Quantum algorithms (CO 781/CS 867/QIC 823, Winter 2011)
Andrew Childs, University of Waterloo

LECTURE 11: The HSP in the Heisenberg group

We showed that the quantum query complexity of the general hidden subgroup problem is polynomial by measuring $\rho_H^{\otimes \mathrm{poly}(\log|G|)}$ using a particular measurement strategy (the *pretty good measurement*) that identifies H with high probability. One strategy for finding an efficient quantum algorithm for the HSP is to find an efficient way of implementing that particular measurement. In this lecture, we will describe an efficient quantum algorithm for the HSP in the Heisenberg group that effectively implements the pretty good measurement.

The Heisenberg group

There are several different ways to define the Heisenberg group. For those familiar with quantum error correcting codes on higher-dimensional systems, perhaps the most familiar definition is as follows. Given a prime number p, define operators X and Z acting on an orthonormal basis of states $\{|x\rangle : x \in \mathbb{Z}_p\}$ by

$$X|x\rangle = |x+1 \bmod p\rangle \tag{1}$$

$$Z|x\rangle = \omega_p^x |x\rangle. \tag{2}$$

These operators satisfy the relation $ZX = \omega_p XZ$. Using this relation, any product of X's and Z's can be written in the form $\omega_p^a X^b Z^c$, where $a, b, c \in \mathbb{Z}_p$. Thus the operators X and Z generate a group of order p^3, which is precisely the Heisenberg group. Writing the group elements in the form (a, b, c) with $a, b, c \in \mathbb{Z}_p$, it is straightforward to work out the group law

$$(a, b, c) \cdot (a', b', c') = (a + a' + b'c, b + b', c + c'). \tag{3}$$

Equivalently, the Heisenberg group is the group of lower triangular 3×3 matrices

$$\left\{ \begin{pmatrix} 1 & 0 & 0 \\ b & 1 & 0 \\ a & c & 1 \end{pmatrix} : a, b, c \in \mathbb{F}_p \right\} \tag{4}$$

over $\mathbb{F}_p$, and the semidirect product $\mathbb{Z}_p^2 \rtimes_\varphi \mathbb{Z}_p$, where $\varphi : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_p^2)$ is defined by $\varphi(c)(a, b) = (a + bc, b)$.

To solve the HSP in the Heisenberg group, it is sufficient to be able to distinguish the following cyclic subgroups of order p:

$$H_{a,b} := \langle (a, b, 1) \rangle = \{(a, b, 1)^x : x \in \mathbb{Z}_p\}. \tag{5}$$

The reduction to this case is essentially the same as the reduction of the dihedral hidden subgroup problem to the case of a hidden reflection, so we omit the details. The elements of such a subgroup are

$$(a, b, 1)^2 = (2a + b, 2b, 2) \tag{6}$$

$$(a, b, 1)^3 = (a, b, 1)(2a + b, 2b, 2) = (3a + 3b, 3b, 3) \tag{7}$$

$$(a, b, 1)^4 = (a, b, 1)(3a + 3b, 3b, 3) = (4a + 6b, 4b, 4) \tag{8}$$

$$(a, b, 1)^5 = (a, b, 1)(4a + 6b, 4b, 4) = (5a + 10b, 5b, 5) \tag{9}$$

etc., and a straightforward inductive argument shows that a general element has the form

$$(a, b, 1)^x = (xa + \tbinom{x}{2}b, xb, x). \tag{10}$$

Furthermore, it is easy to see that the p^2 elements $(\ell, m, 0)$ for $\ell, m \in \mathbb{Z}_p^2$ form a left transversal of $H_{a,b}$ in the Heisenberg group for any $a, b \in \mathbb{Z}_p$.

Fourier sampling

Suppose we are given a function that hides $H_{a,b}$ in the Heisenberg group. Then the standard method can be used to produce the coset state

$$|(\ell, m, 0)H_{a,b}\rangle = \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{Z}_p} |\ell + xa + \tbinom{x}{2}b, m + xb, x\rangle \tag{11}$$

for some uniformly random, unknown $\ell, m \in \mathbb{Z}_p$. Our goal is to determine the parameters $a, b \in \mathbb{Z}_p$ using the ability to produce such states.

At this point, we could perform weak Fourier sampling over the Heisenberg group without discarding any information. However, as in the case of the dihedral group, it will be simpler to consider an abelian Fourier transform instead of the full nonabelian Fourier transform. Using the representation theory of the Heisenberg group, one can show that this procedure is essentially equivalent to nonabelian Fourier sampling.

Fourier transforming the first two registers over $\mathbb{Z}_p^2$, we obtain the state

$$(F_{\mathbb{Z}_p} \otimes \mathbb{F}_{\mathbb{Z}_p} \otimes I_p)|(\ell, m, 0)H_{a,b}\rangle = \frac{1}{p^{3/2}} \sum_{x,s,t \in \mathbb{Z}_p} \omega_p^{s(\ell + xa + \binom{x}{2}b) + t(m + xb)} |s, t, x\rangle. \tag{12}$$

Now suppose we measure the values s, t appearing in the first two registers. In fact this can be done without loss of information, since the density matrix of the state (mixed over the uniformly random values of ℓ, m) is block diagonal, with blocks labeled by s, t. Collecting the coefficients of the unknown parameters a, b, the resulting p-dimensional quantum state is

$$|\widehat{H_{a,b;s,t}}\rangle := \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{Z}_p} \omega_p^{s(xa + \binom{x}{2}b) + t(xb)} |x\rangle \tag{13}$$

$$= \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{Z}_p} \omega_p^{a(sx) + b(s\binom{x}{2} + tx)} |x\rangle. \tag{14}$$

where the values $s, t \in \mathbb{Z}_p$ are known, and are obtained uniformly at random. We would like to use samples of this state to determine $a, b \in \mathbb{Z}_p$.

Two states are better than one

With only one copy of this state, there is insufficient information to recover the hidden subgroup: Holevo's theorem guarantees that a measurement on a p-dimensional quantum state can reliably communicate at most p different outcomes, yet there are p^2 possible values of $(a, b) \in \mathbb{Z}_p^2$. Thus we have to use at least two copies of the state. One can show that there exist single-register

measurements on this state that yield enough information to recover a, b with $\mathrm{poly}(\log p)$ samples—in fact, a random measurement has this property with high probability. But no single-register measurement is known from which a and b can be extracted *efficiently* (i.e., in time $\mathrm{poly}(\log p)$).

However, by making a joint measurement on two copies of the state, we can recover the information about a, b that is encoded in a quadratic function in the phase. To see this, consider the two-copy state

$$|\widehat{H_{a,b;s,t}}\rangle \otimes |\widehat{H_{a,b;u,v}}\rangle = \frac{1}{p} \sum_{x,y \in \mathbb{Z}_p} \omega_p^{a(sx+uy)+b(s\binom{x}{2}+tx+u\binom{y}{2}+vy)} |j, j'\rangle \tag{15}$$

$$= \frac{1}{p} \sum_{x,y \in \mathbb{Z}_p} \omega_p^{\alpha a+\beta b} |x, y\rangle, \tag{16}$$

where

$$\alpha := sx + uy \tag{17}$$

$$\beta := s\tbinom{x}{2} + tx + u\tbinom{y}{2} + vy \tag{18}$$

and where we suppress the dependence of α, β on s, t, u, v, x, y for clarity. If we could replace $|x, y\rangle$ by $|\alpha, \beta\rangle$, then the resulting state would be simply the Fourier transform of $|a, b\rangle$, and an inverse Fourier transform would reveal the solution. So let's compute the values of α, β in ancilla registers, giving the state

$$\frac{1}{p} \sum_{x,y \in \mathbb{Z}_p} \omega_p^{\alpha a+\beta b} |x, y, \alpha, \beta\rangle, \tag{19}$$

and attempt to uncompute the first two registers.

For fixed values of $\alpha, \beta, s, t, u, v \in \mathbb{Z}_p$, the quadratic equations (17)–(18) could have zero, one, or two solutions $x, y \in \mathbb{Z}_p$. Thus we cannot hope to erase the first and second registers by a classical procedure conditioned on the values in the third and fourth registers (and the known values of s, t, u, v). However, it is possible to implement a quantum procedure to erase the first two registers by considering the full set of solutions

$$S_{\alpha,\beta}^{s,t,u,v} := \{(x, y) \in \mathbb{Z}_p^2 : sx + uy = \alpha \text{ and } s\tbinom{x}{2} + tx + u\tbinom{y}{2} + vy = \beta\}. \tag{20}$$

The state (19) can be rewritten

$$\frac{1}{p} \sum_{x,y \in \mathbb{Z}_p} \omega_p^{\alpha a+\beta b} \sqrt{|S_{\alpha,\beta}^{s,t,u,v}|}\, |S_{\alpha,\beta}^{s,t,u,v}, \alpha, \beta\rangle, \tag{21}$$

where we use the convention that $|S\rangle := \sum_{s \in S} |s\rangle / \sqrt{|S|}$ denotes the normalized uniform superposition over the elements of the set S. Thus, if we could perform a unitary transformation satisfying

$$|S_{\alpha,\beta}^{s,t,u,v}\rangle \mapsto |\alpha, \beta\rangle \text{ for } |S_{\alpha,\beta}^{s,t,u,v}| \neq 0 \tag{22}$$

(and defined in any way consistent with unitarity for other values of α, β), we could erase the first two registers of (19), producing the state

$$\frac{1}{p} \sum_{\alpha,\beta \in \mathbb{Z}_p} \omega_p^{\alpha a+\beta b} \sqrt{|S_{\alpha,\beta}^{s,t,u,v}|}\, |\alpha, \beta\rangle. \tag{23}$$

(Note that in fact we could just apply the transformation (22) directly to the state (16); there is no need to explicitly compute the values α, β in an ancilla register.)

We refer to the inverse of the transformation (22) as *quantum sampling*, since the goal is to produce a uniform superposition over the set of solutions, a natural quantum analog of *random sampling* from those solutions.

Since the system of equations (17)–(18) consists of a pair of quadratic equations in two variables over $\mathbb{F}_p$, it has either zero, one, or two solutions $x, y \in \mathbb{F}_p$. In particular, a straightforward calculation shows that the solutions can be expressed in closed form as

$$x = \frac{\alpha s + sv - tu \pm \sqrt{\Delta}}{s(s+u)} \qquad\qquad y = \frac{\alpha u + tu - sv \mp \sqrt{\Delta}}{u(s+u)} \tag{24}$$

where

$$\Delta := (2\beta s + \alpha s - \alpha^2 - 2\alpha t)(s+u)u + (\alpha u + tu - sv)^2. \tag{25}$$

Provided $su(s+u) \neq 0$, the number of solutions is completely determined by the value of Δ. If Δ is a nonzero square in $\mathbb{F}_p$, then there are two distinct solutions; if $\Delta = 0$ then there is only one solution; and if Δ is a non-square then there are no solutions. In any event, since we can efficiently compute an explicit list of solutions in each of these cases, we can efficiently perform the transformation (22).

It remains to show that the state (23) can be used to recover a, b. This state is close to the Fourier transform of $|a, b\rangle$ provided the solutions are nearly uniformly distributed. Since the values of s, t, u, v are uniformly distributed over $\mathbb{F}_p$, it is easy to see that Δ is uniformly distributed over $\mathbb{F}_p$. This means that Δ is a square about half the time, and is a non-square about half the time (with $\Delta = 0$ occurring only with probability $1/p$). Thus there are two solutions about half the time and no solutions about half the time. This distribution of solutions is uniform enough for the procedure to work.

Applying the inverse quantum Fourier transform over $\mathbb{Z}_p \times \mathbb{Z}_p$, we obtain the state

$$\frac{1}{p^2} \sum_{\alpha,\beta,k,\ell \in \mathbb{Z}_p} \omega_p^{\alpha(a-k)+\beta(b-\ell)} \sqrt{|S_{\alpha,\beta}^{s,t,u,v}|}\, |k, \ell\rangle. \tag{26}$$

Measuring this state, the probability of obtaining the outcome $k = a$ and $\ell = b$ for any particular values of s, t, u, v is

$$\frac{1}{p^4} \left(\sum_{\alpha,\beta \in \mathbb{Z}_p} \sqrt{|S_{\alpha,\beta}^{s,t,u,v}|} \right)^2. \tag{27}$$

Since those values occur uniformly at random, the overall success probability of the algorithm is

$$\frac{1}{p^8} \sum_{s,t,u,v \in \mathbb{Z}_p} \left(\sum_{\alpha,\beta \in \mathbb{Z}_p} \sqrt{|S_{\alpha,\beta}^{s,t,u,v}|} \right)^2 \geq \frac{1}{p^{12}} \left(\sum_{s,t,u,v \in \mathbb{Z}_p} \sum_{\alpha,\beta \in \mathbb{Z}_p} \sqrt{|S_{\alpha,\beta}^{s,t,u,v}|} \right)^2 \tag{28}$$

$$\geq \frac{1}{p^{12}} \left(\sum_{\alpha,\beta \in \mathbb{Z}_p} \frac{p^4}{2 + o(1)} \sqrt{2} \right)^2 \tag{29}$$

$$= \frac{1}{2}(1 - o(1)), \tag{30}$$

which shows that the algorithm succeeds with probability close to $1/2$.