Université de Bordeaux
Master Mathématiques et Applications
Année 2017-2018

Algorithmique Arithmétique

16 décembre 2017

Documents allowed
The exercises are independent

Part 1 : Quantum computing

In this part, we will consider the following *search problem* : given a boolean function $\mathcal{A} : \{0,1\}^n \to \{0,1\}$, how many calls to $\mathcal{A}$ do we need to find $y \in \{0,1\}^n$ such that $\mathcal{A}(y) = 1$ (or to decide that there is none ?). It is clear that in classical computing we cannot do better in the worst case that calling $\mathcal{A}$ a number of times $O(2^n)$. In the quantum setting, we will see that there is a quantum algorithm that solves this problem using $O(2^{n/2})$ calls to the quantum version of $\mathcal{A}$.

We start to gather a few standard geometric properties of unitary reflections. We take the following notations : for $N \geq 1$, the Hilbert space $\mathbb{C}^N$ is endowed with the hermitian product $\langle u|v\rangle = \sum_{j=1}^{N} \overline{u_j} v_j$, and we set $\|u\| = \sqrt{\langle u|u\rangle}$. To $u \in \mathbb{C}^N$ such that $\|u\| = 1$, we associate the reflection $\rho_u : \mathbb{C}^N \to \mathbb{C}^N$ defined by $\rho_u(x) = x - 2\langle u|x\rangle\, u$.

1. Show that $\rho_u(u) = -u$, that $\rho_u(x) = x$ if $x \in (\mathbb{C}u)^\perp$, and that $\rho_u^2 = \mathrm{Id}$.

2. Show that $\rho_u \in U(\mathbb{C}^N)$.

3. Show that, if $W \in U(\mathbb{C}^n)$, $W\rho_u W^{-1} = \rho_{W(u)}$.

4. Let $u, v \in \mathbb{C}^N$ such that $\langle u|v\rangle = \cos\theta$ for some angle $\theta \in (0,\pi)$. Let $P = \mathbb{C}u \oplus \mathbb{C}v$. Show that $R := \rho_v \circ \rho_u$ is on P the rotation of angle 2θ and is on $P^\perp$ the identity *(you can compute the matrix of R in the orthonormal basis $\{e_1, e_2\}$ of P such that $e_1 = u$ and $v = (\cos\theta)e_1 + (sin\theta)e_2$ and/or you can draw a convincing picture).*

Now we go back to the search problem and assume that the classical oracle $\mathcal{A}$ is turned to a quantum oracle U. With the notations of the lectures : $\mathcal{B} = \mathbb{C}\,|0\rangle \oplus \mathbb{C}\,|1\rangle$, $N = 2^n$, and $\{|x\rangle\,,\ x \in \{0,1\}^n\}$ denotes the computational basis of $\mathcal{B}^{\otimes n}$, U is defined by

$$U\,|x\rangle = \begin{cases} |x\rangle \ \text{ if } \mathcal{A}(x) = 0 \\ -\,|x\rangle \ \text{ if } \mathcal{A}(x) = 1 \end{cases}$$

Moreover we will assume for simplicity that there is a unique y_0 such that $\mathcal{A}(y_0) = 1$.

5. Show that U is the reflection of $\mathcal{B}^{\otimes n}$ relative to $|y_0\rangle$
6. Let $|\varphi\rangle := \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} |x\rangle$ and let V be the reflection relative to $|\varphi\rangle$. Let $R := -VU$. Show that R is a rotation in the plane $P = \mathbb{C}\,|\varphi\rangle \oplus \mathbb{C}\,|y_0\rangle$ of angle $\alpha \approx \frac{2}{\sqrt{N}}$.
7. Show that, if $s = \lfloor \frac{\pi\sqrt{N}}{4} \rfloor$, measuring $|\psi\rangle := (VU)^s |\varphi\rangle$ in the computational basis will output y_0 with probability tending to 1 when n tends to ∞.
8. Show that V can be decomposed into a polynomial number of elementary gates *(for this you can express V in terms of the reflection relative to $|0^n\rangle$)*.
9. Conclude with a description of a quantum algorithm that finds y_0 with high probability using $O(\sqrt{N})$ quantum queries to U and a polynomial number of elementary gates.

Part 2 : Lattices

We take the following notation : for $y_1, \ldots, y_m \in \mathbb{R}^n$, we set

$$L(y_1, \ldots, y_m) := \{\lambda_1 y_1 + \cdots + \lambda_m y_m \mid (\lambda_1, \ldots, \lambda_m) \in \mathbb{Z}^m\}$$

the set of *integer* linear combinations of the vectors $y_1, \ldots, y_m$.

We consider the following problems :

(1) Lattice basis problem

Given $y_1, \ldots, y_m \in \mathbb{Z}^n$, compute a basis $z_1, \ldots, z_k$ of $L(y_1, \ldots, y_m)$ together with a matrix $\Lambda = (\lambda_{i,j}) \in \mathbb{Z}^{m\times k}$ such that, for $1 \le j \le k$, $z_j = \sum_{i=1^m} \lambda_{i,j} y_i$. Note that we do not assume that the vectors y_i are linearly independent, nor that the lattice L is of full rank n.

(2) Lattice membership problem

Given $y_1, \ldots, y_m \in \mathbb{Z}^n$, and $u \in \mathbb{Z}^n$, decide if $u \in L(y_1, \ldots, y_m)$ and, if so, compute $(\lambda_1, \ldots, \lambda_m) \in \mathbb{Z}^m$ such that $u = \lambda_1 y_1 + \cdots + \lambda_m y_m$.

(3) Integer linear system of equations :

Given $A \in \mathbb{Z}^{n\times m}$ and $b \in \mathbb{Z}^n$, decide if there exists $x \in \mathbb{Z}^m$ such that $Ax = b$ and, if so, compute such an x.

(4) Modular system of equations :

Given $A \in \mathbb{Z}^{n\times m}$, $b \in \mathbb{Z}^n$ and $c \in \mathbb{Z}^n$, decide if there exists $x \in \mathbb{Z}^m$ such that $Ax = b \bmod c$ and, if so, compute x. (Here $Ax = b \bmod c$ means : for all $1 \le i \le n$, $(Ax)_i = b_i \bmod c_i$.)

1. Show that Problem (2) reduces to Problem (1).
2. Show that Problem (3) reduces to Problem (2).
3. Show that Problem (4) reduces to Problem (3).

Now we want to address Problem 1. For this we introduce the notion of a matrix $A \in \mathbb{Z}^{m\times n}$ in *Hermite normal form* (HNF). Let k denote the rank of A. For the column of index j, let $r(j)$ denote the first index such that $A_{r(j),j} \neq 0$ (with the convention $r(j) = \infty$ if the column is identically 0^n).

We say that A is in HNF if :

(a) The first k columns are non zero and the remaining ones are equal to zero.

(b) $r(1) < r(2) < \cdots < r(k)$.

(c) $A_{r(j),j} > 0$ for all $1 \leq j \leq k$

(d) $0 \leq A_{r(j),\ell} < A_{r(j),j}$ for all $1 \leq j < \ell \leq k$.

Moreover, we recall that $\mathrm{SL}_m(Z) = \{U \in \mathbb{Z}^{m\times m} \mid \det(U) = \pm 1\}$ is the group of *unimodular matrices*. We will prove :

Theorem : For all $A \in \mathbb{Z}^{n\times m}$, there exists $U \in \mathrm{SL}_m(\mathbb{Z})$ such that $AU = B$ is in HNF. Moreover there is an algorithm to compute U (and B) having polynomial algebraic complexity.

4. Draw a picture of a matrix in HNF form ; give a few examples of matrices in HNF form and of matrices which are not in HNF form.
5. Show that if $y_1, \ldots, y_m$ denote the columns of A, and if $AU = B$ like in the Theorem, the non zero columns of B give a basis of $L(y_1, \ldots, y_m)$.
6. Derive that the Theorem above answers Problem (1).
7. We call *elementary operations* any of the following operations on A :

$$y_i \leftarrow -y_i \qquad y_i \leftrightarrow y_j \qquad y_i \leftarrow y_i + \lambda y_j \ (j \neq i,\ \lambda \in \mathbb{Z})$$

   Show that each of them amounts to multiplying A on the right by a unimodular matrix.
8. Assume that the first row of A is non zero ; using successive Euclidean divisions between the coefficients of the first row of A, show that a succession of elementary operations on A will transform A into a matrix $A' \in \mathbb{Z}^{n\times m}$ with a first row of the form $[A'_{1,1}, 0, \ldots, 0]$, where $A'_{1,1} > 0$.
9. Give an algorithm that transforms A in HNF form through a succession of elementary operations.
10. Execute this algorithm on the following matrix in order to compute its HNF form (the explicit computation of the matrix U is not required) :

$$A = \begin{pmatrix} 2 & 5 & 8 \\ 3 & 6 & 3 \\ 6 & 1 & 1 \\ 2 & 6 & 1 \end{pmatrix}$$

11. Prove the Theorem. What would you suggest to control the *binary* complexity of this algorithm ? (no proof required here).