MASTER 2 INFORMATIQUE FONDAMENTALE

Article Report - Quantum circuits and low-degree polynomials over $\mathbb{F}_2$

Alice Joffard

Lyon, December 5, 2016

Contents

1 Introduction

The article we are going to study here is the June 2016 paper of Ashley Montanaro, *Quantum circuits and low-degree polynomials over* $\mathbb{F}_2$ [4]. The idea of this paper is to associate a unique polynomial over $\mathbb{F}_2$ to any quantum circuit C made of Hadamard, Z, CZ and CCZ gates, and, in particular, to relate somehow the amplitude $\langle 0|C|0\rangle$ to the number of roots of the polynomial.

This association between quantum circuits and polynomials over $\mathbb{F}_2$ has already been explored in several articles. Indeed, in 2008, Dawson et al. [2] explained how to obtain polynomials from a quantum circuit made of Hadamard and Toffoli gates, and then relate the amplitudes of the circuit to the number of roots of the polynomials. Their idea is really similar to the one developed in this article, but the fact that the author chose a different set of gates allows him to make a more obvious correspondence and an easier proof. Then, in 2013, Rudolph [5] used Dawson et al's ideas to associate a graph to any quantum circuit made of Hadamard and Toffoli gates, and express the amplitudes of the circuit in terms of the permanent of the graph, which is a polynomial over $\mathbb{F}_2$. However, again, the correspondence used by the author in this paper is more direct and easier to understand.

In his paper, Montanaro starts by showing how we can construct the polynomial from the circuit, and then proves the result linking the amplitude to the roots of the polynomial. I chose to focus mainly on those two parts, as it is the key idea of the article. Then, the author makes several observations about this correspondence, that I chose to talk about, as they are quite simple and help us to understand better the correspondence. Then, he uses his result to give a proof of the already known #P-hardness of computing the number of roots of a degree-3 $\mathbb{F}_2$ polynomial [3]. I chose to develop this proof as an application, but the author actually uses it to say that his result won't allow us to compute exact circuit amplitudes more efficiently. He then shows that we can compute it approximately with some probability in polynomial time, but compares this computation with classical computation, and shows that the quantum computation is rarely significantly more efficient. Finally, the author shows how his main result can be used to simulate quantum circuits. I decided not to talk about those previous results as they are very specific and tedious.

2 Correspondence between quantum circuits and polynomials over $\mathbb{F}_2$

To make the correspondence, the author starts from a quantum circuit C, acting on l qubits, whose gates are picked in the following list :

- Hadamard, acting on one qubit and corresponding to the matrix

$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix}$$

- Z acting on one qubit and corresponding to the matrix

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- Controlled-Z, acting on two qubits and corresponding to the matrix

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

  Note that the choice of the target qubit among the two qubits doesn't change the corresponding matrix, so that we won't precise the target in the future.

- Controlled-Controlled-Z, acting on three qubits and corresponding to the matrix

$$CCZ = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

Again, the choice of the target qubit among the three qubits doesn't change the corresponding matrix and we won't precise the target in the future.

At this point, the author does not state that this set of gate is universal for quantum computation, but I think it is important to notice that any quantum circuit can be approximately written with those. Indeed, we already know that the set of gates {Hadamard, Toffoli} is universal for quantum computation [1]. But, the Toffoli gate corresponds to a CCZ conjugated by H on the target qubit. Therefore, the set of gates {Hadamard, CCZ} is also universal, so is the chosen set of gates {Hadamard, Z, CZ, CCZ}.

We can now create the polynomial from the circuit. First, we rewrite the circuit C so that on each of the l qubit, the first and last gate is a Hadamard, and call C' the circuit without those gates, as shown in Figure 1.

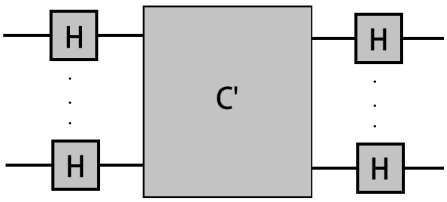

Figure 1: The circuit C and its internal circuit C'.

Note that we can always do that : Since $H.H = I_2$, all we have to do is add two Hadamard gates on the beginning of every channel that doesn't start with H and on the end of every channel that doesn't end with H, one will be the wanted external H, the other will be a part of C'.

Then, divide each channel of C' into portions that are either between two consecutive Hadamards or at the left or right of every Hadamard, and affect a new variable to each of those portions. Now, to each gate Z, CZ or CCZ, affect a term, being the product of all the variables corresponding to the portions of qubits on which the gate acts. Then, to each gate H, affect a term, being the product of its input and output's portion variables. Now, sum all the terms. We finally obtain a polynomial $f_C : \{0,1\}^n \to \{0,1\}$, where $n = h + l$, h being the number of Hadamard gates in C'. An example of a circuit C, its associated circuit C' and the computation of its corresponding polynomial is given in Figure 2.

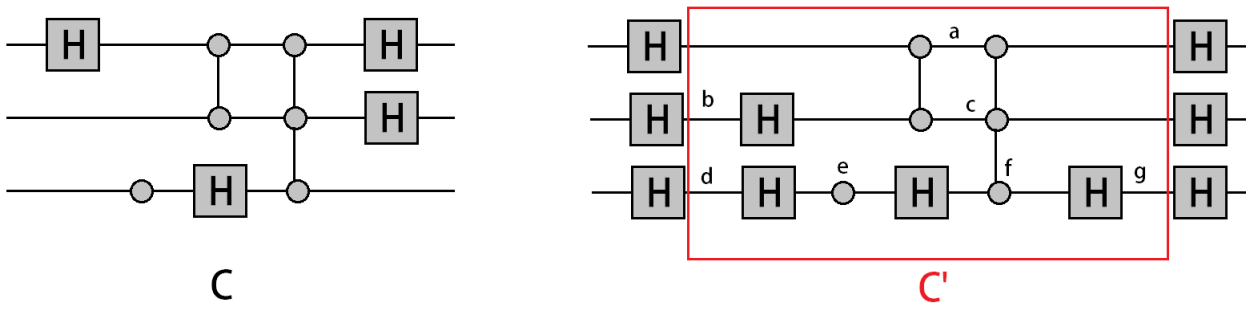

Figure 2: Example of a circuit C, its associated circuit C', and the computation of its corresponding polynomial $f_C = ac + acf + bc + de + e + ef + fg$. The terms correspond to the gates from the first channel to the third, from left to right. Note that we don't need to precise the control and target qubit for the CZ and CCZ gates, as the resulting polynomial would be the same in any case.

Now that we know how to associate a polynomial over $\mathbb{F}_2$ to the quantum circuit, we can already make several observations.

Observation 1. First, we can notice that if there is exactly one polynomial associated to a given circuit, the opposite is not true : A given polynomial can correspond to different circuits. Indeed, we can easily replace a Hadamard by a CZ gate and obtain the same polynomial.

Observation 2. For every degree-3 polynomial $f : \{0,1\}^n \to \{0,1\}$ with no constant term, there exists a circuit C on n qubits such that $f = f_C$. Indeed, we can always take the circuit with no internal Hadamard, that has therefore one variable per qubit, and associates Z gates to degree-one terms, CZ gates to degree-two gates and CCZ to degree-three gates. Note that as we are in $\mathbb{F}_2$, the degree-two and degree-three terms necessarily involve different variables.

Observation 3. There exists a degree-3 polynomial f : $f : \{0,1\}^n \to \{0,1\}$ such that every circuit corresponding to f requires n qubits. Indeed, the polynomial $\Sigma_{i=1}^{n} x_i$, for example, requires exactly n qubits.

These observations motivate us to introduce the quantum circuit width $w(f)$ of a degree-3 polynomial f over $\mathbb{F}_2$, defined as the minimal number of qubits required for any quantum circuit associated to f.

3 Interpretation of the amplitude $\langle 0|C|0\rangle$

We can establish the main proposition of the article, relating $\langle 0|C|0\rangle$, that is the abbreviation for $\langle 0|^{\otimes l} C |0\rangle^{\otimes l}$, that is the amplitude of the output $|0\rangle^{\otimes l}$ when we set the input of C to $|0\rangle^{\otimes l}$, to the

gap of the polynomial, that is the difference between its number of zeroes and its number of ones.

Proposition 1. *Let C be a quantum circuit consisting of Hadamards, Z, CZ and CCZ gates, starting and ending with a column of Hadamard gates, and containing h internal Hadamard gates. Then,* $\langle 0|C|0\rangle = \frac{gap(f_C)}{2^{\frac{h}{2}+l}}$.

Proof. We start the proof by rewriting C' without any internal Hadamard gate. For that, for every internal Hadamard gate of C', we add an ancilla qubit initialized on $|0\rangle$ and replace the Hadamard by the circuit shown on Figure 3.

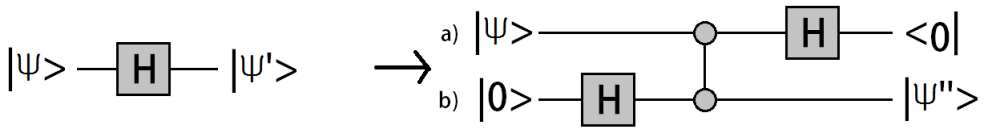

Figure 3: The circuit by which we replace every Hadamard gate of C'.

This modification does not influence the corresponding polynomial, as the new Hadamard gates are external. However, let us see how it influences the value of our amplitude $\langle 0|C|0\rangle$. The author gives the result directly, but I prefer to explicit the calculation behind the result to understand it better. We assume $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

We have

$$|\Psi'\rangle = \alpha|+\rangle + \beta|-\rangle = \frac{1}{\sqrt{2}}((\alpha+\beta)|0\rangle + (\alpha-\beta)|1\rangle)$$

On the other hand, when applying the Hadamard gate to b), we get $|+\rangle$.

The state on the two qubits is therefore

$$\frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle) \otimes (|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}(\alpha|00\rangle + \alpha|01\rangle + \beta|10\rangle + \beta|11\rangle)$$

.

Applying the Controlled-Z gate then gives the state

$$\frac{1}{\sqrt{2}}(\alpha|00\rangle + \alpha|01\rangle + \beta|10\rangle - \beta|11\rangle) = \frac{1}{\sqrt{2}}(\alpha|0\rangle \otimes (|0\rangle + |1\rangle) + \beta|1\rangle \otimes (|0\rangle - |1\rangle))$$

Now, by applying the Hadamard gate to a), we get the total state

$$\frac{1}{\sqrt{2}}(\alpha|+\rangle\otimes(|0\rangle+|1\rangle)+\beta|-\rangle\otimes(|0\rangle-|1\rangle))$$

Or

$$\frac{1}{\sqrt{2}}.\frac{1}{\sqrt{2}}.((\alpha+\beta)|00\rangle+(\alpha-\beta)|01\rangle+(\alpha-\beta)|10\rangle+(\alpha+\beta)|11\rangle)$$

Therefore, by forcing a) to be on the state $|0\rangle$, we obtain on b) the state

$$|\Psi''\rangle=\frac{1}{\sqrt{2}}.\frac{1}{\sqrt{2}}((\alpha+\beta)|0\rangle+(\alpha-\beta)|1\rangle)=\frac{1}{\sqrt{2}}|\Psi'\rangle$$

By repeating this operation on every h Hadamard gate of C', we will then obtain a circuit D on $l+h$ qubits, with no internal Hadamard, and such that $\langle 0|D|0\rangle=\frac{1}{\sqrt{2}^h}\langle 0|C|0\rangle$.

We can now focus on the circuit D. The internal circuit D' contains no Hadamard, only Z, CZ and CCZ gates. In this configuration, we only have one portion per qubit, so one variable per qubit. If Z_i acts on the i_{th} qubit, CZ_{ij} on the i_{th} and j_{th}, and CCZ_{ijk} on the i_{th}, j_{th} and k_{th}, we have, $\forall x\in\{0,1\}^{l+h}$, $\langle x|Z_i|x\rangle=(-1)^{x_i}$, $\langle x|CZ_{ij}|x\rangle=(-1)^{x_ix_j}$, and $\langle x|CCZ_{ijk}|x\rangle=(-1)^{x_ix_jx_k}$. Since all those gates are diagonals, we can obtain $\langle x|D'|x\rangle$ by multiplying $\langle x|G|x\rangle$ for all gates G of D', and each $\langle x|G|x\rangle$ correspond to -1 to the power of the term of the polynomial associated to G, so that $\langle x|D'|x\rangle=(-1)^{f_c(x)}$. In particular, if we take $|x\rangle=H^{\otimes(l+h)}|0\rangle$, we obtain $\langle 0|D|0\rangle=\langle 0|H^{\otimes(l+h)}D'H^{\otimes(l+h)}|0\rangle=\frac{1}{2^{l+h}}\Sigma_{y\in\{0,1\}^{l+h}}(-1)^{f_c(y)}=\frac{gap(f_c)}{2^{l+h}}$.

Therefore, we finally obtain the result we wanted to prove

$$\langle 0|C|0\rangle=\frac{\sqrt{2}^h gap(f_C)}{2^{l+h}}=\frac{gap(f_C)}{2^{\frac{h}{2}+l}}\qquad\square$$

From this proposition, we can already deduce a simple observation :

Observation 4. For C a quantum circuit on l qubits and $f_C:\{0,1\}^n\to\{0,1\}$ its corresponding polynomial, we have $|gap(f_C)|\leq 2^{\frac{h}{2}+l}$. Indeed, this comes from the fact that, as $\langle 0|C|0\rangle$ is an amplitude, $|\langle 0|C|0\rangle|\leq 1$.

4 Application : Complexity of gap computation

We now have a formula that links the amplitude $\langle 0|C|0\rangle$ of the quantum circuit C to the gap of its corresponding polynomial over $\mathbb{F}_2$. The author then uses this result to give a new proof of the following result :

Proposition 2. *It is #P-hard to compute gap(f) for any degree-3 polynomial f.*

Proof. We start by proving that computing $\langle 0|C''|0\rangle$ for a circuit C'' that only contains Hadamard, Toffoli and X gates is #P-hard. Indeed, we know that the set of gates {Toffoli, X} is universal for classical circuits, so that for any $g : \{0,1\}^n \to \{0,1\}$ computed by a classical circuit C with $poly(n)$ gates, there exists a quantum circuit C' with $poly(n)$ X and Toffoli gates, that sends $|x\rangle_I |y\rangle_O |0\rangle_A^{\otimes a}$ to $|x\rangle_I |g(x)\oplus y\rangle_O |0\rangle_A^{\otimes a}$ where I corresponds to the n input qubits, O to the output qubit and A to the ancillas. From this circuit C', we design a second quantum circuit C'' like presented on Figure 4.

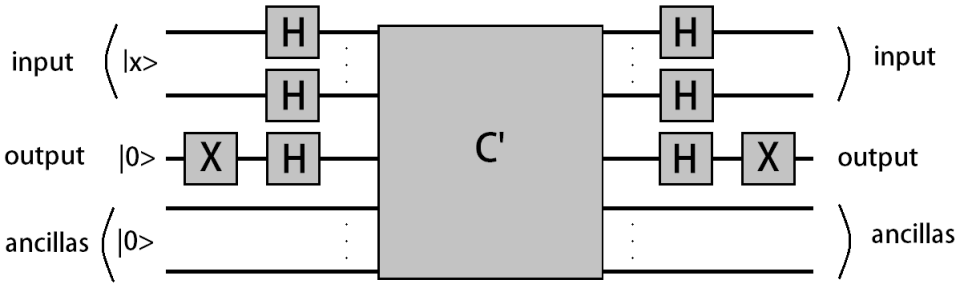

Figure 4: The quantum circuit C'' made from C'.

We want to calculate $\langle 0|C''|0\rangle$. When putting $|0\rangle^{\otimes n}$ as an input, before the C' circuit, without taking into account the ancillas, we get the state :

$$|\Psi\rangle = |+\rangle^{\otimes n} |-\rangle = \frac{1}{\sqrt{2}^n} (\Sigma_{k\in\{0,1\}^n} |k\rangle) \otimes \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

Then, by applying the C' circuit, we get :

$$|\Psi'\rangle = \frac{1}{\sqrt{2}^n} (\Sigma_{k\in\{0,1\}^n} |k\rangle) \otimes \frac{(|g(k)\rangle - |g(k)\oplus 1\rangle)}{\sqrt{2}}$$

If $g(k) = 0$, we get $\frac{(|g(k)\rangle - |g(k)\oplus 1\rangle)}{\sqrt{2}} = \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$, and if $g(k) = 1$, we get $\frac{(|g(k)\rangle - |g(k)\oplus 1\rangle)}{\sqrt{2}} = \frac{(|1\rangle - |0\rangle)}{\sqrt{2}}$.

Therefore, in any case, $\frac{(|g(k)\rangle - |g(k)\oplus 1\rangle)}{\sqrt{2}} = (-1)^{g(k)}|-\rangle$, and we get the state

$$|\Psi'\rangle = \frac{1}{\sqrt{2^n}}\Sigma_{k\in\{0,1\}^n}(-1)^{g(k)}|k\rangle_I \otimes |-\rangle_O$$

By applying again the Hadamard and the X gate to the output qubit, we go back to the state $|0\rangle$. Now, to obtain $\langle 0|C''|0\rangle$, all we have to do is multiplying $\langle 0|^{\otimes n}.H^{\otimes n} = \langle +|^{\otimes n}$ to the state on the input qubit $\frac{1}{\sqrt{2^n}}\Sigma_{k\in\{0,1\}^n}(-1)^{g(k)}|k\rangle_I$. This finally gives

$$\langle 0|C''|0\rangle = \frac{1}{2^n}\Sigma_{k\in\{0,1\}^n}(-1)^{g(k)} = \frac{gap(g)}{2^n}.$$

Thus, calculating the number of solutions of $g = 1$, g being computed by a classical circuit, reduces to calculating $\langle 0|C''|0\rangle$, that is therefore by definition #P-hard.

Now, C'' was made of Hadamard, Toffoli and X gates. But, each of those gates can be written with Hadamard, Z, CZ and CCZ gates. Indeed, we have $X = HZH$, and Toffoli is therefore a Controlled-Controlled-HZH, that is CCZ conjugated by H on the target qubit. Thus, calculating $\langle 0|C''|0\rangle$ for a quantum circuit C'' with Hadamard, Toffoli and X gates reduces to calculating $\langle 0|C|0\rangle$ for a quantum circuit C with Hadamard, Z, CZ and CCZ gates, that is therefore #P-hard.

But, according to Proposition 1., computing $\langle 0|C|0\rangle$ reduces to computing the gap of its corresponding polynomial. Therefore, we get the expected result, computing $gap(f)$ is #P-hard.□

5 Discussion

Even if the idea developed in this paper is not entirely new, the fact that the author chose a new set of gates allows him to be very clear. Indeed, the correspondence between the quantum circuit and its polynomial is particularly easy to understand compared to the correspondence used in the previous articles [2,5]. That being said, the chosen set of gates seems a bit odd, first because it's not often seen in the literature, and also because it is redundant, as the set {Hadamard,CCZ} is already universal without having to add Z and CZ. Indeed, both the gates Z and CZ can be obtained with a CCZ just by taking ancillas qubits in the state $|1\rangle$ as control bits. In terms of the corresponding polynomial, it simply means that instead of the second degree and first degree terms created by respectively CZ and Z gates, we would obtain third degree terms with two or one constant variable

equal to 1, which is of course equivalent. The only difference by using this approach is that the chosen set of gates would be more standard, but the correspondence would also be less easy to understand. The author clearly chose the clarity over the commonness of the gates set, he actually does not talk about its universality and does not even discuss this choice.

In the correspondence made by the author, we have that to any quantum circuit corresponds a unique polynomial over $\mathbb{F}_2$, but not the other way around. Indeed, several different circuits can correspond to the same polynomial. However, it could be interesting to associate a unique circuit to any polynomial, to eventually be able to investigate the properties of the polynomials thanks to the properties of the circuits, like we do in the application on section 4. The author introduced the notion of width, that can already be used to narrow the number of possible circuits for a given polynomial, but it still doesn't construct a unique circuit for a polynomial. For example, the two circuits in Figure 5 are different, but have the same polynomial their number of qubits is the width of the polynomial.

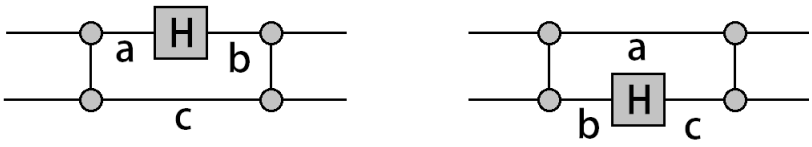

Figure 5: Two circuits that have the same associated polynomial $f_C = ab + bc + ac$ and its width as number of qubits

To make the circuit associated to a polynomial unique, we could define an order on the gates, for example we could obligate the Hadamard gates to be on the highest possible qubit possible. The set of rules we would use would be arbitrary but would allow us to define a bijection between the circuits and the polynomials that could be useful in the future applications.

In the continuity of this paper, another idea would be to use this link between quantum circuits and polynomials as an application for specific classes of circuits. For example, we know how to compute the gap of a degree-2 polynomial in polytime, that makes the computation of the amplitude of a circuit whose gates are in the set {Hadamard, Z, CZ} also in polytime. Other features of other particular circuits may be easier to see in terms of the associated polynomial.

6 References

1. Aharonov, D. (2003). A simple proof that Toffoli and Hadamard are quantum universal. arXiv preprint quant-ph/0301040.

2. Dawson, C. M., Haselgrove, H. L., Hines, A. P., Mortimer, D., Nielsen, M. A., Osborne, T. J. (2004). Quantum computing and polynomial equations over the finite field $\mathbb{Z}_2$. arXiv preprint quant-ph/0408129.

3. Ehrenfeucht, A., Karpinski, M. (1990). The computational complexity of (xor, and)-counting problems. International Computer Science Inst..

4. Montanaro, A. (2016). Quantum circuits and low-degree polynomials over $\mathbb{F}_2$. arXiv preprint arXiv:1607.08473.

5. Rudolph, T. (2009). Simple encoding of a quantum circuit amplitude as a matrix permanent. Physical Review A, 80(5), 054302.