- $x^2 - 2y^2 = 1$, Solutions $(3, 2); (17, 12); \ldots$
- Has infinite number of solutions
- Harder than factoring

Classical Method for Pell's equation

- Based on continued fractions
- Approximations of the continued fraction of $\sqrt{d}$ give the solution
- Example

$$\begin{aligned} x^2 - 2y^2 &= 1, \\ \sqrt{2} &= 1 + \cfrac{1}{2 + \frac{1}{2 + \frac{1}{2 + \cdots}}} \\ \sqrt{2} &\approx 1 + \frac{1}{2} = \frac{3}{2} = \frac{x}{y} \end{aligned}$$

- Observe that $3^2 - 2 \cdot 2^2 = 9 - 8 = 1$

Continued Fraction Method

- Why does this work?
- Is every approximation a solution?
- What is the complexity of the algorithm?

Continued Fraction Method - cont'd

- Example - cont'd

$$
\begin{aligned}
\sqrt{2} &\approx 1+\frac{1}{2+\frac{1}{2}} = 1+\frac{2}{5} = \frac{7}{5} = \frac{x}{y} \\
\sqrt{2} &\approx 1+\frac{1}{2+\frac{1}{2+\frac{1}{2}}} = 1+\frac{1}{2+\frac{2}{5}} \\
&= 1+\frac{5}{12} = \frac{17}{12} = \frac{x}{y}
\end{aligned}
$$

- $7^2 - 2\cdot 5^2 = 49 - 50 = -1 \neq 1$
- $17^2 - 2\cdot 12^2 = 289 - 288 = 1$

Continued Fraction Method - cont'd

- Not every approximation gives a solution to the Pell's equation
- We might have to take many terms in the continued fraction before we get the solution
- Typically if we use the input size as $\log d$, size of the solution will be $O(\sqrt{d}) \approx O(e^{\log d})$

A Close Look at the Solutions

- Every solution can be uniquely identified with $x + y\sqrt{d}$, $x, y > 0$
- Smallest solution with $x + y\sqrt{d}$ is called the Fundamental solution

$$x_1 + y_1\sqrt{d}$$

- Every other solution can be obtained as power of the fundamental solution

$$x + y\sqrt{d} = (x_1 + y_1\sqrt{d})^n$$

- It suffices to compute the fundamental solution

A Closer Look at the Solutions

d	x
10	19
13	649
29	9801
53	66249
61	1766319049
109	158070671986249
181	2469645423824185801
277	159150073798980475849
397	838721786045180184649
409	25052977273092427986049
421	3879474045914926879468217167061449

Regulator

- $O(x_1 + y_1\sqrt{d}) = O(e^{\sqrt{d}})$
- Just to write down the solution will take exponential amount of write operations
- We will rather compute a representation of the solution
- Regulator $R_d = \ln(x_1 + y_1\sqrt{d})$, and $x_1 + y_1\sqrt{d}$ is the smallest in magnitude of all solutions
- R_d being irrational is computed to n digit accuracy
- Even for this reduced problem the best classical algorithm has a running time $O(e^{\sqrt{\log d}}\,\mathrm{poly}(n))$

Overview of Hallgren's Algorithm

- Reformulate the Pell's equation as a period finding problem
  - Form a function $h(x)$ with period R_d
- Modify the quantum period finding algorithm to find irrational period
  - The quantum part of the algorithm
  - Computes only the integral part of R_d
- Perform classical post processing given the integral part of R_d
  - Compute the fractional part of R_d making use of the integral part of R_d provided by the previous step

Some Algebraic Number Theory

- Let $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$
- The solutions of Pell's equation are elements in $\mathbb{Q}(\sqrt{d})$
- $\mathcal{O}$ is called the ring of algebraic integers

$$\mathcal{O} = \{a \in \mathbb{Q}(\sqrt{d}) \mid f(a) = 0, f(x) \in \mathbb{Z}[x]\}$$

- $\mathbb{Z}[x]$ consists of polynomials with integral coefficients
- Units of $\mathcal{O}$ are elements in $\mathcal{O}$ that they have multiplicative inverses

$$\mathcal{O}^\times = \{\text{ Units of } \mathcal{O}\} = \{u \in \mathcal{O} \mid u^{-1} \text{ exists }\}$$

Algebraic Number Theory - cont'd

- $x + y\sqrt{d}$ is a solution of $x^2 - dy^2 = 1$ if and only if $x + y\sqrt{d}$ is a unit of $\mathcal{O}$
- ϵ_o smallest unit in $\mathcal{O}^\times$, with $\epsilon_o > 1$
- $\mathcal{O}^\times = \{\pm\epsilon_o^k \mid k \in \mathbb{Z}\}$
- $R_d = \ln \epsilon_o$
- All the solutions of $x^2 - dy^2$ can be obtained from the fundamental unit ϵ_o

Algebraic Number Theory - cont'd

- Product of sets $A, B \subseteq \mathbb{Q}(\sqrt{d})$, then

$$A \cdot B = \{\sum_{i=1}^{n} a_i b_i \mid n > 0, a_i \in A, b_i \in B\}$$

- Ideal $I \subseteq \mathbb{Q}(\sqrt{d})$ such that $I \cdot \mathcal{O} = I$
  - Integral Ideal $I \subseteq \mathcal{O}$
  - Fractional Ideal $I \subseteq \mathbb{Q}(\sqrt{d})$
  - Principal Ideal $I = \gamma\mathcal{O}$
- If $\epsilon \in \mathcal{O}$, then $\epsilon\mathcal{O} = \mathcal{O}$
- Equality of ideals $\alpha\mathcal{O} = \beta\mathcal{O}$ if and only if $\alpha = \beta\epsilon$, where ϵ is a unit in $\mathcal{O}$

Reformulating Pell's equation

- Let $\mathcal{P} = \{\gamma\mathcal{O} \mid \gamma \in \mathbb{Q}(\sqrt{d})\}$
- Consider $g : \mathbb{R} \to \mathcal{P}$

$$g(x) = e^x\mathcal{O} = I_x$$

- $g(x)$ is periodic with R_d

$$\begin{aligned} g(x + kR_d) &= e^{x+kR_d}\mathcal{O}, \\ &= e^x\epsilon_o^k\mathcal{O} = e^x\mathcal{O} \\ &= g(x) \end{aligned}$$

Using a periodic function to find R_d

- Naive algorithm to compute R_d
  - Find $g(x) = I_x$
  - Find $y > x$ such that $g(y) = I_x$
  - $y - x = kR_d$
- Another naive algorithm
  - Assume that the ideals could be ordered somehow
  - Given I_x find $g^{-1}(I_x)$
  - Find an ideal I_y next to I_x such that $I_y = I_x$
  - $g^{-1}(I_y) - g^{-1}(I_x) = kR_d$

Problems with the Naive Algorithms

- $y > e^{R_d}$ is exponentially large in $\log d$
- I_x is an infinite set, comparing two ideals poses problem
- There are infinitely many ideals between $x, x + \delta$ for which $I_x = I_{x+\delta}$, $\mathbb{Q}(\sqrt{d})$ and $\mathcal{P}$ are both dense
- We need to somehow order the ideals
- We need to move from one ideal to another
- Finite precision arithmetic

More Algebraic Number Theory

- $\mathcal{O}$ is a $\mathbb{Z}$-module, so it behaves like a vector space

$$\begin{aligned} \mathcal{O} &= m + n\frac{D+\sqrt{D}}{2}, D = \begin{cases} d, & d \equiv 1 \mod 4 \\ 4d, & d \equiv 2,3 \mod 4 \end{cases}, \\ \mathcal{O} &= \mathbb{Z} + \frac{D+\sqrt{D}}{2}\mathbb{Z} \end{aligned}$$

- For any principal ideal $I = \gamma\mathcal{O}$

$$I = \gamma\mathbb{Z} + \gamma\frac{D+\sqrt{D}}{2}\mathbb{Z}$$

Comparing Principal Ideals

- The basis is not unique, we can rewrite I as

$$I = k\left(a\mathbb{Z} + \frac{b+\sqrt{D}}{2}\mathbb{Z}\right)$$

$$\begin{array}{ll} -a < b \leq a, & a > \sqrt{D} \\ \sqrt{D} - a < b \leq \sqrt{D}, & a < \sqrt{D} \end{array}$$

- Presentation of an ideal is the triplet (a, b, k) which is computable in polynomial time given γ.
- Addresses the problem of comparing infinite sets. Equality of ideals is equivalent to having the same presentation

Discretizing Ideals

- Reduced principal ideals have the form

$$I = \mathbb{Z} + \frac{b + \sqrt{D}}{2}\mathbb{Z}$$

- Reduced principal ideals are finite in number
- Addresses the problem of density of sets $\mathbb{Q}(\sqrt{d})$ and $\mathcal{P}$
- Cycle of Reduced Principal Ideals

$$J = \{\mathcal{O} = J_0, J_1, \ldots, J_{m-1}\}$$

Moving Among Ideals

- $I = \mathbb{Z} + \gamma\mathbb{Z}$, then define

$$\rho(I) = \frac{1}{\gamma} I$$

- Gives another principal ideal
- If $I \in J$ then $\rho(I) \in J$
- If repeated then finally it gives a reduced principal ideal
- If I was reduced principal ideal $\rho(I)$is another reduced principal ideal
- Since there are a finite number of reduced principal ideals it cycles

Moving Among Ideals - cont'd

- $\sigma(I) : \sqrt{d} \mapsto -\sqrt{d}$
- Inverse operation of moving back is given by $\rho^{-1} = \sigma\rho\sigma$
- This addresses the problem of moving between the ideals back and forth

Ordering Ideals

- Let $I_y = \gamma I_x$. Then the distance between I_y and I_x is

$$\delta(I_x, I_y) = \ln \gamma$$

- Distance from $\mathcal{O}$: $\delta(e^x \mathcal{O}) = \delta(\mathcal{O}, e^x \mathcal{O}) = \ln e^x = x$
- Distance allows us to order the ideals along the number line in the same form as the input x
- Addresses the problems of invertibility and ordering
- If $I_x = I_y$, then $\delta(I_x, I_y) = y - x = kR_d$
- $\delta(I, \rho(I))$ can be computed in polynomial time

Spacing of Ideals

- $\delta(J_i, J_{i+1}) \geq \frac{3}{32D}$
- $\delta(J_i, J_{i+2}) \geq \ln 2$
- $\delta(J_i, J_{i+1}) \leq \frac{1}{2} \ln D$
- If we succesively apply ρ to a non reduced ideal I, until we just get a reduced principal ideal I_{red}, then

$$|\delta(I, I_{red})| \leq \ln D$$

and $I_{red} \in \{J_{k-1}, J_k, J_{k+1}\}$

Jumping Across Ideals

- We note that the ideals are exponential in number so moving across efficiently requires more than use of reduction operator ρ
- Use the product of ideals to move faster than ρ
- $I_1 \cdot I_2$ is much farther from $\mathcal{O}$ than either of I_1, I_2
- $\delta(I_1 \cdot I_2) = \delta(I_1) + \delta(I_2)$
- Product of ideals is not necessarily reduced so we reduce it to bring it back to the principal cycle of reduced ideals
- We denote this operation by $*$

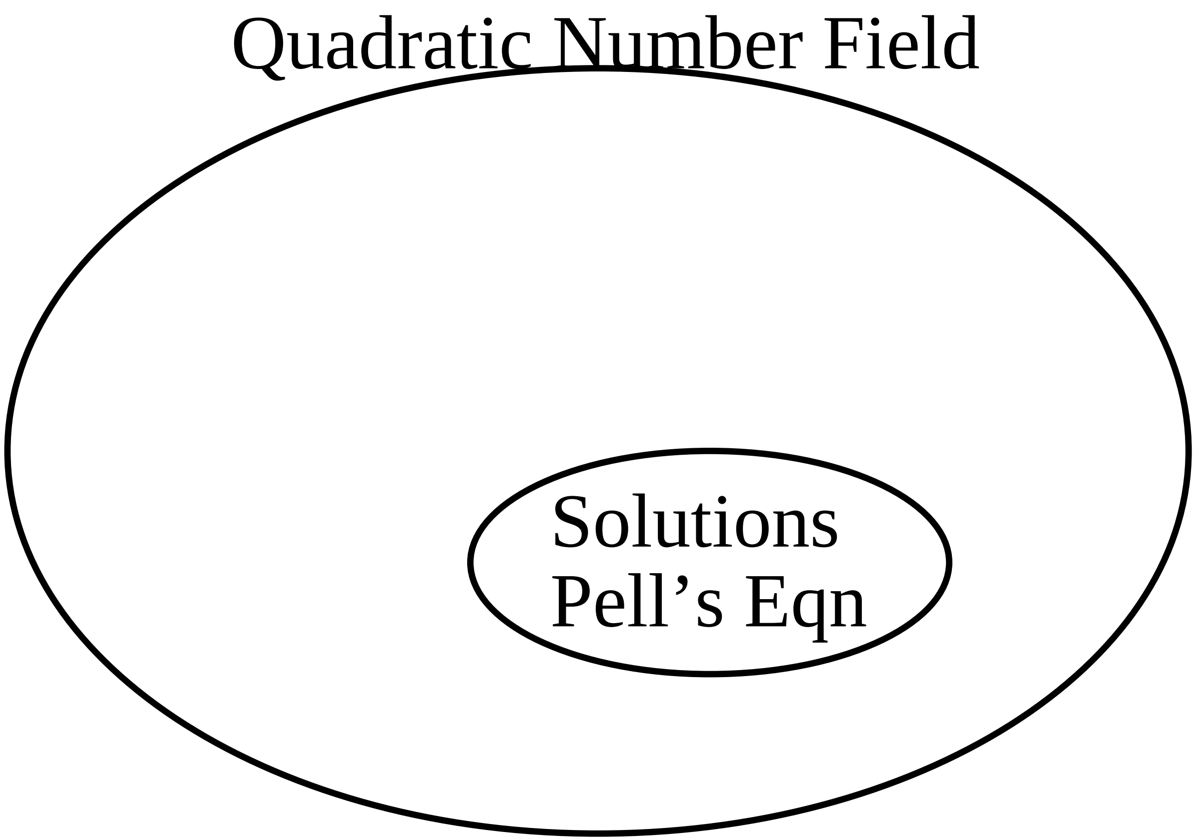
Review

- We need positive, intgeral solutions for $x^2 - dy^2 = 1$
- Each solution can be encoded as $x + y\sqrt{d}$ an element in $\mathbb{Q}(\sqrt{d})$
- All solutions can be obtained from the smallest solution $x_1 + y_1\sqrt{d}$
- We introduced the Regulator $R_d = \ln(x_1 + y_1\sqrt{d})$

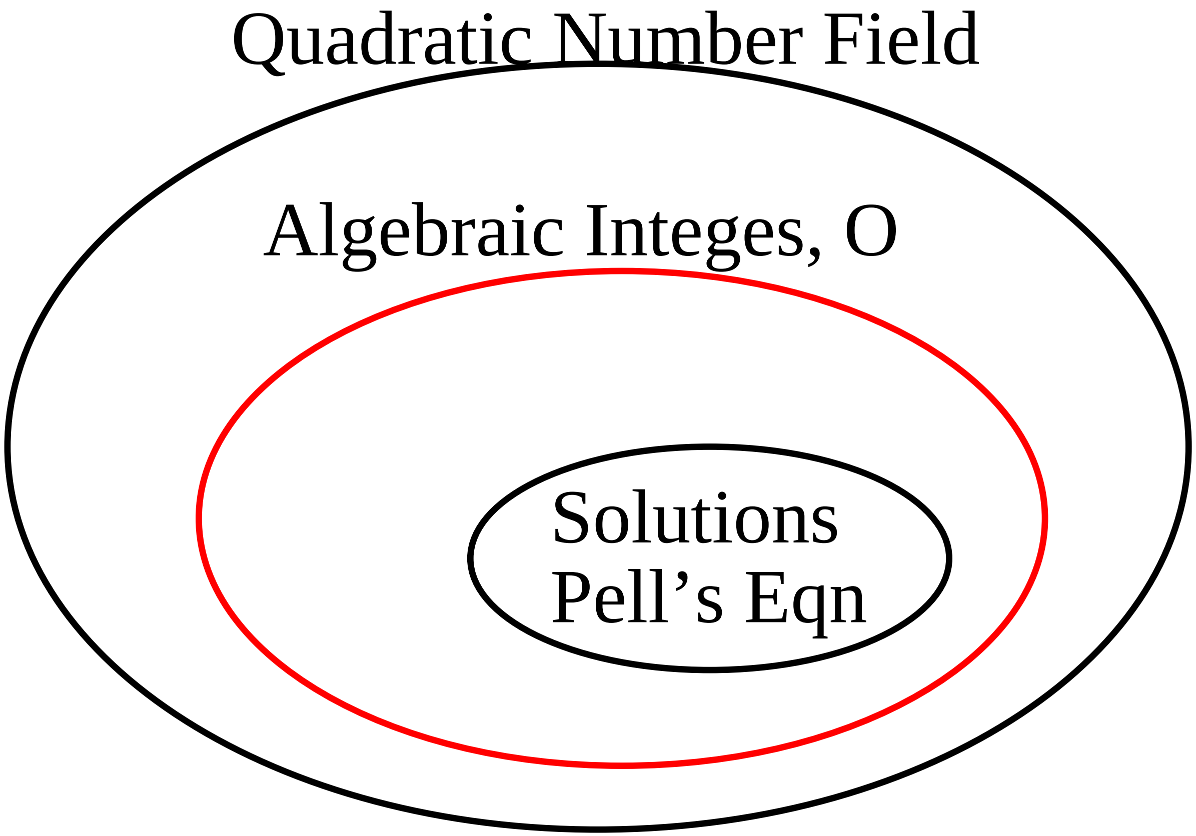
Review - cont'd

- Every solution is an element of $\mathbb{Q}(\sqrt{d})$
- More specifically every solution is also an element of the ring of algebraic integers in $\mathbb{Q}(\sqrt{d})$
- A solution of Pell's equation is precisely the set elements in $\mathcal{O}$ which have multiplicative inverses
- Our goal is to compute the generator of this subgroup which is precisely the regulator R_d

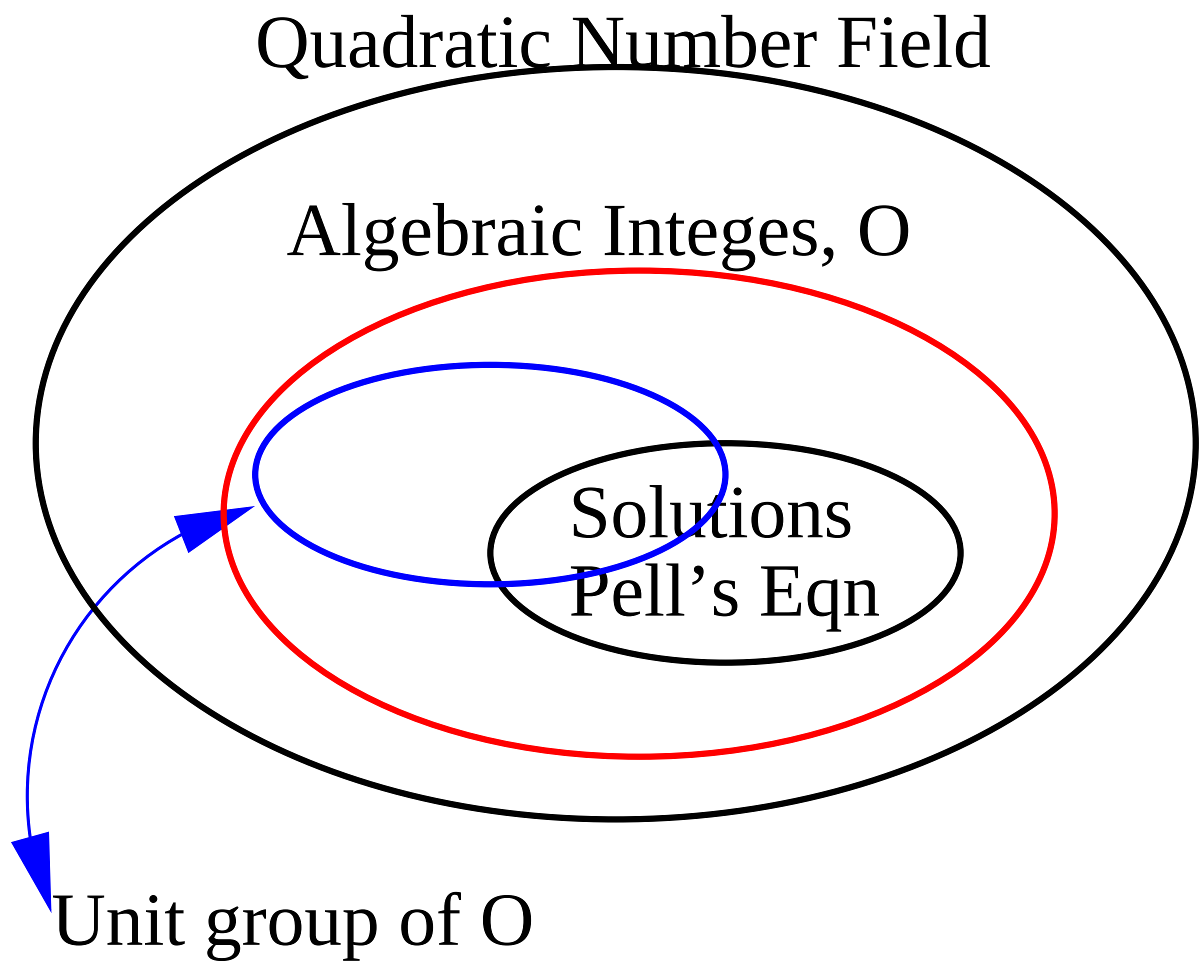
Review - cont'd



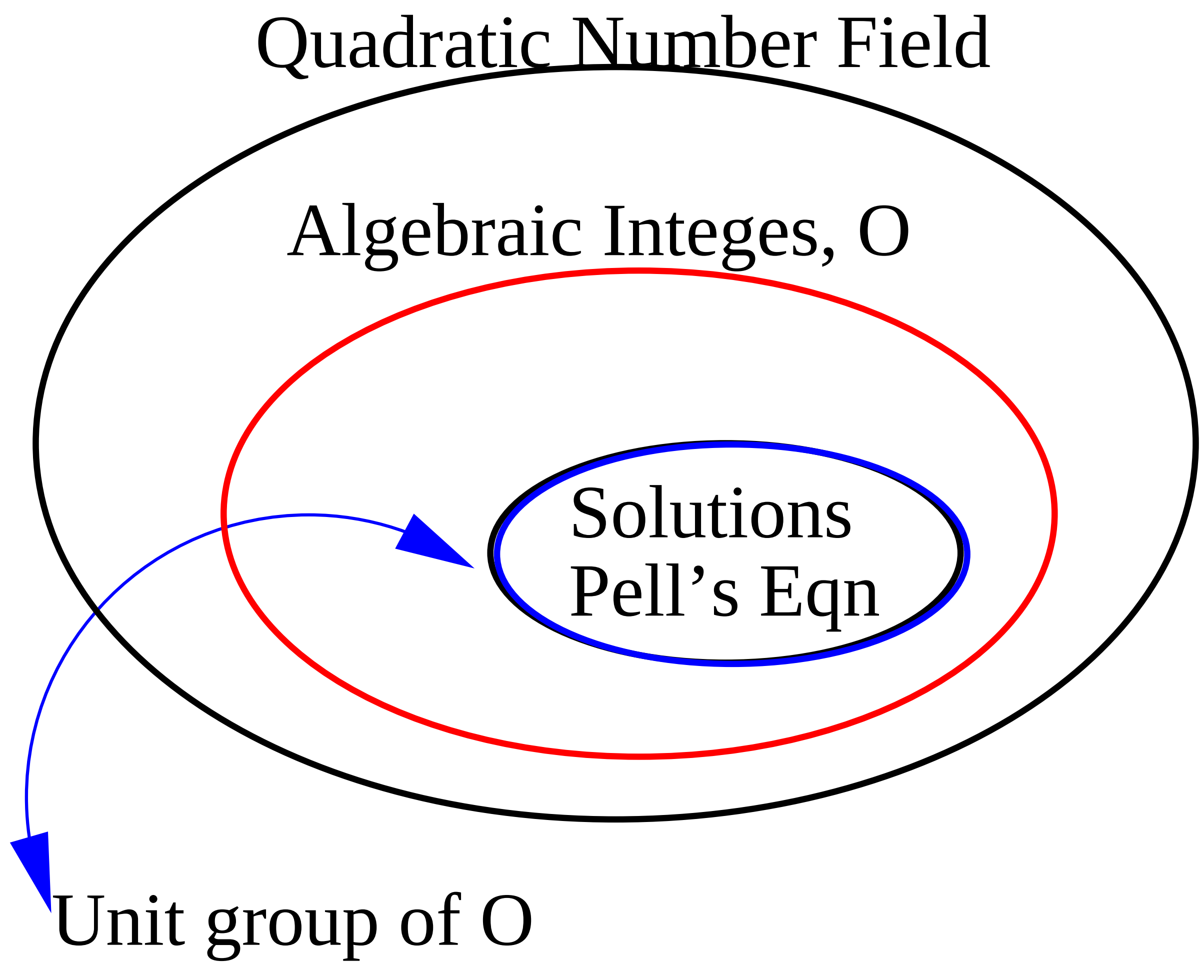
Review - cont'd



Review - cont'd



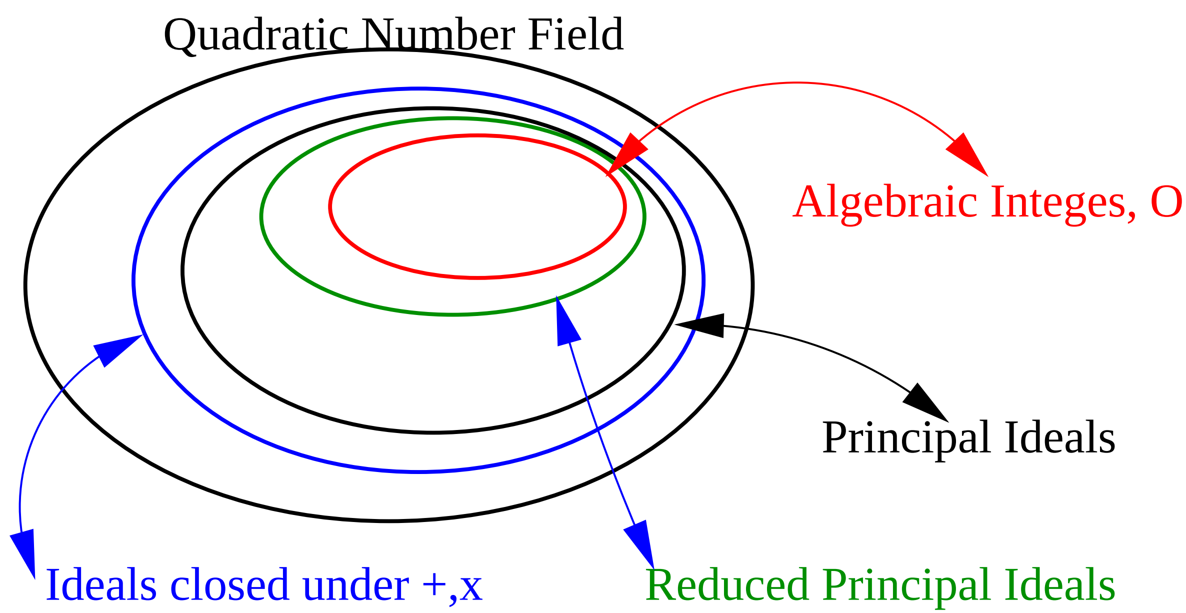
Review - cont'd



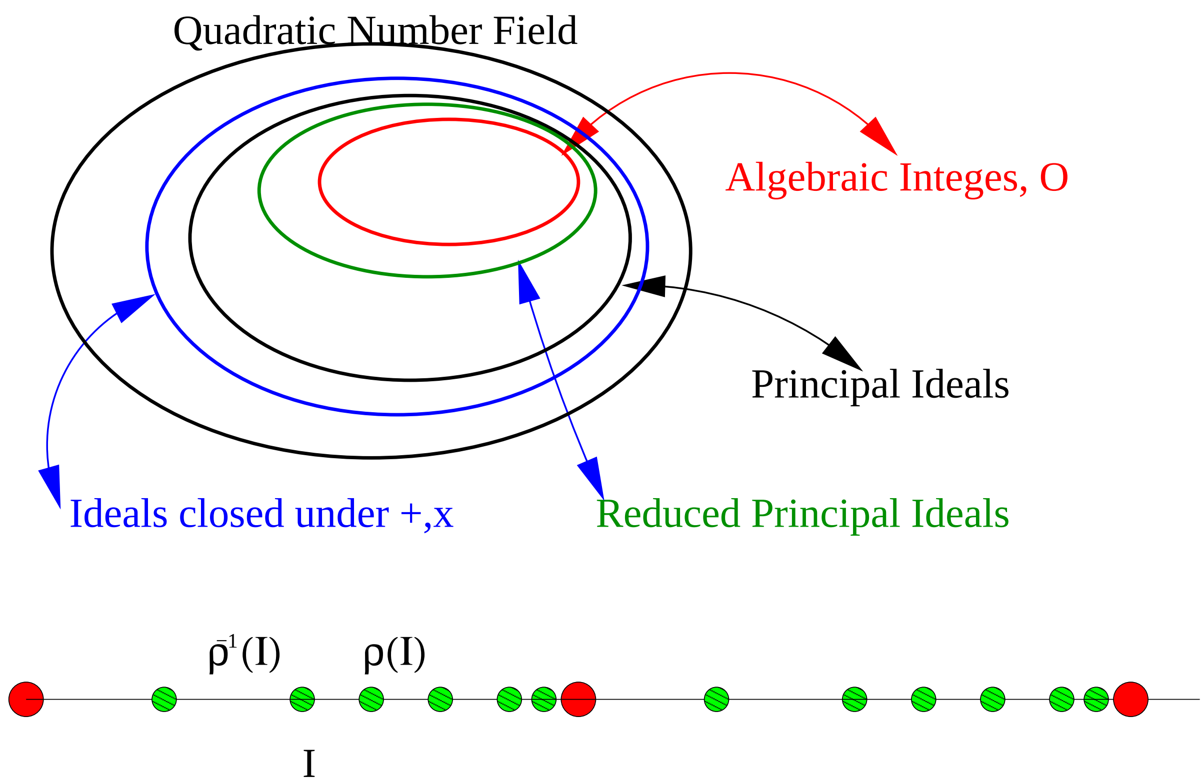
Review - cont'd

- We then defined the ideals as special sets in $\mathbb{Q}(\sqrt{d})$ which are loosely speaking closed under addition and multiplication
- A special type of ideals are the principal ideals which take the form $I = \gamma\mathcal{O}$
- We defined a periodic function that is periodic with R_d from $\mathbb{R}$ to the set of principal reduced ideals
- They can all be ordered with respect to their distance from $\mathcal{O}$
- We can move among the ideals using ρ and ρ^{-1}
- We have a means of moving from one ideal to another exponentially large steps

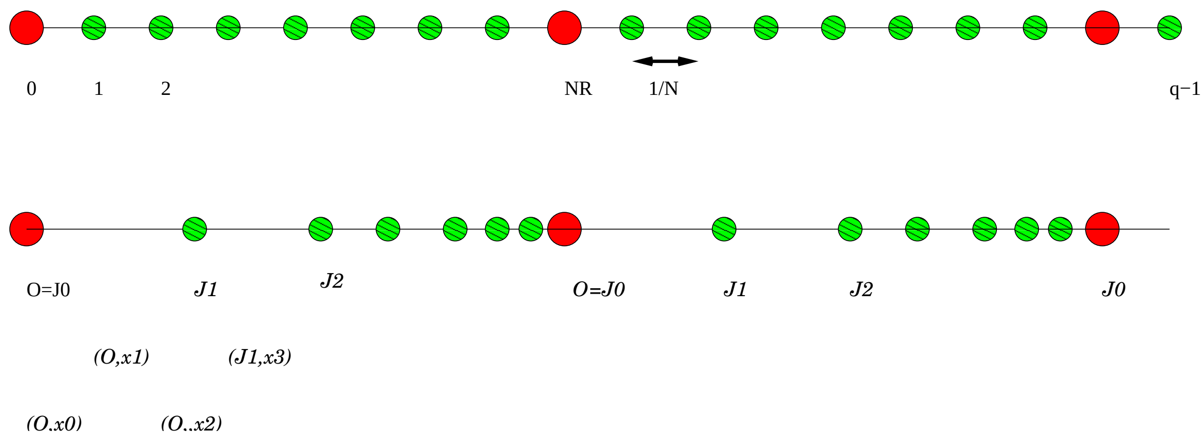
Review - cont'd



Review - cont'd

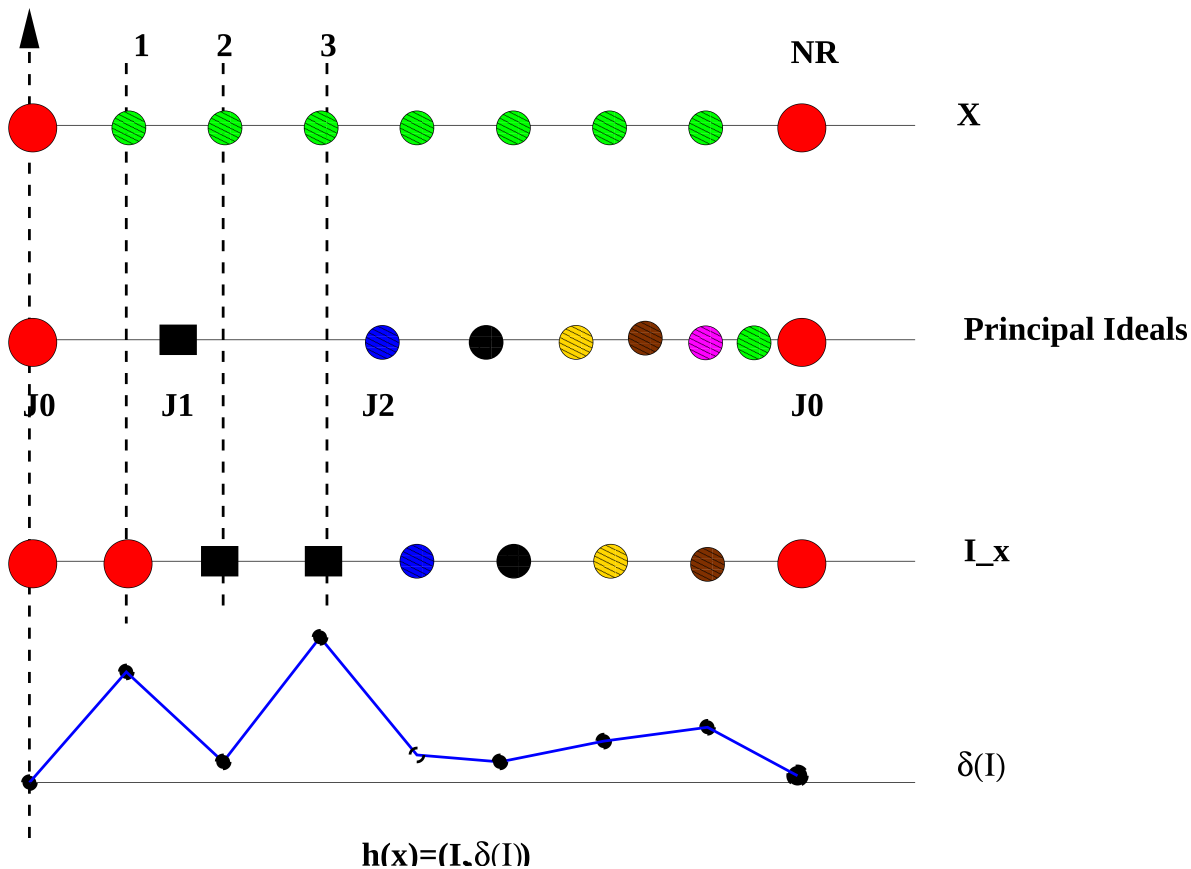


Hallgren's Periodic Function



- $h(x) = (g(x), x - \delta(g(x))) = (I_x, x - \delta(I_x))$
- I_x is the nearest reduced principal ideal to the left of x i.e, $\delta(I_x) < x$
- $h(x)$ is periodic with R_d
- $h(x)$ is one to one

Hallgren's Periodic Function

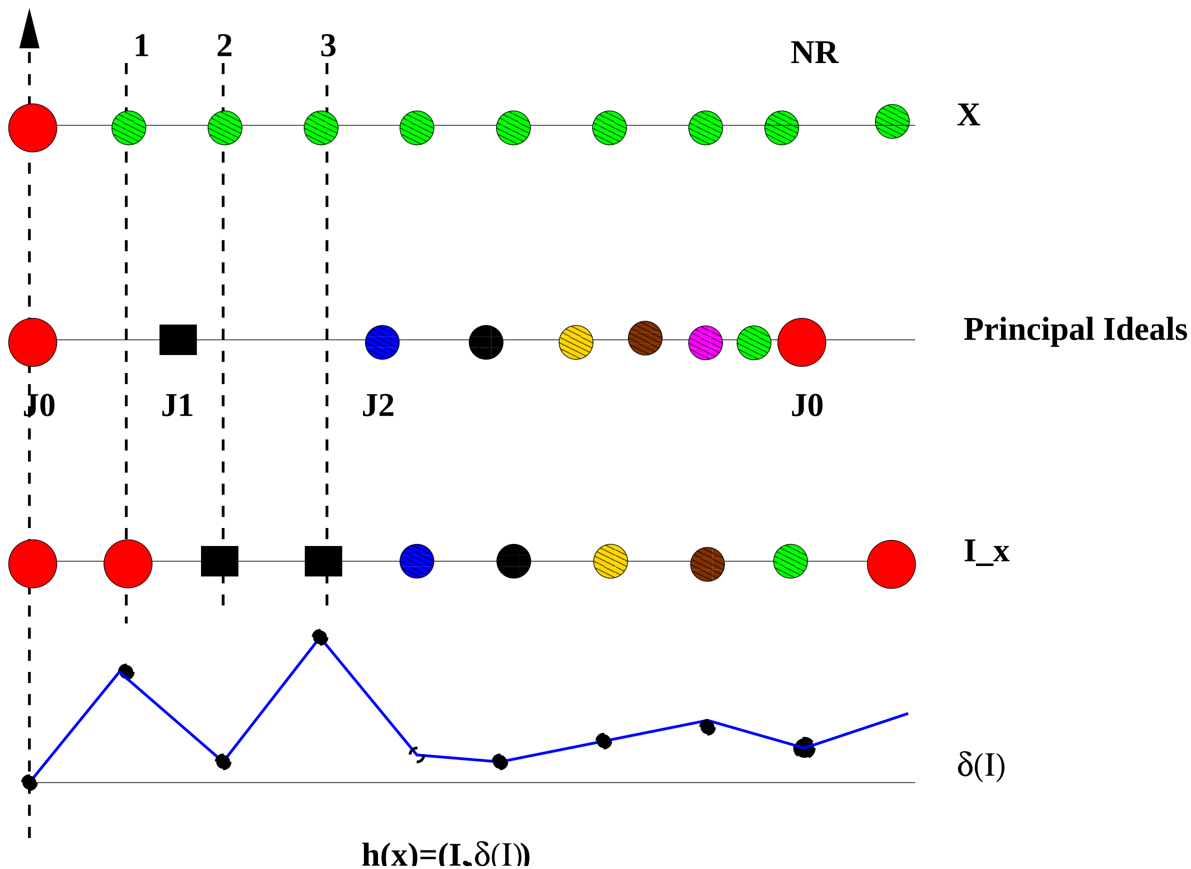


- $h(x) = (g(x), x - \delta(g(x))) = (I_x, x - \delta(I_x))$

Discretizing $h(x)$

- For practical implementation we would like to discretize $h(x)$
- Assuming that x is discretized with a step of $1/N$ the discretized function $h_N(k) = \lfloor h(k/N) \rfloor_N$
- $h_N(k)$ is weakly periodic with $P = NR_d$
- $h_N(k + \lfloor lNR_d \rfloor) = h_N(k)$ or $h_N(k + \lceil lNR_d \rceil) = h_N(k)$

Hallgren's Periodic Function



- After discretization $h(x)$ is weakly periodic not periodic

Quantum Period Finding Algorithms

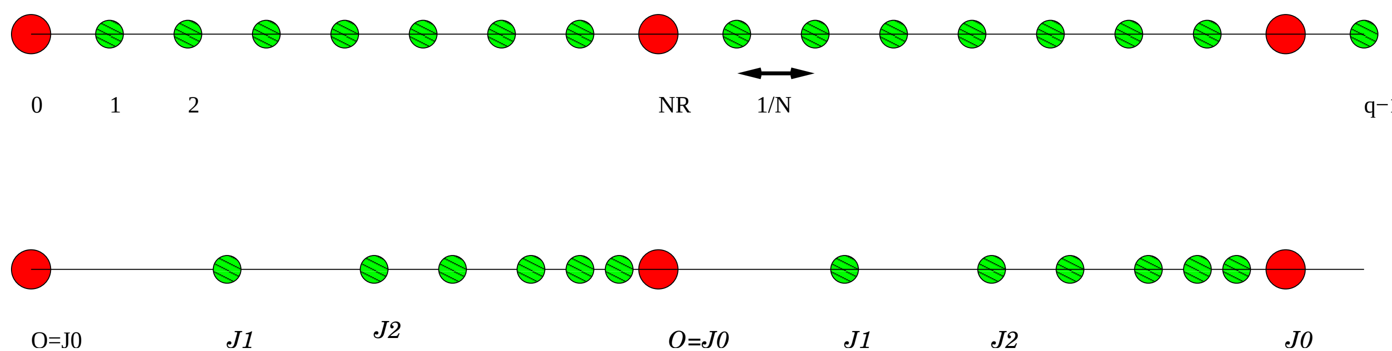
- A state in superposition
- Transformation to a state with a suitable function
- Partial measurement
- Fourier transform to get rid of offset
- Measurement
- Classical post processing

Hallgren's Period Finding Algorithm

- Form is an uniform superpostion of q states where $q = pNR_d + r$

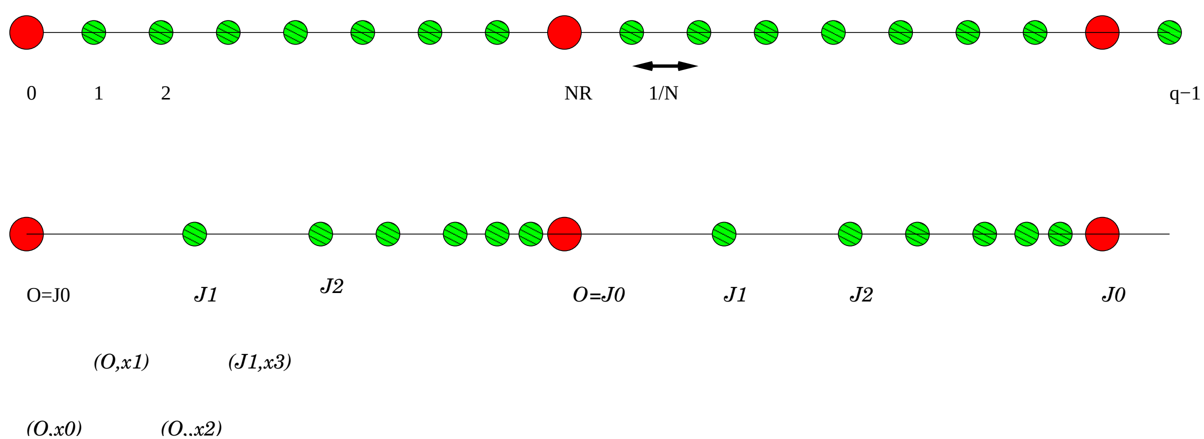
$$|\psi\rangle = \frac{1}{\sqrt{q}} \sum_{j=0}^{q-1} |j\rangle|0\rangle$$

- Compute $h_N(|\psi\rangle)$

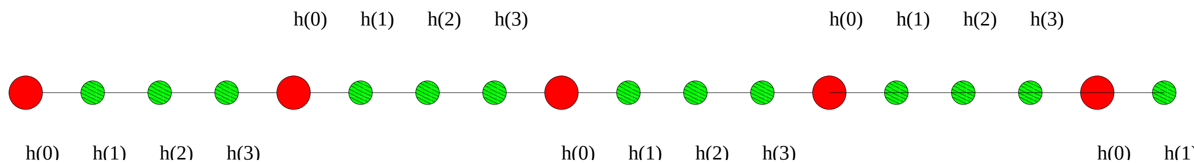


Superposition

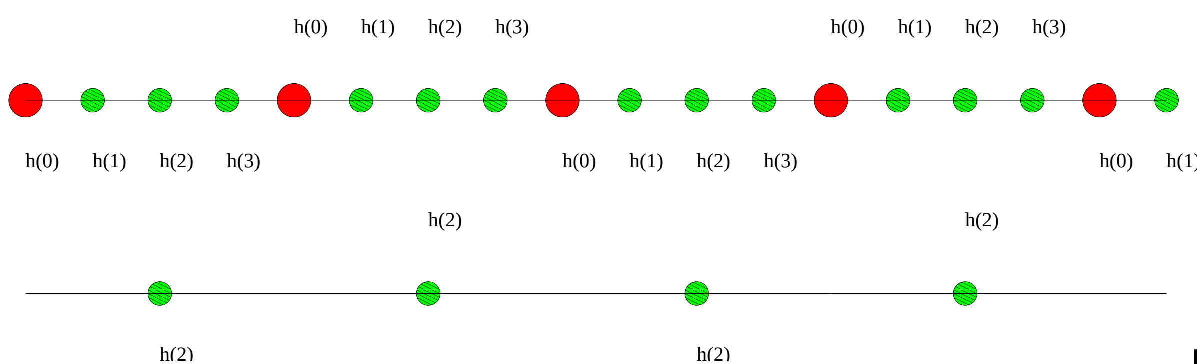
$$h_N|\psi\rangle = \frac{1}{\sqrt{q}} \sum_{j=0}^{q-1} |j\rangle |h_N(j)\rangle$$



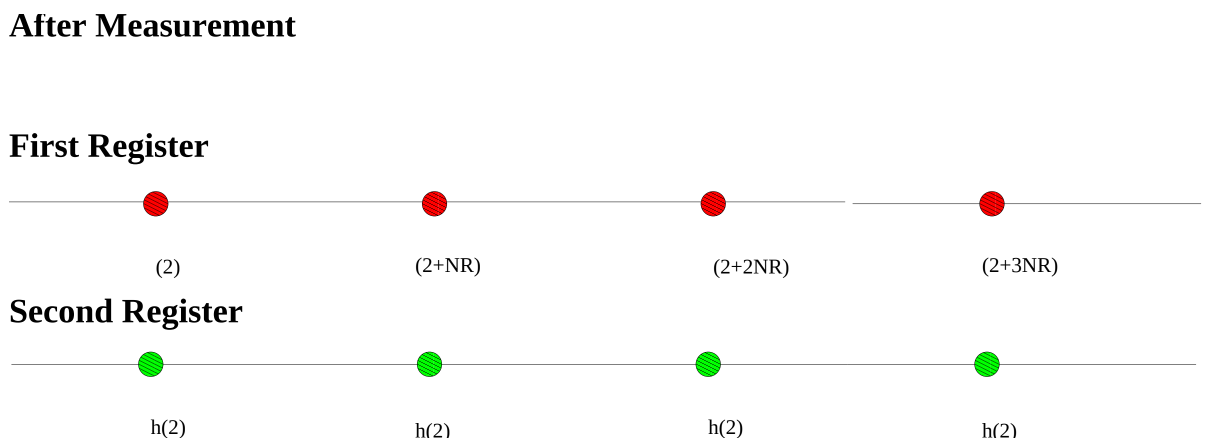
Partial Measurement



- $$h_N|\psi\rangle = \frac{1}{\sqrt{q}} \sum_{j=0}^{NR_d-1} \left(\sum_{l=0}^{p-1} |j + [lNR_d]\rangle \right) |h_N(j)\rangle$$
- Measure the second register, say we measure $h_N(k)$



Partial Measurement - cont'd



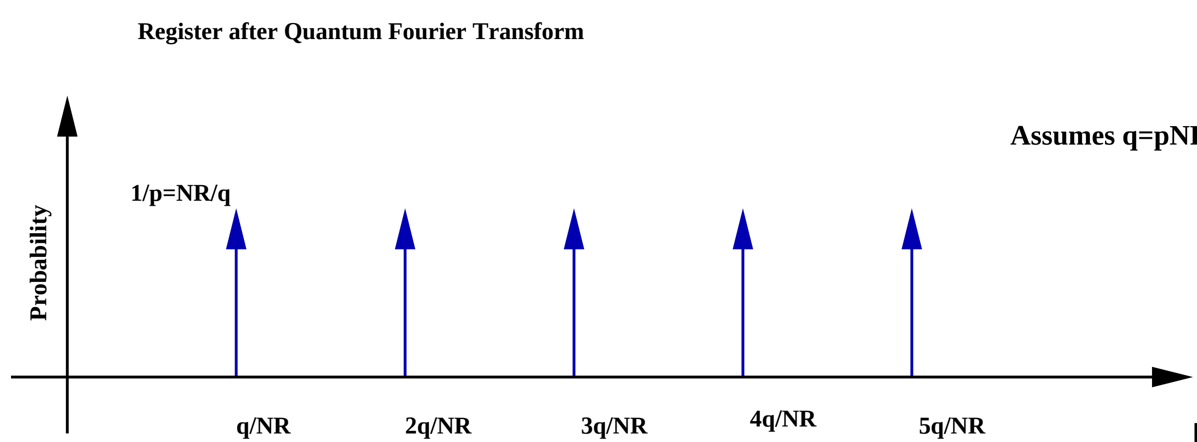
- On measurement the state will collapse to

$$|\psi\rangle = \frac{1}{\sqrt{p}} \sum_{n=0}^{p-1} |k + [nNR_d]\rangle |h_N(k)\rangle$$

QFT to Remove Offset

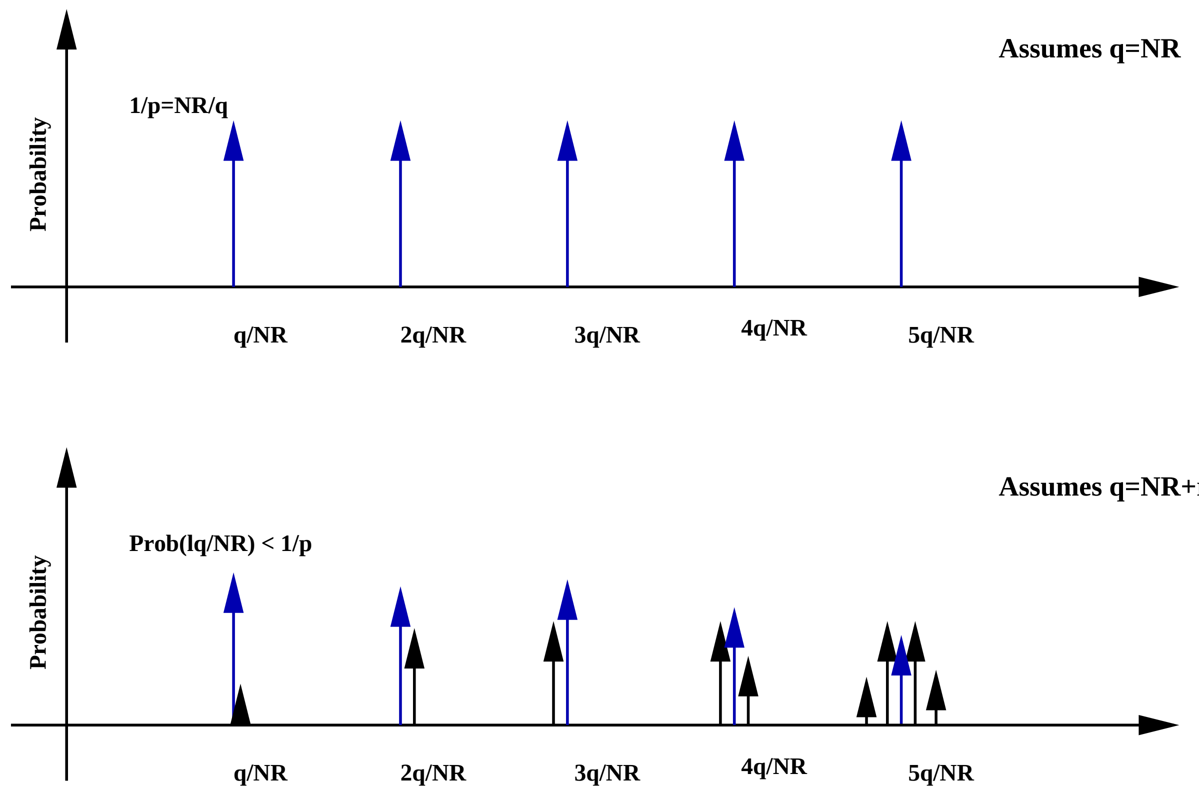
- Take the Quantum Fourier transform

$$\begin{aligned}\mathcal{F}|\psi\rangle &= \frac{1}{\sqrt{pq}}\sum_{n=0}^{p-1}\sum_{j=1}^{q-1} e^{2\pi i(k+[nNR_d])}|j\rangle, \\ &= \sum_{j=0}^{q-1} a_j|j\rangle\end{aligned}$$

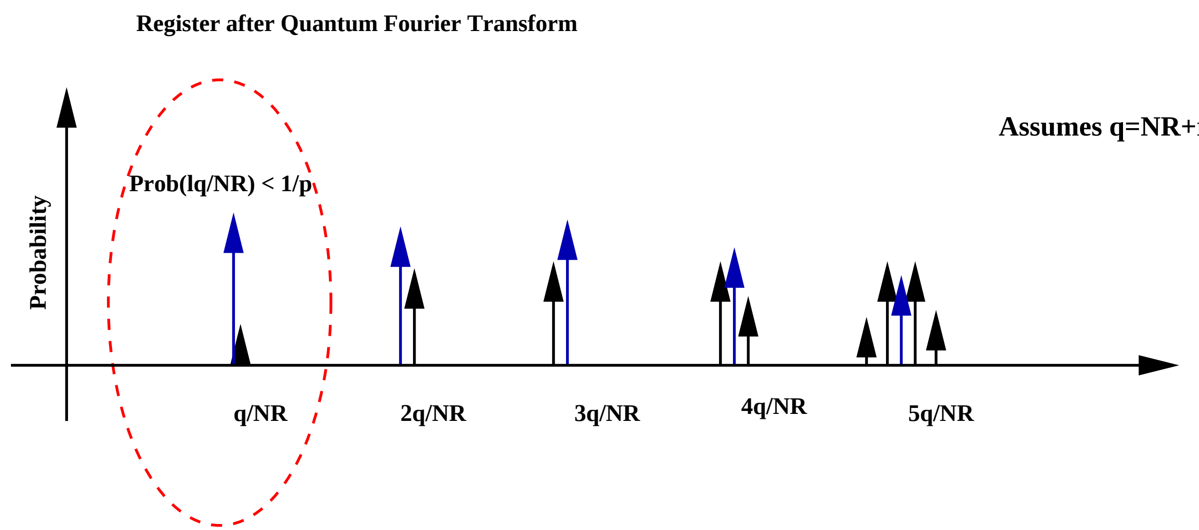


QFT - cont'd

Register after Quantum Fourier Transform



Identifying Periodicity



- We are interested in
  - $j = lq/NR$
  - j is small, more precisely, $j < \frac{q}{\log NR_d}$
- $Prob(j)$ must be large

Identifying Periodicity - cont'd

- For sufficiently large $q \geq 3(NR_d)^2$, many j such that
  - j is a multiple of q/NR_d
  - $j < \frac{q}{\log NR_d}$
- Probability of such j is highly likely,

$$Prob(j) > \frac{\alpha}{\log NR_d},$$

α a constant

Extracting Periodicity

- But how do we extract the periodicity from the state?
- Measure and repeat to get another measurement such that
  - $c = [kq/NR_d]$
  - $d = [lq/NR_d]$
- We do not know k, l, R_d
- Compute the convergents of $\frac{c}{d}$
- $$|\frac{c}{d} - \frac{a}{b}| < \frac{1}{2b^2}$$

Extracting Periodicity - cont'd

- Compute the convergents of c/d then

$$\frac{k}{l} = \frac{c_n}{d_n} \text{ and } k = c_n,$$

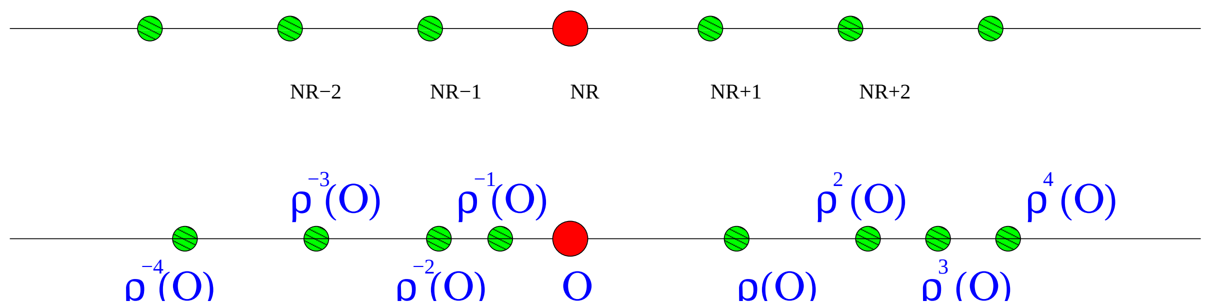
for some n

- $c = [\frac{kq}{NR_d}] = \frac{kq}{NR_d}$
- Estimate the period as

$$\overline{NR_d} = [\frac{kq}{c}]$$

- Check if $\overline{NR_d} = c_n q/c$ satisfies $|lR_d - \overline{NR_d}| < 1$

Extracting Periodicity - cont'd



- If $|\overline{NR_d} - jR_d| < 1$, then $h(\overline{NR_d})$ is an ideal among $\{\rho^{-4}(\mathcal{O}), \rho^{-3}(\mathcal{O}), \ldots, \mathcal{O}, \ldots, \rho^3(\mathcal{O}), \rho^4(\mathcal{O})\}$
- Because $\delta(I, \rho^2(I)) > \ln 2 > 0.693$

Integral Part of R_d

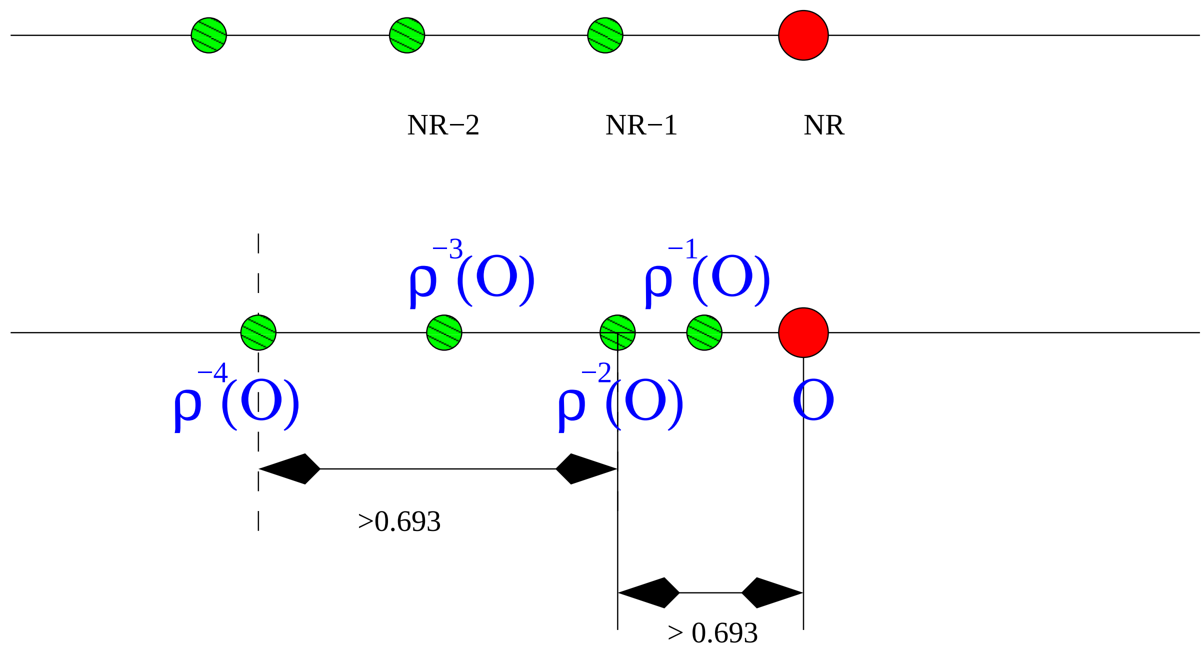
- Integral part of R_d

$$\lfloor R_d \rfloor = \left\lfloor \frac{\overline{NR_d}}{N} \right\rfloor$$

- We know R_d to a precision $1/N$
- With probability $\geq 1/\operatorname{poly}(\log NR_d)$ this algorithm will return $\overline{NR_d}$ such that $|\overline{NR_d} - NR_d| < 1$

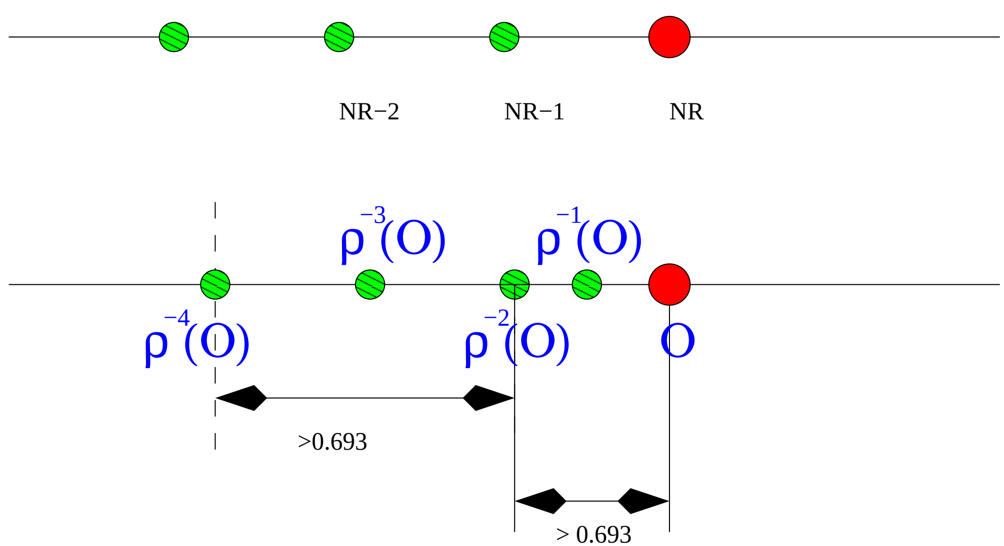
Computing the Fractional part of R_d

- Given $\lfloor R_d \rfloor$
- Compute $h(\lfloor R_d \rfloor) = (I_x, x - \delta(I_x))$



- We know that $\delta(I, \rho^2(I)) > \ln 2 = 0.693$

Computing the Fractional part of R_d - c



- Therefore $\delta(I, \rho^4(I)) > 2\ln 2 > \lceil R_d \rceil$
- This implies that $\mathcal{O}$ must be one of the ideals $\{\rho^{-3}(\mathcal{O}), \rho^{-2}(\mathcal{O}), \rho^{-1}(\mathcal{O}), \mathcal{O}\}$
- $\delta(I, \mathcal{O}))$ can be computed in polynomial and this gives the fractional part of R_d

Summary of the Algorithm

- Start with a superpostion of inputs
- Compute Hallgren's periodic fucntion for all these inputs
- Perform partial measurement
- Perform QFT to get rid of offset
- Perform a measurement to get c
- Repeat to get another value d
- Extract the Integral part of R_d
- Compute the fractional part of R_d

Applications

- Principal Ideal Problem
  - Given an ideal determine if it is a principal ideal
- Class Group structure
  - Determine the structure of the group $\mathcal{I}_{inv}/\mathcal{P}$

Principal Ideal Problem

- Recall an ideal $I \subseteq \mathbb{Q}(\sqrt{d})$ such that $I \cdot \mathcal{O} = I$
- Principal ideal $I = \gamma\mathcal{O}$
- All ideals of the form $I = \alpha\mathbb{Z} + \beta\mathbb{Z}$
- Given an ideal, decide if there exists a γ such that $I = \gamma\mathcal{O}$

Computing the Class Group

- Invertible ideals
  - An ideal I is called invertible if there exists another ideal J such that $I \cdot J = \mathcal{O}$
  - Let $\mathcal{I} = \{I \mid I^{-1}$ exists $\}$
  - $\mathcal{P} = \{I \mid I = \gamma\mathcal{O}\}$
  - Let $C = \mathcal{I}/\mathcal{P}$
  - C is a finite abelian group and called the class group
  - Class group problem is to determine the structure of C

Generalizations

- A general problem is to compute the unit group of a $\mathcal{O} \subseteq \mathbb{Q}(\theta)$ where $[\mathbb{Q}(\theta) : \mathbb{Q}] = n$
- For Pell's equation $n = 2$
- Similarly the class group and the principal ideal problem also can be generalized
- Two algorithms for the same have appeared recently by Hallgren and Vollmer, Schmidt independetly this year

Questions ?

Questions ?

Thank You