statement: $x = (G_1, G_2)$

witness: $\phi : G_1 \to G_2$

$P(x,w)$ $\quad$ $V(x,z)$

$\varphi_1 \leftarrow \text{Perm}(G_1)$, $H := \varphi_1(G_1)$ $\xrightarrow{H}$ $i \leftarrow \{1,2\}$

$\xleftarrow{i}$

if $i = 1$ send φ_1, else $\varphi_1 \circ \phi^{-1}$ $\xrightarrow{\varphi_i : G_i \to H}$ check $\varphi_i(G_i) = H$? if yes 1 otherwise 0

$G_2 \xrightarrow{\phi} G_1 \xrightarrow{\varphi_1} H$

$\boxed{1} \cdot \boxed{2}\ 3\ 4 = N$

$\{ \boxed{2\ 3\ 1\ 0\ 4}\ \boxed{1\ 4\ 0\ 3\ 2}\ \dots \} P$

$G_{i^*} \to G_* \xrightarrow{\varphi} H$

$S(x,z)$
- $i^* \leftarrow \{1,2\}$
- $\varphi \leftarrow \text{perm}(G_{i^*})$
- $H := \varphi(G_{i^*})$
- $i \leftarrow V^*(H)$
- output $\leftarrow V^*(\varphi)$
- if $i = i^*$ return output else $\perp$

$x \leftarrow N$, $p \geq P$, return $p(x)$

TS: aborts w/ prob. $\frac{1}{2}$, but has correct dist. if it doesn't

target: play the game normally, but randomly abort w/ prob. half

$S^Q_1(x,z)$ (z is quantum)
- $i^* \leftarrow \{1,2\}$
- $\varphi \leftarrow \text{perm}(G_{i^*})$
- $H := \varphi(G_{i^*})$
- $i \leftarrow \boxed{V^*(H)}$ (quantum poly-time)
- output $\leftarrow V^*(\varphi)$
- if $i = i^*$ return output else $|\perp\rangle\langle\perp|$

$\Rightarrow$ $S_2^Q(x,z)$:
- $i^* \leftarrow \{1,2\}$
- $\tilde{\varphi} \leftarrow \text{perm}(G_1)$
- $\varphi :=$ if $i^* = 1$ then $\varphi = \tilde{\varphi}$ else $\tilde{\varphi} \circ \phi^{-1}$
- $H := \varphi(G_{i^*})$
- $i \leftarrow V^*(H)$
- output $\leftarrow V^*(\varphi)$
- if $i = i^*$ then return output else $|\perp\rangle\langle\perp|$

$\Rightarrow$ $S_3^Q(x,z)$:
- $i^* \leftarrow \{1,2\}$
- $\tilde{\varphi} \leftarrow \text{perm}(G_1)$
- $\varphi :=$ if $i^* = 1$ then $\varphi = \tilde{\varphi}$ else $\tilde{\varphi} \circ \phi^{-1}$
- $H := \tilde{\varphi}(G_1)$
- $i \leftarrow V^*(H)$
- output $\leftarrow V^*(\varphi)$
- if $i = i^*$ then return output else $|\perp\rangle\langle\perp|$

$\Rightarrow$ $S_4^Q(x,z)$:
- $\tilde{\varphi} \leftarrow \text{perm}(G_1)$
- $H := \tilde{\varphi}(G_1)$
- $i \leftarrow V^*(H)$
- $i^* \leftarrow \{1,2\}$
- $\varphi :=$ if $i^* = 1$ then $\varphi = \tilde{\varphi}$ else $\tilde{\varphi} \circ \phi^{-1}$
- output $\leftarrow V^*(\varphi)$
- if $i = i^*$ then return output else $|\perp\rangle\langle\perp|$

$\Rightarrow$ $S_5^Q(x,z)$:
- $\tilde{\varphi} \leftarrow \text{perm}(G_1)$
- $H := \tilde{\varphi}(G_1)$
- $i \leftarrow V^*(H)$
- $\varphi :=$ if $i = 1$ then $\varphi = \tilde{\varphi}$ else $\tilde{\varphi} \circ \phi^{-1}$
- output $\leftarrow V^*(\varphi)$ } play the game normally
- $i^* \leftarrow \{1,2\}$
- if $i = i^*$ then return output else $|\perp\rangle\langle\perp|$ } abort w/ $\frac{1}{2}$

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

$\rho_{S_1} = \rho_{S_2} = \rho_{S_3} = \dots = \rho_{S_6} = \frac{1}{2}\rho_V + \frac{1}{2}|\perp\rangle\langle\perp|$

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

$\text{tr}\, |\perp\rangle\langle\perp| \rho_V |\perp\rangle\langle\perp| = 0$

$P_\perp = |\perp\rangle\langle\perp|$

$\bar{P}_\perp = I - |\perp\rangle\langle\perp|$

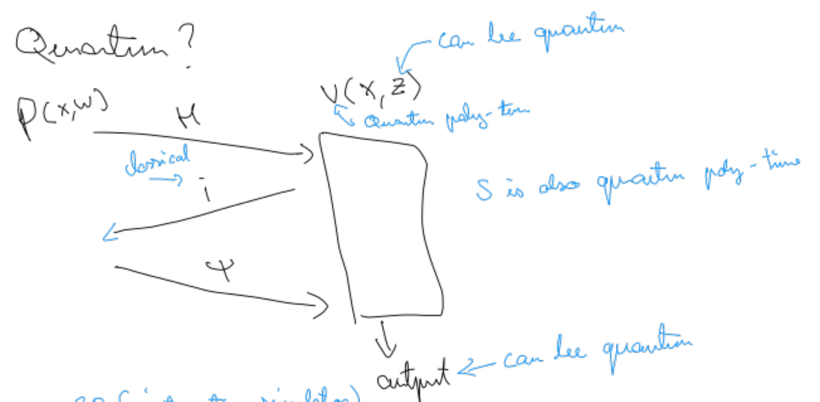
$i =$	1	2
H	$H = \varphi(G_1)$, $\tilde{\varphi} = \varphi$: $H = \varphi(G_1)$	$\varphi \leftarrow$, $H = \varphi(G_2)$; $\tilde{\varphi} = \varphi \circ \phi^{-1}(G_2)$
φ	Give φ; Give $\varphi / \tilde{\varphi}$	Give ψ; Give $\psi = \tilde{\varphi} \circ \phi^{-1}$

$G_1 \xrightarrow{\tilde{\varphi}} H$

$i = 2$: $G_2 \xrightarrow{\phi^{-1}} G_1 \xrightarrow{\tilde{\varphi}} H$

$G_2 \xrightarrow{\psi} H$

What about Quantum?



SD (interaction, simulator)

$\Rightarrow$ TD (interaction, simulator)

TS: $\text{tr}(P_\perp S_1^Q(x,z)) = \frac{1}{2}$ prob $\frac{1}{2}$ aborting

$\text{tr}(P_\perp \rho_{S_1}) = \text{tr}(P_\perp \rho_{S_6}) = \text{tr}\left(P_\perp\left(\frac{1}{2}\rho_V + \frac{1}{2}|\perp\rangle\langle\perp|\right)\right) = \text{tr}\left(\underbrace{\frac{1}{2}P_\perp \rho_V}_{=0} + \frac{1}{2}|\perp\rangle\langle\perp|\right) = \frac{1}{2}$

TS: Dist. conditioned on not abort is the same

$\rho_V = \langle P(x,w), V^*(x,z)\rangle = \dfrac{\bar{P}_\perp S_1^Q(x,z)\bar{P}_\perp}{\text{tr}\,\bar{P}_\perp S_1^Q(x,z)\bar{P}_\perp} = \dfrac{\bar{P}_\perp \rho_{S_6} \bar{P}_\perp}{\text{tr} -:-} = \dfrac{\bar{P}_\perp\left(\frac{1}{2}\rho_V + \frac{1}{2}|\perp\rangle\langle\perp|\right)\bar{P}_\perp}{\text{tr} -:-} = \dfrac{\frac{1}{2}\rho_V}{\frac{1}{2}\cdot 1} = \rho_V$

TS: 1) Simulator aborts w/ small prob ε $\quad \text{tr}\, P_\perp S(x,z) \leq \varepsilon$

2) Dist. conditioned on not aborting is "correct" $\quad \dfrac{\bar{P}_\perp S^Q(x,z)\bar{P}_\perp}{\text{tr}\,\bar{P}_\perp S^Q(x,z)\bar{P}_\perp} = \langle P(x,w), V^*(x,z)\rangle$

$\Rightarrow$ ZK

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

Lemma 8 *Let P be an orthogonal projector on $\mathcal{H}$, let $\rho \in S(\mathcal{H})$, let $\varepsilon \geq 0$. Assume that $\text{tr}\, P\rho \geq 1 - \varepsilon$ (i.e., the measurement $\{P_{yes} := P, P_{no} := 1 - P\}$ returns yes with high probability).*

Then there is a state $\rho' \in S(\mathcal{H})$ such that

(a) $\text{TD}(\rho, \rho') \leq \sqrt{\varepsilon}$.

(b) There are states $|\Psi_i\rangle \in \text{im}\, P$ and values p_i with $\sum_i p_i = 1$, $p_i \geq 0$ such that $\rho' = \sum_i p_i |\Psi_i\rangle\langle\Psi_i|$. (In other words, when measuring ρ', the measurement would always return yes, i.e., ρ' satisfies the property specified by P.)

$\text{tr}\, \bar{P}_\perp \rho_S \geq 1 - \varepsilon$

$P|\Psi_i\rangle = |\Psi_i\rangle$

$\exists \tilde{\rho} : \text{TD}(\hat{\rho}, \rho_S) \leq \sqrt{\varepsilon}$

$\bar{P}_\perp \hat{\rho} \bar{P}_\perp = \tilde{\rho}$

$\text{TD}(\dots) = \sqrt{\varepsilon} + \sqrt{\varepsilon} + \varepsilon \in O(\sqrt{\varepsilon})$

$\rho_V \overset{\varepsilon}{—} t_S \rho_V \overset{\sqrt{\varepsilon}}{—} \tilde{\rho} \overset{\sqrt{\varepsilon}}{—} \rho_S$

$\text{TD}(\bar{P}_\perp \rho_S \bar{P}_\perp, \bar{P}_\perp \tilde{\rho} \bar{P}_\perp) \leq \text{TD}(\rho_S, \hat{\rho}) \leq \sqrt{\varepsilon}$

$\text{TD}(\hat{\rho}, t_S \rho_V) \leq \sqrt{\varepsilon}$

$\rho_S = \rho_V$ $\quad$ $t_S \rho_V$

(abort + correct)

$\bar{P}_\perp \rho_S \bar{P}_\perp = t_S \rho_V$

$t_S = \text{tr}\, \bar{P}_\perp \rho_S \bar{P}_\perp$

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

$\text{TD}(\rho_V, t_S \rho_V) = \text{tr}\, |(1 - t_S)\rho_V| \overset{*}{=}$

$= (1 - t_S) \cdot \text{tr}\, \rho_V = 1 - t_S \leq \varepsilon$