(1)

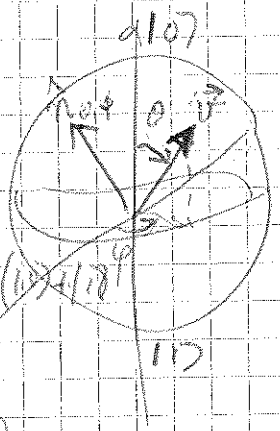
new cryptography

QIT

- Kinematics of entanglement - correlations
- teleportation
- remote state preparation
- entanglement concentration
- entanglement distillation
- entanglement cost
- additivity theorem — 10 yrs. of work by mathematicians

Kinematics

2-level system (qubit) however simplified on the Bloch sphere



$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle$$

overall phase irrelevant

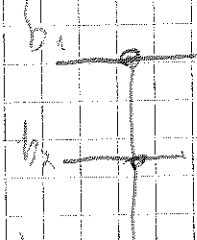
- ordinary
- rotations + unitary evolution of $|\psi\rangle$
- measure along axis $\hat{n}, -\hat{n}$:

$p_{up} = |\hat{n}_{\theta,\varphi}\cdot\vec{v}|^2$ — measure "up" with

$p_{down} = 1 - p_{up}$ — measure down

(b) quantum gate

Toffoli gate



"flip b_3 if b_1 & b_2"

quantum

$|a_1 a_2\rangle \to |a_1 a_2\rangle$

$|0,0\rangle \to |0,0\rangle$

$\vdots$

$|1,0\rangle \to |1,0\rangle$

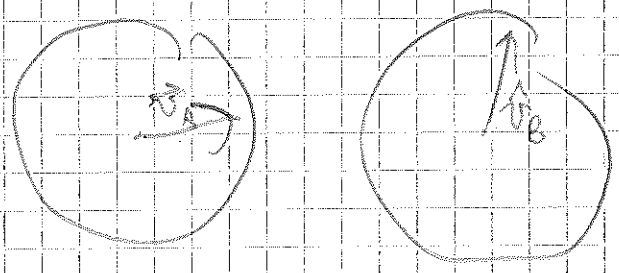
$|1,1\rangle \to |1,0\rangle$

all classical computation

quantum computation

exponentially more efficient for cryptanalysis

(3) back to thermodynamics

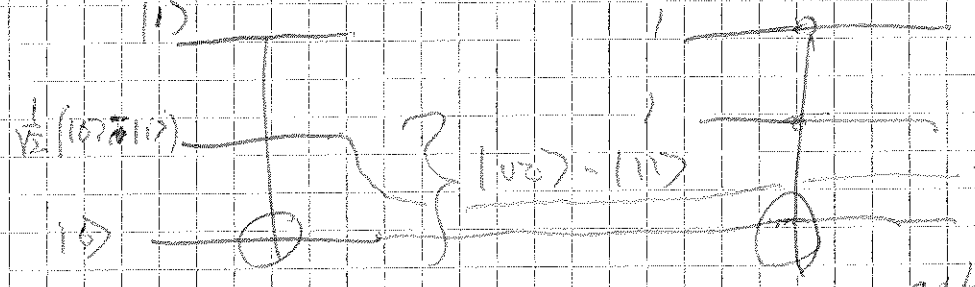


unentangled state of 2 qubits

$(\alpha|0\rangle+\beta|1\rangle)\otimes(\gamma|0\rangle+\delta|1\rangle)$ → 4 terms

other possible state

$\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)$ "spin singlet"



actually

$|+\rangle(\frac{1}{\sqrt{2}}|0\rangle-|1\rangle)$

Algebraic truth:

A measures $n_{\theta,\phi}$

B measures $n_{\theta,\pi}$

$\forall\ \theta,\Phi$, results are
- random
- opposite

— no trace of this randomness but spin to elsewhere in the world.

entire $\xi_{ABC}=\frac{1}{2}|100\rangle\times\langle 001|+\frac{1}{2}|111\rangle\times\langle 111|$

could come from

$\psi_{ABC}=\frac{1}{\sqrt{2}}(|100\rangle+|111\rangle)$ → E knows everything

(27) So, shared entanglement is an important primitive.

How do A & B get it?

more generally, A has state $\sum_i |\psi_{A_1 i}, \psi_{A_2 i}\rangle$

wants to "move particle 2 to B", so that finally $\sum_i |\psi_{A_1 i}, \psi_{B i}\rangle$

— teleportation

— carry particle

— suppose the "way is blocked"

Fig. 1

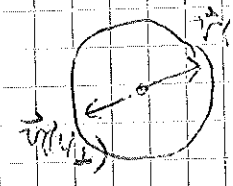
- distribute $|\beta_{00}\rangle$ before
- define $\hat{H}$ on Bloch sphere

etc.

remote state preparation

— setting ↑ knowledge of α & β.

NB $|0\rangle - |1\rangle = |\psi, \psi_\perp\rangle - |\psi_\perp, \psi\rangle$



A measures $\hat{H}_{\oplus, \ominus}$

↓ she gets $|\psi\rangle$, B has $|\psi\rangle$ — done!

otherwise, failure (why?)

(5) what to do?

suppose N states $(\alpha_1, \beta_1), (\alpha_2, \beta_2) \ldots (\alpha_N, \beta_N)$ are to be sent.

Lots of $|0\rangle$-$|1\rangle$ states

A → B message – successful column

takes ~ $N \log N$ bits,

1 bit per RSP!

– entanglement recovery.

none

supposed to have $|\Psi\rangle$, $\rho = |\Psi\rangle\langle\Psi|$

actually have $\rho = (1-p)|\Psi\rangle\langle\Psi| + p|\Psi_\perp\rangle\langle\Psi_\perp|$

(depolarizing noise) $p = \frac{1}{2} \Rightarrow 100\%$ noise

$\rho = (1-p')|\Psi\rangle\langle\Psi| + p'\rho_{mix}$

(6) A & B shared 1 bit

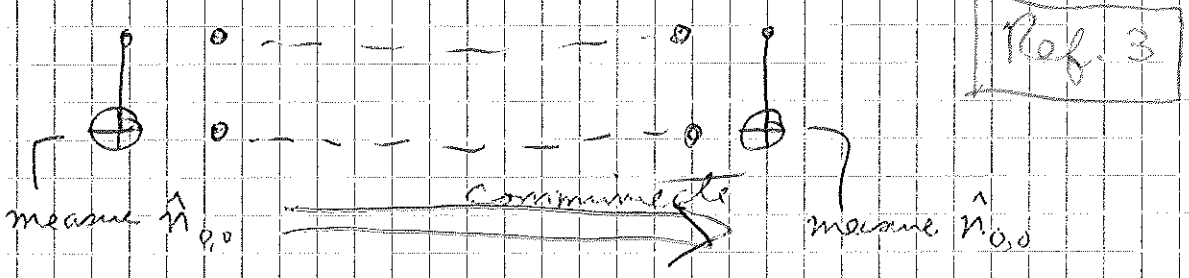
$\rho^{\otimes 2} |\beta_{00}\rangle\langle\beta_{00}|$

actually

$\rho = (1-p') |\beta_{00}\rangle\langle\beta_{00}| + p' \rho_{mix}$

$\rho^{\otimes N}$ many copies

what to do? Distill!

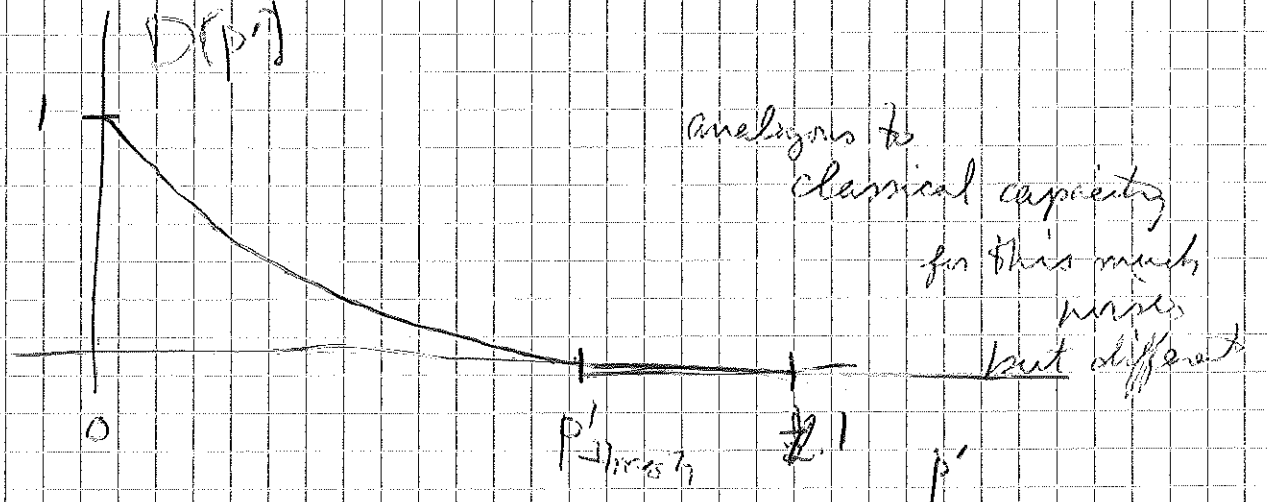


- for $p' = 0$ always agree

$p' \neq 0$ sometimes agree, but if agree p' is increased.

There's a $p'_{threshold}$ below which distillation works.

how much $|\beta_{00}\rangle$ do we get?



Simple bound on D proposed, disproved after ~10 yrs of work.