Secure alignment of coordinate systems

Asia-Pacific Conference and Workshop in Quantum Information Science

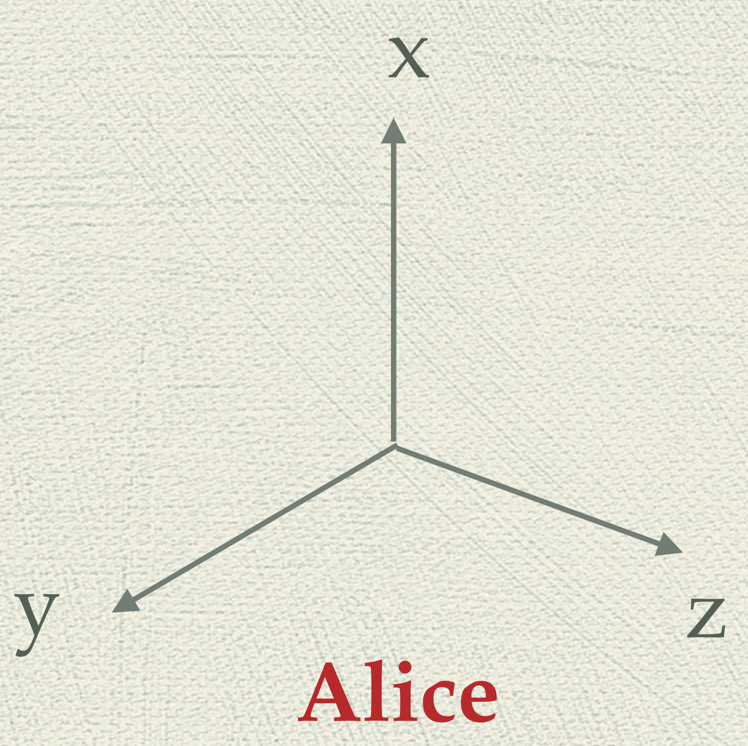
Vahid Karimipour,
Sharif University of Technology,
Tehran, Iran.

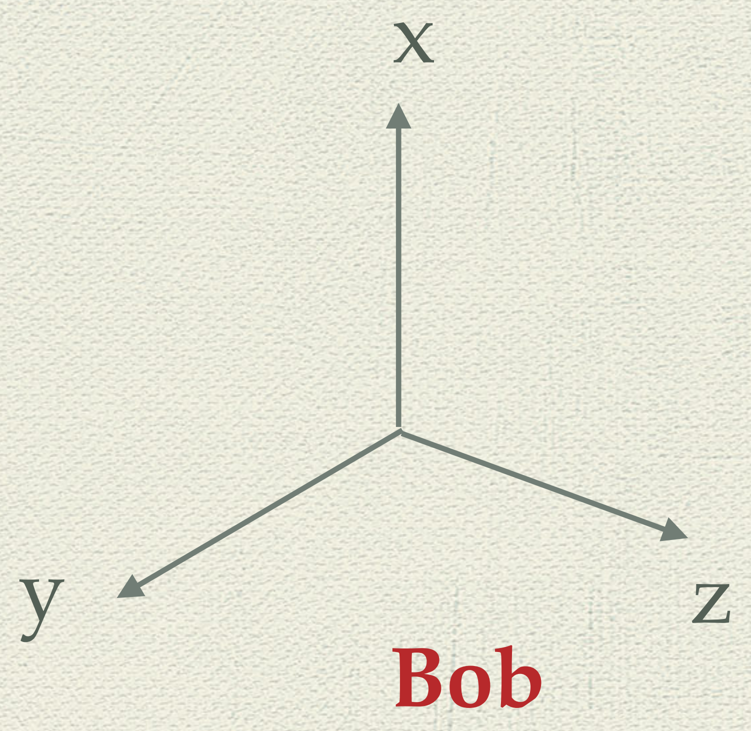
Many QI tasks need a Common Reference Frame

Teleportation

Even sending classical information through a quantum channel needs a Common Reference Frame

The Goal:
To set up a shared reference frame





Unspeakable Information

10101000100001000010000

Unspeakable Information

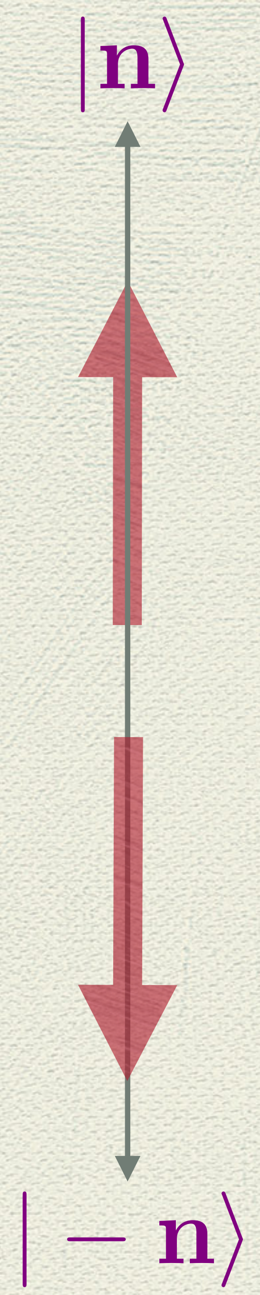
How do you define "Left" in a dictionary?

sharing a direction with a single spin

Alice

Bob

Random Guess



$$P(\mathbf{n}|\mathbf{m}) = |\langle \mathbf{n}|\mathbf{m}\rangle|^2$$

$$P(-\mathbf{n}|\mathbf{m}) = |\langle -\mathbf{n}|\mathbf{m}\rangle|^2$$

$$F(\mathbf{m}) = P(\mathbf{n}|\mathbf{m})|\langle\mathbf{n}|\mathbf{m}\rangle|^2 + P(-\mathbf{n}|\mathbf{m})|\langle-\mathbf{n}\mathbf{m}\rangle|^2$$

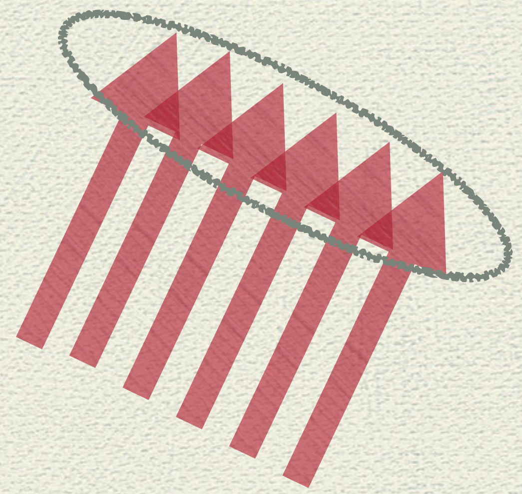
$$= |\langle\mathbf{n}|\mathbf{m}\rangle|^4 + |\langle-\mathbf{n}|\mathbf{m}\rangle|^4$$

$$\overline{F} = \int d\mathbf{m} F(\mathbf{m}) = \frac{2}{3}$$

Using N spins

Optimal measurement

N



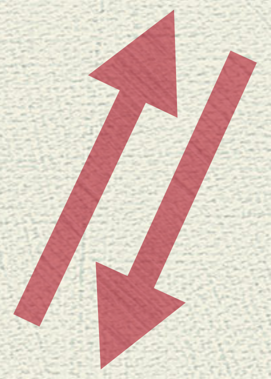
N

$$\overline{F} = \frac{N+1}{N+2}$$

Massar and Popescu, PRL (1995).

An interesting question

OR



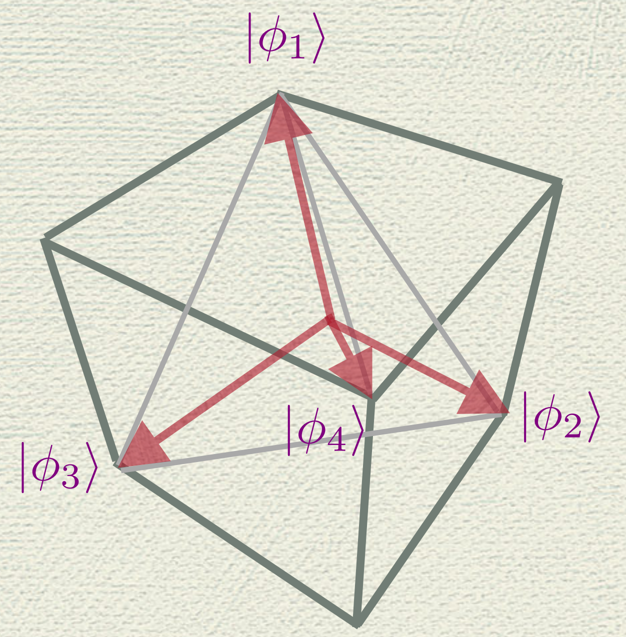
Which pair is better?

Gisin and Popescu, PRL(1999).

$|m\rangle$

$|m\rangle$

$|\psi_m\rangle$

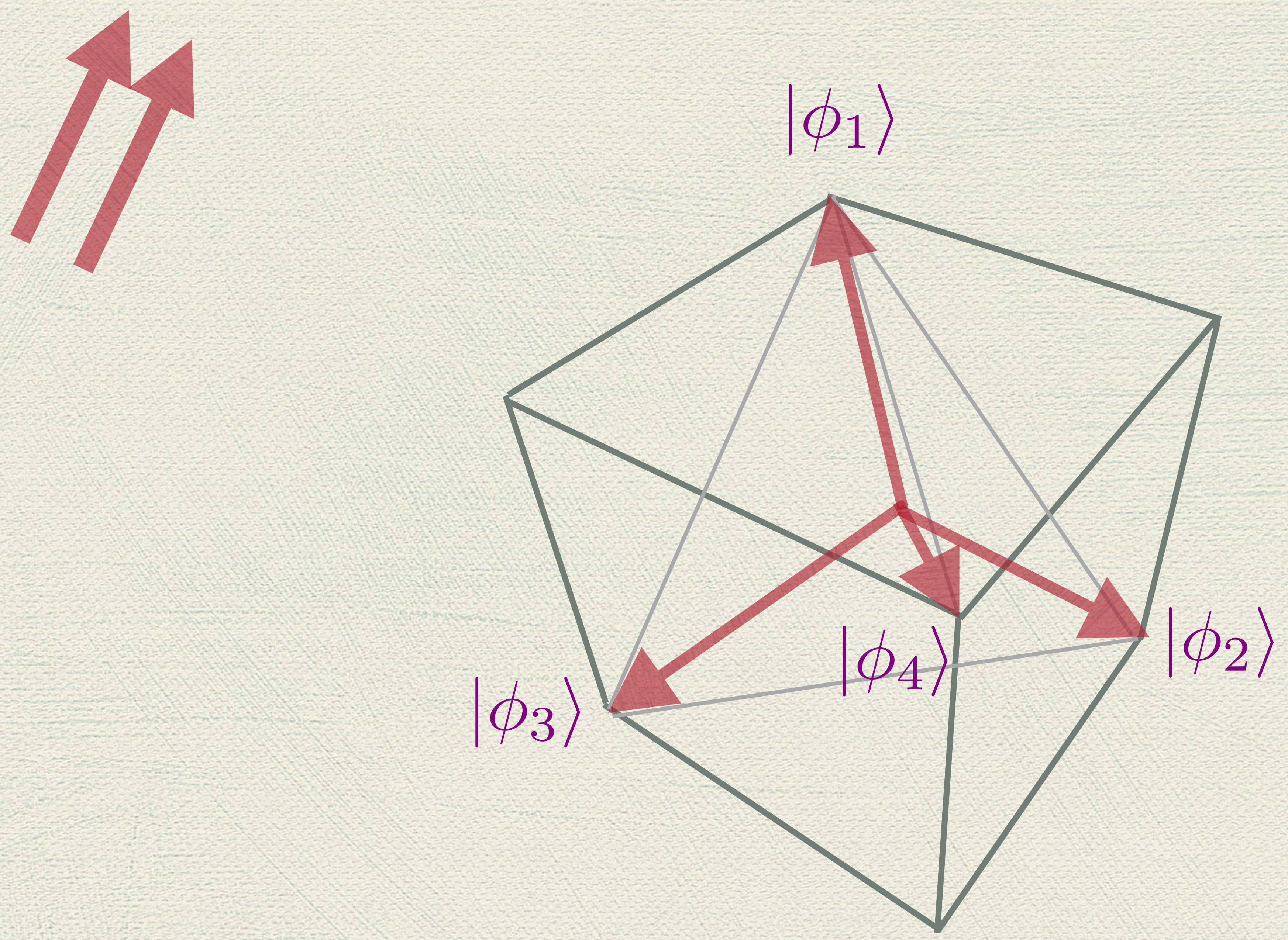


E_n

$$P(n \mid m) = \langle \psi_m | E_n | \psi_m \rangle$$

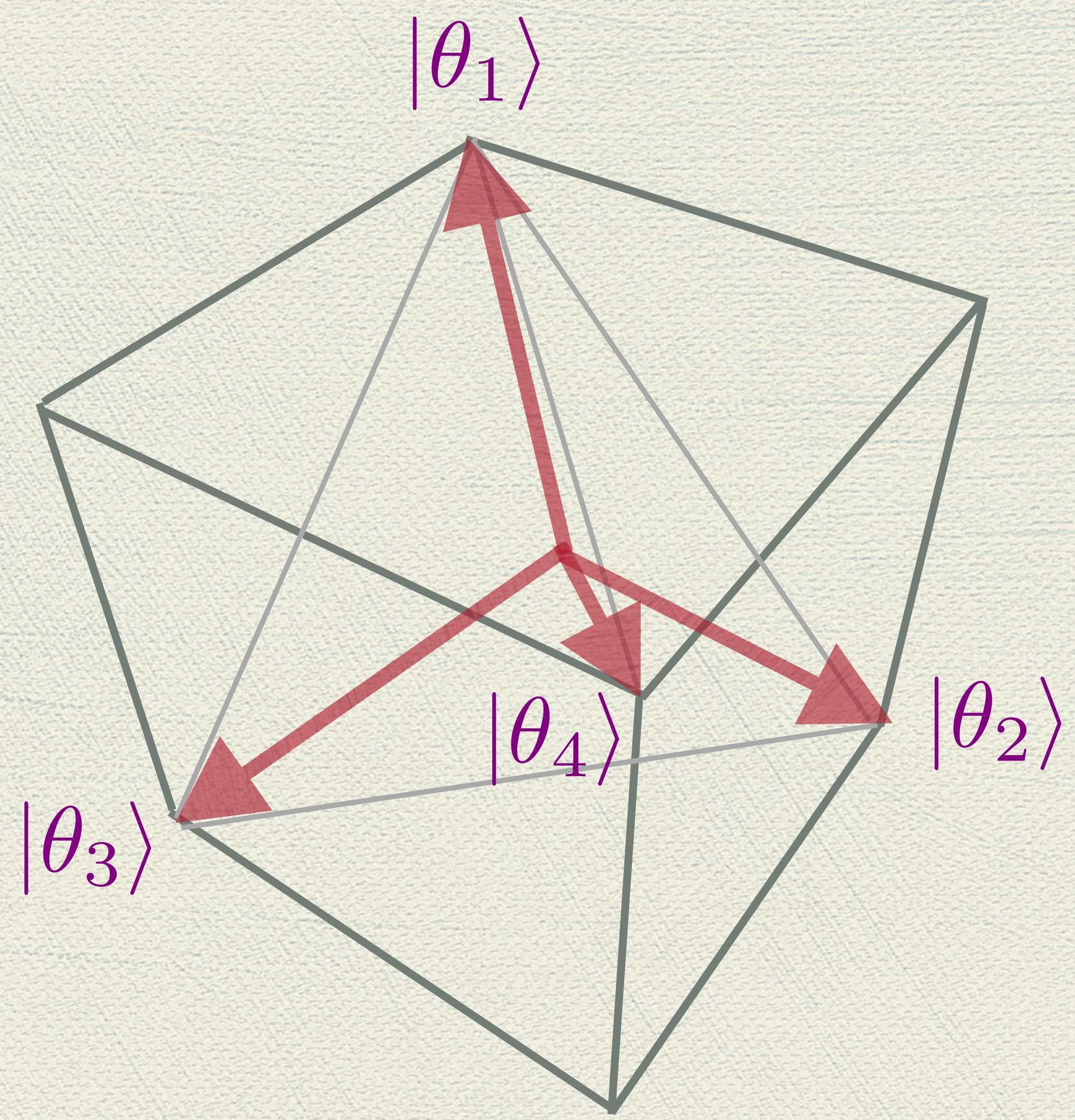
$$F(n,m) = \frac{1 + n \cdot m}{2}$$

$$F = \int dn \int dm \; \mathrm{P(n|m)} \; F(n,m)$$



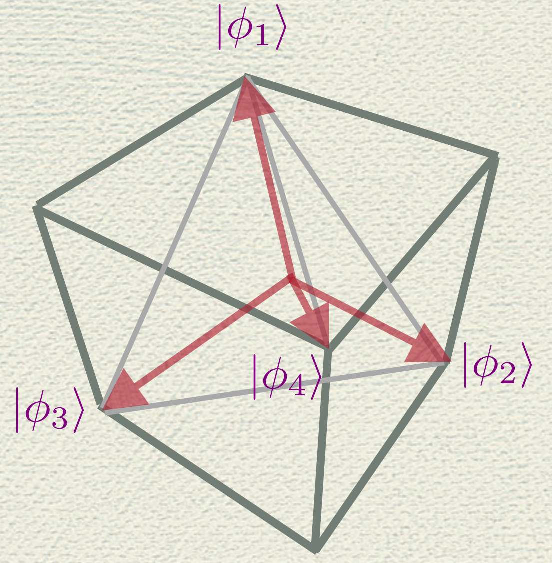
$$\overline{F} = 0.75$$

$$|\phi_j\rangle = \frac{\sqrt{3}}{2}|\mathbf{n}_j, \mathbf{n}_j\rangle + \frac{1}{2}|\psi^-\rangle$$

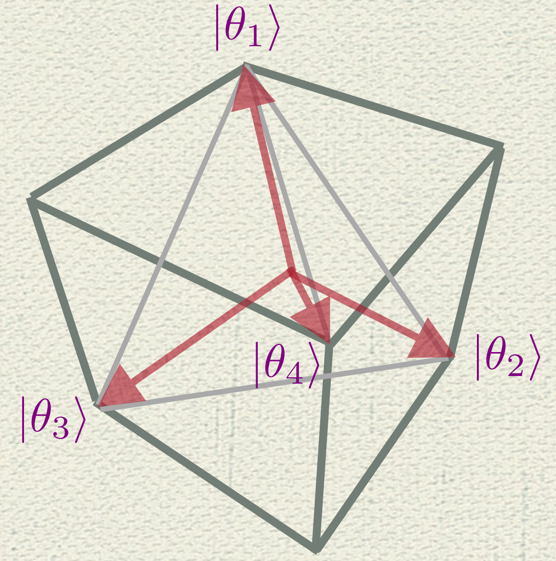


$$\overline{F} = 0.79$$

$$|\theta_i\rangle = \alpha|\mathbf{n}_i, -\mathbf{n}_i\rangle + \beta|\omega\rangle$$



There is no universal NOT



N

$$\overline{F} = \frac{N+1}{N+2}$$

N

Massar and Popescu, PRL (1995).

Existence of Continuous Optimal measurement

Derka, Buzek, and Ekert, PRL (1998)

Construction of finite Optimal measurement

Latorre, Pascual, and Tarrach (1998)

Construction of minimal Optimal measurement for N<7

The problem of security

Eve can do measurement on half of the spins

Using entanglement

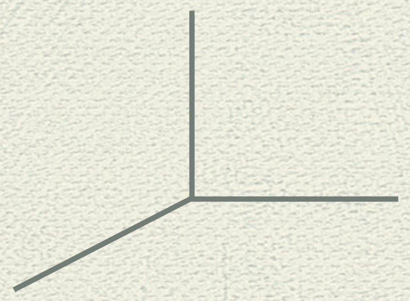
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

F. Rezazadeh, A. Mani, V. Karimipour
Phys. Rev. A, 96, 022310 (2017)

The idea of QKD:

Alice

Bob



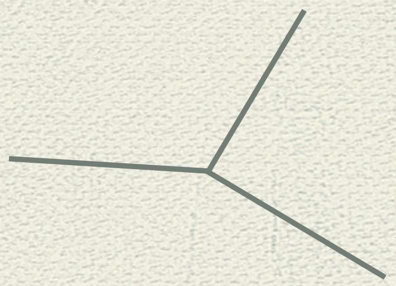
QKD: Publicly announce bases

Keep the results for yourself.

The idea of Direction Sharing

Alice

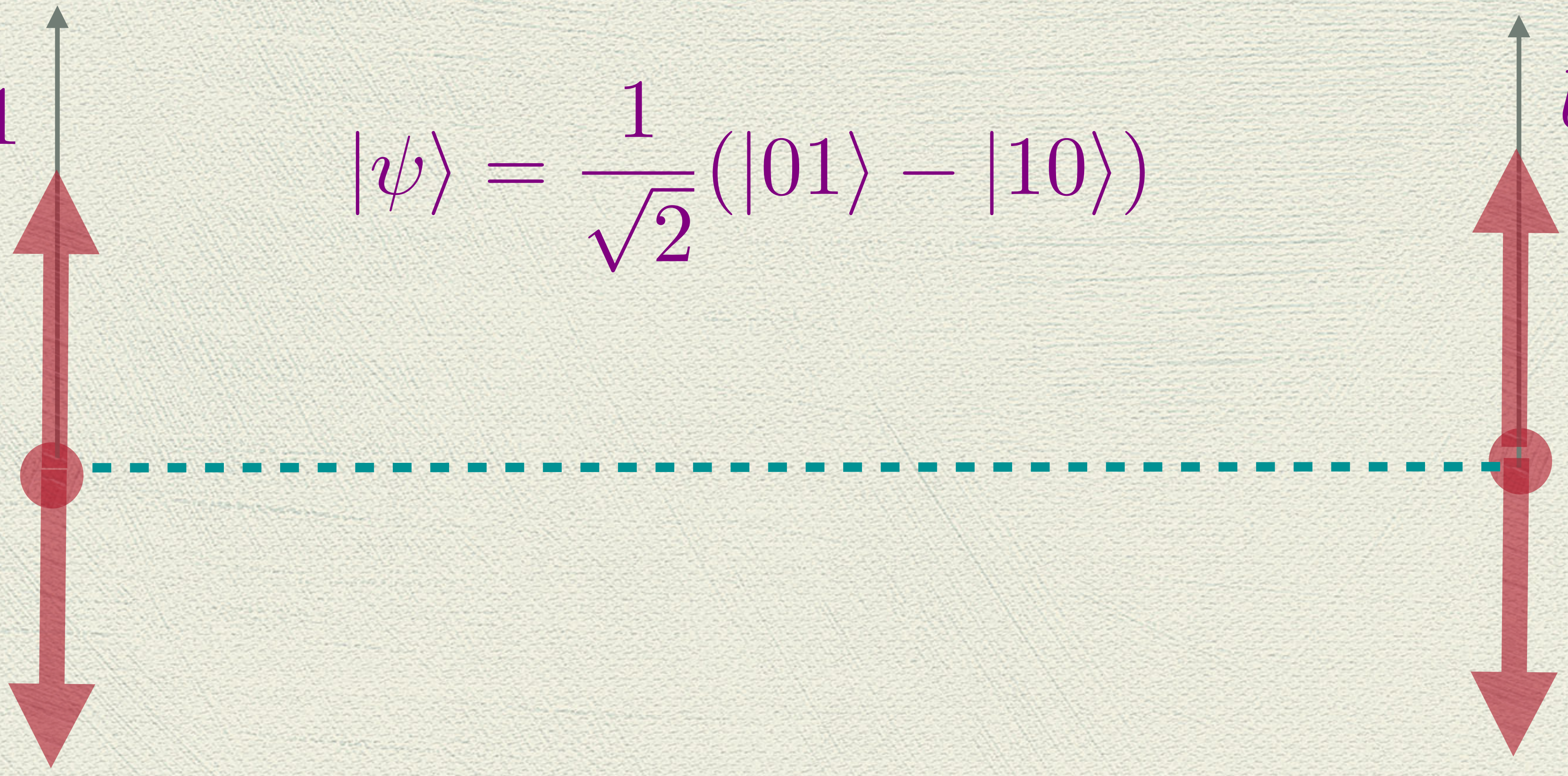
Bob



Publicly announce the results

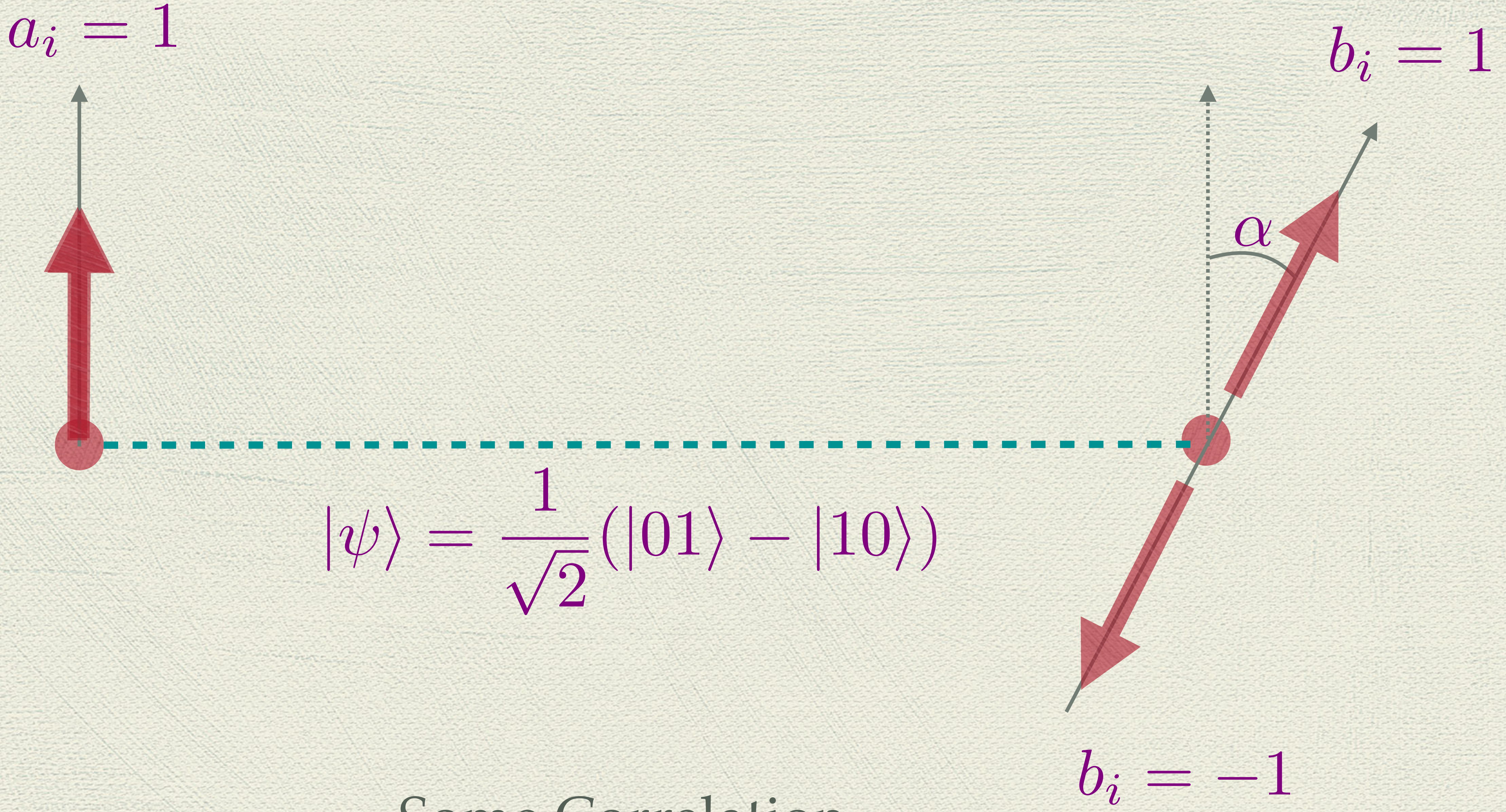
And use the correlations to align the bases

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$



Perfect Correlation

$$q_N = \frac{1}{N}\sum_i a_i b_i = 1$$



Some Correlation

$$q_N = \frac{1}{N}\sum_i a_i b_i$$

When we have infinite pairs

$$q_N = \frac{1}{N} \sum_i a_i b_i$$

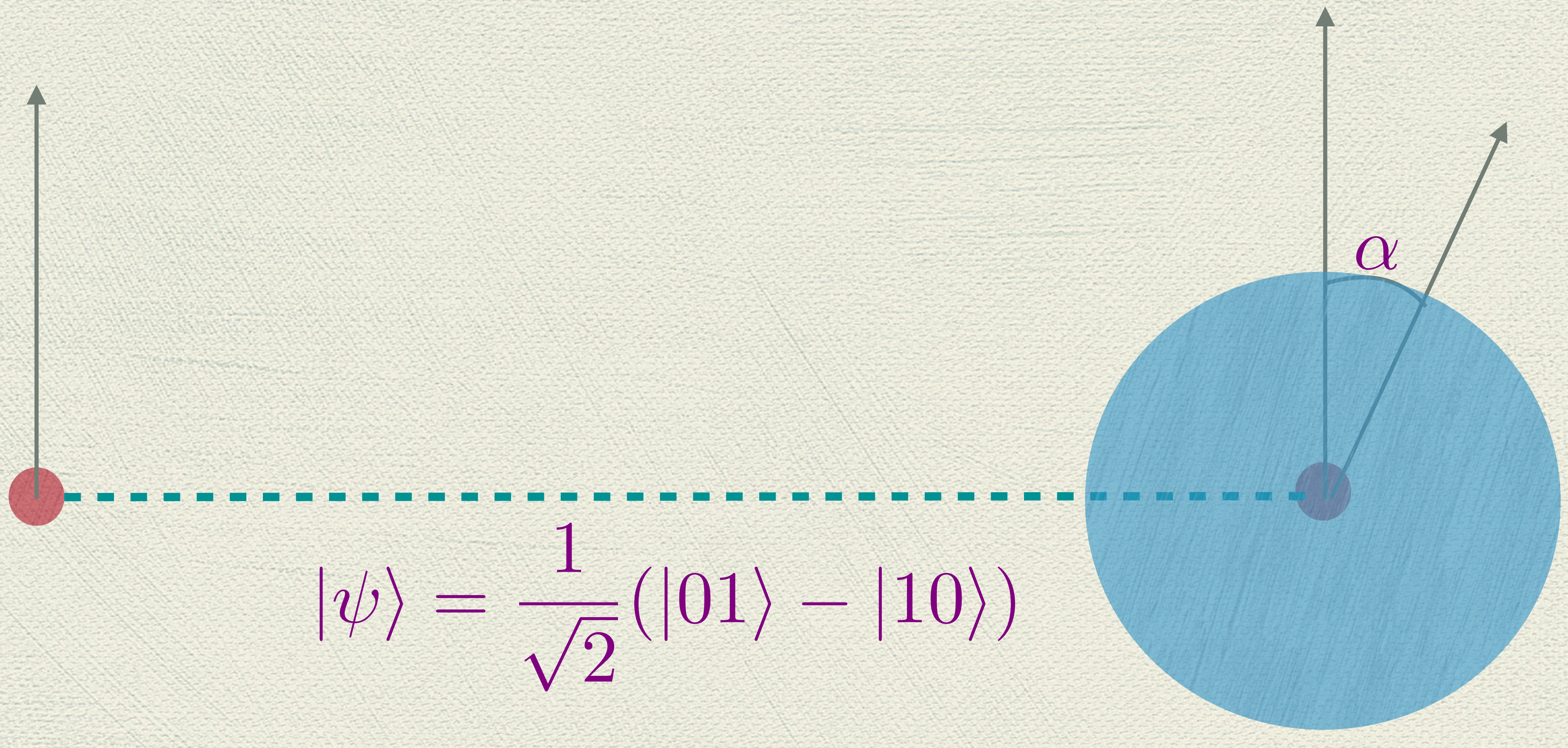
$N \longrightarrow \infty$

↓

$$q_\infty = P_{++} + P_{--} - P_{+-} - P_{-+}$$

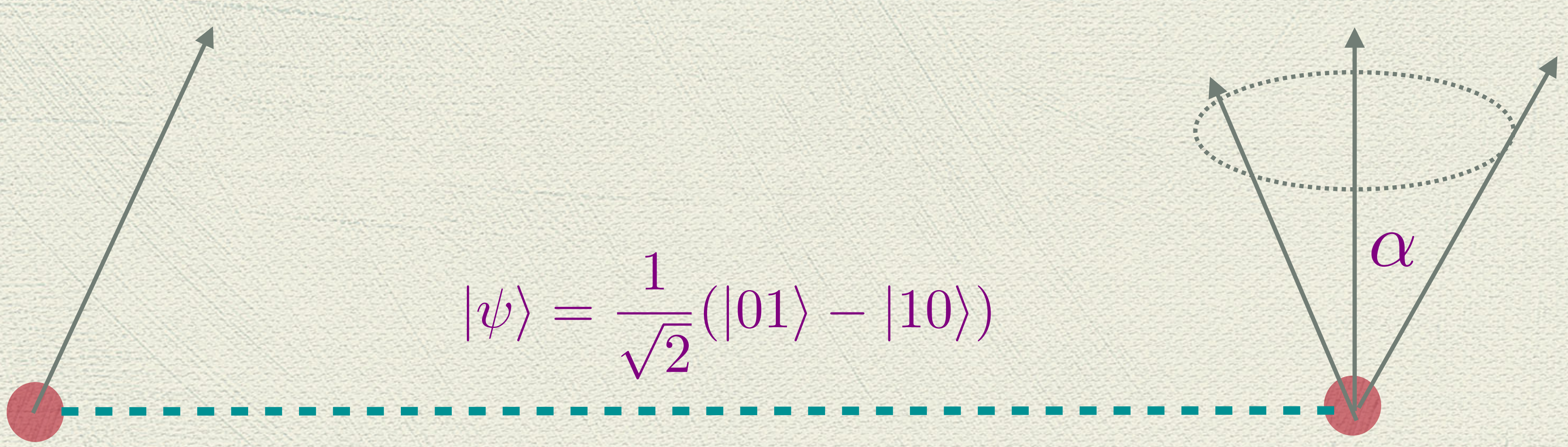
$$q_\infty = \cos \alpha$$

A naive method: Brute force search



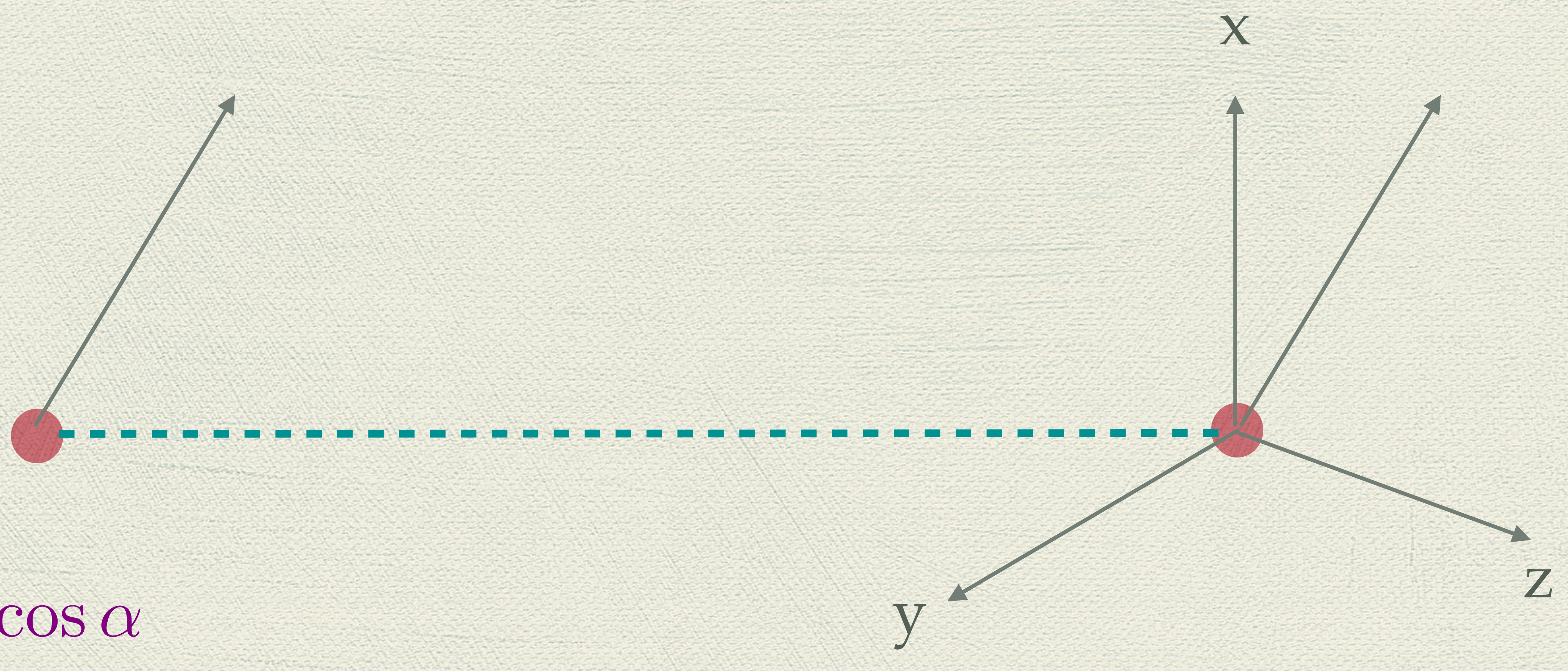
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

One measurement is not enough!



$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

With three measurements:



$$q_x = \cos\alpha$$

$$q_y = \cos\beta$$

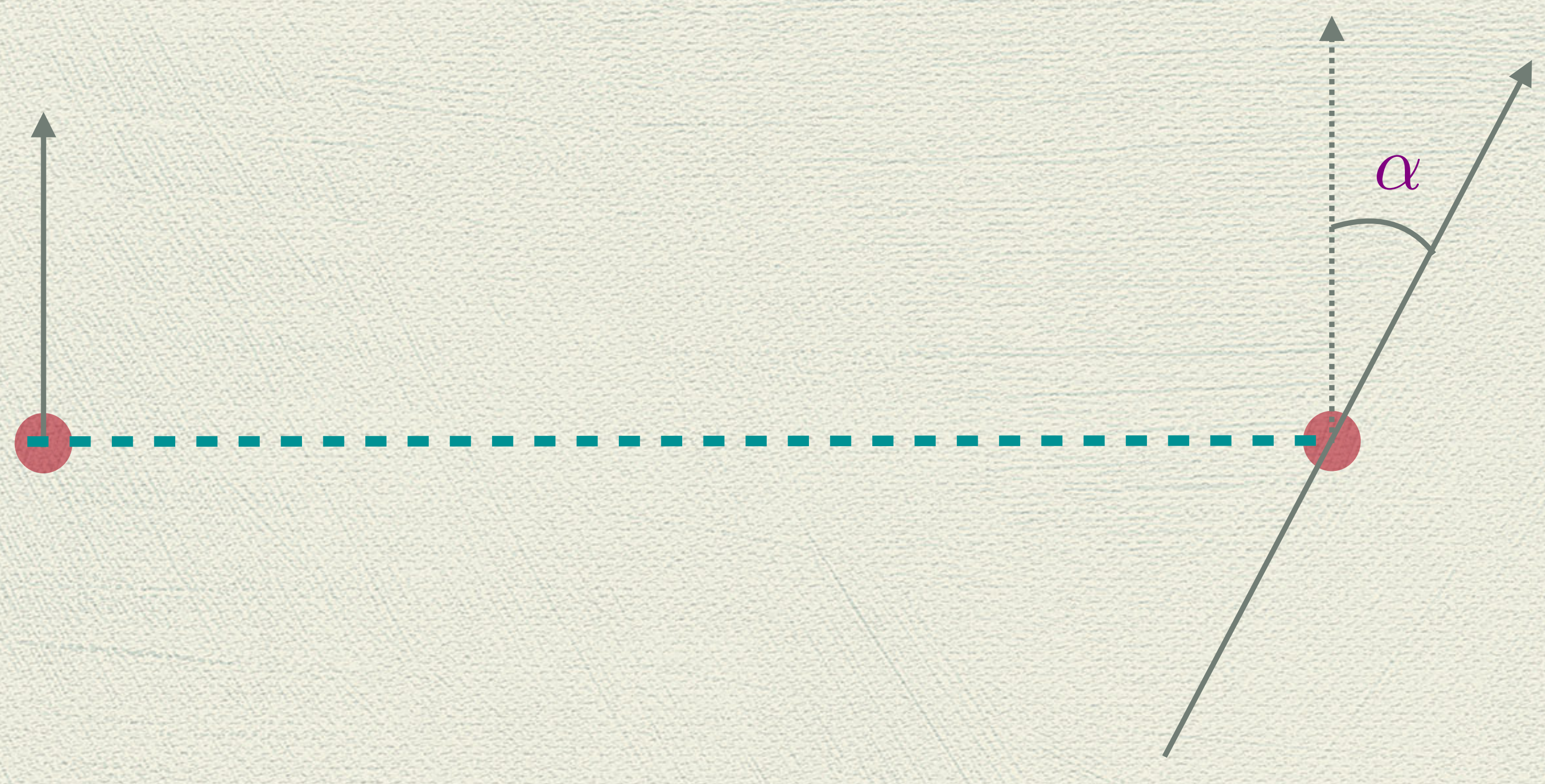
$$q_z = \cos\gamma$$

$$\mathbf{m} = q_x\ \mathbf{x} + q_y\ \mathbf{y} + q_z\ \mathbf{z}$$

However

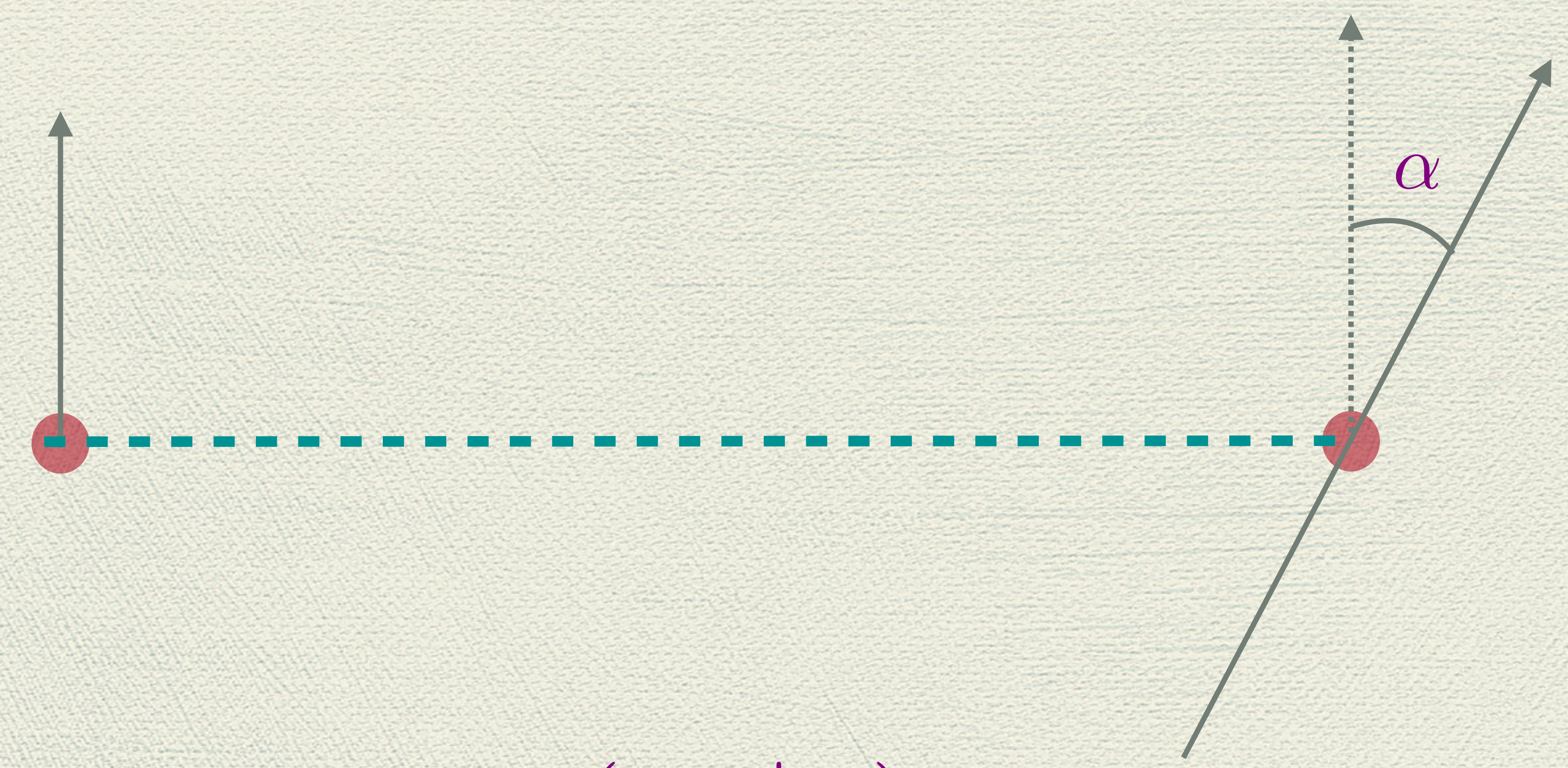
The number of pairs is not infinite!

So we have to estimate the angle from a correlation which has fluctuations.



$$P(q_N|\alpha)$$

The probability that the correlation is q_N if the angle is α



$$P(q_N|\alpha)$$

$$\langle q_N \rangle = \cos\alpha$$

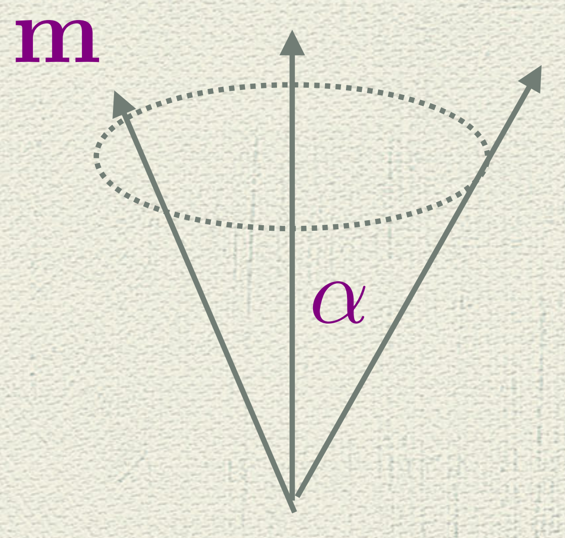
$$\langle q_N^2 \rangle = \cos^2\alpha + \frac{1}{N}\sin^2\alpha$$

The Baeysian Approach

$$P(\alpha|q_N)$$

What is the probability that the angle is α if the correlation is q_N

$$P(\mathbf{m} \mid q_N)$$



$$P(\mathbf{m}|q_N) = \frac{P(q_N|\mathbf{m})P(\mathbf{m})}{P(q_N)}$$

$$P(q_N) = \int P(q_N|\mathbf{m})P(\mathbf{m})d\mathbf{m}$$

$$\mathbf{m}_e = \int \mathbf{m}P(\mathbf{m} \mid q_N)d\mathbf{m}$$

$$\cos\alpha_e = \frac{N}{N+2}q_N$$

A first estimate

$$\mathbf{m}_e = \cos\alpha_e\ \mathbf{x} + \cos\beta_e\ \mathbf{y} + \cos\gamma_e\ \mathbf{z}$$

However the vector is not normalized:

$$\cos^2\alpha_e + \cos^2\beta_e + \cos^2\gamma_e \neq 1$$

$$Pr(inadmissible) < (\frac{N}{N+2})^2(\frac{2}{3} + \frac{4}{3N})$$

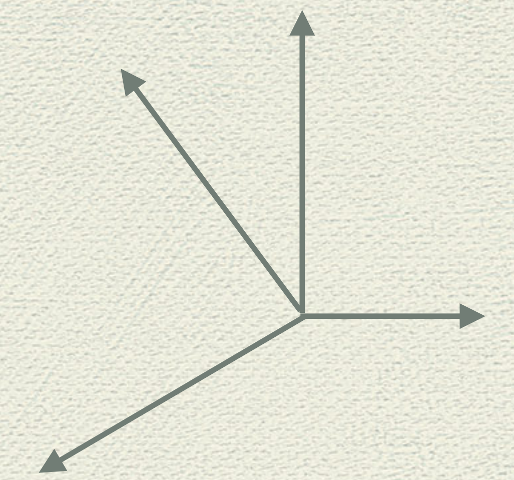
A rough estimate

$$Pr(inadmissible) < \frac{2}{3}$$

Exact calculation

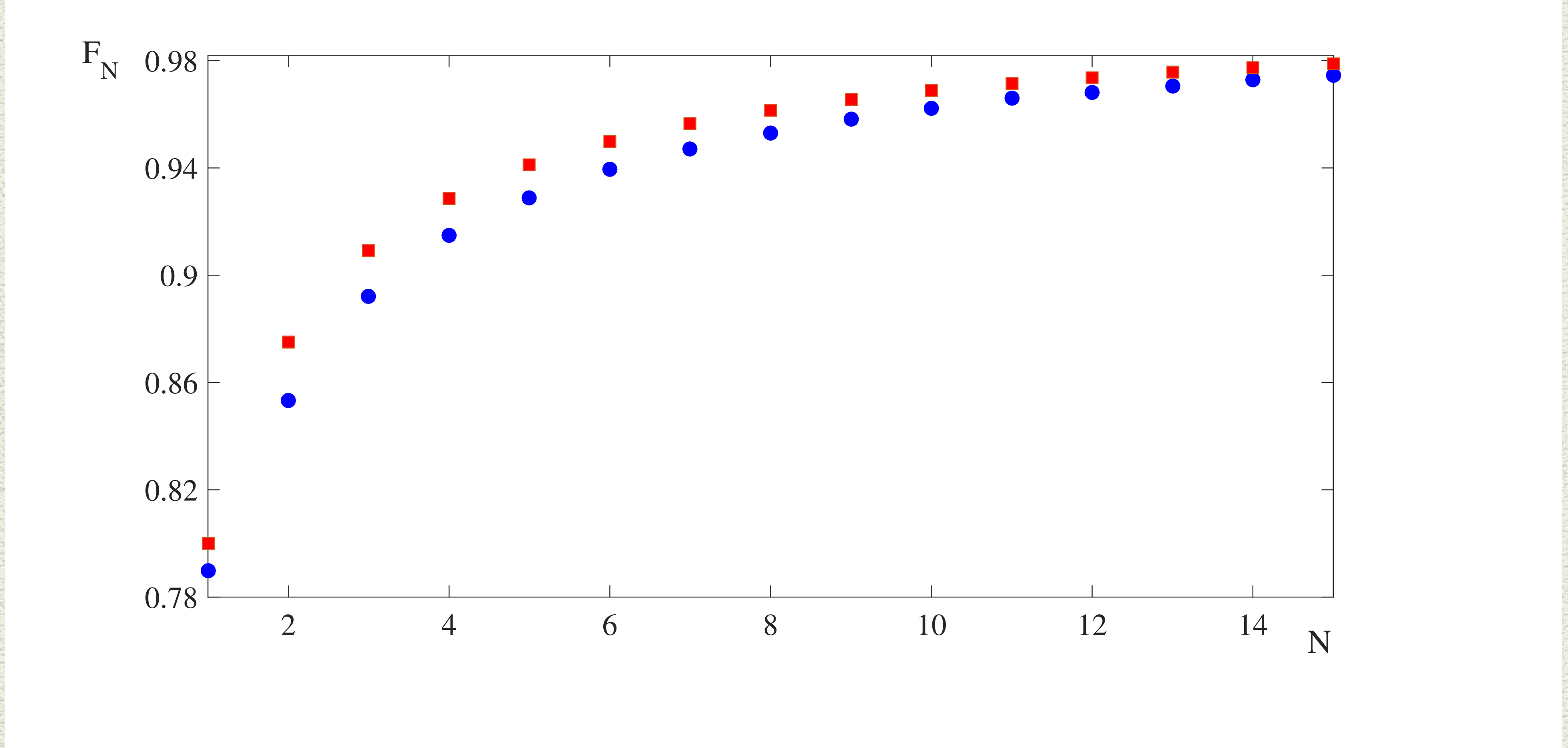
$$Pr(inadmissible) \approx \frac{1}{3}$$

A good estimate with three measurements



$$\mathbf{m}_e = \frac{1}{\sqrt{q_x^2 + q_y^2 + q_z^2}} (q_x\mathbf{x} + q_y\mathbf{y} + q_z\mathbf{z})$$

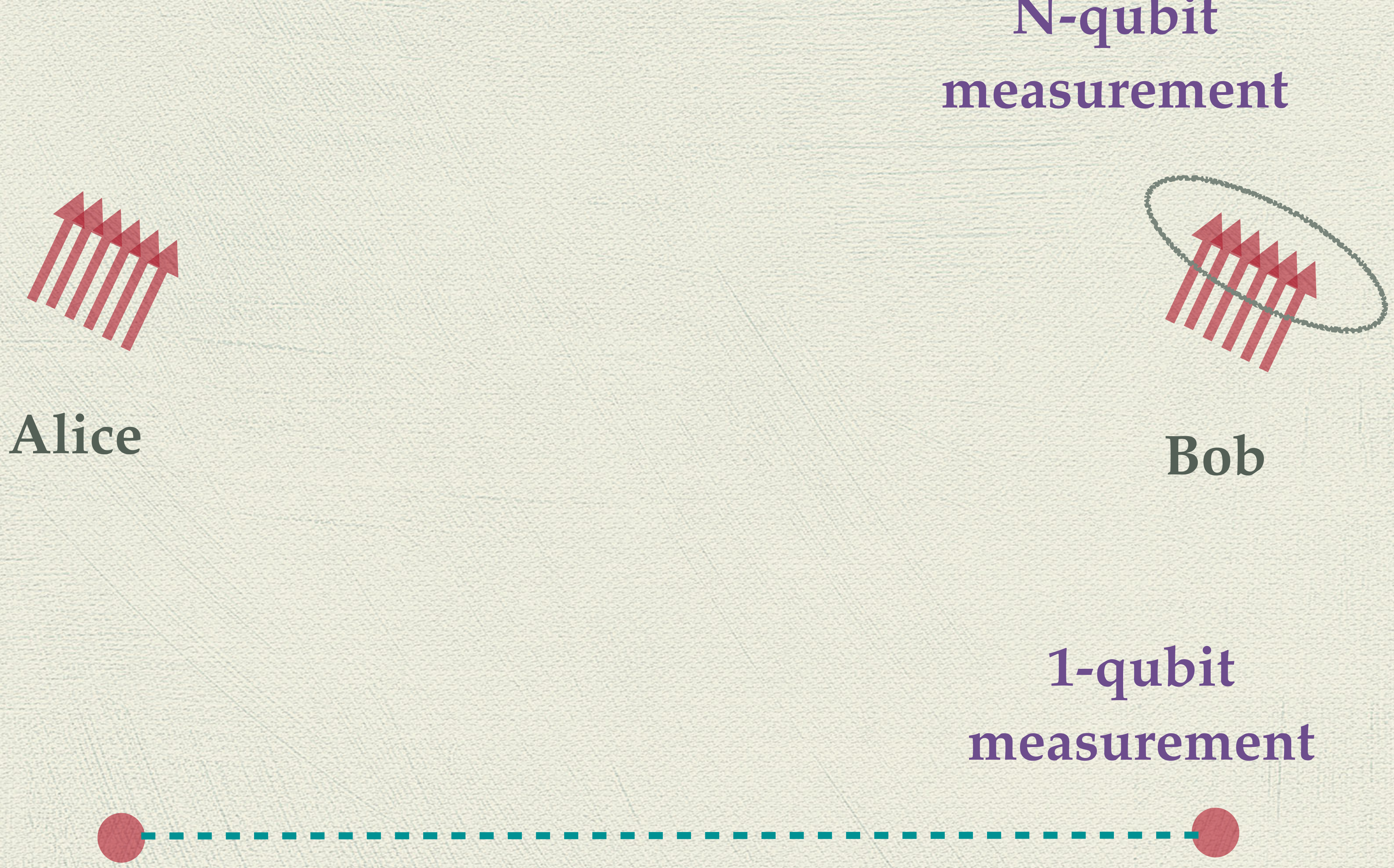
Comparison with previous methods



- Our method
- Other methods

$$\overline{F}_N = \frac{3N+1}{3N+2}$$

Advantages of our method-1



2- The problem of security

Eve cannot unravel the shared direction, since only

unspeakable

information is being communicated.

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

Thank you for your attention