Intertwining

by

Steven E. Landsburg

A *two by two* game is a game with two players, each of whom has a two-point strategy space. To such a game there is an *associated quantum game* in which each player's strategy space consists of the set of all probability distributions on the unit quaternions. Roughly, the associated quantum game is the game that results when players communicate their strategies to a referee through maximally entangled quantum channels. Quantum games were introduced in [EW] and [EWL]; see [QGT] for an overview.

This paper completes the project, begun in [NE], of classifying all possible Nash equilibria in these quantum games. [NE] reduces the classification problem to a problem about quaternions (Problem A below). This paper solves that problem and therefore completes the classification.

In more detail: I showed in [NE] that, up to a suitable notion of equivalence, players' equilibrium strategies, which are *a priori* arbitrary probability distributions on the unit quaternions, can in fact be taken to be supported on at most four points. Moreover, when either player's strategy is concentrated on one, three or four points, it is fairly easy to describe what the equilibrium must look like.

That leaves the case where each player chooses a probability distribution supported on exactly two points. In that case, I showed that (again up to a suitable notion of equivalence), the two players' strategies are supported on sets of the form $\{1, \mathbf{u}\}$ and $\{\mathbf{p}, \mathbf{pv}\}$ for some $\mathbf{p}, \mathbf{u}, \mathbf{v}$ such that $\mathbf{u}^2 = \mathbf{v}^2 = -1$ and $(\mathbf{p}, \mathbf{pv}, \mathbf{pu}, \mathbf{pvu})$ has the property of being *fully intertwined*, which I shall now define:

Given a quaternion $\mathbf{p} = A + Bi + Cj + Dk$ $(A, B, C, D \in \mathbf{R})$, I define $K(\mathbf{p}) = ABCD$. I say that a 4-tuple of quaternions $(\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s})$ is *intertwined* if $K(X\mathbf{p}+Y\mathbf{q}) = \alpha K(X\mathbf{r}+Y\mathbf{s})$ for some non-zero real constant α. Here X and Y are polynomial variables and equality means equality of polynomials. I say that $(\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s})$ is *fully intertwined* if both $(\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s})$ and $(\mathbf{p}, \mathbf{r}, \mathbf{q}, \mathbf{s})$ are intertwined.

Therefore the problem to be solved is:

Problem A. Find all triples of unit quaternions $(\mathbf{p}, \mathbf{v}, \mathbf{u})$ such that $\mathbf{v}^2 = \mathbf{u}^2 = -1$ and $(\mathbf{p}, \mathbf{pv}, \mathbf{pu}, \mathbf{pvu})$ is fully intertwined.

Thanks to Keith Dennis, Dan Grayson and Mike Stillman.

Theorem 6 of the present paper solves Problem A by classifying all such triples into roughly a dozen families. With one exception, these families are at most four-dimensional and easy to describe. The exceptional family is harder to describe but only one-dimensional. Thus the thrust of the Theorem 6 is that all potential Nash equilibria are easy to describe, except for a small subset of codimension 3.

The classification proceeds from the observation that $(\mathbf{p},\mathbf{q},\mathbf{r},\mathbf{s})$ is intertwined if and only if at least one of the following holds (writing $\mathbf{p}=\mathbf{p}_1+\mathbf{p}_2 i+\mathbf{p}_3 j+\mathbf{p}_4 k$, etc.):

$$\begin{gathered}(X\mathbf{p}+Y\mathbf{q})_i=\alpha_i(X\mathbf{r}+Y\mathbf{s})_{\sigma(i)})\\ \text{for some nonzero } \alpha_1,\dots\alpha_4\in\mathbf{R} \text{ and some permutation } \sigma \text{ of } \{1,2,3,4\}\end{gathered}\tag{$INT1$}$$

$$K(X\mathbf{p}+Y\mathbf{q})=K(X\mathbf{r}+Y\mathbf{s})=0\tag{$INT2$}$$

I will say that $(\mathbf{p},\mathbf{q},\mathbf{r},\mathbf{s})$ is *intertwined of Type One* if (INT1) holds and *intertwined of Type Two* if (INT2) holds.

I will say that $(\mathbf{p},\mathbf{q},\mathbf{r},\mathbf{s})$ is *fully intertwined of Type One* if both $(\mathbf{p},\mathbf{q},\mathbf{r},\mathbf{s})$ and $(\mathbf{p},\mathbf{r},\mathbf{q},\mathbf{s})$ are intertwined of Type One. I will say that $(\mathbf{p},\mathbf{q},\mathbf{r},\mathbf{s})$ is *fully intertwined of Type Two* if it is fully intertwined, and at least one of $(\mathbf{p},\mathbf{q},\mathbf{r},\mathbf{s})$, $(\mathbf{p},\mathbf{r},\mathbf{q},\mathbf{s})$ is intertwined of Type Two.

Then Problem A can be divided into two pieces:

Problem A1. Classify all triples $(\mathbf{p},\mathbf{v},\mathbf{u})$ such that $\mathbf{v}^2=\mathbf{u}^2=-1$ and such that $(\mathbf{p},\mathbf{pv},\mathbf{pu},\mathbf{pvu})$ is fully interwined of Type One.

Problem A2. Classify all triples $(\mathbf{p},\mathbf{v},\mathbf{u})$ such that $\mathbf{v}^2=\mathbf{u}^2=-1$ and such that $(\mathbf{p},\mathbf{pv},\mathbf{pu},\mathbf{pvu})$ is fully intertwined of Type Two.

In Section 1, I address a problem that is both more general and more special than Problem A1, namely:

Problem B. Find all triples of unit quaternions $(\mathbf{r},\mathbf{v},\mathbf{u})$ such that $\mathbf{r}^2=\mathbf{v}^2=\mathbf{u}^2=-1$ and $(\mathbf{r},\mathbf{rv},\mathbf{ru},\mathbf{rvu})$ is intertwined of Type One.

Problem B is more general than Problem A1 because it requires (Type One) intertwining but not *full* Type One intertwining. But it is also more special than Problem A because of the requirement that $\mathbf{r}^2 = -1$.

In Section 2, I apply the results of Section 1 to the solution of Problem A. A key observation is that any solution to Problem A1 must be of the form $(S\mathbf{r}+T\mathbf{rv}, \mathbf{v}, \mathbf{u})$ where $(\mathbf{r}, \mathbf{v}, \mathbf{u})$ is a solution to Problem B.

This paper uses the following conventions and notation:

1) $\mathbf{r}, \mathbf{u}$, and $\mathbf{v}$ always represent quaternion square roots of -1. $\mathbf{p}$ always represents an arbitrary unit quaternion. I will often write quaternions as 4-tuples of real numbers.

2) For the applications to quantum game theory, it is natural to identify a quaternion $\mathbf{p}$ with its negative $-\mathbf{p}$. Therefore *throughout this paper, equality of quaternions is used to mean equality up to a sign*; that is, I write $\mathbf{p} = \mathbf{q}$ to mean $\mathbf{p} = \pm\mathbf{q}$.

3) In accordance with 2), I will use the word *unique* to mean "unique up to a sign".

4) I write $\mathbf{p} \sim \mathbf{q}$ to mean that $\mathbf{q} = \alpha\mathbf{p}$ for some nonzero real number α.

5) Given two expressions of the form A/B, C/D, $A, B, C, D \in \mathbf{R}$, I write $A/B = C/D$ to mean that $AD = BC$, and $A = B = 0$ if and only if $C = D = 0$.

6) When $\mathbf{p}$ and $\mathbf{q}$ are unit quaternions, I will write $< \mathbf{p}, \mathbf{q} >$ for the circle generated by $\mathbf{p}$ and $\mathbf{q}$, i.e. the set $\{S\mathbf{p} + T\mathbf{q} | S^2 + T^2 = 1\}$

Section 1: Solution to Problem B.

Throughout this section, $\mathbf{r}, \mathbf{v}$ and $\mathbf{u}$ are square roots of -1 and I write $\mathbf{r} = (0, A, B, C)$.

Note that if $(\mathbf{r}, \mathbf{rv}, \mathbf{ru}, \mathbf{rvu})$ is intertwined, then $\mathbf{ru}$ must have a coordinate equal to zero. Up to permuting i, j and k, this is either the first or the second coordinate. Thus we have either $\mathbf{r} \perp \mathbf{u}$ or (still up to a permutation) $\mathbf{r} \perp i\mathbf{u}$. Theorems 2 and 3 solve Problem B in these two cases and hence, taken together, provide a complete solution to that problem.

Theorem 1. Suppose $(\mathbf{r}, \mathbf{rv}, \mathbf{ru}, \mathbf{rvu})$ is intertwined of Type One and $ABC = 0$.

Then, up to permuting i, j and k, one of the following holds:

1.i) $\mathbf{u} \in \{i, j, k\}$

1.ii) $\mathbf{r}, \mathbf{u}, \mathbf{v} \in < i, j >$

Proof. Case One: Exactly one of A, B, C is nonzero (that is, $\mathbf{r} \in \{i, j, k\}$). Type One intertwining implies that exactly one component of $\mathbf{ru}$ is nonzero, from which (1.i) follows.

Case Two: Exactly two of A, B, C are nonzero; without loss of generality suppose $\mathbf{r} = (0, A, B, 0)$ with $AB \neq 0$.

Then Type One intertwining implies that $\mathbf{ru}$ has exactly two nonzero components. Orthogonality requires these components to be the first and last (unless $\mathbf{u} = k$ in which case we're done anyway); that is $\mathbf{ru} = (G, 0, 0, H)$ with $GH \neq 0$. In other words, $\mathbf{r}, \mathbf{u} \in < i, j >$.

Now orthogonality allows us to write

$$\mathbf{rv} = (J, -BX, AX, K)$$

from which it follows that

$$\mathbf{rvu} = (-HX, M, N, GX)$$

If $X = 0$ then $\mathbf{v} \in < i, j >$ and condition (1.ii) holds, so we can assume otherwise. Then intertwining gives an equality of sets

$$\{-B/A, A/B\} = \{-H/G, G/H\}$$

That is, either $AH = BG$ or $AG = -BH$, so that $\mathbf{u} \in \{i, j\}$, giving condition (1.i). ∎

Theorem 2. Suppose $\mathbf{r} = (0, A, B, C)$ with $ABC \neq 0$. Then there are at most six pairs $(\mathbf{u}, \mathbf{v})$ such that $\mathbf{r} \perp \mathbf{u}$ and $(\mathbf{r}, \mathbf{rv}, \mathbf{ru}, \mathbf{rvu})$ is Type One intertwined.

Proof. Suppose $\mathbf{r} \perp \mathbf{u}$ and $(\mathbf{r}, \mathbf{rv}, \mathbf{ru}, \mathbf{rvu})$ is Type One intertwined. We can write

$$\mathbf{ru} = (\,0, \quad G, \quad H, \quad I\,) \quad (GHI \neq 0) \qquad \text{and} \qquad \mathbf{rv} = (\,J, \quad \alpha A, \quad \beta B, \quad \gamma C\,) \tag{2.1}$$

The intertwining condition implies

$$\mathbf{rvu} = (\,N, \quad \sigma(\alpha)G, \quad \sigma(\beta)H, \quad \sigma(\gamma)I\,)$$

for some permutation σ.

Writing out the four components of the equation (1.1) and reducing mod the relations

$$AG + BH + CI = \alpha A^2 + \beta B^2 + \gamma C^2 = 0$$

$$A^2 + B^2 + C^2 = 1$$

we get:

$$AG(\alpha + \sigma(\alpha)) + BH(\beta + \sigma(\beta)) + CI(\gamma + \sigma(\gamma)) = 0 \tag{2.2}$$

$$CH(\gamma + \sigma(\beta)) - BI(\beta + \sigma(\gamma)) = AN - GJ \tag{2.3}$$

$$AI(\alpha + \sigma(\gamma)) - CG(\gamma + \sigma(\alpha)) = BN - HJ \tag{2.4}$$

$$BG(\beta + \sigma(\alpha)) - AH(\alpha + \sigma(\beta)) = CN - IJ \tag{2.5}$$

We now consider three cases:

Case I: σ is the identity. Then from the conditions $\mathbf{r} \perp \mathbf{rv}$, $\mathbf{ru} \perp \mathbf{rvu}$ and (2.2), we see that the (obviously nonzero) vector $(\alpha, \beta, \gamma)^T$ is killed by the matrix

$$M = \begin{pmatrix} A^2 & B^2 & C^2 \\ G^2 & H^2 & I^2 \\ AG & BH & CI \end{pmatrix}$$

so that

$$0 = \begin{vmatrix} A^2 & B^2 & C^2 \\ G^2 & H^2 & I^2 \\ AG & BH & CI \end{vmatrix} = -(BI - CH)(CG - AI)(BG - AH)$$

The three factors on the right are the second, third and fourth components of $\mathbf{u}$. Without loss of generality, the first of these is zero, so $\mathbf{u} \in < j, k >$. This and the condition $\mathbf{r} \perp \mathbf{u}$ suffice to determine $\mathbf{u}$ uniquely.

It is easy to check that the matrix M cannot be rank 1, so that the vector (α, β, γ), which sits in the null space of M, is determined up to a multiplicative constant. Now the equations (2.3)- (2.5) determine J and N (and hence $\mathbf{v}$) up to that same multiplcative constant; this plus the condition $||\mathbf{rv}|| = 1$ suffice to uniquely determine $\mathbf{rv}$ and hence $\mathbf{v}$. (In fact, one checks easily that $\mathbf{v} = \bar{\mathbf{r}} i \mathbf{r}$.) Thus in this case the pair $(\mathbf{u}, \mathbf{v})$ is unique.

Case II: σ is a transposition; without loss of generality, σ interchanges β and γ. Then equation (2.2) becomes

$$AG(2\alpha - \beta - \gamma) = 0$$

so arguing as in Case I, we get

$$0 = \begin{vmatrix} A^2 & B^2 & C^2 \\ G^2 & I^2 & H^2 \\ 2 & -1 & -1 \end{vmatrix} = (B^2 + H^2) - (C^2 + I^2)$$

Combining this condition with the norm-one conditions and the orthogonality condition $AG+BH+CI = 0$, it is tedious but straightforward to solve for G, H and I in terms of A, B and C (thus determining all possible values for $\mathbf{u}$) and then use (2.3)-(2.5) to compute $\mathbf{v}$. The result is that either

$$\mathbf{u} \sim (0, C-B, A, -A) \quad \text{and} \quad \mathbf{v} \sim (0, A^2 + 2BC, A(B-C), A(C-B)) \tag{2.6}$$

or

$$\mathbf{u} \sim (0, -B-C, A, A) \quad \text{and} \quad \mathbf{v} \sim (0, A^2 - 2BC, A(B+C), A(B+C)) \tag{2.7}$$

Thus there are at most two pairs $(\mathbf{u}, \mathbf{v})$ satisfying the conditions of Case II.

Case III: σ is a three-cycle. Without loss of generality, σ maps

$$\alpha \mapsto \gamma \mapsto \beta \mapsto \alpha \tag{2.8}$$

Arguing as in Case I, we get

$$0 = \begin{vmatrix} A^2 & B^2 & C^2 \\ H^2 & I^2 & G^2 \\ CI & AG & BH \end{vmatrix}$$

Reducing the above determinant mod the orthogonality and norm-one conditions in a variety of ways, we get

$$AG(C^2 - G^2) + BH(I^2 - B^2) = 0 \tag{2.9a}$$

$$AG(H^2 - A^2) + CI(B^2 - I^2) = 0 \tag{2.9b}$$

$$BH(A^2 - H^2) + CI(G^2 - C^2) = 0 \tag{2.9c}$$

After applying the orthogonality condition $AG + BH + CI = 0$ to solve for I, (2.9a) and (2.9b) form a pair of (distinct) cubics in G and H for which there are at most nine solutions.

We can discard the solution $G = H = I = 0$ and the two solutions $G = 0, H = \pm C, I = \mp B$, because these do not satisfy the intertwining condition. (Note also that the latter two solutions fail to satisfy (2.9c).) That leaves at most six solutions, which come in pairs representing the same $\mathbf{u}$. Thus there are at most three possible values for $\mathbf{u}$. To complete the proof, note that $\mathbf{r}$ and $\mathbf{ru}$ uniquely determine $\mathbf{rv}$ (and hence $\mathbf{v}$) just as in Case I.

Therefore we have at most three pairs $(\mathbf{u}, \mathbf{v})$, which, when added to the one pair from Case I and the two pairs from Case II, yield a total of six. $\blacksquare$

Example 2A. Given $\mathbf{r} = (0, A, B, C) = (0, 2/7, 3/7, 6/7)$, we construct the pairs $(\mathbf{v}, \mathbf{u})$ that arise from Case III of the proof.

First combine equations (2.9a) through (2.9c) with the orthogonality condition $AG + BH + CI = 0$ and the norm one condition $G^2 + H^2 + I^2 = 1$. This gives (up to a sign) three solutions for $\mathbf{ru} = (0, G, H, I)$. Substitute any of these solutions into the matrix depicted immediately above equations (2.9). and let $(\alpha, \beta, \gamma)^T$ be a generator for the kernel of the resulting matrix. Now solve (2.3)- (2.5) for J and N (where σ is the permutation (2.8).) Finally, replace $\alpha, \beta, \gamma, J, N$ with $t\alpha, t\beta, t\gamma, tJ, tN$ where t is a scalar chosen to make $||\mathbf{rv}|| = 1$.

To three digits' accuracy, we get the following solutions:

$$\begin{array}{rr} \mathbf{r} = (0, .286, .429, .857) & \mathbf{rv} = (.577, -.247, -.660, .412) \\ \mathbf{ru} = (0, -.857, -.286, .429) & \mathbf{rvu} = (.577, -.412, .247, -.660) \end{array}$$

$$\begin{array}{rr} \mathbf{r} = (0, .286, .429, .857) & \mathbf{rv} = (-.707, -.589, -.234, .314) \\ \mathbf{ru} = (0, -.917, .382, .115) & \mathbf{rvu} = (.513, -.336, -.787, -.063) \end{array}$$

$$\begin{array}{rr} \mathbf{r} = (0, .286, .429, .857) & \mathbf{rv} = (-.293, .140, -.864, .386) \\ \mathbf{ru} = (0, -.021, .897, -.442) & \mathbf{rvu} = (-.125, -.009, .438, .890) \end{array}$$

I will refer back to this example in the proof of Theorem 4.

Theorem 3. Suppose $\mathbf{r} = (0, A, B, C)$ with $ABC \neq 0$. Suppose $\mathbf{r} \perp i\mathbf{u}$ and $(\mathbf{r}, \mathbf{rv}, \mathbf{ru}, \mathbf{rvu})$ is Type One intertwined. Then at least one of the following holds:

3.i) $\mathbf{u} = i$

3.ii) $\mathbf{v} = \mathbf{r}i\mathbf{r}$

3.iii) $\mathbf{v} = \mathbf{r}j\mathbf{r}$ or $\mathbf{r}k\mathbf{r}$ and $\mathbf{r}$ uniquely determines $\mathbf{u}$.

3.iv)

$$\mathbf{r}, \mathbf{u}, \mathbf{v} \in \left\langle i, \frac{j \pm k}{\sqrt{2}} \right\rangle$$

and $\mathbf{v}$ is uniquely determined by $\mathbf{r}$ and $\mathbf{u}$.

3.v) $(\mathbf{u}, \mathbf{v})$ is one of at most two additional pairs not satisfying any of the above conditions.

Proof. As in the proof of Theorem 2, we can write

$$\mathbf{ru} = (\, G, \quad 0, \quad H, \quad I\,) \quad (GHI \neq 0) \qquad \mathbf{rv} = (\, J, \quad \alpha A, \quad \beta B, \quad \gamma C\,)$$

$$\mathbf{rvu} = (\, \sigma(\alpha) G, \quad N, \quad \sigma(\beta) B, \quad \sigma(\gamma) C\,)$$

We can assume $(\alpha, \beta, \gamma) \neq 0$ (otherwise $\mathbf{u} = (\overline{\mathbf{rv}})(\mathbf{rvu}) = \mathbf{u} = i$).

The four components of (1.1), reduced mod the orthogonality and norm-one relations, are:

$$BH(\gamma + \sigma(\gamma) - \beta - \sigma(\beta)) = GJ + AN \tag{3.1}$$

$$AG(\alpha + \sigma(\alpha)) + BI(\beta + \sigma(\gamma)) - CH(\gamma + \sigma(\beta)) = 0 \tag{3.2}$$

$$BG(\beta + \sigma(\alpha)) - AI(\alpha + \sigma(\gamma)) = HJ - CN \tag{3.3}$$

$$CG(\gamma + \sigma(\alpha)) + AH(\alpha + \sigma(\beta)) = IJ + BN \tag{3.4}$$

Case I: σ is the identity. The orthogonality conditions and (3.2) show that the non-zero vector $(\alpha, \beta, \gamma)^T$ is killed by

$$\begin{pmatrix} A^2 & B^2 & C^2 \\ G^2 & H^2 & I^2 \\ 2AG & BI - CH & BI - CH \end{pmatrix} \tag{3.5}$$

with determinant

$$(BI - CH)\Big((CG + AH)^2 - (AI - BG)^2\Big)$$

We have $BI \neq CH$ (otherwise, the orthogonality condition $BH + CI = 0$ implies $BCHI = 0$, contradiction). Thus $(CG + AH) = \pm(AI - BG)$. From this and orthogonality we have two subcases:

Subcase IA: $G = -A$, $H = C$, $I = -B$ (or similarly with signs reversed on A, B and C, in which case make appropriate adjustments in the argument to follow). This gives $\mathbf{u} = i$ as needed.

Subcase IB: $C = \pm B$, $I = \mp H$. Then the matrix (3.5) becomes

$$\begin{pmatrix} A^2 & B^2 & B^2 \\ G^2 & H^2 & H^2 \\ 2AG & \pm 2BH & \pm 2BH \end{pmatrix} \tag{3.5$'$}$$

If $(3.5')$ has rank one, Subcase IA applies. We can therefore assume $(3.5')$ has rank two, so its kernel is generated by $(0,1,-1)$. Thus $\alpha = 0$ and $\gamma = -\beta$. It follows that

$$\mathbf{r}, \mathbf{u}, \mathbf{v} \in \left\langle i, \frac{j \pm k}{\sqrt{2}} \right\rangle$$

Writing $\mathbf{u} = (0, X, Y, \pm Y)$, it's now easy to check that

$$\mathbf{v} \sim (0, 2ABX - Y, 2B^2X, \pm 2B^2X) \tag{3.6}$$

so that $\mathbf{v}$ is uniquely determined by $\mathbf{r}$ and $\mathbf{u}$ per condition (3.iv).

Case II: σ interchanges β and γ. Then (3.2) becomes

$$2(AG\alpha + BI\beta - CH\gamma) = 0$$

so that $(\alpha, \beta, \gamma)^T$ is killed by the matrix

$$\begin{pmatrix} A^2 & B^2 & C^2 \\ G^2 & I^2 & H^2 \\ AG & BI & -CH \end{pmatrix} \tag{3.7}$$

It is easy to see that (3.7) has rank one if and only if $\mathbf{u} = i$, in which case we are done, so assume (3.7) has rank 2. Then (α, β, γ) must be proportional to the cross product of the first two rows; in particular $\alpha = 0$. (We are using the orthogonality relation $BH + CI = 0$.) Now (3.1)- (3.4) reduce to

$$\begin{pmatrix} G & A & 0 & 0 \\ 0 & 0 & BI & -CH \\ -H & C & BG - AI & 0 \\ -I & -B & 0 & CG + AH \end{pmatrix} \cdot \begin{pmatrix} J \\ N \\ \beta \\ \gamma \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

The matrix on the left is easily seen to be of rank three unless $CG + AH = 0$ (consider the $(2,2)$ minor and use the fact that $BG - AI = (B/C)(CG + AH)$); in that case $\mathbf{u} = i$ and we are done. Thus we can assume the matrix to be rank three, in which case its kernel is generated by

$$(-ABC, BCG, -C^2, B^2)$$

It follows that $\mathbf{rv} = (A, 0, C, -B) = -i\mathbf{r}$, giving condition (3.ii).

Case III: σ is a transposition involving α; without loss of generality σ interchanges α and β. Writing $H = -CX$, $I = BX$ and using (3.2), $(\alpha, \beta, \gamma)^T$ is killed by the matrix

$$M = \begin{pmatrix} A^2 & B^2 & C^2 \\ H^2 & G^2 & I^2 \\ AG - CH & AG + BI & BI - CH \end{pmatrix} = \begin{pmatrix} A^2 & B^2 & C^2 \\ C^2X^2 & G^2 & B^2X^2 \\ AG + C^2X & AG + B^2X & (B^2 + C^2)X \end{pmatrix}$$

so that

$$|M| = 0 \tag{3.8}$$

The the pair (G, X) must satisfy both the cubic equation (3.8) and the quadratic equation

$$G^2 + B^2X^2 + C^2X^2 - 1 = 0 \tag{3.9}$$

It's easy to check that (3.9) is irreducible and does not divide (3.8); therefore there are at most six common solutions. Two of these solutions are of the form $(G = \pm A, X = \pm 1)$ and correspond to $\mathbf{u} = i$. The remaining four solutions come in pairs, yielding (up to a sign), at most two values for $\mathbf{u}$. It suffices, therefore, to show that when $\mathbf{u} \neq i$, $\mathbf{r}$ and $\mathbf{u}$ determine $\mathbf{v}$ uniquely (which establishes condition (3.v)).

Subcase IIIA: M has rank two. Then (α, β, γ) is determined up to a multiplicative constant. We can assume that

$$\left| \begin{pmatrix} G & A \\ I & B \end{pmatrix} \right| \neq 0$$

(otherwise $\mathbf{u} = i$), so that equations (3.1) and (3.4) determine J and N up to that same multiplicative constant, thereby determining $\mathbf{v}$.

Subcase IIIB: M has rank one. We can assume $I = C$, $H = \epsilon A$ and $B = \delta G$ for some $\delta, \epsilon \in \{\pm 1\}$. Then the rank one condition implies that either $A = \epsilon B - \delta C$ or $(A, B, C) \sim (\delta, -\delta\epsilon, 1)$. But if $A = \epsilon B - \delta C$, then the orthogonality condition $BH + CI$ becomes $B^2 \pm BC + C^2 = 0$, which is impossible in real numbers. Thus $(A, B, C) \sim (\delta, -\delta\epsilon, 1)$, which, given the conditions on G, H, I, implies that $\mathbf{u} = i$.

Case IV: σ is a 3-cycle; we can assume that σ maps

$$\alpha \mapsto \gamma \mapsto \beta \mapsto \alpha$$

Setting $H = -CX, I = BX$ and combining the orthogonality conditions with (3.2) as in previous cases we get

$$0 = \begin{vmatrix} A^2 & B^2 & C^2 \\ H^2 & I^2 & G^2 \\ AG - CH & 2BI & AG - CH \end{vmatrix} = \begin{vmatrix} A^2 & B^2 & C^2 \\ C^2X^2 & B^2X^2 & G^2 \\ AG + C^2X & 2B^2X & AG + C^2X \end{vmatrix}$$

$$= B^2(G - AX)^2(AG + C^2X)$$

We know $B \neq 0$, and can assume $G - AX \neq 0$ (otherwise $\mathbf{u} = i$), so that $G = -C^2X/A$. This determines $\mathbf{u} \sim (0, -AB^2, B(A^2 + C^2), C(A^2 + C^2)$. Plugging the value of G into (3.2), we find that $\beta = 0$. Therefore $(\alpha, \gamma) \sim (C^2, -A^2)$, and then from the (redundant) equations (3.1), (3.3) and (3.4) we also have $(\alpha, \gamma, J) \sim (C^2, -A^2, -ABC)$. It follows that $\mathbf{v} = \mathbf{r}j\mathbf{r}$ per condition (3.iii). ■

Example 3A. In case III, with $\mathbf{r} = (0, 2/7, 3/7, 6/7)$, the two possible values for $(\mathbf{v}, \mathbf{u})$ are described approximately by

$$\begin{array}{rr} \mathbf{r} = (0, .286, .429, .857) & \mathbf{rv} = (.458, -.851, .145, .211) \\ \mathbf{ru} = (-.935, 0, -.318, .159) & \mathbf{rvu} = (-.316, .001, .948, .039) \end{array}$$

$$\begin{array}{rr} \mathbf{r} = (0, .286, .429, .857) & \mathbf{rv} = (.977, -.008, -.189, .097) \\ \mathbf{ru} = (-.019, 0, .894, -.447) & \mathbf{rvu} = (.008, .998, -.025, -.051) \end{array}$$

Section 2: Solution to Problem A.

Throughout this section, $\mathbf{v}$ and $\mathbf{u}$ are square roots of -1 and $\mathbf{p}$ is an arbitrary unit quaternion. Theorem 4 gives a complete solution to Problem A1, Theorem 5 gives a complete solution to Problem A2, and Theorem 6 combines these into a complete solution to Problem A, as outlined in the introduction to this paper.

Theorem 4. Suppose $(\mathbf{p}, \mathbf{pv}, \mathbf{pu}, \mathbf{pvu})$ is fully intertwined of Type One. Then, up to permuting i, j and k, at least one of the following holds:

4.i) $\mathbf{u} = i, \quad \mathbf{v} \in \{\overline{\mathbf{p}} j \mathbf{p}, \overline{\mathbf{p}} k \mathbf{p}\}$

4.ii) $\mathbf{u} = i, \quad \mathbf{v} \in < i, \overline{\mathbf{p}} i \mathbf{p} >$

4.ii′) $\mathbf{u} \in < i, \overline{\mathbf{p}} i \mathbf{p} >, \quad \mathbf{v} = \overline{\mathbf{p}} i \mathbf{p}$

4.iii) $\mathbf{p} \in < 1, j >< 1, i >, \quad \mathbf{u} = i, \quad \mathbf{v} \in \overline{\mathbf{p}} < i, k > \mathbf{p}$

4.iii′) $\mathbf{p} \in < 1, i >< 1, j >, \quad \mathbf{v} = \overline{\mathbf{p}} i \mathbf{p}, \quad \mathbf{u} \in < i, k >$

4.iv) $\mathbf{u} = i$ and $\mathbf{v}$ is (uniquely) determined by one of the following three conditions:

$$\mathbf{pv} \sim \big(-A(C^2 + D^2), -B(C^2 + D^2), C(A^2 + B^2), D(A^2 + B^2) \big)$$

$$\mathbf{pv} \sim \big(-C(BC + AD), D(BC + AD), B(AC - BD), A(AC - BD) \big)$$

$$\mathbf{pv} \sim \big(D(AC - BD), C(AC - BD), -A(BC + AD), B(BC + AD) \big)$$

where $\mathbf{p} = (A, B, C, D)$

4.iv′) $\mathbf{v} = \overline{\mathbf{p}}i\mathbf{p}$ and $\mathbf{u}$ is uniquely determined by one of the following three conditions:

$$\mathbf{pu} \sim \big(-A(C^2+D^2), -B(C^2+D^2), C(A^2+B^2), D(A^2+B^2)\big)$$

$$\mathbf{pu} \sim \big(-D(BD+AC), C(BD+AC), A(AD-BC), B(AD-BC)\big)$$

$$\mathbf{pu} \sim \big(C(AD-BC), D(AD-BC), -B(BD+AC), A(BD+AC)\big)$$

where $\mathbf{p} = (A, B, C, D)$

4.v) $\mathbf{p} \in < 1, i > \cup < j, k > \quad \mathbf{u}, \mathbf{v} \in \{i\} \cup < j, k >$

4.vi) $\mathbf{p} \in < i, j >< 1, \mathbf{v} >, \quad \mathbf{u} = \mathbf{v} \in < i, j >$

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

$$\mathbf{p} \sim (A, A, 0, 2C) \quad \text{or} \quad \mathbf{p} \sim (A, -A, -2B, 0)$$

and $\mathbf{u}, \mathbf{v}$ determined by expressions (2.6) or (2.7).

4.viii) $(\mathbf{p}, \mathbf{v}, \mathbf{u})$ is a real point on a certain one-dimensional algebraic variety $\mathcal{X}_0$.

4.ix) $\mathbf{p} = (0, A, B, \pm B), \mathbf{u} = (0, X, Y, \pm Y)$ and $\mathbf{v}$ is uniquely determined by equation (3.6).

4.x) $\mathbf{p} = (AY - 2BX, 0, BY, \mp BY), \quad \mathbf{u} = (0, X, Y, \pm Y)$ and $\mathbf{v}$ is uniquely determined by equation (3.6).

Proof. First suppose $\mathbf{u} = i$. Write $\mathbf{p} = (A, B, C, D)$ and $\mathbf{pv} = (J, K, L, M)$. Then intertwining of $(\mathbf{p}, \mathbf{pu}, \mathbf{pv}, \mathbf{pvu})$ requires an equality of sets (with multiplicities)

$$\{-B/A, A/B, D/C, -C/D\} = \{-K/J, J/K, M/L, -L/M\} \tag{4.1}$$

(Here we use the convention that $a/0 = b/0$ if and only if a and b are both non-zero.)

Note that if $A = B = 0$ or $C = D = 0$ then (4.1) implies condition (4.i) or (4.v), so we can assume otherwise.

There are eight ways (4.1) can hold, each of which gives a system of two equations to which we append the orthogonality condition $AJ + BK + CL + DM = 0$, yielding the following systems:

$$AK - BJ = DL - CM = AJ + BK + CL + DM = 0 \tag{4.1a}$$

$$AK - BJ = DM + CL = AJ + BK + CL + DM = 0 \tag{4.1b}$$

$$AJ + BK = DL - CM = AJ + BK + CL + DM = 0 \tag{4.1c}$$

$$AJ + BK = DM + CL = AJ + BK + CL + DM = 0 \tag{4.1d}$$

$$AL - BM = DK - CJ = AJ + BK + CL + DM = 0 \tag{4.1e}$$

$$AL - BM = DJ + CK = AJ + BK + CL + DM = 0 \tag{4.1f}$$

$$AM + BL = DK - CJ = AJ + BK + CL + DM = 0 \tag{4.1g}$$

$$AM + BL = DJ + CK = AJ + BK + CL + DM = 0 \tag{4.1h}$$

One of these systems must hold.

Systems (4.1a), (4.1f) and (4.1g) are always of full rank and have the unique solutions listed in (4.iv). System (4.1b) implies $J = K = 0$ whence either $A = B = 0$ or $C = D = 0$ contrary to assumption; similar remarks apply to (4.1c).

System (4.1d) is always of rank 1 and implies (4.ii).

System (4.1e) is of full rank unless $AD + BC = 0$, i.e. $\mathbf{p} \in < 1, j >< 1, i >$. It always has the solution $\mathbf{v} = \overline{\mathbf{p}} k \mathbf{p}$ (as in (4.i)) and in the case of less than full rank it has the solution set given in (4.iii). Similar remarks apply to system (4.1h) after reversing j and k.

This proves the theorem in case $\mathbf{u} = i$ and so (by symmetry) in case $\mathbf{u} \in \{i, j, k\}$. Henceforth, then, we assume

$$\mathbf{u} \notin \{i, j, k\} \tag{4.2}$$

.

Next, assume $\mathbf{v} = \overline{\mathbf{p}} i \mathbf{p}$. If we write $\mathbf{p} = (A, B, D, C)$ and $\mathbf{pu} = (J, K, M, L)$, then Type One intertwining again implies (4.1) and hence one of the eight systems (4.2a-4.2h). Under the new interpretation of the variables, systems (4.1b) and (4.1c) remain irrelevant as before. Systems (4.1a), (4.1f) and (4.1g) imply (4.iv$'$) (in the statment of (4.iv$'$), the variables C and D have been restored to their original meanings as the third and fourth components of $\mathbf{p}$, not the fourth and third.) System (4.1d) implies (4.ii$'$). Systems (4.1e) and (4.1h), when they are of full rank, imply $\mathbf{u} = j$ or $\mathbf{u} = k$; after permuting i, j and k this gives (4.i). When (4.1h) is not of full rank it implies (4.iii$'$) and when (4.1e) is not of full rank it implies (4.iii$'$) with j and k reversed.

This proves the theorem when $\mathbf{v} = \overline{\mathbf{p}} i \mathbf{p}$ and thus by symmetry we can assume

$$\mathbf{v} \notin \{\overline{\mathbf{p}} i \mathbf{p}, \overline{\mathbf{p}} j \mathbf{p}, \overline{\mathbf{p}} k \mathbf{p}\} \tag{4.3}$$

Choose $\mathbf{r} \in < \mathbf{p}, \mathbf{pv} >$ such that $\mathbf{r}^2 = -1$. Then $(\mathbf{r}, \mathbf{rv}, \mathbf{ru}, \mathbf{rvu})$ is (not necessarily fully) Type One intertwined, and we have $\mathbf{p} = S\mathbf{r} + T\mathbf{rv}$ for some (S, T) on the unit circle. Write $\mathbf{r} = (0, A, B, C)$.

If $ABC = 0$ then Theorem 1 applies so we can assume $\mathbf{r}, \mathbf{u}, \mathbf{v} \in < i, j >$. Write

$$\begin{aligned} \mathbf{r} &= (0, A, B, 0) & \mathbf{rv} &= (J, 0, 0, K) \\ \mathbf{ru} &= (G, 0, 0, H) & \mathbf{rvu} &= (0, M, N, 0) \end{aligned}$$

where

$$A^2 + B^2 = G^2 + H^2 = J^2 + K^2 = 1 \tag{4.4}$$

By intertwining, $AB = 0$ iff $GH = 0$, in which case $\mathbf{u} \in \{i, j, k\}$ contrary to 4.2), so we can assume $ABGH \neq 0$, and similarly $JKMN \neq 0$. We can also assume $ST \neq 0$ (because otherwise, after exchanging i with k, (4.v) holds and we are done).

Set

$$\mathcal{X} = \left(\frac{GS}{JT}, \frac{MT}{AS}, \frac{NT}{BS}, \frac{HS}{KT} \right)$$

$$\mathcal{Y} = \left(-\frac{GT}{JS}, \frac{-MS}{AT}, \frac{-NS}{BT}, \frac{-HT}{KS} \right)$$

Then Type One intertwining implies some system of four equations of the form

$$\mathcal{X}_i = \mathcal{Y}_{\sigma(i)}$$

where σ is a permutation of $\{1, 2, 3, 4\}$.

It is easy to check that σ cannot have a fixed point (given that all of the variables are nonzero). Moreover, from the forms of $\mathcal{X}$ and $\mathcal{Y}$ we can clearly assume that $\sigma = \sigma^{-1}$. Thus there are three cases:

a) If σ is the product of transpositions $(1, 2)(3, 4)$, then $MJ + GA = BH + KN = 0$. With (4.2), (4.3) and (4.4), this implies $\mathbf{u} = \mathbf{v}$ and

$$\mathbf{p} = \mathbf{r}(S + T\mathbf{v}) \in < i, j >< 1, \mathbf{v} >$$

which is (4.vi).

b) If σ is the product of transpositions $(1, 3)(2, 4)$, then $JN + BG = AH + MK = 0$. The analysis is exactly as in case a) with i and j reversed.

c) If σ is the product of transpositions $(1, 4)(2, 3)$ then $GK + HJ = AN + BM = S^2 - T^2 = 0$, which implies $\mathbf{u} \in \{i, j\}$ contrary to (4.2).

This completes the proof in case $ABC = 0$. Thus we can assume

$$ABC \neq 0 \tag{4.5}$$

By intertwining, $\mathbf{ru}$ contains a zero coefficient so that we can assume either $\mathbf{r} \perp \mathbf{u}$ or $\mathbf{r} \perp i\mathbf{u}$.

If $\mathbf{r} \perp \mathbf{u}$ then Theorem 2 applies. From the proof of Theorem 2 we have three cases:

a) In Theorem 2, Case I, we $\mathbf{v} = \overline{\mathbf{r}} i \mathbf{r} = \overline{\mathbf{p}} i \mathbf{p}$ and so are done by (4.3).

b) In Theorem 2, Case II, $\mathbf{u}$ and $\mathbf{v}$ are given by (2.6) or (2.7). We assume (2.6) holds; if (2.6) is replaced by (2.7) the argument is essentially identical. Write $\mathbf{p} = S\mathbf{r} + T\mathbf{rv}$ and compute the four components of $\mathbf{pu}/\mathbf{p}$ and of $\mathbf{pvu}/\mathbf{pv}$. Note that $(\mathbf{pu}/\mathbf{p})_1 = (\mathbf{pvu}/\mathbf{pv})_1$ and $(\mathbf{pu}/\mathbf{p})_2 = (\mathbf{pvu}/\mathbf{pv})_2$. Thus intertwining requires either

$$(\mathbf{pu}/\mathbf{p})_3 = (\mathbf{pu}/\mathbf{p})_3 \quad (\mathbf{pu}/\mathbf{p})_4 = (\mathbf{pu}/\mathbf{p})_4 \quad S^2 + T^2 = 1$$

or

$$(\mathbf{pu}/\mathbf{p})_3 = (\mathbf{pu}/\mathbf{p})_4 \quad (\mathbf{pu}/\mathbf{p})_4 = (\mathbf{pu}/\mathbf{p})_3 \quad S^2 + T^2 = 1$$

For the first of these systems of equations, all solutions fall into four categories: Either $B+C = \pm\sqrt{2}$, $B = \sqrt{\pm C^2 \mp 1}$, $B = \sqrt{\pm C^2 \pm 1}$, or $BC = 0$. Any of these possibilities implies $ABC = 0$ and therefore violates (4.5).

For the second system, there are three families of solutions: those violating (4.5), those with $B = -C$, which gives $\mathbf{v} = \overline{\mathbf{r}} i \mathbf{r} = \overline{\mathbf{p}} i \mathbf{p}$, violating (4.3), and those with

$$\frac{S}{T} = \pm \frac{\sqrt{1 - B^4 + 2B^2C^2 - C^4}}{1 + B^2 - C^2}$$

The latter satisfy (4.vii).

c) In Theorem 2, Case III, the coordinates of $(\mathbf{r}, \mathbf{v}, \mathbf{u})$ (as defined in (2.1)) satisfy equations (2.9a) through (2.9c). We will establish that under these conditions $(\mathbf{p}, \mathbf{v}, \mathbf{u})$ lies on a fixed one- dimensional variety $\mathcal{X}_0$, yielding (4.viii).

Let $\mathcal{V}$ be the algebraic variety that parameterizes the relevant pairs $(\mathbf{r}, \mathbf{v}, \mathbf{u})$; explicitly, $\mathcal{V}$ is defined by the variables $(A, B, C, G, H, I, J, N, \alpha, \beta, \gamma)$ and the equations (2.9a) through (2.9c), together with the orthogonality condition $AG + BH + CI = 0$, the norm-one conditions $||\mathbf{r}|| = ||\mathbf{ru}|| = ||\mathbf{rv}|| = 1$, the requirement that $ABCGHI \neq 0$, the requirement that $(\alpha, \beta, \gamma)^T$ is nonzero and killed by the matrix whose determinant is displayed just above equations (2.9), and the explicit formulas for J and N that can be derived from equations (2.3) through (2.5).

Let $\mathbf{S}^3$ be the unit quaternions, $\mathbf{S}^2 = \{(0, A, B, C) | A^2 + B^2 + C^2 = 1\} \subset \mathbf{S}^3$ (so that $\mathbf{S}^2$ is identified with the square roots of -1), and $\mathbf{S}^1 = \{(S, T) | S^2 + T^2 = 1\}$.

Now map

$$\begin{array}{cccc} f: & \mathcal{V} \times \mathbf{S}^1 & \to & \mathbf{S}^3 \times \mathbf{S}^2 \times \mathbf{S}^2 \\ & ((\mathbf{r}, \mathbf{v}, \mathbf{u}), (S, T)) & \mapsto & (S\mathbf{r} + T\mathbf{rv}, \mathbf{v}, \mathbf{u}) \end{array}$$

and let $\mathcal{X} = f(\mathcal{V})$ Let

$$\mathcal{X}_0 = \{(\mathbf{p}, \mathbf{v}, \mathbf{u}) \in \mathcal{X} | (\mathbf{p}, \mathbf{pv}, \mathbf{pu}, \mathbf{pvu}) \text{ is fully intertwined}\}$$

Let $\mathcal{V}_0$ be the pullback:

$$\begin{array}{ccc} \mathcal{V}_0 & \hookrightarrow & \mathcal{V} \times \mathbf{S}^1 \\ \downarrow & & \downarrow f \\ \mathcal{X}_0 & \hookrightarrow & \mathcal{X} \end{array}$$

We want to show that $\mathcal{X}_0$ is at most one-dimensional (a la (4.viii)), for which it suffices to show that $\mathcal{V}_0$ at most one-dimensional. For this in turn it suffices to show that the fibers of the composition

$$\begin{array}{cccccc} \pi: & \mathcal{V}_0 & \xrightarrow{\pi_1} & \mathcal{V} & \xrightarrow{\pi_2} & \mathbf{S}^2 \\ & ((\mathbf{r}, \mathbf{v}, \mathbf{u}), (S, T)) & \mapsto & (\mathbf{r}, \mathbf{v}, \mathbf{u}) & \mapsto & \mathbf{r} \end{array}$$

are a) finite and b) almost always empty.

By Theorem 2, the fibers of π_2 are finite. Therefore it suffices to show that the fibers of π_1 are finite and almost always empty.

So consider a fiber $F = \pi_1^{-1}(\mathbf{r}, \mathbf{v}, \mathbf{u})$. If F is nonempty, choose $((\mathbf{r}, \mathbf{v}, \mathbf{u}), (S, T)) \in F$. The intertwining condition gives an equality of sets

$$\left\{ \frac{(S + T\alpha)A}{(S + T\gamma)G}, \frac{(S + T\beta)B}{(S + T\alpha)H}, \frac{(S + T\gamma)C}{(S + T\beta)I} \right\} = \left\{ \frac{(S\alpha - T)A}{(S\gamma - T)G}, \frac{(S\beta - T)B}{(S\alpha - T)H}, \frac{(S\gamma - T)C}{(S\beta - T)I} \right\} \tag{4.7}$$

If for any i the i^{th} expression on the left equals the i^{th} expression on the right, then two of α, β, γ must be equal. From this and (2.2) (plus the orthogonality condition $AB + BH + CI = 0$), all three are equal, giving the contradiction

$$\alpha = \alpha(A^2 + B^2 + C^2) = \alpha A^2 + \beta B^2 + \gamma C^2 = 0 \tag{4.8}$$

Therefore the two sets in (4.7) are related by a three-cycle; without loss of generality suppose that the first, second and third expressions on the left are equal to the second, third and first on the right.

In particular, then, we have two homogeneous quadratics in (S, T)

$$\begin{aligned} AH(S+T\alpha)(S\alpha-T) &= BG(S\beta-T)(S+T\gamma) \\ BI(S+T\beta)(S\beta-T) &= CH(S+T\alpha)(S\gamma-T) \end{aligned} \tag{4.9}$$

and the fiber F can be nonempty only if these two quadratics have a simultaneous solution; i.e. if their resultant ρ vanishes.

So to show that almost all fibers of π_1 are empty, it suffices to show that ρ fails to vanish at some point on each two-dimensional irreducible component of $\mathcal{V}$. Because $\mathcal{V}$ is finite over $\mathbf{S}^2$ (we are invoking Theorem 2 again) it suffices to show that ρ fails to vanish everywhere on some fiber of $\mathcal{V} \to \mathbf{S}^2$.

This can be shown by choosing $\mathbf{r} \in \mathbf{S}^2$ and calculating. We arbitrarily choose $\mathbf{r} = (0, 2/7, 3/7, 6/7)$ so that $\pi_2^{-1}(\mathbf{r})$ consists of the points described in Example 2A. Evaluating ρ at these points, and enlisting the aid of a good symbolic calculator, we get the values $\rho = 4/63$ and

$$\rho = \frac{2\bigl(32755360406561 \pm 1785121807271\sqrt{337}\bigr)}{1361366980723449}$$

In particular, none of these values is zero.

Finally, to show that that all fibers are finite, it suffices to show that the two quadratics (4.9) are not simultaneously identically zero at any point of $\mathcal{V}$. To see this is impossible, equate all coefficients on S^2, ST and T^2 to zero and note that it follows that $\alpha = \beta = \gamma$, which yields the contradiction (4.8).

This completes the proof in the case $\mathbf{r} \perp \mathbf{u}$. We may therefore assume that $\mathbf{r} \perp i\mathbf{u}$, i.e. Theorem 3 applies and one of conditions (3.i)- (3.v) holds. If (3.i), (3.ii) or (3.iii) holds, we are done by (4.2) or (4.3).

If (3.iv) holds, we can write $\mathbf{r} = (0, A, B, -B)$, $\mathbf{rv} = (J, 0, \beta B, \beta B)$, $\mathbf{ru} = (G, 0, H, H)$, $\mathbf{rvu} = (0, N, \beta H, -\beta H)$ (or similarly with signs changed on the fourth coordinates). If $\mathbf{p} = \mathbf{r}$ or $\mathbf{p} = \mathbf{rv}$ we have (4.ix) or (4.x) so suppose otherwise. Then $\mathbf{p} = S\mathbf{r} + T\mathbf{rv}$ with $ST \neq 0$.

Note that $B \neq 0$ by (4.5), $H \neq 0$ because otherwise $B = 0$ by intertwining, and $\beta \neq 0$ because then we would have $\mathbf{rv} = 1$ and $\mathbf{u} = \mathbf{rvu} \in \{i, j, k\}$ (by intertwining), violating (4.2).

It's easy to verify that $(\mathbf{pu}/\mathbf{p})_i = (\mathbf{pvu}/\mathbf{pv})_i$ for $i = 3, 4$. But we cannot have the same equation for both $i = 1$ and $i = 2$, for then we would have $GJ = AN = 0$; from this and (3.1) we have $BH\beta = 0$, contradicting the preceding paragraph.

Therefore $(\mathbf{pu}/\mathbf{p})_1 = (\mathbf{pvu}/\mathbf{pv})_2$, which implies $AG + JN = 0$. Write $J = XA, G = -XN$ for some X. Then the norm one conditions give

$$A^2(1 - X^2) = 2B^2(\beta^2 - 1)$$

$$N^2(1 - X^2) = 2H^2(1 - \beta^2)$$

It follows that $\beta = \pm 1$; we can assume $\beta = 1$, whence $J = \pm A$, whence $\mathbf{v} \in \{i, \bar{\mathbf{r}}i\mathbf{r}\}$. But if $\mathbf{v} = i$ then (3.6) implies $B = 0$ and if $\mathbf{v} = \bar{\mathbf{r}}i\mathbf{r}$ then (3.6) implies $BH = 0$, both of which are cases we've already dismissed. Thus we can assume away (3.iv).

Now we can assume (3.v), which arises from Case IIIB in the proof of Theorem 3. We will construct a variety $\mathcal{X}_0'$ of dimension at most one containing the point $(\mathbf{p}, \mathbf{v}, \mathbf{u})$. We can then replace the variety $\mathcal{X}_0$, constructed earlier, with the union $\mathcal{X}_0 \cup \mathcal{X}_0'$ to conclude that (4.viii) applies. Let $\mathcal{V}'$ be the variety defined by variables $(A, B, C, G, X, \alpha, \beta, \gamma, J, N)$ and the equations (3.8) and (3.9), together with orthogonality conditions, norm one conditions, and equations for α, β, γ, J and N analogous to those used earlier in the definition of $\mathcal{V}$, together with $ABCGHI \neq 0$. Mimicking the construction of $\mathcal{X}_0$, the analogue of (4.9) is

$$\left\{\frac{G(S+T\beta)}{JT}, \frac{NT}{A(S+T\alpha)}, -\frac{C(S+T\alpha)X}{B(S+T\beta)}\right\} = \left\{\frac{G(S\beta-T)}{JS}, \frac{NS}{A(S\alpha-T)}, -\frac{C(S\alpha-T)X}{B(S\beta-T)}\right\}$$

and, as in the earlier construction, we conclude that the terms on the left must be equal to the those on the right after applying a three-cycle.

This gives two possible systems of quadratics in S and T (analogous to (4.11):

$$\begin{gathered} AG(S+\beta T)(S\alpha - T) = JNST \\ -BNT(S\beta - T) = ACX(S+T\alpha)(S\alpha - T) \end{gathered} \tag{4.12}$$

or

$$\begin{gathered} AG(S+\alpha T)(S\beta - T) = JNST \\ -BG(S+\beta T)(S\beta - T) = CXJT(S\alpha - T) \end{gathered} \tag{4.12$'$}$$

We assume (4.12) holds; the argument for (4.12′) is essentially identical.

To complete the construction, we must show that the resultant of the system (4.12) fails to vanish at the points constructed in Example 3A, and that the polynomials of (4.12) are not identically zero anywhere on $\mathcal{V}$.

Resorting again to a symbolic calculator, one checks that the resultants are:

$$\frac{9\big(-73693611015200767 \pm 2250627766396874\sqrt{1261}\big)}{468732633845533101247}$$

In particular, neither is zero.

Finally, suppose the two equations (4.12) are identically zero at some point on $\mathcal{V}$. Equating the coefficients on S^2, ST and T^2 to zero, we contradict the assumption $AG \neq 0$. ■

Theorem 5. Suppose $(\mathbf{p}, \mathbf{pv}, \mathbf{pu}, \mathbf{pvu})$ is fully intertwined of Type 2. Then, up to permuting i, j and k, at least one of the following holds:

5.o) At least one of the conditions (4.iv), (4.iv′) or (4.v) holds.

5.i) $\mathbf{u} = \mathbf{v} \perp \mathbf{p} \perp 1$

5.ii) $\mathbf{u} = \mathbf{v} \perp i\mathbf{p} \perp 1$

5.iii) $\mathbf{v} = (j \pm k)/\sqrt{2} \quad \mathbf{p} \in < 1, i\mathbf{v} > \cup < i, i\mathbf{v} > \quad \mathbf{u} = \overline{\mathbf{p}} i \mathbf{p}$

5.iii′) $\mathbf{u} = (j \pm k)/\sqrt{2} \quad \mathbf{p} \in < 1, i\mathbf{u} > \cup < i, i\mathbf{u} > \quad \mathbf{v} = i$

Proof. We assume that

$$K(X\mathbf{p} + Y\mathbf{pv}) = K(X\mathbf{pu} + Y\mathbf{pvu}) = 0 \tag{5.1}$$

Symmetric arguments apply when $\mathbf{pv}$ and $\mathbf{pu}$ are reversed.

Necessarily, $\mathbf{p}$ has at least one component equal to zero. So up to permuting i, j and k there are six cases:

Case I: $\mathbf{p} = 1$. Then (5.1) plus orthogonality gives (up to a permutation) $\mathbf{pv} = (0, 0, E, F)$ and $\mathbf{pu} = (0, G, H, I)$. If $G = 0$, (4.v) holds, so assume otherwise. Then $-\mathbf{pvu} = (EH + FI, FH - EI, -FG, EG)$ so (5.1) gives (still up to a permutation) two subcases:

Subcase IA: $EH + FI = 0$. Then full intertwining requires $GHI = 0$ so without loss of generality $H = 0$, giving either $F = 0$ or $I = 0$. Either way, (4.v) holds.

Subcase IB: $H = FG = 0$, giving $F = 0$ and (4.v) holds again.

Case II: $\mathbf{p} = i$. We can argue exactly as in Case I. with the components permuted.

Case III: $\mathbf{p} = (A, B, 0, 0)$, $AB \neq 0$. Without loss of generality $\mathbf{pv}$ has a zero in the third place; write $\mathbf{pv} = (-BS, AS, 0, F)$. Write $\mathbf{pu} = (-BT, AT, G, H)$. Then $\mathbf{pu}$ and $\mathbf{pvu}$ must have a zero in some common position; up to symmetry there are three subcases:

Subcase IIIA: $\mathbf{pu}$ and $\mathbf{pvu}$ have zeros in the first place. Then $T = F(BG - AH) = 0$. If $F = 0$ we get (4.v). Otherwise $H = B$ and $G = A$, so $\mathbf{u} = j$. Now full intertwining implies that $\mathbf{pvu} = (0, F, -BS, AS)$ has a second component equal to zero, so that either $F = 0$ or $S = 0$, either of which gives (4.v).

Subcase IIIB: $\mathbf{pu}$ and $\mathbf{pvu}$ have zeros in the third place. Then $G = FT - HS = 0$. This implies $\mathbf{u} = \mathbf{v}$ and hence (5.ii) (with j in place of i).

Subcase IIIC: $\mathbf{pu}$ and $\mathbf{pvu}$ have zeros in the fourth place. Then $H = GS = 0$.

Suppose first that $H = G = 0$. Then $\mathbf{u} = i$, $\mathbf{pv} = (-BS, AS, 0, F)$ and $\mathbf{pvu} = (-AS, -BS, F, 0)$. Full intertwining requires either $F = 0$ or $S = 0$; thus $\mathbf{v} \in \{i, \overline{\mathbf{p}}k\} \subset \{i\} \cup < j, k >$ per condition (4.v).

This disposes of the case $H = G = 0$ and leaves the case $H = S = 0$. Then full intertwining requires $GT = 0$; we have already disposed of the case $G = 0$, so assume $T = 0$. Then $\{\mathbf{u}, \mathbf{v}\} = \{\overline{\mathbf{p}}j, \overline{\mathbf{p}}k\} \subset < j, k >$ in accordance with (4.v).

Case IV: $\mathbf{p} = (0, A, B, 0)$, $AB \neq 0$. The reasoning is completely parallel to Case III, yielding in various subcases either (4.v) or (5.1).

Case V: $\mathbf{p} = (0, A, B, C)$, $ABC \neq 0$. Then we can write $\mathbf{pv} = (0, D, E, F)$. In particular, $\mathbf{p}$ is orthogonal to $\mathbf{v}$. Now $\mathbf{pu}$ and $\mathbf{pvu}$ have zeros in the same place. This gives (up to symmetry) two subcases:

Subcase VA: $\mathbf{pu}$ and $\mathbf{pvu}$ have zeros in the first place. I claim $\mathbf{v} = \mathbf{u}$. Proof: Otherwise, because $\mathbf{p}$ is orthogonal to both $\mathbf{v}$ and $\mathbf{u}$, $\{\mathbf{p}, \mathbf{v}, \mathbf{u}\}$ is a basis for the square roots of -1. Moreover, $\mathbf{vu}$ is orthogonal to everything in this basis; thus $\mathbf{vu} = \pm 1$, contradiction. This establishes the claim, and hence (5.1).

Subcase VB: $\mathbf{pu}$ and $\mathbf{pvu}$ have zeros in the second place. Write $\mathbf{pu} = (G, 0, -CT, BT)$.

Then the second component of $\mathbf{pvu}$ is $0 = (BF - CE)(G - AT)$.

Sub-subcase VB1: $BF = CE$. Write $E = BS$, $F = CS$. Then orthogonality and the norm one condition imply $D^2 = B^2 + C^2 \neq 0$ and $\mathbf{v} = (0, 0, -C/D, B/D) \in < j, k >$. Now we have $\mathbf{pv} = (0, D, -AB/D, -AC/D)$ and $\mathbf{pvu} = (DT, 0, CG/D, -BG/D)$. Full intertwining implies that either $AT = G$ or $AC^2T = -B^2G$, $AB^2T = -C^2G$.

In case $AT = G$, we must have $|T| = 1$ so we can take $T = -1$, giving $\mathbf{u} = i$; now the first line of condition (4.iv) holds (with the A, B, C, D of (4.iv) replaced by $0, A, B, C$).

In case $AC^2T = -B^2G$ and $AB^2T = -C^2G$, it follows that $G = -AT$ and $B = \pm C$. The norm one conditions for $\mathbf{p}$ and $\mathbf{pu}$ let us take $|T| = 1$, whence $\mathbf{u} = \overline{\mathbf{p}}i\mathbf{p}$. Together with $B = \pm C$, this gives (5.iii) (with $\mathbf{p} \in < i, i\mathbf{v} >$).

Sub-subcase VB2: $G = AT$. Then we can take $T = -1$, giving $\mathbf{u} = i$. Now full intertwining gives either $BF = CE$ or $-BE = CF$. If $BF = CE$ we are back in sub-subcase VB1. Thus we can assume $-BE = CF$. Then orthogonality implies $AD = 0$, whence $D = 0$. But then $0 = K(X\mathbf{pv} + Y\mathbf{pvu}) = K(X\mathbf{p} + Y\mathbf{pu}) \neq 0$, contradiction.

Case VI: $\mathbf{p} = (A, 0, B, C)$, $ABC \neq 0$. This reasoning is entirely analogous to Case V, yielding (5.ii), (4,iv), or (5.iii) (with $\mathbf{p} \in < 1, i\mathbf{v} >$). ■

Combining Theorems 4 and 5, we have:

Theorem 6. Suppose that $\mathbf{v}^2 = \mathbf{u}^2 = -1$ and that $(\mathbf{p}, \mathbf{pv}, \mathbf{pu}, \mathbf{pvu})$ is fully intertwined. Then the triple $(\mathbf{p}, \mathbf{v}, \mathbf{u})$ satisifes (at least) one of the conditions listed in the statements of Theorems 4 and 5.

Concluding Remark. Theorem 6 classifies all solutions to Problem A. These solutions fall into several families, each of which is at most four dimensional.

With one exception, each of these families is presented in a form that makes it trivial to check a proposed solution for membership. The exception is the one-dimensional family (4.viii).

Therefore Theorem 6 provides the following useful information: First, there are only four dimensions worth of solutions to Problem A. Second, all of these solutions are easily identifiable except for a subset of dimension one.

References

[EW] J. Eisert and M. Wilkens, "Quantum Games", *J. of Modern Optics* 47 (2000), 2543-2556.

[EWL] J. Eisert, M. Wilkens and M. Lewenstein, "Quantum Games and Quantum Strategies", *Physical Review Letters 83* (1999), 3777-3080.

[NE] S. Landsburg, "Nash Equilibria in Quantum Games" preliminary version at http://www.landsburg.com/qgt.pdf

[QGT] S. Landsburg, "Quantum Game Theory", *Notices of the American Mathematical Society*, April 2004.