PROGRAMMABLE QUANTUM PROCESSORS: PROBABILISTIC APPROACH

VLADIMíR BUŽEK[1,2], MÁRIO ZIMAN[1], AND MARK HILLERY[3]

[1] *Research Center for Quantum Information, Institute of Physics, Slovak Academy of Sciences, 845 11 Dúbravská cesta 9, Bratislava, Slovakia*

[2] *Department of Mathematical Physics, National University of Ireland, Maynooth, Co. Kildare, Ireland*

[1] *Department of Physics and Astronomy, Hunter College of CUNY, 695, Park Avenue, New York, NY 10021, U.S.A.*

We discuss a concept of universal quantum processors. The processor itself is represented by a fixed array of gates. The input of the processor consists of two registers. In the program register the set of instructions (program) is encoded. This program is applied to the data register. In general one can consider two types of processors: deterministic programmable processors and probabilistic processors. In this paper we consider processors that can perform any operation on a single qudit of the dimension N with a certain probability (probabilistic processors). If the operation is unitary, the probability is in general $1/N^2$, but for more restricted sets of operators the probability can be higher. We show that this probability can be when the processor is used in loops with special error correcting program states. We also consider programmable measurement devices that can perform specific generalized measurement that are determined by the

1 Introduction

Schematically we can represent a classical computer as a device with a processor, which is a fixed piece of hardware, that performs operations on a *data* register according to a program encoded initially in the *program* register. The action of the processor is fully determined by the program. The processor is *universal* if we can realize *any* operation on the data by entering the appropriate program into the program register.

In this paper we shall examine a quantum version of this picture. Specifically, in close analogy with recent papers by Nielsen and Chuang [1] and Vidal, Massanes, and Cirac [2], we will study how a quantum program initially put into a program register can cause a particular operation to be applied to a data register initially prepared in an unknown state.

Nielsen and Chuang [1] originally formulated the problem in terms of a programmable array of quantum gates, which can be described as a fixed unitary operator, P_{dp}, that acts on both the program and the data. The initial state, $|\Theta_U\rangle_p$, of the program register stores information about the one-qubit unitary transformation U that is going to be performed on a single-qubit data register initially prepared in a state $|\psi\rangle_d$. The total dynamics of the programmable quantum gate array is then given by

$$P_{dp}\left[|\psi\rangle_d \otimes |\Theta_U\rangle_p\right] = (U|\psi\rangle_d) \otimes |\tilde{\Theta}_U\rangle_p, \tag{1}$$

where only pure data states were considered. The program register at the output of the gate is in the state $|\tilde{\Theta}_U\rangle_p$ - which was shown to be independent of the input data state $|\psi\rangle_d$.

Nielsen and Chuang proved that any two *inequivalent* operations U and V require orthogonal program states, i.e. $\langle\Theta_U|\Theta_V\rangle = 0$. Thus, in order to perfectly store a given operation U_j from some set $\{U_j|j \in J\}$, a vector state $|\Theta_{U_j}\rangle$ from an orthonormal basis $\{|\Theta_{U_j}\rangle|j \in J\}$ has to be used. Since the set of unitary operations is infinite, the result of Nielsen and Chuang implied that no universal gate array can be constructed using finite resources, that is, with a finite dimensional program register. They did show, however, that if the gate array is probabilistic, a universal gate array is possible. A probabilistic array is one that requires a measurement to be made at the output of the program register, and the output of the data register is only accepted if a particular result, or set of results, is obtained. This will happen with a probability, which is less than one.

Vidal, Massanes and Cirac [2] have recently presented a probabilistic programmable quantum gate array with a finite program register, which can realize a one parameter family of operations, where the parameter is continuous, with arbitrarily high probability. The higher the probability of success, the greater the dimensionality of the register, but the number of transformations that can be realized is infinite. They have also considered *approximate* programmable quantum gate arrays, which perform an operation E_U very similar to the desired U, that is $F(E_U, U) \geq 1 - \epsilon$ for some transformation fidelity F.

In the present paper we will address the problem of implementing an unknown operation U, encoded in the state of a program register $|\Theta_U\rangle_p$, on the data state $|\psi\rangle_d$. The gate arrays we present are probabilistic; the program register must be measured at the end of the procedure. In Section II we present a simple example of how to apply an arbitrary operation to a single qubit initially prepared in a state $|\psi\rangle$. The gate array (called *quantum information distributor*) consists of four Controlled-NOT (C-NOT) gates, and can implement four programs perfectly. These programs cause that one of the operations I, σ_x, $-i\sigma_y$, or σ_z is performed on the data qubit. Here I is the identity and σ_j, where $j = x, y, z$ is a Pauli matrix. By choosing programs that are linear combinations of the four basic ones, it is possible to probabilistically perform any linear operation on the data qubit. In Section III we generalize the idea to an arbitrary dimensional quantum system, a qudit.

2 Operations on qubits

We would like to construct a device that will do the following: The input consists of a qubit, $|\psi\rangle_d$, and a second state, $|\Theta_U\rangle_p$, which may be a multiqubit state, that acts as a program. The output of the device will be a state $U|\psi\rangle_d$, where U is an operation that is specified by $|\Theta_U\rangle_p$. Can we find a network and a program vector to implement all unitary operations on $|\psi\rangle_d$?

We can, in fact, do this by using the network for a quantum information distributor (QID) as introduced in Ref. [3] (this is a modification of the quantum cloning transformation [4,5]). In this network the program register is represented by a two qubit state $|\Theta_A\rangle_p$. Before we present the network for the programmable gate array, we shall introduce notation for its components. A Controlled-NOT gate D_{jk} acting on qubits j and k performs the transformation,

$$D_{jk}|m\rangle_j|n\rangle_k = |m\rangle_j|m \oplus n\rangle_k, \tag{2}$$

where j is the control bit, k is the target bit, and m and n are either 0 or 1. The addition is modulo 2. The QID network consists of four Controlled-NOT gates, and acts on three qubits (a single data qubit denoted by a subscript 1 and two program qubits denoted by subscripts 2 and 3, respectively). Its action is given by the operator $P_{123} = D_{31}D_{21}D_{13}D_{12}$. As our first task, we shall determine how this network acts on input states where qubit 1 is in the state $|\psi\rangle$, and qubits 2 and 3 are in Bell basis states. The Bell basis states are defined by

$$\begin{aligned}
|\Phi_+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \equiv |\Theta_{01}\rangle\,; \qquad |\Phi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \equiv |\Theta_{11}\rangle\,;\\
|\Psi_+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \equiv |\Theta_{00}\rangle\,; \qquad |\Psi_-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \equiv |\Theta_{10}\rangle\,. (3)
\end{aligned}$$

We find that

$$\begin{aligned}
P_{123}|\psi\rangle_1|\Phi_+\rangle_{23} &= (\sigma_x|\psi\rangle_1)|\Phi_+\rangle\,;\\
P_{123}|\psi\rangle_1|\Phi_-\rangle_{23} &= (-i\sigma_y|\psi\rangle_1)|\Phi_-\rangle\,;\\
P_{123}|\psi\rangle_1|\Psi_+\rangle_{23} &= |\psi\rangle_1)|\Psi_+\rangle\,;\\
P_{123}|\psi\rangle_1|\Psi_-\rangle_{23} &= (\sigma_z|\psi\rangle_1)|\Psi_-\rangle.
\end{aligned} \tag{4}$$

Any operation on qubits can be expanded in terms of Pauli matrixes and the identity. The above equations mean that the Bell basis vectors are "programs" for a complete set of operations.

We now need to determine whether there is a program for any operator that could act on $|\psi\rangle$. The operator need not be unitary; it could be a result of coupling $|\psi\rangle$ to an ancilla, evolving the coupled system (a unitary process), and then measuring the ancilla. Therefore, if A is now any linear operator acting on a two dimensional quantum system, the transformations in which we are interested are given by

$$|\psi\rangle \rightarrow \frac{1}{\|A\psi\|}A|\psi\rangle. \tag{5}$$

Let us denote the operators, which can be implemented by Bell state programs, by $S_{00} = I$, $S_{01} = \sigma_x$, $S_{10} = \sigma_z$, and $S_{11} = -i\sigma_y$. Any 2×2 matrix can be expanded in terms of these operators, so that we have

$$A = \sum_{j,k=0}^{1} \tilde{a}_{jk} S_{jk}. \tag{6}$$

We now define $a_{jk} = \tilde{a}_{jk}/\sqrt{\eta}$, where $\eta = \sum_{j,k=0}^{1} |\tilde{a}_{jk}|^2$, so that $1 = \sum_{j,k=0}^{1} |a_{jk}|^2$.

Now let us go back to our network and consider the program vector given by

$$|\Theta_A\rangle = \sum_{j,k=0}^{1} a_{jk} |\Theta_{jk}\rangle, \tag{7}$$

and at the output of the program register we shall measure the projection operator corresponding to the vector $(1/2)\sum_{j,k=0}^{1} |\Theta_{jk}\rangle$. If the measurement is successful, the state of the data register is, up to normalization, given by

$$|\psi\rangle \rightarrow \left(\sum_{j,k=0}^{1} a_{jk} S_{jk} \right) |\psi\rangle . \tag{8}$$

After this state is normalized, it is just $(1/\|a\psi\|)|\psi\rangle$. This means that for any transformation of the type given in Eq. (5), we can find a program for our network that will carry it out.

3 QID: Generalization to qudits

In order to extend the network presented in the previous section to higher dimensions, we must first introduce a generalization of the two-qubit C-NOT gate [3]. As we noted previously, it is possible express the action of a C-NOT gate as a two-qubit operator of the form

$$D_{ab} = \sum_{k,m=0}^{1} |k\rangle_a \langle k| \otimes |m \oplus k\rangle_b \langle m| \, . \tag{9}$$

In principle one can also introduce an operator $D_{ab}^{\dagger}$ defined as

$$D_{ab}^{\dagger} = \sum_{k,m=0}^{1} |k\rangle_a \langle k| \otimes |m \ominus k\rangle_b \langle m| \, . \tag{10}$$

In the case of qubits these two operators are equal, but this will not be the case when we generalize the operator to Hilbert spaces whose dimension is larger than 2 [3]. In particular, we can generalize the operator D for dimension $N > 2$ by defining

$$D_{ab} = \sum_{k,m=0}^{N-1} |k\rangle_a \langle k| \otimes |(m + k) \mathrm{mod}\, N\rangle_b \langle m| \, , \tag{11}$$

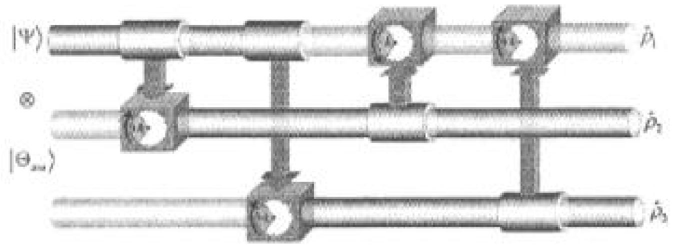

Figure 1. A logic network for the universal quantum processor as given by the unitary transformation (15).

which implies that

$$D^{\dagger}_{ab} = \sum_{k,m=0}^{N-1} |k\rangle_a\langle k| \otimes |(m-k) \bmod N\rangle_b\langle m| \, . \tag{12}$$

From this definition it follows that the operator D_{ab} acts on the basis vectors as

$$D_{ab}|k\rangle|m\rangle = |k\rangle|(k+m) \bmod N\rangle \, , \tag{13}$$

which means that this operator has the same action as the conditional adder and can be performed with the help of the simple quantum network discussed in [6]. Now we see that for $N > 2$ the two operators D and $D^{\dagger}$ do differ; they describe conditional shifts in opposite directions. Therefore the generalizations of the C-NOT operator to higher dimensions are just *conditional shifts*.

In analogy with the quantum computational network discussed in the previous section, we assume the network for the probabilistic universal quantum processor to be

$$P_{123} = D_{31}D^{\dagger}_{21}D_{13}D_{12} \, . \tag{14}$$

The data register consists of system 1 and the program register of systems 2 and 3. The state $|\Theta_U\rangle_{23}$ acts as the "software" which the operation to be implemented on the qudit data state $|\Psi\rangle_1$. The output state of the three qudit system, after the four controlled shifts are applied, reads

$$|\Omega\rangle_{123} = D_{31}D^{\dagger}_{21}D_{13}D_{12}|\Psi\rangle_1|\Theta_U\rangle_{23} \, . \tag{15}$$

A graphical representation of the logical network (15) with the conditional shift gates D_{ab} in Fig. 1.

We now turn to the fundamental program states. A basis consisting of maximally entangled two-particle states (the analogue of the Bell basis for spin-$\frac{1}{2}$ particles) is given by [7]

$$|\Theta_{mn}\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\Big(i\frac{2\pi}{N}mk\Big)|k\rangle|(k-n)\mathrm{mod}\,N\rangle\,, \tag{16}$$

where $m, n = 0, \ldots, N-1$. If $|\Theta_{mn}\rangle_p$ is the initial state of the program register, and $|\Psi\rangle = \sum_j \alpha_j |j\rangle_d$ (here, as usual, $\sum_j |\alpha_j|^2 = 1$) is the initial state of the data register, then (after little algebra) follows that [8]

$$P_{123}|\Psi\rangle_1|\Theta_{mn}\rangle_{23} = (U^{(mn)}|\Psi\rangle)|\Theta_{mn}\rangle, \tag{17}$$

where the fundamental unitary transformations

$$U^{(mn)} = \sum_{s=0}^{N-1} \exp\frac{-2i\pi sm}{N}|s-n\rangle\langle s|. \tag{18}$$

This result is similar to the one we found in the case of a single qubit. We would now like to examine which transformations we can perform on the state in the data register by using a program consisting of a linear combination of the vectors $|\Theta_{mn}\rangle$ followed by the action of the processor P_{123} and a subsequent measurement of the program register.

The operators $U^{(mn)}$ satisfy the orthogonality relation

$$\mathrm{Tr}\left[(U^{(m'n')})^\dagger U^{(mn)}\right] = N\delta_{mm'}\delta_{nn'}. \tag{19}$$

The space of linear operators $\mathcal{T}(\mathcal{H})$ defined on some Hilbert space $\mathcal{H}$ with the scalar product given by (19) we know as *Hilbert-Schmidt space*. Thus the unitary operators $U^{(mn)}$ form an orthogonal basis in it and any operator $A \in \mathcal{T}(\mathcal{H})$ can be expressed in terms of them

$$A = \sum_{m,n=0}^{N-1} q_{mn}U^{(mn)}. \tag{20}$$

The orthogonality relation allows us to find the expansion coefficients in terms of the operators

$$q_{mn} = \frac{1}{N}\mathrm{Tr}\left[\left(U^{(mn)}\right)^\dagger A\right]. \tag{21}$$

Equations (19) and (20) imply that

$$\sum_{m,n=0}^{N-1} |q_{mn}|^2 = \frac{1}{N}\mathrm{Tr}(A^\dagger A). \tag{22}$$

Therefore, the program vector that implements the operator A is given by

$$|v_A\rangle_{23} = \left[\frac{N}{\mathrm{Tr}(A^\dagger A)}\right]^{1/2} \sum_{m,n=0}^{N-1} q_{mn}|\Theta_{mn}\rangle_{23}. \tag{23}$$

Application of the processor to the input state $|\Psi\rangle_1|v_A\rangle_{23}$ yields the output state

$$|\Omega\rangle_{123} = \sum_{mn} q_{mn} U^{(mn)}|\Psi\rangle_1 \otimes |\Theta_{mn}\rangle_{23}. \tag{24}$$

To obtain the final result we perform a projective measurement of the program register onto vector $|M\rangle = \frac{1}{N}\sum_{m,n=0}^{N-1}|\Theta_{mn}\rangle$ If the outcome of the measurement is positive, then we get the required transformation A acting on an unknown, arbitrary input state $|\Psi\rangle_1$. In this case the probability of success is $1/N^2$.

4 Perspectives

4.1 Amplification of the probability of success

We have shown that using the QID processor the probability of the implementation of any unitary transformation on a qudit is $p = 1/N^2$, where N denotes the dimension of the qudit (data) Hilbert space. For a certain subclasses of unitary transformations we can do better [9], i.e. the probability can be increased. The question is whether the probability of success can be made arbitrarily close to unity. Unfortunately this upper bound cannot be achieved, because no universal deterministic processor can be designed (for review on deterministic regime of quantum processors see Hillery et al. [10,?]).

However, using a conditional type of dynamics (in accordance with Vidal, Massanes and Cirac proposal [2]) the probability can be made arbitrarily close to unity [9]. In this scenario we used conditioned loops to correct those runs of the processors with wrong results. In particular, it is possible to correct the action of the QID processor by using the same processor many times and always initialize a new program state with respect to the measurement outcome. For n repetitions the success probability equals $p = 1-[1-1/N^2]^n$, where N is the dimension of the data register.

4.2 Implementation of generalized measurements

For a given processor only a subset of all program states can be used to encode a unitary transformation[10,11]. For all others program states the resulting transformation is not linear. Measuring the outcome j the data state transforms according to the rule

$$\varrho \to \varrho_j' = \frac{1}{p_j}\sqrt{F_j}\varrho\sqrt{F_j} \tag{25}$$

where $p_j = \mathrm{Tr}\varrho F_j$ is the probability of the particular outcome. Because this probability depends on ϱ, this transformation does not satisfy the linearity criterion. Note that if unitary transformation is realized (on QID), then $F_j = U_j U_j^\dagger/N^2 = I/N^2$ for all j, and consequently $p_j = 1/N$. However, if the transformation is non-unitary, then the probability distribution p_j is not constant and it contains some information about the initial state of the data. So the probabilistic processor can be exploited to implement generalized measurements of the data system. For instance, QID can be used to realize complete state reconstruction of the qubit state [11,12].

4.3 Universal programmable measurement devices

Using the concept of programmable quantum processors one can design universal programmable measurement devices (programmable quantum multimeters [13,14]) that can realize any generalized measurement from a *chosen*, but finite, set of measurements (see also [15]). Here again the performed POVM is determined by a state of the program register.

Acknowledgments

This work was supported in part by the European Union projects QGATES and QUPRODIS, and by the National Science Foundation under the grant PHY-9970507. One of us (V.B.) would like to thank the Science Foundation Ireland for support.

References

1. M. A. Nielsen and I. L. Chuang, Phys. Rev. Lett. **79**, 321 (1997)
2. G. Vidal, L. Massanes, and J.I. Cirac, Phys. Rev. Lett. **88**, 047905 (2002).
3. S. Braunstein, V. Bužek, and M. Hillery, *Phys. Rev. A* **63**, 052313 (2001).
4. V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
5. V. Bužek, S. Braunstein, M. Hillery, and D. Bruß, Phys. Rev. A **56**, 3446 (1997).
6. V. Vedral, A. Barenco, and A. Ekert, Phys. Rev. A **54**, 147 (1996).
7. D. I. Fivel, Phys. Rev. Lett. **74**, 835 (1995).
8. M.Hillery, V.Bužek, and M.Ziman, Phys. Rev. A **65**, 022301 (2002).
9. M.Ziman, M.Hillery, and V.Bužek Phys. Rev. A, submitted.
10. M.Hillery, M.Ziman, and V.Bužek Phys. Rev. A **66**, 042302 (2002).
11. M.Ziman, M.Hillery, V.Bužek in preparation
12. M.Roško, V.Bužek, P.R.Chouha, and M.Hillery, Phys. Rev. A, submitted.
13. M. Dušek and V.Bužek, Phys. Rev. A **66**, 022112 (2002)
14. M. Dušek, J.Fiurášek, M.Hendrych, and V.Bužek, in these proceedings.
15. G.M.D'Ariano, in these proceedings.