Quantum Information III

Edited by

T. Hida
K. Saitô

World Scientific

Proceedings of the Third International Conference

Quantum Information III

Meijo University, Japan 7–10 March 2000

Edited by

T. Hida & K. Saitô

Meijo University
Japan

World Scientific
Singapore • New Jersey • London • Hong Kong

Published by

World Scientific Publishing Co. Pte. Ltd.

P O Box 128, Farrer Road, Singapore 912805

USA office: Suite 1B, 1060 Main Street, River Edge, NJ 07661

UK office: 57 Shelton Street, Covent Garden, London WC2H 9HE

Library of Congress Cataloging-in-Publication Data

International Conference on Quantum Information (3rd ; 2000 ; Meijo University)
Quantum information III : proceedings of the third international conference, Meijo University, Japan, 7–10 March 2000 / edited by T. Hida & K. Saitô.
p. cm.
ISBN 9810245270
1. Quantum computers--Congresses. I. Title: Quantum information 3. II. Title: Quantum information three. III. Hida, Takeyuki, 1927- . IV. Saitô, K. (Kimiaki), 1959- V. Title.

QA76.889 .I535 2000
004.1--dc21 2001026181

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

Printed in Singapore by World Scientific Printers

Quantum Information III

Preface

The Third International Conference on Quantum Information was held at Meijo University in Nagoya, Japan, March 7–10, 2000.

This volume contains the papers of invited lectures and contributed talks at this conference. The editors are pleased to accept all the papers for publication in this volume at the suggestion of the referees so that this volume is most valuable.

The following topics were discussed at the conference:

1) Complexity in Quantum System
2) Quantum Stochastic Processes, Quantum Stochastic Analysis
3) Quantum Computation
4) White Noise Theory
5) Infinite Dimensional Stochastic Analysis
6) Variational Calculus
7) Random Fields
8) Time Reversal Symmetry of Fluctuation

This conference was supported by the Research Project "Quantum Information Theoretical Approach to Life Science" for the Academic Frontier in Science promoted by the Ministry of Education in Japan and was also supported by Meijo University.

We would like to express our sincere thanks to the Faculty of Science and Technology of Meijo University for their assistance during the conference.

December 30, 2000
Takeyuki Hida
Kimiaki Saitô
Meijo University

Quantum Information III

Contents

Quantum Information III, pp. 1–20
Eds. T. Hida and K. Saitô

A Generalization of Grover's Algorithm

LUIGI ACCARDI
RUBEN SABBADINI

Centro Vito Volterra
Università degli Studi di Roma "Tor Vergata"
Via Orazio Raimondo, 00173 Roma, Italia

ABSTRACT

We investigate the necessary and sufficient conditions in order that a unitary operator can amplify a pre-assigned component relative to a particular basis of a generic vector at the expence of the other components. This leads to a general method which allows, given a vector and one of its components we want to amplify, to choose the optimal unitary operator which realizes that goal. Grover's quantum algorithm is shown to be a particular case of our general method.

However the general structure of the unitary we find is remarkably similar to that of Grover's one: a sign flip of one component combined with a reflection with respect to a vector. In Grover's case this vector is fixed; in our case it depends on a parameter and this allows optimization.

1 Unitary operators which increase the probability of the $|0>$ component of a pre-assigned vector

Let $|i>$ $(i = 0, \ldots, N-1)$ be an orthonormal basis of $\mathbf{R}^N$. The mathematical core of Grover's algorithm is the construction of a unitary operator $\mathbf{U}$ which increases the probability of one of the components of a given unit vector, in the given basis, at the expence of the remaining ones. The necessity of such an amplification of probabilities arises in several problems of quantum computation. For example in the Ohya-Masuda [4] quantum SAT algorithm such a problem arises. In a recent interesting paper Ohya and Volovich have proposed a new method of amplification, based on non linear chaotic dynamics [14]. In the present paper we begin to study the following problem: is it possible to extend Grover's algorithm so that it becomes applicable to a more general class of initial vectors, for example those wich arise in the Ohya-Masuda algorithm? A preliminary step to solve this problem is to determine the most general unitary operator which performs the same task of Grover's operator. This is done in Theorem (1.1) below. The result is rather surprising: we find that, up to the choice of four ± 1 (phases), there exists exactly one class of such unitary operators, labeled by an arbitrary parameter in the interval $[0, 1]$. Moreover these unitaries can be written in a form similar to Grover's one, i.e. a reflection with respect to a given unit vector possibly preceeded by a sign flip of one component combined with, where the unit vector in question depends on this parameter in $[0, 1]$. The free parameter in our problem allows to solve a new problem, which could not be formulated within the framework of Grover's explicit construction, namely the *optimization problem* with respect to the given parameter. We prove that, even in the case of Grover's original algorithm, this additional freedom allows to speed up considerably the amplification procedure. In a forthcoming paper [15] we plan to apply the present method to the Ohya-Masuda algorithm. Since an operator U is unitary if and only if it leaves unaltered the scalar products of vectors with real components in a given basis, we shall restrict our attention to unitary operators with real coefficients in a given basis (as the Grover's ones). This restrictes the problem to $\mathbf{R}^N$.

THEOREM 1 Given the linear functionals:

$$\eta : a = (a_i) \in \mathbf{R}^N \mapsto \eta(a) = \sum_{i=0}^{N-1} \eta_i a_i \tag{1}$$

$$c : a = (a_i) \in \mathbf{R}^N \mapsto c(a) = \sum_{i=0}^{N-1} \gamma_i a_i \tag{2}$$

with γ_i and η_i real and ε_1, $\varepsilon_2 \in \{\pm 1\}$, necessary and sufficient condition for the operator $\mathbf{U}$, defined by:

$$\mathbf{U} \sum a_i|i> = \varepsilon_1(a_0 + \eta(a))|0> + \varepsilon_2 \sum_{i\neq 0} (a_i + c(a))\,|i> \tag{3}$$

to be unitary is that there exist a real number β_0 such that:

$$|\beta_0| \leq 1 \tag{4}$$

$$\gamma_0 = \varepsilon_5 \frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} \tag{5}$$

$$\gamma_i = -\frac{1+\varepsilon_3\beta_0}{N-1} \qquad i \neq 0 \tag{6}$$

$$\eta_0 = -1 + \varepsilon_4\beta_0 \tag{7}$$

$$\eta_i = \varepsilon_3\gamma_0 \qquad i \neq 0 \tag{8}$$

where ε_3, ε_4, ε_5 are arbitrarily chosen in the set $\{\pm 1\}$.

PROOF In finite dimension unitarity is equivalent to isometry. Therefore $\mathbf{U}$ is unitary if and only if, for every $|a> = \sum_{i=0}^{N-1} a_i|i>$ the following isometricy condition is satisfied:

$$\sum a_i^2 = (a_0+\eta)^2 + \sum_{i\neq 0}(a_i+c)^2 = a_0^2 + \eta^2 + 2a_0\eta + \sum_{i\neq 0} a_i^2 + (N-1)c^2 + 2c\sum_{i\neq 0} a_i$$

where we write η, c for $\eta(a)$, $c(a)$. This condition can be written in the form:

$$\eta^2 + 2a_0\eta + (N-1)c^2 + 2c\sum_{i\neq 0} a_i = 0 \tag{9}$$

With the notation:

$$\gamma(a) = \gamma := (N-1)c^2 + 2c\sum_{i\neq 0} a_i \tag{10}$$

Equation (9) is equivalent to:

$$\eta^2 + 2a_0\eta + \gamma = 0 \tag{11}$$

and its possible solutions are:

$$\eta(a) = \eta = -a_0 + \varepsilon_4 \sqrt{a_0^2 - \gamma(a)} \tag{12}$$

Given (12) the funtional $\eta(a)$ will be linear if and only if $\forall a_0, \ldots, a_N$:

$$a_0^2 - \gamma(a) = \left(\sum_j \beta_j a_j \right)^2 \tag{13}$$

for some real numbers β_j indipendent of a.

Since the functional $c(a)$ is linear and given by (2), because of (12) and (13), condition (9) becomes:

$$-a_0^2 + (N-1) \left(\sum_j \gamma_j a_j \right)^2 + \left(\sum_j \beta_j a_j \right)^2 + 2 \sum_j \gamma_j a_j \sum_{i \neq 0} a_i =$$

$$-a_0^2 + 2 \sum_j \gamma_j a_j \sum_{i \neq 0} a_i + \sum_{i,j} \left[(N-1) \gamma_i \gamma_j + \beta_i \beta_j \right] a_i a_j = 0$$

or equivalently:

$$a_0^2 \left[(N-1)\gamma_0^2 + \beta_0^2 - 1 \right] + \sum_{i,j \neq 0} \left[2\gamma_j + (N-1)\gamma_i \gamma_j + \beta_i \beta_j \right] a_i a_j +$$

$$+2 \sum_{i \neq 0} \left[\gamma_0 + (N-1) \gamma_0 \gamma_i + \beta_0 \beta_i \right] a_0 a_i = 0 \tag{14}$$

The identity (14) holds $\forall a_0, \ldots, a_N$, if and only if:

$$(N-1)\gamma_0^2 + \beta_0^2 - 1 = 0 \tag{15}$$

$$2\gamma_j + (N-1)\gamma_i \gamma_j + \beta_i \beta_j = 0 \quad \forall i, j \neq 0 \quad i \neq j \tag{16}$$

$$2\gamma_i + (N-1)\gamma_i^2 + \beta_i^2 = 0 \quad \forall i \neq 0 \tag{17}$$

$$\gamma_0 + (N-1)\gamma_0 \gamma_i + \beta_0 \beta_i = 0 \quad \forall i \neq 0 \tag{18}$$

Equation (15) and the reality condition on η imply that (4) and (5) hold. From (18) we deduce that, for $i \neq 0$:

$$\gamma_i = -\frac{\gamma_0 + \beta_0 \beta_i}{\gamma_0 (N-1)} \tag{19}$$

and, replacing this into (17), we find:

$$-\frac{2(\gamma_0+\beta_0\beta_i)}{\gamma_0(N-1)}+\frac{(\gamma_0+\beta_0\beta_i)^2}{\gamma_0^2(N-1)}+\beta_i^2=0$$

or:

$$\left[(N-1)\,\gamma_0^2+\beta_0^2\right]\beta_i^2=\gamma_0^2$$

which, because of (15), is equivalent to:

$$\beta_i=\varepsilon_3\gamma_0=\varepsilon_3\varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} \tag{20}$$

with $\varepsilon_3=\pm 1$. Replacing (20) into (19) we arrive to (6)

Replacing (24),..., (27) into (1) and (2), we conclude that a necessary condition for the linearity of **U** is that η and c must have the form:

$$\eta(a)=(-1+\varepsilon_4\beta_0)a_0+\varepsilon_4\varepsilon_3\gamma_0\sum_{k\neq 0}a_k=(-1+\varepsilon_4\beta_0)a_0+\varepsilon_4\varepsilon_3\varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}}\sum_{k\neq 0}a_k \tag{21}$$

$$c(a)=\gamma_0a_0-\frac{1+\varepsilon_3\beta_0}{N-1}\sum_{k\neq 0}a_k=\varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}}a_0-\frac{1+\varepsilon_3\beta_0}{N-1}\sum_{k\neq 0}a_k \tag{22}$$

Conversely, if conditions (4), ..., (8) are satisfied, then also (14), which is equivalent to (9), is satisfied and therefore **U** is isometric, hence unitary. This can also be seen by a direct computation (see appendix A).

REMARK Because of (4) there exists a $\theta\in[0,2\pi)$ such that β_0 has the form:

$$\beta_0=\varepsilon_3 cos\ \theta \tag{23}$$

and therefore, from (5):

$$\sqrt{N-1}\gamma_0=\varepsilon_5\sqrt{1-\beta_0^2}=sin\ \theta \tag{24}$$

i.e. the parameters β_0 and γ_0 live onto an ellipse in the $(\beta_0,\ \gamma_0)$-plane. With these notations one has:

$$\eta(a)=(-1+\varepsilon_3\varepsilon_4 cos\ \theta)\,a_0+\varepsilon_3\varepsilon_4\frac{sin\ \theta}{\sqrt{N-1}}\sum_{k\neq 0}a_k \tag{25}$$

$$c(a) = \frac{sin\ \theta}{\sqrt{N-1}} a_0 - \frac{1 + cos\ \theta}{N-1} \sum_{k \neq 0} a_k \tag{26}$$

REMARK The case $\gamma = 0$ leads to $\eta = 0$ or $\eta = -2a_0$; in both cases we have:

$$\mathbf{U} \sum a_i |i> = \pm \varepsilon_1 a_0 \ |0> + \varepsilon_2 \sum_{i \neq 0} (a_i + c) \ |i>$$

The operators $\mathbf{U}(\gamma \equiv 0(a))$ are in this class, however they play a significant role in Grover's algorithm because they may be used to change the sign of a component leaving the others u inaltered (*flip*).

If we are interested in unitaries which modify the component a_0 of a, we must look for solutions with $\gamma \neq 0$.

COROLLARY 2 If in (21) and (22) we choose:

$$\varepsilon_1 \varepsilon_4 = \varepsilon_3 = \varepsilon_5 = 1$$

$$\varepsilon_2 = -1$$

$$\beta_0 = \frac{N-2}{N}$$

$$\gamma_0 = \frac{2}{N}$$

then the corresponding operator $\mathbf{U}$ is Grover's unitary (see section 4).

PROOF It is known that Grover's unitary is characterized by (see section 4):

$$a_0 \mapsto \frac{N-2}{N} a_0 + \frac{2}{N} \sum_{k \neq 0} a_k =: \varepsilon_1 [a_0 + \eta(a)] \tag{27}$$

$$a_i \mapsto -a_i + \frac{2}{N} \left(-a_0 + \sum_{k \neq 0} a_k \right) =: \varepsilon_2 [a_i + c(a)] \tag{28}$$

On the other hand, from equations (25) and (26) we have:

$$\varepsilon_1 [a_0 + \eta(a)] = \varepsilon_1 \varepsilon_4 \left(\beta_0 a_0 + \varepsilon_3 \gamma_0 \sum_{k \neq 0} a_k \right) \tag{29}$$

$$\varepsilon_2\left[a_i + c(a)\right] = \varepsilon_2\left(a_i + \gamma_0 a_0 - \frac{1+\varepsilon_3\beta_0}{N-1}\sum_{k\neq 0} a_k\right) \tag{30}$$

with γ_0 given by (5). Comparing this with (27) and (28) we see that the condition for equality is:

$$\varepsilon_1\varepsilon_4\beta_0 = \frac{N-2}{N}$$

Now let us choose $\varepsilon_1\varepsilon_4 = 1$ and $\beta_0 = \frac{N-2}{N}$ then:

$$\gamma_0 = \varepsilon_5\sqrt{\frac{1-\frac{(N-2)^2}{N^2}}{N-1}} = \varepsilon_5\frac{2}{N}$$

that leads to $\varepsilon_5 = 1$. Therefore, if $\varepsilon_2 = -1$, the coefficient of the third term in (30) becomes:

$$-\varepsilon_2\frac{1+\varepsilon_3\beta_0}{N-1} = \frac{1+\varepsilon_3\frac{N-2}{N}}{N-1} = \frac{N+\varepsilon_3 N - 2\varepsilon_3}{N(N-1)}$$

that gives the correct parameter $\frac{2}{N}$ if and only if $\varepsilon_3 = 1$.

2 Canonical form and reflections

THEOREM 1 Any unitary operator $\mathbf{U}(\beta_0,\varepsilon)$ with real coefficients in the basis ($|i>$) and satisfying the conditions of Theorem (1.1), can be written in the form:

$$\mathbf{U}(\beta_0,\varepsilon) := \varepsilon_1\varepsilon_4|0>\left(\beta_0 \;<0| + \varepsilon_3\varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}}\sum_{k\neq 0}<k|\right) +$$

$$+\varepsilon_2\sum_{i\neq 0}|i>\left(<i| + \varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}}<0| - \frac{1+\varepsilon_3\beta_0}{N-1}\sum_{k\neq 0}<k|\right) \tag{31}$$

Moreover a unit vector $u \in \mathbf{R}^N$ such that:

$$\mathbf{U}(\beta_0,\varepsilon) = \varepsilon_2\left(\mathbf{1} - 2|u><u|\right) \tag{32}$$

exists if and only if ε is such that

$$\varepsilon_2 = \varepsilon_1 \varepsilon_4 \varepsilon_3 \tag{33}$$

In this case $|u>$ has the form:

$$|u> = \frac{1}{\sqrt{2}} \left| -\varepsilon_5 \sqrt{1-\varepsilon_3\beta_0}, \sqrt{\frac{1+\varepsilon_3\beta_0}{N-1}}, \ldots, \sqrt{\frac{1+\varepsilon_3\beta_0}{N-1}} \right\rangle \tag{34}$$

REMARK Notice that unitary operator (32) simply realizes the reflection of the $|u>$-component of any vector with respect to the $|u>$-axis.
PROOF The identity (31) follows immediately from (2), (21) and (22).

The operator $\mathbf{U}(\beta_0, \varepsilon)$ of the equation (31) can be rapresented in the following way:

$$\mathbf{U}(\beta_0,\varepsilon) := \varepsilon_2 \mathbf{1} - \left\{ |0> \left[(\varepsilon_2 1 - \varepsilon_1\varepsilon_4\beta_0) < 0| - \varepsilon_1\varepsilon_4\varepsilon_3\varepsilon_5 \frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} \sum_{k\neq 0} < k| \right] + \right.$$

$$\left. + \varepsilon_2 \sum_{i\neq 0} |i> \left(-\varepsilon_5 \frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} < 0| + \frac{1+\varepsilon_3\beta_0}{N-1} \sum_{k\neq 0} < k| \right) \right\} \tag{35}$$

Now an easy calculation shows that, given a vector $|u>$ of the form (35), the right end side of (32) is equal to:

$$\varepsilon_2 \mathbf{1} - \left\{ |0> \left[\varepsilon_2 (1-\varepsilon_3\beta_0) < 0| - \varepsilon_2\varepsilon_5 \frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} \sum_{k\neq 0} < k| \right] + \right.$$

$$\left. + \varepsilon_2 \sum_{i\neq 0} |i> \left((-\varepsilon_5 \frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} < 0| + \frac{1+\varepsilon_3\beta_0}{N-1} \sum_{k\neq 0} < k| \right) \right\} \tag{36}$$

For $\beta_0 \neq 0, 1$ (36) and (35) are equal if and only if (33) holds. and the last operator is a projector if and only if:

$$\varepsilon_2 = \varepsilon_1 \varepsilon_4 \varepsilon_3 \tag{37}$$

because the off-diagonal terms must be equal. From this the thesis follows observing that multiplying (37) for $\varepsilon_2\varepsilon_3$ we obtain:

$$\varepsilon_3 = \varepsilon_1 \varepsilon_4 \varepsilon_2 \tag{38}$$

COROLLARY 2 Grover's operator is the product of a operator of the form (32) with a *flip*, realized with a operator $\mathbf{U}(\gamma = 0,\ \forall a)$, as in the Remark after previous Theorem 2.1.

PROOF As it is implicit in its definition (see Section 4), Grover's operator is a *flip* followed by a reflection of the $|v>$-component with respect to the $|v>$-axis, where $|v>:= N^{-1/2}|1,\ldots,1>$.

REMARK Theorem (2.1) shows that Grover's unitary and the generalized ones presented in this paper are analogue, and the realizability of the former implies the realizability of the latter.

REMARK If in (35) the identity (37) holds then, remembering (23) and (24), we can rewrite (35) inthe form:

$$|u>= \left| -\sin\frac{\theta}{2},\ \frac{\cos\frac{\theta}{2}}{\sqrt{N-1}},\ \ldots,\ \frac{\cos\frac{\theta}{2}}{\sqrt{N-1}} \right\rangle \tag{39}$$

which, up to a phase, is the most general form of a vector in $\mathbf{R}^N$ with $N-1$ components equal.

REMARK A matrix rapresentation of the operator $\mathbf{U}(\beta_0, \varepsilon)$ in the basis $(|i>)$, with $\varepsilon_2 = \varepsilon_1\varepsilon_4\varepsilon_3$ is:

$$\mathbf{U}(\beta_0,\varepsilon) = \varepsilon_2 \begin{pmatrix} 1+\varepsilon_3\beta_0 - 1 & \varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} & \varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} & \cdots & \varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} \\ \varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} & 1-\frac{1+\varepsilon_3\beta_0}{N-1} & -\frac{1+\varepsilon_3\beta_0}{N-1} & \cdots & -\frac{1+\varepsilon_3\beta_0}{N-1} \\ \varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} & -\frac{1+\varepsilon_3\beta_0}{N-1} & 1-\frac{1+\varepsilon_3\beta_0}{N-1} & \cdots & -\frac{1+\varepsilon_3\beta_0}{N-1} \\ \vdots & \vdots & & \ddots & \\ \varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} & -\frac{1+\varepsilon_3\beta_0}{N-1} & -\frac{1+\varepsilon_3\beta_0}{N-1} & \cdots & 1-\frac{1+\varepsilon_3\beta_0}{N-1} \end{pmatrix} =$$

$$= \varepsilon_2\mathbf{1} - \varepsilon_2 \begin{pmatrix} 1-\varepsilon_3\beta_0 & -\varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} & \cdots & -\varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} \\ -\varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} & \frac{1+\varepsilon_3\beta_0}{N-1} & ts & \frac{1+\varepsilon_3\beta_0}{N-1} \\ \vdots & \vdots & \ddots & \vdots \\ -\varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} & \frac{1+\varepsilon_3\beta_0}{N-1} & ts & \frac{1+\varepsilon_3\beta_0}{N-1} \end{pmatrix} =$$