Quantum game theory investigates the behavior of strategic agents with access to quantum technology. In some models (see [CHTW] or [DL] for example), players can randomize their strategies by observing quantum mechanical variables (such as the spins of electrons). In others, players use quantum devices to communicate with each other or with the referee. The present paper is exclusively concerned with models of quantum communication.

The most widely studied such model is the EWL model introduced by Eisert, Wilkens and Lewenstein ([EW], [EWL]). The EWL model supplements classical game theory by specifying a protocol for the communication of strategies and computation of payoffs. For example, starting with an ordinary two-by-two game, EWL envisions a referee who issues each player a penny in the state $\text{H}$ (“heads up”). The player indicates his choice of strategy by returning the penny either unflipped or flipped. The referee observes the pair of returned pennies, which are in one of four states $\text{H} \otimes \text{H}$, $\text{H} \otimes \text{T}$, etc., and calculates payoffs accordingly.

Now replace the pennies with subatomic particles (though I will continue to call them pennies) in the maximally entangled state $\text{H} \otimes \text{H} + \text{T} \otimes \text{T}$. Each player returns his penny after acting on it by the special unitary operator of his choice. The pennies are returned to the referee, who makes an observation with one of four possible outcomes, and calculates payoffs accordingly.

Players are free to discard their entangled pennies and substitute classical pennies, but in equilibrium they won’t want to.

This model is of interest because it captures, in a fairly general setting, the behavior of players who use quantum technology to manipulate their communications, taking as given the protocol by which those communications will be deciphered.

In the EWL model, each player’s strategy space naturally expands from the two-point space to the group $\text{SU}_2$, which we identify with the three-sphere $S^3$. The space of mixed quantum strategies, then, is the space of probability distributions on $S^3$. In principle, the vastness of this space makes it difficult to
find equilibria or to establish that they’ve all been found. Quite a bit of attention has been lavished on identifying equilibria in particular two-by-two EWL games.

The chief contribution of this paper is to classify all Nash equilibria in mixed quantum strategies up to a natural notion of equivalence, and to show that they all take quite simple forms. In equilibrium, each player’s mixed strategy is supported on at most four points. Moreover, these points must lie in certain quite restrictive geometric configurations. This transforms the search for equilibria from a potentially intractable problem into an almost mechanical one.

I call a game “generic” if, for each player, the four possible payoffs and the six pairwise sums of those payoffs are all distinct. In this paper, I will state and prove the main theorem for generic games, referring the reader to my unpublished working paper [NE] for the (considerably uglier) generalization to the non-generic case.

Section 1 lays out the details of the EWL model. Section 2 presents the main technical lemmas. Section 3 contains the main classification theorem (3.3). Section 4 addresses some natural questions raised by the statement of the main theorem. Section 5 collects a few additional remarks and applications; the most striking is that in any mixed strategy quantum equilibrium of any two-by-two zero sum game, each player earns exactly the average of the four possible payoffs.

1. The Eisert-Wilkens-Lewenstein Model.

A classical penny can be either in the state $H$ (“heads”) or $T$ (“tails”). The states of a quantum penny are represented by expressions $\alpha H + \beta T$ where $\alpha$ and $\beta$ are complex numbers, not both zero. Two such expressions represent the same state if (and only if) one is a (complex) scalar multiple of the other.

An entangled pair of pennies is in a state represented by a non-zero expression

$$\alpha H \otimes H + \beta H \otimes T + \gamma T \otimes H + \delta T \otimes T$$

where the coefficients are complex numbers, and where a scalar multiple represents the same state.

Start with a two-by-two game $G$ where each player’s strategy space is $\{C, D\}$. Each player acquires (or is issued) one of two entangled pennies, which start out in the maximally entangled state

$$H \otimes H + T \otimes T$$
They return their pennies unflipped to indicate a play of C or flipped to indicate a play of D. After the pennies are returned, the referee observes whether they’ve been flipped and makes payoffs accordingly.

As long as players obediently play either C or D, the game is unchanged from its old, non-quantum version. But quantum mechanics allows players to act on their pennies by arbitrary special unitary matrices. Acting by the identity matrix means leaving the penny unflipped. Acting by the matrix

\[
\begin{pmatrix}
0 & 1 \\
-1 & 0
\end{pmatrix}
\]

means flipping the penny. Other unitary matrices correspond to physical operations with no classical analogues.

If Players One and Two act by the unitary matrices

\[
\begin{pmatrix}
A & B \\
-B & A
\end{pmatrix}
\]

and

\[
\begin{pmatrix}
P & Q \\
-Q & P
\end{pmatrix}
\]

then the pennies come back to the referee in the state

\[
(\mathbf{A} \mathbf{H} - \mathbf{B} \mathbf{T}) \otimes (\mathbf{P} \mathbf{H} - \mathbf{Q} \mathbf{T}) + (\mathbf{B} \mathbf{H} + \mathbf{A} \mathbf{T}) \otimes (\mathbf{Q} \mathbf{H} + \mathbf{P} \mathbf{T})
\]

which expands to

\[
(AP + BQ)\mathbf{H} \otimes \mathbf{H} + (A\mathbf{Q} + B\mathbf{P})\mathbf{H} \otimes \mathbf{T} + (-B\mathbf{P} + A\mathbf{Q})\mathbf{T} \otimes \mathbf{H} + (\mathbf{A} \mathbf{F} + \mathbf{B} \mathbf{Q})\mathbf{T} \otimes \mathbf{T}
\]

If the players choose classical strategies (either the identity matrix or the matrix (1.0.1)), the pennies come back to the referee in one of four states

\[
\begin{align*}
\mathbf{CC} &= \mathbf{H} \otimes \mathbf{H} + \mathbf{T} \otimes \mathbf{T} \\
\mathbf{CD} &= \mathbf{H} \otimes \mathbf{T} + \mathbf{T} \otimes \mathbf{H} \\
\mathbf{DC} &= \mathbf{H} \otimes \mathbf{T} - \mathbf{T} \otimes \mathbf{H} \\
\mathbf{DD} &= \mathbf{H} \otimes \mathbf{H} - \mathbf{T} \otimes \mathbf{T}
\end{align*}
\]

and the referee makes payoffs accordingly. If players adopt more general strategies, returning the pennies in state (1.0.2), the referee’s observation causes them to collapse into one of the states (1.0.3a-d) with probabilities calculated (according to the laws of quantum mechanics) as follows:
First write (1.0.2) as a linear combination

\[ \alpha_1 CC + \alpha_2 DD + \alpha_3 CD + \alpha_4 DC \]  

(with complex scalar coefficients). Then the probabilities of the four states are proportional to \(|\alpha_1|^2, |\alpha_2|^2, |\alpha_3|^2, |\alpha_4|^2\).

Notice that the referee cannot detect (and therefore cannot prohibit) the play of nonclassical strategies.

All the referee ever observes is a pair of pennies in one of the states (1.0.3a-d).

Now identify Player One’s strategy space with the unit quaternions by mapping the matrix with top row \((A, B)\) to the quaternion \(A + Bj\); identify Player Two’s strategy space with the unit quaternions by mapping the matrix with top row \((P, Q)\) to the quaternion \(P - jQ\). From (1.0.2) one readily calculates the coefficients in (1.0.4) and discovers the following remarkably simple formula:

**Proposition 1.1.** Suppose Player One plays the quaternion \(p\) and Player Two plays the quaternion \(q\). Then for \(t = 1, \ldots, 4\), we have

\[ |\alpha_t| = 2|\pi_t(pq)| \]

where the \(\pi_t\) are the coordinate functions defined by

\[ p = \pi_1(p) + \pi_2(p)i + \pi_3(p)j + \pi_4(p)k \]

Motivated by Proposition 1.1 and the preceding discussion, we make the following definitions:

**Definitions and Remarks 1.2.** Let \(G\) be a two by two game with strategy spaces \(S_i = \{C, D\}\) and payoff functions \(P_i : S_1 \times S_2 \to \mathbb{R}\). Then the associated quantum game \(G^Q\) is the two-player game in which each strategy space is the unit quaternions, and payoffs are calculated as

\[ P_i^Q(p, q) = \pi_1(pq)P_i(C, C) + \pi_2(pq)P_i(D, D) + \pi_3(pq)P_i(C, D) + \pi_4(pq)P_i(D, C) \]

Note that for any strategy \(p\) chosen by Player 1, and for any probability distribution whatsoever over the four outcomes \((C, C)\), etc., Player 2 can always adopt a strategy \(q\) that effects this probability distribution. Let \(a^2, b^2, c^2, d^2\) be the desired probabilities, let \(r = a + bi + cj + dk\) and set \(q = p^{-1}r\). Therefore, in the game \(G^Q\), there can never be an equilibrium in pure strategies unless one of the four strategy pairs leads to an optimal outcome for both players.
Thus in $G^Q$, pure-strategy equilibria are both rare and uninteresting.

Next we consider mixed strategies. A mixed quantum strategy for $G$ is a mixed strategy in the game $G^Q$, i.e. a probability distribution on the space of unit quaternions.

If $p$ is a unit quaternion, I will sometimes identify $p$ with the mixed strategy supported entirely on $p$.

If $\nu$ and $\mu$ are mixed strategies, I will write $P_{i}^Q(\nu,\mu)$ for the corresponding expected payoff to player $i$; that is:

$$P_{i}^Q(\nu,\mu) = \int P_i(p, q)d\nu(p)d\mu(q)$$

**Example 1.3. The Prisoners' Dilemma.** In [EW], Eisert and Wilkens [EW] analyze the quantum version of the Prisoners’ Dilemma:

<table>
<thead>
<tr>
<th>Player One</th>
<th>Player Two</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td>(3, 3)</td>
</tr>
<tr>
<td></td>
<td>(0, 5)</td>
</tr>
<tr>
<td>D</td>
<td>(5, 0)</td>
</tr>
<tr>
<td></td>
<td>(1, 1)</td>
</tr>
</tbody>
</table>

which has the following equilibrium in mixed quantum strategies:

Player 1 plays the quaternions 1 and $i$, each with probability 1/2.
Player 2 plays the quaternions $j$ and $k$, each with probability 1/2.

To check that this is indeed a Nash equilibrium, first take Player 1’s strategy as given and suppose Player 2 plays the quaternion $q = q_1 + q_2i + q_3j + q_4k$, so that $iq = (-q_2) + q_1i + (-q_4)j + q_3k$. Then Player 2’s expected payoff is

$$\frac{1}{2}P_2(1, q) + \frac{1}{2}P_2(i, q) = \frac{1}{2}(q_1^2 \cdot 3 + q_2^2 \cdot 1 + q_3^2 \cdot 5 + q_4^2 \cdot 0) + \frac{1}{2}((-q_2)^2 \cdot 3 + q_1^2 \cdot 1 + (-q_4)^2 \cdot 5 + q_3^2 \cdot 0)$$

$$= 2q_1^2 + 2q_2^2 + (5/2)q_3^2 + (5/2)q_4^2$$

which is to be maximized subject to the condition that $q$ is a unit quaternion, i.e.

$$q_1^2 + q_2^2 + q_3^2 + q_4^2 = 1$$

Clearly this is maximized when $q_0 = q_1 = 0$, e.g. at $j$ and $k$. Thus Player 2 is optimizing, and similarly for Player 1.
Note that this equilibrium, in which each player receives an expected payoff of $5/2$, is Pareto-superior to the classical equilibrium (though still Pareto-supoptimal).

Our goal is to classify the Nash equilibria in $G^Q$. The definitions that occupy the remainder of this section kick off that process by partitioning the set of Nash equilibria into natural equivalence classes.

**Definition 1.4.** Two mixed strategies $\mu$ and $\mu'$ are equivalent if
\[
\int \pi_t(pq)d\mu(q) = \int \pi_t(pq)d\mu'(q)
\]
for all unit quaternions $p$ and all $t = 1, 2, 3, 4$.

In other words, $\mu$ and $\mu'$ are equivalent if in every quantum game and for every quantum strategy $p$, we have $P_1(p, \mu) = P_1(p, \mu')$ and $P_2(p, \mu) = P_2(p, \mu')$.

**Example 1.5.** The strategy supported on the singleton $\{p\}$ is equivalent to the strategy supported on the singleton $\{-p\}$ and to no other singleton.

**Definition 1.6.** Let $\nu$ be a mixed strategy and $u$ a unit quaternion. The right translate of $\nu$ by $u$ is the measure $\nu_u$ defined by $(\nu_u)(A) = \nu(Au)$ where $A$ is any subset of the unit quaternions and $Au = \{xu | x \in A\}$. Similarly, the left translate of $\nu$ by $u$ is defined by $(u\nu)(A) = \nu(uA)$. The following proposition is immediate:

**Proposition 1.7.** Let $(\nu, \mu)$ be a pair of mixed strategies and $u$ a unit quaternion. Then in any game $G^Q$, $(\nu, \mu)$ is a mixed strategy Nash equilibrium if and only if $(\nu_u, u^{-1}\mu)$ is.

**Definition 1.8.** Two pairs of mixed strategies $(\nu, \mu)$ and $(\nu', \mu')$ are equivalent if there exists a unit quaternion $u$ such that $\nu'$ is equivalent to $\nu u$ and $\mu'$ is equivalent to $u^{-1}\mu$. Note that this definition is independent of any particular game.

**Proposition 1.9.** In a given game, a pair of mixed strategies is a Nash equilibrium if and only if every equivalent pair of mixed strategies is also a Nash equilibrium.

**2. Preliminary Results.**

Theorems 2.1, 2.2 and 2.4 are the main results which will be used in Section 3 to classify Nash equilibria.

**Theorem 2.1.** Every mixed strategy is equivalent to a mixed strategy supported on (at most) four points. Those four points can be taken to form an orthonormal basis for $\mathbb{R}^4$. 
Proof. First, choose any orthonormal basis \( \{ q_1, q_2, q_3, q_4 \} \) for \( \mathbb{R}^4 \). For any quaternion \( p \), write (uniquely)

\[
p = \sum_{\alpha=1}^{4} A_\alpha(p)q_\alpha
\]

where the \( A_\alpha(p) \) are real numbers.

Define a probability measure \( \nu \) supported on the four points \( q_\alpha \) by

\[
\nu(q_\alpha) = \int_{S^3} A_\alpha(q)^2 d\mu(q)
\]

For any two quaternions \( p \) and \( q \), define

\[
X(p, q) = \sum_{\alpha=1}^{4} \pi_\alpha(p)\pi_\alpha(q)X_i
\]

(2.1.1)

Then for any \( p \) we have

\[
P(p, \mu) = \int_{S^3} P(pq) d\mu(q)
\]

\[
= \int_{S^3} P \left( \sum_{\alpha=1}^{4} A_\alpha(q)pq_\alpha \right) d\mu(q)
\]

\[
= \sum_{\alpha=1}^{4} P(pq_\alpha) \int_{S^3} A_\alpha(q)^2 d\mu(q) + 2 \sum_{\alpha \neq \beta} X(pq_\alpha, pq_\beta) \int_{S^3} A_\alpha(q)A_\beta(q) d\mu(q)
\]

\[
= P(p, \nu) + 2 \sum_{\alpha \neq \beta} X(pq_\alpha, pq_\beta) \int_{S^3} A_\alpha(q)A_\beta(q) d\mu(q)
\]

To conclude that \( \mu \) is equivalent to \( \nu \) it is sufficient (and necessary) to choose the \( q_\alpha \) so that for each \( \alpha \neq \beta \) we have

\[
\int_{S^3} A_\alpha(q)A_\beta(q) d\mu(q) = 0
\]

For this, consider the function \( B : \mathbb{R}^4 \times \mathbb{R}^4 \rightarrow \mathbb{R} \) defined by

\[
B(a, b) = \int_{S^3} \pi_1(\overline{a}q)\pi_1(\overline{b}q) d\mu(q)
\]

\( B \) is a bilinear symmetric form and so can be diagonalized; take the \( q_\alpha \) to be an orthonormal basis with respect to which \( B \) is diagonal. Then we have (for \( \alpha \neq \beta \))

\[
\int_{S^3} A_\alpha(q)A_\beta(q) d\mu(q) = \int_{S^3} \pi_1(\overline{q_\alpha}q)\pi_1(\overline{q_\beta}q) d\mu(q)
\]

\[
= B(q_\alpha, q_\beta) = 0
\]

7
Theorem 2.2. Taking Player 2’s (mixed) strategy $\mu$ as given, Player 1’s optimal response set is equal to the intersection of $S^3$ with a linear subspace of $\mathbb{R}^4$.

(Recall that we identify the unit quaternions with the three-sphere $S^3$.)

Proof. Player One’s problem is to choose $p \in S^3$ to maximize

$$P_1(p, \mu) = \int P_1(pq)d\mu(q) \quad (2.2.1)$$

Expression (2.2.1) is a (real) quadratic form in the coefficients $\pi_i(p)$ and hence is maximized (over $S^3$) on the intersection of $S^3$ with the real linear subspace of $\mathbb{R}^4$ corresponding to the maximum eigenvalue of that form.

Definition 2.3. We define the function $K : S^3 \to \mathbb{R}$ by $K(A + Bi + Cj + Dk) = ABCD$. Thus in particular $K(p) = 0$ if and only if $p$ is a linear combination of at most three of the fundamental units $\{1, i, j, k\}$.

Theorem 2.4. Let $\mu$ be a mixed strategy supported on four orthogonal points $q_1, q_2, q_3, q_4$ played with probabilities $\alpha, \beta, \gamma, \delta$. Suppose $p$ is an optimal response to $\mu$ in some game where it is not the case that $X_1 = X_2 = X_3 = X_4$. Then $p$ must satisfy:

$$(\alpha - \beta)(\alpha - \gamma)(\alpha - \delta)K(pq_1) + (\beta - \alpha)(\beta - \delta)(\beta - \gamma)K(pq_2)$$

$$+ (\gamma - \alpha)(\gamma - \beta)(\gamma - \delta)K(pq_3) + (\delta - \alpha)(\delta - \beta)(\delta - \gamma)K(pq_4) = 0 \quad (2.4.1)$$

Proof. Set $p_n = \pi_n(p)$ and consider the function

$$\mathcal{P} : S^3 \times \mathbb{R}^4 \to \mathbb{R} \quad (p, x) \mapsto \sum_{n=1}^4 p_n^2x_n d\mu(q)$$

In particular, if we let $X = (X_1, X_2, X_3, X_4)$ then $\mathcal{P}(p, X) = P_1(p, \mu)$.

The function $\mathcal{P}$ is quadratic in $p$ and linear in $x$; explicitly we can write

$$\mathcal{P}(p, x) = \sum_{i,j,k} t_{ijk} p_i p_j x_k$$

for some real numbers $t_{ijk}$. 

8
Set

\[ M_{ij}(x) = \sum_{k=1}^{4} t_{ijk} x_k \]
\[ N_{ij}(p) = \sum_{k=1}^{4} t_{ikj} p_j \]

so that

\[ M(x) \cdot \begin{pmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{pmatrix} = N(p) \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \] (2.4.2)

If \( p \) is an optimal response to the strategy \( \mu \), then \( (p_1, p_2, p_3, p_4)^T \) must be an eigenvector of \( M(X) \), say with associated eigenvalue \( \lambda \). From this and (2.4.2) we conclude that

\[ N(p) \cdot \begin{pmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \lambda \cdot \begin{pmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{pmatrix} = N(p) \cdot \begin{pmatrix} \lambda \\ \lambda \\ \lambda \\ \lambda \end{pmatrix} \]

where the second equality holds by an easy calculation.

Thus \( N(p) \) must be singular. But it follows from a somewhat less easy calculation that the determinant of \( N(p)/2 \) is given by the left side of (2.4.1).

3. Classification.

**Definition 3.1.** Let \( G \) be a two-by-two game with payoff pairs \( (X_1, Y_1), \ldots, (X_4, Y_4) \) (listed in arbitrary order). \( G \) is a **generic game** if the \( X_i \) are all distinct, the \( Y_i \) are all distinct, the twofold sums \( X_i + X_j \) are all distinct and the twofold sums \( Y_i + Y_j \) are all distinct.

Theorem 3.3 will classify Nash Equilibria in \( G^Q \) where \( G \) is any generic two-by-two game. Subtler versions of the same arguments work for non-generic games (yielding somewhat messier results); see [NE].

To state Theorem 3.3 we need a definition:

**Definition 3.2.** Let \( p, q, r, s \) be quaternions; write \( p = p_1 + p_2i + p_3j + p_4k \), etc. Then the quadruple \( (p, q, r, s) \) is **intertwined** if there is a nonzero constant \( \alpha \) such that

\[ \alpha(X p + Y q) = X r + Y s \]

identically in the polynomial variables \( X \) and \( Y \).

Thus if the components of \( p, q, r, s \) are all nonzero, then \( (p, q, r, s) \) is intertwined if and only if the four quotients \( \frac{p_{1}}{q_{1}}, \frac{p_{2}}{q_{2}}, \frac{p_{3}}{q_{3}}, \frac{p_{4}}{q_{4}} \) are equal (in some order) to the four quotients \( \frac{r_{1}}{s_{1}}, \frac{r_{2}}{s_{2}}, \frac{r_{3}}{s_{3}}, \frac{r_{4}}{s_{4}} \).
The intertwined quadruple \((p, q, r, s)\) is \textit{fully intertwined} if \((p, r, q, s)\) is also intertwined.

We can now state the main theorem:

**Theorem 3.3.** Let \(G\) be a generic game. Then up to equivalence, every equilibrium in \(G^Q\) is of one of the following types:

a) Each player plays each of four orthogonal quaternions with probability 1/4.

b) Each player’s strategy is supported on three of the four quaternions \(1, i, j, k\).

c) \(\mu\) is supported on two orthogonal points \(1, v\); \(\nu\) is supported on two orthogonal points \(p, pu\), and the quadruple \((p, pv, pu, pvu)\) is fully intertwined.

d) Each of \(\mu\) and \(\nu\) is supported on two orthogonal points, each played with probability 1/2. Moreover, the supports of \(\mu\) and \(\nu\) lie in parallel planes.

e) Each player plays a pure strategy from the four point set \(\{1, i, j, k\}\).

**Proof.** Let \((\nu, \mu)\) be an equilibrium. By (2.1) we can assume that each of \(\nu\) and \(\mu\) is supported on a set of at most four orthogonal points. Applying a translation as in (1.8) we can assume that the support of \(\mu\) contains the quaternion 1. Then from standard facts about orthogonality in the space of quaternions, the support of \(\mu\) is contained in a set of the form \(\{1, u, v, uv\}\) where \(u^2 = v^2 = -1\) and \(uv + vu = 0\), played with probabilities of \(\alpha, \beta, \gamma, \delta \geq 0\). We will maintain these assumptions and this notation while proving Theorems 3.4, 3.5, 3.9, and 3.10, which together imply Theorem 3.3.

**Theorem 3.4.** \(\nu\) is a pure strategy if and only if \(\mu\) is a pure strategy.

**Proof.** If \(\nu\) is a pure strategy, Player Two can guarantee any desired probability distribution over four outcomes; by genericity his optimal probability distribution is unique.

**Theorem 3.5.** If the support of \(\nu\) contains four points then \(\mu\) assigns probability 1/4 to each of four strategies.

**Proof.** Explicitly write \(u = Ai + Bj + Ck, v = Di + Ej + Fk, uv = Gi + Hj + Ik\). Write

\[
\mathcal{M} = \begin{pmatrix}
AB & DE & GH \\
AD & DF & GI \\
BC & EF & HI
\end{pmatrix}
\]

By (2.2) the quadratic form

\[
p \mapsto P_1(p, \mu)
\]
is constant on the unit sphere $S^3$. Therefore its non-diagonal coefficients are all zero. Computing these coefficients explicitly and dividing by (non-zero) expressions of the form $(x_i - x_j)$, we get

$$M \cdot (\beta, \gamma, \delta)^T = (0, 0, 0)^T \quad (3.5.2)$$

But $M$ also kills the column vector $(1, 1, 1)^T$. Thus we have two cases:

Case I. $\beta = \gamma = \delta$. Then the four diagonal terms of (3.5.1) (which must all be equal) are given by $(X_1 + X_2 + X_3 + X_4)\beta + X_i(\alpha - \beta)$, with $i = 1, 2, 3, 4$. Since the $X_i$ are not all equal, it follows $\alpha = \beta = \gamma = \delta = 1/4$, proving the theorem.

Case II. $M$ has rank at most one. From this and the orthogonality of $u, v, uv$, we have $\{u, v, uv\} \cap \{i, j, k\} \neq \emptyset$. Assume $u = i$ (the other cases are similar). Then $A = 1$, $B = C = D = G = 0$, $H = -F$ and $I = E$. The four diagonal entries of (3.3.1) are now equal; call their common value $\lambda$ so that we have

$$\begin{pmatrix}
\alpha & \beta & E^2\gamma + F^2\delta & E^2\delta + E^2\gamma + F^2\delta \\
\beta & \alpha & E^2\gamma + F^2\delta & E^2\delta + E^2\gamma + F^2\delta \\
E^2\gamma + F^2\delta & E^2\gamma + F^2\delta & \alpha & \beta \\
E^2\delta + E^2\gamma + F^2\delta & E^2\delta + E^2\gamma + F^2\delta & \beta & \alpha
\end{pmatrix} \begin{pmatrix}X_1 \\ X_2 \\ X_3 \\ X_4\end{pmatrix} = \begin{pmatrix}\lambda \\ \lambda \\ \lambda \\ \lambda\end{pmatrix} \quad (3.5.3)$$

Combining (3.5.2), (3.5.3), the conditions $\alpha + \beta + \gamma + \delta = E^2 + F^2 = 1$ and the genericity conditions, we get $\alpha = \beta = \gamma = \delta$ as required.

**Corollary 3.5A.** If either player’s strategy has a four-point support, then each player plays each of four orthogonal quaternions with probability $1/4$.

**Proof.** Apply Theorem 3.5 twice, one as stated and once with the players reversed.

Theorem 3.9, dealing with the case where $\nu$ is supported on exactly three points, requires some preliminary lemmas:

**Lemma 3.6.** It is not the case that Player Two plays $1, u, v$ each with probability $1/3$.

**Proof.** If $1, u, v$ are played with probability $1/3$ then one computes that the eigenvalues of the form (2.2.1) are $X_1 + X_2 + X_3$, $X_1 + X_2 + X_4$, $X_1 + X_3 + X_4$, $X_2 + X_3 + X_4$, which are all distinct by genericity. Thus Player One responds with a pure strategy, and Theorem 3.4 provides a contradiction.

**Lemma 3.7.** Suppose the support of $\nu$ is contained in the linear span of $1, i, j$, and suppose that $1$ and $i$ are both optimal responses for Player Two. Then one of the following is true:

a) The support of $\nu$ is contained in the three point set $\{1, i, j\}$
b) The support of $\nu$ is contained in a set of the form \( \{1, E_i + F_j, -F_i + E_j\} \) with $E_i + F_j$ and $-F_i + E_j$ played equiprobably.

Moreover, if b) holds and either $j$ or $k$ is also an optimal response for Player Two, then 1 is played with probability zero.

**Proof.** Suppose $\nu$ is supported on three orthogonal quaternions $q_1 = A + B_i + C_j$, $q_2 = D + E_i + F_j$, $q_3 = G + H_i + I_j$, played with probabilities $\phi, \psi, \xi$. The first order conditions for Player Two’s maximization problem must be satisfied at both 1 and $i$; this (together with genericity for the game $G$) gives

\[
\begin{pmatrix}
AC & DF & GI \\
BC & EF & HI
\end{pmatrix}
\begin{pmatrix}
\phi \\
\psi \\
\xi
\end{pmatrix}
= \begin{pmatrix}
0 \\
0 \\
0
\end{pmatrix}
= \begin{pmatrix}
AC & DF & GI \\
BC & EF & HI
\end{pmatrix}
\begin{pmatrix}
1 \\
1 \\
1
\end{pmatrix}
\] (3.7.1)

so that by (3.6) with the players reversed, the matrix on the left has rank at most one. This (together with the orthogonality of $q_1, q_2, q_3$) gives $\{q_1, q_2, q_3\} \cap \{1, i, j\} \neq \emptyset$. We can assume $q_1 = 1$ (all other cases are similar); thus $A = 1, B = C = D = G = 0, \ H = -F, I = E$. Now (3.7.1) says $EF(\psi - \xi) = 0$. If $EF = 0$, then a) holds and if $\psi - \xi = 0$ then b) holds.

Now suppose $j$ is also an optimal response for Player Two. Then $0 = P_2(\nu, i) - P_2(\nu, j) = \phi(Y_2 - Y_3)$, so that by genericity $\phi = 0$. A similar argument works if $k$ is optimal.

**Lemma 3.8.** Suppose $\nu$ is supported on exactly three points and continue to assume that $\mu$ is supported on a subset of $\{1, u, v, uv\}$. Then at least two of the four quaternions $1, u, v, uv$ are optimal responses for Player One.

**Proof.** By (3.5), $\mu$ is supported on at most three points; we can rename so those points are $1, u, v$. These are played with probabilities $\alpha, \beta, \gamma$ and we can rename again so that $\alpha$ lies (perhaps not strictly) between $\beta$ and $\gamma$.

If $p$ is any optimal response by Player One, apply (2.4) with $\delta = 0$ (and possibly $\gamma = 0$) to get

\[
\sigma_1K(p) + \sigma_2K(pu) + \sigma_3K(pv) + \sigma_4K(puv) = 0
\] (3.8.1)

where $\sigma_1 = (\alpha - \beta)(\alpha - \gamma)\alpha$, etc., so that

\[
\sigma_1, \sigma_4 \leq 0 \quad \text{and} \quad \sigma_2, \sigma_3 \geq 0
\] (3.8.2)

Case I: Suppose none of the $\sigma_i$ is equal to zero. Then $\gamma \neq 0$ so a) holds.
By (2.2), the support of \( \nu \) spans a three-dimensional hyperplane in \( \mathbb{R}^4 \) and thus must include some quaternion of the form \( A + Bu \) \((A, B \in \mathbb{R})\). Inserting \( p = A + Bu \) into (3.8.1) gives

\[
AB(\sigma_1 B^2 - \sigma_2 A^2)K(1 + u) = 0
\]

(3.8.3)

Thus either \( AB = 0 \) (in which case either \( p = 1 \) or \( p = u \)) or \( K(1 + u) = 0 \). This and similar arguments establish the following:

1. If 1 and \( u \) are both suboptimal responses, then \( K(1 + u) = 0 \). (3.8.3a)
2. If 1 and \( v \) are both suboptimal responses, then \( K(1 + v) = 0 \). (3.8.3b)
3. If \( u \) and \( uv \) are both suboptimal responses, then \( K(1 + v) = 0 \). (3.8.3c)
4. If \( v \) and \( uv \) are both suboptimal responses, then \( K(1 + u) = 0 \). (3.8.3d)

Taken together, these imply that if the lemma fails, then \( K(1 + u) = K(1 + v) = 0 \). From this it follows that \( \{u, v, uv\} \cap \{\pm i, \pm j, \pm k\} \neq \emptyset \); assume without loss of generality that \( u = i \) and therefore \( v \) is in the linear span of \( \{j, k\} \). (Generality is not lost because the argument to follow works just as well, with obvious modifications, in all the remaining cases.)

Now we have

\[
P_1(A + Bv, \mu) = \alpha P_1(A + Bv) + \beta P_1(Ai + Bvi) + \gamma P_1(Av - B)
\]

\[
= A^2 \left( \alpha P_1(1) + \beta P_1(i) + \gamma P_1(v) \right) + B^2 \left( \alpha P_1(v) + \beta P_1(vi) + \gamma P_1(1) \right)
\]

which is maximized at an endpoint, so either 1 or \( v \) is an optimal response for Player One. Similarly, at least one from each pair \( \{1, uv\} \), \( \{u, v\} \), and \( \{u, uv\} \) is an optimal response, from which b) (and therefore the lemma) follows.

Case II: Suppose at least one of the \( \sigma_i \) is equal to zero. Up to renaming \( u \) and \( v \), there are three ways this can happen:

Subcase IIA: \( \alpha = \beta, \gamma = 0 \). As above, Player One’s optimal response set contains a quaternion of the form \( (A + Bu) \). But \( P_1(A + Bu, \mu) \) is independent of \( A \) and \( B \), so both 1 and \( u \) are optimal, proving the theorem. (Note that \( v \) and \( uv \) are also both optimal, so that in fact by (3.5A) this case never occurs.)
Subcase IIB: \( \alpha = \beta, \gamma \neq 0 \). By Lemma (3.6), \( \gamma \neq \alpha, \beta \). Thus \( \sigma_3 \) and \( \sigma_4 \) are nonzero, so (3.8.3b), (3.8.3c) and (3.8.3d) (but not (3.8.3a)) still hold. But \( \sigma_1 = \sigma_2 = 0 \) so the same techniques now yield

If 1 and \( u \) are both suboptimal responses, then \( K(1 + u) = 0 \). \hspace{1cm} (3.8.3e)

If 1 and \( v \) are both suboptimal responses, then \( K(1 + v) = 0 \). \hspace{1cm} (3.8.3f)

We can now repeat the argument from Case I.

Subcase IIC: \( \alpha \neq \beta, \gamma = 0 \). Now we have \( \sigma_1, \sigma_2 \neq 0, \sigma_3 = \sigma_4 = 0 \), so that (3.8.3a) through (3.8.3c) still hold, along with (3.8.3e) and (3.8.3f). We can now repeat the argument from Case I.

**Theorem 3.9.** If \( \nu \) is supported on exactly three points, then up to equivalence, both \( \mu \) and \( \nu \) are supported on three-point subsets of \( \{1, i, j, k\} \).

**Proof.** By (3.5) we can assume that \( \mu \) is supported on \( \{1, u, v\} \). By (3.8) we can assume without much loss of generality that 1 and \( u \) are optimal responses for Player One. (The argument below works equally well, with obvious modifications, for other pairs.) Let \( w \) be a quaternion orthogonal to 1 and \( u \) such that the support of \( \nu \) is contained in the linear span of 1, \( u \) and \( w \).

By (2.2), any quaternion of the form \( X + Yu + Zw \) is an optimal response for Player One, so by (2.4) we have

\[
\sigma_1 K(X + Yu + Zw) + \sigma_2 K(Xu - Y + Zwu) + \sigma_3 K(Xv + Yu + Zwv) + \sigma_4 K(Xuv - Yv + Zwuv) = 0
\]

identically in \( X, Y, Z \). Writing out the left side as a polynomial in these three variables, the coefficients, all of which must vanish, can be expressed in terms of the components of \( u, v, w \). Setting all these expressions equal to zero and solving, we find that \( \{u, v, w\} \in \{\pm i, \pm j, \pm k\} \). (The details of this tedious but straightforward calculation can be found on pages 32-33 of [NE].) We assume \( u = i, w = j \).

**Claim:** Player Two’s strategy is not supported just on 1 and \( i \). **Proof:** If so, the fact that \( P_1(1, \mu) = P_1(i, \mu) \) implies that \( \mu \) assigns equal weights to 1 and \( i \), which implies \( P_1(j, \mu) = P_1(k, \mu) \), contradicting the fact that \( j \) but not \( k \) is optimal for Player One.

Thus the support of \( \mu \) is a three-point subset of \( \{1, i, j, k\} \). It now follows from Lemma (3.8) (together with the assumption that the support of \( \nu \) contains three points) that the support of \( \nu \) is \( \{1, i, j\} \), completing the proof.
**Theorem 3.10.** Suppose $\nu$ is supported on two points. Then $\mu$ is supported on $1$, $u$ and $\nu$ is supported on two quaternions $p, pv$ where either

a) The quadruple $(p, pu, pv, pvu)$ is fully intertwined or

b) $u = v$ and each player plays each strategy with probability $1/2$.

**Proof.** Suppose 1 and $u$ are played with probabilities $\alpha$ and $\beta$.

Any unit quaternion of the form $Xp + Ypv$ is an optimal response for Player One; thus (2.4) with $q_1 = 1, q_2 = u, \gamma = \delta = 0$ gives

$$(\alpha - \beta) (\alpha^2 K(Xp + Ypv) - \beta^2 K(Xpv + Ypv)) = 0$$

This, plus the identical observation with the players reversed, establishes full intertwining except when $\alpha = \beta = 1/2$. In that case, $P_1(p, \mu) = P_1(pu, \mu)$ so $pu$ must be optimal; i.e. we can take $v = u$. 

This completes the proof of Theorem 3.3.

**Example 3.11.** We apply Theorem 3.3 to find all mixed strategy quantum equilibria in the Prisoner’s Dilemma (1.3).

First, there are certainly equilibria of the form (3.3a): Each player chooses any four orthogonal quaternions and plays each with probability $1/4$. Any such pair of strategies is an equilibrium; in any such equilibrium, each player earns an expected payoff of $9/4 = 2.25$.

There are also equilibria of the form (3.3d); (1.3.2) is such an equilibrium. Up to equivalence, this is the only one. Sketch of proof: Player 2 plays 1 and $v$ equiprobably where $v = Si + Tj + Uk$. Write down the first order conditions for Player One’s problem to find a circle of optimal responses. Player One chooses $p$ and $pv$ on this circle; from the explicit first order conditions we can take $p$ proportional to

$$\left(U(21 - 24S^2 - 20T^2 + 3\sqrt{49 - 48S^2 - 40T^2}, T(23 - 24S^2 - 20T^2 + \sqrt{49 - 48S^2 - 40T^2}, 4S(6S^2 + 5t^2 - 6), 0)\right)$$

(We can assume this choice of $p$ because any two points on the optimal circle yield the same maximization problem for Player Two—this is essentially because two strategies are played equiprobably.) Now we can write down the first order conditions for Player Two’s problem and require that they be satisfied at 1. For $S \neq 0, 1$, the resulting equations imply $T^2 < 0$ or $U^2 < 0$, contradiction. For $S = 0$, the first order
conditions are automatically satisfied but the quaternion 1 minimizes rather than maximizes Player Two’s payoff (an optimal response is \(i\)); this rules out \(S = 0\). That leaves \(S = 1\), which is (1.3.2).

An analogous search for equilibria of the form (3.3c) would require substantially more computational resources than are available to the author. (For one thing, there are now six independent first order conditions instead of three; for another, it now matters which points on his optimal circle Player One chooses.) However, such equilibria can be ruled out on the basis of [I], which characterizes all fully intertwined quadruples. Checking each of the possibilities is straightforward, though (very) tedious.

There are no equilibria of the form (3.3e) thanks to the remarks in (1.2).

Finally, I claim there are no equilibria of the form (3.3b). Suppose for example that Player Two’s strategy is supported on \(\{1, i, j\}\) with probabilities \(p, q, r\). Then three of the strategies 1, i, j, k must return the same payoff to Player One; that is, three of the expressions
\[
3p + q \quad p + 3q + 5r \quad 5q + 3r \quad 5p + r
\]

must be equal. Together with \(p, q, r > 0\) and \(p + q + r = 1\), this implies \((p, q, r) = (14/25, 9/25, 2/25)\) or \((p, q, r) = (14/31, 12/31, 5/31)\). In the former case, Player 1’s unique optimal play is \(k\) (for a payoff of 72/25, as opposed to 51/25 for plays of 1, i, j); thus we can rule this out. In the latter case, Player One’s optimal responses are \(i, j, k\) so he plays these with some probabilities \(p’, q’, r’\). But then Player One’s payoffs for 1, i, j are \(p’ + 5q’, 3p’ + 5r’, 3q’ + r’\), and for these to be equal we must have \(p’ < 0\) (specifically \(p’ = -5/11\)); contradiction. Thus Player Two’s strategy is not supported on \(\{1, i, j\}\). The same calculation rules out the other three-element subsets of \(\{1, i, j, k\}\) as well.

**Remark.** The statement of Theorem 3.3 makes it natural to ask for a classification of fully intertwined quadruples of the form \((p, pv, pu, pvu)\) with \(u, v\) square roots of \(-1\). That classification is provided in [I]. The thrust of the result is this: All such quadruples fall into one of approximately 15 families. Each of these families is at most four-dimensional. For all but one of the families, it is easy to tell by inspection whether a given quadruple satisfies the membership condition. The exceptional family is one-dimensional.

In short: Condition b) of Theorem 3.3 allows only four dimensions worth of possible equilibria, all of which are easily identifiable except for a one-dimensional subset.
I have listed these fifteen families in the appendix; again, see [I] for the (tedious) proof that this list is exhaustive.

4. Minimal Payoffs and Opting Out

Theorem 3.3. classifies all mixed strategy Nash equilibria in generic games. Here we briefly address the issue of whether these equilibria survive in a larger game where the players can opt out of the assigned communication protocol.

A key tool is the very simple Theorem 4.1; this and its corollary 4.1A apply to all two by two games (whether generic or not) and are of independent interest:

**Theorem 4.1.** Let $G$ be a game with payoff pairs $(X_1,Y_1),\ldots,(X_4,Y_4)$. Then in any mixed strategy quantum equilibrium, Player One earns at least $(X_1 + X_2 + X_3 + X_4)/4$.

**Proof.** Player One maximizes the quadratic form (2.2.1) over the sphere $S^3$. The trace of this form is $X_1 + X_2 + X_3 + X_4$, so the maximum eigenvalue must be at least $(X_1 + X_2 + X_3 + X_4)/4$. □

**Corollary 4.1A.** If, in Theorem 4.1, the game $G$ is zero-sum, then in any mixed strategy quantum equilibrium, Player One earns exactly $(X_1 + X_2 + X_3 + X_4)/4$.

**Proof.** Apply (4.1) to both players. □

4.2. Remarks on Opting Out. A player can throw away his entangled penny and substitute an unentangled penny (or for that matter a purely classical penny, but this offers no additional advantage, because the unentangled quantum penny can always be returned in one of the two classical states $H$ or $T$). However, a simple quantum mechanical calculation shows that if Player One unilaterally substitutes an unentangled penny, then no matter what strategies the players follow from there, the result is a uniform distribution over the four possible outcomes. By Theorem 4.1, Player One considers this weakly inferior to any $G^Q$ equilibrium. Thus, even if we allow players to choose their pennies, all of the $G^Q$ equilibria survive.

Appendix: Intertwining

The following result is proved in [I]:

**Theorem 4.1.** Suppose $(p, pv, pu, pvu)$ is fully intertwined, where $p$ is an arbitrary unit quaternion and $u, v$ are square roots of $-1$. Then, up to permuting $i, j$ and $k$, and writing $\langle p, q \rangle$ for the circle
generated by \( p \) and \( q \), at least one of the following holds:

i) \( u = i, \quad v \in \{ p_i, p_j, p_k, p \} \)

ii) \( u = i, \quad v \in < i, p \)  

ii') \( u \in < i, p >, \quad v = p_i \)

iii) \( p \in < 1, i > < 1, j >, \quad u = i, \quad v \in p < i, k > \)

iii') \( p \in < 1, i > < 1, j >, \quad v = p_i \), \( u \in < i, k > \)

iv) \( u = i \) and \( v \) is (uniquely) determined by one of the following three conditions:

\[
\begin{align*}
    pv & \sim (-A(C^2 + D^2), -B(C^2 + D^2), C(A^2 + B^2), D(A^2 + B^2)) \\
    pv & \sim (-C(BC + AD), D(BC + AD), B(AC - BD), A(AC - BD)) \\
    pv & \sim (D(AC - BD), C(AC - BD), -A(BC + AD), B(BC + AD))
\end{align*}
\]

where \( p = (A, B, C, D) \)

iv') \( v = p_i \) and \( u \) is uniquely determined by one of the following three conditions:

\[
\begin{align*}
    pu & \sim (-A(C^2 + D^2), -B(C^2 + D^2), C(A^2 + B^2), D(A^2 + B^2)) \\
    pu & \sim (-D(BD + AC), C(BD + AC), A(AD - BC), B(AD - BC)) \\
    pu & \sim (C(AD - BC), D(AD - BC), -B(BD + AC), A(BD + AC))
\end{align*}
\]

where \( p = (A, B, C, D) \)

v) \( p \in < 1, i > \cup < j, k > \quad u, v \in \{ i \} \cup < j, k > \)

vi) \( p \in < i, j > < 1, v >, \quad u = v \in < i, j > \)

vii) For some \( (A, B, C) \) with \( A^2 + B^2 + C^2 = 1 \) we have:

\[
\begin{align*}
    p & \sim (A, A, 0, 2C) \quad \text{or} \quad p \sim (A, -A, -2B, 0)
\end{align*}
\]

and \( u, v \) given by one of the following pairs of expressions:

\[
\begin{align*}
    u & \sim (0, C - B, A, -A) \quad \text{and} \quad v \sim (0, A^2 + 2BC, A(B - C), A(C - B)) \\
    \text{or} \quad u & \sim (0, -B - C, A, A) \quad \text{and} \quad v \sim (0, A^2 - 2BC, A(B + C), A(B + C))
\end{align*}
\]
viii) $p = (0, A, B, \pm B), u = (0, X, Y, \pm Y)$ and $v \sim (0, 2ABX - Y, 2B^2X, \pm 2B^2X)$

ix) $p = (AY - 2BX, 0, BY, \mp BY)$, with $u$ and $v$ as in (viii).

x) $u = v \perp p \perp 1$

xi) $u = v \perp i\,p \perp 1$

xii) $v = (j \pm k)/\sqrt{2} \quad p \in \langle 1, i, v \rangle \cup \langle i, u \rangle \quad u = p^{\dagger}p$

xii') $u = (j \pm k)/\sqrt{2} \quad p \in \langle 1, i, u \rangle \cup \langle i, u \rangle \quad v = i$

xiii) $(p, v, u)$ is a real point on a certain one-dimensional algebraic variety $X_0$.

References


