LaTeXdocument CNES Grover.tex/ Roma, 12.11.2000

Generalized Grover's quantum algorithm

Luigi Accardi
Ruben Sabbadini

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

ABSTRACT

The Necessary and Sufficient Conditions in order that an unitary = operator can amplify the component of a *generic* vector related to = a particular base vector, at other components' expence, are = investigated. This leads to a class of suitable methods in wich is = possible to choose the optimum one, related to the problem we want to = solve, i.e. the vector whose component we want to amplify. = *Grover's quantum algorithm* is demonstrated to be in that class, = very near to the optimum method. A possible application to the the = *Ohya–Masuda quantum SAT algorithm* is shown as an example for = further improvements. =20

1 An algorithm to increase the probability of $|0>$ at each step = for every vector $|a>$

THEOREM Given the linear functionals:

$$\eta(a) \sum_{i0}^{N} \eta_i a_i \tag{1}$$

$$c(a)\sum_{i0}^{N}\gamma_i a_i \tag{2}$$

with γ_i and η_i real, Necessary and Sufficient Conditions = in order that the operator **U**:

$$\mathbf{U}\sum a_i|i> \varepsilon_1(a_0+\eta(a))|0> +\varepsilon_2\sum_{i\not{0}} = (a_i+c(a))\,|i> \tag{3}$$

were unitarian are:

$$\begin{cases} \gamma_0\varepsilon_5\frac{\sqrt{1-\beta_0^2}}{=\sqrt{N-1}} & (a) \\ \eta_i\varepsilon_3\gamma_0 & = \quad (b) \\ = \gamma_i - \frac{1+\varepsilon_3\beta_0}{N-1} & = \quad (c) \\ \eta_0 - 1 + \varepsilon_4\beta_0 & (d) \end{cases} \tag{4}$$

with ε_1, ε_2, ε_3, ε_4, $\varepsilon_5 \pm 1.$=20

PROOF

The following isomery condition is a necessary condition:

$$\sum a_i^2(a_0+\eta)^2 + \sum_{i\not{0}}(a_i+c)^2a_0^2 + \eta^2 + 2a_0\eta + \sum_{i\not{0}} a_i^2 + (N-1)c^2 + 2c\sum_{i\not{0}} a_i$$

$$\eta^2 + 2a_0\eta + (N-1)c^2 + 2c\sum_{i\not{0}} a_i 0 \tag{5}$$

The equation (**??**) has the following structure:

$$\eta^2 + 2a_0\eta + \gamma 0 \tag{6}$$

with:

$$\gamma(N-1)c^2 + 2c\sum_{i\not{0}} a_i \tag{7}$$

and its possible solutions are:

$$\eta - a_0 + \varepsilon_4\sqrt{a_0^2-\gamma} \tag{8}$$

The case $\gamma 0$ is trivial because it leads to $\eta 0$ or to $= \eta - 2a_0$; in any case we have:

$$\mathbf{U}\sum a_i|i> \pm\varepsilon_1 a_0\ |0> + = \varepsilon_2\sum_{i\not{0}}(a_i+c)\ |i>$$

that leaves the probability of $|0>$ the same. We must look for $=\gamma \not 0$ solutions to modify the component a_0 of a.

But $\gamma \not\emptyset$ corresponds to the following condition linked to $=$ the linearity of the funzional $\eta(a)$:

$$a_0^2 - \gamma \left(\sum_j \beta_j a_j \right)^2 \tag{9}$$

with the β_j indipendent from a; then the (**??**) must be $=$ valid $\forall a_0, = 20 \ldots, a_N. = 20$

The further linearity condition of the funtional $c(a)$ leads to:

$$c(a) \sum_j \gamma_j a_j \tag{10}$$

with the γ_i indipendent from a. From (**??**) we have:

$$\begin{gathered}
-a_0^2 + (N-1) \left(\sum_j \gamma_j a_j \right)^2 + \left(\sum_j \beta_j a_j = ht)^2 + 2 \sum_j \gamma_j a_j \sum_{i\not 0} a_i 0 \\
-a_0^2 + 2 \sum_j \gamma_j a_j \sum_{i\not 0} a_i + \sum_{i,j} \left[= (N-1)\gamma_i \gamma_j + \beta_i \beta_j \right] a_i a_j 0 \\
a_0^2 \left[(N-1)\gamma_0^2 + \beta_0^2 - 1 \right] + \sum_{i,j \neq 0} \left[2\gamma_j + (N-1)\gamma_i \gamma_j + \beta_i \beta_j \right] a_i a_j + \\
+ 2 \sum_{i\not 0} \left[\gamma_0 + (N-1)\gamma_0 \gamma_i + \beta_0 \beta_i \right] a_0 a_i 0
\end{gathered} \tag{11}$$

If the previous (**??**) must be valid $\forall a_0, \ldots, a_N, =$ then its coefficients ought each to be zero, then:

$$\left\{ \begin{array}{rll}
= (N-1)\gamma_0^2 + \beta_0^2 - 10 & & = \quad (a) \\
2\gamma_j + (N-1)\gamma_i \gamma_j + \beta_i \beta_j 0 & \forall = i, j \not\emptyset & (b) \\
2\gamma_i + (N-1)\gamma_i^2 + \beta_i^2 0 & \forall = i \not\emptyset & (c) \\
\gamma_0 + (N-1)\gamma_0 \gamma_i + \beta_0 \beta_i 0 & \forall = i \not\emptyset & (d)
\end{array} \right. \tag{12}$$

¿From the (**??**d) we have:

$$\gamma_i - \frac{\gamma_0 + \beta_0 \beta_i}{\gamma_0 (N-1)} \tag{13}$$

that, substituted into the (**??**c), gives:

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

or:

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

then, using (**??**a):

$$\beta_i\varepsilon_3\gamma_0\varepsilon_5\frac{\sqrt{1-\beta_0^2}}{=\sqrt{N-1}} \tag{14}$$

with $\varepsilon_3 \pm 1.$=20

Substituted the (**??**) into the (**??**) we arrive to:

$$\gamma_i-\frac{1+\varepsilon_3\beta_0}{N-1} \tag{15}$$

The equation (**??**a) let us to write:

$$\beta_0 cos\ \theta; \qquad \sqrt{N-1}\gamma_0 sin\ \theta \tag{16}$$

i.e. the parameters β_0 and γ_0 live onto the enlipse in = the $\beta_0\gamma_0$-plane Substituting the (**??**), the = (**??**) and the (**??**) into the (**??**) and the = (**??**), we finally obtain:

$$\eta=(a)(-1+\varepsilon_4\beta_0)a_0+\varepsilon_4\varepsilon_3\gamma_0\sum_{k\not{0}}a_k(-1=+\varepsilon_4\beta_0)a_0+\varepsilon_4\varepsilon_3\varepsilon_5\frac{\sqrt{1-\beta_0^2}}{=\sqrt{N-1}}\sum_{k\not{0}}a_k$$

$$(-1+\varepsilon_4 cos\ \theta)\,a_0+\varepsilon_3\varepsilon_4\varepsilon_5\frac{sin\ \ =\theta}{\sqrt{N-1}}\sum_{k\not{0}}a_k \tag{17}$$

$$c(a)\gamma_0 a_0-\frac{1+\varepsilon_3\beta_0}{N-1}\sum_{k\not{0}}a_k\varepsilon_5\frac{\sqrt{1-\beta_0^2}}{=\sqrt{N-1}}a_0-\frac{1+\varepsilon_3\beta_0}{N-1}\sum_{k\not{0}}a_k$$

$$\varepsilon_5\frac{sin\ \theta}{\sqrt{N-1}}a_0-\frac{1+\varepsilon_3 cos\ \theta}{=N-1}\sum_{k\not{0}}a_k \tag{18}$$

that are the same as in the (**??**), the (**??**) and the = (**??**).

Let us go now to verify that the (**??**) are also Sufficient = Conditions. We are going to see that the isometric condition (**??**) = is satisfied by the operator **U** of eq. (**??**) (with the free = parameters given by the (**??**)). Substituting the (**??**) and = (**??**) - really obtained using conditions (**??**) into the = (**??**) and the (**??**) - into the (**??**) to have:

$$\eta(a)^2(-1+\varepsilon_4\beta_0)^2a_0^2+\frac{1-\beta_0^2}{N-1}=\left(\sum_{k\not0}a_k\right)^2+2\varepsilon_4\varepsilon_3\varepsilon_5a_0(-1+\varepsilon_4\beta_=0)\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}}\sum_{k\not0}a_k$$

$$2a_0\eta=(a)2(-1+\varepsilon_4\beta_0)a_0^2+2\varepsilon_4\varepsilon_3\varepsilon_5a_0\sqrt{1-\beta_0^2}\bar{o}ver\sqrt{N-1}\sum_{k\not0}a_k$$

$$\eta(a)^2+2a_0\eta(a)(-1+\beta_0^2)a_0^2+\frac{1-\beta_0^2}{=N-1}=\left(\sum_{k\not0}a_k\right)^2+2\varepsilon_3\varepsilon_5a_0\beta_0\frac{\sqrt{1-\beta_=0^2}}{\sqrt{N-1}}\sum_{k\not0}a_k$$

$$(N-1)c(a)^2(1-\beta_0^2)a_0^2+\frac{(1+\varepsilon_3\beta_0)^2}{(N-1)^2}=\left(\sum_{k\not0}a_k\right)^2=-2\varepsilon_5a_0\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}}(1+\varepsilon_3\beta_0)\sum_{k=t0}a_k$$

$$2c(a)\sum_{k\not0}a_k2\varepsilon_5a_0\frac{\sqrt{1-\beta_0^2}}{=\sqrt{N-1}}\sum_{k\not0}a_k-2\frac{1+\varepsilon_3\beta_0}{N-1}=\left(\sum_{k\not0}a_k\right)^2$$

We can now verify that $\eta(a)^2+2a_0\eta(a)-\gamma$:

$$(\beta_0^2-1)a_0^2+\frac{1-\beta_0^2}{N-1}=\left(\sum_{k\not0}a_k\right)^2+2\varepsilon_3\varepsilon_5a_0\beta_0\frac{\sqrt{1-\beta_=0^2}}{\sqrt{N-1}}\sum_{k\not0}a_k$$

$$(-1+\beta_0^2)a_0^2=-\frac{(1+\varepsilon_3\beta_0)^2}{(N-1)^2}\left(\sum_{k\not0}a_k\right)^2+==2\varepsilon_5a_0\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}}(1+\varepsilon_3\beta_0)\sum_{k\neq0}a_k+$$

$$-2\varepsilon_5a_0\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}}\sum_{k\not0}a_k=+2\frac{1+\varepsilon_3\beta_0}{N-1^2}\left(\sum_{k\not0}a_k\right)^2$$

that leads to:

$$(\beta_0^2-1)a_0^2+\frac{1-\beta_0^2}{N-1}=\left(\sum_{k\not 0}a_k\right)^2+2\varepsilon_3\varepsilon_5 a_0\beta_0\frac{\sqrt{1-\beta_=0^2}}{\sqrt{N-1}}\sum_{k\not 0}a_k$$

$$(-1+\beta_0^2)a_0^2=+\frac{2(1+\varepsilon_3\beta_0)-(1+\varepsilon_3\beta_0)^2}{(N-1)^2}=\left(\sum_{k\not 0}a_k\right)^2+$$

$$+=2\varepsilon_5 a_0\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}}(1+\varepsilon_3\beta_0-1)\sum_{k=ot0}a_k$$

that rapresents an identity.

We have then obtained the proof that the operator **U** described in = the (**??**), under the conditions (**??**),(**??**) and = (**??**), rapresents all and only the isometric operators that modify = a component at other components' expence. But an operator on a finite = Hilbert space is isometric if and only if it is unitary, and this = completes the proof.

COROLLARY 1 Grover's method (see the following eq.s = (21) and (22)) corresponds to the choise $\varepsilon_1\varepsilon_4 1$, $=\varepsilon_2-1$, $\varepsilon_3 1$, $\beta_0\frac{N-2}{N}$, $=\gamma_0\frac{2}{N(N-1)}$, then $tg\ =\theta\frac{2\sqrt{N-1}}{N-2}$.

PROOF

¿From eq.s (**??**) and (**??**) we have:

$$\varepsilon_1\left[a_0+\eta(a)\right]\varepsilon_1\varepsilon_4\left(\beta_0 a_0+\varepsilon_3\gamma_0\sum_{k\not 0}a_k\right)\bar{l}abelgr19 \tag{19}$$

$$\varepsilon_2\left[a_i+c(a)\right]=\varepsilon_2\left(a_i+\gamma_0 a_0-\frac{1+\varepsilon_3\beta_0}{N-1}\sum_{k\neq 0}a_k\right) \tag{20}$$

with:

$$\beta_i\varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}}$$

that, compared with (20) and (21) gives:

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

da cui $\varepsilon_1\varepsilon_4 1$ and $\beta_0\frac{N-2}{N}$ and:

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

as in (21) and in (22) with $\varepsilon_2 - 1$. And finally:

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

=20 that gives the right parameter $\gamma_0\frac{2}{N}$ if and only if $=\varepsilon_3 1$. The goniometric form of the previous equations easily = comes from the (**??**).

COROLLARY 2 Optimum method for the case looked into = by Grover, i.e. a vector a of the form:

$$|a_G>: a_0|0>+b\sum_{i\not{0}}|i>$$

with:

$$a_0^2+(N-1)b^2 1 \tag{21}$$

demands the following choise for the free parameters $=\varepsilon_1\varepsilon_4\varepsilon_3\varepsilon_5 1$, $\beta_0 a_0$, then $tg\ =\theta\sqrt{N-1}\frac{b}{a_0}$.

PROOF

¿From eq.s (**??**) and (**??**) we have:

$$\mathbf{U}|a_G>: \mathbf{U}\left(a_0|0>+b\sum_{i\not{0}}|i>\right)$$

$$\varepsilon_1\varepsilon_4\left[\beta_0 a_0+\varepsilon_3\varepsilon_5\sqrt{(N-1)(1-\beta_0^2)}b\bar{r}ight]|0>+$$

$$+\varepsilon_2\left[b+\varepsilon_5\frac{\sqrt{1-\beta_0^2}}{=\sqrt{N-1}}a_0-(1+\varepsilon_3\beta_0)\,b\right]\sum_{i\not{0}}|i>=$$

$$\varepsilon_1\varepsilon_4\left(cos\ \theta a_0+\varepsilon_3\varepsilon_5\sqrt{N-1}sen\ =\theta\ b\right)|0>+$$

$$+\varepsilon_2\left(\varepsilon_5\frac{sen\ \theta}{\sqrt{N-1}}a_0-\varepsilon_3 cos\ =\theta\ b\right)\sum_{i\not{0}}|i>$$

and the maximum is reached for:

$$\frac{\partial}{\partial \beta_0}\left(cos\ \theta = a_0 + \varepsilon_3\varepsilon_5\sqrt{N-1}sen\ \theta\ b\right)$$

$$-sen\ \theta a_0 + \varepsilon_3\varepsilon_5\sqrt{N-1}cos\ \theta\ b0$$

then:

$$tg\ \theta\ \varepsilon_3\varepsilon_5\sqrt{N-1}\frac{b}{a_0}$$

that gives $\beta_0 cos\ \theta\ \pm a_0$. And, choosing the $+ =$ sign, we have:

$$a_0 \mapsto \varepsilon_1\varepsilon_4\left[a_0^2 + \varepsilon_3\varepsilon_5(1-a_0^2)\right]1$$

where the last passage derives form the choise $= \varepsilon_1\varepsilon_4\varepsilon_3\varepsilon_5 1$. And:

$$b \mapsto \varepsilon_2\left(\varepsilon_5 b a_0 - \varepsilon_3 a_0 b\right)0$$

and this completes the proof.

2 Here Grover's algorithm is applied to a generic vector $|a>$

=20

Let

$$|a>: \sum_i a_i|i>$$

and

$$|v>: \frac{1}{\sqrt{N}}\sum_k |k>$$

be two vectors.

Let then:

$$|\tilde{a}>: \mathbf{U}_f\mathbf{Z}\mathbf{U}_f|a> -a_0 = |0> + \sum_{i\not{0}} a_i|i>$$

be another vector followed from a.

Calculating in advance:

$$< v|\tilde{a} > \frac{1}{\sqrt{N}} \sum_{k} |k > \left(-a_0 = |0 > + \sum_{i\not{0}} a_i |i > \right) \frac{1}{\sqrt{N}} \left(-a_0 + \sum_{k\not{0}} a_k \right)$$

Then, given $\mathbf{P} : |v >< v|$:

$$\mathbf{D}|\tilde{a} >: (-1 + 2\mathbf{P}) \, |\tilde{a} > -|\tilde{=}a > +2 < v|\tilde{a} > \; |v > -|\tilde{a} > + \frac{2}{\sqrt{N}} \left(-a_0 = + \sum_{k\not{0}} a_k \right) \; |v >$$

$$\left[\left(1 - \frac{2}{N} \right) a_0 + \frac{2}{= N} \sum_{k\not{0}} a_k \right] |0 > + \sum_{i\not{0}} \left[-a_i + \frac{2}{N} \left(-a_0 = + \sum_{k\not{0}} a_k \right) \right] \; |i >$$

Then:

$$a_0 \mapsto \frac{N-2}{N} a_0 + \frac{2}{N} \sum_{k\not{0}} a_k a_0 + \eta = (a) \tag{22}$$

$$a_i \mapsto -a_i + \frac{2}{= N} \left(-a_0 + \sum_{k\not{0}} a_k \right) - a_i + c(a) \tag{23}$$

If $a_k a_h \forall k, \; h \; \not{0}$ (the Grover's agorithm case) then:

$$a_0 \mapsto \frac{N-2}{N} a_0 + \frac{2(N-1)}{N} a_i$$

$$a_i \mapsto \left[-1 + \frac{2(N-1)}{N} \right] a_i - \frac{2}{N} a_0$$