# Speedup of Iterated Quantum Search by Parallel Performance

**Yuri Ozhigov**[*]
*Department of Applied Mathematics,*
*Moscow State University of Technology "Stankin,"*
*Vadkovsky per. 3a, 101472, Moscow, Russia*

Given a sequence $f_1(x_1), f_2(x_1, x_2), \ldots, f_k(x_1, \ldots, x_k)$ of boolean functions, each $f_i$ takes the value 1 at a single point of the form $x_1^0, x_2^0, \ldots, x_i^0$, $i = 1, 2, \ldots, k$. The length of all $x_i^0$ is $n$, $N = 2^n$. It is shown how to find $x_k^0$ $(k \geq 2)$ using $k\pi\sqrt{N}/4\sqrt{2}$ simultaneous evaluations of functions of the form $f_i, f_{i+1}$ with an error probability of order $k/\sqrt{N}$. This is $\sqrt{2}$ times faster than $k$ sequential applications of the Grover algorithm for quantum search. Evolutions of amplitudes in parallel quantum computations are approximated by systems of linear differential equations. Some advantage of simultaneous evaluations of all $f_1, \ldots f_k$ are discussed.

## 1. Introduction

### 1.1 Structure of the work

After giving some background and setting the problem, a short introduction to abstract quantum computations is presented in section 3. In section 4 linear differential equations are applied to a tight analysis of the famous Grover algorithm of the fast quantum search.

Section 5 is the key. Here a parallel quantum algorithm for repeated search is defined and studied by means of differential equations. In section 6 we briefly run through a parallel algorithm for iterated search with simultaneous queries of all oracles.

### 1.2 Background

One of the most promising quantum mechanical applications to algorithm theory is associated with the fundamental algorithm of exhaustive search, or finding a solution of the equation $f(x) = 1$ for a boolean function $f$. In 1996 Lov Grover showed in [23] how a quantum computer can solve this equation for the case of a unique solution in time $O(\sqrt{N})$ where $N$ is the number of all possible values for $x$, whereas every probabilistic classical algorithm requires time $O(N)$. At about the same time

[*] Electronic mail address: y@oz.msk.ru.

it was shown in [7] that there are no substantially faster algorithms for this problem. Later, a tight estimation for the time of Grover's algorithm as $\pi\sqrt{N}/4$ with probability of error about $1/N$ was established in [8]. Further development of the fast quantum search can be found in [4, 12, 18, 20, 25, 27, 28, 40].

Earlier patterns of quantum speedup were constructed by P. Shor in [41]. There the algorithms for finding a factorization of an integer and a discrete logarithm are presented. Algorithms of such a sort are studied in a lot of works (e.g., [16, 24, 29, 42, 43, 44]).

Classical computations admitting quantum speedup are rare exceptions from other classical computations in the following sense. Denote all words of a length $n$ in the alphabet $\{0,1\}$ by $\{0,1\}^n$. We can represent a general form of classical computation as $T$ iterated applications of some oracle $g$: $\{0,1\}^n \to \{0,1\}^n$:

$$x \to g(x) \to g(g(x)) \to \cdots \to g(g(\ldots(g(x)))). \tag{1}$$

In [35] it is shown that if $T = O(N^{1/(7+\epsilon)})$, $\epsilon > 0$ then, for the bulk of all $g$, such a computation has no quantum speedup. Similar results for search problems were obtained in [7, 8, 36, 48]. A lower bound as $O(N)$ was found as the time of quantum computations of functions with functional argument $F : \{f\} \to \{0,1\}$ in [5]. Here $f$ are boolean functions on a domain of cardinality $N$. At the same time using a memory of $O(N)$ qubits it is possible to compute such functions in time $N/2$ [14]. This brings up the question: What general type of classical computations of the form of equation (1) admits a quantum speedup beyond any possible speedup of $g$? As follows from [35], for the bulk of functions $g$ this speedup can result only from parallel applications of $g$.

Regarding other aspects of quantum evolutions see also [26, 34, 38].

## 2. Setting the problem

Consider the following situation. We want to gather a mosaic from scattered stones in a rectangular list with the corresponding picture. Each stone is of a unique form. We can gather this mosaic layer by layer and use a simple search among stones still scattered to fill any layer based on the previous one. Then we in fact fulfill an iterated search classically, because to find the stones for the following layer we must already have the previous layer filled.

We formalize this as a special type of iterated algorithm: an iterated search (IS). Suppose we have a sequence $S_1, S_2, \ldots, S_k$ of similar search problems where $S_i$ is to find a unique solution $x_i^0$ of an equation $f_i(x_i) = 1$ where a boolean function $f_i$ is accessible if and only if we know all $x_j^0$, $j < i$. Let $|x_i| = n$, $N = 2^n$, $k \ll N$, and $|x|$ denotes the length of word $x$. The aim is to obtain $x_k^0$, $k \geq 2$. In view of the results in [8] sequential applications of Grover's search for $x_1^0, x_2^0, \ldots, x_k^0$ give an answer in time $k\pi\sqrt{N}/4$ with error probability about $k/N$. To do this we must have all oracles $f_i$, $i = 1, 2, \ldots, k$, where a dependence $f_i$ of all $x_j$, $j < i$ can be included with $f_i$. So we can assume that $f_i$ has the form $f_i(x_1, x_2, \ldots, x_i)$ and each equality $f_i(x_1, \ldots, x_i) = 1$ has the unique solution $x_1^0, x_2^0, \ldots, x_i^0$, $i = 1, 2, \ldots, k$. Considering all oracles $f_i$ as physical devices which cannot be cloned we assume that they are at our disposal at the same time, so we can apply them simultaneously. Here an advantage is taken of interference between the results of their actions. This results in a speedup of computation compared to the sequential mode. Why does this speedup arise? It arises because of a leak of amplitude at each step of sequential searching. An amplitude of $x_i^0$ in search number $i$ increases step-by-step in the course of Grover's search, after the first few $l$ steps it becomes approximately $(2l + 1)/\sqrt{N}$, when amplitudes of other $x_i \neq x_i^0$ decrease. This prevailing of the amplitude corresponding to $x_i^0$ (a leak of amplitude) can be immediately used for the next $i + 1$ search.

We shall show how this effect can be used to solve the problem of IS in time $O(k\pi\sqrt{N}/4\sqrt{2})$ which is $\sqrt{2}$ times faster than by $k$ sequential applications of Grover's algorithm. Note that this speedup does not require any extra hardware, the effect is reached by simultaneous action of oracles. Thus we shall have a modification of the fast quantum search, the parallel quantum algorithm for iterated search, which is described later. In this paper we mostly consider the particular case $k = 2$ of IS, we call this problem a repeated search (RS).

Compare the parallel algorithm for RS with the algorithm of nested quantum search (NQS) presented in [12]. For the case of unique solutions for each $f_i$, NQS is equivalent to a sequential implementation of simple quantum search. This means that NQS does not use a possible interference between two sequential searches. The main advantage of the parallel algorithm for RS presented here is that it uses this interference between searches for solutions of $f_1(x) = 1$ and $f_2(x, y) = 1$ and thus reaches the $\sqrt{2}$-times speedup.

The RS problem is connected with the known problem of structured search (SS). The problem of SS is to find a unique solution $x_0, y_0$ of $f(x, y) = 1$ provided we have a function $g$ whose support $\{x | g(x) = 1\}$ of cardinality $M$ contains $x_0$. The RS problem is a particular case of SS when $M = 1$. The case $1 \ll M \ll N$ was investigated by Farhi and Gutmann in [20]. They found a quantum algorithm for this case with time complexity $O(\sqrt{MN})$, and also wrote that the best known strategy for the case $M = 1$ is the sequential application of Grover's algorithm. In the present paper it is shown how this evident strategy can be improved by a constant factor $\sqrt{2}$. Note that our approach differs from [20]. Farhi and Gutmann used only algebraic properties of

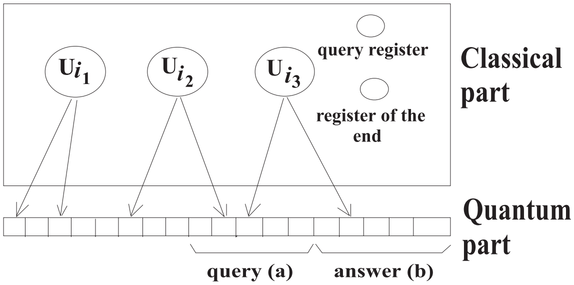

**Figure 1.** A model quantum computer.

Grover's algorithm whereas for the RS problem we need to work with an evolution of amplitudes in a computation.

## 3. Quantum computations and differential equations

After early studies of R. Feynman [22], P. Benioff [6], and D. Deutsch [15] numerous approaches to quantum computations have appeared (e.g., [11, 32, 45, 47]). Leaving aside the problem of decoherence and quantum codes (e.g., [1, 13, 30, 39]) we shall regard ideal computations in closed systems without decoherence. We use the abstract model of a quantum computer independent of the formalism of classical algorithm theory. This model consists of two parts: classical and quantum (see Figure 1).

A state $C$ of the *classical part* consists of the following objects.

1. Registers with labels corresponding to transformations $U_{i_j}$ of a finite set $\{U_i\}$ of elementary unitary transformations with no more than three qubits each. (Strictly speaking transformations on two qubits would suffice: see, [17].) Moreover, as follows from [2, 33] there is a variety of possible choices for the set $\{U_{i_j}\}$.

2. Pointers aimed from these registers to as many qubits from the quantum part as there are arguments of the corresponding unitary transformation. Here each qubit is involved in exactly one transformation.

3. Registers of an end of computation and of a query: $e(C)$ and $\mathrm{qu}(C)$ respectively.

A *quantum part* is a tape partitioned into cells with one qubit each. Every qubit has two basic states $|0\rangle, |1\rangle$, so its quantum state $\lambda|0\rangle + \mu|1\rangle$, $|\lambda|^2 + |\mu|^2 = 1$, belongs to the circle of radius 1 in two-dimensional Hilbert space $\mathrm{C}^2$. If $n$ is a length of tape, all states of the tape belong to the tensor product $\mathcal{H} = \underbrace{\mathrm{C}^2 \otimes \mathrm{C}^2 \otimes \cdots \otimes \mathrm{C}^2}_{n}$ of spaces, corresponding to all qubits, that is, $\mathcal{H} = \mathrm{C}^{2^n}$. Each state of the quantum part is a superposition $\chi = \sum_{i=0}^{N-1} \lambda_i e_i$ of basic states $e_0, \ldots, e_{N-1}$ with complex amplitudes $\lambda_i$ where $\sum_{i=0}^{N-1} |\lambda_i|^2 = 1$ and $N = 2^n$. We can assume that all $e_i \in \{0,1\}^n$.

An *observation* of this state $\chi$ is a random variable which takes each value $e_i$ with the probability $|\lambda_i|^2$.

A *working transformation* of the quantum part corresponding to a fixed state of the classical part has the form $U_{i_1} \otimes U_{i_2} \otimes \cdots \otimes U_{i_k}$ where each $U_{i_j}$ acts on qubits which the corresponding pointer aims to.

Let $f_1, \ldots, f_l$ be functions of the form $\{0,1\}^n \to \{0,1\}^m$ and for each $i = 1, 2, \ldots, l$ there are special places in the quantum tape reserved for an argument $a_i$ of $f_i$ (query) and for a value of $f_i$ (answer). Denote by $b_i$ the initial contents of the answer.

A *query transformation* $\mathrm{Qu}_{\bar{f}}$ is $\mathrm{Qu}_{f_1} \otimes \mathrm{Qu}_{f_2} \otimes \cdots \otimes \mathrm{Qu}_{f_l}$ where for each $i = 1, \ldots, l$

$$\mathrm{Qu}_{f_i} |a_i, b_i\rangle \to |a_i, b_i \oplus f_i(a_i)\rangle,$$

$\oplus$ is the bitwise addition modulo 2. We call these functions $\mathrm{Qu}_{f_i}$ *oracles*.

A *quantum algorithm* is an algorithm that determines evolution of the classical part:

$$C_0 \to C_1 \to \cdots \to C_T \tag{2}$$

(in particular it determines a number $T$). A classical part plays the role of controller for the quantum part and determines its evolution (see Figure 2).

A *quantum computation* consists of two sequences: equation (2) and

$$Q_0 \to Q_1 \to \cdots \to Q_T \tag{3}$$

where for each $i = 0, 1, \ldots, T-1$ $e(C_i) = 0$; $e(C_T) = 1$ and every passage $Q_i \to Q_{i+1}$ is:

- a working transformation, corresponding to $C_i$, if $\mathrm{qu}(C_i) = 0$, $e(C_i) = 0$,
- a query transformation $\mathrm{Qu}_{\bar{f}}$, if $\mathrm{qu}(C_i) = 1$, $e(C_i) = 0$.

A *result* of this quantum computation is the contents of the first $n_0$ qubits of the quantum tape after observation of the final state $Q_T$. An

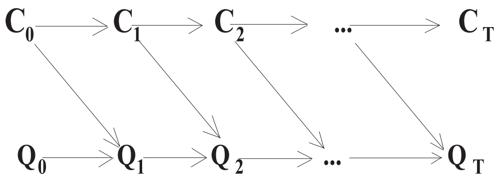

**Figure 2.** A quantum computation.

initial state $(C_0, Q_0)$ of the computer is obtained from an input data $\bar{x}$ by some routine procedure.

A *time* of computation for equations (2) and (3) is the number of query transformations (queries) in it. We see that in this model some oracles may be called simultaneously, which causes interference between results of their actions. We shall prove that such interference can speed up computations in the case of RS.

From a physical standpoint, systems of linear differential equations are a natural tool for the study of quantum computation. The wave function $\psi$, which determines an evolution of a quantum computer, satisfies the Shrödinger equation $\partial\psi/\partial t = iH\psi$, where $H$ is hamiltonian within a real factor. An evolution of $\psi$ is determined by the unitary operator $U(t) : \psi(t) = U\psi(0)$ which satisfies the equation $\dot{U} = iHU$. This equation is a prototype for all systems of differential equations studied in the following. We need only to choose the hamiltonian so that the amplitude of a target state peaks at a point $t_{\text{quant}}$ which is less than the time of the best classical computation. In rare cases quantum parallelism makes this possible.

Some other aspects of parallelism in computing may be found in [9, 10, 31, 46].

## 4. An exact description of simple quantum search by differential equations

### 4.1 Notations

Assume the notations of Dirac where a vector $\bar{a} \in C^m$ as a column of coordinates is denoted by $|\bar{a}\rangle$. A row obtained from $|\bar{a}\rangle$ by the transposition and complex conjugation is denoted by $\langle\bar{a}|$. A dot product of $\bar{a}, \bar{b} \in C$ will be $\langle\bar{a}|\bar{b}\rangle$. The result of applying operator $A$ to vector $|\bar{a}\rangle$ is denoted by $A|\bar{a}\rangle$. For every transformation $A, B$ of the form $\mathcal{L}_1 \to \mathcal{L}_2$, $\mathcal{L}_2 \to \mathcal{L}_3$ we denote by $AB$ their composition, which acts from right to left such that $AB(x) = A(B(x))$. Given vectors $a \in \mathcal{L}$, $b \in \mathcal{M}$ from linear spaces $\mathcal{L}, \mathcal{M}$ the state $|a\rangle \otimes |b\rangle \in \mathcal{L} \otimes \mathcal{M}$ is denoted by $|a, b\rangle$. For a function $F$: $F|X, Y\rangle = |X, \phi(Y)\rangle$ we denote by $F|_Y$ its restriction on $Y$: $F|_Y|Y\rangle = |\phi(Y)\rangle$.

Let $f$ be a function of the form $A \to A$. We define an $i$th iteration of $f$: $f^{\{i\}}$ by the following induction on $i$. Basis: $f^{\{1\}} = f$. Step: $f^{\{i+1\}} = ff^{\{i\}}$.

### 4.2 Grover's quantum algorithm for simple search and its implementation in our model

Grover's algorithm for finding a unique solution $x_0$ of an equation $f(x) = 1$ for a boolean $f$ is sequential application of the unitary transformation $G = -WR_0WR_t$ to the initial state $\chi_0 = 1/\sqrt{N}\sum_{i=0}^{N-1}|e_i\rangle$ where the Walsh–

Hadamard transformation is $W = \underbrace{J \otimes \cdots \otimes J}_{n}$,

$$J = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix},$$

$$R_0|e\rangle = \begin{cases} |e\rangle, & \text{if } e \neq \bar{0}, \\ -|0\rangle, & \text{if } e = \bar{0}, \end{cases}$$

$$R_t|e\rangle = \begin{cases} |e\rangle, & \text{if } e \neq x_0, \\ -|x_0\rangle, & \text{if } e = x_0. \end{cases}$$

It can be easily seen that $W$ can be implemented on our model of a quantum computer.

To implement $R_t$ it is sufficient to apply $\mathrm{Qu}_f$ to the state

$$\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |e_i\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

where the last qubit is the place for the oracle's answer.

To implement $R_0$ we need $n+1$ ancillary qubits initialized to 0. Consider some function $\phi$ acting on three qubits: $|$main, ancilla, *res*$\rangle$ as follows:

$$\begin{aligned} &|000\rangle \to |000\rangle \\ &|100\rangle \to |101\rangle \\ &|001\rangle \to |001\rangle \\ &|101\rangle \to |111\rangle. \end{aligned}$$

Apply $\phi$ sequentially after each step moving pointers to the right one qubit in the main and ancillary areas (see Figure 3). This makes $res = 1$ if and only if at least one of the main qubits is 1. Then inverse the phase of 0 in the qubit *res* and fulfill all reverse transformations with $\phi$ in reverse order restoring the initial states of ancillary qubits.

Let $\chi_i = a_i \sum_{e' \neq e} |e'\rangle + b_i|e\rangle, \chi_{i+1} = G\chi_i$, $e$ is a state of the quantum part corresponding to a target word $x_0$. The difference between $x_0$ and $e$ is that $e$ also contains ancillary qubits having values that will be restored after each step of computation (it can be simply traced in what follows).

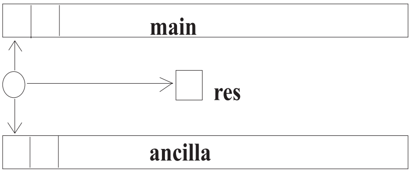

**Figure 3.** Ancillary registers.

The main property of Grover's transformation may be represented by the following equations (see [8, 23]):

$$\begin{cases} b_{i+1} & = \left(1 - \frac{2}{N}\right) b_i + 2\left(1 - \frac{1}{N}\right) a_i, \\ a_{i+1} & = -\frac{2}{N} b_i + \left(1 - \frac{2}{N}\right) a_i. \end{cases} \tag{4}$$

### 4.3 The passage to the system of differential equations

Equation (4) can be rewritten in the form:

$$\begin{cases} b_{i+1} - b_i & = -\frac{2}{N} b_i + 2\left(1 - \frac{1}{N}\right) a_i, \\ a_{i+1} - a_i & = -\frac{2}{N} b_i - \frac{2}{N} a_i, \end{cases} \tag{5}$$

where the initial condition of the quantum part gives $a_0 = b_0 = 1/\sqrt{N}$. Equation (5) with the initial condition is the system of difference equations approximating the following system of linear differential equations:

$$\begin{cases} \dot{b}\delta & = -\frac{2}{N} b + 2\left(1 - \frac{1}{N}\right) a, \\ \dot{a}\delta & = -\frac{2}{N} b - \frac{2}{N} a, \end{cases} \tag{6}$$

with two unknown functions $a(t), b(t)$, constant $\delta > 0$, and the initial condition $a(0) = b(0) = \sqrt{N}$, where $a_i, b_i$ approximate $a(i\delta), b(i\delta)$; $\delta$ is a step. A difference between solutions of equations (5) and (6) on a segment of the form $t \in [0, O(\delta\sqrt{N})]$ is $O(\sqrt{N}\delta^2)$, hence the error of this approximation may be made as small as required by varying $\delta$ (an integral part of number $x$ is denoted by $[x]$).

Solving equation (6) we obtain

$$\ddot{b} + \frac{4}{\delta^2 N} b + O\left(\frac{b}{\delta^2 N^2}\right) + \ddot{b} O\left(\frac{1}{N}\right) + \dot{b} O\left(\frac{1}{N\delta}\right) = 0.$$

Hence within time $O(1/\sqrt{N})$ a solution $b$ of equation (6) can be approximated by a solution of

$$\ddot{b} + \frac{4}{\delta^2 N} b = 0 \tag{7}$$

with the initial conditions $b(0) = 1/\sqrt{N}$, $1/2(\dot{b}(0)\delta + 2/N b(0)) = 1/\sqrt{N}$ on the segment $[0, 2/\omega]$, where $\omega = 2/\delta\sqrt{N}$. The required solution of equation (7) with this accuracy is $b = \sin(\omega t) + 1/\sqrt{N}\cos(\omega t)$, and the maximum of amplitude 1 is at the point $t_0 = \pi\sqrt{N}/4\delta - \delta/2$. Then $\left[t_0/\delta\right] = \left[\pi\sqrt{N}/4\right] \pm 1$ recurrent steps of equation (4) are necessary and sufficient to achieve this value of $b$ with this accuracy. Thus we obtain that the accuracy $O(1/\sqrt{N})$ is reached in $\left[\pi\sqrt{N}/4\right]$ iterations of the Grover algorithm. In [8] the authors obtained an exact solution of equation (4) and thus proved that in fact a probability of error is even about $1/N$. The approximation of the amplitude evolution by systems of differential equations is a more universal method. For example, it makes handling the more involved case of a parallel algorithm for RS possible, which is the subject of section 5.

## 5. Parallel algorithm for repeated quantum search

### 5.1 Definitions and result

Let $u$, $x$, and $y$ be variables with values from three different copies of $\mathcal{H}_0 = \mathrm{C}^N$, $a = a_1 \otimes a_2 \in \mathrm{C}^4$, where $a_1 = a_2 = 1/\sqrt{2}(|0\rangle - |1\rangle)$. We assume the notations $f_1(x)$, $f_2(x,y)$ for two oracles in the repeated quantum search and let $e_1, e_2$ be values for $x, y$ representing unique solutions of the equations $f_1 = 1$, $f_2 = 1$. We denote the corresponding states of the quantum tape by the same letters.

Put $\mathcal{H} = \mathcal{H}_0 \otimes \mathcal{H}_0 \otimes \mathcal{H}_0 \otimes \mathrm{C}^4$. Let

$$\begin{aligned} F_1|u,x,y,a\rangle &= |u,x,y,a_1 \oplus f_1(u), a_2\rangle, \\ F_2|u,x,y,a\rangle &= |u,x,y,a_1, a_2 \oplus f_2(x,y)\rangle, \\ P|u,x,y,a\rangle &= |u \oplus x, x, y, a\rangle. \end{aligned}$$

Then

$$F_1|u,x,y,a\rangle = \begin{cases} |u,x,y,a\rangle, & \text{if } u \neq e_1, \\ -|u,x,y,a\rangle, & \text{if } u = e_1; \end{cases}$$

$$F_2|u,x,y,a\rangle = \begin{cases} |u,x,y,a\rangle, & \text{if } |x,y\rangle \neq |e_1,e_2\rangle, \\ -|u,x,y,a\rangle, & \text{if } |x,y\rangle = |e_1,e_2\rangle. \end{cases}$$

Define the following auxiliary unitary transformations on $\mathcal{H}$:

$$\begin{aligned} \mathcal{R}_0 &= I \otimes R_{0x} \otimes R_{0y} \otimes I; \\ \mathcal{W} &= I \otimes W_x \otimes W_y \otimes I; \\ \mathcal{F} &= P(F_1 \,|_{u,a_1} \otimes F_2 \,|_{x,y,a_2})P, \end{aligned}$$

where the lower indices $x, y$ point to the corresponding area for applying Walsh–Hadamard transformations and rotations of the phase of 0, and $I$ denotes the identity.

The key unitary transformation of a parallel algorithm for RS is

$$Z = \mathcal{W}\mathcal{R}_0\mathcal{W}\mathcal{F}. \tag{8}$$

The *parallel algorithm* for RS is the sequential application of $Z$ beginning with the initial state

$$\chi_0 = |\bar{0}\rangle \otimes \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |e_i\rangle \otimes \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |e_i\rangle \otimes a$$

$[\pi\sqrt{N}/2\sqrt{2}]$ times.

**Theorem 1.** Let $t = [\pi\sqrt{N}/2\sqrt{2}]$. Then the observation of $Z^{\{t\}}(\chi_0)$ gives $x = e_1$, $y = e_2$ with probability of error $O(1/\sqrt{N})$.

## 5.2 An advantage of the parallel quantum algorithm

It follows from the definition of $Z$ that oracles $F_1$ and $F_2$ for functions $f_1, f_2$ work simultaneously in parallel, hence the algorithm requires approximately $[\pi\sqrt{N}/2\sqrt{2}]$ simultaneous queries to obtain a result, when the sequential application of simple quantum searches with $f_1$ and then with $f_2$ requires $[\pi\sqrt{N}/2]$ time steps to obtain a result with the same probability. Note that for a simple search the constant factor $\pi\sqrt{N}/4$ cannot be essentially improved [8].

Suppose that every query is fulfilled by a physical device (oracle) of the peculiar type corresponding to a form of query. Thus we consider oracles as a type of hardware. A set with a minimum of oracles which is necessary for the solution of RS consists of one oracle for $f_1$ and one for $f_2$. We can run these oracles simultaneously in the parallel algorithm and obtain a result $\sqrt{2}$ times faster than by sequential search. But if we have *two copies* of each oracle it is possible to achieve the same performance by sequential search if we divide the whole domain $\{0,1\}^n$ into two equal parts of $N/2$ elements each and apply a simple quantum search initially with two copies of oracle $f_1$—one for each part—then, having $e_1$, with two copies of oracle $f_2$. But this way is expensive if every copy of the oracle has a large cost, or impossible if every oracle is unique, say issues from a natural phenomenon. Only in this case of the minimal possible set of oracles $f_1, f_2$ does the application of a parallel quantum algorithm for RS give an increase in performance of $\sqrt{2}$ times. This speedup can also be obtained for IS if we apply this algorithm sequentially for the pairs $f_i, f_{i+1}$, $i = 1, 2, \ldots, k-1$. The resulting error probability will be $O(k/\sqrt{N})$.

The main feature of the parallel algorithm is the speedup without any extra hardware. It is significant because Grover's algorithm for the simple quantum search cannot be sped up even by a constant factor.

The remainder of this paper is devoted to the proof of Theorem 1 and perspectives of this approach.

## 5.3 A primary analysis of the parallel algorithm for repeated search

Note that each of $W_y$, $R_{0y}$ commutes with $W_x$, $R_{0x}$, $P$, $F_1$; $P$ commutes with $F_2$, hence $Z$ can be represented in the form

$$Z = -[(I \otimes W_x R_{0x} W_x \otimes I)PF_1P][-(I \otimes (W_y R_{0y} W_y) \otimes I)F_2],$$

or in the form

$$Z = \{-W_x R_{0x} W_x \mathcal{F}_1\}\{-W_y R_{0y} W_y F_2\}, \tag{9}$$

where

$$\mathcal{F}_1|u,x,y,a\rangle = \begin{cases} |u,x,y,a\rangle & \text{if } x \neq e_1, \\ -|u,x,y,a\rangle & \text{if } x = e_1. \end{cases}$$

Equation (9) is exactly the repetition of Grover's transformations with oracles $F_2, \mathcal{F}_1$ in this order, hence we can apply equation (4) for the resulting amplitudes of these transformations. Let the $Z$-iterations be $\chi_0 \to \chi_1 \to \cdots \to \chi_t, \chi_{i+1} = Z(\chi_i), i = 0, 1, \ldots, t-1$;

$$\chi_i = b_i|e_1 e_2\rangle + a_i|e_1 N_2\rangle + \alpha_i|N_1 N_2\rangle + \beta_i|N_1 e_2\rangle, \tag{10}$$

where $e_1$ and $e_1, e_2$ are the target states. Unique solutions for $f_1(x) = 1$ and for $f_2(x,y) = 1$ respectively, $N_1 = \sum_{i=2}^{N} e_i$, $N_2 = \sum_{i\neq 2} e_i$ (we omit ancillary qubits).

We represent the transformation $\chi_i \to Z(\chi_i)$ as two sequential steps:

$$\chi_i \overset{1}{\to} Z_1(\chi_i) = \chi_i' \overset{2}{\to} Z_2(\chi_i') = \chi_{i+1},$$

where $Z_1 = -W_y R_{0y} W_y F_2$, $Z_2 = -W_x R_{0x} W_x \mathcal{F}_1$. To calculate the change of amplitude resulting from the application of $Z_1$ (or $Z_2$) we shall fix a value of $x$ (or $y$ respectively).

- *Step 1.* Denote amplitudes of basic states in $\chi_i'$ by the corresponding letters with primes:

  $$\chi_i' = b_i'|e_1 e_2\rangle + a_i'|e_1 N_2\rangle + \alpha_i'|N_1 N_2\rangle + \beta_i'|N_1 e_2\rangle.$$

  Then for the two essentially different ways to fix a basic state for $x$: $x = e_1$ or $x + e_j$, $j \neq 1$ we shall have the different expressions for new amplitudes. Use the property of the diffusion transformation $WR_0W$ to be an inversion about average [23]. Let $\lambda_{\text{av}}$ be an average amplitude of the corresponding quantum state.

  (a) $\underline{x = e_1}$.

  $$\lambda_{\text{av}} = \tfrac{(N-1)a_i - b_i}{N}, \quad b_i' = 2\lambda_{\text{av}} + b_i, \quad a_i' = 2\lambda_{\text{av}} - a_i,$$

  $$b_i' = \frac{2(N-1)a_i - 2b_i}{N} + b_i = b_i\left(1 - \frac{2}{N}\right) + 2a_i\left(1 - \frac{1}{N}\right),$$

  $$a_i' = \frac{2(N-1)a_i - 2b_i}{N} - a_i = -b_i\frac{2}{N} + a_i\left(1 - \frac{2}{N}\right).$$

  (b) $\underline{x = e_j,\ j \neq 1}$.

  $$\lambda_{\text{av}} = \tfrac{(N-1)\alpha_i + \beta_i}{N}, \quad \alpha_i' = 2\lambda_{\text{av}} - \alpha_i, \quad \beta_i' = 2\lambda_{\text{av}} - \beta_i,$$

  $$\alpha_i' = \frac{2(N-1)\alpha_i + 2b_i}{N} - a_i = \alpha_i\left(1 - \frac{2}{N}\right) + 2\beta_i\frac{2}{N},$$

  $$\beta_i' = \frac{2(N-1)\alpha_i + 2\beta_i}{N} - \beta_i = \alpha_i\left(1 - \frac{1}{N}\right) - \beta_i\left(1 - \frac{2}{N}\right).$$

- *Step 2*. $\chi'_i \overset{2}{\to} Z_1(\chi'_i) = \chi_{i+1}$.

  We have two different ways to fix a basic state for $y$: $y = e_2$ or $y = e_j$, $j \neq 2$.

  (a) $\underline{y = e_2}$.

$$\begin{aligned}
\lambda_{\text{av}} &= \frac{(N-1)\beta'_i - b'_i}{N},\\
b_{i+1} &= 2\lambda_{\text{av}} + b'_i = b'_i\left(1 - \frac{2}{N}\right) + 2\beta'_i\left(1 - \frac{1}{N}\right),\\
\beta_{i+1} &= 2\lambda_{\text{av}} - \beta'_i = \beta'_i\left(1 - \frac{2}{N}\right) - b'_i\frac{2}{N}.
\end{aligned}$$

  (b) $\underline{y = e_j,\ j \neq 2}$.

$$\begin{aligned}
\lambda_{\text{av}} &= \frac{(N-1)\alpha'_i - a'_i}{N},\\
a_{i+1} &= 2\lambda_{\text{av}} + a'_i = a'_i\left(1 - \frac{2}{N}\right) + 2\alpha'_i\left(1 - \frac{1}{N}\right),\\
\alpha_{i+1} &= 2\lambda_{\text{av}} - \alpha'_i = \alpha'_i\left(1 - \frac{2}{N}\right) - a'_i\frac{2}{N}.
\end{aligned}$$

Hence, the recurrent formulas for amplitudes of sequential Steps 1 and 2 acquire the form:

$$\begin{aligned}
b_{i+1} &= b_i\left(1 - \frac{2}{N}\right)^2 + 2a_i\left(1 - \frac{1}{N}\right)\left(1 - \frac{2}{N}\right) + 4\alpha_i\left(1 - \frac{1}{N}\right)^2\\
&\quad -2\beta_i\left(1 - \frac{2}{N}\right)\left(1 - \frac{1}{N}\right);\\
a_{i+1} &= a_i\left(1 - \frac{2}{N}\right)^2 - b_i\frac{2}{N}\left(1 - \frac{2}{N}\right) + 2\alpha_i\left(1 - \frac{2}{N}\right)\left(1 - \frac{1}{N}\right)\\
&\quad +2\beta_i\frac{2}{N}\left(1 - \frac{1}{N}\right);\\
\alpha_{i+1} &= \alpha_i\left(1 - \frac{2}{N}\right)^2 + \beta_i\frac{2}{N}\left(1 - \frac{2}{N}\right) - a_i\left(1 - \frac{2}{N}\right)\frac{2}{N} + b_i\frac{4}{N^2};\\
\beta_{i+1} &= 2\alpha_i\left(1 - \frac{1}{N}\right)\left(1 - \frac{2}{N}\right) - \beta_i\left(1 - \frac{2}{N}\right)^2\\
&\quad -b_i\left(1 - \frac{2}{N}\right)\frac{2}{N} - 2a_i\left(1 - \frac{1}{N}\right)\frac{2}{N}.
\end{aligned}$$

Thus the matrix of one step of the algorithm has the form

$$Z = \begin{pmatrix} 1 & 2 & 4 & -2\\ -\frac{2}{N} & 1 & 2 & \frac{4}{N}\\ \frac{4}{N^2} & -\frac{2}{N} & 1 & \frac{2}{N}\\ -\frac{2}{N} & \frac{4}{N} & 2 & -1 \end{pmatrix}.$$

The system of recurrent equations can be rewritten as the following system of difference equations.

$$\begin{aligned}
b_{i+1} - b_i &= 2a_i + 4\alpha_i - 2\beta_i + b_i O_1\left(\frac{1}{N}\right) + a_i O_2\left(\frac{1}{N}\right)\\
&\quad + \alpha_i O_3\left(\frac{1}{N}\right) + \beta_i O_4\left(\frac{1}{N}\right);\\
a_{i+1} - a_i &= -\frac{2}{N} b_i + 2\alpha_i + a_i O_5\left(\frac{1}{N}\right) + b_i O_6\left(\frac{1}{N^2}\right)\\
&\quad + \alpha_i O_7\left(\frac{1}{N}\right) + \beta_i O_8\left(\frac{1}{N}\right);\\
\alpha_{i+1} - \alpha_i &= -\frac{2}{N} a_i + \beta_i O_{13}\left(\frac{1}{N}\right) + a_i O_{14}\left(\frac{1}{N^2}\right)\\
&\quad + b_i O_{15}\left(\frac{1}{N^2}\right) + \alpha_i O_{16}\left(\frac{1}{N}\right);\\
\beta_{i+1} - \beta_i &= -\frac{2}{N} b_i + 2\alpha_i - 2\beta_i + a_i O_9\left(\frac{1}{N}\right) + \alpha_i O_{10}\left(\frac{1}{N}\right)\\
&\quad + \beta_i O_{11}\left(\frac{1}{N}\right) + b_i O_{12}\left(\frac{1}{N^2}\right).
\end{aligned} \tag{11}$$

### 5.4 An approximation of amplitude evolution by differential equations

Let $\{\bar{c}_i\}$ be a sequence of vectors from $C^k$: $\bar{c}_i = (c_i^1, c_i^2, \ldots, c_i^k)$, $\overset{j}{ci} \in C$, which satisfies the following system of difference equations

$$\bar{c}_{i+1} - \bar{c}_i = A\bar{c}_i, \tag{12}$$

where $A$ is a matrix of size $k \times k$ with complex elements.

Let $m$ be an integer and a function $C(t)$: $R \to C^k$ is a solution of the system of differential equations

$$\dot{C}(t) = mAC(t) \tag{13}$$

with the initial condition

$$C(0) = \bar{c}_0. \tag{14}$$

Then the exact solution of the Cauchy problem (equations (13) and (14)) is $C(t) = R(t)\bar{c}_0$, where the resolvent matrix $R(t) = \exp(mAt)$. Equation (12) will be the system of difference equations approximating $C(t)$ by Euler's method if we consider $\bar{c}_i$ as an approximation of $C(i/m)$, $i = 0, 1, \ldots$. The accuracy of approximation may be obtained by the Taylor formula $C((i+1)/m) = C(i/m) + 1/m\dot{C}(i/m) + 1/2m^2\ddot{C}(t_1)$, $i/m < t_1 < (i+1)/m$. Here the error $\epsilon_1$ of one step of equation (12) is the third summand $1/2m^2\ddot{C}(t_1) = 1/2A^2C(t_1)$. Thus the error at the first step is $1/2A^2\exp(mA\theta_1)\bar{c}_0$, at the second step: $1/2A^2\exp(mA\theta_2)\bar{c}_1 + \exp(mA1/m)1/2A^2\exp(mA\theta_1)\bar{c}0 = 1/2A^2\exp(mA\theta_2)(\bar{c}_0 + A\bar{c}_0 + 1/2A^2$

$\exp(mA\theta_1)\bar{c}_0) + \exp(A)1/2A^2 \exp(mA\theta_1)\bar{c}_0$, and so forth, at the $i$th step the error will be $\epsilon_i \le 3/2 \sum_{j=1} i \exp(A\alpha_j)A^2\bar{c}_0$, where $0 < \alpha_j < 1$. Hence if $\|\bar{c}_0\| \le h$, then the error after the $i$th step is $\epsilon_i = O(ih)$. Particularly, for the initial conditions $\|c_0\| = O(1/N)$ a good approximation can be obtained if $i = o(N)$, and thus we can solve the Cauchy problem instead of equation (11) for $i = O(\sqrt{N})$ having an error as small as required for sufficiently large $N$.

Define a new function $B(\tau)$ as $B(tm) = C(t)$. In terms of $B$ the Cauchy problem acquires the form

$$\frac{\mathrm{d}}{\mathrm{d}\tau}B(\tau) = AB(\tau), \qquad B(0) = c_0. \tag{15}$$

Apply this to the solution $\bar{c}_i = |b_i, a_i, \alpha_i, \beta_i\rangle$ of equation (11), where $\bar{c}_0 = |1/N, 1/N, 1/N, 1/N\rangle$. Put $B = |b, a, \alpha, \beta\rangle$ for the scalar functions $b, a, \beta, \alpha$ and denote the argument of the function $B$ by $t$. Then equation (15), approximating equation (11), acquires the form:

$$\begin{aligned}
\dot{b} &= 2a + 4\alpha - 2\beta + bO_1\left(\frac{1}{N}\right) + \epsilon_1 + aO_0\left(\frac{1}{N}\right);\\
\dot{a} &= -\frac{2}{N}b + 2\alpha + \epsilon_2 + O_2\left(\frac{1}{N}\right)a;\\
\dot{\beta} &= -\frac{2}{N}b + 2\alpha - 2\beta + \epsilon_4 + O_4\left(\frac{1}{N}\right)a;\\
\dot{\alpha} &= -\frac{2}{N}a + \epsilon_3,
\end{aligned} \tag{16}$$

where $\epsilon_i = aO_{0i}(1/N^2) + bO_{1i}(1/N^2) + \beta O_{2i}(1/N) + \alpha O_{3i}(1/N)$, $i = 1, 2, 3, 4$, with the initial condition

$$b(0) = a(0) = \beta(0) = \alpha(0) = \frac{1}{N}. \tag{17}$$

Then for $t = O(\sqrt{N})$, $i = [t]$ the vector of error will be $\bar{\delta} = \bar{B}(t) - \bar{c}_i = O(1/\sqrt{N})$, $N \to \infty$ and with this accuracy we can write $b(i) \approx b_i$ for the amplitude $b_i$ of target state $|e_1, e_2\rangle$.

### 5.5 Tight analysis of the parallel quantum algorithm for repeated search

Now we take up the system of linear differential equations (16) with the initial conditions of equation (17). Our goal is to solve it on a segment of the form $0 \le t \le O(\sqrt{N})$. Equation (16) can be represented in the form $\dot{B} = MB$, where its matrix $M = Z - 1 = \tilde{A}_0 + E + H$ (1 denotes the identity matrix) for the matrices

$$\tilde{A}_0 = \begin{pmatrix} 0 & 2 & 4 & 0 \\ -\frac{2}{N} & 0 & 2 & 0 \\ 0 & -\frac{2}{N} & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \qquad E = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -\frac{2}{N} & 0 & 2 & -2 \end{pmatrix},$$

$$H = \begin{pmatrix} d_1 & d_1 & d_1 & -2+d_1 \\ d_2 & d_1 & d_1 & d_1 \\ d_2 & d_2 & d_1 & d_1 \\ d_2 & d_1 & d_1 & d_1 \end{pmatrix},$$

where $d_l$ denotes different expressions of the form $O(N^{-l})$, $l = 1, 2$.

We shall show that the deposit of $\tilde{A}_0$ to the solution of equations (16) and (17) is significant and deposits of $E$ and $H$ are negligible. What is the main difficulty here? Consider the resolvent matrix for the Cauchy problem (equations (16) and (17)), this is the solution $R(t)$ of the differential equation for matrices: $\dot{R} = MR$ with the initial condition $R(0) = 1$. Then we have $C(t) = RC(0)$. The matrix $R$ has the form $\exp(Mt)$. But in our case the matrices $\tilde{A}_0, E, H$ do not commutate, hence we cannot use the standard properties of exponent. In order to cope with this task we first solve the Cauchy problem at hand neglecting deposits of $E$ and $H$ to the main matrix $M$. The validity of this approximation is shown in section 5.6.

Now consider the reduced equation $\dot{C}(t) = AC(t)$ with the initial condition $C(0) = c_0$. Excluding the last column and row containing only zeroes we obtain the new matrix $A_0$. The characteristic equation for $A_0$ is $\lambda^3 + 8/N\lambda - 16/N^2 = 0$ and its nonzero solutions within $O(1/N)$ are $\lambda_{1,2} = \pm 2\sqrt{2}i/\sqrt{N}$. Then standard calculations give the approximation of the solution as

$$\begin{aligned} b &= \frac{1}{2} - \frac{1}{2}\cos\frac{2\sqrt{2}t}{\sqrt{N}}, \\ a &= \frac{1}{\sqrt{2N}}\sin\frac{2\sqrt{2}t}{\sqrt{N}} + \frac{1}{N}\cos\frac{2\sqrt{2}t}{\sqrt{N}}, \\ \alpha &= \frac{1}{2N}\cos\frac{2\sqrt{2}t}{\sqrt{N}} + \frac{1}{2N} \end{aligned} \tag{18}$$

within $|O(1/\sqrt{N}), O(1/N), O(1/N\sqrt{N})\rangle$. The amplitude $b$ from equation (18) peaks at the point $t_1 = \pi\sqrt{N}/2\sqrt{2}$ where $b(t_1) = 1$ within $O(1/\sqrt{N})$. Assuming that deposits of $E$ and $H$ to the solution are small, we obtain that the amplitude of target state $|e_1, e_2\rangle$ will be $1 - O(1/\sqrt{N})$ after $[\pi\sqrt{N}/2\sqrt{2}]$ steps of the parallel algorithm which is $\sqrt{2}$ times smaller than the time of sequential quantum search.

## 5.6 Completion of the proof

In the preprint version of this paper the deposits of $E$ and $H$ were estimated by the conventional procedure of approximating a solution of differential equations (see the Appendix in [37]). This is the immediate but cumbersome way to prove that this deposit is vanishing. After publication of the preprint version, Farhi and Gutmann developed a way to simplify this construction by uniting by pairs the sequential transformations in a parallel algorithm [21]. In this section this idea is combined with the approach of the first version.

First, turn to the orthonormal basis $E_1 = |e_1 e_2\rangle$, $E_2 = 1/\sqrt{N}|e_1 N_2\rangle$, $E_3 = 1/N|N_1 N_2\rangle$, $E_4 = 1/\sqrt{N}|N_1 e_2\rangle$. The matrix $Z$ in this basis acquires the form

$$A_1 = \begin{pmatrix} 1 & \frac{2}{\sqrt{N}} & \frac{4}{N} & -\frac{2}{\sqrt{N}} \\ -\frac{2}{\sqrt{N}} & 1 & \frac{2}{\sqrt{N}} & \frac{4}{N} \\ \frac{4}{N} & -\frac{2}{\sqrt{N}} & 1 & \frac{2}{\sqrt{N}} \\ -\frac{2}{\sqrt{N}} & \frac{4}{N} & \frac{2}{\sqrt{N}} & -1 \end{pmatrix}.$$

Now group together each pair of unitary transformations in the algorithm: $\chi_{2k} \to \chi_{2k+1} \to \chi_{2k+2}$ and denote by $B$ the corresponding matrix: $B_0 = A_1^2$. It is sufficient to prove that $\|B_0^{[\pi\sqrt{N}/4\sqrt{2}]}|0,0,1,0\rangle - |1,0,0,0\rangle\| = O(1/\sqrt{N})$, because one application of $A_1$ can only increase the error by $O(1/\sqrt{N})$.

The Cauchy problem for the recursion $\bar{c}_{i+1} = B_0 \bar{c}_i$ has the form $\dot{\bar{c}} = (B_0 - 1)\bar{c}$, $\bar{c} = \bar{c}_0$, and its resolvent has the form $R = \exp Bt$, where $B = B_0 - 1$. We have:

$$B \approx \frac{4}{\sqrt{N}} \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

within $O(1/N)$.

Thus we can consider only a projection of $\bar{c}$ to the subspace $\mathcal{H}_1$ spanned by $E_1, E_2, E_3$. Denote by $D$ the matrix

$$\begin{pmatrix} 0 & -\frac{i}{\sqrt{2}} & 0 \\ \frac{i}{\sqrt{2}} & 0 & -\frac{i}{\sqrt{2}} \\ 0 & \frac{i}{\sqrt{2}} & 0 \end{pmatrix}.$$

Then the restriction of $B$ to $\mathcal{H}_1$ has the form $4\sqrt{2}i/\sqrt{N}D$. It is easily seen that $D^{2k+1} = D$, $D^{2k} = D^2$ for $k = 1, 2, \ldots$. The initial state is $|0,0,1\rangle$ within $O(1/\sqrt{N})$. Put $k = 4\sqrt{2}/\sqrt{N}$. Then within $O(1/\sqrt{N})$ we have $|b, a, \alpha\rangle \approx C|0,0,1\rangle$, where

$$\begin{aligned} C &= \exp(kiDt) = \cos(kDt) + i\sin(kDt) \\ &= 1 - \frac{(kDt)^2}{2} + \frac{(kDt)^4}{4!} - \cdots + i\left(kDt - \frac{(kDt)^3}{3!} + \cdots\right) \\ &= 1 - D^2(1 - \cos kt) + iD\sin kt \end{aligned}$$

that immediately gives equation (18) and the theorem is proved.

## 6. Parallel implementation of iterated quantum search

### 6.1 Parallel quantum algorithm for iterated search

Now take up an IS problem for arbitrary $k$. Consider an evolution of amplitudes arising when $k$ oracles work in parallel. Let $\chi_i = \overset{i}{a}_0|N_1, N_2, \dots, N_k\rangle + \overset{i}{a}_1|e_1, N_2, \dots, N_k\rangle + \cdots + \overset{i}{a}_k|e_1, e_2, \dots, e_k\rangle + R_i$ (this generalizes equation (10)), where $R_i$ contains only basic states of the form $|\dots, N_p, \dots, e_q, \dots\rangle$. The natural generalization of the transformation equation (8) will be

$$Z_k = (-1)^k \mathcal{W}^{(k)} \mathcal{R}_0^{(k)} \mathcal{W}^{(k)} \mathcal{F}^{(k)},$$

where $\mathcal{W}^{(k)} = W_1 \otimes W_2 \otimes \cdots \otimes W_k \otimes I$, each Walsh–Hadamard transformation $W_i$ acts on $x_i$, $i = 1, 2, \dots, k$, $\mathcal{R}_0^{(k)} = R_{01} \otimes \cdots \otimes R_{0k} \otimes I$, each rotation of 0 phase $R_{0i}$ acts on $x_i$, $i = 1, 2, \dots, k$, $\mathcal{F}^{(k)} = F_1 \otimes \cdots \otimes F_k \otimes I$, each $F_i$ acts on $x_i$ and inverses the sign of $e_i$, identities $I$ act on ancilla.

Let a matrix $A$ determine an evolution of the quantum state in a parallel algorithm such that $\chi_i = A\chi_{i-1}$. $A$ represents the operator in $2^{kn}$-dimensional space. We reduce $A$ to an operator $A_r$ acting on $k + 1$-dimensional space generated by the vectors $|N_1, N_2, \dots, N_k\rangle, |e_1, N_2, \dots, N_k\rangle, \dots, |e_1, e_2, \dots, e_k\rangle$. Then represent $A_r$ as $A_r = A_0 + B$, where $A_0$ is a Jacobi matrix of the form

$$\begin{pmatrix} 0 & 2 & 0 & \dots & 0 \\ -\frac{2}{N} & 0 & 2 & \dots & 0 \\ \dots & \dots & \dots & \ddots & \dots \\ 0 & \dots & -\frac{2}{N} & 0 & 2 \\ 0 & \dots & 0 & -\frac{2}{N} & 0 \end{pmatrix}. \tag{19}$$

This matrix has the nonzero elements 2 (above the main diagonal) and $-2/N$ (behind it). Its size is $(k + 1) \times (k + 1)$. Assume that the effect of reduction: $A$ to $A_r$ and the deposit of $B$ are negligible. For $k > 2$ this fact can be proved by using iterated approximations (see the Appendix in [37]). An evolution of amplitude can be represented approximately as the solution of the Cauchy problem

$$\dot{\bar{a}} = A\bar{a}, \qquad a(0) = |N^{-k/2}, \dots, N^{-k/2}\rangle, \tag{20}$$

where $\bar{a}(i) \approx |\overset{i}{a}_1, \dots, \overset{i}{a}_k\rangle$, $i$ integer, we assume that $k \ll \sqrt{N}$.

### 6.2 Perspectives of a parallel quantum algorithm for iterated search

One can ask: Can we obtain a speedup by a big constant factor for IQS when applying parallel action of more than two oracles? In all probability the answer is no.

Estimate the growth of target amplitude as given. Canceling all $-2/N$ we can only increase this growth. This results in a simple system of linear differential equations whose solution is $a_k(t) = N^{-k/2} + 2^k \int_0^{t\{k\}} N^{-k/2} dt = N^{-k/2} + 2^k N^{-k/2} t^k/k!$. The parallel algorithm for IQS can exceed sequential quantum search only if $a_k(t)$ is substantially large for $t < k\sqrt{N}$. For example, let the parallel algorithm work only one quarter of the time required for the sequential search. Then it cannot reach the vanishing error probability for any $k$, because for such $t = \pi\sqrt{N}k/16$ $a_k \approx (\pi/8)^k\, k^k/k! < 1$.

Nevertheless, the parallel quantum algorithm has one advantage. Compare sequential and parallel quantum algorithms for IS in the case $1 \ll k \ll \sqrt{N}$, if total time $t = \sqrt{N}$. If $t = \sqrt{N}$ then $t$ sequential applications of $Z^{(k)}$ raise the amplitude $a_k$ up to the value $a_k(t) = a^k/k!$, $a = 2 - \epsilon$, where $\epsilon \to 0$ $(N \to \infty)$. Hence the resulting probability is $P_{\text{par}} = \left(a^k/k!\right)^2$.

On the other hand, if we have a total time $\sqrt{N}$ then we can apply sequential quantum searches with time $\sqrt{N}/k$ for each $x_i^0$, $i = 1, 2, \ldots, k$. The probability $P_{\text{seq}}$ to find $x_k^0$ will be less than $\left(2/k\right)^{2k}$ because for each search it does not exceed $\left(2/k\right)^2$. Consequently, $P_{\text{par}}$ exceeds $P_{\text{seq}}$ in more than $2^{2k}$ times.

This feature of the parallel algorithm for IS may be useful when quantum computations are organized with an additional classical parallelism. The classical type of parallelism does not use quantum entanglement between different processors but can raise the resulting probability by using extra memory.

### 6.3 Conclusion

To sum up, the parallel algorithm constructed for repeated quantum search is $\sqrt{2}$ times faster than sequential application of fast quantum search and it requires the same hardware. The advance is taken from interference arising when two oracles act simultaneously on the set of entangled qubits. This parallel quantum algorithm can be applied to the problem of $k$ dependent iterations of quantum search in areas of $N$ elements each, with the same effect of speedup in $\sqrt{2}$ times. Here the error probability will be vanishing if $k \ll o(\sqrt{N})$, $N \to \infty$.

In addition, for the fixed total time $\sqrt{N}$ a probability of success for the parallel algorithm is $2^{2k}$ times as big as for the sequential algorithm.

The effective speedup of $\sqrt{2}$ times cannot be increased, essentially by the same procedure, if we increase the number of oracles involved in the simultaneous action. Nevertheless, a possibility for further speedup of the iterated quantum search still remains.

## 7. Acknowledgments

I am grateful to Victor Maslov for his support and help, to Kamil Valiev for the interesting discussions, and especially to Lov Grover for his attention to my work.

I would like also to express my gratitude to Edward Farhi and Sam Gutmann who have read the preprint version of this work and suggested the simplification of the proof.

## References

[1] D. Aharonov and M. Ben-Or, "Fault-Tolerant Quantum Computation with Constant Error," submitted to *SIAM Journal of Computations*, lanl e-print quant-ph/9611025.

[2] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, "Elementary Gates for Quantum Computation," *Physical Review A*, **52** (1995) 3457–3467.

[3] A. Barenco, A. Ekert, K-A, Suominen, and P. Torma, "Approximated Quantum Fourier Transform and Decoherence," lanl e-print quant-ph/9601018.

[4] D. Biron, O. Biham, E. Biham, M. Grassl, and D. A. Lidar, "Generalized Grover Search Algorithm for Arbitrary Initial Amplitude Distribution," to appear in *Physical Review A*, lanl e-print quant-ph/9801066.

[5] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. De Wolf, "Tight Quantum Bounds by Polynomials," lanl e-print quant-ph/9802049.

[6] P. Benioff, "Quantum Mechanical Hamiltonian Models of Turing Machines," *Journal of Statistical Physics*, **22** (1982) 515–546.

[7] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and Weaknesses of Quantum Computing," *SIAM Journal of Computation*, **26** (5) (1997) 1510–1523, lanl e-print quant-ph/9701001.

[8] M. Boyer, G. Brassard, P. Hoyer, and A. Tapp, "Tight Bounds on Quantum Searching," in *Fourth Workshop on Physics and Computation*, edited by T. Toffoli, M. Biaford, and J. Leao (New England Complex Systems Institute, 1996).

[9] V. Belavkin and V. Maslov, "Design of the Optimal Dynamics Analysis: Mathematical Aspects of Sound and Visual Pattern Recognition," in *Mathematical Aspects of Computer*, edited by V. P. Maslov and V. P. Belavkin (Mir, Moscow, 1988).

[10] V. P. Belavkin and M. Ohya, "Quantum Entanglements and Entangled Mutual Entropy," lanl e-print quant-ph/9812082.

[11] E. Bernstein and U. Vazirani, "Quantum Complexity Theory," *SIAM Journal of Computation*, **26** (5) (1997) 1411–1473.

[12] N. J. Cerf, L. K. Grover, and C. P. Williams, "Nested Quantum Search and NP-complete Problems," lanl e-print quant-ph/9806078.

[13] I. L. Chuang, R. Laflamme, P. W. Shor, and W. H. Zurek, "Quantum Computers, Factoring, and Decoherence," *Science*, **270** (1995) 1633–1635.

[14] W. van Dam, "Quantum Oracle Interrogation: Getting All Information for Almost Half the Price," *Proceedings of the 39th Annual IEEE Symposium of Computer Science (FOCS'98)*, 362–367, lanl e-print quant-ph/9805006.

[15] D. Deutsch, "Quantum Theory, the Church–Turing Principle and the Universal Quantum Computer," *Proceedings of the Royal Society A*, **400** (1985) 97–117.

[16] D. Deutsch and R. Jozsa, "Rapid Solution of Problems by Quantum Computation," *Proceedings of the Royal Society A*, **449** (1992) 553–558.

[17] D. P. DiVincenzo, "Two-bit Gates are Universal for Quantum Computation," *Physical Review A*, **51** (1995) 1015–1022.

[18] C. Durr and P. Hoyer, "A Quantum Algorithm for Finding the Minimum," lanl e-print quant-ph/9607014.

[19] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, "A Limit on the Speed of Quantum Computation in Determining Parity," *Physical Review Letters*, **81** (1998) 5442–5444, lanl e-print quant-ph/9802045.

[20] E. Farhi and S. Gutmann, "Quantum Mechanical Square Root Speedup in a Structured Search Problem," lanl e-print quant-ph/9711035.

[21] E. Farhi and S. Gutmann, private communication.

[22] R. P. Feynman, "Simulation Physics with Computers," *International Journal of Physics*, **21** (1982) 467–488.

[23] L. K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," *Proceedings, STOC 1996*, 212–219, Philadelphia, PA, USA.

[24] L. K. Grover, "A Fast Quantum Mechanical Algorithm for Estimating the Median," lanl e-print quant-ph/9607024.

[25] T. Hogg, "A Framework for Structured Quantum Search," *Physica D*, **120** (1998) 102–116, lanl e-print quant-ph/9701013.

[26] A. S. Holevo, "Coding Theorems for Quantum Channels," lanl e-print quant-ph/9809023.

[27] J. A. Jones, M. Mosca, and R. H. Hansenabs, "Implementation of a Quantum Search Algorithm on a Nuclear Magnetic Resonance Quantum Computer," *Nature*, **393** (1998) 344–346, lanl e-print quant-ph/9805069.

[28] R. Jozsa, “Searching in Grover’s Algorithm,” lanl e-print quant-ph/9901021.

[29] A. Yu. Kitaev, “Quantum Measurements and the Abelian Stabilizer Problem,” lanl e-print quant-ph/9511026.

[30] A. Yu. Kitaev, “Fault-tolerant Quantum Computation by Anyons,” lanl e-print quant/ph/9707021.

[31] G. L. Litvinov, V. P. Maslov, and G. B. Shpiz, “Nondigital Implementation of Real Numbers’ Arithmetic by Means of Quantum Computer Media,” lanl e-print quant-ph/9904025.

[32] S. Lloyd, “A Potentially Realizable Quantum Computer,” *Science*, **261** (1993) 1569–1571.

[33] S. Lloyd, “Almost Any Quantum Logic Gate is Universal,” *Physical Reviews Letters*, **75** (1995) 346–349.

[34] N. Margolus and L. B. Levitin, “The Maximum Speed of Dynamical Evolution,” *Physica D*, **120** (1998) 188–195.

[35] Y. Ozhigov, “Quantum Computers Speedup Classical with Probability Zero,” *Chaos, Solitons, and Fractals*, **10** (10) (1999) 1707–1714, lanl e-print quant-ph/9803064.

[36] Y. Ozhigov, “Lower Bounds of Quantum Search for Extreme Point,” *Proceedings of the Royal Society A*, **455** (1999) 2165–2172.

[37] Y. Ozhigov, “Speedup of Iterated Quantum Search by Parallel Performance,” lanl e-print quant-ph/9904039.

[38] R. Penrose, *Shadows of the Mind* (Oxford University Press, New York, 1994).

[39] J. Preskill, “Fault Tolerant Quantum Computation,” to appear in *Introduction to Quantum Computations*, edited by H-K. Lo, S. Popescu, and T. P. Spiller, lanl e-print quant-ph/9712048.

[40] D.A. Ross, “A Modification of Grover’s Algorithm as a Fast Database Search,” lanl e-print quant-ph/9807078.

[41] P. W. Shor, “Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” *SIAM Journal of Computation*, **26** (5) (1997) 1484–1509.

[42] D. Simon, “On the Power of Quantum Computation,” *SIAM Journal of Computation*, **26** (5) (1997) 1474–1483.

[43] A. M. Steane, “Space, Time, Parallelism and Noise Requirements for Reliable Quantum Computing,” lanl e-print quant-ph/9708021.

[44] B. M. Terhal and J. A. Smolin, “Single Quantum Querying of a Database,” lanl e-print quant-ph/9705041.

[45] "J. Watrous, On One-Dimensional Quantum Cellular Automata," *Proceedings of the 36th Annual IEEE Symposium on Foundations of Computer Science* (1995).

[46] S. Wolfram, *Cellular Automata and Complexity: Collected Papers* (Addison-Wesley, Reading, 1994).

[47] A. Yao, "Quantum Circuit Complexity," *Proceedings of the 34th Annual Symposium on Foundations of Computer Science*, 1993, 352–361.

[48] C. Zalka, "Grover's Quantum Searching Algorithm is Optimal," lanl e-print quant-ph/9711070.