Speedup of iterated quantum search by parallel performance

Yuri Ozhigov *

Abstract

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 of which f_i takes the value 1 in a single point of the form $x_1^0, x_2^0, \ldots, x_i^0$, $i = 1, 2, \ldots, k$. A length of all x_i^0 is n, $N = 2^n$. It is shown how to find x_k^0 $(k \geq 2)$ using $\frac{k\pi\sqrt{N}}{4\sqrt{2}}$ simultaneous evaluations of functions of the form f_i, f_{i+1} with an error probability of order $k/\sqrt{N}$ which is $\sqrt{2}$ times as fast as by the k sequential applications of Grover algorithm for the 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 background and setting of a problem I present the short introduction to abstract quantum computations in the section 3. In the section 4 linear differential equations are applied to a tight analysis of the famous Grover algorithm of the fast quantum search.

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

1.2 Background

The most promising quantum mechanical application to the algorithm theory is associated with the fundamental algorithm of exhaustive search or finding a solution of equation $f(x) = 1$ for a Boolean function f. In 1996 Lov Grover in the work [Gr1] showed how quantum computer can solve this equation for the case of unique solution in a time $O(\sqrt{N})$ where N is the number of all possible values for x, whereas every probabilistic classical algorithm requires a time $O(N)$. At about the same time in the work [BBBV] it was shown that there are not substantially faster algorithm for this problem. Later a tight estimation for the time of Grover's algorithm

*Department of applied mathematics, Moscow state university of technology "Stankin", Vadkovsky per. 3a, 101472, Moscow, Russia, e-mail: y@ oz.msk.ru

as $\frac{\pi\sqrt{N}}{4}$ with the probability of error about $1/N$ was established in the work [BBHT]. A further development of the fast quantum search can be found in the works [DH], [FG], [Jo], [CGW], [Ro], [BBBGDL], [JMH], [H].

The earlier patterns of quantum speedup was constructed by P. Shor (look at the work [Sh]). There are the algorithms finding a factorization of an integer and a discrete logarithm. Algorithms of such a sort are presented in a lot of works (look for example at [DJ], [Gr2], [Ki1], [Si], [St], [TS], etc.).

The classical computations admitting quantum speedup are rare exclusions from all 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 $g:\ \{0,1\}^n \longrightarrow \{0,1\}^n$:

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

In the work [Oz1] it is shown that if $T = O(N^{\frac{1}{7+\epsilon}}),\ \epsilon > 0$, then for the bulk of all g such computation has not any quantum speedup. Similar results for search problems were obtained in the works [BBBV], [BBHT], [Oz2], [Za]. A lower bound as $O(N)$ for a time of quantum computations of functions with functional argument $F:\ \{f\} \longrightarrow \{0,1\}$ was found in the work [BBCMW]. Here f are Boolean functions on domain of cardinality N. At the same time using a memory of $O(N)$ qubits it is possible to compute such functions in a time $N/2$ (look at [vD]). This brings up the question: what a general type of classical computations of the form (1) admits a quantum speedup beyond any possible speedup of g? As follows from the work [Oz1] for the bulk of functions g this speedup can result only from a parallel application of g.

About other aspects of quantum evolutions look also at [ML], [Ho], [Pe].

2 Setting of 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 basing 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 one filled.

We formalize this as the special type of iterated algorithms: 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 equation $f_i(x_i) = 1$ where a Boolean function f_i is accessible iff we know all $x_j^0,\ \ j < i$, $|x_i| = n,\ \ N = 2^n,\ \ k \ll N$, $|x|$ denotes a length of word x. The aim is to discover x_k^0, $k \geq 2$. In view of the result of the work [BBHT] cited above sequential applications of Grover's search for $x_1^0, x_2^0, \ldots, x_k^0$ give an answer in the time $\frac{k\pi\sqrt{N}}{4}$ with error probability about k/N. To do this we must have all oracles $f_i,\ \ i = 1, 2, \ldots, k$, where the dependence f_i of all $x_j,\ \ j < i$ can be included to 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 can not be cloned we assume that they are in our disposal at the same time, so we can apply them simultaneously. In such application advantage is taken of interference between the results of their actions. This results in a speedup of computation comparatively with the sequential mode. Why this speedup can arise? It arises because of a

leak of amplitude in each step of sequential search. A leak of amplitude issues from that an amplitude of x_i^0 in search number i increases step by step in course of Grover's search, after few first l steps it becomes approximately $\frac{2l+1}{\sqrt{N}}$, when amplitudes of others $x_i \neq x_i^0$ decrease. This prevailing of the amplitude corresponding to x_i^0 (a leak of amplitude) can be immediately used for the next $i+1$-th search. We shall show how this effect can be used to solve the problem of iterated search in a time $O(\frac{k\pi\sqrt{N}}{4\sqrt{2}})$ which is $\sqrt{2}$ times as fast as by k sequential applications of Grover's algorithm. Thus we shall have a modification of the fast quantum search - the parallel quantum algorithm for iterated search which will be described later. In this article we take up mostly the particular case $k = 2$ of IS, we name this problem repeated search (RS).

RS-problem is connected with the known problem of structured search (SS). The problem of structured search is to find a unique solution x_0, y_0 of $f(x, y) = 1$ provided we have a function g whose support $\{x \mid g(x) = 1\}$ of cardinality M contains x_0. 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 the work [FG]. They have found quantum algorithm for this case with a time complexity $O(\sqrt{MN})$, and also they wrote that the best known strategy for the case $M = 1$ is the sequential application of Grover algorithm. In the present paper it is shown how this evident strategy can be improved in constant factor $\sqrt{2}$. At last note that our approach differs from the work [FG]. Farhi and Gutmann used only algebraic properties of Grover's algorithm whereas for RS-problem we need to work with an evolution of amplitudes in computation.

3 Quantum computations and differential equations

After early studies of R. Feynman ([Fe]), P. Benioff ([Be]) and D. Deutsch ([De]) numerous approaches to quantum computations have appeared (look at [BV], [Wa], [Ya], [Ll1]). Leaving aside the problem of decoherence and quantum codes (look at the articles [AB] , [CLSZ], [Ki2], [Pr]) we shall regard ideal computations in closed systems. We use the abstract model of quantum computer independent of the formalism of classical algorithm theory. This model consists of two parts: classical and quantum (look at the picture 1).

A state C of *Classical part* consists of the following objects.

1) Registers with labels corresponding to transformations U_{i_j} of the finite set $\{U_i\}$ of elementary unitary transformations with no more than 3 qubits each. (Strictly speaking transformations on two qubits would suffice: look for example at the work [DiV]). Moreover, as follows from the works [Ll2], [BBCDMSSSW] there is a variety of possible choices of 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 curcle of radius 1 in two dimensional Hilbert space C^2. If n is a length of tape, all states of the tape belong to the tensor product $\mathcal{H} = \underbrace{\mathrm{C}^2 \bigotimes \mathrm{C}^2 \bigotimes \ldots \bigotimes \mathrm{C}^2}_{n}$ of spaces, corresponding to all qubits that is $\mathcal{H} = \mathrm{C}^{2^n}$. Each state of quantum part is a superposition $\chi = \sum\limits_{i=0}^{N-1} \lambda_i e_i$ of basic states

$e_0, \ldots, e_{N-1}$ with complex amplitudes λ_i where $\sum\limits_{i=0}^{N-1} |\lambda_i|^2 = 1$, $N = 2^n$. We can assume that all $e_i \in \{0,1\}^n$.

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

A *Working transformation* of quantum part corresponding to a fixed state of classical part has the form $U_{i_1} \bigotimes U_{i_2} \bigotimes \ldots \bigotimes U_{i_k}$ 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 $\{0,1\}^n \longrightarrow \{0,1\}^m$ 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 an initial contents of the place for answer.

A *Query transformation* $\mathrm{Qu}_{\bar{f}}$ is $\mathrm{Qu}_{f_1} \bigotimes \mathrm{Qu}_{f_2} \bigotimes \ldots \bigotimes \mathrm{Qu}_{f_l}$ where for each $i = 1, \ldots, l$ $\mathrm{Qu}_{f_i} |a_i, b_i\rangle \longrightarrow |a_i, b_i \bigoplus f_i(a_i)\rangle$, $\bigoplus$ is bitwise addition modulo 2. We name these functions Qu_{f_i} oracles.

A *Quantum algorithm* is an algorithm determining evolution of the classical part:

$$C_0 \longrightarrow C_1 \longrightarrow \ldots \longrightarrow C_T \tag{2}$$

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

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

$$Q_0 \longrightarrow Q_1 \longrightarrow \ldots \longrightarrow Q_T \tag{3}$$

where for each $i = 0, 1, \ldots, T-1$ $e(C_i) = 0$; $e(C_T) = 1$ and every passage $Q_i \longrightarrow Q_{i+1}$ 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 a contents of first n_0 qubits of quantum tape after the observation of final state Q_T. An 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 (2),(3) is a 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 case of repeated search.

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

Some other aspects of parallelism in computing may be found in [BM], [BO], [LMS], [Wo].

4 An exact description of simple quantum search by differential equations

4.1 Notations

Assume the notations of Dirac where a vector $\bar{a} \in \mathrm{C}^m$ 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 $\bar{a}, \bar{b} \in \mathrm{C}$ will be $\langle\bar{a}|\bar{b}\rangle$. A result of application of operator A to a vector $|\bar{a}\rangle$ is denoted by $A|\bar{a}\rangle$. For every transformations $A,\ B$ of the forms $\mathcal{L}_1 \longrightarrow \mathcal{L}_2,\ \mathcal{L}_2 \longrightarrow \mathcal{L}_3$ 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 $|a\rangle \bigotimes |b\rangle \in \mathcal{L} \bigotimes \mathcal{M}$ 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 $A \longrightarrow A$. 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 equation $f(x) = 1$ for a Boolean f is sequential applications of the following unitary transformation: $G = -WR_0WR_t$ to the initial state $\chi_0 = \frac{1}{\sqrt{N}} \sum\limits_{i=0}^{N-1} |e_i\rangle$ where Walsh-Hadamard transformation is $W = \underbrace{J \bigotimes \ldots \bigotimes J}_{n}$,

$$J = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix},\quad R_0|e\rangle = \begin{cases} |e\rangle, & \text{if } e \neq \bar{0}, \\ -|0\rangle, & \text{if } e = \bar{0}, \end{cases} \quad R_t|e\rangle = \begin{cases} |e\rangle, & \text{if } e \neq x_0, \\ -|x_0\rangle, & \text{if } e = x_0. \end{cases}$$

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

To implement R_t it is sufficient to apply Qu_f to the state $\frac{1}{\sqrt{N}} \sum\limits_{i=0}^{N-1} |e_i\rangle \bigotimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$, where the last qubit is the place for oracle's answer.

To implement R_0 we need $n+1$ ancillary qubits initialized by 0. Consider some function ϕ acting on three qubits: $|\text{main, ancilla, } res\rangle$ as follows.

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

Apply ϕ sequentially after each step moving pointers to right on one qubit in the main and ancillary areas (look at the picture 3). This makes $res = 1$ iff 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 ϕ in the reverse order restoring the initial states of ancillary qubits.

Let $\chi_i = a_i \sum\limits_{e' \neq e} |e'\rangle + b_i|e\rangle$, $\chi_{i+1} = G\chi_i$, e is a state of quantum part, corresponding to a target word x_0. The difference between x_0 and e is that e contains also ancillary qubits whose

values will be restored after each step of computation (it can be simply traced in what follows). The main property of Grover's transformation may be represented by the following equations (look at [Gr1], [BBHT]).

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

4.3 The passage to the system of differential equations

The system (4) can be rewritten in the following form

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

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

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

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 $a(i\delta), b(i\delta)$; δ is a step. A difference between solutions of (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 done as small as required by varying δ (an integral part of number x is denoted by $[x]$).

Solving (6) we obtain

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

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

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

with the initial conditions $b(0) = \frac{1}{\sqrt{N}}$, $\frac{1}{2}(\dot{b}(0)\delta + \frac{2}{N}b(0)) = \frac{1}{\sqrt{N}}$ on the segment $[0, 2/\omega]$, where $\omega = 2/\delta\sqrt{N}$. The required solution of (7) with this accuracy is $b = \sin(\omega t) + \frac{1}{\sqrt{N}}\cos(\omega t)$, and the maximum of amplitude 1 is in the point $t_0 = \frac{\pi\sqrt{N}}{4}\delta - \frac{\delta}{2}$. Then $\left[\frac{t_0}{\delta}\right] = \left[\frac{\pi\sqrt{N}}{4}\right] \stackrel{+}{-} 1$ recurrent steps (4) are necessary and sufficient to achieve this value of b with this accuracy Thus we obtain that the accuracy $O(\frac{1}{\sqrt{N}})$ is reached in $\left[\frac{\pi\sqrt{N}}{4}\right]$ Grover's iterations. In the work [BBHT] its authors obtained an exact solution of (4) and thus proved that in fact a probability of error is even about $1/N$. The approximation of amplitude's evolution by systems of differential equations is more universal method. For example it makes possible to handle with the more involved case of parallel algorithm for RS which is the subject of next section.

5 Parallel algorithm for the repeated quantum search

5.1 Definitions and result

Let $u,\ x,\ y$ be variables with values from three different copies of $\mathcal{H}_0 = \mathrm{C}^N$, $a = a_1 \bigotimes a_2 \in \mathrm{C}^4$, where $a_1 = a_2 = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. 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 such values for x, y which represents unique solutions of equations $f_1 = 1,\ f_2 = 1$. We denote the corresponding states of quantum tape by the same letters.

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

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

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 $\mathcal{H}$: $\mathcal{R}_0 = I \bigotimes R_{0x} \bigotimes R_{0y} \bigotimes I;\ \mathcal{W} = I \bigotimes W_x \bigotimes W_y \bigotimes I;\ \ \mathcal{F} = P(F_1\ |_{u,a_1} \bigotimes F_2\ |_{x,y,a_2})P$, where the lower indices x, y point the corresponding area of application for Walsh-Hadamard transformations and rotations of the phase of 0, I denotes the identity.

The key unitary transformation of 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 applications of Z beginning with the initial state

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

$\left[\frac{\pi\sqrt{N}}{2\sqrt{2}}\right]$ times.

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

5.2 An advantage of 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 $\left[\frac{\pi\sqrt{N}}{2\sqrt{2}}\right]$ simultaneous queries to obtain a result, when the sequential application of simple quantum searches with f_1 and then with f_2 requires $\left[\frac{\pi\sqrt{N}}{2}\right]$ time steps to obtain a result with the same probability. Note that for a simple search constant factor $\frac{\pi\sqrt{N}}{4}$ can not be essentially improved (look at [BBHT]).

Suppose that every query is fulfilled by a physical device (oracle) of the peculiar type corresponding to a form of query. 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. With these oracles we can run them simultaneously in the parallel algorithm and obtain a result $\sqrt{2}$ times faster than by the 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 at first with two copies of f_1-oracle - one for each part, then, having e_1, with two copies of f_2-oracle. But this last way is expensive if every copy of oracle has a large cost, or impossible at all if every oracle is unique, say issues from a natural phenomenon. Just in this case of minimal possible set of oracles f_1, f_2 the application of parallel quantum algorithm for RS gives the increasing of performance in $\sqrt{2}$ times. This speedup can be also 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 remaining part of this work is devoted to the proof of Theorem and perspectives of this approach.

5.3 A primary analysis of parallel algorithm for RS

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

$$Z = -[(I \bigotimes W_x R_{0x} W_x \bigotimes I) P F_1 P][-(I \bigotimes (W_y R_{0y} W_y) \bigotimes I) F_2],$$

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

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

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

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

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, $N_1 = \sum\limits_{i=2}^{N} e_i$, $N_2 = \sum\limits_{i \neq 2} e_i$ (we omit ancillary qubits).

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

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

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 χ_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 (look at [Gr1]). Let λ_{av} be an average amplitude of corresponding quantum state.

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

$\lambda_{av} = \frac{(N-1)a_i - b_i}{N}$, $b'_i = 2\lambda_{av} + b_i$, $a'_i = 2\lambda_{av} - a_i$,

$$\begin{array}{ll} b'_i = \frac{2(N-1)a_i - 2b_i}{N} + b_i & = b_i(1 - \frac{2}{N}) + 2a_i(1 - \frac{1}{N}), \\ a'_i = \frac{2(N-1)a_i - 2b_i}{N} - a_i & = -b_i\frac{2}{N}) + a_i(1 - \frac{2}{N}). \end{array}$$

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

$\lambda_{av} = \frac{(N-1)\alpha_i + \beta_i}{N}$, $\alpha'_i = 2\lambda_{av} - \alpha_i$, $\beta'_i = 2\lambda_{av} - \beta_i$,

$$\begin{array}{ll} \alpha'_i = \frac{2(N-1)\alpha_i + 2b_i}{N} - a_i & = \alpha_i(1 - \frac{2}{N}) + 2\beta_i\frac{2}{N}), \\ \beta'_i = \frac{2(N-1)\alpha_i + 2\beta_i}{N} - \beta_i & = \alpha_i(1 - \frac{1}{N}) - \beta_i(1 - \frac{2}{N}). \end{array}$$

Step 2. $\chi'_i \xrightarrow{2} Z_1(\chi'_i) = \chi_{i+1}$.

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

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

$$\lambda_{av} = \frac{(N-1)\beta'_i - b'_i}{N}, \quad \begin{array}{ll} b_{i+1} & = 2\lambda_{av} + b'_i = b'_i(1 - \frac{2}{N}) + 2\beta'_i(1 - \frac{1}{N}), \\ \beta_{i+1} & = 2\lambda_{av} - \beta'_i = \beta'_i(1 - \frac{2}{N}) - b'_i\frac{2}{N}. \end{array}$$

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

$$\lambda_{av} = \frac{(N-1)\alpha'_i - a'_i}{N}, \quad \begin{array}{ll} a_{i+1} & = 2\lambda_{av} + a'_i = a'_i(1 - \frac{2}{N}) + 2\alpha'_i(1 - \frac{1}{N}), \\ \alpha_{i+1} & = 2\lambda_{av} - \alpha'_i = \alpha'_i(1 - \frac{2}{N}) - a'_i\frac{2}{N}. \end{array}$$

Hence, the recurrent formulas for amplitudes of sequential steps 1,2 acquire the following form:

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

Thus the matrix of one step of 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.

$$\begin{array}{ll} b_{i+1} - b_i & = 2a_i + 4\alpha_i - 2\beta_i + b_iO_1(\frac{1}{N}) + a_iO_2(\frac{1}{N}) + \alpha_iO_3(\frac{1}{N}) + \beta_iO_4(\frac{1}{N}); \\ a_{i+1} - a_i & = -\frac{2}{N}b_i + 2\alpha_i + a_iO_5(\frac{1}{N}) + b_iO_6(\frac{1}{N^2}) + \alpha_iO_7(\frac{1}{N}) + \beta_iO_8(\frac{1}{N}); \\ \alpha_{i+1} - \alpha_i & = -\frac{2}{N}a_i + \beta_iO_{13}(\frac{1}{N}) + a_iO_{14}(\frac{1}{N^2}) + b_iO_{15}(\frac{1}{N^2}) + \alpha_iO_{16}(\frac{1}{N}); \\ \beta_{i+1} - \beta_i & = -\frac{2}{N}b_i + 2\alpha_i - 2\beta_i + a_iO_9(\frac{1}{N}) + \alpha_iO_{10}(\frac{1}{N}) + \beta_iO_{11}(\frac{1}{N}) + b_iO_{12}(\frac{1}{N^2}). \end{array} \tag{11}$$

5.4 An approximation of amplitude's evolution by differential equations

Let $\{\bar{c}_i\}$ be a sequence of vectors from C^k : $\bar{c}_i = (c_i^1, c_i^2, \ldots, c_i^k)$, $c_i^j \in \mathrm{C}$, 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 $C(t) :\ \mathrm{R} \longrightarrow \mathrm{C}^k$ 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 (13),(14) is $C(t) = R(t)\bar{c}_0$, where the resolvent matrix $R(t) = \exp(mAt)$. The system (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 $C(\frac{i+1}{m}) = C(\frac{i}{m}) + \frac{1}{m}\dot{C}(\frac{i}{m}) + \frac{1}{2m^2}\ddot{C}(t_1)$, $\frac{i}{m} < t_1 < \frac{i+1}{m}$. Here the error ϵ_1 of the one step of the recursion (12) is the third summand $\frac{1}{2m^2}\ddot{C}(t_1) = \frac{1}{2}A^2C(t_1)$. Thus the error at the first step is $\frac{1}{2}A^2\exp(mA\theta_1)\bar{c}_0$, at the second step: $\frac{1}{2}A^2\exp(mA\theta_2)\bar{c}_1 + \exp(mA\frac{1}{m})\frac{1}{2}A^2\exp(mA\theta_1)\bar{c}0 = \frac{1}{2}A^2\exp(mA\theta_2)(\bar{c}_0 + A\bar{c}_0 + \frac{1}{2}A^2\exp(mA\theta_1)\bar{c}_0) + \exp(A)\frac{1}{2}A^2\exp(mA\theta_1)\bar{c}_0$, etc., at the i-th step the error will be $\epsilon_i \leq \frac{3}{2}\sum\limits_{j=1} i\exp(A\alpha_j)A^2\bar{c}_0$, where $0 < \alpha_j < 1$. Hence if $\|\bar{c}_0\| \leq h$, then the error after i-th step is $\epsilon_i = O(ih)$. Particularly, for the initial conditions $\|c_0\| = O(\frac{1}{N})$ a good approximation can be obtained if $i = o(N)$, and thus we can solve the Cauchy problem instead of (11) for $i = O(\sqrt{N})$ having error as small as required for sufficiently large N.

Define a new function $B(\tau)$ as follows $B(tm) = C(t)$. In terms of B the Cauchi problem (13), (14) acquires the form

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

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

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

where $\epsilon_i = aO_{0i}(\frac{1}{N^2}) + bO_{1i}(\frac{1}{N^2}) + \beta O_{2i}(\frac{1}{N}) + \alpha O_{3i}(\frac{1}{N})$, $i = 1, 2, 3, 4$, 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 $\bar{\delta} = \bar{B}(t) - \bar{c}_i = O(1/\sqrt{N})$, $N \longrightarrow \infty$ 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 RS

Now we shall take up the system of linear differential equations (16) with the initial conditions (17). Our goal is to solve it on a segment of the form $0 \le t \le O(\sqrt{N})$. The system (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

$$\tilde{A}_0 = \begin{pmatrix} 0 & 2 & 4 & 0 \\ -\frac{2}{N} & 0 & 2 & 0 \\ 0 & -\frac{2}{N} & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, E = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -\frac{2}{N} & 0 & 2 & -2 \end{pmatrix}, H = \begin{pmatrix} d_1 & d_1 & d_1 & -2+d_1 \\ d_2 & d_1 & d_1 & d_1 \\ d_2 & d_2 & d_1 & d_1 \\ d_2 & d_1 & d_1 & d_1 \end{pmatrix},$$

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 (16),(17) is the main and deposits of E and H are negligible. What is the main difficulty here? Consider the resolvent matrix for the Cauchy problem (16), (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 shall at first solve the Cauchy problem at hand neglecting deposits of E and H to the main matrix M. The legality of this approximation is shown in the Appendix.

Now take up 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 $\lambda^3 + \frac{8}{N}\lambda - \frac{16}{N^2} = 0$ and its nonzero solutions in within $O(\frac{1}{N})$ are $\lambda_{1,2} = \stackrel{+}{-} 2\sqrt{2}i/\sqrt{N}$. Then standard calculations give the approximation of solution as

$$\begin{aligned} b &= \tfrac{1}{2} - \tfrac{1}{2}\cos\tfrac{2\sqrt{2}t}{\sqrt{N}}, \\ a &= \tfrac{1}{\sqrt{2N}}\sin\tfrac{2\sqrt{2}t}{\sqrt{N}} + \tfrac{1}{N}\cos\tfrac{2\sqrt{2}t}{\sqrt{N}}, \\ \alpha &= \tfrac{1}{2N}\cos\tfrac{2t}{\sqrt{N}} + \tfrac{1}{2N} \end{aligned} \qquad (18)$$

in within $|O(\frac{1}{\sqrt{N}}), O(\frac{1}{N}), O(\frac{1}{N\sqrt{N}})\rangle$. The amplitude b from (18) peaks in the point $t_1 = \frac{\pi\sqrt{N}}{2\sqrt{2}}$ where $b(t_1) = 1$ in within $O(\frac{1}{\sqrt{N}})$. 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 $\left[\frac{\pi\sqrt{N}}{2\sqrt{2}}\right]$ steps of parallel algorithm which is $\sqrt{2}$ times as small as the time of sequential quantum search.

5.6 Completion of the proof

In the first version of this paper the deposit of E and H was estimated by the conventional procedure of approximation a solution of differential equation (look at the Appendix). This is the immediate but cumbersome way to prove that this deposit is vanishing. After the publication of the first version of this paper Farhi and Gutmann informed me how to simplify this construction by uniting by pairs the sequential transformations in parallel algorithm ([FG1]). In this section I combine this idea with the approach of the first version.

At first turn to the orthonormal basis $E_1 = |e_1e_2\rangle$, $E_2 = \frac{1}{\sqrt{N}}|e_1N_2\rangle$, $E_3 = \frac{1}{N}|N_1N_2\rangle$, $E_4 = \frac{1}{\sqrt{N}}|N_1e_2\rangle$. 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: $\chi_{2k} \longrightarrow \chi_{2k+1} \longrightarrow \chi_{2k+2}$ and denote by B the corresponding matrix: $B_0 = A_1^2$. It is sufficient to prove that $\|B_0^{[\frac{\pi\sqrt{N}}{4\sqrt{2}}]}|0,0,1,0\rangle - |1,0,0,0\rangle\| = O(\frac{1}{\sqrt{N}})$, because one application of A_1 can only increase the error by $O(\frac{1}{\sqrt{N}})$.

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:

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

in within $O(\frac{1}{N})$.

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 $\frac{4\sqrt{2}i}{\sqrt{N}}D$. It is easily seen that $D^{2k+1} = D$, $D^{2k} = D^2$ for $k = 1, 2, \ldots$. If the number of steps is $\left[\frac{\pi\sqrt{N}}{2\sqrt{2}}\right]$ then $t = \left[\frac{\pi\sqrt{N}}{4\sqrt{2}}\right]$. Here in within $O(\frac{1}{\sqrt{N}})$ we have

$$\begin{aligned} |b,a,\alpha\rangle &\approx \exp(\tfrac{4\sqrt{2}i}{\sqrt{N}}Dt) = \exp(\pi iD) = \cos(\pi D) + i\sin(\pi D) \\ &= 1 - \tfrac{(\pi D)^2}{2} + \tfrac{(\pi D)^4}{4!} - \ldots + i(\pi D - \tfrac{(\pi D)^3}{3!} + \ldots) \\ &= 1 - D^2(1 - \cos\pi) + iD\sin\pi = 1 - 2D^2 \end{aligned}$$

that is

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

The initial state is $|0,0,1\rangle$ in within $O(\frac{1}{\sqrt{N}})$. Application of this matrix to the initial state gives $|1,0,0\rangle$ with this accuracy. Theorem is proved.

6 Parallel implementation of iterated quantum search

6.1 Parallel quantum algorithm for IS

Now take up an IS problem for arbitrary k. Consider an evolution of amplitudes arising when k oracles work in parallel. Let $\chi_i = a_0^i|N_1, N_2, \ldots, N_k\rangle + a_1^i|e_1, N_2, \ldots, N_k\rangle + \ldots + a_k^i|e_1, e_2, \ldots, e_k\rangle + R_i$ (it generalizes (10)), where R_i contains only basic states of the form $|\ldots, N_p, \ldots, e_q, \ldots\rangle$. The natural generalization of the transformation (8) will be

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

where $\mathcal{W}^{(k)} = W_1 \bigotimes W_2 \bigotimes \ldots \bigotimes W_k \bigotimes I$, each W-H transformation W_i acts on x_i, $i = 1, 2$, $\ldots$, k, $\mathcal{R}_0^{(k)} = R_{01} \bigotimes \ldots \bigotimes R_{0k} \bigotimes I$, each rotation of 0's phase R_{0i} acts on x_i, $i = 1, 2, \ldots, k$, $\mathcal{F}^{(k)} = F_1 \bigotimes \ldots \bigotimes F_k \bigotimes I$, each F_i acts on x_i and inverses the sign of e_i, identities I act on ancilla.

Let a matrix A determines an evolution of quantum state in 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 $|N_1, N_2, \ldots, N_k\rangle, |e_1, N_2, \ldots, N_k\rangle, \ldots, |e_1, e_2, \ldots, e_k\rangle$. Then represent A_r as $A_r = A_0 + B$, where A_0 is Jacobi matrix of the form

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

This matrix has the following nonzero elements: 2 - above the main diagonal and $-\frac{2}{N}$ - 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. Generally speaking for $k > 2$ this assumption should be proved. An evolution of amplitude can be represented approximately as the solution of Cauchy problem

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

where $\bar{a}(i) \approx |a_1^i, \ldots, a_k^i\rangle$, i integer, we assume that $k \ll \sqrt{N}$.

Given eigenvalues of matrix (19), a general solution can be obtained by the standard procedure. These eigenvalues for Jacobi matrix is known (look at [Bel], Chapter 2, ex. 32), there are $\lambda_m = -\frac{4i}{\sqrt{N}} \cos m\theta, \quad m = 1, 2, \ldots, k, \theta = \frac{\pi}{k+2}$. We shall not solve (20) here.

6.2 Perspectives of parallel quantum algorithm for iterated search

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

Estimate the growth of target amplitude from above. Canceling all $-\frac{2}{N}$ we can only increase this growth. This results in a simple system of linear differential equations whose solution is $a_k(t) = N^{-k/2} + 2^k \int_0^{t^{\{k\}}} N^{-k/2} dt = N^{-k/2} + 2^k N^{-k/2} \frac{t^k}{k!}$. 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 the quarter of time required for the sequential search. Then it can not reach the vanishing error probability for any k, because for such $t = \frac{\pi\sqrt{N}k}{16}$ $a_k \approx \left(\frac{\pi}{8}\right)^k \frac{k^k}{k!} < 1$.

Nevertheless, parallel quantum algorithm has one advantage. Compare sequential and parallel quantum algorithms for IS in 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 $a_k(t) = \frac{a^k}{k!}$, $a = 2 - \epsilon$, where $\epsilon \longrightarrow 0$ $(N \longrightarrow \infty)$. Hence the resulting probability is $P_{par} = \left(\frac{a^k}{k!}\right)^2$.

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

6.3 Conclusion

To sum up, the parallel algorithm constructed above for repeated quantum search is $\sqrt{2}$ times as fast as sequential application of fast quantum search and it requires the same hardware. The advance is taken of 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 $k = o(\sqrt{N})$, $N \longrightarrow \infty$.

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

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

7 Acknowledgements

I am grateful to Victor Maslov for his support, to Oleg Khrustalev, Anatolyi Fomenko, Voislav Golo, Grigori Litvinov, Yuri Solomentsev and Kamil Valiev for the interesting discussions and help.

I am especially grateful to Lov Grover for his attention to my work and useful discussions and to Peter Hoyer for valuable comments to my previous works. I also thank Charles Bennett, David DiVincenzo, Lev Levitin, Richard Cleve, Richard Jozsa and others for the fruitful discussions at the conference NASA QCQC'98.

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

References

[AB] D. Aharonov, M. Ben-Or, Fault-Tolerant Quantum Computation With Constant Error, *Proc. Of the 29th Annual Symposium on Theory of Computing (STOC) 1997, lanl e-print quant-ph/9611025*

[BBCDMSSSW] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, H. Weinfurter, Elementary gates for quantum computation, *Phys. Rev. , 1995, A 52, 3457-3467*

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

[BBBGDL] D. Biron, O. Biham, E. Biham, M. Grassl, D. A. Lidar, Generalized Grover Search Algorithm for Arbitrary Initial Amplitude Distribution *lanl e-print quant-ph/9801066*

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

[Bel] R. Bellman, Introduction to matrix analysis, *MCGR-HILL Book Company, INC., NY, 1960*

[Be] P. Benioff, Quantum mechanical Hamiltonian models of Turing machines, *J. Stat. Phys. 22 (1982), 515-546*

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

[BBHT] M. Boyer, G. Brassard, P. Hoyer, A. Tapp, Tight bounds on quantum searching. In *Fourth Workshop on Physics and Computation* (ed. T. Toffoli & M. Biaford & J. Leao), 1996, pp. 36-43. New England Complex Systems Institute.

[BM] V. Belavkin, V. Maslov, Design of the optimal dynamics analysis: mathematical aspects of sound and visual pattern recognition, *In: Mathematical aspects of computer, V.P. Maslov, V.P. Belavkin eds., Mir, Moscow, 1988.*

[BO] V. P. Belavkin, M. Ohya, Quantum entanglements and entangled mutual entropy ,*lanl e-print quant-ph/9812082*

[BV] E. Bernstein, U. Vazirani, Quantum complexity theory, (1993) *SIAM Journal of Computation 1997, 26(5), 1411-1473*

[CGW] N. J. Cerf, L. K. Grover, C. P. Williams, Nested quantum search and NP-complete problems, *lanl e-print quant-ph/9806078*

[CLSZ] I. L. Chuang, R. Laflamme, P. W. Shor, W. H. Zurek, Quantum computers, factoring, and decoherence, *Science, 1995, v. 270, 1633-1635*

[vD] W. van Dam, Quantum oracle interrogation: getting all information for almost half the price *lanl e-print quant-ph/9805006*

[De] D. Deutsch, Quantum theory, the Church-Turing principle and the universal quantum computer, *Proc. R. Soc, 1985, A 400, 97-117*

[DJ] D. Deutsch, R. Jozsa, Rapid solution of problems by quantum computation, *In Proc. R. Soc. Lond., 1992, A (449) 553-558*

[DiV] D. P. DiVincenzo, Two-bit gates are universal for quantum computation, *Phys. Rev. A 51, 1015-1022, 1995*

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

[FGGS] E. Farhi, J. Goldstone, S. Gutmann, M. Sipser, A limit on the Speed of Quantum Computation in Determining Parity, *lanl e-print quant-ph/9802045*

[FG] E. Farhi, S. Gutmann, Quantum mechanical square root speedup in a structured search problem, *lanl e-print quant-ph/9711035*

[FG1] E. Farhi, S. Gutmann, Private communication

[Fe] R. P. Feynman, Simulation physics with computers, *Int. J. Phys. 21 (1982), 467-488*

[Gr1] L. K. Grover, A fast quantum mechanical algorithm for database search. *Proceedings, STOC 1996, 212-219. Philadelphia PA USA.*

[Gr2] L. K. Grover, A fast quantum mechanical algorithm for estimating the median, *lanl e-print quant-ph/9607024*

[H] T. Hogg, A Framework for Structured Quantum Search *lanl e-print quant-ph/9701013*

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

[JMH] J. A. Jones, M. Mosca, R. H. Hansenabs, Implementation of a Quantum Search Algorithm on a Nuclear Magnetic Resonance Quantum Computer, *lanl e-print quant-ph/9805069*

[Jo] R. Jozsa, Searching in Grover's algorithm *lanl e-print quant-ph/9901021*

[Ki1] A. Yu. Kitaev, Quantum measurements and the Abelian Stabilizer Problem *lanl e-print quant-ph/9511026*

[Ki2] A. Yu. Kitaev, Fault-tolerant quantum computation by anyones, *lanl e-print quant/ph/9707021*

[LMS] G.L. Litvinov, V.P. Maslov, G.B. Shpiz, Nondigital Implementation of Real Numbers' Arithmetic by Means of Quantum Computer Media *lanl e-print quant-ph/9904025*

[Ll1] S. Lloyd, A potentially Realizable Quantum Computer, *Science, 1993, v. 261, 1569-1571*

[Ll2] S. Lloyd, Almost any quantum logic gate is universal, *Phys. Rev. Lett., 1995, 75, 346-349*

[ML] N. Margolus, L. B. Levitin, The maximum speed of dynamical evolution *Physica D120 (1998) 188-195*

[Oz1] Y. Ozhigov, Quantum computers speed up classical with probability zero *Chaos, Solitons and Fractals, 1147, (1999), lanl e-print quant-ph/9803064*

[Oz2] Y. Ozhigov, Lower bounds of quantum search for extreme point *To be published in Proc. Royal. Soc. (Math. Phys. Engineering Science), 1999, lanl e-print quant-ph/9806001*

[Pe] R. Penrose, Shadows of the Mind, New York: Oxford University Press, 1994

[Pr] J. Preskill, Fault tolerant quantum computation, *lanl e-print quant-ph/9712048*

[Ro] D.A. Ross, A Modification of Grover's Algorithm as a Fast Database Search, *lanl e-print quant-ph/9807078*

[Sh] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Comp. 1997, 26, No. 5, 1484-1509*

[Si] D. Simon, On the power of quantum computation, *SIAM J. Comp., 1997, 26, 5, 1474-1483*

[St] A. M. Steane, Space, time, parallelism and noise requirements for reliable quantum computing, *Fortsch. Phys. 1998, 46, 443-458*

[TS] B. M. Terhal, J. A. Smolin, Superfast quantum algorithms for coin weighing and binary search problems *lanl e-print quant-ph/9705041*

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

[Wo] S. Wolfram, Cellular Automata and Complexity: Collected Papers, *Addison-Wesley, 1994*

[Ya] A. Yao, Quantum Circuit Complexity, *Proceedings 34th Annual Symposium on Foundations of Computer Science (FOCS) 1993, 352-361*

[Za] C. Zalka, Grover's quantum searching algorithm is optimal, *lanl e-print quant-ph/9711070*

A Appendix. An iterated approximation for solutions of differential equations

A.1 The method of simple iterations

Here we present the first version of the proof. Let K, L, K_0 be linear operators of the form $\mathrm{C}^m \longrightarrow \mathrm{C}^m$, $K = K_0 + L$, $\sigma(t) :\ \mathrm{R} \longrightarrow \mathrm{C}^m$ be a vector function with scalar argument.

Consider the following Cauchy problem for a system of linear differential equations with unknown vector function $x(t)$

$$\dot{x}(t) = Kx(t) + \sigma(t), \quad x(0) = x_0 \in \mathrm{C}^m, \tag{21}$$

where K_0 is regarded as the main summand and L determines a perturbation such that a solution $x_0(t)$ of the problem

$$\dot{x} = K_0 x, \quad x(0) = x_0$$

is known. Then a solution of (21) can be obtained as a limit of the sequence $x_0, x_1, \ldots$ of vector functions depending on t, which are determined by the following recursion

$$x_{i+1} = x_0 + \int_0^t (Kx_i + \sigma)dt. \tag{22}$$

Define the i-th difference between the approximations as $\delta_i = x_i - x_{i-1}, \;\; i = 1, 2, \ldots$. Then $\delta_1 = \int_0^t Lx_0 dt$, $\delta_{i+1} = \int_0^t K\delta_i dt$. Thus we conclude that

$$\delta_i = K^i \int_0^t \int_0^{t_1} \int_0^{t_2} \ldots \int_0^{t_{i-2}} \delta_1(t_{i-2}) dt_{i-2} \ldots dt_2 dt_1 dt. \tag{23}$$

A.2 The method of complex iterations

The simple method from the previous section can not be immediately applied to our situation because of inconvenient form of our main matrix M. We apply the following idea. In each step of approximation consider separately an approximations on the group of b, a, α and then on β. Here the main matrix $A = A_0 + B$ of the system for b, a, α can be represented as a result of small perturbation B of almost nilpotent matrix which allows to estimate a deposit of perturbation.

These matrices with the notations of (16) have the form

$$A_0 = \begin{pmatrix} 0 & 2 & 4 \\ -\frac{2}{N} & 0 & 2 \\ 0 & -\frac{2}{N} & 0 \end{pmatrix}, \; B = \begin{pmatrix} O_1(\frac{1}{N}) + O_{11}(\frac{1}{N^2}) & O_0(\frac{1}{N}) + O_{01}(\frac{1}{N^2}) & O_{31}(\frac{1}{N}) \\ O_{12}(\frac{1}{N^2}) & O_2(\frac{1}{N}) + O_{02}(\frac{1}{N^2}) & O_{32}(\frac{1}{N}) \\ O_{13}(\frac{1}{N^2}) & O_{03}(\frac{1}{N^2}) & O_{33}(\frac{1}{N}) \end{pmatrix}. \tag{24}$$

Consider the vectors

$$\begin{aligned} |d_\beta\rangle &= |-\tfrac{2}{N} + O14(\tfrac{1}{N^2}), O_4(\tfrac{1}{N}) + O_{04}(\tfrac{1}{N^2}), 2 + O_{34}(\tfrac{1}{N}), -2 + O_{24}(\tfrac{1}{N})\rangle, \\ |\gamma\rangle &= |-2 + O_{21}(\tfrac{1}{N}), O_{22}(\tfrac{1}{N}), O_{23}(\tfrac{1}{N})\rangle. \end{aligned}$$

Preparing to define by induction a sequence of approximations to the solution of (16), (17) we introduce the notations

$$|\bar{c}_i\rangle = |b_i, a_i, \alpha_i\rangle, \;\; |\tilde{c}_i\rangle = |\bar{c}_i, \beta_i\rangle.$$

Then the Cauchy problem (16), (17) is equal to the system

$$\begin{aligned} |\dot{\bar{c}}\rangle &= A|\bar{c}\rangle + \beta|\gamma\rangle, \\ \dot{\beta} &= \langle d_\beta|\tilde{c}\rangle \end{aligned} \tag{25}$$

with the initial condition (17).

Define the sequence of vector functions $|\tilde{c}_i\rangle$ approximating the solution of (25), (17) by the following induction on i.

Basis. $|\tilde{c}_0\rangle = |\bar{c}_0, \beta_0\rangle$, where $|\bar{c}_0\rangle = |b_0, a_0, \alpha_0\rangle$ is a solution of Cauchy problem $|\dot{\bar{c}}\rangle = A_0|\bar{c}\rangle$, $\bar{c}(0) = |\frac{1}{N}, \frac{1}{N}, \frac{1}{N}\rangle$ given by the approximations (18), β_0 is a solution of equation $\dot{\beta}_0 = \langle d_\beta|\tilde{c}_0\rangle$ with the initial condition $\beta_0(0) = \frac{1}{N}$.

Step. $\bar{c}_{i+1}$ is a solution of Cauchy problem

$$\dot{\bar{c}}_{i+1} = A\bar{c}_{i+1} + \beta_i|\gamma_\beta\rangle, \quad \bar{c}_{i+1}(0) = |\frac{1}{N}, \frac{1}{N}, \frac{1}{N}\rangle;$$

β_{i+1} is the solution of $\dot{\beta}_{i+1} = \langle d_\beta|\tilde{c}_{i+1}\rangle,\ \beta_{i+1}(0) = \frac{1}{N}$ with the given vector function $\bar{c}_{i+1}$ obtained above.

Put $\delta_i = \tilde{c}_i - \tilde{c}_{i-1} = |\delta_i^b, \delta_i^a, \delta_i^\alpha, \delta_i^\beta\rangle,\ i = 1, 2, \ldots$. The main fact concerning these approximations is the following

Lemma 1 *For* $0 \le t \le \frac{\pi\sqrt{N}}{2\sqrt{2}}$

$$|\delta_i^b| \le \frac{10t^{i-1}}{N^{\frac{i}{2}}(i-1)!};\ |\delta^\beta|, |\delta_i^a| \le \frac{10t^{i-1}}{N^{\frac{i+1}{2}}(i-1)!};\ |\delta_i^\alpha| \le \frac{10t^{i-1}}{N^{\frac{i}{2}+1}(i-1)!}.$$

This Lemma means that the vectors δ_i form summable row with a module of sum less than $\frac{20}{\sqrt{N}}$ and thus we obtain Theorem. To prove the key Lemma 1 we need to clarify a main property of matrix A.

A.3 A nilpotency of the main matrix

Denote by ϵ_i any number whose absolute value is less or equal to $(10/N)^j$. The main property of the matrix A is represented by the following Lemma.

Lemma 2 *For every* $j = 0, 1, \ldots$

$$A^{2j} = \begin{pmatrix} \epsilon_j & \epsilon_j & \epsilon_{j-1} \\ \epsilon_{j+1} & \epsilon_j & \epsilon_j \\ \epsilon_{j+1} & \epsilon_{j+1} & \epsilon_j \end{pmatrix},\ A^{2j+1} = \begin{pmatrix} \epsilon_{j+1} & \epsilon_j & \epsilon_j \\ \epsilon_{j+1} & \epsilon_{j+1} & \epsilon_j \\ \epsilon_{j+1} & \epsilon_{j+1} & \epsilon_{j+1} \end{pmatrix}.$$

Proof
Induction on j.

A.4 Completion of the proof

Proof of Lemma 1

Induction on i.
Basis.
Consider the passage $\tilde{c}_0 \longrightarrow \tilde{c}_1$, consisting of two parts, we regard them as cases a) and b).
a). $\bar{c}_0 \longrightarrow \bar{c}_1$. This passage is the sequence $\bar{c}_0 = \bar{c}_0^0 \longrightarrow \bar{c}_0^1 \longrightarrow \ldots \longrightarrow \bar{c}_0^t \longrightarrow \ldots \longrightarrow \bar{c}_1$, where $\bar{c}_0^{j+1} = \bar{c}(0) + \int\limits_0^t (A\bar{c}_0^j + \beta_0\bar{\gamma})dt$ (γ in ordinary notations). The j-th difference will be $\Delta_j = \bar{c}_0^j - \bar{c}_0^{j-1} = \int\limits_0^t A\Delta_{j-1}dt$, $\Delta_1 = \int\limits_0^t (B\bar{c}_0^0 + \beta_0\bar{\gamma})dt$.

Assume the following notation for an arbitrary function $F(t)$:
$\int\limits_0^{t\{k\}} F(t)dt = \int\limits_0^t \int\limits_0^t \ldots \int\limits_0^t F(t)dt\ \ldots dt\ dt$. We will write $\bar{a} \preceq \bar{b}$ iff an absolute value of each

component of $\bar{a}$ does not exceed the absolute value of the corresponding component of $\bar{b}$. Then there exists such numbers $l_s,\ s = 1,2,3$ that for every $k = 1,2,\ldots$ we have $\int\limits_0^{t\{k\}} \Delta_1 \preceq \frac{t^k}{k!}|\frac{l_1}{\sqrt{N}}, \frac{l_2}{N}, \frac{l_3}{N^{3/2}}\rangle$.

Now applying sequentially the equality (23) and Lemma 1, we obtain:

$$\Delta_j = A^{j-1}\int\limits_0^{t\{j-1\}} \Delta_1 dt \preceq \left(\frac{10t}{\sqrt{N}}\right)\frac{1}{(j-1)!}\left|\frac{1}{\sqrt{N}}, \frac{1}{N}, \frac{1}{N^{3/2}}\right\rangle.$$

Hence $\bar{c}_1 - \bar{c}_0 = \Delta_1 + \Delta_2 + \ldots \preceq \exp(\frac{10t}{\sqrt{N}})|\frac{1}{\sqrt{N}}, \frac{1}{N}, \frac{1}{N^{3/2}}\rangle$.

b). $\bar{c}_1 \longrightarrow \tilde{c}_1$.

Introduce the following scalar function $\Phi(b,a,\alpha) = \langle d_\beta|b,a,\alpha\rangle$. The difference for it is $\Delta\Phi_i = \Phi_i - \Phi_{i-1}$.

The first β-difference $\delta_1^\beta = \beta_1 - \beta_0$ is the difference between the solutions of equations $\dot{\beta}_0 = \Phi(b_0,a_0,\alpha_0) - 2\beta_0$ and $\dot{\beta}_1 = \Phi(b_1,a_1,\alpha_1) - 2\beta_1$.

Lemma 3 *For each* $i = 1,2,\ldots$

$$\delta_i^\beta = \exp(-2t)\int\limits_0^t \exp(2t)\Delta\Phi_i dt.$$

Proof

δ_i^β is the solution of the Cauchy problem $\dot{\delta}_i^\beta + 2\delta_i^\beta = \Delta\Phi_i,\ \ \delta_i^\beta(0) = 0$, which can be obtained immediately. Lemma 3 is proved.

Applying Lemma 3 we obtain $|\delta_1^\beta| \leq \frac{t}{2N\sqrt{N}}$. Hence for the first step if $t \leq \sqrt{N}$ then $\delta_1 \preceq |\frac{1}{\sqrt{N}}, \frac{10}{N}, \frac{10}{N^{3/2}}, \frac{10}{N^{3/2}}\rangle$. Basis is complete.

Step.

The passage $\tilde{c}_{i-1} \longrightarrow \tilde{c}_i$ consists of two sequential steps:

1) the passage from $\bar{c}_{i-1}$ to $\bar{c}_i$,

2) the passage from $\beta i - 1$ to β_i.

Take up **Step 1**. Applying the method of approximations (22) to the problem (25), we regard $\bar{c}_i$ as the limit of the sequence $\bar{c}_i^0, \bar{c}_i^1, \ldots$, where $\bar{c}_i^0 = \bar{c}_{i-1}$,

$$\bar{c}_i^j = \bar{c}_i^0 + \int\limits_0^t (A\bar{c}_i^{j-1} + \beta_{i-1}\bar{\gamma})dt.$$

The accuracy of j-th approximation relative to the previous one is determined by the difference $\Delta^j = \bar{c}_i^j - \bar{c}_i^{j-1} = |\Delta_j^b, \Delta_j^a, \Delta_j^\alpha\rangle$, given by

$$\begin{aligned} \bar{\Delta}^j &= A^{j-1}\int\limits_0^{t\{j-1\}} \bar{\Delta}^1(t)dt, \quad j > 1, \\ \bar{\Delta}^1 &= \int\limits_0^1 \delta_{i-1}^\beta \bar{\gamma} dt. \end{aligned} \tag{26}$$

Taking into account inductive hypothesis we obtain for the first difference $\bar{\Delta}_i^1 \preceq \int\limits_0^t \frac{t^{i-1}}{(i-1)!N^{i/2}} |\frac{10}{N}, \frac{10}{N^2}, \frac{10}{N^2}\rangle dt$. For the next differences we have $\int\limits_0^{t\{j-1\}} \bar{\Delta}_i^1 dt \preceq \frac{t^{i-1}}{(i-1)!N^{i/2}} \left|\frac{3t^{j-1}}{(j-1)!N}, \frac{10t^{j-1}}{(j-1)!N^2}, \frac{10t^{j-1}}{(j-1)!N^2}\right\rangle$.

Calculating the differences accordingly to the formula (26) and applying Lemma 2 we obtain

$$\begin{array}{rcl} \bar{\Delta}_i^{2j} & = & \frac{t^{i-1}}{(i-1)!N^{i/2}} \left|\frac{30t^{2j-1}\epsilon_j}{(2j-1)!N}, \frac{10t^{2j-1}\epsilon_{j-1}}{(2j-1)!N^2}, \frac{10t^{2j-1}\epsilon_{j-1}}{(2j-1)!N^2}\right\rangle, \\ \bar{\Delta}_i^{2j+1} & = & \frac{t^{i-1}}{(i-1)!N^{i/2}} \left|\frac{30t^{2j}10^j}{(2j+1)!N^{j+1}}, \frac{30t^{2j}10^j}{(2j+1)!N^{j+2}}, \frac{30t^{2j}10^j}{(2j+1)!N^{j+2}}\right\rangle. \end{array}$$

Summing over all j gives the inequalities for $\delta^b, \delta^a, \delta^\alpha$ from the statement of Lemma 1. As for δ^β, we estimate it as in the basis of induction, Then Lemma 3 gives $|\delta_i^\beta| \leq \frac{t^i}{NN^{i/2}i!}$. Step of induction is complete. Lemma 1 is proved. Theorem is proved.