Hedging bets with correlated quantum strategies

Abel Molina and John Watrous

Institute for Quantum Computing and School of Computer Science
University of Waterloo

Setting.—In our work, we consider independently administered copies of tests performed by a subject Alice on a subject Bob. We demonstrate that correlated strategies in quantum information theoretic variants of these tests can exhibit striking non-classical characteristics.

The interactions between Alice and Bob that we consider have the following simple form:

1. Alice prepares a *question* and sends it to Bob.
2. Bob responds by sending an *answer* to Alice.
3. Based on Bob's answer, as well as whatever memory she has of her own question, Alice decides whether Bob has *passed* or *failed* the test.

The restriction to two outcomes is not an inherent limitation of the setting under consideration, but it will serve to illustrate the differences between the classical and quantum settings that represent the main point of our work. For a fixed choice of a test, we will let p denote the *optimal probability* of passing for Bob.

In the classical case, classical information is sent between Alice and Bob, and their behaviour can be randomized. In the quantum case, quantum information is sent between Alice and Bob, possible entangled with other quantum information that they possess. A complete description of the process by which Alice operates is part of the description of a particular test. We make the assumption that Bob has access to the description of the test.

We consider the case in which two repetitions of a test occur in parallel, with Alice operating in them *independently* from each other. In this situation, first two questions are sent by Alice, and then two answers are received from Bob. We ask then two natural questions:

1. What is the optimal probability with which Bob passes *both* tests?
2. What is the optimal probability with which Bob passes *at least one* of the tests?

If Bob is constrained to answer both tests independently, then the answers to the previous questions are be p^2 and $1 - (1 - p)^2$, respectively. We can then ask whether these are still the answers when Bob is not constrained anymore to answer the tests independently. Note that it is not clear how not operating independently might help Bob, since Alice operates independently in both tests.

Results.—Using an *interactive measurement* model for our tests, we express our questions in the *semidefinite programming* framework that originally appeared in [GW07].

In the classical case, the probabilities p^2 and $1 - (1 - p)^2$ are indeed optimal over all possible strategies. This follows from the fact that in the classical case the optimal strategy will always be deterministic. It also follows easily from the semidefinite programming formulation. Note also that in the classical case, it is still optimal to play independently in the more general case in which a

test is repeated in parallel n times, and Bob is trying to maximize his chance of passing at least k of those repetitions.

In the quantum case, it is known that p^2 is indeed the answer to the first question, from results in [GW07] and [MS07], obtained in the semidefinite programming framework. We examine how does the proof from the first question not extend to the second question. We see how, in short, the reason the proof does not extend corresponds to the replacement of a $\geq$ constraint by a $\leq$ constraint in the dual semidefinite program. Then, we provide a example that shows how $1-(1-p)^2$ is not always the answer to the second question. In particular, we consider a simple test in which we prove that the value of p is at most $\cos^2(\pi/8) \approx 0.85$ (and indeed, that value is reached for an optimal strategy). However, when two parallel repetitions of the test are considered, we show that it is possible for Bob to correlate his answers to both tests so that he always passes at least one of them. The test in our example is the following one:

1. Alice prepares a pair of qubits (X, Z) in the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and sends the second qubit to Bob.
2. Bob applies an arbitrary quantum channel to the qubit Z that he receives, with the output of the channel being represented by a qubit Y. Bob sends Y to Alice.
3. Alice performs a projective measurement with respect to $\cos(\pi/8)|00\rangle + \sin(\pi/8)|11\rangle$. The outcome 1 corresponds to Bob passing the test, while the output 0 corresponds to Bob failing the test.

When only one repetition is considered, it is optimal for Bob to let his channel simply be the identity. However, when two parallel repetition of the tests are considered, it is optimal for Bob to let his channel be a controlled phase flip $|00\rangle \mapsto -|00\rangle$, $|01\rangle \mapsto |01\rangle$, $|10\rangle \mapsto |10\rangle$, $|11\rangle \mapsto |11\rangle$ on his two input qubits. This guarantees that at least one of the repetitions is passed (indeed, it is the case that exactly one of them is passed).

The ability of Bob to correlate two independent tests in the way described in the previous paragraph can be seen as a perfect form of *hedging*, as the following (highly fictitious) scenario illustrates. One individual (Bob) is offered the opportunity to take part in two potentially lucrative but somewhat risky games of chance, run by another individual (Alice). The two games are completely independent and identical in nature: for each Bob must put forth \$1 million of his own money to take part, and he has 85% chance to win if he plays optimally. For each game he wins, Bob receives \$3 million (representing a \$2 million gain over his initial \$1 million investment), while he receives nothing (and loses his \$1 million initial investment) if he loses. A \$1 million or greater loss is to be considered ruin for Bob.

The expected gain from each game is \$1,550,000, and the chance for a loss in both, if they are treated independently, is only 2.25%. Bob, however, is a highly risk-averse person: while he would enjoy being a millionaire, he cannot accept a 2.25% chance of ruin. Classically speaking, Bob can do nothing to avoid at least a 2.25% chance of ruin, so he will choose not to play. If the two games are modeled by quantum information as in our example, however, Bob can be *guaranteed* a \$1 million return, and can therefore play without fear: an appropriately chosen quantum strategy allows him to hedge his bets perfectly.

Discussion.—We discover in our work a situation with a counter-intuitive outcome for an interaction between two parties, due to the presence of correlated strategies not possible classically. There are other settings in which quantum effects that are not possible in the classical world have been discovered to be possible in an interaction between two parties. However, our setting differs from some of the best-known such situations, such as the CHSH game [CHSH69], and the Mermin-Peres magic squares game [Mermin90, Peres90]. In our setting, we do not have two parties collaborating

to achieve a non-classical outcome. Instead, we have *prover-verifier* setting, in which Bob is trying to convince Alice in order to pass a test.

Our work is also related to the problem of error reduction for certain kinds of *quantum interactive proof systems* [BM88, GMR89]. In this situation, there is a *string* x known to Alice and Bob, which might or might not be a member of a *language* L. We also have a test of the form we consider in our work, such that whenever $x \in L$ Bob can pass the test with probability at least α, while whenever $x \notin L$ Bob can pass the test with probability at most $\beta < \alpha$. Assuming Bob is playing to maximize his chance of passing, Alice can then use the outcome of the test to make a guess about whether $x \in L$ or not. We can see that this will be very easy to do whenever α is close to 1 and β is close to 0. Error reduction corresponds then to obtaining another test with smaller β and larger α. If if was true that it is optimal for Bob to answer independently, that would easily prove the correctness of a natural strategy to reduce error. In this natural strategy, the new test simply consists of a number of independent instantiations of the original test. The new test accepts if and only if some suitably chosen fraction of these independent tests (e.g. $\frac{\alpha+\beta}{2}$) lead to acceptance. This would improve on the more complicated strategy for reducing error in this situation that appears in [JUW09]. Our result shows that a proof method that uses the optimality of independent answers for Bob does not work if we want to prove the correctness of the natural strategy to reduce error.

Our work does have potential importance in the setting of cryptography, where certain protocols might very well be abstracted as tests of the sort we have considered. The extent to which a dishonest individual can attack such protocols by correlating independent executions is an important security consideration that some would-be cryptographers might fail to consider. Our results demonstrate that quantum attacks to such protocols may exhibit striking non-classical and counter-intuitive properties, and should therefore be given very careful consideration.

A version of the work described here that shows the technical aspects is available as arXiv.org e-Print 1104.1140.

References.—

[BM88] L. Babai and S. Moran. Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity classes. *Journal of Computer and System Sciences*, 36(2):254–276, 1988.

[CHSH69] J. F. Clauser, M.A. Horne, A. Shimony and R. A. Holt. Proposed experiment to test local hidden-variable theories. In *Physical Review Letters*, 23, pages 880–884, 1969.

[GMR89] S. Goldwasser, S. Micali and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, 1989.

[GW07] G. Gutoski and J. Watrous. Toward a general theory of quantum games. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pages 565–574, 2007.

[JUW09] R. Jain, S. Upadhyay and J. Watrous. Two-message quantum interactive proofs are in PSPACE. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 534–543, 2009.

[Mermin90] N.D. Mermin. Simple Unified Form for No-Hidden Variables Theorems. In *Physical Review Letters*, 65, pages 3373–6, 1990.

[Peres90] A. Peres. Incompatible results of quantum measurements. In *Physical Review A*, 151, pages 107–8, 1990.

[MS07] R. Mittal and M. Szegedy. Product rules in semidefinite programming. In *Fundamentals of Computation Theory*, volume 4639 of Lecture Notes in Computer Science, pages 435–445. Springer-Verlag, 2007.