Electronic Colloquium on Computational Complexity, Report No. 59 (2008)

On the Computation of Boolean Functions by Quantum Branching Programs via Fingerprinting

Farid Ablayev Alexander Vasiliev

May 20, 2008

Abstract

We develop quantum fingerprinting technique for constructing quantum branching programs (QBPs), which are considered as circuits with an ability to use classical bits as control variables.

We demonstrate our approach constructing optimal quantum ordered binary decision diagram (QOBDD) for MOD_m and $DMULT_n$ Boolean functions. The construction of our technique also allows to extend the recent result of Ambainis and Nahimovs it is based on. In addition we show how our technique works for encoding quantum information for the equality problem in the simultaneous message passing model.

1 Introduction

The implementation of a large-scale quantum computing device nowadays poses a great challenge for the engineers. At the moment the most realistic way is to construct a quantum computer of a classical device and a small quantum part. That's why the number of qubits needed for physical implementation of an algorithm is a very important complexity measure. In this paper we present a *circuit viewpoint on Quantum Branching Programs* (QBPs) for which this measure explicitly comes out.

Graph based and algebraic definitions of classical and quantum branching programs were explored in numerous papers [NA00, SA04, AGK01, AGKMP]. We suggest that a QBP can be considered as a circuit aided with an ability to use classical bits as control variables for unitary operations. Thus, it is quite adequate model for describing the aforementioned "classical-quantum" computations.

We develop a *quantum fingerprinting technique* oriented for implementation in the QBP model. In general, fingerprinting means presentation of initial object by a compact fingerprint which allows to organize space-efficient computations and reliably extract the result of computation. It is generally used in randomized and quantum algorithms for testing *identity* of different objects such as binary strings, polynomials, matrices and etc. by simply comparing their fingerprints (see book [MR95] for more information on the subject).

The research [BCWW] of Buhrman, Cleve, Watrous, and De Wolf was the first which explicitly formulated and developed fingerprinting technique for the quantum communication model. From 2001 this paper has initiated a bunch of results for quantum communications. Implicitly, the

ISSN 1433-8092

quantum fingerprinting technique has been also used for quantum finite automata [AF98] (later improved in [AN08]) and quantum branching programs [AGK01, AGKMP].

In this paper we generalize the approach of [AN08] and explicitly define the quantum fingerprinting technique oriented for implementation in quantum devices. Our construction use simple controlled rotations about the $\hat{y}$ axis of the Bloch sphere at each step and can be given an illustrative circuit presentation.

For the quantum read-once branching program (quantum OBDD, QOBDD) we consider the Boolean function $MOD_m(x_1, \ldots, x_n)$ which answers whether the number of ones in it's input is a multiple of m. We present a *fingerprinting algorithm* computing this function with the exponential decrease in the size of it's quantum part (the number of qubits). Using known lower bound [AGK01] for the size of QOBDD we state that our algorithm is asymptotically optimal.

The paper is organized as follows. The next section presents definitions, quantum circuit viewpoint on the quantum branching program model, and known lower bound for quantum OBDDs computing Boolean functions. Section 3 presents our fingerprinting technique in general form together with the needed technical statement. Then we apply our fingerprinting technique for constructing an optimal quantum OBDD for Boolean function MOD_m.

The proven lemma from Section 3 allows us to extend the construction of quantum automata recognizing divisibility (the regular language L_m) from [AN08]. This is mentioned in Section 5.

In the last section we apply the developed approach for solving the equality problem in the *simultaneous message passing* model with no shared keys. Actually it gives essentially the same error rate and message size as in [BCWW].

2 Preliminaries and Definitions

The definition of a *linear branching program* is a generalization of the definition of quantum branching program presented in [AGK01]. Deterministic and quantum oblivious branching programs are particular cases of linear branching programs. Let $\mathbf{V}^d$ be a d-dimensional vector space. We use $|\psi\rangle$ and $\langle\psi|$ to denote column vectors and row vectors respectively from $\mathbf{V}^d$, and $\langle\psi_1 \mid \psi_2\rangle$ denotes the inner product. We write ψ when it is not important whether it is in column or row form.

Definition 1 (Linear branching program)**.** *A Linear Branching Program P of width d and length l (a $(d, l) - LBP$) over $\mathbf{V}^d$ is defined as*

$$P = \langle T, |\psi_0\rangle, \mathrm{Accept}\rangle$$

where T is a sequence of l instructions: $T_j = \left(x_{i_j}, U_j(0), U_j(1)\right)$ determined by x_{i_j} tested on the step j where $U_j(0)$ and $U_j(1)$ are $d \times d$ matrices.

Vectors $|\psi\rangle \in \mathbf{V}^d$ are called states (state vectors) of P, $|\psi_0\rangle \in \mathbf{V}^d$ is the initial state of P, and Accept $\subseteq \{1, \ldots, d\}$ *is the accepting set.*

We define a computation of P on an input $\sigma = (\sigma_1, \ldots, \sigma_n) \in \{0,1\}^n$ as follows:

1. *A computation of P starts from the initial state $|\psi_0\rangle$;*
2. *The j'th instruction of P queries a variable x_{i_j}, and applies the transition matrix $U_j = U_j(\sigma_{i_j})$ to the current state $|\psi\rangle$ to obtain the state $|\psi'\rangle = U_j(x_{i_j})\,|\psi\rangle$;*
3. *The final state is*

$$|\psi(\sigma)\rangle = \left(\prod_{j=l}^{1} U_j(\sigma_{i_j})\right)|\psi_0\rangle \quad .$$

The usual complexity measures for $(d, l) - LBP$ are its width d, length l, and size $d \cdot l$.

Deterministic branching programs. A *deterministic* branching program is a linear branching program over a vector space $\mathbb{R}^d$. A state $|\psi\rangle$ of such a program is a Boolean vector with exactly one 1. The matrices U_j correspond to permutations of order d, and so have exactly one 1 in each column. For branching programs over groups this is true for the rows as well; in which case, the U_j are permutation matrices.

Quantum branching programs. We define a *quantum* branching program as a linear branching program over a Hilbert space $\mathcal{H}^d$. The $|\psi\rangle$ for such a program are complex state vectors with $\| |\psi\rangle \|_2 = 1$, and the U_j are complex-valued unitary matrices.

After the l-th (last) step of quantum transformation P measures its configuration $|\psi_\sigma\rangle$ where $|\psi_\sigma\rangle = U_l(\sigma_{i_l})U_{l-1}(\sigma_{i_{l-1}}) \dots U_1(\sigma_{i_1}) |\psi_0\rangle$. Measurement is presented by a diagonal zero-one projection matrix M where $M_{ii} = 1$ if $i \in Accept$ and $M_{ii} = 0$ if $i \notin Accept$. The probability $Pr_{accept}(\sigma)$ of P accepting input σ is defined by

$$Pr_{accept}(\sigma) = ||M |\psi_\sigma\rangle ||^2.$$

A QBP P *computes* f *with one-sided error* if there exists an $\varepsilon > 0$ such that for all $\sigma \in f^{-1}(1)$ the probability of P accepting σ is 1 and for all $\sigma \in f^{-1}(0)$ the probability of P accepting σ is less than $1 - \varepsilon$.

Note that this is a "measure-once" model analogous to the model of quantum finite automata in [MC97], in which the system evolves unitarily except for a single measurement at the end. We could also allow multiple measurements during the computation, by representing the state as a density matrix ρ, and by making the U_j superoperators, but we do not consider this here.

Read-once branching programs.

Definition 2. *We call an* LBP P *an* OBDD *or read-once* LBP *if each variable* $x \in \{x_1, \dots, x_n\}$ *occurs in the sequence* T *of transformations of* P *at most once.*

The "obliviousness" is inherent for an LBP and therefore this definition is consistent with the usual notion of an OBDD. We will use QOBDD for quantum read-once branching programs and OBDD for deterministic ones.

The following general lower bound on the width of QOBDDs is proven in [AGK01].

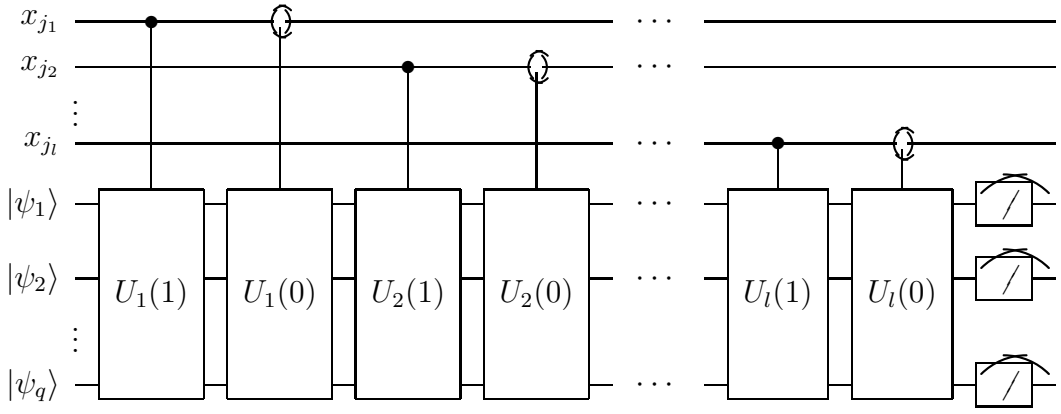
Theorem 1. *Let* $\epsilon \in (0, 1/2)$. *Let* $f(x_1, \dots, x_n)$ *be a Boolean function* $(1/2 + \epsilon)$*-computed (computed with margin* ϵ*) by a quantum read-once branching program* Q. *Then*

$$\text{width}(Q) = \Omega(\log \text{width}(P))$$

where P *is a deterministic OBDD of minimal width computing* $f(x_1, \dots, x_n)$.

Circuit representation. A QBP can be viewed as a quantum circuit aided with an ability to read classical bits as control variables for unitary operations. That is any quantum circuit is a

QBP which does not depend essentially on it's classical inputs.



Here $x_{j_1}, \ldots, x_{j_l}$ is the sequence of (not necessarily distinct) variables denoting classical control bits.

Note that for a QBP in the circuit setting another important complexity measure explicitly comes out – a number of qubits q physically needed to implement a corresponding quantum system with classical control. From definition it follows that $\log d \leq q \leq d/2$. The maximum of $d/2$ is reached when all the qubits do not interfere and thus are isolated quantum systems.

Definition 3. *We call a (d, l)-QBP P a q-qubit QBP if the program P can be implemented as a classically controlled quantum system based on q qubits.*

3 Quantum Fingerprinting

Fingerprinting is the technique that allows to present objects (words over some finite alphabet) by their *fingerprints*, which are significantly smaller than the originals. Moreover, they are intended to reliably extract the important information about the input with one-sided error. The fingerprinting technique of [BCWW] allows to built an optimal Simultaneous Message Passing (SMP) quantum protocol for identification of two binary strings. Here we present the fingerprinting technique adapted for implementation by quantum computational devices. It is based on the recent work of Ambainis and Nahimovs [AN08], thus refining their construction of an optimal quantum finite automaton for a specific regular language L_m. We apply this method for the construction of an optimal QBP for MOD_m Boolean function. We also show that this approach provides analogous to [BCWW] result for the Equality problem in the SMP model.

Our approach has the following properties:

- It is oriented for models with classical control and thus for QBPs.
- Fingerprints are easy to create, we use only controlled rotations about the same axis by the similar angle and Hadamard gates.
- The proven lemma guarantees the existence of a "good" set of parameters which allows to bound the error probability by an $0 < \epsilon < 1$.

Fingerprinting technique For the problem being solved we choose some cardinal m, an error rate $\epsilon > 0$, fix $t = \lceil (2/\epsilon) \ln 2m \rceil$, and construct a mapping $g : \{0,1\}^n \to \mathbb{Z}$. Then for arbitrary binary string $\sigma = \sigma_1 \dots \sigma_n$ we create it's fingerprint $|h_\sigma\rangle$ composing t single qubit fingerprints $|h^i_\sigma\rangle$:

$$\begin{aligned} |h^i_\sigma\rangle &= \cos \tfrac{2\pi k_i g(\sigma)}{m} |0\rangle + \sin \tfrac{2\pi k_i g(\sigma)}{m} |1\rangle \\ |h_\sigma\rangle &= \tfrac{1}{\sqrt{t}} \sum_{i=1}^{t} |i\rangle |h^i_\sigma\rangle \end{aligned}$$

That is, the last qubit is rotated by t different angles about the $\hat{y}$ axis of the Bloch sphere.

The chosen parameters $k_i \in \{1, \dots, m-1\}$ for $i = \overline{1,t}$ are "good" in the following sense.

Definition 4. *A set of parameters $K = \{k_1, \dots, k_t\}$ is called "good" for $g \neq 0 \bmod m$ if*

$$\frac{1}{t^2} \left(\sum_{i=1}^{t} \cos \frac{2\pi k_i g}{m} \right)^2 < \epsilon.$$

Informally, that kind of set guarantees, that the probability of error will be bounded by a constant below 1.

The following lemma proves the existence of a "good" set and follows the proof of the corresponding statement from [AN08].

Lemma 1. *There is a set K with $|K| = t = \lceil (2/\epsilon) \ln 2m \rceil$ which is "good" for all $g \neq 0 \bmod m$.*

Proof. Using Azuma's inequality (see, e.g., [MR95]) we prove that a random choice of the set K is "good" with positive probability .

Let $1 \leq g \leq m-1$ and let K be the set of t parameters selected uniformly at random from $\{0, \dots, m-1\}$.

We define random variables $X_i = \cos \frac{2\pi k_i g}{m}$ and $Y_k = \sum_{i=1}^{k} X_i$. We want to prove that Azuma's inequality is applicable to the sequence $Y_0 = 0$, Y_1, Y_2, Y_3, ..., i.e. it is a martingale with bounded differences. First, we need to prove that $E[Y_k] < \infty$.

From the definition of X_i it follows that

$$E[X_i] = \frac{1}{m} \sum_{j=0}^{m-1} \cos \frac{2\pi j g}{m}$$

Consider the following weighted sum of mth roots of unity

$$\frac{1}{m} \sum_{j=0}^{m-1} \exp\left(\frac{2\pi j g}{m} i \right) = \frac{1}{m} \cdot \frac{\exp(2\pi i g m/m) - 1}{\exp(2\pi i g/m) - 1} = 0,$$

since g is not a multiple of m.

$E[X_i]$ is exactly the real part of the previous sum and thus is equal to 0.

Consequently, $E[Y_k] = \sum_{i=1}^{k} E[X_i] = 0 < \infty$.

Second, we need to show that the conditional expected value of the next observation, given all the past observations, is equal to the last observation.

$$E[Y_{k+1} | Y_1, \dots, Y_k] = \frac{1}{m} \sum_{j=0}^{m-1} \left(Y_k + \cos \frac{2\pi j g}{m} \right) = Y_k + \frac{1}{m} \sum_{j=0}^{m-1} \cos \frac{2\pi j g}{m} = Y_k$$

Since $|Y_{k+1} - Y_k| = |X_{k+1}| \leq 1$ for $k \geq 0$ we apply Azuma's inequality to obtain

$$Pr(|Y_t - Y_0| \geq \lambda) = Pr\left(|\sum_{i=1}^{t} X_i| \geq \lambda\right) \leq 2\exp\left(-\frac{\lambda^2}{2t}\right)$$

Therefore, we induce that the probability of K being not "good" for $1 \leq g \leq m-1$ is at most

$$Pr\left(|\sum_{i=1}^{t} X_i| \geq \sqrt{\epsilon}t\right) \leq 2\exp\left(-\frac{\epsilon t}{2}\right) \leq \frac{1}{m}$$

for $t = \lceil (2/\epsilon)\ln 2m \rceil$.

Hence the probability that constructed set is not "good" for at least one $1 \leq g \leq m-1$ is at most $(m-1)/m < 1$. Therefore, there exists a set which is "good" for all $1 \leq g \leq m-1$. This set will also be "good" for all $g \neq 0 \bmod m$ because $\cos\frac{2\pi k(g+jm)}{m} = \cos\frac{2\pi kg}{m}$. □

We use this result for our fingerprinting technique choosing the set $K = \{k_1, \ldots, k_t\}$ which is "good" for all $g = g(\sigma) \neq 0$. That is, it allows to distinguish those inputs whose image is 0 modulo m from the others.

That hints on how this technique may be applied:

1. We construct $g(x)$, that maps all acceptable inputs to 0 modulo m and others to arbitrary non-zero (modulo m) integers.

2. After the necessary manipulations with the fingerprint the $H^{\otimes \log t}$ operator is applied to the first $\log t$ qubits. This operation "collects" all of the cosine amplitudes at the all-zero state. That is, we obtain the state of type

$$|h'_\sigma\rangle = \frac{1}{t}\sum_{i=1}^{t} \cos\left(\frac{2\pi k_i g(\sigma)}{m}\right)|00\ldots0\rangle\,|0\rangle + \sum_{i=2}^{2t} \alpha_i\,|i\rangle$$

3. Then this state is measured in the standard computational basis and we accept the input if the outcome is the all-zero state. This happens with probability

$$Pr_{accept}(\sigma) = \frac{1}{t^2}\left(\sum_{i=1}^{t} \cos\frac{2\pi k_i g(\sigma)}{m}\right)^2,$$

which is 1 for inputs, whose image is 0 mod m, and is bounded by ϵ for the others.

4 Computation of some Boolean functions in the QOBDD model

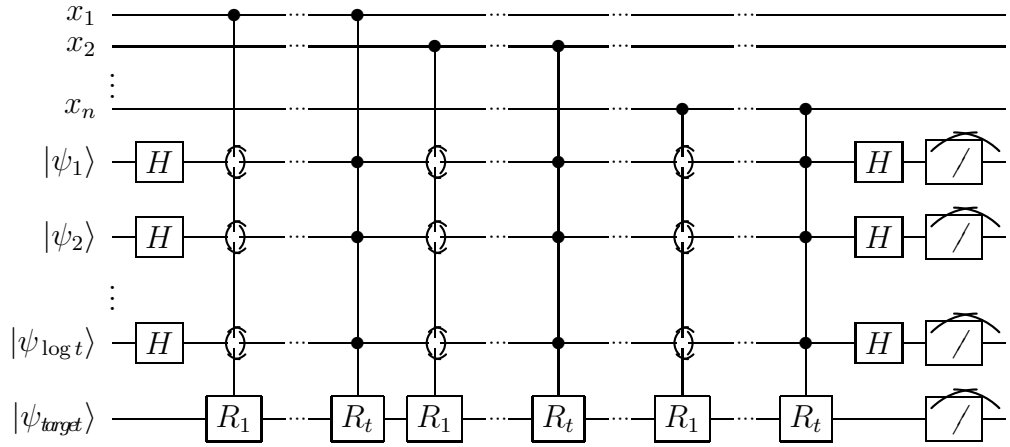
4.1 Computation of the MOD_m function

Consider the following symmetric Boolean function MOD_m: for an input $\sigma = \sigma_1 \ldots \sigma_n \in \{0,1\}^n$ we have $MOD_m(\sigma) = 1$ iff a number of ones in σ is a multiple of m, where $m \geq 2$ is an integer.

Theorem 2. *The function MOD_m can be presented by a $O(\log\log m)$-qubit QOBDD P (read-once $O(\log\log m)$-qubit QBP) with one-sided error $0 < \epsilon < 1$.*

Proof. Let $\epsilon > 0$ and fix $t = \lceil (2/\epsilon) \ln 2m \rceil$.

First we present an $\log 2t$-qubit QOBDD P for MOD_m in a circuit setting and then we prove that it computes MOD_m with one-sided error. Program P is presented by the following quantum circuit:



Initially $|\psi_1\rangle = |\psi_2\rangle = \cdots = |\psi_{\log t}\rangle = |\psi_{target}\rangle = |0\rangle$. Unitary transformations $R_i = R_{\hat{y}}\left(\frac{4\pi k_i}{m}\right)$, $i \in \{1, \ldots, t\}$, are rotations of the "target qubit" by an angle $4\pi k_i/m$ and the set of parameters $K = \{k_1, \ldots, k_t\}$ is "good" according to the Definition 4. For an input $\sigma = \sigma_1 \ldots \sigma_n \in \{0,1\}^n$ treated as unary representation of a number $g(\sigma) = \sum_{i=1}^n \sigma_i$ the program P creates (step by step while reading the input σ) it's fingerprint $|h_\sigma\rangle$ as the composition of t single qubit fingerprints $|h_\sigma^i\rangle$:

$$\begin{aligned} |h_\sigma^i\rangle &= \cos \tfrac{2\pi k_i g(\sigma)}{m} |0\rangle + \sin \tfrac{2\pi k_i g(\sigma)}{m} |1\rangle \\ |h_\sigma\rangle &= \tfrac{1}{\sqrt{t}} \sum_{i=1}^{t} |i\rangle |h_\sigma^i\rangle \end{aligned}$$

Now it's easy to see that we have applied the *Quantum Fingerprinting* technique described in Section 3 with $g(x) = \sum_{i=1}^n x_i$ and parameter m set to the modulo of MOD_m.

Afterwards we apply the $H^{\otimes \log t} \otimes I$ operator which transforms the fingerprint $|h_\sigma\rangle$ into the

$$|h'_\sigma\rangle = \frac{1}{t} \sum_{i=1}^{t} \cos\left(\frac{2\pi k_i g(\sigma)}{m}\right) |00\ldots0\rangle |0\rangle + \sum_{i=2}^{2t} \alpha_i |i\rangle$$

for some amplitudes α_i, which are not important for us.

The final state is measured in the standard computational basis. The input σ is accepted if quantum register is all-zero (i.e. $|h'_\sigma\rangle = |00\ldots0\rangle |0\rangle$), otherwise the input σ is rejected. From the construction of P we have for arbitrary input σ the acceptance probability as follows:

$$Pr_{accept}(\sigma) = \frac{1}{t^2} \left(\sum_{i=1}^{t} \cos \frac{2\pi k_i g(\sigma)}{m} \right)^2$$

Thus if $MOD_m(\sigma) = 1$ that is, $g(\sigma) = 0 \bmod m$ then $Pr_{accept}(\sigma) = 1$. If $MOD_m(\sigma) = 0$ that is, $g(\sigma) \neq 0 \bmod m$ then the probability of obtaining the $|00\ldots0\rangle |0\rangle$ state is less than ϵ because of the "goodness" of the set of parameters $k_1, \ldots, k_t$.

Note that the number of qubits used in this construction is $\log t + 1 = O(\log \log m)$ which is asymptotically optimal due to the result of Theorem 1 and the fact that any deterministic OBDD for MOD_m requires width $\Omega(m)$. □

4.2 Computation of the $DMULT_n$ function

Our technique can be used to compute the decision variant of the multiplication function ($DMULT_n$).

Let $x = (x_0, \ldots, x_{n-1})$, $y = (y_0, \ldots, y_{n-1})$, and $z = (z_0, \ldots, z_{2n-1})$. x, y, and z would also denote the numbers with corresponding binary encodings (e.g., $x = \sum_{i=0}^{n-1} 2^i x_i$).

Definition 5. $DMULT_n(x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1}, z_0, \ldots, z_{2n-1}) = 1$ *iff*

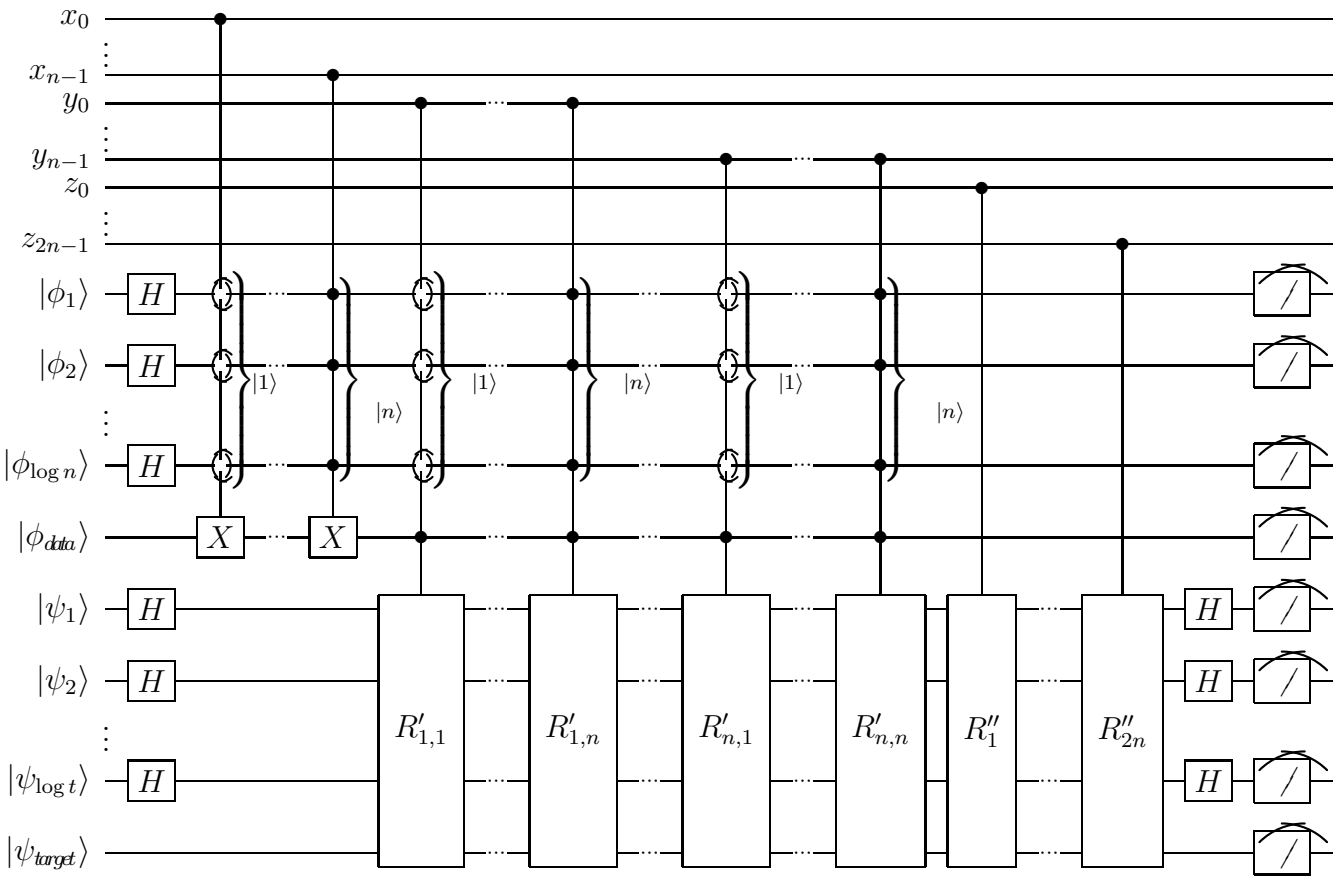
$$\sum_{i,j=0}^{n-1} 2^{i+j} x_i y_j = \sum_{i=0}^{2n-1} 2^i z_i,$$

i.e. when $xy = z$.

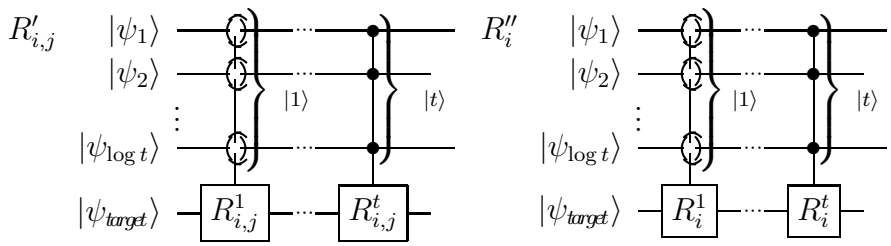
This function can be computed by checking whether $xy - z$ is zero via fingerprinting.

Theorem 3. *For any* $\epsilon \in (0,1)$ *the function* $DMULT_n$ *can be computed with one-sided error* ϵ *by a QOBDD of width* $O(n^2)$.

Proof. Consider the following algorithm



Initially $|\psi\rangle = |\phi_1\rangle \ldots |\phi_{\log n}\rangle\, |\phi_{data}\rangle\, |\psi_1\rangle \ldots |\psi_{\log t}\rangle\, |\psi_{target}\rangle = |00\ldots0\rangle$. The unitary transformations $R'_{i,j}$ for $i,j \in \{1,\ldots,n\}$ and R''_i for $i \in \{1,\ldots,2n\}$ are defined by the following circuits



Here $R^l_{i,j} = R_{\hat{y}}\left(\frac{4\pi k_l 2^{(i-1)+(j-1)}}{2^{2n}}\right)$, $R^l_i = R_{\hat{y}}\left(-\frac{4\pi k_l 2^{i-1}}{2^{2n}}\right)$, and the set of parameters $K = \{k_1, \ldots, k_t\}$ is "good" according to the Definition 4 with $t = \lceil (2/\epsilon) \ln (2 \cdot 2^{2n}) \rceil = O(n)$.

The first layer of H gates creates the following superposition

$$\frac{1}{\sqrt{tn}} \sum_{j=1}^{n} \sum_{l=1}^{t} |j\rangle |0\rangle |l\rangle |0\rangle$$

Then we "remember" all of x_j variables in the first $\log n + 1$ qubits. That is, having read $\sigma_j = 1$ ($j \in \{0, \ldots, n-1\}$) the state $|j+1\rangle |0\rangle$ is transformed into $|j+1\rangle |1\rangle$. When all of the $x_0 = \sigma_0, \ldots, x_{n-1} = \sigma_{n-1}$ are read the system will end up in the state

$$\frac{1}{\sqrt{tn}} \sum_{j=0}^{n-1} \sum_{l=1}^{t} |j+1\rangle |\sigma_j\rangle |l\rangle |0\rangle .$$

At the next phase for each $y_i = 1$ ($i \in \{0, \ldots, n-1\}$) we check for all $j \in \{0, \ldots, n-1\}$ whether $|\phi_1\rangle \ldots |\phi_{\log n}\rangle |\phi_{data}\rangle$ is in the state $|j+1\rangle |1\rangle$ with non-zero amplitude (this happens only if $x_i = 1$) and if so, we rotate the last qubit of the state $|l\rangle |\cdot\rangle$ by an angle $\frac{4\pi k_l 2^{i+j)}}{2^{2n}}$ for each $l \in \{1, \ldots, t\}$. That is, $|\psi_{target}\rangle$ is in some sense rotated by t similar angles around the $\hat{y}$ of the Bloch sphere.

Afterwards, for those of z_i ($i \in \{0, \ldots, 2n-1\}$) whose value is 1 the last qubit of $|l\rangle |\cdot\rangle$ is rotated by an angle $-\frac{4\pi k_l 2^i}{2^{2n}}$ around the $\hat{y}$ of the Bloch sphere for each $l \in \{1, \ldots, t\}$.

Thus, right before the last application of the $H^{\otimes \log t}$ operator our system evolves to the state:

$$|\psi'\rangle = \frac{1}{\sqrt{tn}} \sum_{j=0}^{n-1} \sum_{l=1}^{t} |j+1\rangle |\sigma_j\rangle |l\rangle \left(\cos \frac{2\pi k_l g(\sigma,\gamma,\delta)}{2^{2n}} |0\rangle + \sin \frac{2\pi k_l g(\sigma,\gamma,\delta)}{2^{2n}} |1\rangle\right),$$

where $g(x, y, z) = xy - z$ is exactly what we need to compute.

Thus, applying the Hadamard transform to the qubits $|\psi_1\rangle \ldots |\psi_{\log t}\rangle$ we obtain the state

$$\begin{aligned} |\psi''\rangle &= \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} |j+1\rangle |\sigma_j\rangle \left(\frac{1}{t} \sum_{l=1}^{t} \cos \frac{2\pi k_l g(\sigma,\gamma,\delta)}{2^{2n}} |00\ldots0\rangle |0\rangle\right) + \\ &+ \sum_{i=2}^{2t} \sum_{j=0}^{n-1} \alpha_{i,j} |j+1\rangle |\sigma_j\rangle |i\rangle \end{aligned}$$

The input is accepted if the measurement outcome of $|\psi_1\rangle \ldots |\psi_{\log t}\rangle |\psi_{target}\rangle$ is $|00\ldots0\rangle |0\rangle$. Thus, the accepting probability is

$$Pr_{accept}(\sigma, \gamma, \delta) = \frac{1}{t^2} \left(\sum_{l=1}^{t} \cos \frac{2\pi k_l g(\sigma, \gamma, \delta)}{2^{2n}}\right)^2$$

When $DMULT_n(\sigma, \gamma, \delta) = 1$, $g(\sigma, \gamma, \delta)$ is 0 and we accept with probability 1. Otherwise, $g(\sigma, \gamma, \delta) \neq 0$ and the probability of accepting the input from $DMULT_n^{-1}(0)$ is bounded by ϵ since the set $K = \{k_1, \ldots, k_t\}$ is "good" and

$$Pr_{accept}(\sigma, \gamma, \delta) = \frac{1}{t^2} \left(\sum_{l=1}^{t} \cos \frac{2\pi k_l g(\sigma, \gamma, \delta)}{2^{2n}}\right)^2 < \epsilon$$

The number of qubits q needed for our construction is $q = \log n + \log t + 2 = O(\log n)$ while the width of the program is $2^q = 4nt = O(n^2)$. □

5 Recognizing divisibility in the QFA model

Using the proof from the section 3 we can state that the the result of Ambainis and Nahimovs [AN08] concerning recognition of the language L_m by a 1-way *Quantum Finite Automata* (QFA) can be extended to the case of arbitrary integer $m \geq 2$.

6 Equality problem in the SMP model

As an another application of the described approach consider the equality problem in the *simultaneous message passing* model without shared key (see [BCWW]). In this model Alice and Bob receive their binary strings σ and γ respectively and need to send a message as small as possible to the referee, who makes a test and decides whether $\sigma = \gamma$ or not. We construct a protocol analogous to that of *Buhrman et al* and thus prove the following theorem.

Theorem 4. *There is a quantum protocol that solves the equality problem in the SMP model with one-sided error probability bounded below 1 using $O(\log n)$ qubits of communication.*

Proof. We apply the fingerprinting technique from Section 3 here followed by the "swap-test" from [BCWW]. We set m to the 2^n (where $|\sigma| = |\gamma| = n$), construct $g(x) = \sum_{i=1}^{n} 2^{i-1} x_i$ as a numeric value of the input, fix an $0 < \epsilon < 1$, and choose a "good" set of $t = \lceil (2/\epsilon) \ln 2m \rceil$ parameters $K = \{k_1, \ldots, k_t\}$. Now Alice and Bob create their fingerprints $|h_\sigma\rangle$ and $|h_\gamma\rangle$ as

$$\begin{aligned} |h_\sigma\rangle &= \tfrac{1}{\sqrt{t}} \sum_{i=1}^{t} |i\rangle \left(\cos \tfrac{2\pi k_i g(\sigma)}{m} |0\rangle + \sin \tfrac{2\pi k_i g(\sigma)}{m} |1\rangle \right) \\ |h_\gamma\rangle &= \tfrac{1}{\sqrt{t}} \sum_{i=1}^{t} |i\rangle \left(\cos \tfrac{2\pi k_i g(\gamma)}{m} |0\rangle + \sin \tfrac{2\pi k_i g(\gamma)}{m} |1\rangle \right) \end{aligned}$$

and send them to the referee, who applies the transformation $(H \bigotimes I)$ (controlled-SWAP) $(H \bigotimes I)$ to the state $|0\rangle |h_\sigma\rangle |h_\gamma\rangle$ and measures the first qubit of the resulting state $1/2 |0\rangle (|h_\sigma\rangle |h_\gamma\rangle + |h_\gamma\rangle |h_\sigma\rangle) + 1/2 |1\rangle (|h_\sigma\rangle |h_\gamma\rangle - |h_\gamma\rangle |h_\sigma\rangle)$. The referee outputs "yes" if the state $|0\rangle$ was observed which happens with probability $Pr_{accept}(\sigma, \gamma) = \frac{1}{2}(1 + |\langle h_\sigma \mid h_\gamma \rangle|^2)$, that is

$$\begin{aligned} Pr_{accept}(\sigma, \gamma) &= \tfrac{1}{2} + \tfrac{1}{2t^2} \left| \sum_{i=1}^{t} \cos \tfrac{2\pi k_i g(\sigma)}{m} \cos \tfrac{2\pi k_i g(\gamma)}{m} + \sin \tfrac{2\pi k_i g(\sigma)}{m} \sin \tfrac{2\pi k_i g(\gamma)}{m} \right|^2 \\ &= \tfrac{1}{2} + \tfrac{1}{2t^2} \left| \sum_{i=1}^{t} \cos \tfrac{2\pi k_i (g(\sigma) - g(\gamma))}{m} \right|^2 \end{aligned}$$

When $\sigma = \gamma$ this equals 1 and the probability of obtaining $|0\rangle$ when $\sigma \neq \gamma$ is bounded by

$$Pr_{accept}(\sigma, \gamma) < \frac{1}{2} + \frac{1}{2}\epsilon < 1$$

The number of qubits sent to the referee is $2 \log 2t = O(\log \log m) = O(\log n)$. In [BCWW] it was also shown that $\Omega(\log n)$ qubits are needed to solve the posed equality problem, so our approach is asymptotically optimal like that of [BCWW]. □

Acknowledgements We thank Juhani Karhumaki for invitation to the University of Turku and a number of interesting discussions on the subject of the paper.

Research was supported by the University of Turku and the Russian Fund for Basic Research (under the grant 08-07-00449).

References

[AF98] A. Ambainis and R. Freivalds, *1-way quantum finite automata: strengths, weaknesses and generalization*. Proceeding of the 39th IEEE Conference on Foundation of Computer Science, 1998, See also arXiv:quant-ph/9802062 v3, pp. 332–342.

[AN08] A. Ambainis and N. Nahimovs, *Improved constructions of quantum automata*, arXiv:0805.1686v1, 2008.

[AGK01] F. Ablayev, A. Gainutdinova, and M. Karpinski, *On computational power of quantum branching programs*. Lecture Notes in Computer Science, no. 2138, Springer-Verlag, 2001, See also arXiv:quant-ph/0302022 v1, pp. 59–70.

[AGKMP] F. Ablayev, A. Gainutdinova, M. Karpinski, C. Moore, and C. Pollette, *On the computational power of probabilistic and quantum branching programs of constant width*. Information and Computation (2005).

[BCWW] H. Buhrman, R. Cleve, J. Watrous, R. de Wolf, *Quantum fingerprinting*, Physical Review Letters, 87(16):167902, 2001.

[MC97] C. Moore and J.P. Crutchfield, *Quantum automata and quantum grammars*. Theoretical Computer Science 237: 275–306, 2000.

[MR95] R. Motwani, P. Raghavan, *Randomized Algorithms*. Cambridge University Press, 1995.

[NA00] M. Nakanishi, K. Hamaguchi, and T. Kashiwabara, *Ordered quantum branching programs are more powerful than ordered probabilistic branching programs under a bounded-width restriction*. Proc. 6th Intl. Conf. on Computing and Combinatorics (COCOON), Lecture Notes in Computer Science 1858: 467–476, 2000.

[SA04] M. Sauerhoff and D. Sieling, *Quantum branching programs and space-bounded nonuniform quantum complexity*. ph/0403164, March 2004.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de/