INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL
J. Phys. A: Math. Gen. **34** (2001) L681–L687 PII: S0305-4470(01)29430-X

LETTER TO THE EDITOR

Can quantum chaos enhance the stability of quantum computation?

Tomaž Prosen and Marko Žnidarič

Physics Department, Faculty of Mathematics and Physics, University of Ljubljana, Slovenia

Received 2 October 2001
Published 16 November 2001
Online at stacks.iop.org/JPhysA/34/L681

Abstract

We consider the stability of a general quantum algorithm (QA) with respect to a fixed but unknown residual interaction between qubits, and show a surprising fact, namely that the average fidelity of quantum computation increases on decreasing the average time correlation function of the perturbing operator in sequences of consecutive quantum gates. Our thinking is applied to the quantum Fourier transformation, where an alternative 'less regular' QA is devised, which is qualitatively more robust against static random residual n-qubit interaction.

PACS numbers: 03.67.Lx, 05.45.-a, 05.45.Mt

Recent investigations of theoretical and experimental possibilities of quantum information processing have made the idea of quantum computation [1] very attractive and important (see e.g. [2] for a review). Having apparatus which is capable of manipulation and measurement of pure states of individual quantum systems, one can make use of the massive intrinsic parallelism of coherent quantum time evolution.

The main idea of quantum computation is the following: consider a many-body system of n elementary two-level quantum excitations—*qubits*, which is called the *quantum register*, store the data for quantum computation in the initial state of a register $|r\rangle$ which is a superposition of an exponential number $\mathcal{N} = 2^n$ of basic qubit states, then perform certain unitary transformation U by decomposing $U = U(T)\cdots U(2)U(1)$ into a sequence of T elementary one-qubit and two-qubit *quantum gates* $U(t)$, $t = 1, 2, \ldots, T$, such decomposition being called a *quantum algorithm* (QA), and in the end obtain the results by performing measurements of qubits on a final register state $U|r\rangle$. QA is called *efficient* if the number of needed elementary gates T grows with at most *polynomial* rate in $n = \log_2 \mathcal{N}$, and only in this case can it generally be expected to outperform the best classical algorithms (in the limit $n \to \infty$). At present only a few efficient QAs are known, and perhaps the most generally useful is the quantum Fourier transformation (QFT) [3].

There are two major obstacles for performing practical quantum computation: first, there is a problem of *decoherence* [4] resulting from an unavoidable *time-dependent* coupling between qubits and the environment. If the perturbation couples only a small number of qubits at a time then such errors can be eliminated at the expense of extra qubits by *quantum error correcting codes* [5] (see [6] for another approach). Second, even if one knows an efficient error correcting code or assumes that quantum computer is ideally decoupled from the environment, there will typically exist a small *unknown* or *uncontrollable* residual interaction among qubits, which one may describe by a general *static* perturbation. Therefore, understanding the *stability* of QAs with respect to various types of perturbation is an important problem (see [7–9] for some results on this topic).

Motivated by [10], we propose a new approach to the stability of quantum computation with respect to a static but incurable (perhaps unknown) perturbing interaction. We consider the QA as a time-dependent dynamical system and relate its fidelity measuring the Hilbert space distance between computed states of exact and perturbed algorithm in terms of integrated time autocorrelation of the perturbing operator (generalizing [11]). The derived relation looks very surprising: it tells us that faster decay of time correlations of the perturbation between sequences of successive quantum gates means larger fidelity, and vice versa. We propose to use our rule of thumb as a guide to devise or to improve QAs, either by introducing extra 'chaotic' gates or by rewriting the gates in a different order in order to make time evolution $U(t)$ 'more chaotic'. As an important example, the well known QFT algorithm, whose internal dynamics appears unpleasantly 'regular', has been improved in a way such that the modified algorithm becomes qualitatively more robust against static random perturbation of the gates. We think our effect should be considered in experimental realization of QFTs which are underway [12].

Let us write the *partial evolution operator* for a sequence of consecutive gates from t' to t, $t' < t$, as $U(t,t') = U(t)U(t-1)\cdots U(t'+2)U(t'+1)$, with $U(t,t) \equiv 1$, and perturb the quantum gates by a (generally time-dependent) perturbation of strength δ generated by Hermitian operators $V(t)$

$$U_\delta(t) = \exp(-\mathrm{i}\delta V(t))U(t). \tag{1}$$

Propagating the initial register state $|r\rangle$ with exact and perturbed algorithms we focus on the *fidelity* of the QA defined as

$$F(T) = \frac{1}{\mathcal{N}} \operatorname{tr} U_\delta^\dagger(T,0)U(T,0) \tag{2}$$

as an average over all initial register states. Defining the Heisenberg time evolution from t' to t, $V(t,t') = U^\dagger(t,t')V(t)U(t,t')$, we rewrite the fidelity as

$$F(T) = \frac{1}{\mathcal{N}} \operatorname{tr}\left(\mathrm{e}^{\mathrm{i}\delta V(1,0)}\mathrm{e}^{\mathrm{i}\delta V(2,0)}\cdots\mathrm{e}^{\mathrm{i}\delta V(T,0)}\right) \tag{3}$$

by T insertions of the unity $U^\dagger(t,0)U^\dagger(t,0) = 1$ and observing $U^\dagger(t,0)U_\delta^\dagger(t)U(t,0) = \exp(\mathrm{i}\delta V(t-1,0))$ as t runs from T down to 1.

Next we make a series expansion in δ expressing the fidelity in terms of correlation functions

$$F(T) = 1 + \frac{1}{\mathcal{N}}\sum_{m=1}^{\infty}\frac{i^m\delta^m}{m!}\sum_{t_1,\ldots,t_m=1}^{T}\operatorname{tr}\left(\hat{\mathcal{T}}\prod_{j=1}^{m}V(t_j,0)\right) \tag{4}$$

where $\hat{\mathcal{T}}$ is a left-to-right time ordering (w.r.t. indices t_j). We can make the series starting at second order $m = 2$ by assuming the average perturbation to be *traceless*, $\operatorname{tr}\bar{V} = (1/T)\sum_{t=1}^{T}\operatorname{tr}V(t,0) \equiv 0$ (otherwise, the effect of subtracting the trace average is a simple complex rotation of fidelity). To second order in δ, the fidelity can be written as

$$F(T) = 1 - \frac{\delta^2}{2}\sum_{t,t'=1}^{T}C(t,t') + \mathcal{O}(\delta^3) \tag{5}$$

in terms of a two-point time correlation (correlator) of the perturbation $C(t,t') := C(t',t) := \mathrm{tr}(V(t',0)V(t,0))/\mathcal{N} = \mathrm{tr}(V(t')V(t,t'))/\mathcal{N}$. The relation (5) is very interesting: it tells us that the QA is more stable if the time correlations of the perturbation are smaller on average, meaning that the 'chaotic' quantum time evolution is more stable than the 'regular' one [11]. One may use this general philosophy as a guide to design QAs, or to improve the existing ones by rearranging quantum gates.

However, the behaviour of the correlation function depends also on the explicit time (in-) dependence of the perturbation $V(t)$. For example, if the perturbation $V(t)$ is an *uncorrelated noise*, as it would be in the case of coupling to an *ideal heat bath*, then the matrix elements of $V(t)$ may be assumed to be *Gaussian random* with variances $\langle V_{jk}(t)V_{lm}(t')\rangle_{\mathrm{noise}} = (1/\mathcal{N})\delta_{jm}\delta_{kl}\delta_{tt'}$. Hence one finds $\langle C(t,t')\rangle_{\mathrm{noise}} = \delta_{tt'}$, and averaging of a formula (4) yields the noise-averaged fidelity $\langle F(T)\rangle_{\mathrm{noise}} = \exp(-\delta^2 T/2)$, which is *independent of the QA $U(t)$*. On the other hand, for a *static* residual interaction $V(t) \equiv V$ one may expect slower correlation decay, depending on the 'regularity' of the evolution operator U, and hence faster decay of fidelity. Importantly, note that in a physical situation, where perturbation is expected to be a combination $V(t) = V_{\mathrm{static}} + V_{\mathrm{noise}}(t)$, the fidelity drop due to a static component is expected to *dominate* long-time quantum computation $T \to \infty$ over the noise component (e.g. due to decoherence), as soon as the QA exhibits long-time correlations of the operator V_{static}. Since the sequence of gates to accomplish a certain task U is by no means unique, the natural question arises of how to write the QA in order to have the fastest decay of time correlations with respect to a static, say Gaussian random (GUE), perturbation.

We consider QFT working in a Hilbert space of dimension $\mathcal{N} = 2^n$ with basis qubit states denoted by $|k\rangle$, $k = 0,\ldots,2^n-1$. The unitary matrix U_{QFT} performs the following transformation on a state with expansion coefficients x_k:

$$U_{\mathrm{QFT}}\left(\sum_{k=1}^{\mathcal{N}-1} x_k|k\rangle\right) = \sum_{k=1}^{\mathcal{N}-1}\tilde{x}_k|k\rangle \tag{6}$$

where $\tilde{x}_k = \frac{1}{\sqrt{\mathcal{N}}}\sum_{j=1}^{\mathcal{N}-1}\exp(2\pi \mathrm{i} jk/\mathcal{N})x_j$. The 'dynamics' of QFT consists of three kinds of unitary gate: one-qubit gates A_j acting on the jth qubit

$$\mathrm{A}_j = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \tag{7}$$

diagonal two-qubit gates $\mathrm{B}_{jk} = \mathrm{diag}\{1,1,1,\exp(\mathrm{i}\theta_{jk})\}$, with $\theta_{jk} = \pi/2^{k-j}$, and transposition gates T_{jk}, which interchange jth and kth qubits. There are n A-gates, $n(n-1)/2$ B-gates and $[n/2]$ transposition gates, where $[x]$ is an integer part of x. The total number of gates for the whole algorithm is therefore $T = [n(n+2)/2]$. For instance, in the case of $n = 4$ we have a sequence of $T = 12$ gates (time runs from right to left)

$$U_{\mathrm{QFT}} = \mathrm{T}_{03}\mathrm{T}_{12}\mathrm{A}_0\mathrm{B}_{01}\mathrm{B}_{02}\mathrm{B}_{03}\mathrm{A}_1\mathrm{B}_{12}\mathrm{B}_{13}\mathrm{A}_2\mathrm{B}_{23}\mathrm{A}_3. \tag{8}$$

In what follows we shall focus on a static random perturbation, that is $V(t) \equiv V$ is a random $\mathcal{N}$-dimensional GUE matrix with normalized second moments $\langle V_{jk}V_{lm}\rangle = \delta_{jm}\delta_{kl}/\mathcal{N}$, where $\langle\cdot\rangle$ denotes an average over GUE. For small perturbation strength δ the quantity controlling the fidelity (5) is the correlator

$$\langle C(t,t')\rangle = \frac{1}{\mathcal{N}}\langle \mathrm{tr}(V(t,t')V)\rangle = \left|\frac{1}{\mathcal{N}}\,\mathrm{tr}\,U(t,t')\right|^2. \tag{9}$$

Averaging over GUE is done only to ease up analytical calculation and to yield a quantity that is independent of a particular realization of perturbation. Qualitatively similar (numerical) results are obtained without the averaging. We have $\langle C(t,t)\rangle \equiv 1$ due to normalization of the second moments of GUE, while for an arbitrary fixed V the diagonal correlator is

$$C(t,t) = C(0,0) = \frac{1}{\mathcal{N}} \operatorname{tr} V^2. \tag{10}$$

In a sum of correlation function (5) we must therefore distinguish two contributions: (i) the diagonal correlator (10) just sets an overall scale. This is a *static* quantity as it depends on the strength of a perturbation V only and can be included in δ by normalizing $\operatorname{tr} V^2/\mathcal{N} = 1$. (ii) The off-diagonal contribution is mainly determined by the rate of decay of $C(t,t')$ as $t - t'$ increases, which is an essential *dynamical* feature of the QA.

We have calculated the correlator $\langle C(t,t')\rangle$ for QFT (9), which is shown in the top panel of figure 1. One can clearly see square red plateaus on the diagonal due to blocks of successive B-gates. Similar square plateaus can also be seen off diagonal (from orange to yellow to green), so the correlation function has a staircase-like structure, with the A-gates responsible for the drops and B-gates responsible for the flat regions in between. This can be easily understood. For 'distant' qubits $k-j \gg 1$ the gates B_{jk} are close to identity and therefore cannot reduce the correlator. This slow correlation decay results in the correlation sum $\chi := \frac{1}{2}\sum_{t,t'=1}^{T} C(t,t')$ being proportional to $\chi \propto n^3$ (sum of the first n squares) as compared with the theoretical minimum $\chi \propto T \propto n^2$.

In view of this, we shall now try to rewrite the QFT with the goal of accomplishing $\chi \propto n^2$. From (9) we learn that the gates that are *traceless* (e.g. A-gates) reduce the correlator very effectively. In the plain QFT algorithm (8) we have $n-1$ blocks of B-gates, where in each block all B-gates act on the same first qubit, say j. In each such block, we propose to replace B_{jk} with a new gate $\mathrm{G}_{jk} = \mathrm{R}_{jk}^{\dagger}\mathrm{B}_{jk}$, where unitary gate R_{jk} will be chosen so as to commute with all the diagonal gates B_{jl} in the block, whereas at the end of the block we shall insert R_{jk} in order to 'annihilate' $\mathrm{R}_{jk}^{\dagger}$ so as to preserve the evolution matrix of a whole block. Unitarity condition $\mathrm{R}_{jk}^{\dagger}\mathrm{R}_{jk} = 1$ and $[\mathrm{R}_{jk}, \mathrm{B}_{jl}] = 0$ for all j, k, l leave us with a six-parametric set of matrices R_{jk}. By further enforcing $\operatorname{tr}\mathrm{R}_{jk} = 0$ in order to maximally reduce the correlator, we end up with four free real parameters in R_{jk}. One of the simplest choices, that has been proved to be equally as suitable as any other, is the following:

$$\mathrm{R}_{jk} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \tag{11}$$

Furthermore, we find that R-gates also commute among themselves, $[\mathrm{R}_{jk}, \mathrm{R}_{jl}] = 0$, which enables us to write a sequence of R-gates however we like, for example in the same order as a sequence of Gs, so that pairs of gates G_{jk}, R_{jk} operating on the same pair of qubits (j,k), whose product is a *bad gate* B_{jk}, are never neighbouring. This is best illustrated by an example. For instance, the block $\mathrm{B}_{01}\mathrm{B}_{02}\mathrm{B}_{03}$ will be replaced by $\mathrm{R}_{01}\mathrm{R}_{02}\mathrm{R}_{03}\mathrm{R}_{01}^{\dagger}\mathrm{B}_{01}\mathrm{R}_{02}^{\dagger}\mathrm{B}_{02}\mathrm{R}_{03}^{\dagger}\mathrm{B}_{03} = \mathrm{R}_{01}\mathrm{R}_{02}\mathrm{R}_{03}\mathrm{G}_{01}\mathrm{G}_{02}\mathrm{G}_{03}$. This is how we construct an *improved Fourier transform algorithm* (IQFT). For IQFT we need one additional type of gate; instead of diagonal B-gates, we use nondiagonal R and G. To illustrate the obvious general procedure we write out the whole IQFT algorithm for $n = 4$ qubits (compare with (8))

$$U_{\mathrm{IQFT}} = \mathrm{T}_{03}\mathrm{T}_{12}\mathrm{A}_0\mathrm{R}_{01}\mathrm{R}_{02}\mathrm{R}_{03}\mathrm{G}_{01}\mathrm{G}_{02}\mathrm{G}_{03}\mathrm{A}_1\mathrm{R}_{12}\mathrm{R}_{13}\mathrm{G}_{12}\mathrm{G}_{13}\mathrm{A}_2\mathrm{R}_{23}\mathrm{G}_{23}\mathrm{A}_3. \tag{12}$$

Such an IQFT algorithm consists of a total of $T = [n(2n+1)/2]$ gates (note that it does not pay to replace the block with a single B gate as we have done, so we could safely leave $\mathrm{B}_{23} \equiv \mathrm{R}_{23}\mathrm{G}_{23}$). The correlation function for the IQFT algorithm is shown in the bottom panel of figure 1. Almost all off-diagonal correlations are greatly reduced (to the level $\propto 1/\mathcal{N}^2$),

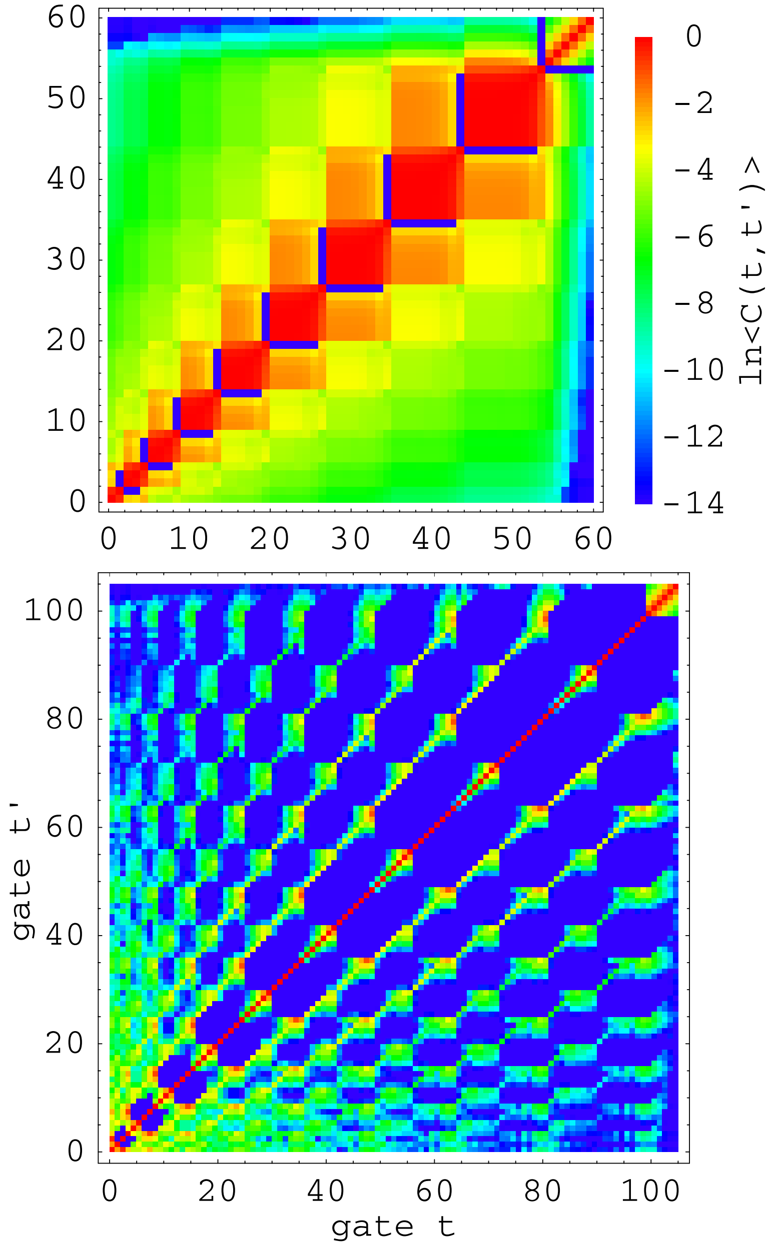

Figure 1. Correlation function $\langle C(t, t')\rangle$ for $n = 10$ qubits and GUE perturbation. The top panel shows standard QFT (8) with $T = 60$, while the bottom panel shows IQFT with $T = 105$ gates. Colour represents the size of elements in a log-scale from red (e^{-0}) to blue (e^{-14} and less).

leaving us only with a dominant diagonal. If we had only diagonal elements, the fidelity would be $\langle F(T)\rangle = 1 - \delta^2 \frac{T}{2}$ (as in the case of noisy perturbation or decoherence, however with a different physical meaning of the strength scale δ) where the number of gates scales as $T \propto n^2$. From the pictures (1) it is clear that we have very fast correlation decay for IQFT so the correlation sum χ has decreased from $\chi \propto n^3$ to $\chi \propto n^2$ behaviour. To further

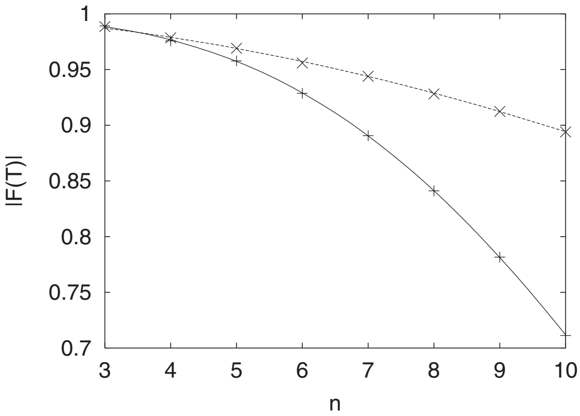

Figure 2. Dependence of fidelity $|\langle F(T)\rangle|$ on the number of qubits n for QFT (pluses) and IQFT algorithms (crosses), for fixed $\delta = 0.04$. Numerical averaging over 50 GUE realizations is performed. The full curve is $\exp(-\delta^2\{0.236n^3 - 0.38n^2 + 1.45n\})$ and the dashed one is $\exp(-\delta^2\{0.61n^2 + 0.89n\})$. For $n = 10$ the trace is approximated by an average over 200 Gaussian random register states.

illustrate this, we have numerically calculated the fidelity by simulating the QA and applying perturbation $\exp(-\mathrm{i}\delta V)$ at each gate. The results are shown in figure 2. The difference between $\propto n^2$ and $\propto n^3$ behaviour is nicely seen. As we have argued before, the sum of the two-point correlator (5) gives us only the first nontrivial order in the δ-expansion. For dynamical systems, being either integrable or mixing and ergodic, it has been shown [11] that higher orders of (4) can also typically be written as simple powers of the correlation sum χ, so the fidelity has a simple functional form $F(t) = \exp(-\chi\delta^2)$. Although the QA has quite inhomogeneous time dependence, we may still hope that $\exp(-\chi\delta^2)$ is also a reasonable approximation to the fidelity at higher orders in δ. This is in fact the case as can be seen in figure 3. Note also that the leading coefficient in the exponent for IQFT, $\lim_{n\to\infty} \chi/n^2 = 0.61$, is close to the theoretical minimum of 0.5.

As the definition of what is a fundamental single gate is somewhat arbitrary, the problem of minimizing the sum χ depends on a given technical realization of gates and the nature of the residual perturbation V for an experimental setup. We should mention that the optimization becomes harder if we consider *few-body* (e.g. two-body random) perturbation. This is connected with the fact that quantum gates are two-body operators and can perform only a very limited set of rotations on a full Hilbert space, and consequently have a limited capability of reducing correlation functions in a single step. However, our simple approach based on n-body random matrices seems reasonable if errors due to unwanted few-body qubit interactions can be eliminated by other methods [5, 6].

In conclusion, we have presented a novel approach to the stability of time-dependent quantum dynamics applied to the fidelity of quantum computation. For an uncorrelated time-dependent perturbation, the decay of fidelity does not depend on dynamics; however, for a static perturbation characterizing faulty gates the system is more stable, as reflected in a higher fidelity, the more 'chaotic' it is and the faster correlation decay it has. Our idea is demonstrated on the example of the QFT algorithm perturbed by a GUE matrix, devising an alternative QFT which is qualitatively more robust against a static random perturbation of the gates. It is an interesting question how this dynamical enhancement of stability relates to 'chaotic melting' of a static quantum computer [13].

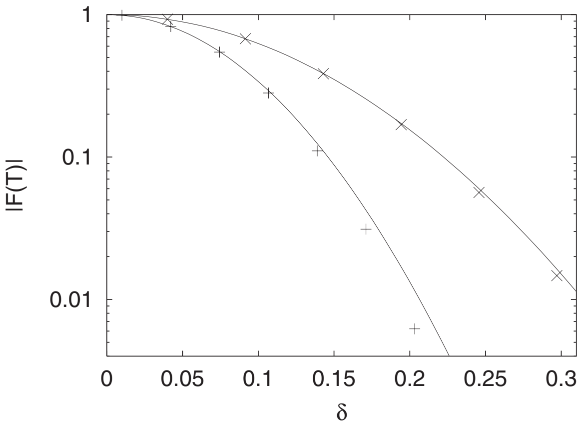

Figure 3. Dependence of fidelity $|\langle F(T)\rangle|$ on δ for QFT (pluses) and IQFT (crosses), for fixed $n = 8$. Solid curves are functions $\exp(-\chi\delta^2)$ (see the text) with χ calculated analytically (9) and equal to $\chi = 108$ for QFT and 46.6 for IQFT.

Discussions with T H Seligman are gratefully acknowledged. The work has been supported by the ministry of Education, Science and Sport of Slovenia.

References

[1] Feynman R P 1986 *Found. Phys.* **16** 507
[2] Nielsen M A and Chuang I L 2001 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
Steane A 1998 *Rep. Prog. Phys.* **61** 117
Ekert A and Jozsa R 1996 *Rev. Mod. Phys.* **68** 733
DiVincenzo D P 1995 *Science* **270** 255
[3] Shor P W 1994 *Proc. 35th Annu. Symp. on Foundations of Computer Science* ed S Goldwasser (Los Alamitos, CA: IEEE Computer Society Press)
Coppersmith D 1994 *IBM Research Report* RC19642
Deutsch D 1994 unpublished
[4] Chuang I L *et al* 1995 *Science* **270** 1633
[5] Steane A 1996 *Phil. Trans. R. Soc.* A **452** 2551
Calderbank A R and Shor P W 1996 *Phys. Rev.* A **54** 1098
[6] Tian L and Lloyd S 2000 *Phys. Rev.* A **62** R50301
[7] Gea-Banacloche J 1998 *Phys. Rev.* A **57** R1
Gea-Banacloche J 1999 *Phys. Rev.* A **60** 185
Gea-Banacloche J 2000 *Phys. Rev.* A **62** 62 313
[8] Song P H and Shepelyansky D L 2001 *Phys. Rev. Lett.* **86** 2162
(Georgeot B and Shepelyansky D L 2001 *Preprint* quant-ph/0101004)
Georgeot B and Shepelyansky D L 2001 *Phys. Rev. Lett.* **86** 5393
(Georgeot B and Shepelyansky D L 2001 *Preprint* quant-ph/0102082)
[9] Miguel C, Paz J P and Perazzo R 1996 *Phys. Rev.* A **54** 2606
Miguel C, Paz J P and Zurek W H 1997 *Phys. Rev. Lett.* **78** 3971
Cirac J I and Zoller P 1995 *Phys. Rev. Lett.* **74** 4091
[10] Peres A 1995 *Quantum Theory: Concepts and Methods* (Dordrecht: Kluwer) p 366
[11] Prosen T 2001 *Preprint* quant-ph/0106149
[12] Weinstein Y S *et al* 2001 *Phys. Rev. Lett.* **86** 1889
Vandersypen L M K *et al* 2000 *Phys. Rev. Lett.* **85** 5452
[13] Benenti G, Casati G and Shepelyansky D L 2000 *Preprint* quant-ph/0009084