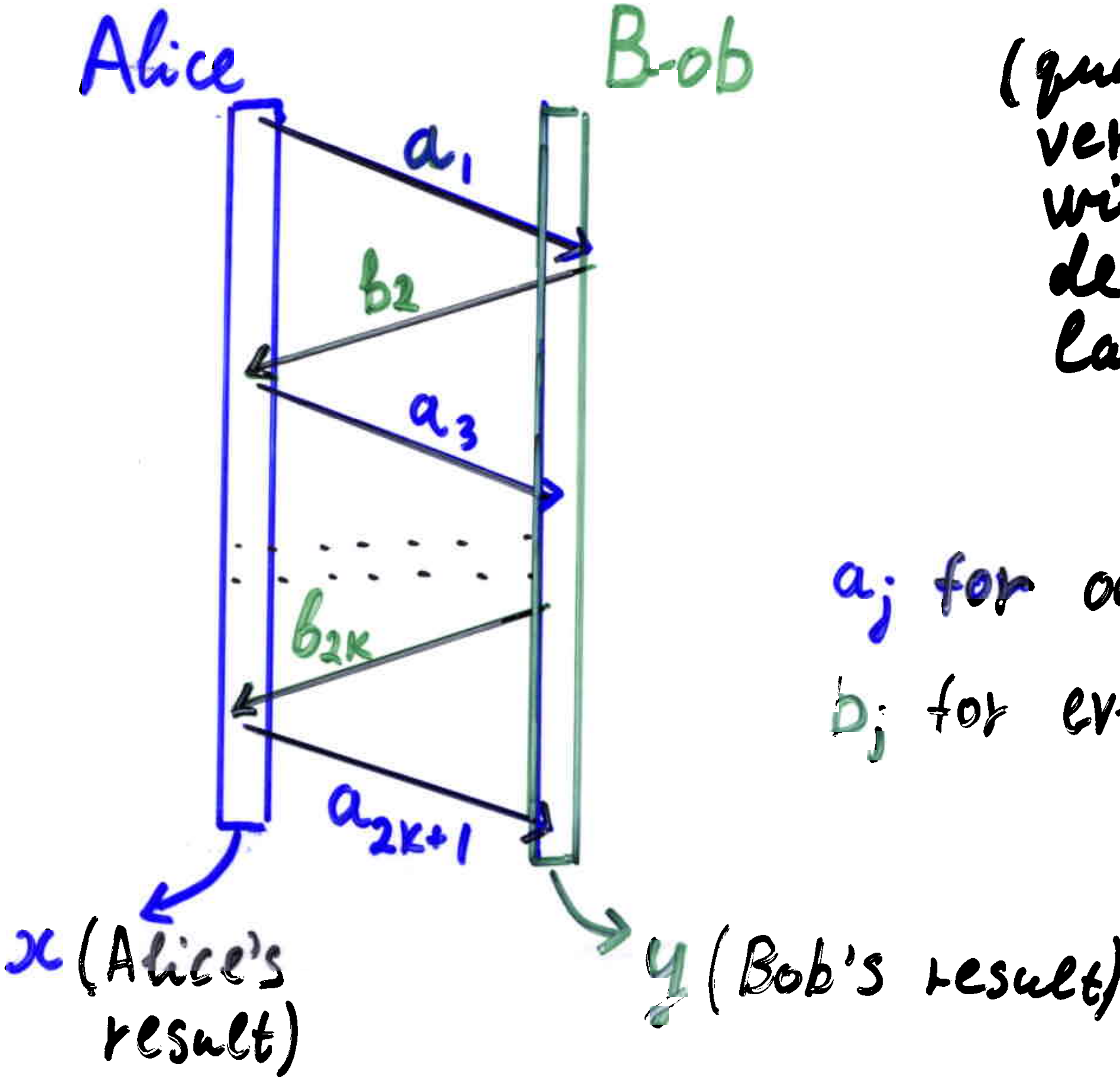
A negative result about quantum coin flipping.

(classical) communication game



(quantum version will be defined later)

a_j for odd j

b_j for even j

The game is defined by Alice's protocol A and Bob's protocol B

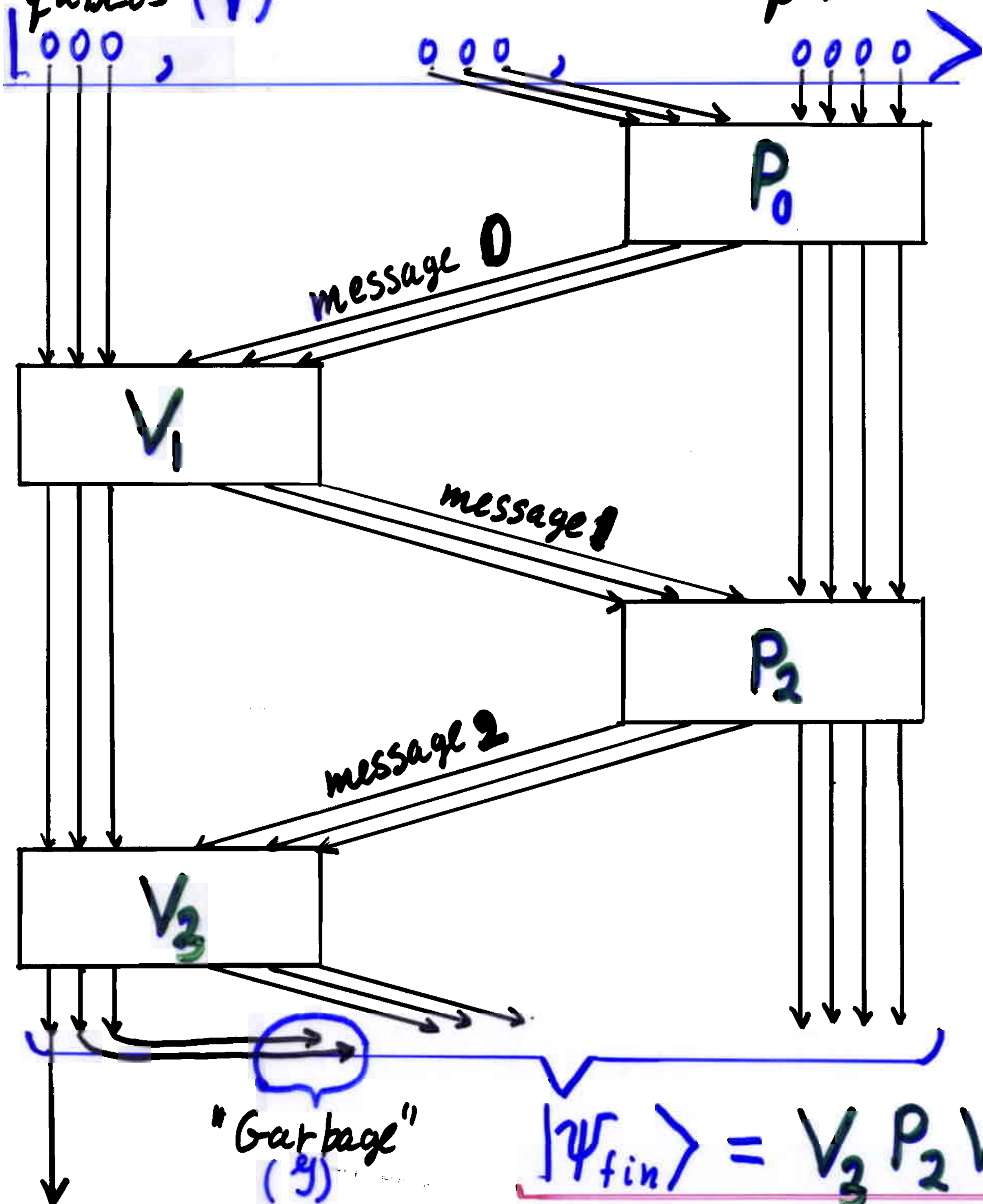
B

The structure of the game (quantum)

$$\mathcal{H} = \mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}$$

(J. Watrous 1999)

Verifier's private qubits $(\mathcal{V})$ — Message qubits $(\mathcal{M})$ — Prover's private qubits $(\mathcal{P})$



$(I_{\mathcal{V}} \otimes P_0)$

$(V_1 \otimes I_{\mathcal{P}})$

$(I_{\mathcal{V}} \otimes P_2)$

$(V_3 \otimes I_{\mathcal{P}})$

$$|\psi_{fin}\rangle = V_3 P_2 V_1 P_0 |0\rangle$$

Output qubit : "1" = "accept" (x)

"0" = "reject" (not x)

Coin flipping game (strong version)

$x, y \in \{0,1\}$ $\quad$ $\boxed{P_{x,y} = \mathrm{Prob}\begin{bmatrix}\text{Alice gets } x \\ \text{Bob gets } y\end{bmatrix}}$

1) Both players are honest (follow the protocol):

$$\boxed{P_{00} = P_{11} = \frac{1}{2}, \qquad P_{01} = P_{10} = 0}$$

2) If Bob cheats (while Alice being honest),

$$\boxed{\mathrm{Prob}[\text{Alice gets } 0] \in [\tfrac{1}{2} - \varepsilon, \tfrac{1}{2} + \varepsilon]}$$

3) If Alice cheats:

$$\boxed{\mathrm{Prob}[\text{Bob gets } 0] \in [\tfrac{1}{2} - \varepsilon, \tfrac{1}{2} + \varepsilon]}$$

Such a game is impossible (in the classical setting) for any $\varepsilon < \frac{1}{2}$.

New result: impossible in the quantum setting for any $\varepsilon < \frac{1}{\sqrt{2}} - \frac{1}{2}$.

Weaker (more specific) conditions

Game 1: (natural) Alice wants to bias the result towards 0,
Bob wants to bias the result towards 1.

Game 2: (strange) The cheater wants the other player to get 1.

Definition: $\boxed{P_{x*} = \max_{\tilde{B}} \operatorname{Prob}[\text{Alice gets } x]}$

(over all cheating strategies $\tilde{B}$)

$\boxed{P_{*y} = \max_{\tilde{A}} \operatorname{Prob}[\text{Bob gets } y]}$

Game 1: $P_{00} = P_{11} = \frac{1}{2}$ $\quad P_{01} = P_{10} = 0$

We want to guarantee: $P_{*0} \leq \frac{1}{2} + \varepsilon \qquad P_{1*} \leq \frac{1}{2} + \varepsilon$

Game 2: We would want to guarantee: $P_{*1} \leq \frac{1}{2} + \varepsilon\,, \quad P_{1*} \leq \frac{1}{2} + \varepsilon$

Two general results about communication games:

Theorem 1.

$$\boxed{P_{x*}\,P_{*y} \geq P_{xy}}$$

for both classical and quantum games

Corollary: Game 2 is impossible for any $\varepsilon < \frac{1}{\sqrt{2}} - \frac{1}{2}$

Proof: $P_{1*}\,P_{1*} \geq P_{11} = \frac{1}{2} \Longrightarrow P_{1*} \geq \frac{1}{\sqrt{2}}$ or $P_{*1} \geq \frac{1}{\sqrt{2}}$

Theorem 2 (Classical only)

$$\boxed{(1-P_{x*})(1-P_{*y}) \leq \sum_{\substack{x' \neq x \\ y' \neq y}} P_{x'y'}}$$

for classical games

Corollary: The classical version of Game 1 is impossible for any $\varepsilon < \frac{1}{2}$.

Proof $(1-P_{1*})(1-P_{*0}) \leq P_{01} = 0 \Longrightarrow P_{1*} = 1$ or $P_{*0} = 1$

The quantum version of Game 1 might be possible. (This is an open question.)

> **Theorem 3** (A. Ambainis, 2001)
>
> \# of rounds $\geq \Omega(\log \log \varepsilon^{-1})$

Classical games in detail

Alice generates a random number r

Bob generate a random number s

$$a_1 = A_1(r) \quad (\text{Alice} \to \text{Bob})$$

$$b_2 = B_2(s; a_1) \quad (\text{Bob} \to \text{Alice})$$

$$a_3 = A_3(r; b_2) \quad (\text{Alice} \to \text{Bob})$$

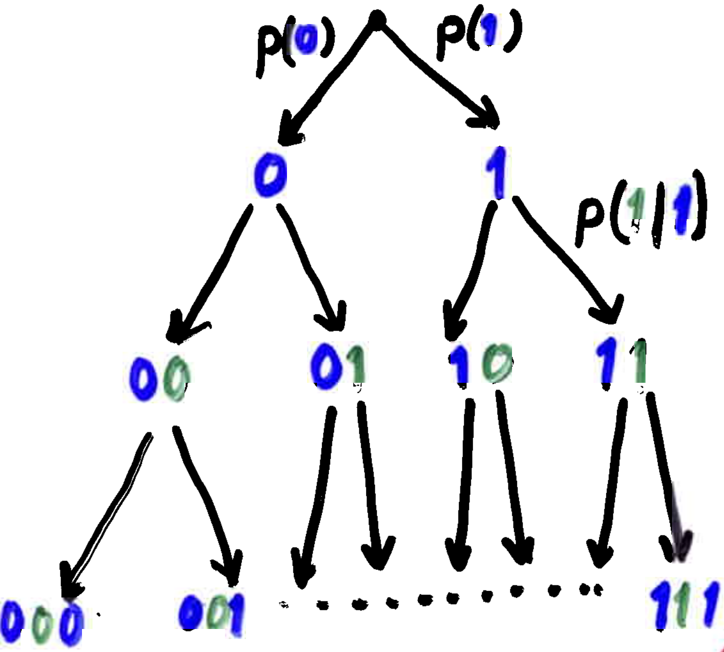
$$\cdots$$

$$a_{2k+1} = A_{2k+1}(r; b_2, \ldots, b_{2k}) \quad (\text{Alice} \to \text{Bob})$$

$$x = A(r; b_2, \ldots, b_{2k})$$

$$y = B(s; a_1, \ldots, a_{2k+1})$$

Game tree



State of the game:

$$u = (a_1, b_2, a_3, \ldots, b_{2k})$$

Transition probabilities:

$$p(a_3 \mid a_1, b_2) = \frac{\#\{r : a_1 = A_1(r),\ a_3 = A_2(r; b_2)\}}{\#\{r : a_1 = A_1(r)\}}$$

Alice's transition probabilities depend only on Alice's protocol $\Longrightarrow$ Alice can use public coins instead of the private number r

(Same for Bob)

Private coins = Public coins

(information-theoretic version

Optimal cheating strategy (classical).

We are dealing with an information-theoretic version of interactive proofs.

$$\boxed{\begin{array}{c}\text{Honest player} = \text{Verifier} \\ \text{Cheater} = \text{prover}\end{array}}$$

Suppose that Alice is honest,
Bob is cheating

Bob computes his success probability bottom-up.

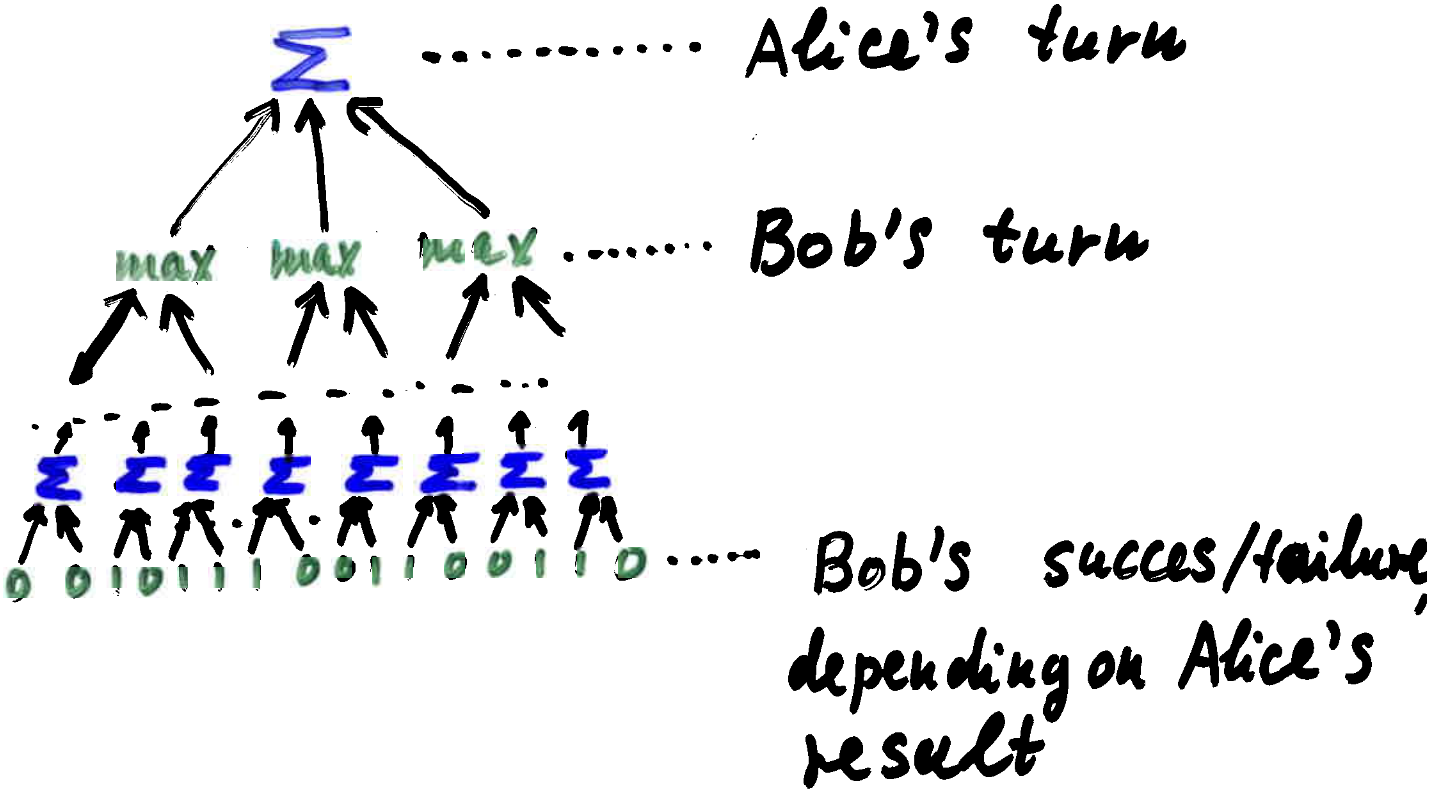
$$Z(\ldots, a_{2k-1}) = \max_{b_{2k}} Z(\ldots, a_{2k-1}, b_{2k})$$

(Bob makes the best move b_{2k})

$$Z(\ldots, b_{2k}) = \sum_{a_{k+1}} p(a_{k+1}|\ldots, b_{2k})\, Z(\ldots, b_{2k}, a_{2k+1})$$

(Alice chooses a_{2k+1} probabistically according to the protocol)

We get a formula with max and Σ gates



Key idea

Combine 3 functions of a game state:

$w(u)$ = probability of state u in the honest game

$Z^A(u)$ = max probability of Bob's success (Bob tricks Alice)

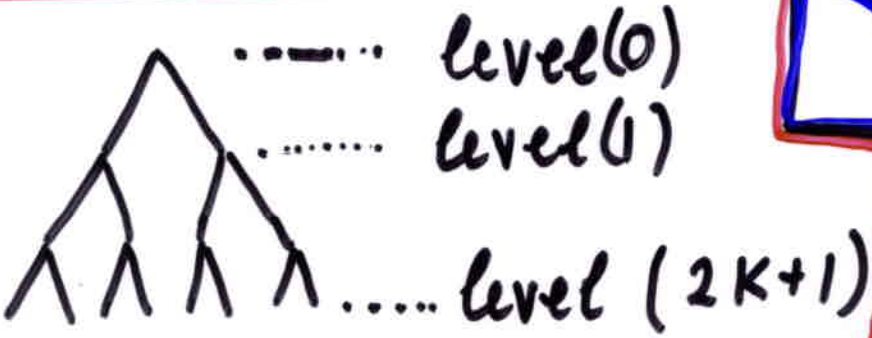
$Z^B(u)$ = max probability of Alice's success in tricking Bob

Define

$$\boxed{F_j = \sum_{u \in level(j)} \underbrace{w(u)\, Z^A(u)\, Z^B(u)}}$$

at level $2K+1$ equals

$$\begin{cases} w(u), & \text{if the outcome is } (x,y) \\ 0, & \text{otherwise} \end{cases}$$



Lemma 1 $\boxed{F_j \geqslant F_{j+1}}$

Proof Alice's turn:

$$w(u, a) = p(a \mid u)\, w(u)$$

$$Z^A(u) = \sum_a p(a \mid u)\, Z^A(u, a)$$

$$Z^B(u) = \max_a Z^B(u, a) \geqslant Z^B(u, a)$$

for any a

$$\Downarrow$$

$$w(u)\, Z^A(u)\, Z^B(u) \geqslant \sum_a w(u, a)\, Z^A(u, a)\, Z^B(u, a)$$

Proof of Theorem 1 (classical case)

$$p_{x*}\, p_{*y} = Z^A()\, Z^B() = \underline{\underline{F_0 \geq F_{2k+1}}} = p_{xy}$$

Proof of Theorem 2

$$0 \leq Z^A(u) \leq 1 \qquad\qquad 0 \leq Z^B(u) \leq 1$$

Wrong in the quantum case

$$G_j = \sum_u \underbrace{w(u)\,(1 - Z^A(u))\,(1 - Z^B(u))}$$

at the end of the game gives the probability of the (not x, not y) event

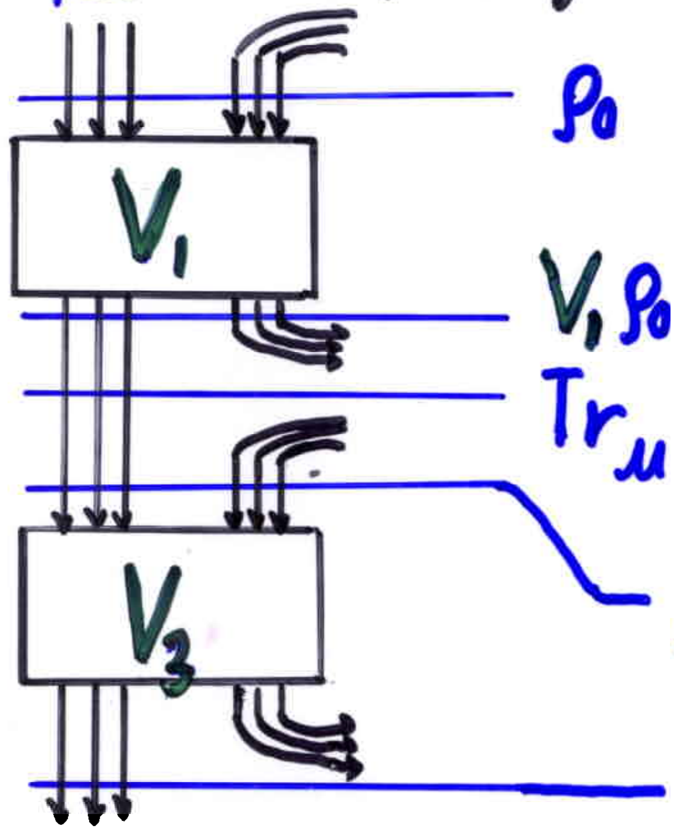
$$\underline{G_j \leq G_{j+1}}$$

$$(1 - p_{x*})\,(1 - p_{*y}) = \underline{\underline{G_0 \leq G_{2k+1}}} = \sum_{\substack{x' \neq x \\ y' \neq y}} p_{x'y'}$$

QIP in terms of mixed states

(tracing out prover's private qubits)

$|0\rangle$ $\mathcal{M}$ (message Hilbert space)



ρ_0 $\boxed{\mathrm{Tr}_{\mathcal{M}}\,\rho_0 = |0\rangle\langle 0|}$

$V_1 \rho_0 V_1^{+} = \rho_1$

$\mathrm{Tr}_{\mathcal{M}}\left(V_1 \rho_0 V_1^{+}\right)$

ρ_2 $\boxed{\mathrm{Tr}_{\mathcal{M}}\,\rho_2 = \mathrm{Tr}_{\mathcal{M}}\left(V_1 \rho_0 V_1^{+}\right)}$

$\mathrm{Tr}_{\mathcal{M}}\left(V_3 \rho_2 V_3^{+}\right)$

Consistent history: $\rho_1, \dots, \rho_K \in D(\mathcal{V} \otimes \mathcal{M})$

$$\boxed{\mathrm{Tr}_{\mathcal{M}}\,\rho_0 = |0\rangle\langle 0|\,, \qquad \mathrm{Tr}_{\mathcal{M}}\,\rho_{2j+2} = \mathrm{Tr}_{\mathcal{M}}\left(V_{2j+1}\,\rho_{2j}\,V_{2j+1}^{+}\right)}$$

Any consistent history is possible with a sutable prover

The reason : Purification theorem

a) $\forall\ \rho \in D(\mathcal{H})$ $\quad \exists\ |\xi\rangle \in \mathcal{H} \otimes \mathcal{P}$ $(\dim \mathcal{P} = \dim \mathcal{H})$

such that $\rho = \mathrm{Tr}_{\mathcal{P}}(|\xi\rangle\langle\xi|)$

purification of ρ

b) If $\rho = \mathrm{Tr}_{\mathcal{P}}(|\xi\rangle\langle\xi|) = \mathrm{Tr}_{\mathcal{P}}(|\eta\rangle\langle\eta|)$

(two purifications)

then $\exists$ unitary operator $V : \mathcal{P} \to \mathcal{P}$

such that $|\eta\rangle = (I_{\mathcal{H}} \otimes V)\,|\xi\rangle$

The only role of the prover is to maintain the purification!

Finding M.A.P. as a semidefinite programming problem.

Variables: $\rho_0, \dots, \rho_{2k}$ (Hermitian matrices of size $\dim \mathcal{V} \cdot \dim \mathcal{M}$ $= \exp(O(n))$)

ρ_{2j} acts on $\mathcal{V} \otimes \mathcal{M}$

$$\begin{cases} \rho_{2j} \geq 0 \quad \text{(positive semidefinite)} \\ \mathrm{Tr}_{\mathcal{M}}\, \rho_{2j+2} = \mathrm{Tr}_{\mathcal{M}}\left(V_{2j+1}\, \rho_{2j}\, V_{2j+1}^{\dagger}\right) \\ \mathrm{Tr}_{\mathcal{M}}\, \rho_0 = |0\rangle\langle 0| \end{cases}$$

$$\mathrm{Prob}[V \text{ accepts}] = \mathrm{Tr}\left(\Pi_{accept}\, \rho_{2k}\right) \to \max$$

$$\left(\Pi_{accept} = V_K^{\dagger}\, \Pi_1^{x}\, V_K\right)$$

Define

$$X = \begin{pmatrix} \boxed{\rho_0} & & & 0 \\ & \boxed{\rho_2} & & \\ & & \ddots & \\ 0 & & & \boxed{\rho_{2k}} \end{pmatrix}$$

$$\begin{cases} X \geq 0 \\ \mathrm{Tr}(Y_\ell X) = b_\ell \\ \mathrm{Tr}(Z X) \to \max \end{cases}$$

The problem is solvable in time poly$(\mathrm{size}(X))$ $= \exp(O(n))$

Linear programming duality

System of linear inequalities in $(u_1, \dots u_n)$

$$
(1)\left\{\begin{array}{lll}
(\vec{a}_1, \vec{u}) = b_1 & \times & c_1 \\
\cdots & & \vdots \\
(\vec{a}_m, \vec{u}) = b_m & \times & c_m \\
(\vec{a}'_1, \vec{u}) \geqslant b'_1 & \times & c'_1 \geqslant 0 \\
\cdots & & \cdots \\
(\vec{a}'_k, \vec{u}) \geqslant b'_k & \times & c'_k \geqslant 0
\end{array}\right.
\qquad \text{Multipliers}
$$

The system has no solution iff one can find multipliers $c_1, \dots, c_m, c'_1, \dots, c'_k$ such that the inequalities add up into "$0 \geqslant 1$"

$$
(1^*)\left\{\begin{array}{l}
\sum'_j c_j \vec{a}_j = 0 \\
\sum'_j c_j b_j = 1 \qquad c'_l \geqslant 0
\end{array}\right.
$$

– This system has a solution

~~generally~~ ~~Application~~: Generalization: If we solve for $(\vec{f}, \vec{u}) \to \max$ conditioned on (1), we may try to deduce the inequality $-(\vec{f}, \vec{u}) \geqslant -g$

$$\max_{\vec{u} \text{ satisfies } (1)} (\vec{f}, \vec{u}) = \min_{\vec{c} \text{ satisfies } (2)} -{\sum_j}' c_j b_j$$

$$(2)\begin{cases} -{\sum_j}' c_j \vec{a}_j = \vec{f} \\ c_l' \geqslant 0 \end{cases}$$

Convex programming duality

$$(1)\begin{cases} \vec{u} \in B_1 \\ \cdots\cdots \\ \vec{u} \in B_m \end{cases} \iff \boxed{\begin{cases} (\vec{a}, \vec{u}) \geqslant b \\ \text{for } [\vec{a}, b] \in \\ B_1^*, \dots, B_m^* \end{cases}}$$

$$(\vec{f}, \vec{u}) \to \max$$

$B_j^* \subseteq \mathbb{R}^{n+1}$

(closed convex cone)

$$\sup_{\vec{u} \text{ satisfies } (1)} (\vec{f}, \vec{u}) \leqslant g \quad \text{iff} \quad [-\vec{f}, -g] \in \underbrace{\overline{B_1^* + \dots + B_m^*}}_{\text{the closure of the sum}}$$

Special case: the region (1) is compact

$$\max_{\vec{u} \text{ satisfies } (1)} (\vec{f}, \vec{u}) = \inf\{g : [-\vec{f}, -g] \in B_1^* + \dots + B_m^*\}$$

Want to transform

$$\left\{\begin{array}{ll} \rho_{2j} \geq 0 & \\ -\mathrm{Tr}_{\mathcal{M}}\, \rho_{2j+2} + \mathrm{Tr}_{\mathcal{M}}\left(V_{2j+1}\, \rho_{2j}\, V_{2j+1}^{\dagger}\right) = 0 & \\ -\mathrm{Tr}_{\mathcal{M}}\, \rho_0 = -|0\rangle\langle 0| & \end{array}\right. \qquad \begin{array}{|c} \text{Multipliers} \\ \hline Y_{2j} \\ Z_{2j+2} \\ Z_0 \end{array}$$

into

$$-\mathrm{Tr}\left(\Pi_{accept}\, \rho_{2k}\right) \geq -g \qquad \boxed{g \to \inf}$$

Y_{2j} acts on $\mathcal{V} \otimes \mathcal{M}$

Z_{2j} acts on $\mathcal{V}$

ρ_{2j} enters as

$$\mathrm{Tr}_{\mathcal{V}\otimes\mathcal{M}}\left(Y_{2j}\, \rho_{2j}\right) - \underbrace{\mathrm{Tr}_{\mathcal{V}}\left(Z_{2j}\left(\mathrm{Tr}_{\mathcal{M}}\, \rho_{2j}\right)\right)}_{=\ \mathrm{Tr}_{\mathcal{V}}\, \mathrm{Tr}_{\mathcal{M}}\left(\underbrace{\left(Z_{2j} \otimes I_{\mathcal{M}}\right)}\, \rho_{2j}\right)} + \mathrm{Tr}_{\mathcal{V}}\left(Z_{2j+2} \times \mathrm{Tr}_{\mathcal{M}}\left(V_{2j+1}\, \rho_{2j}\, V_{2j+1}^{\dagger}\right)\right)$$

ρ_{2j} enters as

$$\mathrm{Tr}_{r_j M}\left(\rho_{2j}\underbrace{\left(Y_{2j} - (Z_{2j}\otimes I_M) + V_{2j+1}^{\dagger}(Z_{2j+2}\otimes I_M)V_{2j+1}\right)}_{=0 \quad (\text{for } j<k)}\right)$$

$$Y_{2j} - (Z_{2j}\otimes I_M) + V_{2j+1}^{\dagger}(Z_{2j+2}\otimes I_M)V_{2j+1} = 0$$

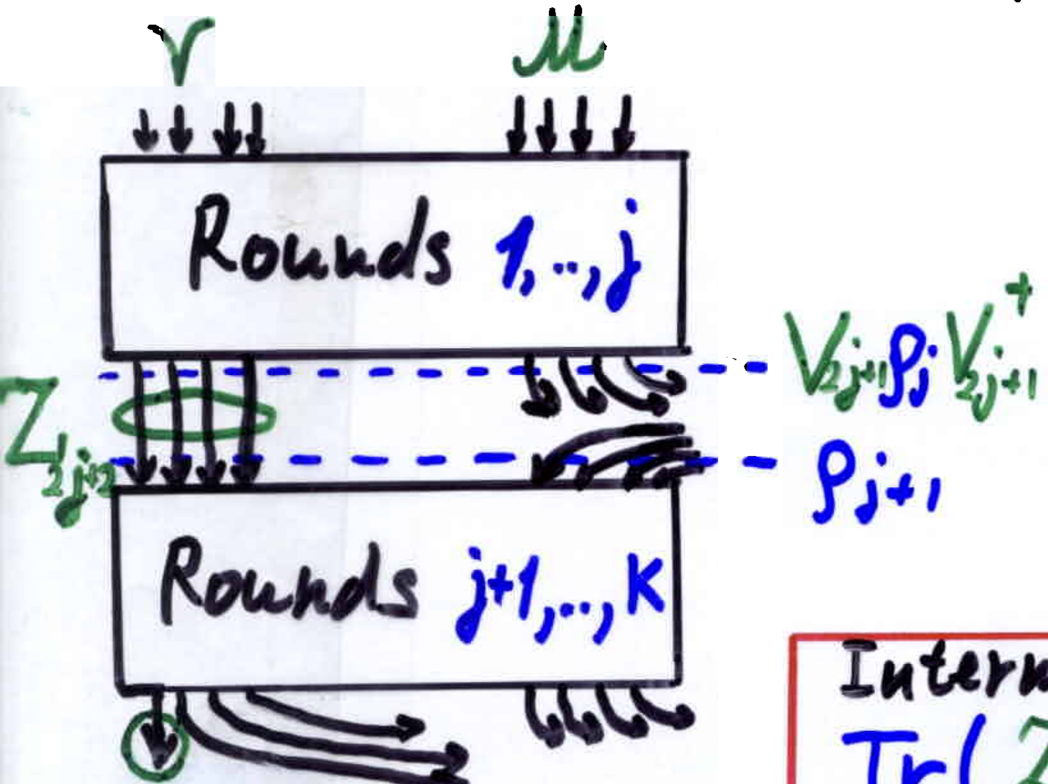
We can exclude Y_{2j} $(Y_{2j}\geq 0)$

$$\boxed{Z_{2j}\otimes I_M \geq V_{2j+1}^{\dagger}(Z_{2j+2}\otimes I_M)V_{2j+1}}$$

The dual problem

Variables: $Z_0, \dots, Z_{2K}$ — Hermitian operators on the space $\mathcal{V}$

Meaning of Z_{2j}: an intermediate goal for the prover



$$\gamma_j = \mathrm{Tr}_{\mathcal{M}}(V_j \rho_j V_j^\dagger) = \mathrm{Tr}_{\mathcal{M}}\, \rho_{j+1}$$

Intermediate goal:

$$\mathrm{Tr}(Z_{2j}\,\gamma_{2j}) \to \max$$

$$Z_{2K} = |1\rangle\langle 1|$$

Final goal: $\mathrm{Tr}(Z_{2K}\,\gamma_{2K}) \to \max$

$$\boxed{\begin{array}{l} Z_{2j+1} \otimes I_{\mathcal{M}} \geq V_{2j+1}^\dagger (Z_{2j+2} \otimes I_{\mathcal{M}}) V_{2j+1} \\ Z_{2K} = |1\rangle\langle 1| \qquad \langle 0|Z_0|0\rangle \to \min \end{array}}$$

$\max\{x, y\}$

$\min \langle + | C | + \rangle$

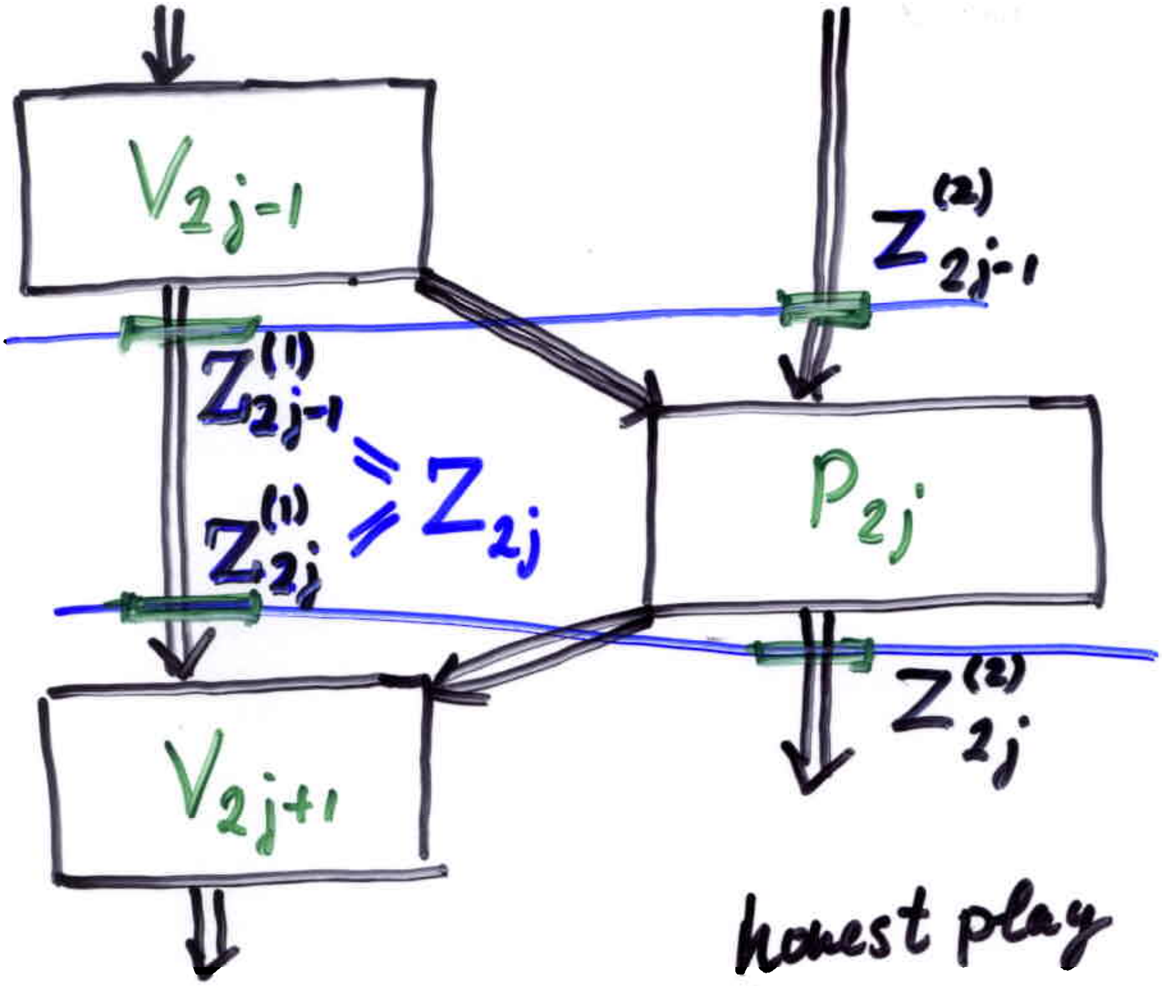
$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$

$\max\{A, B\}$

$$\begin{cases} C \geq A = |0\rangle\langle 0| \\ C \geq B = |1\rangle\langle 1| \end{cases}$$

$$\underbrace{P_{*y} P_{x*} \doteq P_{xy} = 1/2}_{\frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}}}$$

Finally...



honest play

$$F_\ell = \langle \Psi | Z_\ell^{(1)} \otimes I_M \otimes Z_\ell^{(2)} | \Psi \rangle$$

$$\boxed{F_\ell \geqslant F_{\ell+1}}$$

Unfortunately, Z_ℓ is unbounded

$\rightarrow$ no analog of Theorem 2