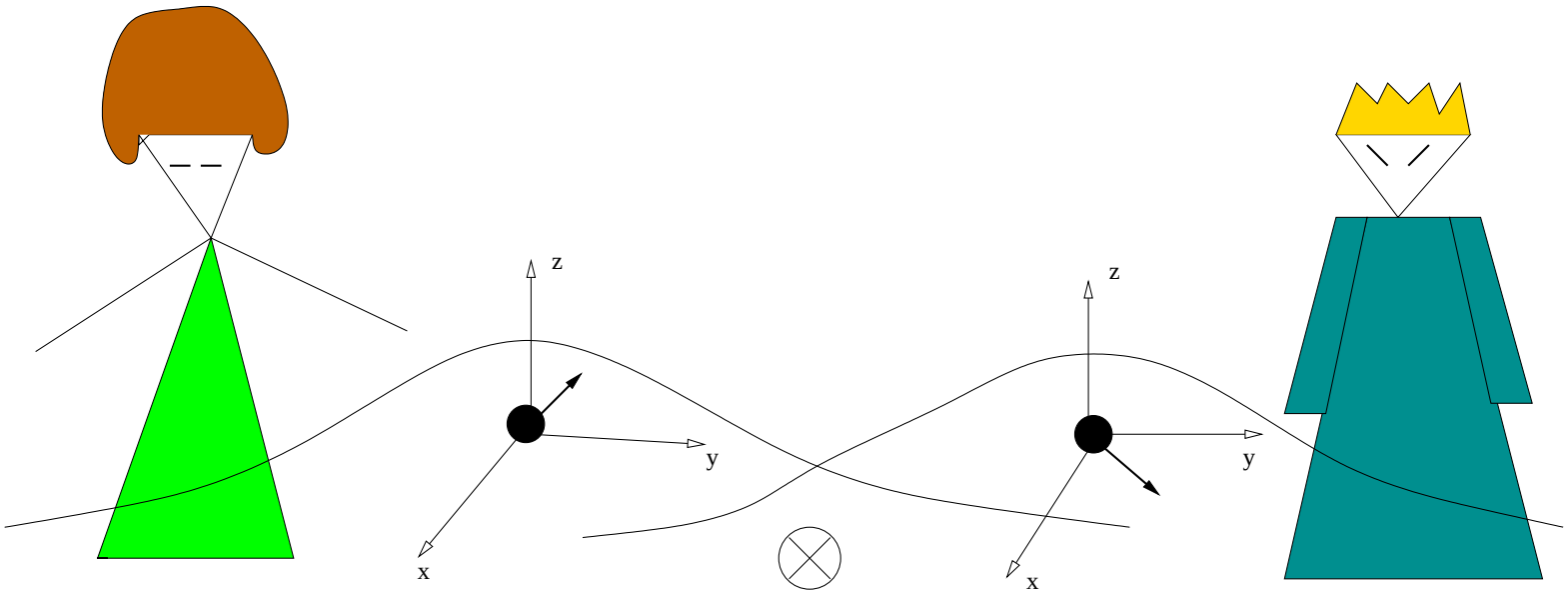
Mean King problem and mutually unbiased bases

Jakub Mielczarek

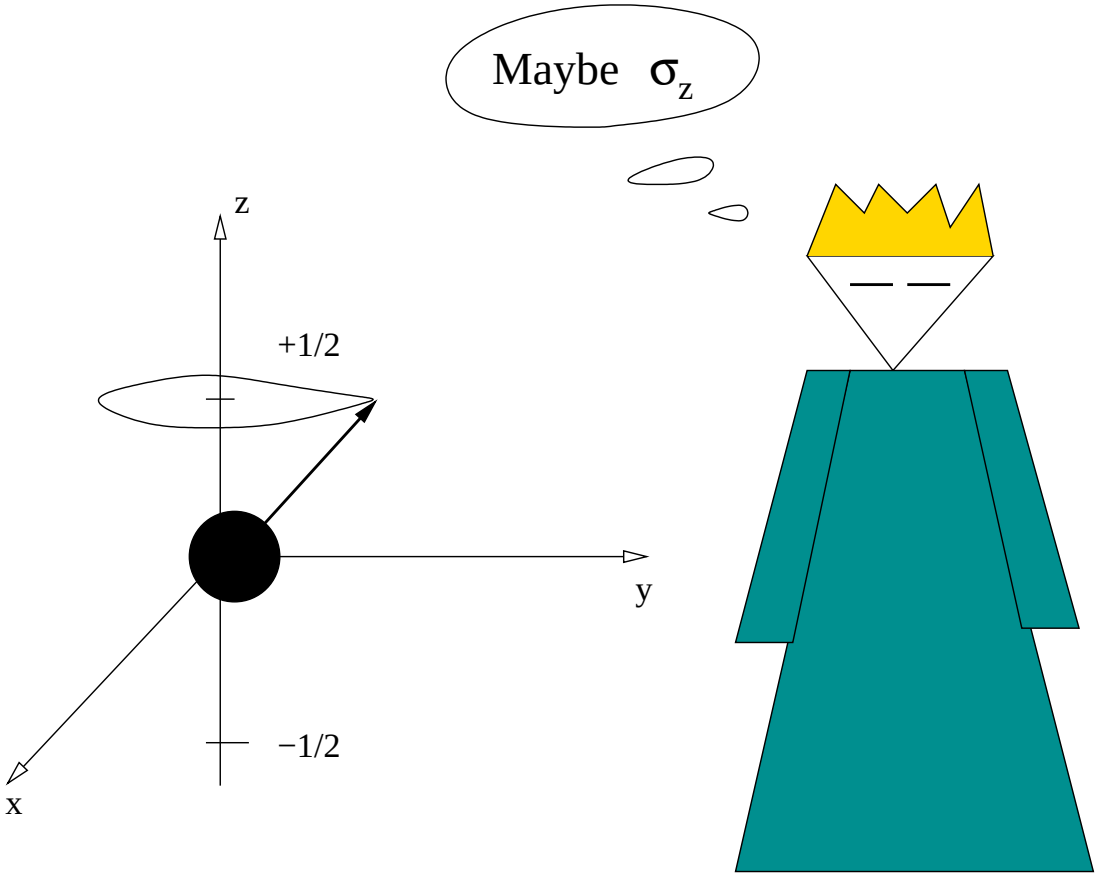
Specjalizacja Fizyki Teoretycznej UJ, rok IV

28 Maja, 2007

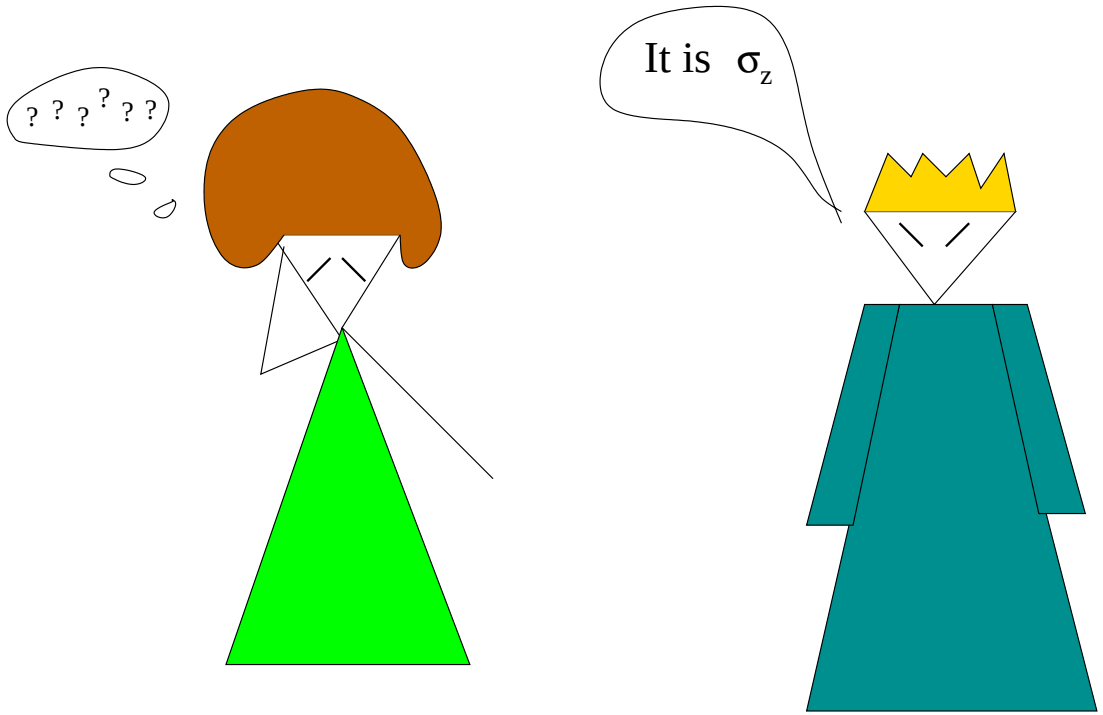
A Mean King challenges a physicist, Alice, who got stranded on the remote island ruled by the King, to prepare a spin1/2 atom in any state of her choosing and to perform a control measurement of her King.



Between her preparation and her measurement, the King's men determine the value of either σ_X, σ_Y or σ_Z.



Only after she completed the control measurement, the physicist is told which spin component has been measured, and she must then state the result of that intermediate measurement correctly. How does she do it?



Basic ideas

Alice and King share a maximally entangled state on $\mathcal{C}^2 \otimes \mathcal{C}^2$:

$$|\Psi\rangle = \frac{1}{\sqrt{2}} \{|0\rangle_A^z \otimes |0\rangle_K^z + |1\rangle_A^z \otimes |1\rangle_K^z\}$$

After King measurement :

$$|out\rangle = |1\rangle_A^z \otimes |1\rangle_K^z$$

$$\begin{aligned}
|1\rangle &= |0\rangle_A^z \otimes |0\rangle_K^z \Rightarrow \langle out|1\rangle = 0 \\
|2\rangle &= |0\rangle_A^z \otimes |1\rangle_K^z \Rightarrow \langle out|2\rangle = 0 \\
|3\rangle &= |1\rangle_A^z \otimes |0\rangle_K^z \Rightarrow \langle out|3\rangle = 0 \\
|4\rangle &= |1\rangle_A^z \otimes |1\rangle_K^z \Rightarrow \langle out|4\rangle = 1
\end{aligned}$$

The qubit case [1]

Bell base :

$$
\begin{aligned}
|B_1\rangle^z &= \frac{1}{\sqrt{2}}\{|0\rangle^z \otimes |0\rangle^z + |1\rangle^z \otimes |1\rangle^z\} \\
|B_2\rangle^z &= \frac{1}{\sqrt{2}}\{|0\rangle^z \otimes |0\rangle^z - |1\rangle^z \otimes |1\rangle^z\} \\
|B_3\rangle^z &= \frac{1}{\sqrt{2}}\{|0\rangle^z \otimes |1\rangle^z + |1\rangle^z \otimes |0\rangle^z\} \\
|B_4\rangle^z &= \frac{1}{\sqrt{2}}\{|0\rangle^z \otimes |1\rangle^z - |1\rangle^z \otimes |0\rangle^z\}
\end{aligned}
$$

[1] L. Vaidman, Y. Aharonov, and D. Z. Albert, Phys. Rev. Lett. **58**, 1385 (1987)., See also T.Durt ,arXiv:quant-ph/0401037

Alice performs a von Neumann measurement

$$
\begin{aligned}
|\Psi_1\rangle^z &= \frac{1}{4}\{|B_1\rangle^z + |B_2\rangle^z + |B_3\rangle^z + i|B_4\rangle^z\} \\
|\Psi_2\rangle^z &= \frac{1}{4}\{|B_1\rangle^z + |B_2\rangle^z - |B_3\rangle^z - i|B_4\rangle^z\} \\
|\Psi_3\rangle^z &= \frac{1}{4}\{|B_1\rangle^z - |B_2\rangle^z + |B_3\rangle^z - i|B_4\rangle^z\} \\
|\Psi_4\rangle^z &= \frac{1}{4}\{|B_1\rangle^z - |B_2\rangle^z - |B_3\rangle^z + i|B_4\rangle^z\}
\end{aligned}
$$

It is easy to check that

$$\begin{aligned} \langle\Psi_1|(|1\rangle_A^z \otimes |1\rangle_K^z) &= \langle\Psi_2|(|1\rangle_A^z \otimes |1\rangle_K^z) = 0 \\ \langle\Psi_3|(|0\rangle_A^z \otimes |0\rangle_K^z) &= \langle\Psi_4|(|0\rangle_A^z \otimes |0\rangle_K^z) = 0 \end{aligned}$$

Therefore, if Alice observes one of the two last (first) states and that afterwards the King reveals that he observed a state in the Z basis she can infer unambiguously that the Mean King observed-measured-prepared the state $|1\rangle_A^z \otimes |1\rangle_K^z$ ($|0\rangle_A^z \otimes |0\rangle_K^z$).

$$
\begin{aligned}
|B_1\rangle^z &= |B_1\rangle^x = |B_1\rangle^y \\
|B_2\rangle^z &= |B_3\rangle^x = |B_3\rangle^y \\
|B_3\rangle^z &= |B_2\rangle^x = i|B_4\rangle^y \\
|B_4\rangle^z &= -|B_4\rangle^x = -i|B_2\rangle^y
\end{aligned}
$$

So that the four states $|\Psi\rangle^z$ are bijectively transformed in the four states $|\Psi\rangle^x$ and $|\Psi\rangle^y$(up to unobservable phase changes).

Therefore Alice can infer without error the values of the spins along three orthogonal directions and consequently save her head.

Def. 1

Two orthonormal bases in $\mathcal{C}^d$, $\mathcal{B}$ and $\mathcal{B}'$ are said mutually unbiased if $\forall \ |b\rangle \in \mathcal{B}, |b'\rangle \in \mathcal{B}'$ relation

$$|\langle b|b'\rangle|^2 = \frac{1}{d}$$

holds.

But what it physically mean and why we want to us it ?

Qunatum state $|\Psi\rangle$ in d-dim Hilbert space can be described by density matrix $\hat{\rho} = |\Psi\rangle\langle\Psi|$ with $\mathrm{tr}\hat{\rho} = 1 \quad \Rightarrow$ density matrix has $d^2 - 1$ degrees of freedom.

Particular measurment yield $d - 1$ independent probalities.

One needs $d + 1$ distinct basis sets to provide required total number $d^2 - 1 = (d + 1)(d - 1)$ independent probalites.

Such a bases are MUB's.

Let see it in $d = 2$ case

$$
\begin{aligned}
|\Psi\rangle &= |A_1\rangle\langle A_1|\Psi\rangle + |A_2\rangle\langle A_2|\Psi\rangle \quad \text{where} \quad |\langle A_1|\Psi\rangle|^2 + |\langle A_2|\Psi\rangle|^2 = 1 \\
|\Psi\rangle &= |B_1\rangle\langle B_1|\Psi\rangle + |B_2\rangle\langle B_2|\Psi\rangle \quad \text{where} \quad |\langle B_1|\Psi\rangle|^2 + |\langle B_2|\Psi\rangle|^2 = 1 \\
|\Psi\rangle &= |C_1\rangle\langle C_1|\Psi\rangle + |C_2\rangle\langle C_2|\Psi\rangle \quad \text{where} \quad |\langle C_1|\Psi\rangle|^2 + |\langle C_2|\Psi\rangle|^2 = 1
\end{aligned}
$$

Measured probabilities are

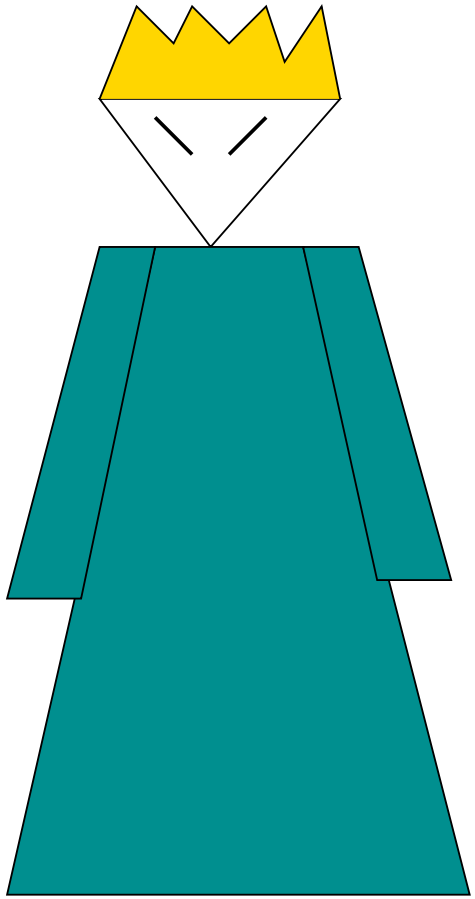
$$
P_A = |\langle A_1|\Psi\rangle|^2, \quad P_B = |\langle B_1|\Psi\rangle|^2, \quad P_C = |\langle C_1|\Psi\rangle|^2
$$

King's problem with mutually unbiased bases

In a d-dimensional complex vector space $\mathcal{C}^d$, we consider $d+1$ orthonormal bases labeled by $A(=0,1,\ldots,d)$. By $|A,a\rangle$ $(a=0,1,\ldots,d-1)$, we denote a state vector in base A.

Bases are mutually unbiased:

$$\left|\langle A,a|A',a'\rangle\right|^2=\delta_{AA'}\delta_{aa'}+(1-\delta_{AA'})\frac{1}{d}.$$



Alice and King share a maximally entangled state on $\mathcal{C}^d \otimes \mathcal{C}^d$:

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle \otimes |k\rangle.$$

for d=2 (qubit case)

$$|\Phi\rangle = \frac{1}{\sqrt{2}} \{|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\}$$

The post-measurement state is then given by

$$|\Phi_{A,a}\rangle \equiv |\overline{A,a}\rangle \otimes |A,a\rangle.$$

Without knowing King's measurement base A and outcome a, Alice performs a projective measurement on the composite system in the base $\{|I\rangle\}_{I=0}^{d^2-1}$ of $\mathcal{C}^d \otimes \mathcal{C}^d$.

After the measurement, Alice is informed of King's measurement base A. Alice's task is now to estimate King's outcome a from her measurement outcome I and King's base A. Let us write Alice's estimate for King's outcome as $s(I,A) \in \{0,1,\ldots,d-1\}$.

Alice's success probability is 1 if and only if the following conditions are satisfied:

$$\langle \Phi_{A,a} | I \rangle = 0 \text{ for } a \neq s(I, A).$$

for d=2 (qubit case) ,$I = 1..4$

A_0)

$I \setminus a$	0	1
1	×	0
2	×	0
3	0	×
4	0	×

, A_1)

$I \setminus a$	0	1
1	×	0
2	0	×
3	0	×
4	×	0

, A_3)

$I \setminus a$	0	1
1	×	0
2	0	×
3	×	0
4	0	×

How it work

Let for example:

$$\langle\Phi|1\rangle = 0, \quad \langle\Phi|2\rangle = x, \quad \langle\Phi|3\rangle = 0, \quad \langle\Phi|4\rangle = x$$

Suppose, she use outcome $\langle\Phi|3\rangle = 0$.

$A_0)$

$I \setminus a$	0	1
1	×	0
2	×	0
3	0	×
4	0	×

, $A_1)$

$I \setminus a$	0	1
1	×	0
2	0	×
3	0	×
4	×	0

, $A_3)$

$I \setminus a$	0	1
1	×	0
2	0	×
3	×	0
4	0	×

King inform Alice that $A = 2$. So outcome of his measurement is $a = 1$.

First we show that the set Φ consisting of $d(d+1)$ states $\{|\Phi_{A,a}\rangle\}_{A=0,a=0}^{A=d,a=d-1}$ is complete in the composite space $\mathcal{C}^d \otimes \mathcal{C}^d$.
Suppose a linear relation with some coefficients $c_{A,a}$ holds,

$$\sum_{A,a} c_{A,a} |\Phi_{A,a}\rangle = 0.$$

Multiplying bra vector $\langle \Phi_{A',a'}|$ from the left

$$\sum_{A,a} c_{A,a} \underbrace{\langle \Phi_{A',a'} | \Phi_{A,a} \rangle}_{\delta_{AA'}\delta_{aa'} + (1-\delta_{AA'})\frac{1}{d}} = 0$$

we find

$$c_{A',a'} + \sum_{A(\neq A')} \frac{1}{d} \sum_{a} c_{A,a} = 0.$$

$$c_{A',a'} = -\sum_{A(\neq A')} \frac{1}{d} \sum_{a} c_{A,a}$$

It implies that the coefficient $c_{A,a}$ should be independent of a.

Now consider the subset Φ' which consists of d^2 states obtained by removing d states $\{|\Phi_{A,a}\rangle\}_{A\neq 0, a=0}$ from Φ.

$A \setminus a$	0	1	...	$d-1$
0	0	1	...	$d-1$
1	0	1	...	$d-1$
2	0	1	...	$d-1$
3	0	1	...	$d-1$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
d	0	1	...	$d-1$

Next we consider another subset Φ''_I obtained by removing $d+1$ states $\{|\Phi_{A,s(I,A)}\rangle\}_{A=0}^{d}$ from Φ for a given I. It is easy to see that the d^2-1 states in Φ''_I are linearly independent and span a d^2-1 subspace of $\mathcal{C}^d \otimes \mathcal{C}^d$.

$A \setminus a$	0	1	2	3	...	$d-1$
0	0	1	2	3	...	$d-1$
1	0	1	2	3	...	$d-1$
2	0	1	2	3	...	$d-1$
3	0	1	2	3	...	$d-1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
d	0	1	2	3	...	$d-1$

For studied qubit case

$A_0)$

$l \setminus a$	0	1
1	×	0
2	×	0
3	0	×
4	0	×

, $A_1)$

$l \setminus a$	0	1
1	×	0
2	0	×
3	0	×
4	×	0

, $A_3)$

$l \setminus a$	0	1
1	×	0
2	0	×
3	×	0
4	0	×

So for $l = 1$ we have

$A \setminus a$	0	1
0	0	1
1	0	1
2	0	1

The conditions

$$\langle \Phi_{A,a} | I \rangle = 0 \text{ for } a \neq s(I, A)$$

require that each state $|I\rangle$ should be orthogonal to the $d^2 - 1$ dimensional subspace spanned by Φ''_I and can be uniquely determined up to an irrelevant phase factor.
It was found [2] that state $|I\rangle$ satisfying this conditions is given by

$$|I\rangle = \frac{1}{\sqrt{d}} \sum_{A=0}^{d} |\Phi_{A,s(I,A)}\rangle - |\Phi\rangle.$$

[2] A. Hayashi, M. Horibe, and T. Hashimoto, arXiv:quant-ph/0502092

It remains to determine the condition for Alice's estimate $s(l, A)$ under which $\{|l\rangle\}_{l=0}^{d^2-1}$ is an orthonormal base in $\mathcal{C}^d \otimes \mathcal{C}^d$.

$$\sum_{A=0}^{d} \delta_{s(l,A),s(l',A)} = 1 \text{ for } l \neq l'$$

$$\begin{aligned} \mathbf{s} &= s_0 s_1 s_2 \cdots s_d, \\ s_A &\in \{0, 1, \ldots, d-1\}. \end{aligned}$$

$$\sum_{A=0}^{d} \delta_{s_A,s'_A} = 1.$$

for d=2:

0	0	0
0	1	1
1	1	0
1	0	1

for d=3:

0	0	0	0
0	2	1	1
0	1	2	2
1	1	1	0
1	0	2	1
1	2	0	2
2	2	2	0
2	1	0	1
2	0	1	2

Here we study the condition derived from the completeness $\sum_{l=0}^{d^2-1} |l\rangle\langle l| = \mathbf{1}$, which is equivalent to the orthogonality. Since the set of states $\{|\Phi_{A,a}\rangle\}_{A=0,a=0}^{A=d,a=d-1}$ is complete, the completeness of $\{|l\rangle\}_{l=0}^{d^2-1}$ can be expressed as

$$\sum_{l=0}^{d^2-1} \underbrace{\langle \Phi_{A,a}|l\rangle}_{\frac{1}{\sqrt{d}}\delta_{a,s(l,A)}} \underbrace{\langle l|\Phi_{A',a'}\rangle}_{\frac{1}{\sqrt{d}}\delta_{a',s(l,A')}} = \underbrace{\langle \Phi_{A,a}|\Phi_{A',a'}\rangle}_{\delta_{AA'}\delta_{aa'}+(1-\delta_{AA'})\frac{1}{d}} .$$

What gives

$$\sum_{l=0}^{d^2-1} \delta_{a,s(l,A)}\,\delta_{a',s(l,A')} = d\,\delta_{A,A'}\delta_{a,a'} + (1-\delta_{A,A'}).$$

Latin squares

The condition

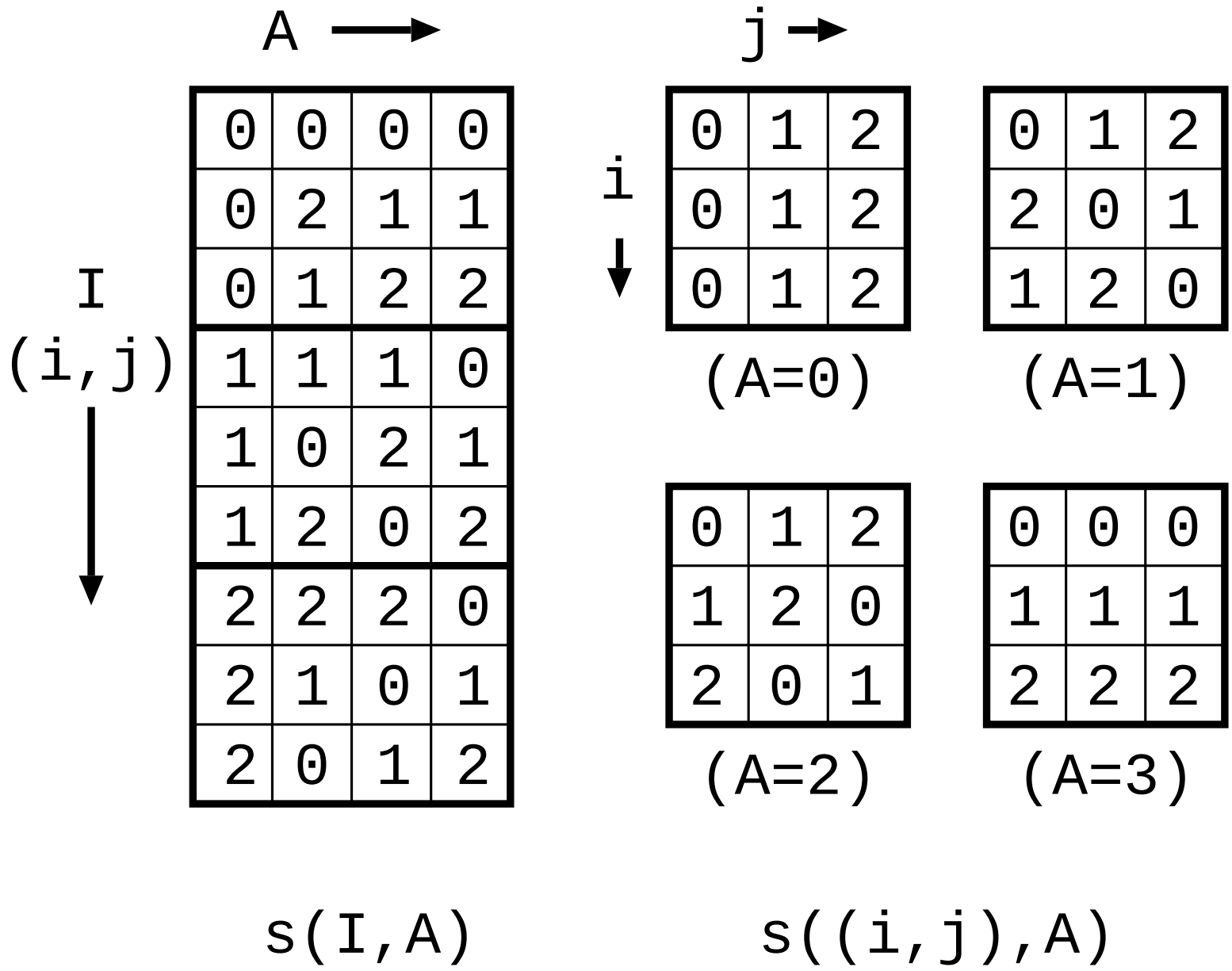
$$\sum_{I=0}^{d^2-1} \delta_{a,s(I,A)}\, \delta_{a',s(I,A')} = d\, \delta_{A,A'} \delta_{a,a'} + (1 - \delta_{A,A'})$$

turns out to be that of the existence of $d+1$ orthogonal d by d Latin squares[3].

Def. 2

Two Latin squares are said to be orthogonal if each group of either Latin square has exactly one point in common with each group in the other.

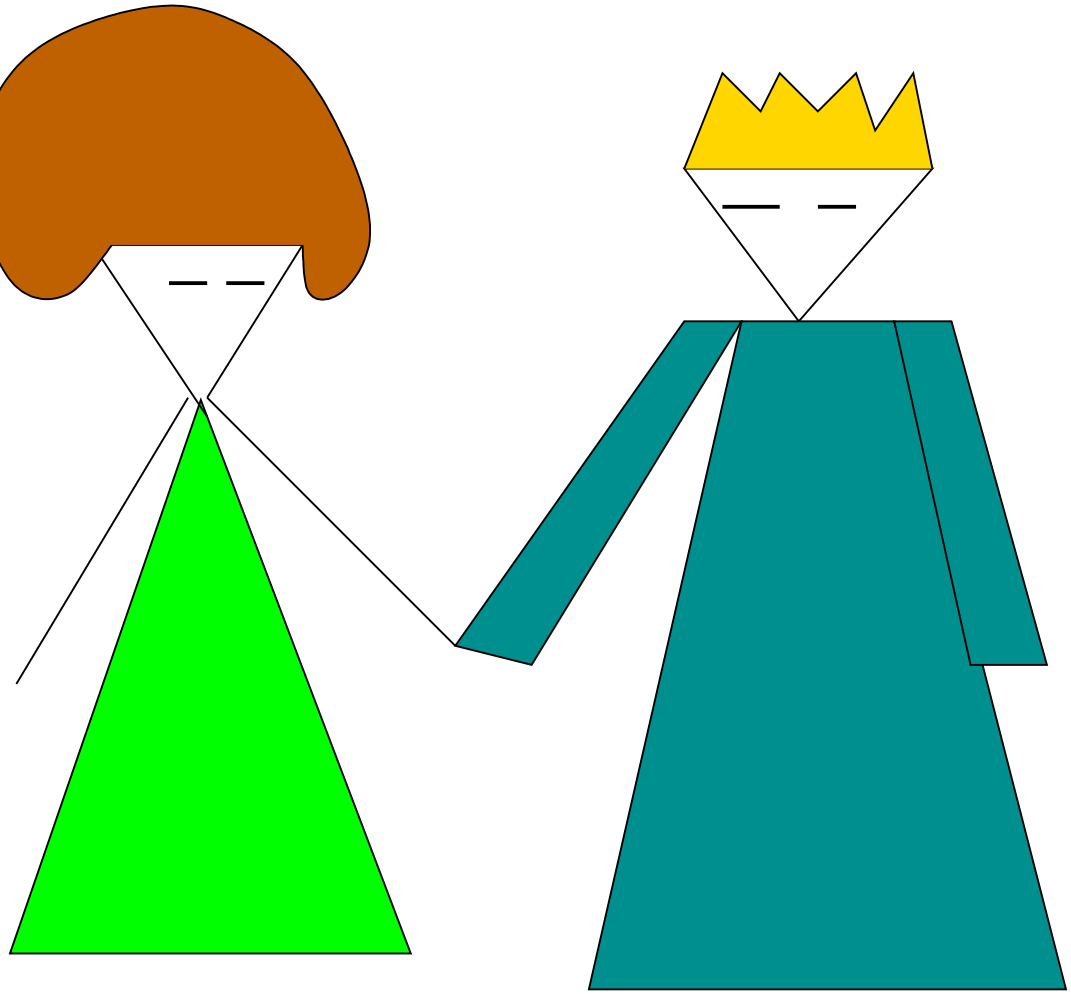
[3] See William K. Wootters, arXiv:quant-ph/0406032


A
I
(i,j)
0 0 0 0
0 2 1 1
0 1 2 2
1 1 1 0
1 0 2 1
1 2 0 2
2 2 2 0
2 1 0 1
2 0 1 2
s(I,A)
j
i
0 1 2
0 1 2
0 1 2
(A=0)
0 1 2
2 0 1
1 2 0
(A=1)
0 1 2
1 2 0
2 0 1
(A=2)
0 0 0
1 1 1
2 2 2
(A=3)
s((i,j),A)

Some known results on the maximum number $M(d)$ of $d \times d$ mutually orthogonal Latin squares are summarized in [4] as follows:

- For any d, $M(d) \leq d + 1$.
- If d is a power of a prime, $M(d) = d + 1$.
- $M(6) = 3$.
- If $d - 1$ or $d - 2$ is divisible by four, and if d is not the sum of the squares of two integers, then $M(d) < d + 1$.
- $M(10) < 11$.

[4] William K. Wootters, arXiv:quant-ph/0406032.



Thank You for attention