6.5979 Lecture 23

- Talk at 11am on Friday by Tony Metger

Defined protocol V_n^{halt}

1) If M does not halt in n steps, then $V_n^{halt} \simeq V_n^{comp}$ (for $n > c_0$) $\simeq V_{2^n}^{halt}$

2) If M does halt in n steps, then $\omega^*(V_n^{halt})$

Thm: $V_{c_0}^{halt}$ decides halting prob. for M

pf: **Completeness:** Suppose M halts in time T

$\Rightarrow V_T^{halt}$ has perfect strat.

$$V_{\log T}^{halt} \simeq^1 V_{\log T}^{comp} \simeq V_T^{halt}$$

$\Rightarrow V_{\log T}^{halt}$ has perfect strat.

$\Rightarrow V_{\log\log T}^{halt}$ has perfect strat.

$\Rightarrow \ldots\ldots$ $V_{C_0}^{halt}$ has perfect strat.

- Soundness: Suppose M doesn't halt

$$V_{C_0}^{halt} \simeq V_{2^{C_0}}^{halt} \simeq V_{2^{2^{C_0}}}^{halt} \cdots$$

$$\varepsilon(V_{C_0}^{halt}, \tfrac{1}{2}) \geq \max\left\{ \{ (V_{2^{C_0}}^{halt}, \tfrac{1}{2}) \}, 2^{2^{C_0}} \right\}$$

$$\geq \max\left\{ \varepsilon\left(V^{\text{halt}}_{2^{2^{c_0}}, \frac{1}{2}}\right), 2^{2^{2^{c_0}}} \right\}$$

$$\geq \ldots$$

$$\Rightarrow \varepsilon\left(V^{\text{halt}}_{c_0, \frac{1}{2}}\right) \geq \infty$$

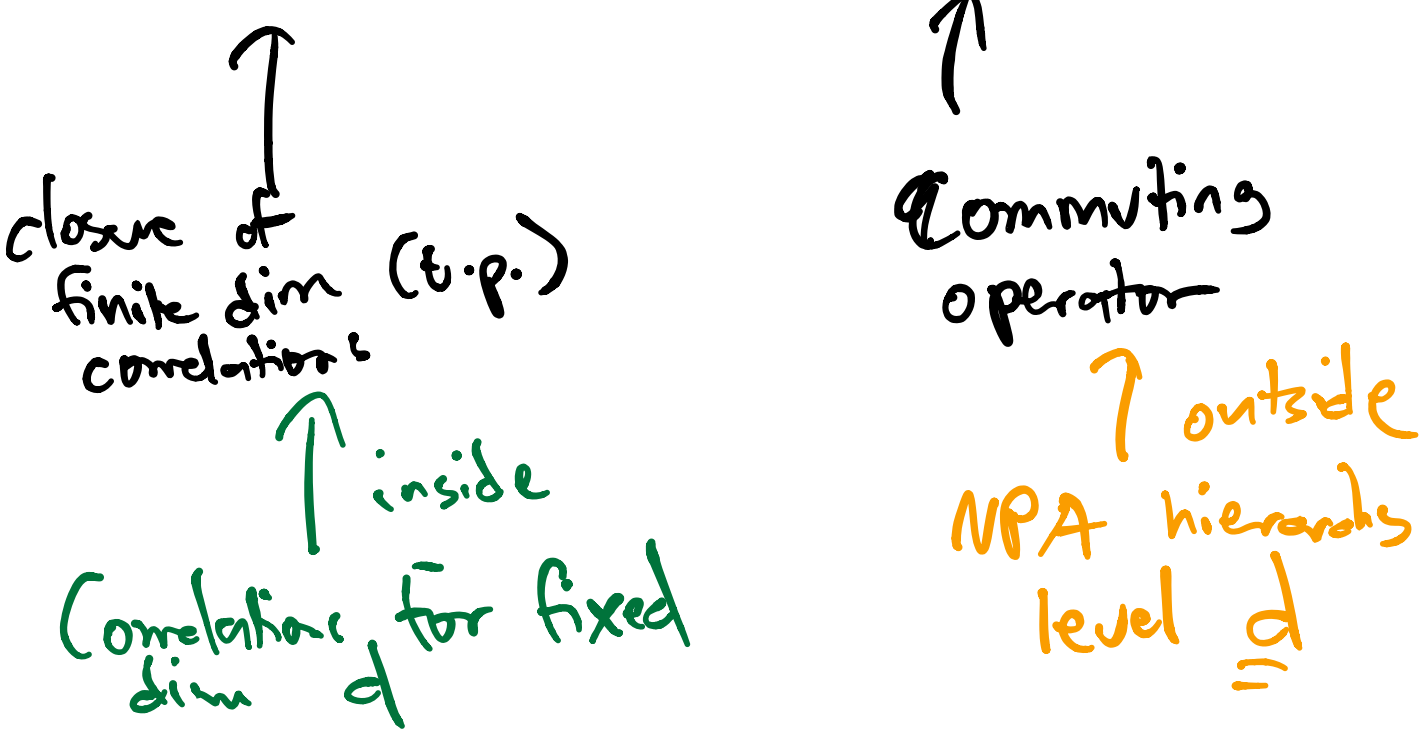
finite dimensional

$\Rightarrow$ There is no entangled strat. achieving val $1/2$

$$\Rightarrow \omega^*\left(V^{\text{halt}}_{c_0}\right) \leq \frac{1}{2}$$

$\Rightarrow V^{\text{halt}}_{c_0}$ is an MIP^* protocol for halting problem w/ instance M

$$C_{qa} \subseteq C_{qc}$$



$C_{qa} = C_{qc} \Rightarrow$ approximations converge to same thing

$\Rightarrow$ $co^*(G)$ is computable

We just showed that $co^*(G)$ is uncomputable (from $MIP^* = RE$)

$\Rightarrow$ $C_{qa} \neq C_{qc}$

Note: this is nonconstructive!

Recall: Pf. that halting is undecidable

Assume $\exists$ V that solves halting

Define M:

1) Runs V("M")

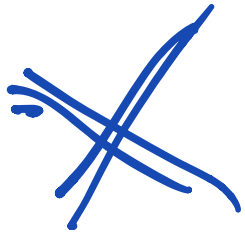
2) If HALT:
   then do infinite loop

   Else: return

What is V("M"):

- If HALT, then M doesn't halt,
  so V is **wrong**

- If NOT HALT, then M halts,
  so V is **wrong**

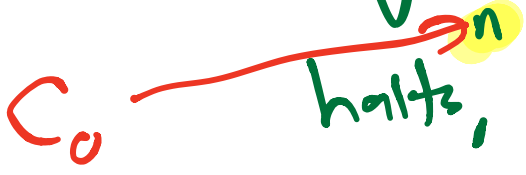


Obs: NPA hierarchy $\Rightarrow \exists$ TM. A that on input G

- If $\omega^{qc}(G) = 1$, then A does not halt
- If $\omega^{qc}(G) < 1$, then A halts

Define V_n^{sep}:

1) Runs A on description of V_n^{sep} for n steps. If C_0 halts, then accept.



2) Otherwise, run $Comp(V_n^{sep}) = V_n^{comp}$

Accept if $V_n^{comp}(x, y, a, b)$ accepts

Claim 1: $\omega^{qc}\left(V^{sep}_{c_0}\right) = 1$

$n > c_0$

Pf: $\Rightarrow$ Suppose $\omega^{qc}\left(V^{sep}_{c_0}\right) < 1.$

then A will halt in $T < \infty$ steps

$\Leftrightarrow \exists\, n'$, $\omega^{qc}\left(V^{sep}_{n'}\right) = 1$

$\Rightarrow \omega^{qc}\left(V^{sep}_{c_0}\right) = 1$

Claim 2: $\omega^{qa}\left(V^{sep}_{n}\right) \leq 1/2$

By Cl. 1, A never halts

$\Rightarrow \xi\left(V^{sep}_{n}, \frac{1}{2}\right) \geq \max\left\{\xi\left(V^{sep}_{2^n}, \frac{1}{2}\right), 2^{2^n}\right\}$

$\geq \ldots\ldots$

$\Rightarrow \xi\left(V^{sep}_{n}, \frac{1}{2}\right) = \infty$

$\Rightarrow$ The perfect strat. for V_n^{sep} is in C_{qc} and not in C_{qa}.

Open: Describe this correlation explicitly or find a simpler one

---

Non-signaling correlations

$$C_c \subsetneq C_q \subsetneq C_{qc} \subsetneq C_{qa} \subsetneq C_{qc}$$

$$\subsetneq C_{ns}$$

minimal relativity restrictions from

$P(a,b|x,y) \in C_{ns}$ iff

$\forall_a x, y, y'$ $P(a|x,y) = P(a|x,y')$

$\forall\, b, b, x, x' \quad p(b|x,y) = p(b|x',y)$

$\exists$ a ns correlation that achieves value I for CHSH

$$p(a|x,y) = \frac{1}{2} \quad \forall\, a, x, y$$

Multiple parties

$$\forall S \quad p(a_{\bar{S}} \mid x_{\bar{S}}, x_S) = p(a_{\bar{S}} \mid x_{\bar{S}}, x'_S)$$

$x_S, x'_S, x_{\bar{S}}$

Define $MIP[C_{ns}]$ // nsMIP — just like $MIP^* = MIP[C_{qa}]$, $MIP^{co} = MIP[C_{qc}]$

nsMIP is less powerful than MIP (or MIP^*)

$$C_{ns}^{2\text{ parties}} = \{\, p(a,b|x,y) :$$

$$\forall a,b,x,y \quad p(a,b|x,y) \geq 0$$

$$\forall x,y, \quad \sum_{a,b} p(a,b|x,y) = 1$$

$$\forall x,x',y,b \quad p(b|x,y) = p(b|x',y) \,\}$$

$$\cdots$$

polytope w/ $\exp$ many facets

$\Rightarrow$ can optimize over C_{ns} with a linear program

$\Rightarrow$ $ns\,MIP \subseteq EXP$

(cf. $MIP = NEXP$)

2-parties $ns\,MIP = PSPACE$

(Ito '09, IKM '09)

$O(\sqrt{\log n})$ parties $ns\,MIP = PSPACE$

Holden Kalai '19

1ns MIP w/ poly(n) provers = EXP

[Kalai, Raz, Rothblum '13]

Why 1ns MIP?

Motivation: MIP protocols require noncommunication which is unrealistic

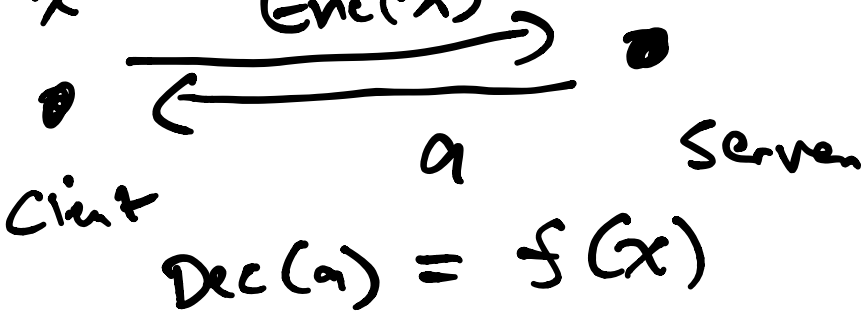
Also, they're sound against arbitrary provers

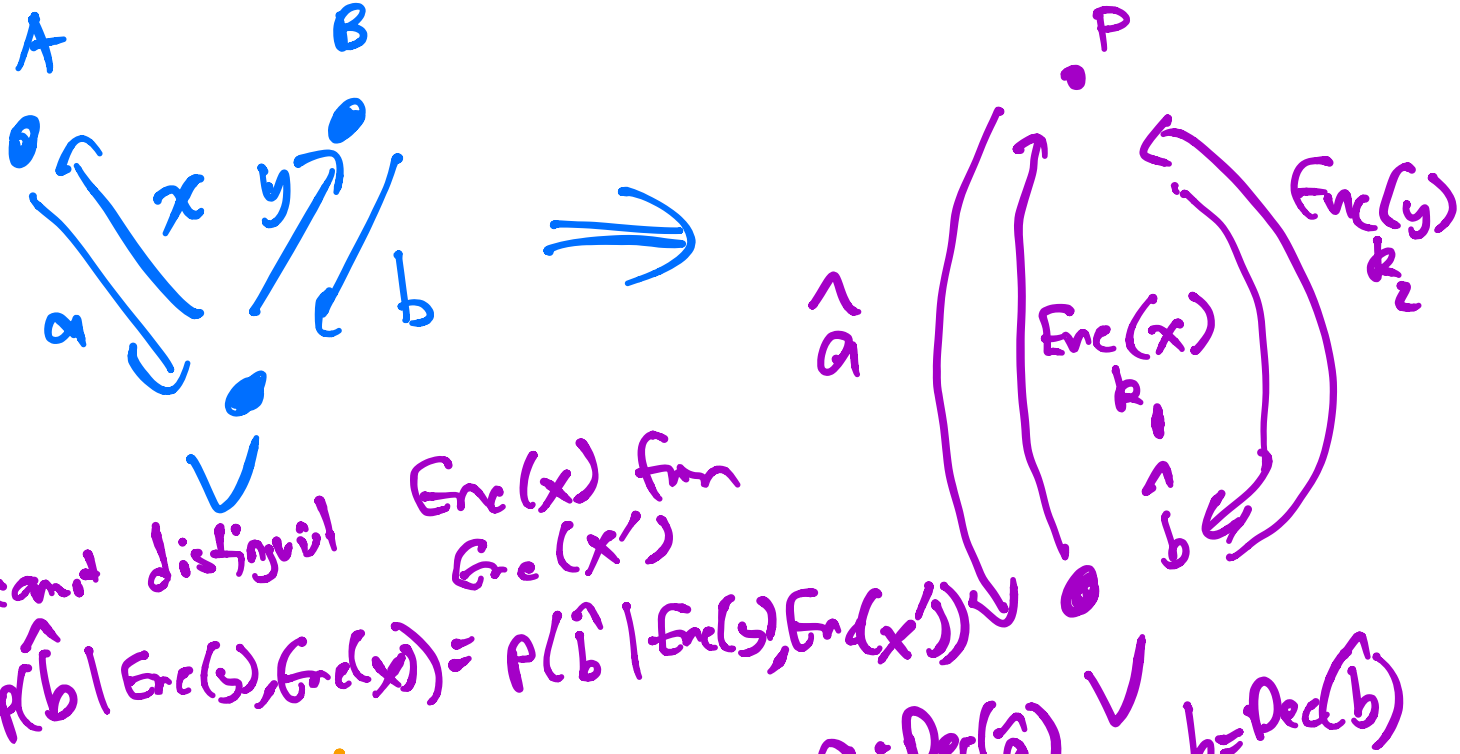
⇓ compiler?

What we want:
- Sound against computationally bounded prover

Proposal: [Aiello et al 2001]

FHE:





P cannot distinguish Enc(x) from Enc(x')

$\Rightarrow P(\hat{b} \mid Enc(y), Enc(x)) = P(\hat{b} \mid Enc(y), Enc(x'))$

Unfortunately, this breaks MIP soundness

e.g. P could apply function to Enc(y) that depends on Enc(x)

(Chiesa et al. ...)

Kalai, Raz, Rothblum '13:

This preserves ns MIP

$\Rightarrow$ Delegate any computation taking time T to single prover

- Prover takes time poly(T)
- Verifie takes time n·poly(T)
- Assume prover cannot break FHE in reasonable time

Currently an active field of research