A TIGHT COMPUTATIONAL INDISTINGUISHABILITY BOUND FOR PRODUCT DISTRIBUTIONS

NATHAN GEIER

GENERAL THEME

- Generalizing statistical bounds to the computational setting.
- Famous example: Yao's XOR Lemma.

If $b \leftarrow \{0,1\}$ is δ-correlated to $D(b)$, then $\bigoplus_{i=1}^{k} b_i$ is δ^k-correlated to $D(b_1), \ldots, D(b_k)$.

Computationally, show how to efficiently transform a correlator for $\bigoplus_{i=1}^{k} b_i$ into a correlator for b (but expect some slackness).

THE DIRECT PRODUCT BOUND

- X_0, X_1 are d_X ind. for circuits of a given size (resp. Y_0, Y_1 with d_y).
- Well known that $d_{XY} \leq d_X + d_Y$.

Statistically, a better bound is known [Folklore, E.g. Kon12]: $d_{XY} \leq d_X + d_Y - d_X \cdot d_Y$.

Suggests that $|X - Y| \leq d$ implies $\left|X^{\otimes k} - Y^{\otimes k}\right| \leq 1 - (1 - d)^k$, instead of $d \cdot k$.

THE DIRECT PRODUCT BOUND

- X_0, X_1 are d_X ind. for circuits of a given size (resp. Y_0, Y_1 with d_y).
- Well known that $d_{XY} \leq d_X + d_Y$.

Statistically, a better bound is known [Folklore, E.g. Kon12]: $d_{XY} \leq d_X + d_Y - d_X \cdot d_Y$.

Suggests that $|X - Y| \leq d$ implies $\left|X^{\otimes k} - Y^{\otimes k}\right| \leq 1 - (1-d)^k$, instead of $d \cdot k$.

- We introduce a new direct and simple proof in the computational setting.

Interesting when $d \cdot k$ is large.

Motivation: amplification of weak OT.

MOTIVATION: AMPLIFICATION OF WEAK OT

- Weak oblivious transfer amplification [DKS99, Wul07].
- Interchanging application of sender security amplification (with receiver security degradation) and receiver security amplification (with sender security degradation).
- XOR amplification, direct product degradation.

MOTIVATION: AMPLIFICATION OF WEAK OT CONT.

- XOR amplification, direct product degradation.
- For example, secret-share database, receiver's choice bit is fixed.

$$c_i = c, \qquad \binom{b_{01}}{b_{11}} \oplus \binom{b_{02}}{b_{12}} \oplus \cdots \oplus \binom{b_{0k}}{b_{1k}} = \binom{b_0}{b_1}$$

- Need the tight bound for a full range of parameters. For example, cannot amplify a $(0.6,0.3)$-weak OT even though $0.6 + 0.3 < 1$.

RELATED WORK

- Maurer and Tessaro [MT10] show how to derive a computational analog for coupling using Holenstein's tight version of the hardcore lemma [Hol05].

General tool to transform coupling proofs to the computational setting.

However, more involved with worse parameters.

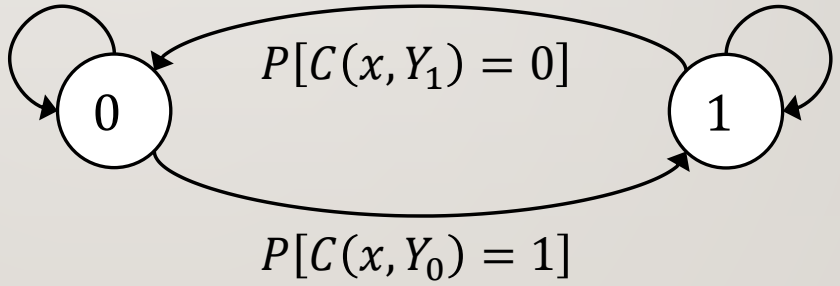
If $\left|X^{\otimes k} - Y^{\otimes k}\right| \leq c$, circuit size multiplied by $1/\varepsilon^2$ instead of $\log(1/\varepsilon)$.

- Halevi and Rabin [HR08] – focus on allowing interaction.

OUR ADVERSARY (N.U.)

- Input: a distinguisher $C(\cdot,\cdot)$ between X_0Y_0 and X_1Y_1, with advantage $d_X + d_Y - d_X \cdot d_Y$.
- If $C(x,\cdot)$ is a d_Y-distinguisher between Y_0 and Y_1 for some hard-coding of x, we are done.
- Otherwise, the following is a d_X-distinguisher between X_0 and X_1:

$b \leftarrow 0$
Repeat:
    $b \leftarrow C(x, Y_b)$



MAIN IDEA

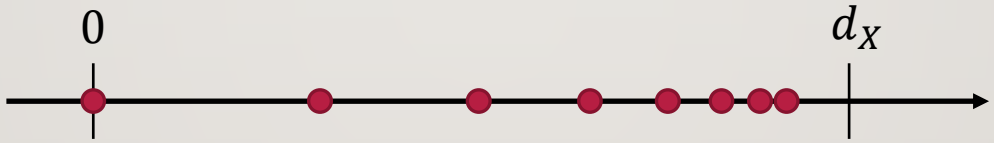
- Amplifying X_0, X_1 distinguisher A:
  Given x, apply $b \leftarrow A(x)$, sample $y \leftarrow Y_b$, output $C(x, y)$.
- If $C(x,\cdot)$ is not good enough for every x, distance from d_X gets multiplied by d_Y.
- Start from $\mathrm{A} \equiv 0$, repeat k times.

$$d_x + d_y - d_x d_y \left\{ \begin{array}{ll} X_1 Y_1 & \\ X_1 Y_{A(x)} & \} \; d_y P[A(X_1) = 0] \\ X_0 Y_{A(x)} & \\ X_0 Y_0 & \} \; d_y P[A(X_0) = 1] \end{array} \right.$$

MAIN IDEA CONT.

- Distance from d_X gets multiplied by d_Y.

$$d_0 = d_x - d_x,\ d_{i+1} \geq d_x - d_x \cdot (d_y)^i.$$



- d_1 same as hybrid argument, continue to get better exponentially approaching d_x.

Add slackness ε_k to get $> d_X$-distinguisher.

THE N-FOLD CASE

Straightforward corollary: the computational generalization of

$$|X - Y| \leq d \Longrightarrow \left|X^{\otimes k} - Y^{\otimes k}\right| \leq 1 - (1 - d)^k$$

With similar slackness/size trade-off.

We also generalize these to the uniform setting (some extra work and no more logarithmic trade-off).

Thank you!