Quantum communication in games

David A. Meyer

Department of Mathematics, University of California/San Diego, La Jolla, CA 92093-0112 USA

Abstract. Several different definitions of quantum games have been proposed over the past five years. Some of the results claimed for the differences between these quantum games and classical games identified as those to which they correspond have been criticized, however, as not being fair comparisons. In this paper I define classical and quantum versions of games with *mediated communication*, and propose that these are the classical and quantum games that should be compared.

MOTIVATION

Universal quantum computation requires coherent control over an arbitrary number of quantum subsystems (*e.g.*, qubits). Substantial experimental progress has been made in the last decade, but quantum computing is still well beyond present technology. Quantum *communication* tasks, however, typically require control over only a small number of qubits. Quantum cryptography requires only one [1, 2, 3] or two qubits [4], for example, while quantum teleportation of a single qubit requires only two others [5]. Each of these tasks has been achieved experimentally, in multiple systems [6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16].

In this paper I define a different class of few qubit quantum communication tasks—the specification of *quantum correlated equilibria* in games. I concentrate on a special case—small games for two players—that is within present experimental reach.

CLASSICAL GAME THEORY

In a 2-*player game* each player i has a set of (*pure*) *strategies* $S^{(i)}$, $i \in \{1,2\}$, and a *payoff function*:

$$u^{(i)} : S = S^{(1)} \times S^{(2)} \to \mathbb{R}$$

that defines the outcome for each player, given a pair of strategies describing the play of both players. Each player's goal is to maximize his payoff (or the expectation value of his payoff in non-deterministic settings).

Consider, for example, the two-player game CHICKEN, in which the players drive cars head-on at one another. Swerving to the right is the "Chicken" (C) strategy; not swerving is the "Dare" (D) strategy [17]. Writing the payoff functions on $S^{(1)} \times S^{(2)} = \{C,D\} \times \{C,D\}$ as matrices with rows (columns) indexed by player 1(2)'s strategies (C,D),

$$u^{(1)} = \begin{pmatrix} 4 & 1 \\ 5 & 0 \end{pmatrix} \quad \text{and} \quad u^{(2)} = \begin{pmatrix} 4 & 5 \\ 1 & 0 \end{pmatrix}. \tag{1}$$

That is, if one player plays C while the other plays D, their payoffs are 1 and 5, respectively. If they both play C, each payoff is 4; and if they both play D, each payoff is 0.

Given this information about a game, the goal of game theory is to 'solve' the game, *i.e.*, to predict how the players will play. The simplest *solution concept* is a *Nash equilibrium*: a set of strategies, one for each player, such that neither player can improve his (expected) payoff by unilaterally changing his strategy [18, 19]. For CHICKEN, it is easy to check that (C,D) and (D,C) are Nash equilibria, with payoffs $(1,5)$ and $(5,1)$, respectively.

This concept extends from pure strategies to *mixed* strategies, *i.e.*, probability distributions over pure strategies. The pure strategies C and D label a basis for the vector space implied by the notation of (1); in this vector space a mixed strategy for either player is a nonnegative vector with L_1-norm 1. The pair of mixed strategies $p^{(1)} = (\frac{1}{2},\frac{1}{2}) = p^{(2)}$ in this notation is also a Nash equilibrium. In this case the players' expected payoffs are

$$E[u^{(1)}] = \sum_{s\in S} u^{(1)}_s p^{(1)}_{s_1} p^{(2)}_{s_2} = \frac{5}{2} = \sum_{s\in S} u^{(2)}_s p^{(1)}_{s_1} p^{(2)}_{s_2} = E[u^{(2)}]. \tag{2}$$

Since there is not a unique Nash equilibrium for CHICKEN, and because (C,C) is a symmetric pair of strategies with payoff for each player greater than in (2), it is not a completely satisfactory solution concept for this game.

There are other solution concepts, however, that account for the possible existence of pre-play communication or external institutions. A *game with mediated (classical) communication* is specified by including a commonly known probability distribution $\mu : S \to \mathbb{R}$ and an external referee who samples it and recommends privately to each player i the pure strategy in the i^{th} component of the sample. If neither player can improve his expected payoff by unilaterally *not* following the referee's recommendation, the probability distribution is a *correlated equilibrium* of the original game [20]. To express this in a way that will most clearly generalize to the quantum mechanical situation, for each player i, let $\mathscr{R}^{(i)}$ denote the set of maps $R = R^{(1)} \times R^{(2)} : S \to S$ for which $R^{(j)} = \text{id}$ if $j \neq i$. These are player i's unilateral deviations from following the referee's recommendation. Then μ is a correlated equilibrium if for each player i,

$$\sum_{s\in S} u^{(i)}_s \mu_s \geq \sum_{s\in S} u^{(i)}_{R(s)} \mu_s = \sum_{s,t\in S} u^{(i)}_t R_{ts} \mu_s \quad \forall R \in \mathscr{R}^{(i)}. \tag{3}$$

The joint probability distribution μ can be a product distribution: $\mu = p^{(1)} p^{(2)}$; if it is also a correlated equilibrium it is necessarily a Nash equilibrium. More generally, the set of all correlated equilibria is compact and convex. The convex hull of the Nash equilibria is a subset of the set of correlated equilibria [21], and there can be correlated equilibria *outside* the convex hull of the Nash equilibria [20]. For example, in CHICKEN the correlated equilibrium with the largest total expected payoff, $(\frac{10}{3}, \frac{10}{3})$, is

$$\mu = \begin{pmatrix} 1/3 & 1/3 \\ 1/3 & 0 \end{pmatrix},$$

which is outside the convex hull of the Nash equilibria:

$$(C,D) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad (D,C) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 1/4 & 1/4 \\ 1/4 & 1/4 \end{pmatrix}.$$

QUANTUM INFORMATION IN GAMES

From the point of view of information theory, in a game with mediated (classical) communication the referee draws a sample from S according to the probability distribution μ and sends to each player i the signal s_i, denoting the $S^{(i)}$ component of the sample. After acting, each player i returns $R^{(i)}(s_i)$ and then the referee evaluates the payoffs using the returned signals. The probability distribution on S resulting from the players' responses is

$$\mu'_t = \sum_{s\in S} R^{(1)}_{t_1 s_1} R^{(2)}_{t_2 s_2} \mu_s.$$

Describing a game with mediated (classical) communication this way suggests an immediate quantum analogue. Define a *game with mediated quantum communication* to be the following scenario: The referee prepares a quantum state $\psi \in \mathbb{C}^{S^{(1)}} \otimes \mathbb{C}^{S^{(2)}}$ and sends to each player i the quantum signal instantiated by the subsystem described by the i^{th} tensor factor. Then each player i acts on his own subsystem and returns it to the referee. Finally, the referee measures the whole system in the basis labelled by S, and computes the payoffs using the observed element of S.

If the players only act by unitary operations $U^{(i)}$, the state the referee measures is

$$\psi'_t = \sum_{s\in S} U^{(1)}_{t_1 s_1} \otimes U^{(2)}_{t_2 s_2} \cdot \psi_s.$$

More generally, the players should really be allowed to make any quantum operation on their subsystem, *i.e.*, player i's action is described by some trace preserving completely positive map on the reduced density matrix $\rho^{(i)}$ of his subsystem. This can transform the initial state $\rho = \psi \otimes \psi^\dagger$ into a mixed state ρ'. Thus, in general, the expected payoff for player i is:

$$E[u^{(i)}] = \sum_{t\in S} u_t^{(i)} \rho'_{tt}.$$

Within this scenario, define a *quantum correlated equilibrium* for a game to be an initial state ψ which gives neither player an incentive to act unilaterally by anything other than the identity operator. Let $\mathscr{A}^{(i)}$ denote the set of maps $A = A^{(1)} \times A^{(2)} : \mathbb{C}^S \otimes (\mathbb{C}^S)^* \to \mathbb{C}^S \otimes (\mathbb{C}^S)^*$, where $A^{(j)}$ is a completely positive trace preserving map on $\mathbb{C}^{S^{(j)}} \otimes (\mathbb{C}^{S^{(j)}})^*$ and $A^{(j)} = I$ if $j \neq i$. Again, these should be interpreted as player i's possible unilateral deviations from the referee's recommendation. Then ψ is a quantum correlated equilibrium if for each player i,

$$\sum_{s\in S} u_s^{(i)} |\psi_s|^2 \geq \sum_{t\in S} u_t^{(i)} \big(A(\rho)\big)_{tt} \quad \forall A \in \mathscr{A}^{(i)}. \tag{4}$$

PROPERTIES OF QUANTUM CORRELATED EQUILIBRIA

The most basic, and perhaps surprising, property of quantum correlated equilibria is that if ψ is quantum correlated equilibrium for a game then the probability distribution defined by $\mu_s = |\psi_s|^2$ is a *classical* correlated equilibrium for the same game. To see this, notice that by construction, the expectation value of the payoff for each player is the same for ψ and μ. $\mathscr{A}^{(i)}$ includes the quantum operation where player i measures his subsystem to obtain $|s_i\rangle$, for $s_i \in S_i$, and then transforms the subsystem into $|R^{(i)}(s_i)\rangle$ for any $R^{(i)} : S_i \to S_i$, while the other player acts only by the identity. By (4), this reduces the expectation value of player i's payoff. But the probability distributions over S created by these quantum operations are the same as those on the right hand side of (3). Thus (3) holds, and μ is a (classical) correlated equilibrium.

This means that any set of payoffs achieved in a quantum correlated equilibrium can also be achieved classically. But it does not imply that classical and quantum correlated equilibria are equivalent solution concepts. Since there are many other quantum operations than those used in the argument in the preceding paragraph, (4) is a larger set of constraints than (3), and generically has fewer solutions. In fact, one might worry that there are no quantum correlated equilibria at all. But (4) does have solutions: Consider a quantum state ψ such that $\psi_{s_1 s_2} = \big(p^{(1)}_{s_1} p^{(2)}_{s_2}\big)^{1/2}$, where $\mu_s = p^{(1)}_{s_1} p^{(2)}_{s_2}$ is the probability distribution for a Nash equilibrium. ψ is thus a product state $\psi^{(1)} \otimes \psi^{(2)}$, so any quantum operation by player 1, for example, leaves it in a product state $\rho' = (\rho^{(1)})' \otimes \rho^{(2)}$, where $\rho^{(2)} = \psi^{(2)} \otimes \psi^{(2)\dagger}$. But this state implies a probability distribution $\rho'_{ss} = (\rho^{(1)})'_{s_1 s_1} p^{(2)}_{s_2}$. Only the probability distribution on player 1's strategies has changed, so since μ is a Nash equilibrium, ρ' cannot improve player 1's expected payoff. Thus quantum correlated equilibria exist for any game with mediated quantum communication: they are Nash equilibria for the same game without communication.

Not every classical correlated equilibrium for a game, however, even in the convex hull of the Nash equilibria, can be realized as $|\psi_s|^2$ for some quantum correlated equilibrium of the same game. This can be shown by calculation in a specific example, and more detailed calculations are necessary to characterize completely the set of quantum correlated equilibria [22].

DISCUSSION

I have formulated the quantum analogue of correlated equilibria in a game with mediated classical communication, having been led there by an information theoretic interpretation of the latter. These are equilibria of the same game, but with mediated *quantum* communication. Although Marinatto and Weber have defined quantum games [23] in a way that is structurally equivalent—what they term an "entangled quantum strategy" is exactly an entangled state prepared by the referee here—they do not allow arbitrary quantum operations by the players, which leads them to unrealistic conclusions about the difference from the classical game. The quantum communication perspective presented here clarifies exactly what is quantum mechanical about the game, and the classical scenario to which it should be compared. The absence of any fair comparison between quantum and classical games has been emphasized by van Enk and Pike [24]; this work is partially motivated by their critique.

What Marinatto and Weber call an "entangled quantum strategy" was first introduced by Eisert, Wilkens and Lewenstein [25] in a scenario that corresponds in our formalism to the referee making the final measurement in a (specific) different basis of the joint Hilbert space. This is a generalization that deserves investigation—in the game with mediated classical communication it corresponds to further processing of the players' actions after they accept or reject the referee's recommendation. This might be something as simple as a coin flip to decide a tie, or as subtle as the change in the bid of the high bidder in a second price auction. In any case, it is again the game *with mediated classical communication* to which the quantum game of Eisert, Wilkens and Lewenstein should be compared for any differences, not the classical game alone.

ACKNOWLEDGMENTS

I thank Markus Hunziker and Joel Sobel for useful conversations about correlated equilibria. This work has been partially supported by the National Security Agency (NSA) and Advanced Research and Development Activity (ARDA) under Army Research Office (ARO) grant number DAAD19-01-1-0520 and by the Air Force Office of Scientific Research (AFOSR) under grant number F49620-01-1-0494.

REFERENCES

1. S. Wiesner, "Conjugate coding", *SIGACT News* **15** (1983) 78–88.
2. C. H. Bennett, G. Brassard, S. Breidbart and S. Wiesner, "Quantum cryptography, or unforgeable subway tokens", in D. Chaum, R. L. Rivest and A. T. Sherman, eds., *Advances in Cryptology: Proceedings of Crypto 82* (New York: Plenum Press 1982) 267–275.
3. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing", *Proceedings of the International Conference on Computers, Systems and Signal Processing* (1984) 175–179.
4. A. K. Ekert, "Quantum cryptography based on Bell's theorem", *Phys. Rev. Lett.* **67** (1991) 661–663.
5. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels", *Phys. Rev. Lett.* **70** (1993) 1895–1899.
6. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental quantum cryptography", *J. Cryptology* **5** (1992) 3–28.
7. A. Muller, J. Breguet and N. Gisin, "Experimental demonstration of quantum cryptography using polarized photons in optical fiber over more than 1 km", *Europhysics Lett.* **23** (1993) 383–388.
8. A. Muller, H. Zbinden and N. Gisin, "Quantum cryptography over 23 km in installed under-lake telecom fibre", *Europhysics Lett.* **33** (1996) 335–339.
9. W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson and C. Simmons, "Practical free-space quantum key distribution over 1 km", *Phys. Rev. Lett.* **81** (1998) 3283–3286.
10. W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt and C. G. Peterson, "Daylight quantum key distribution over 1.6 km", *Phys. Rev. Lett.* **84** (2000) 5652–5655.
11. R. J. Hughes, D. G. L. Morgan and C. G. Peterson, "Quantum key distribution over a 48-km optical fiber network", *J. Mod. Opt.* **47** (2000) 533–547.
12. R. J. Hughes, J. E. Nordholt, D. Derkacs and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night", *New J. Phys.* (2002) 43.1–43.14.
13. D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger, "Experimental quantum teleportation", *Nature* **390** (1997) 575–579.
14. D. Boschi, S. Branca, F. De Martini, L. Hardy and S. Popescu, "Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels", *Phys. Rev. Lett.* **80** (1998) 1121–1125.
15. A. Furusawa, J. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble and E. S. Polzik, "Unconditional quantum teleportation", *Science* **282** (1998) 706–709.
16. M. A. Nielsen, E. Knill and R. Laflamme, "Complete quantum teleportation using nuclear magnetic resonance", *Nature* **396** (1998) 52–55.
17. B. Russell, *Common Sense and Nuclear Warfare* (New York: Simon and Schuster 1959).
18. J. von Neumann and O. Morgenstern, *Theory of Games and Economic Behavior*, third ed. (Princeton: Princeton University Press 1953).
19. J. Nash, "Non-cooperative games", *Ann. of Math.* **54** (1951) 286–295.
20. R. Aumann, "Subjectivity and correlation in randomized strategies", *J. Math. Econom.* **1** (1974) 67–95.
21. J. Harsanyi and R. Selten, "A generalized Nash solution for two-person bargaining games with incomplete information", *Management Science* **14** (1972) P80–P106.
22. D. A. Meyer, "Quantum correlated equilibria in games", UCSD preprint (2004).
23. L. Marinatto and T. Weber, "A quantum approach to static games of complete information", *Phys. Lett. A* **272** (2000) 291–303.
24. S. J. van Enk and R. Pike, "Classical rules in quantum games", *Phys. Rev. A* **66** (2002) 024306.
25. J. Eisert, M. Wilkens and M. Lewenstein, "Quantum games and quantum strategies", *Phys. Rev. Lett.* **83** (1999) 3077–3080.