Communication Capacities of Some Quantum Gates, Discovered in Part through Genetic Programming (with additional figures from the QCMC 2002 poster)

Lee Spector
Cognitive Science
Hampshire College
Amherst, MA 01002, USA
lspector@hampshire.edu

Herbert J. Bernstein
Institute for Science and Interdisciplinary Studies (ISIS) &
Natural Science
Hampshire College
Amherst, MA 01002, USA
hjbNS@hampshire.edu

ABSTRACT

We explore tradeoffs between classical communication and entanglement-generating powers of unitary 2-qubit gates. The exploration is aided by a computational search technique called genetic programming.

This paper, without the additional figures that follow the references, will appear in *Proceedings of the Sixth International Conference on Quantum Communication, Measurement, and Computing* (QCMC), July 22–26, 2002, to be published by Rinton Press.

COMMUNICATION CAPACITIES OF SOME QUANTUM GATES, DISCOVERED IN PART THROUGH GENETIC PROGRAMMING

LEE SPECTOR

Cognitive Science, Hampshire College, Amherst, MA 01002, USA
E-mail: lspector@hampshire.edu

HERBERT J. BERNSTEIN

Institute for Science and Interdisciplinary Studies (ISIS) &
Natural Science, Hampshire College, Amherst, MA 01002, USA
E-mail: hjbNS@hampshire.edu

We explore tradeoffs between classical communication and entanglement-generating powers of unitary 2-qubit gates. The exploration is aided by a computational search technique called genetic programming.

The question of tradeoffs between classical communication and entanglement-generating powers of unitary transformations in quantum computation has great current interest.[1] If simple general rules of tradeoff are worked out, the power of a transformation U to benefit bi-partite interactions will be characterized by a single number, thus abetting and advancing the "resource" or commodity metaphor for quantum information. Bennett has theorized that a single use of any given two-particle transformation U has a unique maximum power for entanglement or communication (forward, backward or two-way) between Alice and Bob. Which of these various effects U produces would depend on the protocol in which it is embedded. The rule is that only U may connect Alice to Bob, as in the previous investigation of two-qubit Hamiltonian interactions epitomized by the myth of Pyramis and Thisbe.[2] The question is how many c-bits of communication and/or e-bits of entanglement one can create per U. The search for algorithms to deploy this power with or without ancilla, and with or without prior entanglement, begins the general work on Bennett's conjecture. In principle the power of U may require asymptotic ratios of the number of e- or c-bits generated to instances of U deployed in the algorithm.

We pursue the search for algorithms relevant to this study using a computational search technique called genetic programming (GP). In prior work we used GP to discover new quantum algorithms for determining properties of unitary oracles.[3] In the present work we used the PushGP GP system[4] (http://hampshire.edu/lspector/push.html) in conjunction with the QGAME quantum computer simulator (http://hampshire.edu/lspector/qgame.html).

We first consider the 2-bit Smolin gate suggested by Smolin (personal communication) and shown in Figure 1 (along with the matrices for most other gates mentioned in this paper). Smolin suggested this gate, which obviously

$$SMOLIN \equiv \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \end{bmatrix} \quad J(\theta) \equiv \begin{bmatrix} cos(\theta) & 0 & 0 & sin(\theta) \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ sin(\theta) & 0 & 0 & -cos(\theta) \end{bmatrix} \quad SWAP \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$BS(\theta) \equiv \begin{bmatrix} cos(\theta) & 0 & 0 & sin(\theta) \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ sin(\theta) & 0 & 0 & -cos(\theta) \end{bmatrix} \quad CNOT \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad CPHASE \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\alpha} \end{bmatrix}$$

$$U_\theta \equiv \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix} \quad H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad QNOT \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad SRN \equiv \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}$$

Figure 1. Matrices for gates used in this paper.

generates entanglement, as a potential counterexample to Bennett's conjecture, suggesting that this gate could produce one bit of entanglement per use but that it could not communicate. We show here that the Smolin gate *can* communicate one c-bit per use, either forward or backward, with no error and no ancilla. The algorithm evolved by GP is as follows: Initialize both qubits to 0 (qubit 0 is Alice's and qubit 1 is Bob's). Alice leaves her qubit unchanged to send a 0 or flips it to send a 1. Execute: $U_{-\frac{\pi}{4}}$ on qubit 1; $QNOT$ on qubit 0; $U_{\frac{\pi}{8}}$ on qubit 0; square-root-of-not (SRN) on qubit 0; $SMOLIN$ on qubits 1 and 0; $U_{-\frac{\pi}{4}}$ on qubit 1. Bob reads the bit from qubit 1 with no probability of error. By symmetry, Bob and Alice's roles could be reversed for backward classical communication (B to A). Gate array diagrams for the algorithms in this paper can be found at http://hampshire.edu/lspector/qcmc-figures.pdf.

We analyzed the evolved algorithm and, in conjunction with our work on a generalized Smolin gate (below), realized that could be expressed more simply as follows: Initialize both qubits to 0. Alice leaves qubit 0 in the 0 state to send a 0 or flips it to send a 1. Execute: $U_{\frac{\pi}{8}}$ on qubit 0; $QNOT$ on qubit 1; $U_{\frac{3\pi}{4}}$ on qubit 1; $SMOLIN$ on qubits 0 and 1; $U_{\frac{3\pi}{4}}$ on qubit 1. Bob reads from qubit 1 with no probability of error.

We recognized the relation between $\frac{\pi}{8}$ in this algorithm and the $\frac{\pi}{4}$ implicit in the Smolin gate and developed a family of gates generalizing this angle. $J(\theta)$ (see Figure 1) defines a one-parameter family of gates, all square roots of identity, for which the perfect 1 c-bit communication strategy is an obvious generalization of the strategy we discovered for the Smolin gate. In fact, the entire family of gates, which runs from $CPHASE$ through Smolin (at $\theta = \frac{\pi}{4}$) to a version of $SWAP$ as θ ranges from 0 to $\frac{\pi}{2}$, can be used for perfect communication, forward or back, using our strategy and no prior entanglement or ancilla. The following scheme was discovered by human analysis (GP independently found equivalent results): Initialize both qubits to 0. Alice leaves qubit 0 unchanged to send a 0 or flips it to send a 1. Execute: $U_{\frac{\theta_j}{2}}$ on qubit 0, where θ_j is the value of θ used in J below; $QNOT$ on qubit 1; $U_{\frac{3\pi}{4}}$ on qubit 1; $J(\theta)$ on qubits 0 and 1; $U_{\frac{3\pi}{4}}$ on qubit 1. Bob reads from

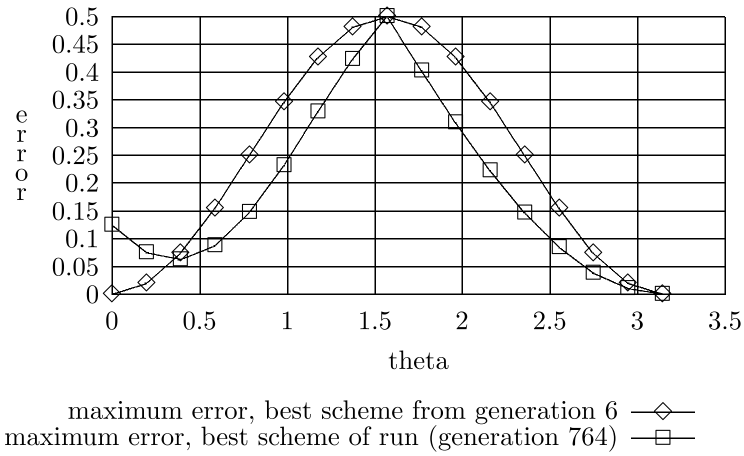

Figure 2. Errors of some evolved strategies for communicating a bit through $BS(\theta)$ with no ancilla and no prior entanglement for various values of θ. The worst case error of a scheme found early in evolution is equivalent to $\frac{sin^2(\theta)}{2}$. A peculiar strategy (using different gates for different θ) found in generation 764 does worse for small θ but better elsewhere.

qubit 1 with no probability of error.

After discovering that the Smolin gate *could* be used for exact communication we developed a new gate that appears to block communication while nonetheless entangling; that is, it seems to fulfill Smolin's initial intent. We define $BS(\theta)$ as in Figure 1. This ranges from $SWAP \times CPHASE$ through a modified Smolin ($SMOLIN \times SWAP$) to $QNOT \times QNOT$ as θ ranges from 0 to $\frac{\pi}{2}$. Clearly the $\frac{\pi}{2}$ endpoint, as a product of local transformations, can neither communicate nor entangle. For other angles this gate can entangle and has some communication potential. Search by GP has thus far discovered error-free communication strategies through $BS(\theta)$ without ancilla only at θ mod $\pi = 0$; see Figure 2.

Although we suspect that perfect communication through $BS(\frac{\pi}{4})$ is not possible without prior entanglement, it is indeed possible with one bit of prior entanglement. The following algorithm was found by GP: Initialize both qubits to 0. Then provide entanglement by executing a Hadamard (H) gate on qubit 0 and a controlled-not ($CNOT$) gate with qubit 0 as the control and qubit 1 as the target. Alice then leaves qubit 0 unchanged to send a 0 or flips it to send a 1. Execute: H on qubit 0; H on qubit 1; $BS(\frac{\pi}{4})$ on qubits 0 and 1. Bob reads from qubit 1 with no probability of error. Note that Bob may also use spin-flip choice to simultaneously send 1 bit to Alice.

Knowing that $BS(\pi)$ can communicate one bit with no prior entanglement, we employed GP to find out if a single execution of $BS(\pi)$, in the presence of one bit of prior entanglement, could communicate 2 bits without error. GP found a way, as follows: Initialize four qubits to 0. Then provide prior entanglement by executing H on qubit 1 and $CNOT$ with qubit 1 as the control and qubit 3 as the target. Qubits 0 and 1 are Alice's and qubits 2 and 3 are Bob's. Alice leaves her qubits unchanged to send 0s or flips them to send 1s. Then execute: $CPHASE(\pi)$ on qubit 0 (control) and qubit 1 (target); $BS(\pi)$ on qubits 2 and 1; $CNOT$ on qubits 2 and 3; $U_{\frac{7\pi}{4}}$ on qubit 2. Bob reads the message from qubits 2 and 3 with no probability of error. Qubit 2 will contain the message set by Alice in qubit 0, and qubit 3 will contain the message set by Alice in qubit 1. This is equivalent to dense coding.

Our work on $BS(\theta)$ and $J(\theta)$ led us to an understanding of the importance of the eigenvalue/eigenvector expansion of these gates. In particular there is a close relation between the communication potential of $J(\theta)$ and the presence of an odd number of positive eigenvalues, as opposed to the lack of communication potential of $BS(\theta)$ where there are an even number of positive eigenvalues. Later analytical investigation shows that $BS(\theta)$ for $0 < \theta < \frac{\pi}{4}$ can always entangle a full e-bit of entanglement, too. And of course multiple uses of $BS(\frac{\pi}{4})$—still in the absence of ancilla—can also communicate one bit per gate. This is accomplished in two steps, by alternating a stage of entanglement generation with a stage of the entanglement-consuming 2-way communication mentioned above. But even this strategy fails to close the apparent gap between the entanglement and communication power of $BS(\theta)$ for $0 < \theta < \frac{\pi}{4}$. The two fully entangled states one generates in this case are non-orthogonal. They image distinct non-orthogonal product states whose restoration in stage 2 cannot unerringly signal a c-bit to both Alice and Bob.

Acknowledgments

We thank C. H. Bennett, A. Harrow, D. W. Leung, and J. A. Smolin for discussions. This effort was supported by the Defense Advanced Research Projects Agency (DARPA) and Air Force Research Laboratory, Air Force Materiel Command, USAF, under agreement number F30502-00-2-0611, and by NSF grant PHY-9722614. Support was also provided by Hampshire College for the Institute for Computational Intelligence and for ISIS.

References

1. D. Collins, N. Linden, and S. Popescu. *Phys. Rev. A* **64**, 032302 (2001), quant-ph/0005102 (2000).
2. C.H. Bennett, J.I. Cirac, M.S. Leifer, D.W. Leung, N. Linden, S. Popescu, and G. Vidal. *Phys. Rev. A* **66**, 012305 (2002), quant-ph/0107035 (2001), *cf.* H.J. Bernstein unpubl. talks (Jun 2001).
3. H. Barnum, H.J. Bernstein, and L. Spector. *J. Phys. A: Mathematical and General* **33(45)**, 8047–8057 (2000).
4. L. Spector and A. Robinson. *Genetic Programming and Evolvable Machines* **3**, 7–40 (2002).

Additional Figures

The remainder of this document contains additional figures from the poster presentation "Communication Capacities of Some Quantum Gates, Discovered in Part through Genetic Programming," by Lee Spector and Herbert J. Bernstein, presented at the *Sixth International Conference on Quantum Communication, Measurement, and Computing* (QCMC), July 22–26, 2002, on the campus of the Massachusetts Institute of Technology.

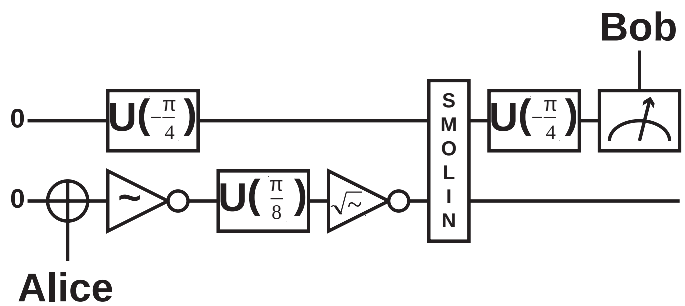

Figure 3. Genetic programming found this zero-error, one c-bit communication protocol for the Smolin gate.

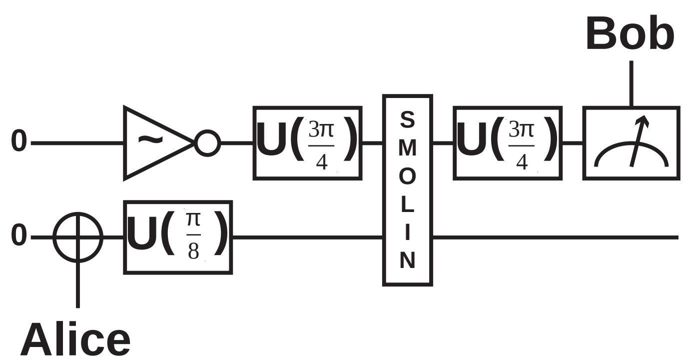

Figure 4. A simpler expression of the Smolin protocol that was discovered by genetic programming.

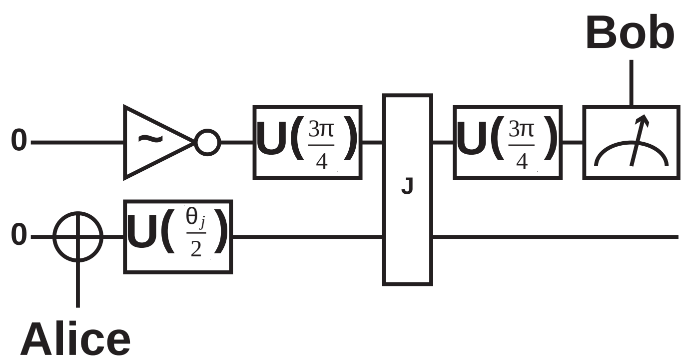

Figure 5. The strategy discovered for the Smolin gate works for any instance of $J(\theta)$ with zero error.

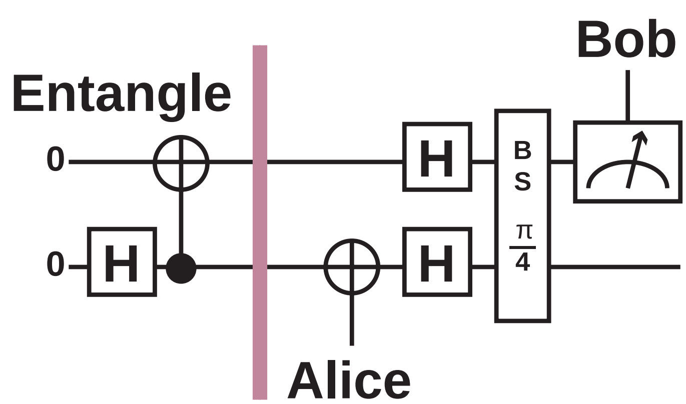

Figure 6. With one bit of prior entanglement we can communicate one c-bit through $BS(\frac{\pi}{4})$ without error (discovered by genetic programming).

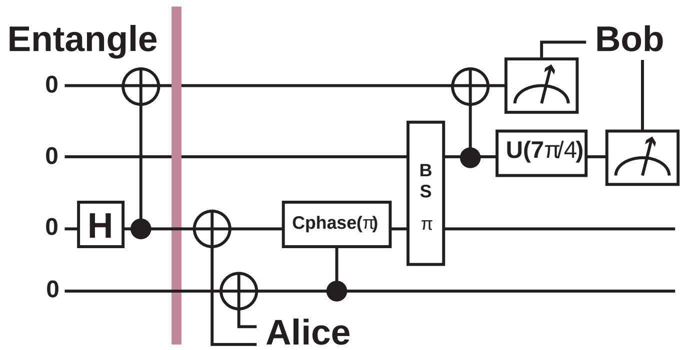

Figure 7. With one bit of prior entanglement we can communicate two c-bits through $BS(\pi)$ without error (discovered by genetic programming).

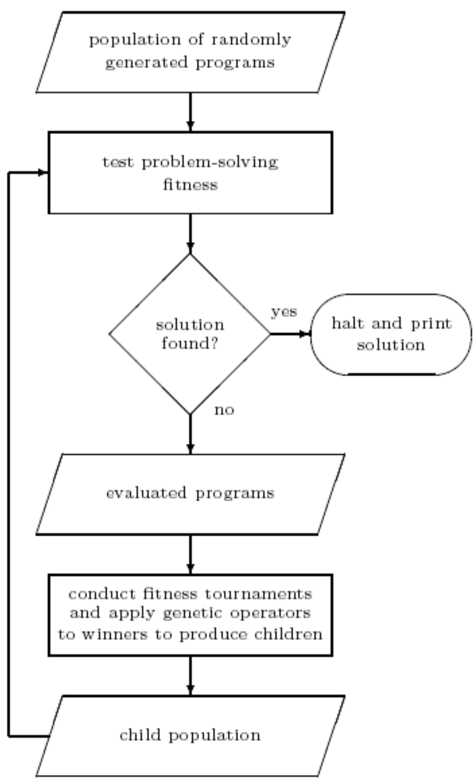

Figure 8. Flowchart of the genetic programming algorithm.

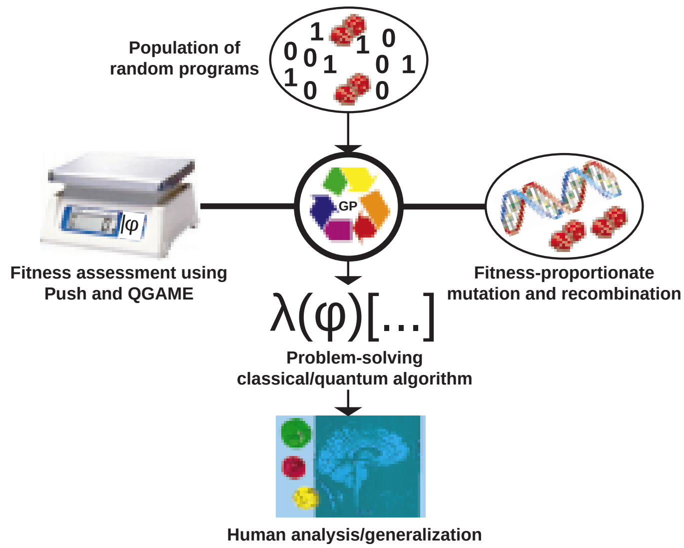

Figure 9. Graphic overview of the use of genetic programming for exploration of quantum algorithms.

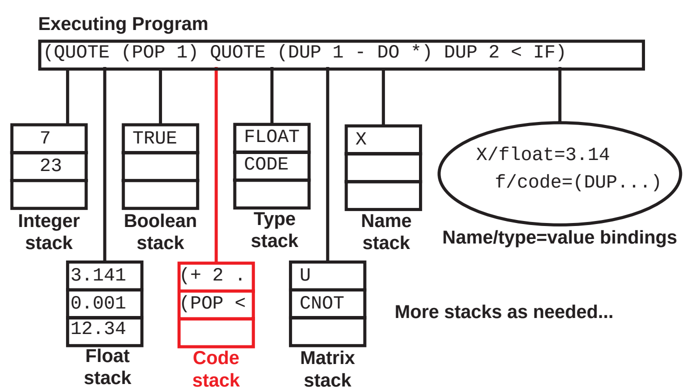

Figure 10. Execution architecture of the Push programming language.

Figure 11. Graphical user interface of the QGAME quantum computer simulator.