$\psi_1 \leftarrow \mathrm{Perm}(G)$

$H = \psi_1(G_1)$

$G_2 \xleftarrow{\phi} G_1 \xrightarrow{\psi_1} H$

dist. is the same ⇒ S_1' succeeds w/ low prob.

$S_1' \to S_2' \to \cdots S^*$

read → can have bad here → bad runtime succeeds w/ low pr.

$S_1^Q(x,z)$:
- $i^* \leftarrow \{1,2\}$
- $\psi \leftarrow \mathrm{Perm}(G_{i^*})$
- $H_{i^*} := \psi(G_{i^*})$
- $i \leftarrow V^*(H)$
- output $\leftarrow V^*(\psi^{-1})$
- if $i = i^*$ then return output else return $\perp \times \perp$

Want to show ⟸

$S_6^Q(x,z)$:
- output $\leftarrow \langle P(x,w), V^*(x,z)\rangle$
- w/ prob. $\frac{1}{2}$ return output else $\perp \times \perp$

Does V^* get same input

S_1
- $i=1$: $\mathrm{Perm}(G_1)$
- $i=2$: $\mathrm{Perm}(G_2)$

S_2
- $i=1$: $\mathrm{Perm}(G_1)$
- $i=2$: $\tau \circ \phi^{-1}(G_2)$ = "$\mathrm{Perm}(G_1)$"

$\phi : G_1 \to G_2$

$S_2^Q(x,z)$:
- $i^* \leftarrow \{1,2\}$
- $\tau \leftarrow \mathrm{Perm}(G_1)$
- $\psi := $ if $i^* = 1$ then $\psi = \tau$ else $\tau \circ \phi^{-1}$
- $H_{i^*} := \psi(G_{i^*})$
- $i \leftarrow V^*(H)$
- output $\leftarrow V^*(\psi^{-1})$
- if $i = i^*$ then return output else return $\perp \times \perp$

$S_3^Q(x,z)$:
- $i^* \leftarrow \{1,2\}$
- $\tau \leftarrow \mathrm{Perm}(G_1)$
- $\psi := $ if $i^* = 1$ then $\psi = \tau$ else $\tau \circ \phi^{-1}$
- $H_1 := \tau(G_1)$
- $i \leftarrow V^*(H)$
- output $\leftarrow V^*(\psi^{-1})$
- if $i = i^*$ then return output else return $\perp \times \perp$

Reorder

$S_4^Q(x,z)$:
- $\tau \leftarrow \mathrm{Perm}(G_1)$
- $H_1 := \tau(G_1)$
- $i \leftarrow V^*(H)$
- $i^* \leftarrow \{1,2\}$
- $\psi := $ if $i^* = 1$ then $\psi = \tau$ else $\tau \circ \phi^{-1}$
- output $\leftarrow V^*(\psi^{-1})$
- if $i = i^*$ then return output else return $\perp \times \perp$

reorder →

$S_5^Q(x,z)$:
- $\tau \leftarrow \mathrm{Perm}(G_1)$
- $H_1 := \tau(G_1)$
- $i \leftarrow V^*(H)$
- $\psi := $ if $i = 1$ then $\psi = \tau$ else $\tau \circ \phi^{-1}$
- output $\leftarrow V^*(\psi^{-1})$

Play the game normally

- $i^* \leftarrow \{1,2\}$
- if $i = i^*$ then return output else return $\perp \times \perp$

Abort w/ prob $\frac{1}{2}$

$P(x_1, x_2)$:
- $\rho \leftarrow \mathrm{Perm}$ x_1, x_2

$A(x_1, x_2)$:
$P = P_{sim}$
$i \leftarrow \{1,2\}$
$P(x_i)$
x_1, x_2
i

if $i = i'$ then return output else return $\perp X \perp$

if $i = i'$ then return output else return $\perp X \perp$

$i = 1$: $H = \tilde{V}(G_1)$
$i = 2$: $H = \gamma_{\pi\phi}(\tilde{V}(G_2)) = V(G_2)$

$\text{map}: x_1 \to x_2$

$0 \xrightarrow{P'} 0 \xrightarrow{P} 0$

$0 \xrightarrow{P} 0$

What changes in quantum? — quantum poly. time

$V(x,z)$ ≈ can be quantum

$P(x,w)$ — H — V — i — classical

$P_\perp = \perp X \perp$

SD(interaction, simulation) becomes TD(simulation, interaction)

TS: $\frac{1}{2} t_n\left(P_\perp S_1^0(x,w)\right) = \frac{1}{2}$ ≈ prob $\frac{1}{2}$ of abort

$t_n(P_\perp S_{s_1}) = t_n(P_\perp S_{s_6}) = t_n\left(P_\perp\left(\frac{1}{2}S_V + \frac{1}{2}\perp X \perp\right)\right) = t_n\left(\overbrace{\frac{1}{2}P_\perp S_V}^{=0} + \frac{1}{2}P_\perp \perp X \perp\right) = \frac{1}{2}$

need $s_1 = s_2 = \dots = s_6$

$s_{s_1} := s_6$

*) Dist is correct conditioned on not aborting

$S_V = \langle P(x,w), V^*(x,z)\rangle$

$\{P_\perp, \bar{P}_\perp\}$
$\bar{P}_\perp = 1 - \perp X \perp$

$$\frac{\bar{P}_\perp S_1(x,w)\bar{P}_\perp}{t_n \bar{P}_\perp S_1(x,w)\bar{P}_\perp} = \frac{\bar{P}_\perp S_6 \bar{P}_\perp}{t_n \bar{P}_\perp S_6 \bar{P}_\perp} = \frac{\bar{P}_\perp\left(\frac{1}{2}S_V + \frac{1}{2}\perp X \perp\right)\bar{P}_\perp}{t_n - -} = \frac{\frac{1}{2}S_V}{\frac{1}{2}} = S_V$$

Assume we have:

1) Simulator aborts w/ small prob ε: $t_n P_\perp S(x,z) \le \varepsilon$

2) Distribution conditioned on ¬abort is correct

$$\frac{\bar{P}_\perp S(x,z)\bar{P}_\perp}{t_n \bar{P}_\perp S(x,z)\bar{P}_\perp} = \langle P(x,w), V^*(x,z)\rangle$$

Then we have Zero Knowledge

$TD(\langle P(x,w), V^*(x,z)\rangle, S^0(x,w)) \in O(\sqrt{\varepsilon})$

S_V = with prover

S_S = simulated

$TD(S_V, S_S) = ?$

$\tilde{S} = S_S$ with Lemma 8. Does not abort

$S_V \overset{\varepsilon}{\approx} t_S S_V \overset{\sqrt{\varepsilon}}{\approx} \tilde{S} \overset{\sqrt{\varepsilon}}{\approx} S_S$

$t_S := t_n \bar{P}_\perp S_S \bar{P}_\perp$

$TD(S_V, t_S S_V) = \frac{1}{2} t_n |S_V - t_S S_V| = \frac{1}{2} t_n |(1 - t_S) S_V| =$

$= (1 - t_S)\frac{1}{2} \le \varepsilon$

$\bar{P}_\perp \tilde{S} \bar{P}_\perp = \tilde{S}$

$\bar{P}_\perp S_S \bar{P}_\perp = t_S S_V$

$TD(t_S S_V, \tilde{S}) = TD(\bar{P}_\perp S_S \bar{P}_\perp, \bar{P}_\perp \tilde{S} \bar{P}_\perp) \le TD(S_S, \tilde{S}) \le \sqrt{\varepsilon}$

$TD(S_V, S_S) \in O(\sqrt{\varepsilon})$

Lemma 8 [TDMeasLemma]

Let P be an orthogonal projector on H, let $S \in S(H)$, let $\varepsilon \ge 0$. Assume that P returns yes w/ prob $1 - \varepsilon$.

Then $\exists S' \in S(H)$

1) $TD(S, S') \le \sqrt{\varepsilon}$

2) There are states $|\psi_i\rangle \in \operatorname{im} P$ such that $S' = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, $\sum p_i = 1$