Cascading Sikora compressions

05 October 2020 6:05 PM

Notation: $(\alpha,\beta,\gamma) \in \mathcal{C}_A(P)$, $p^*_A(P)$, $p^*_B(P)$

$(\alpha,\beta,\gamma) \in \mathcal{C}_A(P)$: $\exists$ some strategy for Alice s.t. when she plays it against an honest Bob, $\Pr[\text{Bob outputs } A] = \alpha$, $\Pr[\text{Bob outputs } B] = \beta$, $\Pr[\text{Bob outputs } \perp] = \gamma$

$p^*_A(P)$: $\max_{(\alpha,\beta,\gamma)\in\mathcal{C}_A(P)} \alpha$ — max prob with which a cheating Alice gets Bob to output A

$p^*_B(P)$: analogous $\max_{(\alpha,\beta,\gamma)\in\mathcal{C}_B(P)} \beta$

Single composition:

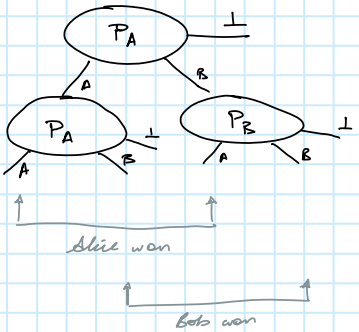
Suppose: P_A is a protocol s.t.
- $(\alpha,\beta,\gamma) \in \mathcal{C}_A(P_A)$ has a simple characterization
- $p^*_A > p^*_B$.

Def^: $P_B :=$ P_A with roles of Alice & Bob switched.

NB: $p^*_A(P_B) = p^*_B(P_A) =: p^*_B$
$p^*_B(P_B) = p^*_A(P_A) =: p^*_A$

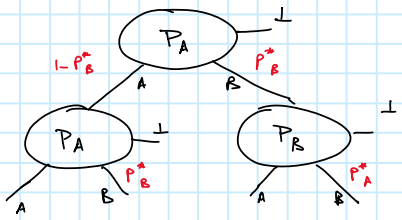
[Rough: $p^*_A = \cos^2\frac{\pi}{8} = 0.852\ldots$ $p^*_B = 3/4 = 0.75$]

Def^: P'_A as follows:



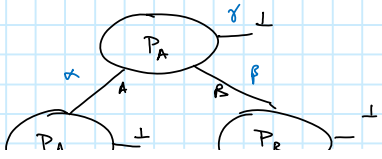
Analysis:

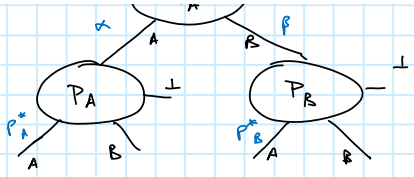
Cheating Bob: (since we don't have cheat vectors for Bob, we use standard comp^).



$p^*_B(P'_A) = (1-p^*_B)p^*_B + p^*_B p^*_A$

Cheating Alice:





$$p^*_A(P'_A) = \max_{\alpha,\beta,\gamma \in C_A(P_A)} \alpha p^*_A + \beta p^*_B$$

Repeated composition:

Suppose: ▸ P_A a protocol s.t.
- $(\alpha,\beta,\gamma) \in C_A(P_A)$ are known
- ~~$p^*_A(P_A) > p^*_B(P_A)$~~ not needed
- $p^*_A(P_A) = p^*_A$, $p^*_B(P_A) =: p^*_B$

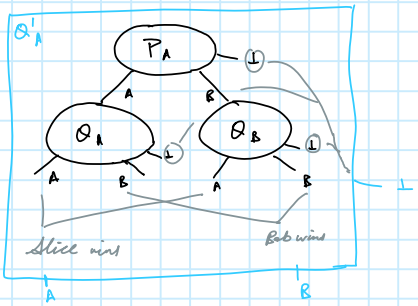
▸ Q_A is a protocol s.t.
- $p^*_A(Q_A) > p^*_B(Q_A)$ — To decide also has the advantage so the protocol can be balanced
- $\| \quad \| \quad \| \quad \|$
- $q^*_A \quad q^*_B$

Def^: $Q_B :=$ Q_A with the roles of Alice & Bob flipped.

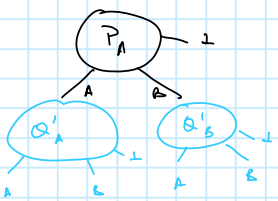
NB: $p^*_A(Q_B) = p^*_B(Q_A) = q^*_B$

$p^*_B(Q_A) = p^*_A(Q_B) = q^*_A$

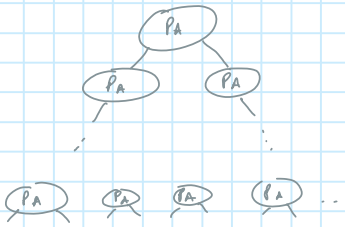
Def^: Q'_A as follows:



In the next step,

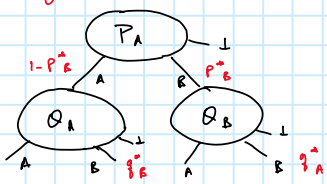


which corresponds to a tree like



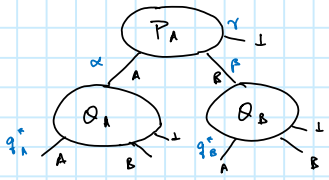
Analysis:

Cheating Bob



$$p^*_B(Q'_A) = (1-p^*_B)\, q^*_B + p^*_B\, q^*_A =: q'^*_B$$

Cheating Alice



$$p^*_A(Q'_A) = \max_{(\alpha,\beta,\gamma) \in C_A(P_A)} \alpha \cdot q^*_A + \beta\, q^*_B =: q'^*_A$$

$$p_A^+(Q'_A) = \max_{(\alpha,\beta,\tau)\in C_A(P_A)} \alpha \cdot q^*_{A} + \beta\, q^*_{B} =: q'^*_{A}$$