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

LECTURE 4: The abelian HSP and decomposition of abelian groups

In this lecture, we will see how to solve the hidden subgroup problem in any finite abelian group of known structure. We will also see how related techniques can be used to deduce the structure of an abelian group even if it is not initially known.

The abelian HSP

Recall that in the hidden subgroup problem, we are given a function $f : G \to S$ (for a known group G and a finite set S) satisfying $f(x) = f(y)$ iff x and y are in the same (left) coset of the hidden subgroup $H \leq G$. In this lecture we will use additive notation for the group operation of an abelian group, so we have $f(x) = f(x)$ iff $x - y \in H$. The strategy for the general abelian HSP closely follows the algorithm for the discrete log problem, which solves a particular instance of the HSP in $\mathbb{Z}_N \times \mathbb{Z}_N$.

We begin by creating a uniform superposition over the group,

$$|G\rangle := \frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle. \tag{1}$$

Then we compute the function value in another register, giving

$$\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x, f(x)\rangle. \tag{2}$$

Discarding the second register then gives a uniform superposition over the elements of some randomly chosen coset $x + H := \{x + h \colon h \in H\}$ of H in G,

$$|x + H\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |x + h\rangle. \tag{3}$$

Such a state is commonly called a *coset state*. Equivalently, since the coset is unknown and uniformly random, the state can be described by the density matrix

$$\rho_H := \frac{1}{|G|} \sum_{x \in G} |x + H\rangle\langle x + H|. \tag{4}$$

Next we apply the QFT over G. Then we obtain the state

$$\begin{aligned} |\widehat{x + H}\rangle &:= F_G |x + H\rangle & (5)\\ &= \frac{1}{\sqrt{|H| \cdot |G|}} \sum_{y \in \hat{G}} \sum_{h \in H} \chi_y(x + h)|y\rangle & (6)\\ &= \sqrt{\frac{|H|}{|G|}} \sum_{y \in \hat{G}} \chi_y(x)\chi_y(H)|y\rangle & (7) \end{aligned}$$

where

$$\chi_y(H) := \frac{1}{|H|} \sum_{h \in H} \chi_y(h). \tag{8}$$

Note that applying the QFT was the right thing to do because the state ρ_H is G-invariant. In other words, it commutes with the regular representation of G, the unitary matrices $U(x)$ satisfying $U(x)|y\rangle = |x+y\rangle$ for all $x, y \in G$: we have

$$\begin{aligned} U(x)\rho_H &= \frac{1}{|G|} \sum_{y \in G} |x+y+H\rangle\langle y+H| && (9)\\ &= \frac{1}{|G|} \sum_{z \in G} |z+H\rangle\langle z-x+H| && (10)\\ &= \rho_H U(-x)^\dagger && (11)\\ &= \rho_H U(x). && (12) \end{aligned}$$

It follows that $\hat{\rho}_H := F_G \rho_H F_G^\dagger$ is diagonal (indeed, we verify this explicitly below), so we can measure without losing any information. We will talk about this phenomenon more when we discuss nonabelian Fourier sampling.

Note that χ_y is a character of H if we restrict our attention that that subgroup. If $\chi_y(h) = 1$ for all $h \in H$, then clearly $\chi_y(H) = 1$. On the other hand, if there is any $h \in H$ with $\chi_y(h) \neq 1$ (i.e., if the restriction of χ_y to H is not the trivial character of H), then by the orthogonality of distinct irreducible characters,

$$\frac{1}{|G|} \sum_{x \in G} \chi_y(x) \chi_{y'}(x)^* = \delta_{y,y'} \tag{13}$$

we have $\chi_y(H) = 0$. Thus we have

$$\widehat{|x+H\rangle} = \sqrt{\frac{|H|}{|G|}} \sum_{y\colon \chi_y(H)=1} \chi_y(x)|y\rangle \tag{14}$$

or, equivalently, the mixed quantum state

$$\hat{\rho}_H := \frac{|H|}{|G|} \sum_{y\colon \chi_y(H)=1} |y\rangle\langle y|. \tag{15}$$

Next we measure in the computational basis. Then we obtain some character χ_y that is trivial on the hidden subgroup H. This information narrows down the possible elements of the hidden subgroup: we can restrict our attention to those elements $g \in G$ satisfying $\chi_y(g) = 1$. The set of such elements is called the *kernel* of χ_y,

$$\ker \chi_y := \{g \in G\colon \chi_y(g) = 1\};$$

it is a subgroup of G. Now our strategy is to repeat the entire sampling procedure many times and compute the intersection of the kernels of the resulting characters. After only polynomially many steps, we claim that the resulting subgroup is H with high probability. It clearly cannot be smaller than H (since the kernel of every sampled irrep contains H), so it suffices to show that each sample is likely to reduce the size of H by a substantial fraction until H is reached.

Suppose that at some point in this process, the intersection of the kernels is $K \leq G$ with $K \neq H$. Since K is a subgroup of G with $H < K$, we have $|K| \geq 2|H|$ (by Lagrange's theorem). Because each character χ_y of G satisfying $\chi_y(H)$ has probability $|H|/|G|$ of appearing, the probability that we see some χ_y for which $K \leq \ker \chi_y$ is

$$\frac{|H|}{|G|}|\{y \in \hat{G} \colon K \leq \ker \chi_y\}|. \tag{16}$$

But the number of such ys is precisely $|G|/|K|$, since we know that if the subgroup K were hidden, we would sample such ys uniformly, with probability $|K|/|G|$. Therefore the probability that we see a y for which $K \leq \ker \chi_y$ is precisely $|H|/|K| \leq 1/2$. Now if we observe a y such that $K \not\leq \ker \chi_y$, then $|K \cap \ker \chi_y| \leq |K|/2$; furthermore, this happens with probability at least $1/2$. Thus, if we repeat the process $O(\log |G|)$ times, it is extremely likely that the resulting subgroup is in fact H.

Decomposing abelian groups

To apply the above algorithm, we must understand the structure of the group G; in particular, we must be able to apply the Fourier transform F_G. For some applications, we might not know the structure of G a priori. But if we assume only that we have a unique encoding of each element of G, the ability to perform group operations on these elements, and a generating set for G, then there is an efficient quantum algorithm (due to Mosca) that decomposes the group as

$$G = \langle \gamma_1 \rangle \oplus \langle \gamma_2 \rangle \oplus \cdots \oplus \langle \gamma_t \rangle$$

in terms of generators $\gamma_1, \gamma_2, \ldots, \gamma_t$. Here $\oplus$ denotes an internal direct sum, meaning that the groups $\langle \gamma_i \rangle$ intersect only in the identity element; in other words, we have

$$G \cong \mathbb{Z}_{|\langle \gamma_1 \rangle|} \times \mathbb{Z}_{|\langle \gamma_2 \rangle|} \times \cdots \times \mathbb{Z}_{|\langle \gamma_t \rangle|}.$$

Given such a decomposition, it is straightforward to implement F_G and thereby solve HSPs in G. We might also use this tool to decompose the structure of the hidden subgroup H output by the HSP algorithm, e.g., to compute $|H|$.

First, it is helpful to simplify the problem by reducing to the case of a p-group for some prime p. For each given generator g of G, we compute its order, the smallest non-negative integer r such that $rg = 0$ (where we are using additive notation; in multiplicative notation we would write $g^r = 1$). Recall that there is an efficient quantum algorithm for order finding. Furthermore, there is an efficient quantum algorithm for factoring, so suppose we can write $r = st$ for some relatively prime integers s, t. By Euclid's algorithm, we can find a, b such that $as + bt = 1$, so $asg + btg = g$. Therefore, we can replace the generator g by the two generators sg and tg and still have a generating set. By repeating this procedure, we eventually obtain a generating set in which all the generators have prime power order.

For a given prime p, let G_p be the group generated by all the generators of G whose order is a power of p. Then $G = \bigoplus_p G_p$: every element of G can be written as a sum of elements from the G_ps (since together they include a generating set), and since G_p is a p-group (i.e., the orders of all its elements are powers of p), $G_p \cap G_{p'} = \{0\}$. Thus, it suffices to focus on the generators of G_p and determine the structure of this p-group. So from now on we assume that the order of G is a power of p.

Now, given a generating set $\{g_1, \ldots, g_d\}$ for G, let q (which is some power of p) be the largest order of any of the generators. We consider a hidden subgroup problem in the group $\mathbb{Z}_q^d$ whose

solution allows us to determine the structure of G. Define $f\colon \mathbb{Z}_q^d \to G$ by

$$f(x_1, \ldots, x_d) = x_1 g_1 + \cdots + x_d g_d.$$

Now $f(x_1, \ldots, x_d) = f(y_1, \ldots, y_d)$ if and only if $(x_1 - y_1)g_1 + \cdots + (x_d - y_d)g_d = 0$, i.e., if and only if $f(x - y) = 0$. The elements of G for which f takes the value 0,

$$K := \{x \in \mathbb{Z}_q^d : f(x) = 0\},$$

form a subgroup of G called the *kernel* of f. Using the algorithm for the hidden subgroup problem in $\mathbb{Z}_q^d$, we can find generators for K. Suppose this generating set is $W = \{w_1, \ldots, w_m\}$, where $w_i \in \mathbb{Z}_q^d$.

The function f is clearly a homomorphism from $\mathbb{Z}_q^d$ to G, and it is also surjective (i.e., onto, meaning that the image of f is all of G), which implies that $\mathbb{Z}_q^d/K \cong G$ (this is called the *first isomorphism theorem*). Thus, to determine the structure of G, it suffices to determine the structure of the quotient $\mathbb{Z}_q^d/K$. In particular, if $\mathbb{Z}_q^d/K = \langle u_1 + K\rangle \oplus \cdots \oplus \langle u_t + K\rangle$, then $G = \langle f(u_1)\rangle \oplus \cdots \oplus \langle f(u_t)\rangle$. The final ingredient is a polynomial-time classical algorithm that produces such a direct sum decomposition of a quotient group.

To find such a decomposition, it is helpful to view the problem in terms of linear algebra. With $x \in \mathbb{Z}_q^d$, we have $x + K = K$ (so that $f(x) = 0$, and there is no need to include x as a generator) if and only if $x \in \operatorname{span}_{\mathbb{Z}_q} W$ (recall that W is a generating set for K). We can easily modify this to allow arbitrary integer vectors $x \in \mathbb{Z}^d$: then $x+K = K$ if and only if $x \in \operatorname{span}_{\mathbb{Z}}(W \cup \{qe_1, \ldots, qe_d\})$, where e_i is the ith standard basis vector. In other words, as x varies over the integer span of the vectors $w_1, \ldots, w_m, qe_1, \ldots, qe_d$, we obtain redundant vectors.

Now we use a tool from integer linear algebra called the *Smith normal form*. A square integer matrix is called *unimodular* if it has determinant ± 1. Given an integer matrix M, its Smith normal form is a decomposition $M = UDV^{-1}$, where $D = \operatorname{diag}(1, \ldots, 1, d_1, \ldots, d_t, 0, \ldots 0)$ is an integer diagonal matrix with its positive diagonal entries satisfying $d_1 \mid d_2 \mid \ldots \mid d_t$. The Smith normal form can be computed classically in polynomial time.

In the present context, let M be the matrix with columns $w_1, \ldots, w_m, qe_1, \ldots, qe_d$. Let $M = UDV^{-1}$ be its Smith normal form, and let $u_1, \ldots, u_t$ be the columns of U corresponding to diagonal entries of D that are not 0 or 1 (i.e., if the ith diagonal entry of D is not 0 or 1, the ith column of U is included). We claim that $\mathbb{Z}_q^d/K = \langle u_1 + K\rangle \oplus \cdots \oplus \langle u_t + K\rangle$.

Since U is nonsingular, it is clear that we still have a generating set if we take all the columns of U. We're claiming that the columns corresponding to 0 or 1 diagonal entries of D are redundant. Let u be the jth column of U; we know that $u + K = K$ (i.e., u is redundant) if $u \in \operatorname{span}_{\mathbb{Z}} \operatorname{cols}(M)$ (where $\operatorname{cols}(M)$ denotes the set of columns of M). Since V is unimodular, $\operatorname{span}_{\mathbb{Z}} \operatorname{cols}(M) = \operatorname{span}_{\mathbb{Z}} \operatorname{cols}(MV)$. So $u + K = K$ if $u \in \operatorname{span}_{\mathbb{Z}} \operatorname{cols}(MV)$, i.e., if $e_j \in \operatorname{span}_{\mathbb{Z}} \operatorname{cols}(U^{-1}MV) = \operatorname{span}_{\mathbb{Z}} \operatorname{cols}(D)$. If the jth diagonal entry of D is 0 or 1, then clearly this is true, so $u + K = K$. This shows that the cosets $u_1 + K, \ldots, u_t + K$ alone indeed generate $\mathbb{Z}_q^d/K$.

It remains to show that they generate $\mathbb{Z}_q^d/K$ as a direct sum. The above argument shows that $d_i u_i + K = K$, and this is not true for any smaller value than d_i, so the order of $u_i + K$ is d_i. Now suppose $\sum_i x_i u_i + K = K$. Then $\sum_i x_i u_i \in \operatorname{span}_{\mathbb{Z}} \operatorname{cols}(M) = \operatorname{span}_{\mathbb{Z}} \operatorname{cols}(MV)$, or in other words, $x \in \operatorname{span}_{\mathbb{Z}} \operatorname{cols}(U^{-1}MV) = \operatorname{span}_{\mathbb{Z}} \operatorname{cols}(D)$. But this implies that x_i is an integer multiple of d_i, which shows that $\langle u_1 + K\rangle \oplus \cdots \oplus \langle u_t + K\rangle$ is indeed a direct sum decomposition.