ZK proofs

Classical proof idea:

Want $S(x,\rho) \approx \langle P, V \rangle^{(x,\rho)}_{(x,\rho)}$

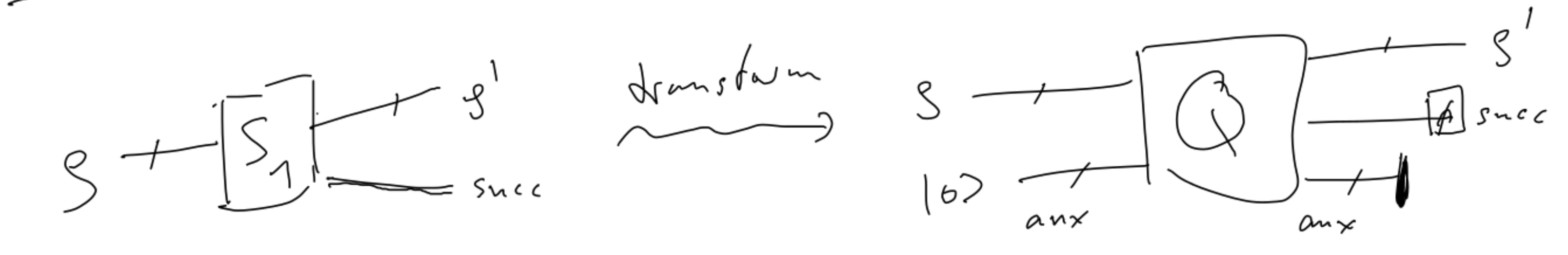
Managed: $S_1(x,\rho) \mid \neg abort = \langle P, V \rangle$ and $Pr[abort] = 1/2$ } also works in Q setting (practice)

Build S:

Run $S_1(x,\rho)$ ←
if $\neg$abort: return
else: restart ⌟

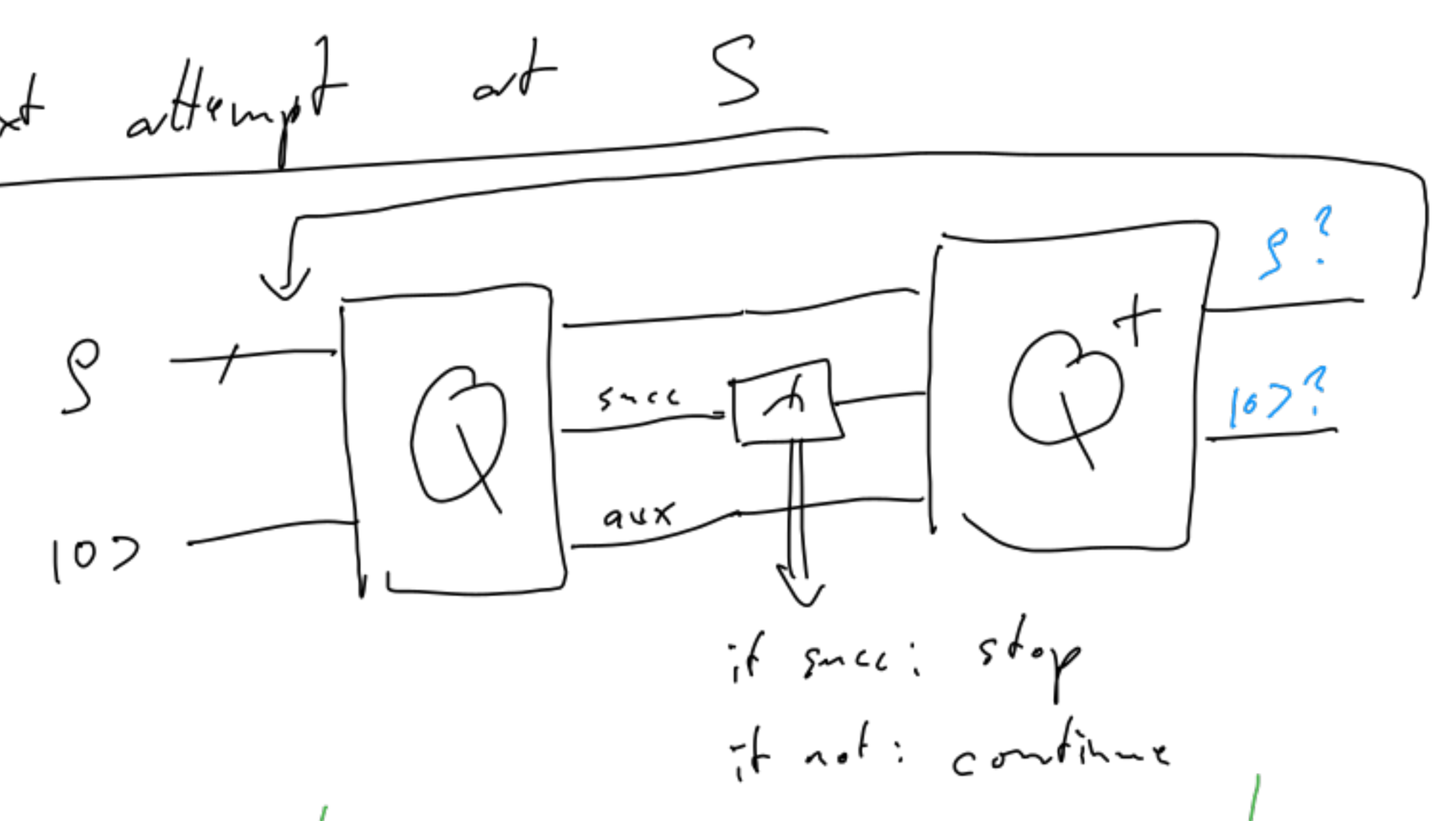
Problem: Cannot copy ρ to re-run S_1

First step Transform S_1 into unitary $S_1 = Q$



⟹ Instead of rewinding S_1, rewind Q

Next attempt at S



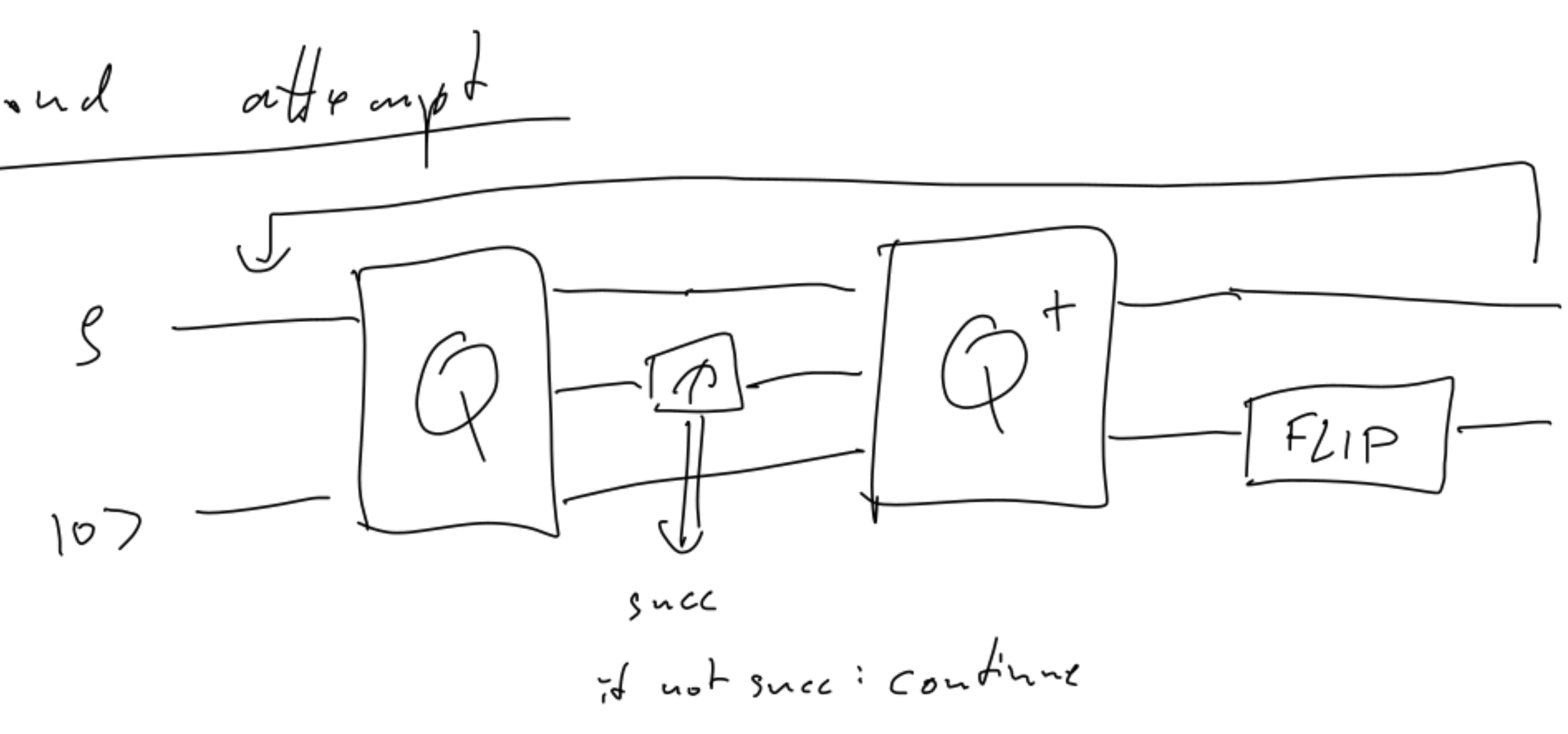
just a binary meas. in different basis

$P_Q = Q^+ \cdot (I \otimes |0\rangle\langle 0| \otimes I) Q$

Two problems:

- Q^+ might not give ρ back
- Second iteration has 0 success prob.

Second attempt



$FLIP\,|0\rangle \to |0\rangle$
$FLIP\,|x\rangle = -|x\rangle$
$(x \neq 0)$

This works: • Cond. on success (after ≤n iterations) we get ~~⟨P,V⟩~~ what Q outputs cond. on success

• $Pr[succ]$ high

Conditions – Q unitary
– $Pr[$succ in $|\psi\rangle|0\rangle \to Q \to$ meas$] = p$ for some $p \leq \frac{1}{2}$ indep of $|\psi\rangle$

Why does measuring success not disturb? (At least not ruinously)

Because $Pr[succ]$ indep. of init state, succ-measurement ~~the~~ does not measure info about init state ⟹ does not disturb (intuitively)

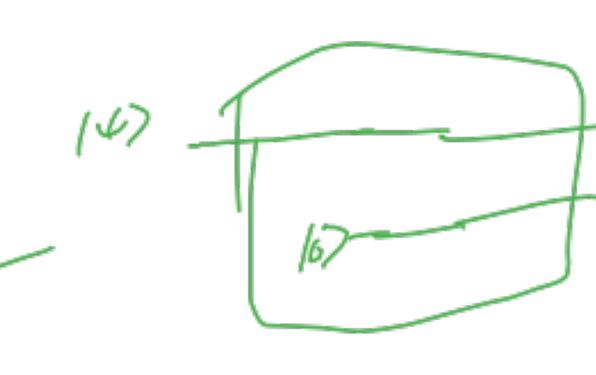
Say init. state is $\rho = |\psi\rangle\langle\psi|$

$$P_Q = Q^+ (I \otimes |0\rangle\langle 0| \otimes I) Q$$

$$\| P_Q (|\psi\rangle \otimes |0\rangle) \|^2 = 1-p \quad \forall |\psi\rangle$$

$$\| $$

$$(\langle\psi| \otimes \langle 0|)\, P_Q^+ \, P_Q \, (|\psi\rangle \otimes |0\rangle)$$



$$\|$$

$$\langle\psi| (I \otimes \langle 0|)\, P_Q\, (I \otimes |0\rangle) |\psi\rangle$$

P_Q^* { init aux $|0\rangle$, run Q, meas, Q^+, measure if aux = $|0\rangle$

$$\|$$

$\langle\psi| P_Q^* |\psi\rangle$ ⟹ $\langle\psi| P_Q^* |\psi\rangle = 1-p \quad \forall|\psi\rangle$

$\langle\psi| (1-p) I |\psi\rangle = 1-p$

$\Rightarrow P_Q^* = (1-p) I$

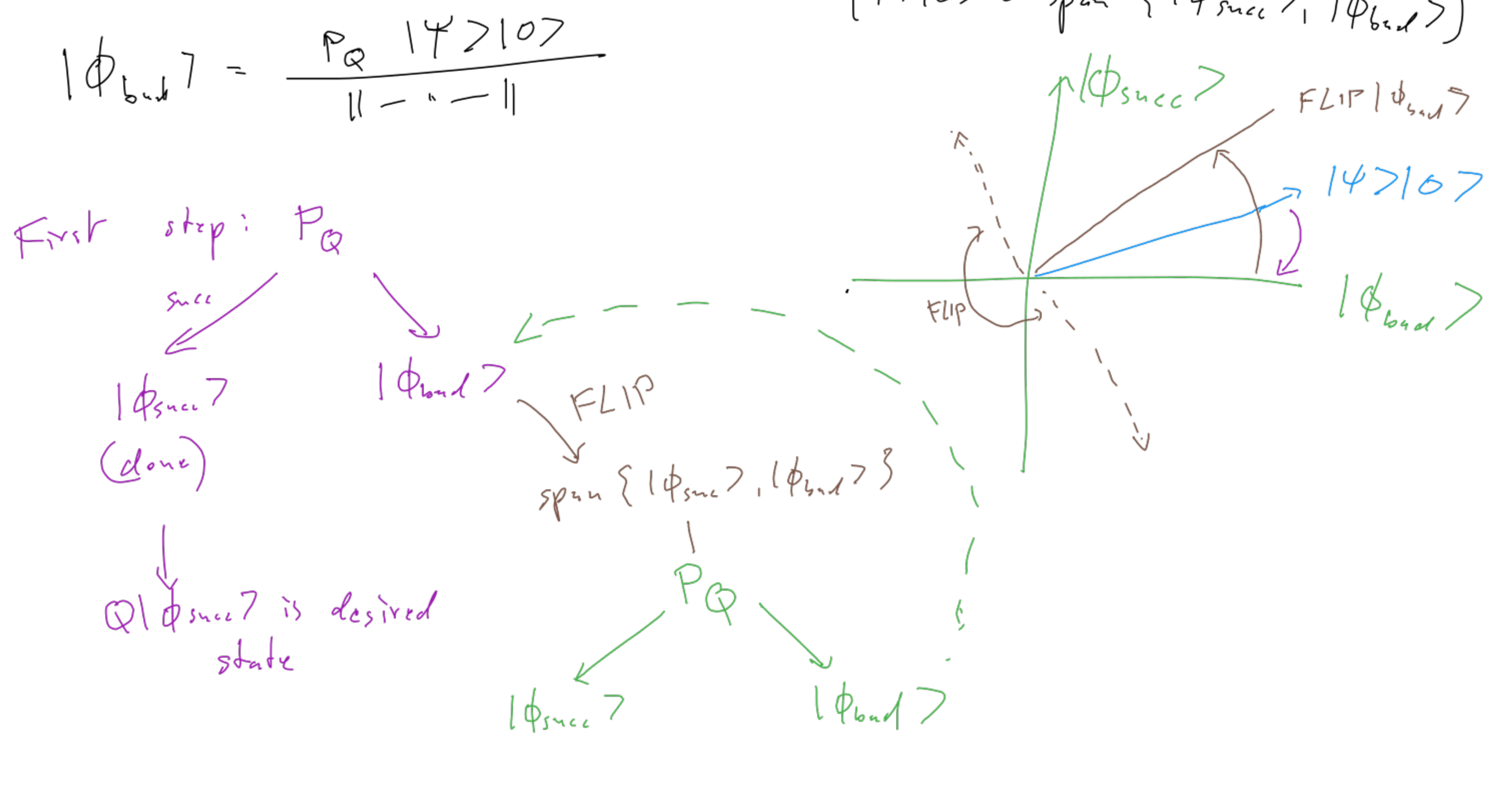
$|\psi\rangle|0\rangle$ init. state

$\overline{P_Q} = 1 - P_Q$

$$|\phi_{succ}\rangle = \frac{\overline{P_Q}\, |\psi\rangle|0\rangle}{\| - " - \|}$$

$$|\phi_{bad}\rangle = \frac{P_Q\, |\psi\rangle|0\rangle}{\| - " - \|}$$

$|\psi\rangle|0\rangle \in span\{|\phi_{succ}\rangle, |\phi_{bad}\rangle\}$



Missing piece:

$FLIP\,|\phi_{bad}\rangle$ stays in span.

$\Delta := I \otimes |0\rangle\langle 0|$

$FLIP = 2\Delta - I$

$$FLIP\,|\phi_{bad}\rangle = (2\Delta - I) \frac{P_Q\, |\psi\rangle|0\rangle}{\| - " - \|} \qquad \| - " - \| = \sqrt{1-p}$$

$$= \frac{2\Delta\, P_Q\, \Delta\, |\psi\rangle|0\rangle}{\sqrt{1-p}} - \frac{P_Q\, |\psi\rangle|0\rangle}{\sqrt{1-p}}$$

$$= 2\,(I \otimes |0\rangle)\,(I \otimes \langle 0|)\, P_Q\, (I \otimes |0\rangle)\,(I \otimes \langle 0|) \frac{|\psi\rangle|0\rangle}{\sqrt{1-p}} - \ldots$$

$P_Q^* = (1-p) I$

$\Delta = (I \otimes |0\rangle)(I \otimes \langle 0|)$

$$= \frac{2\,\Delta\, |\psi\rangle|0\rangle}{\sqrt{1-p}} \sqrt{(1-p)} - \frac{P_Q |\psi\rangle|0\rangle}{\sqrt{1-p}}$$

$$= 2\sqrt{1-p}\, |\psi\rangle|0\rangle - |\phi_{bad}\rangle$$

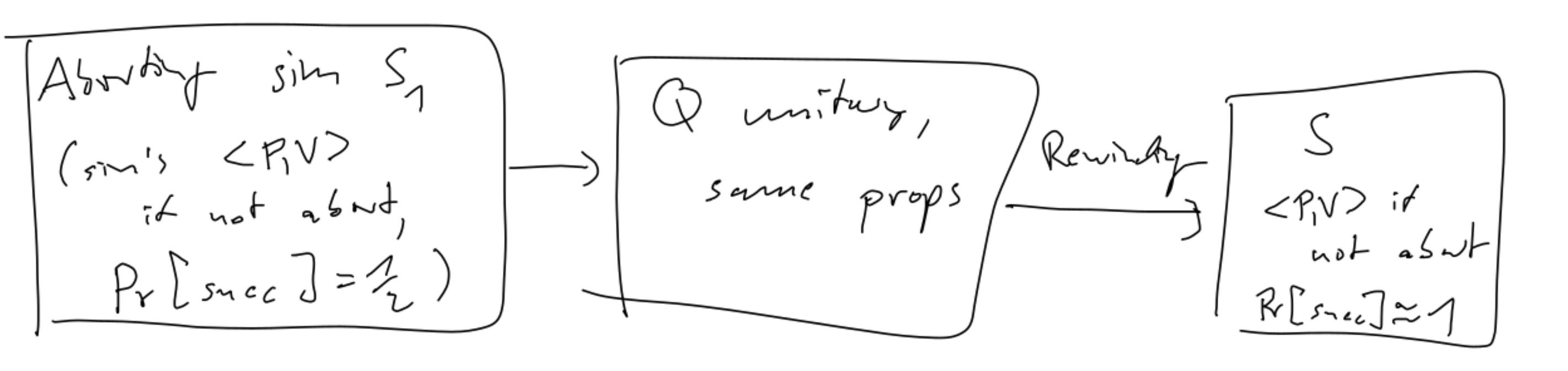
$\Rightarrow FLIP\,|\phi_{bad}\rangle = 2\sqrt{1-p}\, |\psi\rangle|0\rangle - |\phi_{bad}\rangle$

⟹ After FLIP: have a state that gives us succ with prob. $4p(1-p)$

⟹ In first iter: $Pr[succ] = p$
in every other: $Pr[succ] = 4p(1-p)$

⟹ Get succ in $\sim \frac{1}{4p(1-p)}$ iterations

Putting it together:



⟹ GI is QZK.