Recall Lemma 2

$$I(X_i, Y_i ; \Pi \mid Z) \geq IC_{\mu_1 \mid Z_i, \epsilon}(DISJ')$$

Before Proving.

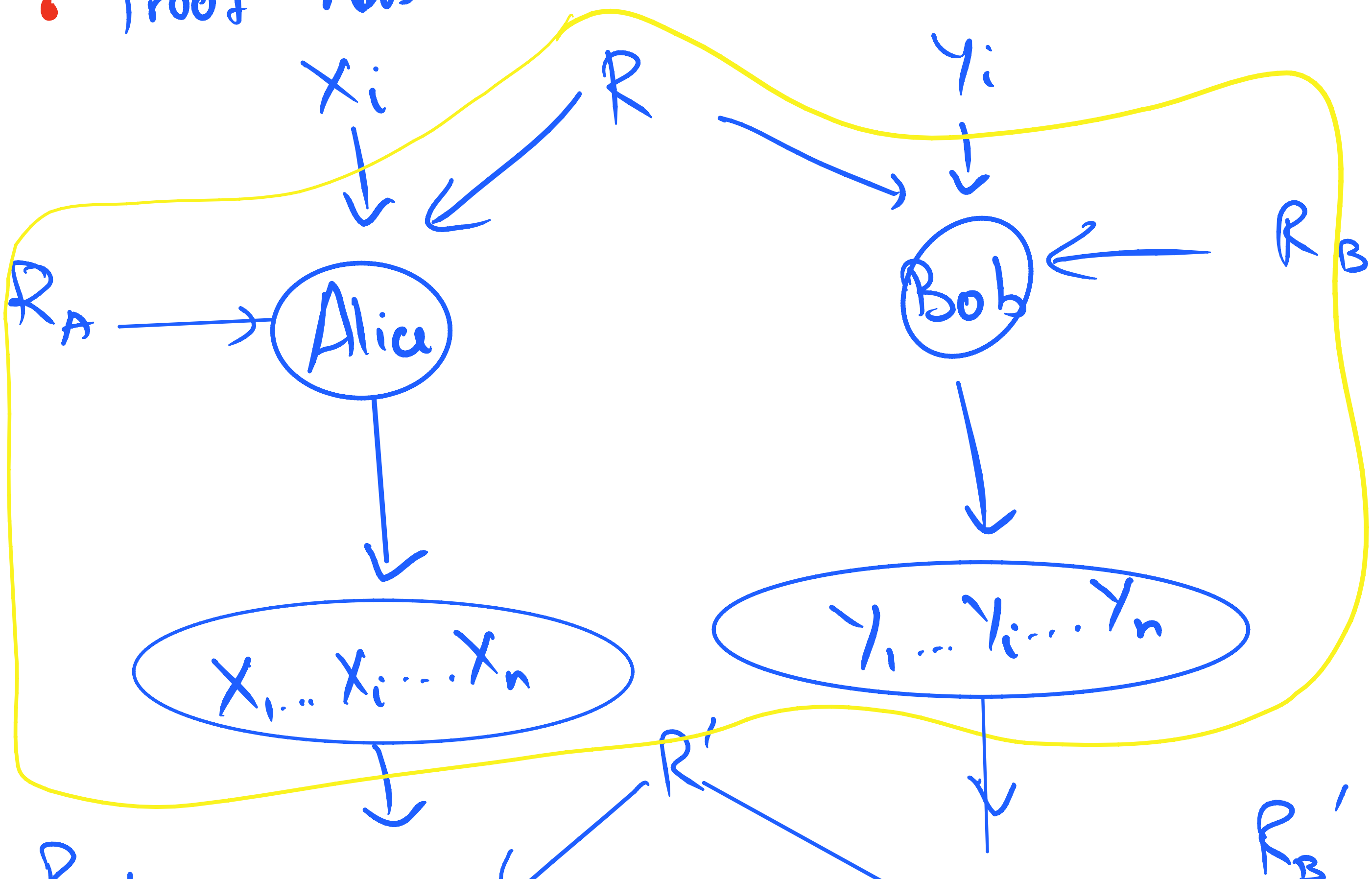
- What is lemma saying? Why is proof not definitional / notational?
- Lemma saying Π reveals information about X_i & Y_i?
- How much? As much as any protocol computing

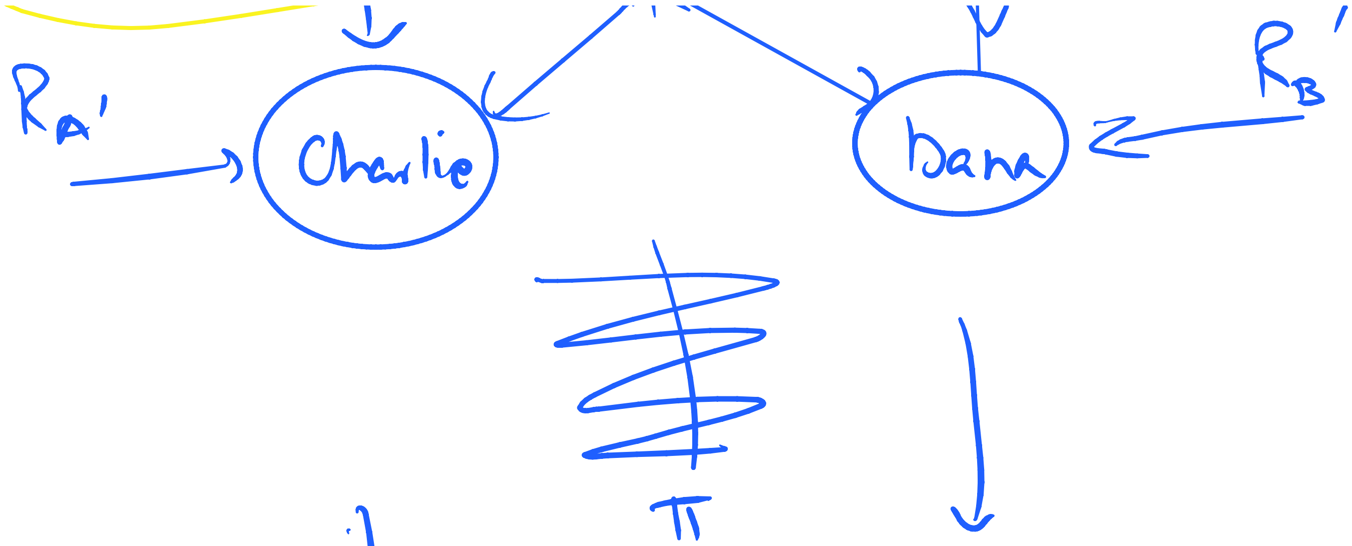
- How much?

  Disjointness on 1-bit inputs

- How can we prove this? What does a proof look like?

- Proof has to be a reduction





$Disj^n(X,Y)$ $\qquad$ $Disj^n(X,Y)$

$\downarrow \quad \overset{?}{=}$ $\qquad$ $\downarrow \quad \overset{?}{=}$

$Disj'(x_i,y_i)$ $\qquad$ $Disj'(X_i,Y_i)$

Key Question: How to get Alice & Bob to produce outputs $(X_1 \ldots X_n)$ & $(Y_1 \ldots Y_n)$ s.t.

① $Disj^n(X,Y) = Disj'(X_i,Y_i)$

① ...

② Π likely to succeed on X, Y
if $(X_i, Y_i) \sim \mu | Z_i$

Answer: (Cleverest part of paper is making this step "natural")

$R = Z_1 \ldots Z_{i-1}, Z_{i+1} \ldots Z_n$

$R_A = \tilde{X}_1 \ldots \tilde{X}_{i-1} \; \tilde{X}_{i+1} \ldots \tilde{Z}_n$

$R_B = \tilde{Y}_1 \ldots \tilde{Y}_{i-1} \; \tilde{X}_{i+1} \ldots \tilde{Z}_n$

$X_j = \tilde{X}_j \wedge Z_j \quad ; \quad Y_j = \tilde{Y}_j \wedge \bar{Z}_j$

Facts

n

Facts

① $$Disj^n(x,y) = \bigvee_{j=1} x_j \wedge y_j$$

$$= \left(\bigvee_{j \neq i} (\tilde{x}_j \wedge z_j \wedge \tilde{y}_j \wedge \bar{z}_j) \right) \vee (x_i \wedge y_i)$$

$$= x_i \wedge y_i = Disj^1(x_i, y_i)$$

② if $(x_i, y_i) \sim \mu_1|z_i$ then

$$(x,y) \sim \mu|_z$$

So if Π solves $DISJ_n(x,y)$ on $\mu|z$, then

Π solves $DISJ_1(x,y)$ on $\mu_1|z_i$!

Conclude: $I(X_i, Y_i, \ldots)$

$$\geq IC_{\mu, 1/2, \epsilon}(DISJ')$$

(Lemma 2) $\blacksquare$

Recall Lemma 3

$$IC_{\mu, 1/2, \epsilon}(DISJ') > 0$$

Why is this not trivial?

- Can exist protocols that are long but leak no information about X_i, Y_i for a long time.

no informa

- So this is not a finite enumeration problem!
- Have to consider protocols of all length ℓ, and prove a lower bound that doesn't go to zero as $\ell \to \infty$

Also: at some point we need to use the fact that Π always correct, and not just on support of μ.

T $\quad$ Π^{00} Π^{01}, Π^{10}, Π^{11}