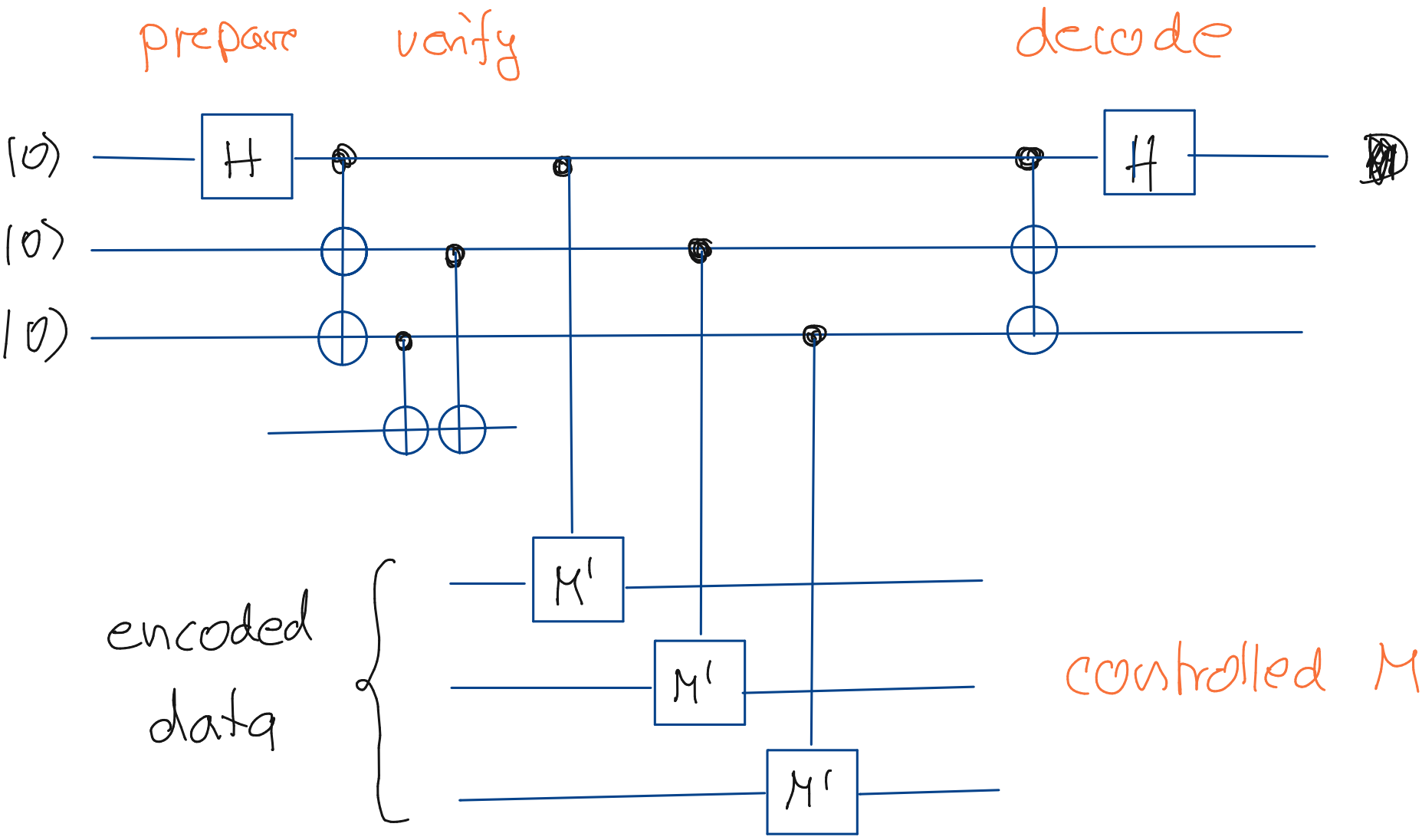
With this we can make the whole measurement circuit fault tolerant



V. Quantum communication

5.1 Classical information transfer, Shannon's theorems

We have already discussed that information is a measure of the a-priori ignorance about an event. A quantitative measure of information about a complete set of events A_i $i = 1, 2.., n$ which occur with

probability

$$0 \leq p(A_i) \leq 1 \qquad \sum_{i=1}^{n} p(A_i) = 1$$

should obey the following properties

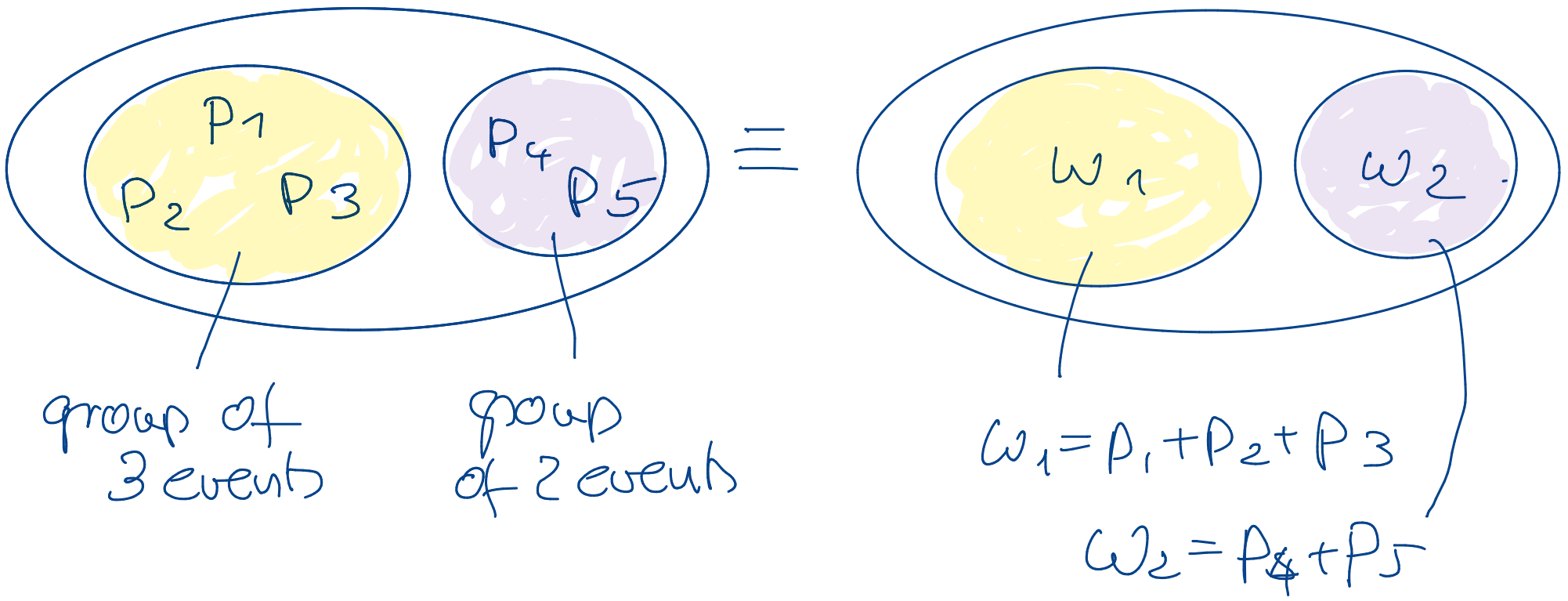
(i) S is continuous function of probabilities

$$S = S(p_1, p_2, \dots, p_n)$$

(ii) $S = 0$ for a certain event (i.e. $p_j = 1$ others 0)

(iii) $S = \max$ for maximum ignorance $p_j \equiv 1/n$ and monotonously increasing with n in this case

(iv) S should obey composition rule such that it behaves as extensive quantity



(256)
$$S(p_1 \cdots p_5) = S(\omega_1 + \omega_2) + \omega_1 S\left(\frac{p_1}{\omega_1}, \frac{p_2}{\omega_1}, \frac{p_3}{\omega_1}\right) + \omega_2 S\left(\frac{p_4}{\omega_2}, \frac{p_5}{\omega_2}\right)$$

Shannon entropy

(257) $$S(p_1, p_2, \dots, p_n) = -a \sum_{j=1}^{n} p_j \ln p_j \qquad a > 0$$

a arbitrary constant: often $a = 1/\ln 2$

$\longrightarrow a \ln p_j \longrightarrow \log_2 p_j$

c-bit

(258) $$H(p) = -p \log p - (1-p) \log(1-p) = S(p, 1-p)$$

Shannon's noiseless coding theorem

to transfer an n-bit word it is sufficient in the limit $n \to \infty$ $n H(p)$ bit where p is the probability of a "0" (or a "1", note $H(p) = H(1-p)$)

there is a unique code containing $1 + nH(p)$ bit.

$\Rightarrow$ classical data compression

example:

(spaces for better reading)

0000 0001 0100 0101 0000 0110 0100 1000 0000 0011
1000 0101 1100 0001 0100 0010 0000 0101 0001 0110
0110 0001 0100 1100 0000 0001 0100 0101 0000 0101
1001 0100 0010 0000 0101 0001 0000 0011 0001 0100
0100 1100 0001 0000 0011 0001 1100 0100 0100 0010
0100 0101 0000 0101 0100 0010 0000 0101 0001 0100
1000 0101 1100 1101 0100 0010 0000 0101 0001 0100
0000 0101 0001 0100 1000 0101 1100 0001 1100 1000

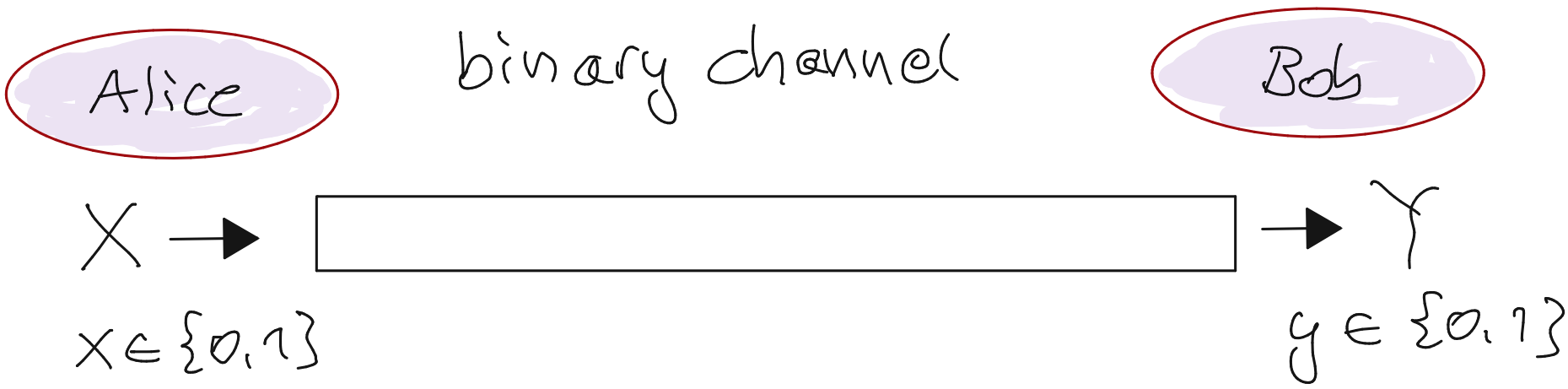
$$p(0) = \frac{225}{320} = 0{,}705 > p(1) = \frac{95}{320} = 0.297$$

code:

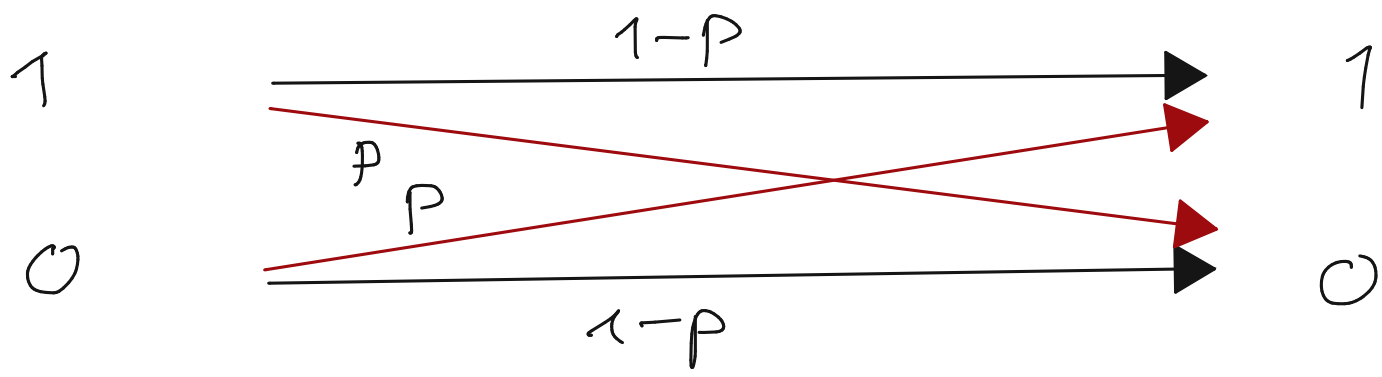
obviously shorter!

10 000 010 1001 10 1010 010 011 10 1000
011 1001 1101 000 010 001 10 1001 000 1010
1010 000 010 1101 10 000 010 1001 10 1001
1011 010 001 10 1001 000 10 1000 000 010
010 1101 000 10 1000 000 1101 010 010 001
010 1001 10 1001 010 001 10 1001 000 010
011 1001 1101 11110 010 001 10 1001 000 010
10 1001 000 010 011 1001 1101 000 1101 011

communication channel



Symmetric binary channel:



mutual information

How much information about input X is in output Y?

$$I(X:Y) \equiv S(X) - S(X|Y) \tag{259}$$

where the conditional entropy reads

$$S(X|Y) = -\sum_j p(x_j) \sum_e p(y_e|x_j) \log p(y_e|x_j) \tag{260}$$

- $p(y|x)$ is conditional probability of y if x is true
- joint probabiity

(261) $$p(x,y) = p(y,x) = p(x|y)p(y) = p(y|x)p(x)$$

If x and y are independent

(262) $$p(y|x) = p(y) \qquad p(y,x) = p(y)p(x)$$

$\Rightarrow$

(263) $$I(X:Y) = \sum_{x,y} p(x,y) \log \frac{p(x,y)}{p(x)p(y)}$$

I.e. if x and y independent random variables

(264) $$I(X:Y) = 0 \quad \text{and} \quad S(X|Y) = S(X)$$

For a binary symmetic channel holds

(265) $$\boxed{I(X:Y) = H(p(y)) - H(p_{error})}$$

Def: channel capacity

(266) $$C \equiv \max_{p(x)} I(X:Y)$$

X : input
Y : output

binary symmetic channel

(267) $$\boxed{C = 1 - H(p_{error})} \qquad 0 \leq C \leq 1$$

Shannon's noisy coding theorem

For any binary channel with capacity C there is a code that allows a data transfer with arbitrary small error probability and transfer rate R

$$0 < R = \frac{\#\text{bit in message}}{\#\text{bit in code}} < C$$

5.2 Quantum information transfer

(A) Direct transfer of quantum information

If we have a (classical) random variable X that takes on the values x_j with probability p_j the information in the measurement of X is Shannon's entropy

(268) $$S_{sh} = -\sum_j p_j \ln p_j$$

Consider now orthogonal quantum states

(269) $$x_j \longrightarrow |x_j\rangle \qquad \langle x_e | x_j \rangle = \delta_{ej}$$

with probability p_j, then

$$\hat{\rho} = \sum_j p_j |x_j\rangle\langle x_j| \tag{270}$$

So eq. (268) can be written as

$$S_{SH} = -Tr\{\rho \ln \rho\} = S_{VN} \tag{271}$$

is the von Neumann entropy. We now use S_{VN} also as a measure of information contained in a quantum state (with $\ln \to \log_2 = \log$)

$$S_{VN} = -Tr\{\vec{\rho} \log \vec{\rho}\} \tag{272}$$

Schumacher theorem

A message of n letters each being a pure state $|\psi(x)\rangle$ with probability $p(x)$, i.e. $\rho = \sum_x p(x) |\psi(x)\rangle\langle\psi(x)|$ requires for storage a Hilbert space $\mathcal{H}_0$ with $\dim(\mathcal{H}_0) = 2^{n S_{VN}(\rho)}$

the generalization to mixed states is less trivial
→ Holevo conjecture

The transfer of qubits through a noisy channel can be realized using quantum error correction
=> Section IV

(B) Entanglement transfer over noisy channels (long distances):

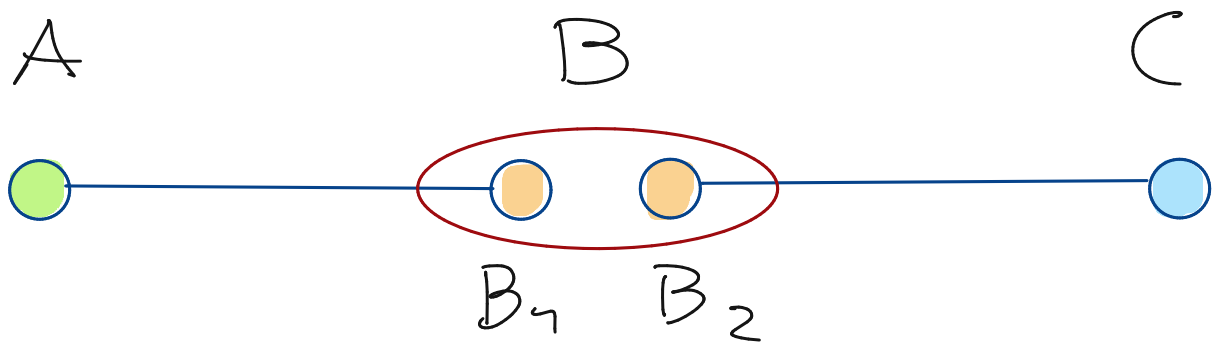
A much more elegant way to transfer a quantum state over noisy channels / long distances is to use quantum teleportation.

To this end we use two elements: entanglement swapping to connect two pairs of entangled qubits separated each by a distance L to a single pair at distance 2L. The second element is entanglement parification

- entanglement swapping

C.H. Bennett et al. PRL 70, 1895 (1993)
M. Zukowski et al. PRL 71, 4287 (1993)

problem: create entangled state between A and C out of entangled pairs A-B and B-C



Bell states (orthogonal)

(273)
$$|\phi_+\rangle \sim |00\rangle + |11\rangle \qquad |\psi_+\rangle \sim |10\rangle + |01\rangle$$
$$|\phi_-\rangle \sim |00\rangle - |11\rangle \qquad |\psi_-\rangle \sim |10\rangle - |01\rangle$$

Assume A-B_1 and B_2-C are entangled in Bell state ϕ_+

$$|\psi\rangle = |\phi_+\rangle_{AB_1} |\phi_+\rangle_{B_2C}$$
$$= \frac{1}{2}\left(|0\rangle_A|0\rangle_{B_1} + |1\rangle_A|1\rangle_{B_1}\right)\left(|0\rangle_{B_2}|0\rangle_C + |1\rangle_{B_2}|1\rangle_C\right)$$

(274)
$$= \frac{1}{2\sqrt{2}}\Big\{|0\rangle_A\underbrace{\left[|\phi_+\rangle + |\phi_-\rangle\right]}_{B_1B_2}|0\rangle_C + |0\rangle_A\underbrace{\left[|\psi_+\rangle + |\psi_-\rangle\right]}_{B_1B_2}|1\rangle_C$$
$$+ |1\rangle_A\underbrace{\left[|\psi_+\rangle - |\psi_-\rangle\right]}_{B_1B_2}|0\rangle_C + |1\rangle_A\underbrace{\left[|\phi_+\rangle - |\phi_-\rangle\right]}_{B_1B_2}|1\rangle_C\Big\}$$

$$= \frac{1}{2}\Big\{|\phi_+\rangle_{AC}|\phi_+\rangle_{B_1B_2} + |\phi_-\rangle_{AC}|\phi_-\rangle_{B_1B_2}$$
$$+ |\psi_+\rangle_{AC}|\psi_+\rangle_{B_1B_2} + |\psi_-\rangle_{AC}|\psi_-\rangle_{B_1B_2}\Big\}$$

Bell measurement of B_1 and B_2 projects to one of the 4 Bell states between A and C

$$|\phi_+\rangle_{AC} \quad |\phi_-\rangle_{AC} \quad |\psi_+\rangle_{AC} \quad |\psi_-\rangle_{AC}$$

01.02. ⟶

- **entanglement purification**

D. Deutsch et al. PRA 54, 3824 (1996)
convergence proof: Macchiavello PLA 246, 385 (1998)

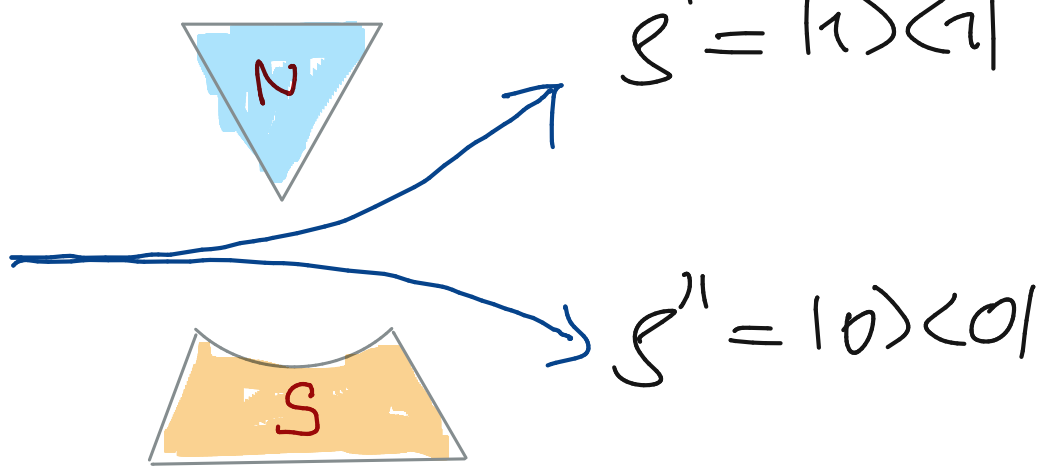
(i) idea: destillation of pure states of single qubits
(later generalization to pairs)

(275) $\varrho_0 = f\,|0\rangle\langle 0| + (1-f)\,|1\rangle\langle 1|$

mixed state in $|0\rangle$ and $|1\rangle$. In principle a simple measurement will select subensembles in pure states

e.g.: Stern Gerlach magnet

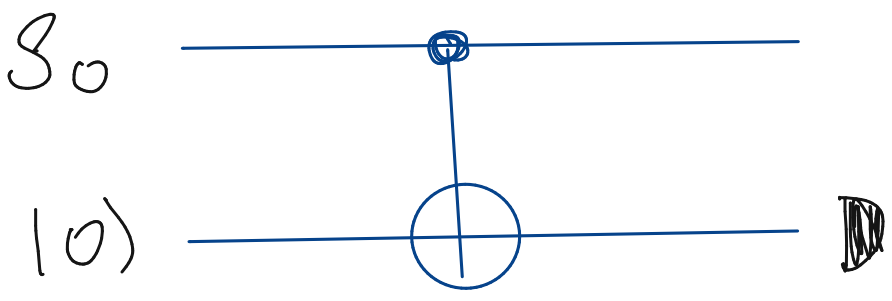
So



Can we do destillation without measurement of the qubit itself? ⟶ ancilla qubit

(276) $\varrho_0 \longrightarrow \varrho_0 \otimes |0\rangle_{AA}\langle 0|$

CNOT

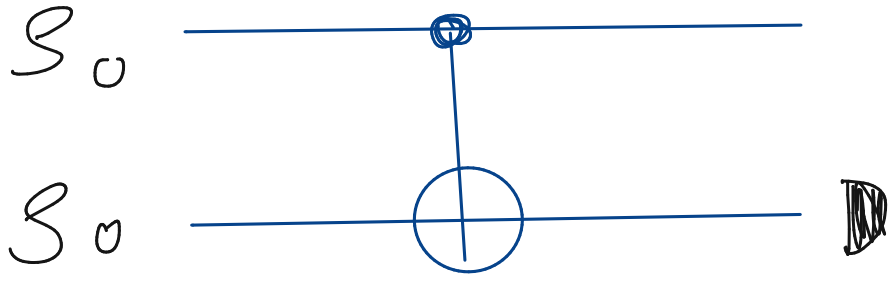


$f\,|0\rangle\langle 0|\,|0\rangle_{AA}\langle 0|$
$+(1-f)\,|1\rangle\langle 1|\,|1\rangle_{AA}\langle 1|$

measurement of ancilla projects to pure states $|0\rangle\langle 0|$ or $|1\rangle\langle 1|$, but we used a pure state (in ancilla channel) in the first place, so this is cheating! ☹

But we can purify ρ_0 with a second qubit in the same mixed state ρ_0:

$\rho_{AB} = \rho_0 \otimes \rho_0$



ρ'_{AB}

$$\rho_{AB} = \rho_0 \cdot \rho_0 =$$

$$= \left(f|0\rangle\langle 0| + (1-f)|1\rangle\langle 1|\right)\left(f|0\rangle\langle 0| + (1-f)|1\rangle\langle 1|\right)$$

CNOT

$\Rightarrow$

$$\rho'_{AB} = \underbrace{\left(f^2|0\rangle\langle 0| + (1-f)^2|1\rangle\langle 1|\right)}_{A}\underbrace{|0\rangle\langle 0|}_{B} + f(1-f)\underbrace{\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right)}_{A}\underbrace{|1\rangle\langle 1|}_{B} \quad (277)$$

totally mixed state

Measurement of B qubit and projection to "$|0\rangle$" yields

$$\rho_A' = \frac{f^2 |0\rangle\langle 0| + (1-f)^2 |1\rangle\langle 1|}{f^2 + (1-f)^2} \tag{278}$$

$$= f' |0\rangle\langle 0| + (1-f') |1\rangle\langle 1|$$

i.e.

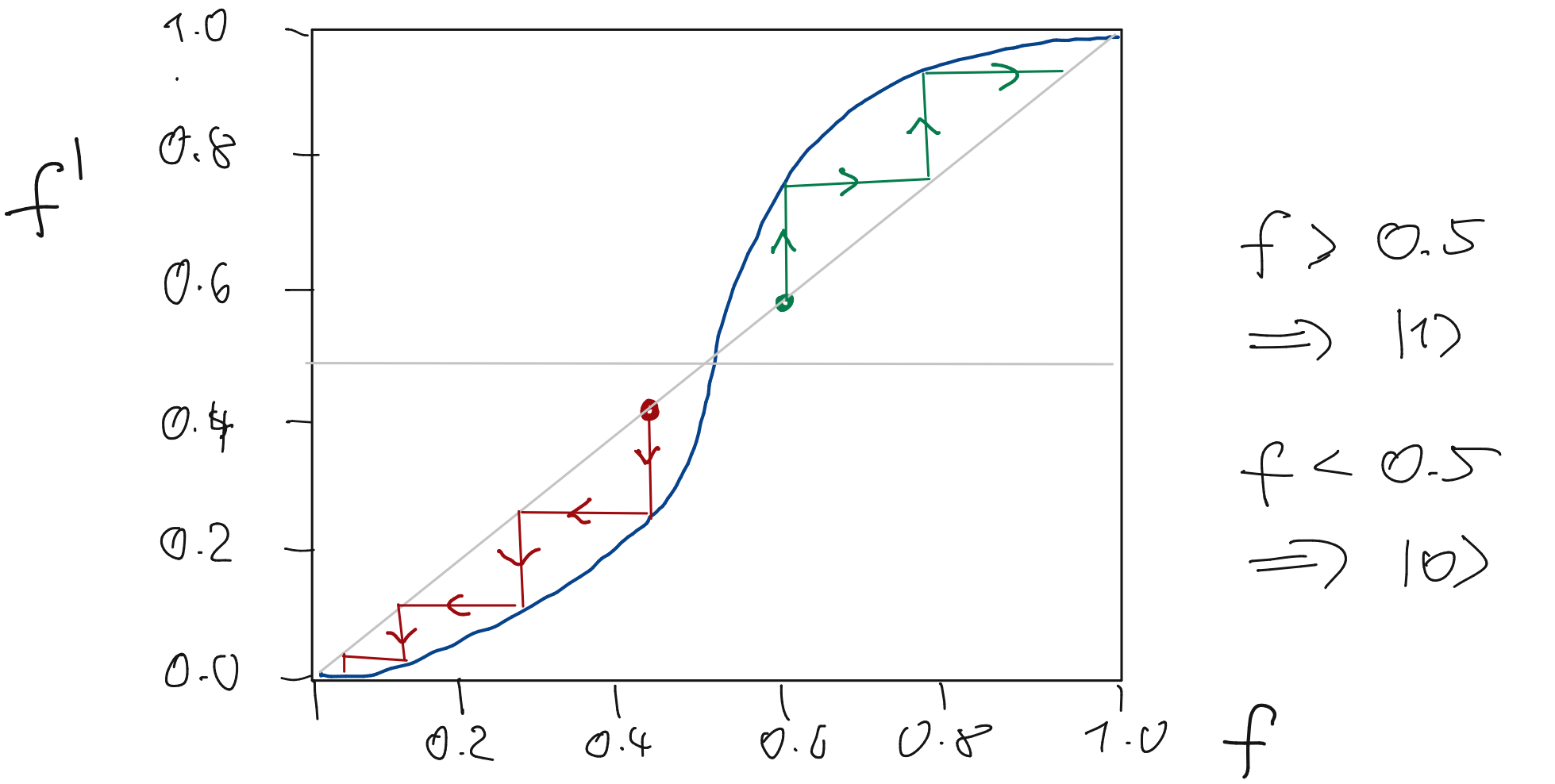
$$f' = \frac{f^2}{f^2 + (1-f)^2} \tag{279}$$

$$(1-f') = \frac{(1-f)^2}{f^2 + (1-f)^2}$$

iteration of the procedure and rejecting "$|1\rangle$"s

$$\left.\begin{array}{l} \rho \\ \rho \\ \rho \\ \rho \\ \rho \\ \rho \\ \rho \end{array}\right\} \begin{array}{l} \rho' \\ \rho' \\ \rho' \\ \rho' \\ \rho' \end{array} \left.\begin{array}{l} \\ \\ \\ \rho'' \\ \rho'' \end{array}\right\} \rho''' \quad \text{etc.}$$

gives increasing fidelity at the expense of particles



(ii) entanglement purification

C. Bennett et al. Phys. Rev. Lett. 76, 722 (1996)

Consider an ensemble of pairs in mixed state.
Use Bell basis

$$\{|\Phi_+\rangle, |\Phi_-\rangle, |\Psi_+\rangle, |\Psi_-\rangle\}$$

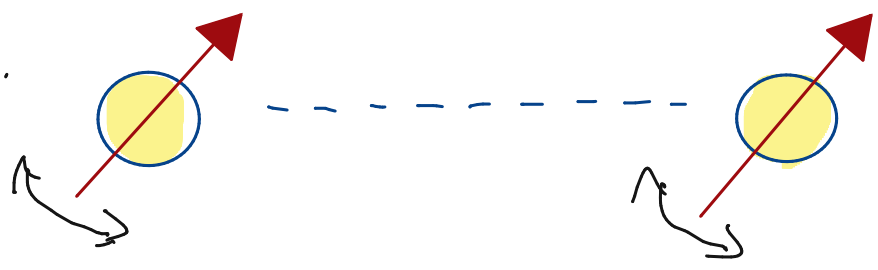
Let us assume that the ensemble of pairs is with probability F in Bell state

$$|\Psi_-\rangle \sim |10\rangle - |01\rangle$$

with is the spin Singlet state $S=0$ and probabilty $(1-F)$ in the totally mixed state of all other Bell states

$$(280) \qquad \mathcal{S} = F\,|\Psi_-\rangle\langle\Psi_-| + \frac{1-F}{3}\left(\mathbb{1} - |\Psi_-\rangle\langle\Psi_-|\right)$$

The total mixture of the spin triplet states $S=1$ can be achieved e.g. by random bilateral rotations of both spins in the pairs



random common magnetic field

This leaves the singlet state $|\Psi_-\rangle$ untouched.

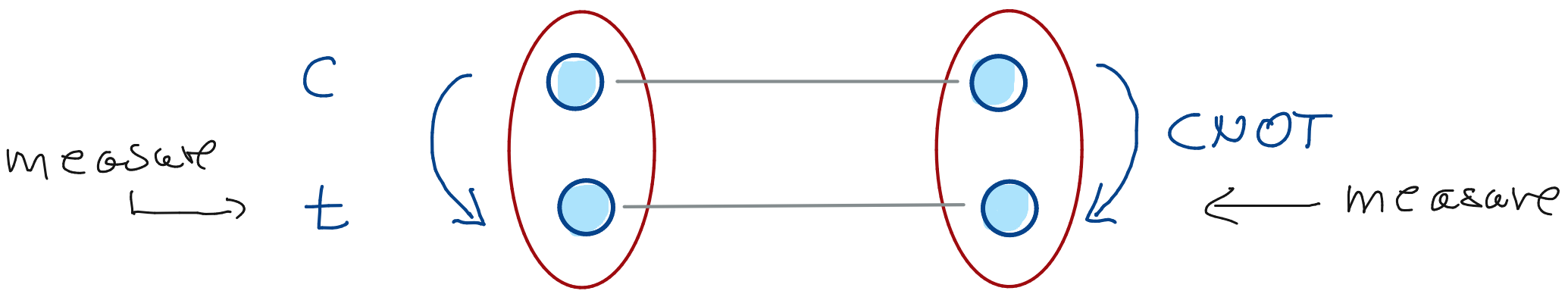
protocol Assume $\boxed{F > \frac{1}{2}}$

(i) σ_y rotation on one of the two spins in each pair

(287) $$\sigma_y^{(1)} |\Psi_\pm\rangle \longrightarrow |\Phi_\mp\rangle$$

i.e.
$$\rho = F\,|\Phi_+\rangle\langle\Phi_+| + \frac{(1-F)}{3}\left(\mathbb{1} - |\Psi_+\rangle\langle\Psi_+|\right)$$

(ii) bilateral CNOT on two pairs



- if target results are the same
  ⟹ keep control pair
- if target results differ
  ⟹ discard all

(iii) if control bits from (ii) are kept
⟹ rotate from $|\Phi_+\rangle$ back to $|\Psi_-\rangle$
Now we have a (smaller) ensemble of

pairs with probability F' in $|\Psi_-\rangle$ state. Applying random bilateral rotations as described above we arrive at

$$\rho' = F'|\Psi_-\rangle\langle\Psi_-| + \frac{1-F'}{3}\left(\mathbb{1} - |\Psi_-\rangle\langle\Psi_-|\right) \tag{282}$$

and the procedure can be iterated.

To calculate the fidelity F' after one protocol step we consider probabilities in step (ii)

bilateral CNOT turns two pairs in Bell states into two pairs of Bell states, e.g.

$$\text{BCNOT}\ |\Psi_+\rangle|\Phi_-\rangle =$$

$$\text{BCNOT}\left[(|10\rangle+|01\rangle)(|00\rangle-|11\rangle)\right] = \tag{283}$$

$$\text{BCNOT}\left[|10\rangle|00\rangle - |10\rangle|11\rangle + |01\rangle|00\rangle - |01\rangle|11\rangle\right]$$

$$|10\rangle|10\rangle - |10\rangle|01\rangle + |01\rangle|01\rangle - |01\rangle|10\rangle$$

$$= |10\rangle(|10\rangle - |01\rangle) - |01\rangle(|10\rangle - |01\rangle)$$

$$= |\Psi_-\rangle|\Psi_-\rangle \qquad \text{etc.}$$

prob.	Control	Target		Control	Target
F^2	ϕ_+	ϕ_+		ϕ_+	ϕ_+
$F(1-F)/3$	ϕ_-	ϕ_+		ϕ_-	ϕ_+
$F(1-F)/3$	ψ_+	ϕ_+		ψ_+	ψ_+
$F(1-F)/3$	ψ_-	ϕ_+		ψ_-	ψ_+
$F(1-F)/3$	ϕ_+	ψ_+		ϕ_+	ψ_+
$(1-F)^2/9$	ϕ_-	ψ_+		ϕ_-	ψ_+
$(1-F)^2/9$	ψ_+	ψ_+		ψ_+	ϕ_+
$(1-F)^2/9$	ψ_-	ψ_+	→	ψ_-	ϕ_+
$F(1-F)/3$	ϕ_+	ϕ_-		ϕ_-	ϕ_-
$(1-F)^2/9$	ϕ_-	ϕ_-		ϕ_+	ϕ_-
$(1-F)^2/9$	ψ_+	ϕ_-		ψ_-	ψ_-
$(1-F)^2/9$	ψ_-	ϕ_-		ψ_+	ψ_-
$F(1-F)/3$	ϕ_+	ψ_-		ϕ_-	ψ_-
$(1-F)^2/9$	ϕ_-	ψ_-		ϕ_+	ψ_-
$(1-F)^2/9$	ψ_+	ψ_-		ψ_-	ϕ_-
$(1-F)^2/9$	ψ_-	ψ_-		ψ_+	ϕ_-

↑ keep $|\phi_+\rangle$

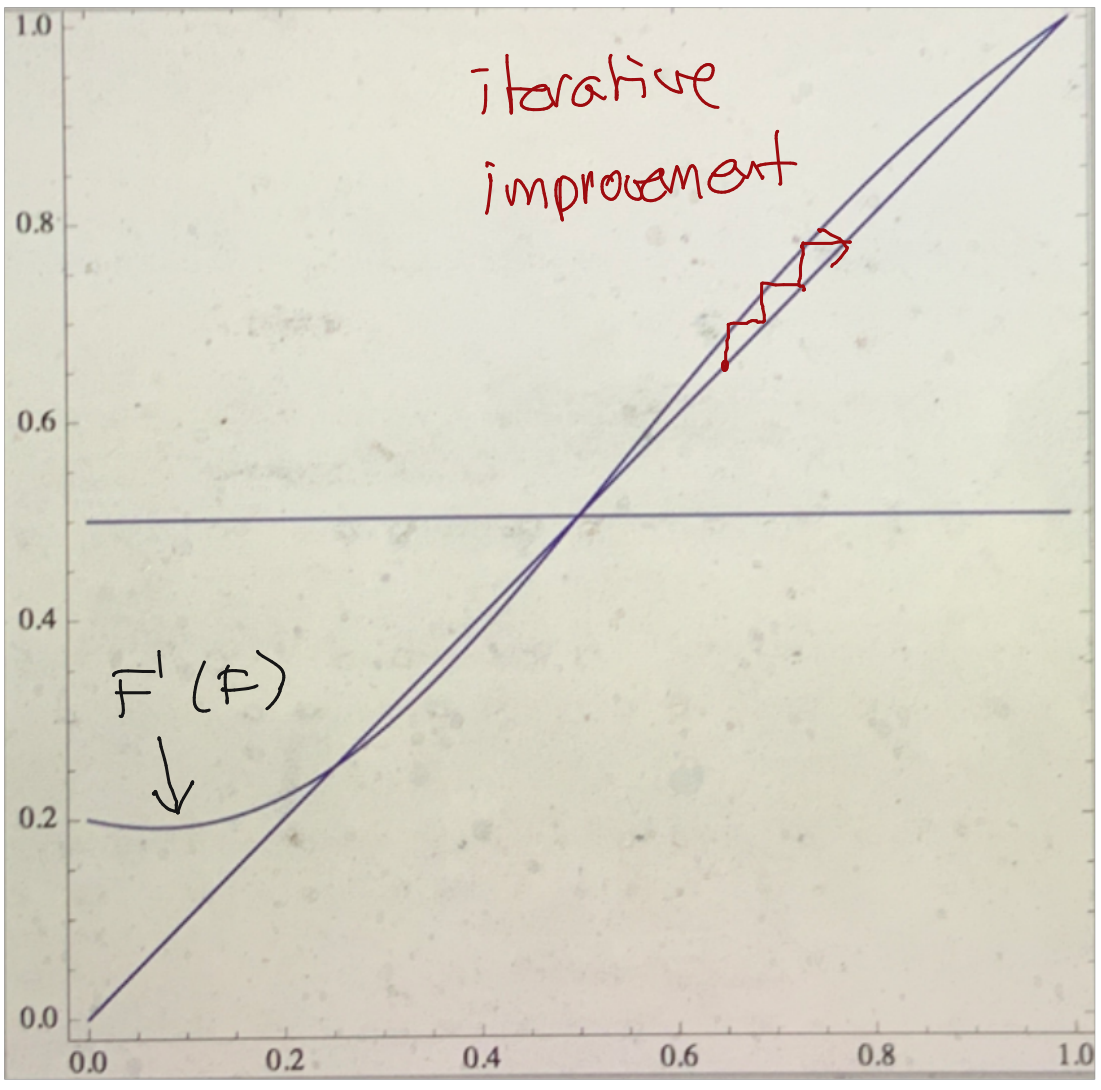
In the post-selected pairs the probability of finding the control pair in state $|\phi_+\rangle$ reads

(284)
$$F' = \frac{F^2 + \frac{1}{9}(1-F)^2}{F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2}$$

$F' > F$ for $\frac{1}{2} < F < 1$

out

F'

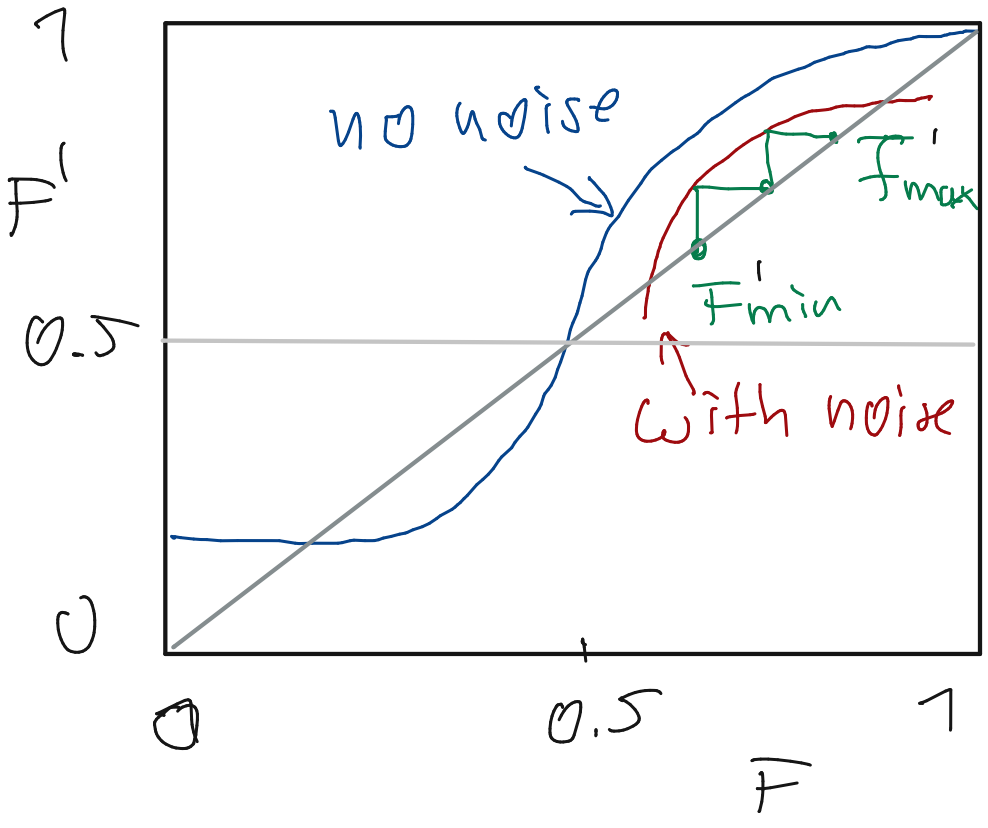


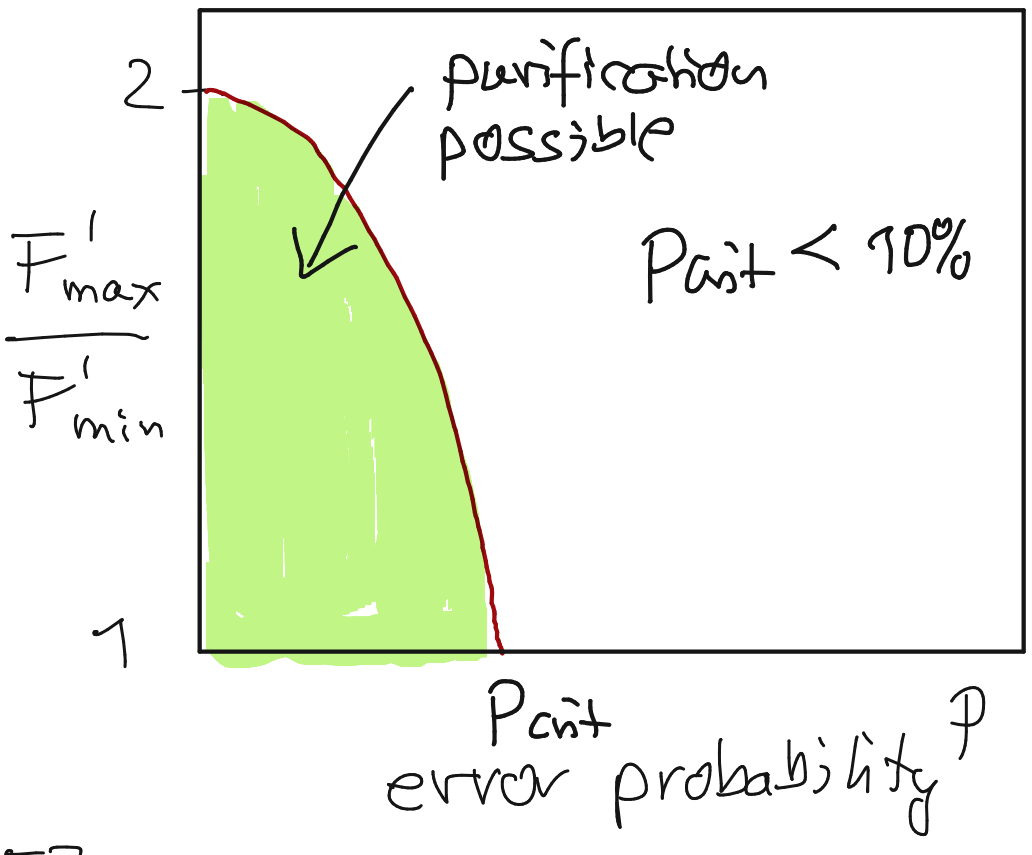
F in

Rem: this procedure is not optimized and there are improved algorithms

In the presense of noise

$$F_{min} > \frac{1}{2} \qquad F' \to F'_{max} < 1$$





(c) quantum repeater

In order to perform a teleportation over large distances one has to create entanglement over large distances.

problems: (i) sources of entangled particles employ (quasi) local interactions

(ii) decoherence probability increases exponentially with distance

$$p = 1 - e^{-\alpha l} \qquad F = e^{-\alpha l}$$

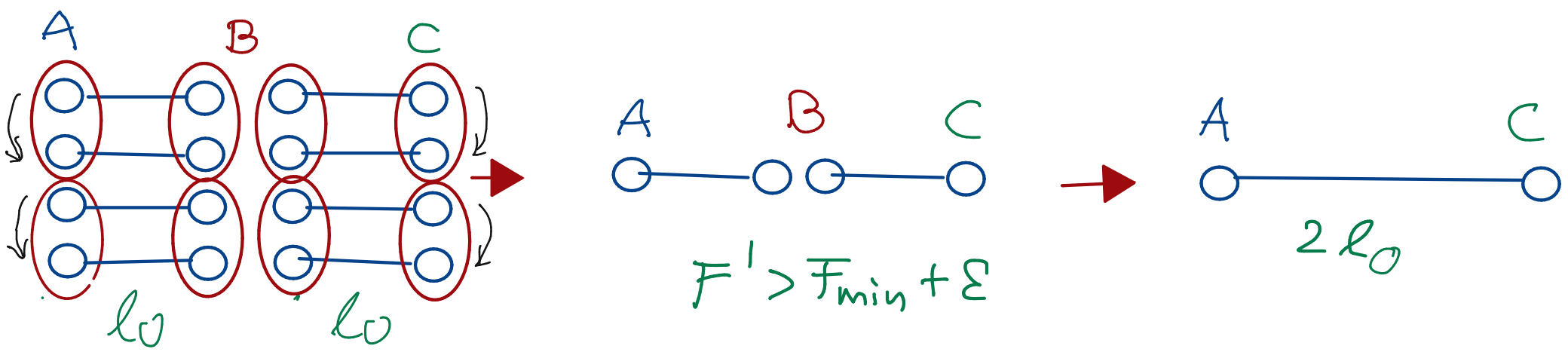
purification requires however minimum error probability

(285) $$F_{min} = e^{-\alpha l_{max}}$$

- classical solution: amplifiers; how to do this for quantum states?

quantum repeater

iterative entanglement purification and entanglement swapping $l_0 < l_{max}$



total distance

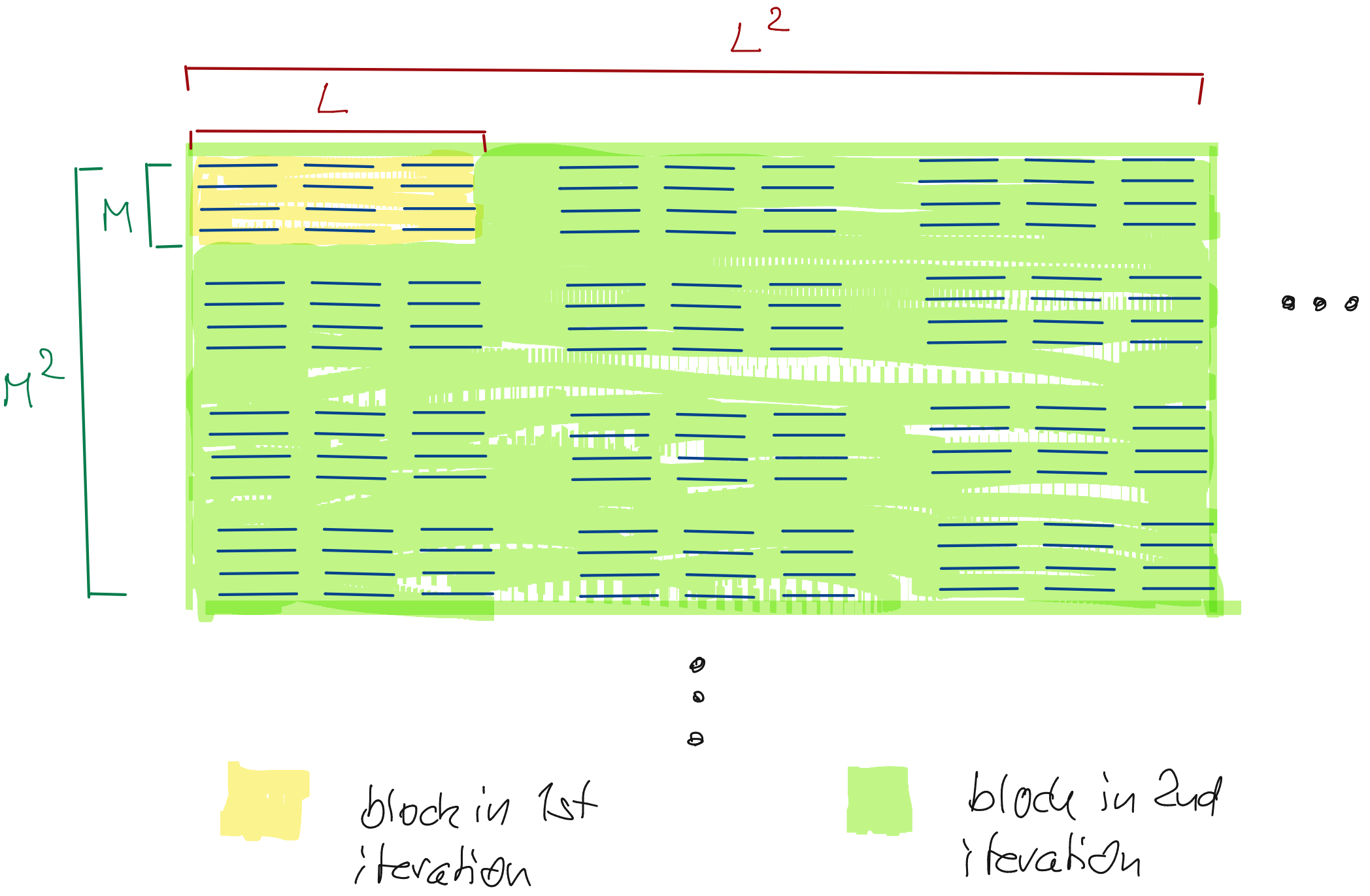
(286) $\ell = N \ell_0 \qquad \ell_0 < \ell_{max}$

but we require a protocol whose ressources do not scale exponentially with N!

→ sequentiell operation not good

→ concatenation of purification & swapping

H.-J. Briegel et al. PRL 81, 5932 (1998)
W. Dür et al PRA 59, 169 (1999)



set $N = L^n$

(i) blockwise connection of L segments

(ii) entanglement purification in every block
$\Rightarrow$ entangled pair of distance L
created from $M \cdot L$ pairs of length 1

(iii) iteration

- distance reached L^k after k iterations
- total number of elementary pairs to reach L^n

$$R = (ML)^n = L^n M^n = N L^{n \log_L M}$$

(287) $$\boxed{R = N^{\log_L M + 1}}$$

only polynomial in N !!

---

not covered:

- physical implementations
- quantum cryptography
- topological quantum computing

$\longrightarrow$ perhaps extra 2 hours on Kitaev's Toric code ?