Phys. Rev. Lett. **82** (1999) 1052–1055.

6 February 1998
quant-ph/9804010

QUANTUM STRATEGIES

David A. Meyer

Project in Geometry and Physics
Department of Mathematics
University of California/San Diego
La Jolla, CA 92093-0112
dmeyer@chonji.ucsd.edu
and Center for Social Computation/Institute for Physical Sciences
Los Alamos, NM

ABSTRACT

We consider game theory from the perspective of quantum algorithms. Strategies in classical game theory are either pure (deterministic) or mixed (probabilistic). While not every two-person zero-sum finite game has an equilibrium in the set of pure strategies, von Neumann showed that there is always an equilibrium at which each player follows a mixed strategy. A mixed strategy deviating from the equilibrium strategy cannot increase a player's expected payoff. We show by example, however, that a player who implements a quantum strategy *can* increase his expected payoff, and explain the relation to efficient quantum algorithms.

1998 Physics and Astronomy Classification Scheme: 03.67.-a, 03.67.Lx, 02.50.Le.
American Mathematical Society Subject Classification: 81P15, 90D05.
Journal of Economic Literature Classification System: C72.
Key Words: quantum computation; game theory.

Attention to the physical representation of information underlies the recent theories of quantum computation, quantum cryptography and quantum communication. In each case representation in a quantum system provides advantages over the classical situation: Simon's quantum algorithm to identify the period of a function chosen by an oracle is more efficient than any deterministic or probabilistic algorithm [1] and provided the foundation for Shor's polynomial time quantum algorithm for factoring [2]. The quantum protocols for key distribution devised by Wiesner, Bennett and Brassard, and Ekert are qualitatively more secure against eavesdropping than any classical cryptosystem [3]. And Cleve and Buhrman, and van Dam, Høyer and Tapp have shown that prior quantum entanglement reduces communication complexity [4]. In this letter we add game theory to the list: quantum strategies can be more successful than classical ones.

While this result may seem obscure or surprising, in fact it is neither. Cryptographic situations, for example, are readily conceived as games; it is reasonable to ask if the advantages of quantum key distribution generalize. Game theory, on the other hand, seems to beg for a quantum version: Classical strategies can be pure or mixed; the correspondence of this nomenclature, due to von Neumann [5], with that of quantum mechanics is surely no accident [6]. Furthermore, games against nature, originally studied by Milnor [7], should include those for which nature is quantum mechanical—this is exactly the setting for quantum error correcting codes [8]. Finally, in their extensive form, games are represented by 'trees' [5], just as are (quantum) algorithms [1]. We will exploit this similarity to analyze the effectiveness of quantum strategies, exemplified in the following very simple game:

PQ Penny Flip: The starship *Enterprise* is facing some imminent—and apparently inescapable—calamity when Q appears on the bridge and offers to help, provided Captain Picard* can beat him at penny flipping: Picard is to place a penny head up in a box, whereupon they will take turns (Q, then Picard, then Q) flipping the penny over (or not), without being able to see it. Q wins if the penny is head up when they open the box.

This is a two-person zero-sum strategic game which might be analyzed traditionally using the payoff matrix:

	NN	NF	FN	FF
N	-1	1	1	-1
F	1	-1	-1	1

where the rows and columns are labelled by Picard's and Q's *pure strategies*, respectively; F denotes a flip and N denotes no flip; and the numbers in the matrix are Picard's payoffs: 1 indicating a win and -1 a loss.† For example, consider the top entry in the second column: Q's strategy is to flip the penny over on his first turn and then not flip it

* Captain Picard and Q are characters in the popular American television (and movie) series *Star Trek: The Next Generation* whose initials and abilities are ideal for this illustration. See [10].

† Since when one player wins, the other loses, we need only list one player's payoffs; whenever this is the case the game is called *zero-sum*. *Strategic* refers to the fact that the players choose their strategies independently of the other player's actions [11,5].

on his second, while Picard's strategy is to not flip the penny on his turn. The result is that the state of the penny is, successively: H, T, T, T, so Picard wins.

Having studied game theory in his Advanced Decision Making course at Starfleet Academy, Captain Picard has no difficulty determining his optimal strategy: Suppose he doesn't flip the penny. Then if Q flips it an even number of times, Picard loses. Similarly, if Picard flips the penny over, then if Q flips it over only once, Picard loses. Thus PQ PENNY FLIP has no deterministic solution [5], no deterministic Nash equilibrium [12]: there is no pair of pure strategies, one for each player, such that neither player can improve his result by changing his strategy while the other player does not. But, as von Neumann proved there must be [11,5], since this is a two-person zero-sum strategic game with only a finite number of strategies, there is a probabilistic solution: It is easy to check that the pair of *mixed* strategies consisting of Picard flipping the penny with probability $\frac{1}{2}$ and Q playing each of his four strategies with probability $\frac{1}{4}$ is a *probabilistic* Nash equilibrium: neither player can improve his *expected* payoff (which is 0 in this case) by changing the probabilities with which he plays each of his pure strategies while the other player does not.

Figuring his chances of winning are 1/2, Captain Picard agrees to play. But he loses. The rules of the game allow Q two moves so, although his analysis indicates no benefit for Q from the second move, Picard tries arguing that they should therefore play several times. To his surprise Q agrees—and proceeds to beat Picard the next 9 times as well. Picard is sure that Q is cheating. Is he?

To understand what Q is doing, let us reanalyze PQ PENNY FLIP in terms of the sequence of moves—in its *extensive form*. Conventionally the extensive form of a game is illustrated by a tree with a distinct vertex for each partial sequence of player actions and outgoing edges from each vertex corresponding to the possible actions on the next move. For our purposes it is more useful to study the quotient of this tree obtained by identifying the vertices at which both the state of the game and the number of preceding moves are the same. Thus we illustrate the extensive form of PQ PENNY FLIP, not with a binary tree of height 3, but with the directed graph shown in Figure 1. The vertices are labelled H or T according to the state of the penny and each diagonal arrow represents a flip while each vertical arrow represents no flip.

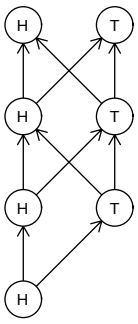

Figure 1. PQ PENNY FLIP in extensive form.

Now it is natural to define a two dimensional vector space V with basis $\{H, T\}$ and

to represent player strategies by sequences of 2×2 matrices. That is, the matrices

$$F := \begin{matrix} \\ H \\ T \end{matrix} \begin{matrix} \begin{matrix} H & T \end{matrix} \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{matrix} \qquad \text{and} \qquad N := \begin{matrix} \\ H \\ T \end{matrix} \begin{matrix} \begin{matrix} H & T \end{matrix} \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{matrix}$$

correspond to flipping and not flipping the penny, respectively, since we define them to act by left multiplication on the vector representing the state of the penny. A *mixed* action is a convex linear combination of F and N, which acts as a 2×2 (doubly) stochastic matrix:

$$\begin{matrix} \\ H \\ T \end{matrix} \begin{matrix} \begin{matrix} H & T \end{matrix} \\ \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix} \end{matrix}$$

if the player flips the penny over with probability $p \in [0,1]$. A sequence of mixed actions puts the state of the penny into a convex linear combination $aH + (1-a)T$, $0 \leq a \leq 1$, which means that if the box is opened the penny will be head up with probability a.

Q, however, is eponymously using a *quantum* strategy, namely a sequence of unitary, rather than stochastic, matrices. In standard Dirac notation [13] the basis of V is written $\{|H\rangle, |T\rangle\}$. A *pure* quantum state for the penny is a linear combination $a|H\rangle + b|T\rangle$, $a, b \in \mathbb{C}$, $a\overline{a} + b\overline{b} = 1$, which means that if the box is opened, the penny will be head up with probability $a\overline{a}$. Since the penny starts in state $|H\rangle$, this is the state of the penny if Q's first action is the unitary operation

$$U_1 = U(a,b) := \begin{matrix} \\ H \\ T \end{matrix} \begin{matrix} \begin{matrix} H & T \end{matrix} \\ \begin{pmatrix} a & \overline{b} \\ b & -\overline{a} \end{pmatrix} \end{matrix}.$$

Recall that Captain Picard is also living up to his initials, using a classical probabilistic strategy in which he flips the penny with probability p. After his action the penny is in a *mixed* quantum state, *i.e.*, it is in the pure state $b|H\rangle + a|T\rangle$ with probability p and in the pure state $a|H\rangle + b|T\rangle$ with probability $1-p$. Mixed states are conveniently represented as *density matrices* [6], elements of $V \otimes V^\dagger$ with trace 1; the diagonal entry (i,i) is the probability that the system is observed to be in state $|i\rangle$. The density matrix for a pure state $|\psi\rangle \in V$ is the projection matrix $|\psi\rangle\langle\psi|$ and the density matrix for a mixed state is the corresponding convex linear combination of pure density matrices. Unitary transformations act on density matrices by conjugation: The penny starts in the pure state $\rho_0 = |H\rangle\langle H|$ and Q's first action puts it into the pure state:

$$\rho_1 = U_1 \rho_0 U_1^\dagger = \begin{pmatrix} a\overline{a} & a\overline{b} \\ b\overline{a} & b\overline{b} \end{pmatrix}.$$

Picard's mixed action acts on this density matrix, not as a stochastic matrix on a probabilistic state, but as a convex linear combination of unitary (deterministic) transformations:

$$\rho_2 = pF\rho_1 F^\dagger + (1-p)N\rho_1 N^\dagger = \begin{pmatrix} pb\overline{b} + (1-p)a\overline{a} & pb\overline{a} + (1-p)a\overline{b} \\ pa\overline{b} + (1-p)b\overline{a} & pa\overline{a} + (1-p)b\overline{b} \end{pmatrix}. \tag{1}$$

For $p = \frac{1}{2}$ the diagonal elements of ρ_2 are each $\frac{1}{2}$. If the game were to end here, Picard's strategy would ensure him an expected payoff of 0, independently of Q's strategy. In fact, if Q were to employ any strategy for which $a\overline{a} \neq b\overline{b}$, Picard could obtain an expected payoff of $|a\overline{a} - b\overline{b}| > 0$ by setting $p = 0, 1$ according to whether $b\overline{b} > a\overline{a}$, or the reverse. Similarly, if Picard were to choose $p \neq \frac{1}{2}$, Q could obtain an expected payoff of $|2p - 1|$ by setting $a = 1$ or $b = 1$ according to whether $p < \frac{1}{2}$, or the reverse. Thus the (mixed, quantum) equilibria for the two-move game are pairs $\left([\frac{1}{2}F + \frac{1}{2}N], [U(a, b)]\right)$ for which $a\overline{a} = \frac{1}{2} = b\overline{b}$ and the outcome is the same as if both players use optimal mixed strategies.

But Q has another move U_3 which again transforms the state of the penny by conjugation to $\rho_3 = U_3\rho_2 U_3^\dagger$. If Q's strategy consists of $U_1 = U(1/\sqrt{2}, 1/\sqrt{2}) = U_3$, his first action puts the penny into a simultaneous eigenvalue 1 eigenstate of both F and N, which is therefore invariant under *any* mixed strategy $pF + (1 - p)N$ of Picard; and his second action inverts his first to give $\rho_3 = |H\rangle\langle H|$. That is, with probability 1 the penny is head up! Since Q can do no better than to win with probability 1, this is an optimal quantum strategy for him. All the pairs $\left([pF + (1 - p)N], [U(1/\sqrt{2}, 1/\sqrt{2}), U(1/\sqrt{2}, 1/\sqrt{2})]\right)$ are (mixed, quantum) equilibria for PQ Penny Flip, with value -1 to Picard; this is why he loses every game.

PQ Penny Flip is a very simple game, but it is structurally similar to the oracle problems for which efficient quantum algorithms are known—with Picard playing the role of the oracle. In Simon's problem the functions $f : \{0, 1\}^n \to \{0, 1\}^n$ which satisfy $f(x) = f(y)$ if and only if $y = x \oplus s$ for some $s \in \{0, 1\}^n$ ($\oplus$ denotes componentwise addition, mod 2), correspond to Picard's pure strategies; we may imagine the oracle choosing a mixed strategy intended to minimize our chances of efficiently determining s probabilistically. Simon's algorithm is a quantum strategy which is more successful than any mixed, *i.e.*, probabilistic, one [1]. Similarly, in the problem of searching a database of size N, the locations in the database correspond to pure strategies; again we may imagine the oracle choosing a mixed strategy designed to frustrate our search for an item at some specified location. Grover's algorithm is a quantum strategy for a game of $2m$ moves alternating between us and the oracle, where $m = O(\sqrt{N})$, which out performs any mixed strategy, *i.e.*, any probabilistic algorithm [14]. These three examples suggest that even though mixed strategies and quantum strategies generalize pure strategies in distinct directions, nevertheless:

Theorem 1: *A player using an optimal quantum strategy in a two-person zero-sum game has expected payoff at least as great as his expected payoff with an optimal mixed strategy.*

Proof (sketch): A sequence of mixed actions puts the game into a convex linear combination $\sum p_i|i\rangle$ of pure states. If one of the players uses a quantum strategy, the state of the game is described instead by a density matrix. We must show that there is always a quantum strategy which reproduces the p_i as the diagonal elements in the density matrix. Assume by induction that this is true up to a move of the classical player. His action has the same effect on the diagonal elements of the density matrix as it does on the p_i in the original (mixed, mixed) equilibrium move sequence. (See Eq. 1.) All that remains to be

shown is that a single action of the quantum player can be chosen to reproduce the effect of a mixed action. It is only necessary to consider $U(2)$ actions on a general 2×2 density matrix. If the phase of the $(1,2)$ element in the density matrix is γ, a straightforward calculation verifies that the unitary matrix $U(ie^{-i\gamma}\sqrt{1-p}, \sqrt{p})$ reproduces the effect of the mixed action $pF + (1-p)N$ on the diagonal elements. ■

Of course, the more interesting question is for which games there is a quantum strategy which improves upon the optimal mixed strategy. By the analogy with algorithms, this is essentially the fundamental question of which problems can be solved more efficiently by quantum algorithms than by classical ones. We may hope that the game theoretic perspective will suggest new possibilities for efficient quantum algorithms.

Another natural question to ask is what happens if both players use quantum strategies. By considering PQ Penny Flip we can prove the following:

Theorem 2: *A two-person zero-sum game need not have a (quantum, quantum) equilibrium.*

Proof: Consider an arbitrary pair of quantum strategies $([U_2], [U_1, U_3])$ for PQ Penny Flip. Suppose $U_3U_2U_1|H\rangle \neq |H\rangle$. Then Q can improve his expected payoff (to 1) by changing his strategy, replacing U_3 with $U_1^{-1}U_2^{-1}$, which is unitary since U_1 and U_2 are. Similarly, suppose $U_3U_2U_1|H\rangle \neq |T\rangle$. Then Picard can improve his expected payoff (to 1) by changing his strategy, replacing U_2 with $U_3^{-1}FU_1^{-1}$, which is unitary since each of U_1, U_3 and F is. Since $U_3U_2U_1|H\rangle$ cannot equal both $|H\rangle$ and $|T\rangle$, at least one of the players can improve his expected payoff by changing his strategy while the other does not. Thus $([U_2], [U_1, U_3])$ cannot be an equilibrium, for any U_1, U_2, U_3, so PQ Penny Flip has no (quantum, quantum) equilibrium. ■

That is, the situation when both players use quantum strategies is the same as when they both use pure (classical) strategies: there need not be any equilibrium solution. This suggests looking for the analogue of von Neumann's result on the existence of mixed strategy equilibria [11,5]. So we should consider strategies which are convex linear combinations of unitary actions—*mixed quantum* strategies.

Theorem 3: *A two-person zero-sum game always has a (mixed quantum, mixed quantum) equilibrium.*

Proof: Since mixed quantum actions form a convex compact subset of a finite dimensional vector space, this is an immediate corollary of Glicksberg's generalization [15] of Nash's proof [16] for the existence of game equilibria. ■

Finally, we remark that while decoherence precludes the play of PQ Penny Flip with a real penny, there are many two state quantum systems which can be put into the superposition of states necessary to implement a quantum strategy. Each of the physical systems in which quantum gate operations have been demonstrated—QED cavities [17], ion traps [18] and NMR machines [19]—could be used to play both classical and quantum

strategies in games of PQ PENNY FLIP. Q's strategy is essentially an error correcting code for bits subject to noise: $U_3 = U(1,0)U(1/\sqrt{2}, 1/\sqrt{2})$ reconstitutes an initial state which is either $|H\rangle$ or $|T\rangle$, if a bit flip error occurs. In this context the superiority of Q's quantum strategy over any classical strategy translates to a *channel capacity* [20] of 1, *independent* of the error rate. In fact, this is a quantum error correcting code [8] for a single *qubit* [21] encoding a classical bit, subject to only bit flip errors and may be compared to the recent experimental demonstration of phase error correction in an NMR system [22].

Acknowledgements

I thank Ian Agol, Thad Brown, Mike Freedman, Jeong Han Kim, Jeff Remmel, Joel Sobel, Francis Zane and several anonymous referees for discussions and comments about this work.

References

[1] D. R. Simon, "On the power of quantum computation", in S. Goldwasser, ed., *Proceedings of the 35th Symposium on Foundations of Computer Science*, Santa Fe, NM, 20–22 November 1994 (Los Alamitos, CA: IEEE Computer Society Press 1994) 116–123.

[2] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", in S. Goldwasser, ed., *Proceedings of the 35th Symposium on Foundations of Computer Science*, Santa Fe, NM, 20–22 November 1994 (Los Alamitos, CA: IEEE Computer Society Press 1994) 124–134.

[3] S. Wiesner, "Conjugate coding", *SIGACT News* **15** (1983) 78–88;
C. H. Bennett and G. Brassard, "Quantum cryptography: Public-key distribution and coin tossing", in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, December 1984 (New York: IEEE 1984) 175–179;
A. Ekert, "Quantum cryptography based on Bell's theorem", *Phys. Rev. Lett.* **67** (1991) 661–663.

[4] R. Cleve and H. Buhrman, "Substituting quantum entanglement for communication", *Phys. Rev. A* **56** (1997) 1201–1204;
W. van Dam, P. Høyer and A. Tapp, "Multiparty quantum communication complexity", quant-ph/9710054.

[5] J. von Neumann and O. Morgenstern, *Theory of Games and Economic Behavior*, third edition (Princeton: Princeton University Press 1953).

[6] J. von Neumann, *Mathematische Grundlagen der Quantenmechanik* (Berlin: Springer-Verlag 1932); transl. by R. T. Beyer as *Mathematical Foundations of Quantum Mechanics* (Princeton: Princeton University Press 1955).

[7] J. Milnor, "Games against nature", in R. M. Thrall, C. H. Coombs and R. L. Davis, eds., *Decision Processes* (New York: John Wiley & Sons 1954) 49–59.

[8] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory", *Phys. Rev. A* **52** (1995) R2493–R2496;

A. M. Steane, "Error correcting codes in quantum theory", *Phys. Rev. Lett.* **77** (1996) 793–797.

[9] E. Schrödinger, "*Die gegenwärtige Situation in der Quantenmechanik*", *Naturwissenschaften* **23** (1935) 807–812; 823–828; 844–849.

[10] L. M. Krauss, *The Physics of Star Trek*, with a forword by Stephen Hawking (New York: HarperCollins 1995).

[11] J. von Neumann, "*Zur theorie der gesellschaftsspiele*", *Math. Ann.* **100** (1928) 295–320.

[12] J. F. Nash, "Equilibrium points in N-person games", *Proc. Nat. Acad. Sci. U.S.A.* **36** (1950) 48–49.

[13] P. A. M. Dirac, *The Principles of Quantum Mechanics*, fourth edition (Oxford: Oxford University Press 1958).

[14] L. K. Grover, "A fast quantum mechanical algorithm for database search", in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, Philadelphia, PA, 22–24 May 1996 (New York: ACM 1996) 212–219.

[15] I. L. Glicksberg, "A further generalization of the Kakutani fixed point theorem, with application to Nash equilibrium points", *Proc. Amer. Math. Soc.* **3** (1952) 170–174.

[16] J. F. Nash, "Non-cooperative games", *Advances in Math.* **54** (1951) 286–295.

[17] Q. A. Turchette, C. J. Hood. W. Lange, H. Mabuchi and H. J. Kimble, "Measurement of conditional phase shifts for quantum logic", *Phys. Rev. Lett.* **75** (1995) 4710–4713.

[18] J. I. Cirac and P. Zoller, "Quantum computation with cold trapped ions", *Phys. Rev. Lett.* **74** (1995) 4091–4094;
C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano and D. J. Wineland, "Demonstration of a fundamental logic gate", *Phys. Rev. Lett.* **75** (1995) 4714–4717.

[19] D. G. Cory, M. D. Price and T. F. Havel, "Nuclear magnetic resonance spectroscopy: an experimentally accessible paradigm for quantum computing", quant-ph/9709001;
I. L. Chuang, N. Gershenfeld, M. G. Kubinec and D. W. Leung, "Bulk quantum computation with nuclear magnetic resonance: theory and experiment", *Proc. Roy. Soc. Lond. A* **454** (1998) 447–467.

[20] C. E. Shannon, "A mathematical theory of communication", *Bell System Tech. J.* **27** (1948) 379–423; 623–656.

[21] B. Schumacher, "Quantum coding (information theory)", *Phys. Rev. A* **51** (1995) 2738–2747.

[22] D. G. Cory, M. D. Price, W. Maas, E. Knill, R. Laflamme, W. H. Zurek, T. F. Havel and S. S. Somaroo, "Experimental quantum error correction", *Phys. Rev. Lett.* **81** (1998) 2152–2155;
D. Leung, L. Vandersypen, X. Zhou, M. Sherwood, C. Yannoni, M. Kubinec and I. Chuang, "Experimental realization of a two bit phase damping quantum code", quant-ph/9811068.