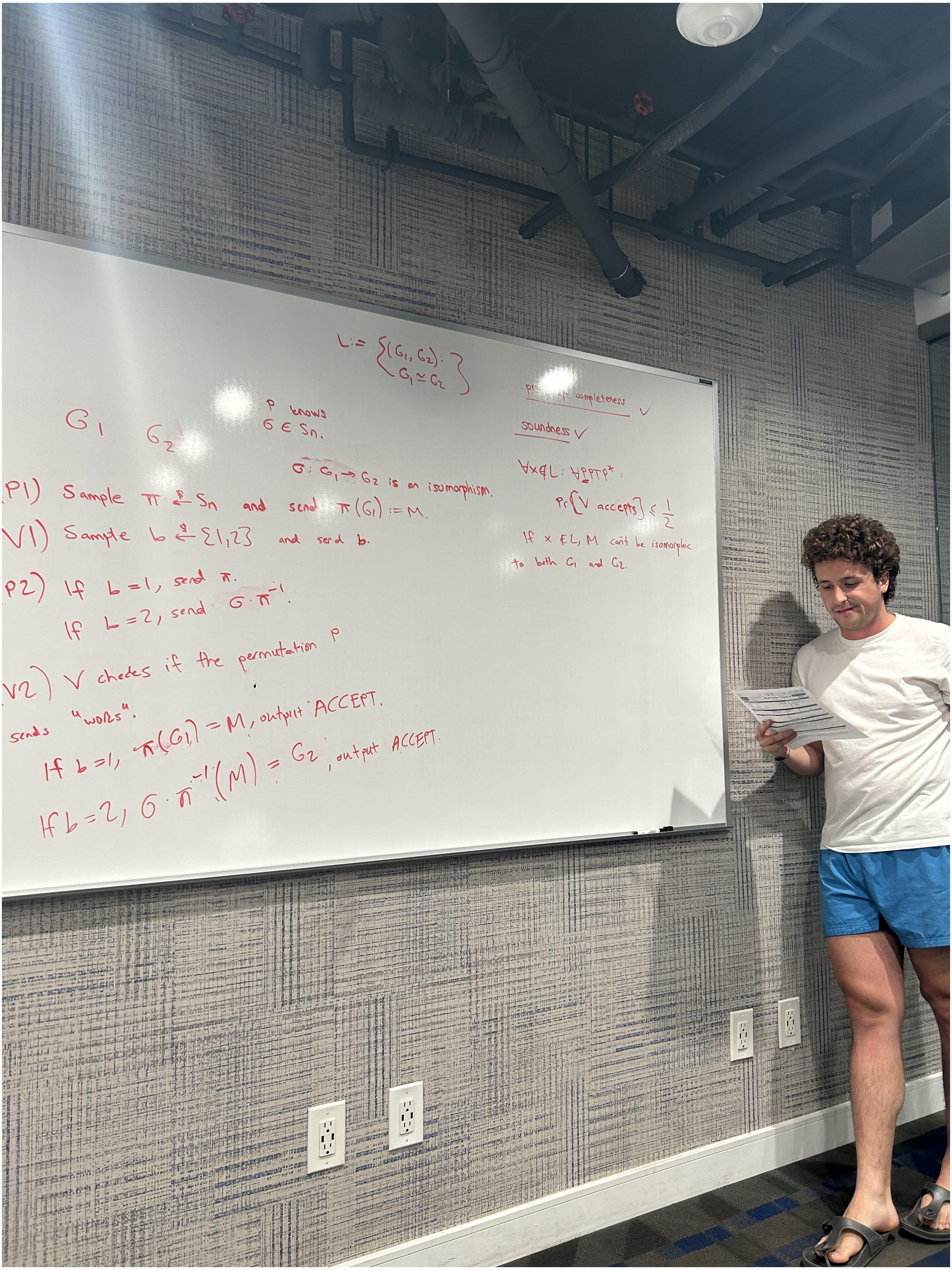
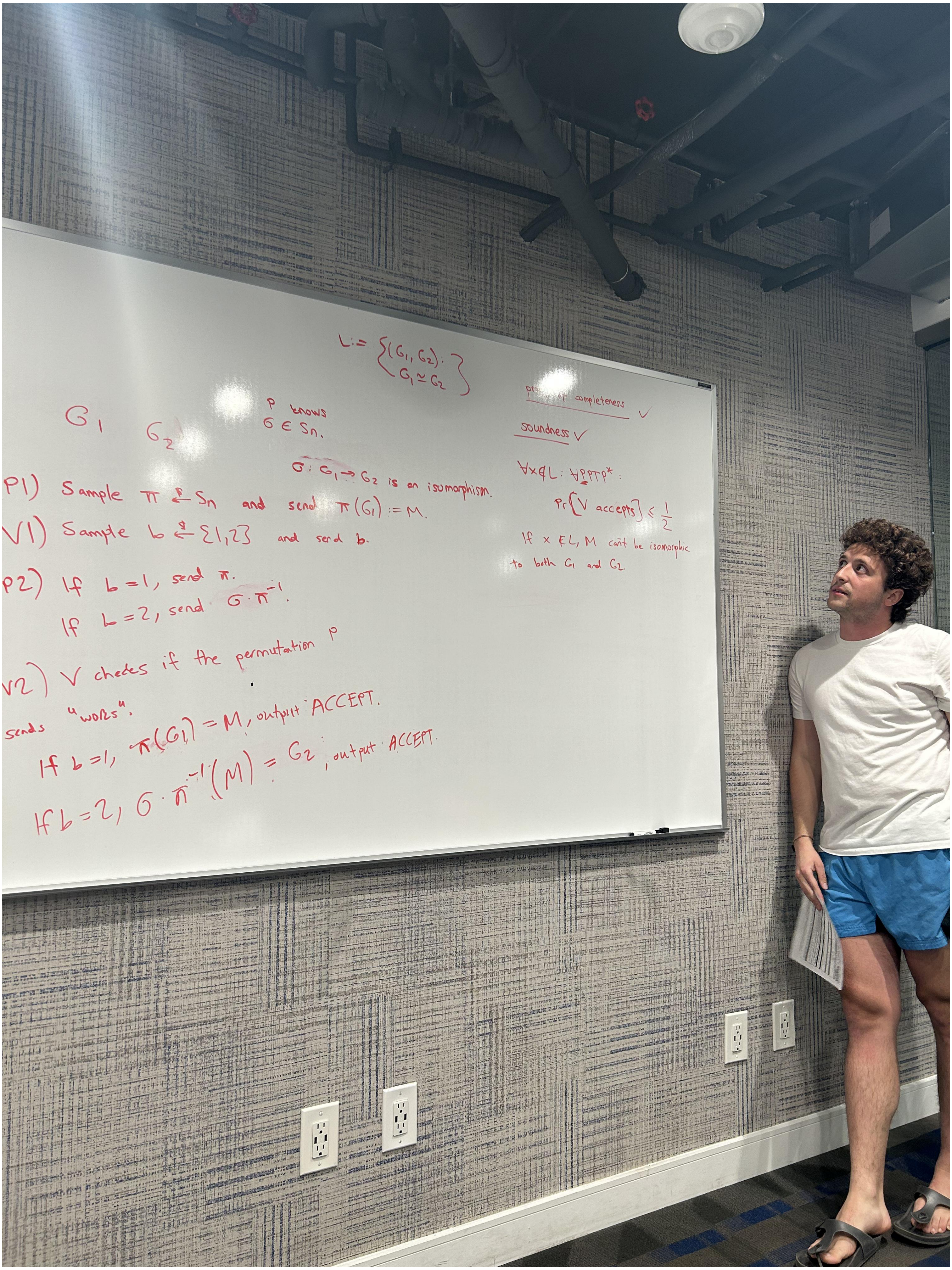

L := {(G1, G2) : G1 ≅ G2}
G1 G2
P knows σ ∈ Sn.
σ : G1 → G2 is an isomorphism.
(P1) Sample π ← Sn and send π(G1) := M.
(V1) Sample b ← {1,2} and send b.
(P2) If b = 1, send π.
If b = 2, send σ·π^-1.
(V2) V checks if the permutation P sends "works".
If b = 1, π(G1) = M, output ACCEPT.
If b = 2, σ·π^-1(M) = G2, output ACCEPT.
completeness ✓
soundness ✓
∀x∉L: ∀P*:
Pr[V accepts] ≤ 1/2
If x ∉ L, M can't be isomorphic to both G1 and G2.



L := {(G1, G2): G1 ≃ G2}
G1 G2
P knows σ ∈ Sn.
σ: G1 → G2 is an isomorphism.
P1) Sample π ← Sn and send π(G1) := M.
V1) Sample b ← {1,2} and send b.
P2) If b = 1, send π.
If b = 2, send σ·π^-1.
V2) V checks if the permutation p sends "works".
If b = 1, π(G1) = M, output ACCEPT.
If b = 2, σ·π^-1(M) = G2, output ACCEPT.
completeness ✓
soundness ✓
∀x∉L: ∀P*:
Pr[V accepts] ≤ 1/2
If x ∉ L, M can't be isomorphic to both G1 and G2.

$L := \left\{ \begin{array}{l} (G_1, G_2): \\ G_1 \simeq G_2 \end{array} \right\}$

$G_1 \quad G_2$

P knows $\sigma \in S_n$.

$\sigma: G_1 \to G_2$ is an isomorphism.

1) Sample $\pi \xleftarrow{\$} S_n$ and send $\pi(G_1) := M$.

1) Sample $b \xleftarrow{\$} \{1,2\}$ and send b.

2) If $b = 1$, send π.

If $b = 2$, send $\sigma \cdot \pi^{-1}$.

2) V checks if the permutation P

ends "works".

If $b = 1$, $\pi(G_1) = M$, output ACCEPT.

If $b = 2$, $\sigma \cdot \pi^{-1}(M) = G_2$, output ACCEPT.

---

① perfect ZK

$\forall$ PPT V^*: $\exists$ <u>expected</u> PPT S^*:

$\forall x \in L$:

$\tau_{real} \equiv \tau_{sim}$

$\langle P, V^* \rangle(x) \equiv S^*(x)$

S^* gets V^*'s code.

② $\forall$ PPT V^*: $\exists$ PPT S^*: $\forall x \in L$:

$\rightarrow \Pr[S^*(x) = \perp] \leq \frac{1}{2}$.

$\rightarrow \Pr[S^*(x) = \alpha] = \Pr[S^*(x) = \alpha \mid S^*(x) \neq \perp]$

$\langle P, V^* \rangle(x) \equiv S^*(x)$