Before we proceed with our main goal we first recall some basic notions from linear algebra:

**Trace of a matrix**

Given an $m \times m$ square matrix $A = [a_{ij}]$, its trace is defined as the sum of its elements along the main diagonal:

$$\text{tr} (A) = \sum_{i=1}^{m} a_{ii} \quad (1)$$

It has the following properties ($A, B, C$ are corresponding matrices):

$$\text{tr} (A+B) = \text{tr} (A) + \text{tr} (B) \quad (2)$$  

$$\text{tr} (xA) = x \cdot \text{tr} (A) \quad (3)$$

$$\text{tr} (A^T) = \text{tr} (A) \quad (4)$$

$$\text{tr} (AB) = \text{tr} (BA) \quad (5)$$

$$\text{tr} (ABC) = \text{tr} (BCA) = \text{tr} (CAB) \quad \text{(cyclic property)} \quad (6)$$

$$\text{tr} (B^*AB) = \text{tr} (A) \quad \text{(similarity invariant)} \quad (7)$$

**Conjugate transpose, Hermitian and Unitary matrices**

The conjugate transpose or Hermitian transpose of an $m \times m$ matrix $A$ is the $m \times m$ matrix $A^*$ obtained by taking the transpose $A^T$ then replacing all its elements with their complex conjugates ($x + iy \rightarrow x - iy$):

$$A_{ij}^* = (A^{ij})^* = (A_{ij})^* = \overline{a_{ij}} \quad (8)$$

A square matrix $A$ is called Hermitian (or self-adjoint) if:

$$A^* = A$$
\[ A^+ = A \]  

and unitary if
\[ A^+ A = I, \quad \text{or} \quad A^+ = A^{-1}. \]  

Note that for a real matrix, Hermitian means symmetric and unitary means orthogonal.

**Pauli matrices**

are defined as the following three, 2x2 matrices:

\[ \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \]  

It is easy to check that the Pauli matrices are Hermitian:
\[ \sigma_i^+ = \sigma_i, \quad i = 1, 2, 3. \]  

Moreover
\[ \varepsilon_{ijk} \sigma_i \sigma_j = 2 \delta_{ij}, \quad \sigma_{i,j}^1 = 1, 2, 3 \]  

\[ \sigma_i \sigma_j + \sigma_j \sigma_i = 2 \delta_{ij} I, \quad \sigma_{i,j}^1 = 1, 2, 3 \]  

\[ [\sigma_i, \sigma_j] = \sigma_i \sigma_j - \sigma_j \sigma_i = 2 i \sum_{k=1}^{3} \varepsilon_{ijk} \sigma_k, \quad \sigma_{i,j}^1 = 1, 2, 3 \]  

\[ \text{If } |\vec{\sigma}| = 1: \]
\[ (\vec{\sigma} \cdot \vec{\sigma}) \sigma_k - \sigma_k (\vec{\sigma} \cdot \vec{\sigma}) = 2 i \sum_{\delta,k=1}^{3} \varepsilon_{\delta,k} \sigma_{\delta} \sigma_k, \quad k = 1, 2, 3 \]
\[ (\vec{\sigma} \cdot \vec{\sigma}) \sigma_k (\vec{\sigma} \cdot \vec{\sigma}) = 2 \sigma_k (\vec{\sigma} \cdot \vec{\sigma}) - \sigma_k, \quad k = 1, 2, 3. \]

**Rotations from Pauli matrices**

If \((x_1, x_2, x_3)\) and \((x'_1, x'_2, x'_3)\) denote the coordinates of a point before and after a rotation of the coordinate system by \(\vec{\sigma} = \alpha \vec{\sigma}\), then
let us form the matrices $X$ and $X'$ via:

$$X = \sum_{i=1}^{3} \chi_i \tau_i = \chi . \bar{\tau} = \begin{pmatrix} \chi_3 & x_1 - i x_2 \\ x_1 + i x_2 & -\chi_3 \end{pmatrix}$$  \hspace{1cm} (18)$$

and

$$X' = \sum_{i=1}^{3} \chi'_i \tau_i = \chi' . \bar{\tau}' = \begin{pmatrix} \chi'_3 & x_1' - i x_2' \\ x_1' + i x_2' & -\chi'_3 \end{pmatrix}$$  \hspace{1cm} (19)$$

here $\bar{\tau}'$ denotes a "matrix vector" with components $\tau_1', \tau_2', \tau_3'$. It is easy to see that both $X$ and $X'$ are Hermitian. In addition:

$$X^2 = \begin{pmatrix} \chi_3 & x_1 - i x_2 \\ x_1 + i x_2 & -\chi_3 \end{pmatrix} \begin{pmatrix} \chi_3 & x_1 - i x_2 \\ x_1 + i x_2 & -\chi_3 \end{pmatrix} = (\chi_1^2 + x_2^2 + x_3^2) \mathbb{I} = \bar{\chi}^2 \mathbb{I}$$  \hspace{1cm} (20)$$

$$X'^2 = \bar{\chi}'^2 \mathbb{I}$$  \hspace{1cm} (21)$$

Since rotations leave the magnitude of the vectors unchanged $\bar{\chi}'^2 = \bar{\chi}^2$,

$$\Rightarrow \quad X'^2 = X^2. \tag{22}$$

Using (13)

$$\tau_i X = \sum_j \tau_j X_{ij} = \sum_i 2 \delta_{ij} x_i = 2 x_i \quad \Rightarrow$$

$$\begin{align*}
\chi_i &= \frac{1}{2} \chi (\tau_i X) \\
\chi'_i &= \frac{1}{2} \chi (\tau'_i X') \tag{23} \\
\end{align*}$$

Thus, expressing the $x_i$ in fit of $x_1, x_2, x_3$ after the rotation, implies finding the corresponding relationship between $X$ and $X'$.

Let us try to connect $X'$ and $X$ via the transformation

$$X' = U X U^+, \tag{24}$$

i.e., we are looking for an $U$ matrix such that (24) holds.
There is no such matrix then we will get into a contradiction fails.)

Form (24) does not contradict the fact that $X'$ is hermitian, we have from:

$$X^t = (u^*u^t)^t = (u^t)^tu^* = u^t u = X^t.'$$

(because $X$ is also hermitian). However, from (20), (21) $=

$$X'^2 = (u^*u^t)(u^*u^t) = (u^*u^t)(u^*u^t) = (u^*u^t)^2 = X^2,$$

If we now make the choice that $U$ is unitary $\Rightarrow$ $U^t u = u 

$$X'^2 = U^t u = U^t (\bar{\alpha}^2 u) = \bar{\alpha}^2 u^t = \bar{\alpha}^2 u = X^2,$$

i.e., satisfies the constraint (22). So far so good!

From (24) and (18) $=

$$X = U \sum_{k=1}^{3} \xi_k^* u^t = \sum_{k=1}^{3} (u^* u^t) \xi_k$$

Inserting this into (23b) $=$

$$X'^2 = \frac{1}{2} \xi (u^* \sum_{k=1}^{3} (u^* u^t) \xi_k) = \sum_{k=1}^{3} \left[ \frac{1}{2} \xi (u^* u^t) \xi_k \right] \xi_k$$

Comparing this with (2.20) (from lecture 2) we find an expression for the elements of the rotation matrix:

$$R_{n,k}(\bar{\alpha}^2) = \frac{1}{2} \xi (u^* u^t) \xi_k.$$ (27)

But we already know the functions $R_{n,k}(\bar{\alpha}^2)$ as (2.21) ! Thus, we are looking for $U$ such that (27) agrees with (2.21). Let us seek $U$ in the form $U = f(\alpha) \mathbbm{1} + i g(\alpha) (\bar{\alpha}^2 \vec{u})$ (28)

where $f(\alpha), g(\alpha)$ are real functions. First, we must satisfy the
\[ UU^+ = 1 \quad \Rightarrow \quad (\mathbf{i} \mathbf{1} + i \mathbf{g} (\mathbf{n} \cdot \mathbf{\bar{v}})) (\mathbf{i} \mathbf{1} - i \mathbf{g} (\mathbf{n} \cdot \mathbf{\bar{v}})^+) = 1 \]

But \( (\mathbf{n} \cdot \mathbf{\bar{v}})^+ = (\mathbf{n} \cdot \mathbf{\bar{v}}) \) (simply because \( \mathbf{n} \) in (18) is Hermitian) \( \Rightarrow \)

\[ UU^+ = f^2 + q^2 (\mathbf{n} \cdot \mathbf{\bar{v}})^2 \quad \text{However, it is easy to see that} \quad (\mathbf{n} \cdot \mathbf{\bar{v}})^2 = 1 \quad \text{(for the same reason as (20), but here} \quad |\mathbf{n}|^2 = 1 \).

\[ \Rightarrow \quad \text{unitarity in equivalent to:} \]

\[ f^2(x) + q^2(x) = 1. \]  

(29)

Next, we notice that

\[ UU^+ (\mathbf{v}_k) = \left( f^2 + i q (\mathbf{n} \cdot \mathbf{\bar{v}}) \right) \mathbf{v}_k \left( f^2 - i q (\mathbf{n} \cdot \mathbf{\bar{v}}) \right) = f^2 \mathbf{v}_k - i f q (\mathbf{n} \cdot \mathbf{\bar{v}}) \mathbf{v}_k + i f q (\mathbf{n} \cdot \mathbf{\bar{v}}) \mathbf{v}_k + g^2 (\mathbf{n} \cdot \mathbf{\bar{v}})^2 \mathbf{v}_k \Rightarrow \text{unitarity (16, 17) } \Rightarrow \]

\[ UU^+ (\mathbf{v}_k) = \left( f^2 - g^2 \right) \mathbf{v}_k + 2 f g \mathbf{v}_k (\mathbf{n} \cdot \mathbf{\bar{v}}) - 2 f g \sum_{\delta \in \mathbb{S}} \varepsilon_{\delta i k} \varepsilon_{\delta j l} \mathbf{v}_l \]  

(30)

\[ R_{\alpha k} (\mathbf{z}) = \frac{1}{2} \left[ \left( f^2 - g^2 \right) \mathbf{v}_k \mathbf{v}_l + 2 f g \mathbf{v}_k (\mathbf{n} \cdot \mathbf{\bar{v}}) - 2 f g \sum_{\delta \in \mathbb{S}} \varepsilon_{\delta i k} \varepsilon_{\delta j l} \mathbf{v}_l \right] \]

Now using the linearity (2, 3) and (13) \( \Rightarrow \)

\[ R_{\alpha k} (\mathbf{z}) = \left[ f^2(x) - g^2(x) \right] \delta_{\alpha k} + 2 f(x) g(x) \sum_{\delta \in \mathbb{S}} \varepsilon_{\alpha i k} \varepsilon_{\delta j l} \]

Let's change the dummy index \( j \) in (32) to \( l \) and note \( \varepsilon_{\alpha i k} = \varepsilon_{\alpha i k} \) (two permutations), to find

\[ R_{\alpha k} (\mathbf{z}) = \left[ f^2(x) - g^2(x) \right] \delta_{\alpha k} + 2 f(x) g(x) \sum_{\delta \in \mathbb{S}} \varepsilon_{\alpha i k} \varepsilon_{\delta j l} \]

(31)

Now this can directly be compared to (2.21) to result in the equations:

\[ f^2(x) - g^2(x) = \cos \alpha, \quad 2 f(x) g(x) = 1 - \cos \alpha, \quad -2 f(x) g(x) = \sin \alpha, \]

Together with (29). The first two lead to give \( f(x) = \pm \cos \frac{\alpha}{2}, \quad g(x) = \pm \sin \frac{\alpha}{2} \). Only the "+" is acceptable (compute \( R \) for \( \alpha = \pi/2 \), then compare) so we finally obtain:

\[ R = \cos \frac{\alpha}{2} \mathbf{1} + i \sin \frac{\alpha}{2} (\mathbf{n} \cdot \mathbf{\bar{v}}) \]  

(32)
It may have appeared as if we pulled out the form (24) from a "magic hat." That is not the case. Form (24) is inspired by Specht's theorem from linear algebra. Specializing for 2x2 matrices only, it says that matrices A and B are unitarily equivalent, that is there exists a unitary matrix U s.t.: 
\[ B = U A U^+ \]  
(33)

if and only if:

a) \( \text{tr}(A) = \text{tr}(B) \),  
b) \( \text{tr}(A^2) = \text{tr}(B^2) \),  
c) \( \text{tr}(AA^+) = \text{tr}(BB^+) \).

Since \( X \) and \( X' \) satisfy all these, we know that such \( U \) must exist.