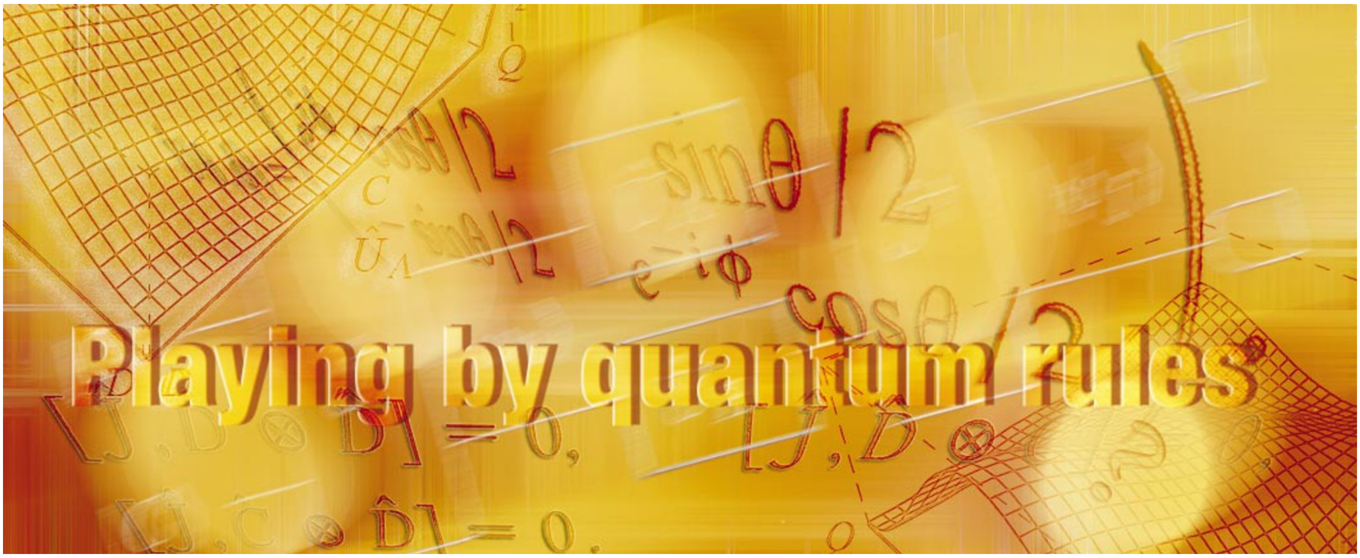

Game theory has been used to study problems from nuclear warfare to animal behaviour. Now physicists are extending it into the quantum realm, opening a new range of potential applications. Erica Klarreich reports.

In the classic puzzle of game theory, two accomplices are awaiting trial, having been caught robbing a bank. Six-month prison sentences lie ahead if both deny involvement. If each blames the other, the police will have enough evidence to send both down for five years. But, crucially, if one keeps silent and the other spills the beans, the informer will get off scot-free while their partner lands a 10-year stretch.

Known as the Prisoners' Dilemma, this puzzle encourages players to adopt destructive tactics. Assuming that the partners are guided by purely selfish motives, the rational option for both is to defect. Both accomplices are then left with five-year sentences, when, had they been able to trust one another and cooperate, they would have got just six months.

Games like these have fascinated mathematicians since the early twentieth century, and they have been used to study a range of subjects from the evolution of animal behaviour to the likelihood of nuclear conflict. Now the field is taking a completely new direction, led by physicists interested in quantum mechanics.

In quantum versions of existing games, new strategies become available to the players. Some researchers say these make the dilemma in the prisoners' game disappear. Others are using the games to develop new algorithms for the quantum computers of the future. In the shorter term, the games could find applications in the stock market.

The first and simplest analysis of a quantum game was published in 1999 by David Meyer, a mathematician at the University of California, San Diego[1]. Meyer considered a game in which two players, Q and P, control a coin that neither can see. Q makes the first and last move. Both players know that the coin starts heads up. On each go, the players can choose to turn the coin over or leave it alone, but neither can see what the other is doing. The game ends after a previously agreed number of moves — if heads shows, Q wins, otherwise P wins. Each player may as well act randomly as there is no other strategy that will improve their chances.

Heading for victory

But transferring the game to the quantum world introduces new possibilities. According to quantum mechanics, objects can exist in mixed states known as superpositions. A hypothetical quantum coin, for example, can exist as heads, tails or a superposition of both. Meyer analysed a new version of the game in which Q is allowed to include quantum combinations of heads and tails, but P is restricted to classical strategies. This advantage, he found, allows Q to win every time.

Again the coin starts heads-side up, and Q's first move is to put the coin into a state that is an equal mixture of heads and tails. P can then either turn the coin or leave it alone. But whatever P chooses to do, it has no effect on the coin. Q cannot see the coin, but knows that P has failed to alter the coin's state. Q ends the game by making a move that is the exact opposite of the first move, which changes the state from an equal mixture of heads and tails back into pure heads.

Meyer's example might seem abstract, but similar games could help researchers in their quest to find uses for future quantum computers. In 1994, physicist Peter Shor of Bell Laboratories in Murray Hill, New Jersey, electrified the world of computer science by devising an algorithm that would allow a

M. QUONG

In a spin: David Meyer's quantum strategy means that a player will always win a coin-flipping game.

quantum computer — if one is ever built — to factor numbers much more efficiently than any classical computer[2].

Shor's discovery prompted a search for other quantum algorithms. "People know efficient quantum algorithms are out there," says Neil Johnson, who works on quantum computation at the University of Oxford. But despite a flurry of activity, only a handful of quantum algorithms that can solve problems more efficiently than their classical rivals have been uncovered.

It is here that quantum games might help. Some mathematical problems can be rephrased as games. The problem of searching for a particular entry in a database, for example, can be turned into a game in which players compete to see who finds the entry first. Algorithms for solving the problem then become strategies for playing the game. Finding a quantum algorithm that solves the problem faster than its classical counterpart is equivalent to identifying a quantum strategy that can beat the classical alternative. "This will probably be one of the first benefits of quantum game theory," predicts Johnson. Indeed, Meyer has already succeeded in casting some known quantum algorithms in terms of quantum games[3], and is now working on generating new ones.

Cryptography may also benefit. Researchers have built prototype quantum 'cryptosystems' that are, in principle, impossible to crack without the infiltrator being detected. Measuring a quantum system changes its state, so in theory no eavesdropper could examine a message without leaving a trace. But in practice, imperfections in the transmission system introduce noise into the signal, potentially obscuring the presence of an eavesdropper. Quantum game theory might help researchers to understand how vulnerable a system is. "Analysing the security of quantum communication is like analysing a quantum game," says Meyer. "The two people trying to communicate securely are playing against an eavesdropper."

Other researchers are interested in expanding the scope of the games, and are studying situations in which both players can use quantum strategies. In 1999, for instance, Jens Eisert, then at the University of Potsdam in Germany, and his colleagues described a quantum version of the Prisoners' Dilemma.

In Eisert's scheme, players can choose a superposition of cooperation and defection. The two players' choices are also 'entangled'. According to quantum mechanics, entangled particles — such as two infrared photons formed by the spontaneous splitting of a higher energy ultraviolet photon — exert an influence over each other. If, for example, the polarization of one of the photons is measured, the polarization of the other will be modified instantaneously. Players' choices can be represented by the state of a particle such as a photon or, as in proposed quantum computers, an electron. If the particles are entangled, the two choices can modify one another when measured, even though neither player has knowledge of the other's decision.

Under the influence

This considerably extends the range of possible tactics. Players no longer have to choose straight cooperation or defection, and they can also try to influence the other's choice by means of entanglement. By considering a limited number of all the possible quantum strategies, Eisert showed that rather than straight defection, a form of cooperation in which entanglement allows the players to influence each other's decision was the best option[4].

But some theorists felt that limiting the range of possible strategies was unnatural. Simon Benjamin of the University of Oxford and Patrick Hayden of the California Institute of Technology have since shown that if two players are allowed the full range of quantum strategies, the best plan is for them to make random choices[5]. However, their analysis of a three-player version of the Prisoners' Dilemma, in which players also have access to the full range of strategies, shows that a form of cooperation emerges as the best approach[6].

Such work has stimulated a spate of research on other games, but researchers warn that the subject is still in its infancy. "At this point every new game has to be analysed from scratch," says Meyer. Applications for the work are also some way off, but physicists are pondering potential uses nonetheless.

One example involves 'minority games' — in which players choose between two options and win a pay-off if they are in the minority — which could benefit from being run as quantum games. Trading shares is a example: players benefit if they are one of just a few to invest in a successful stock. Benjamin and Hayden have shown that some minority games yield higher pay-offs overall if all the players are allowed to use quantum strategies[6].

Building the quantum devices needed to play such games may not be that difficult. Implementing something like Shor's algorithm would require hundreds or thousands of entangled particles, which is technically very challenging. But in simple games such as the quantum Prisoners' Dilemma, only one particle per player is needed. "The technology to play such a game is either present now or is just around the corner," says Seth Lloyd of the Massachusetts Institute of Technology, a physicist who specializes in quantum computing.

At this stage, no one is sure which applications will prove most fruitful. But as the players in this new field hone their skills, the game is on. ■

Erica Klarreich is an intern with *Nature*.

1. Meyer, D. *Phys. Rev. Lett.* **82,** 1052–1055 (1999).
2. Shor, P. in *Proc. 35th Symp. Foundations of Computer Science* (ed. Goldwasser, S.) 124–134 (IEEE Computer Society Press, Washington, 1994).
3. Meyer, D. in *Contemporary Mathematics: Quantum Computation and Quantum Information Science* (American Mathematical Society, Providence, Rhode Island, in the press).
4. Eisert, J., Wilkens, M. & Lewenstein, M. *Phys. Rev. Lett.* **83,** 3077–3080 (1999).
5. Benjamin, S. C. & Hayden, P. M. *Phys. Rev. Lett.* **87,** 069801 (2001).
6. Benjamin, S. C. & Hayden, P. M. *Phys. Rev. A* **64,** 030301 (2001).

Winning strategy: Simon Benjamin's multiplayer games could improve the success of share trading.

Cooperative: Jens Eisert has come up with a quantum solution to the Prisoners' Dilemma.