Quantum Pseudorandomness & Classical Complexity

A

William Kretschmer

(rough/quick introduction)

Question: What are the hardness assumptions one needs to have PRSs & which unlikely collapses (e.g. P=PSPACE or BQP=QMA) would invalidate security of PRSs?

(evidence that

stated differently: What computational power suffices to distinguish PRS from Haar-random?

An "obvious" upper bound seems to be QMA:

Arthur holds many copies of $|\psi\rangle$.
Merlin gives the circuit C that produces $|\psi\rangle$.
Arthur does a swap test b/w $|\psi\rangle$ & $C|\psi\rangle$s

NB1: If $|\psi\rangle$ is PRS, such a circuit exists (of poly size)
If $|\psi\rangle$ is Haar random, no poly size circuit exists.

NB2: "Thus" PRS it appears can be distinguished in QMA

BUT

Subtlety: Arthur is getting a quantum — not standard QMA. which is a decision problem over classical strings.

Approach: One way to approach this question,
is to consider quantum adversaries that
can query a classical oracle
(to some language $L : \{0,1\}^* \to \{0,1\}$).
Now if one can show PRS can be broken
by such an adversary,
it means that if PRS exist,
$L \notin BQP$.

Story: They show such a result for L = PP-complete.
: Thus, if BQP = PP, then PRSs don't exist.

Theorem 1 (Informal version of Theorem 27).
$\exists$ a poly-time alg. augmented w/ a PP oracle
that distinguishes PRSs from Haar-random.

Story: Can we do weaker than PP? Perhaps QMA?
Unlikely

Theorem 2 (Informal version of Thms 30 & 33).
$\exists$ a quantum oracle O s.t.
(i) $BQP^O = QMA^O$ &
(ii) PRUs (& hence PRSs) exist relative to O.

Story: Crypto implication: No computationally secure
classical crypto exists if BQP = QMA
(∵ all primitives can be broken in NP &
NP ⊆ QMA)

Yet, quantum crypto can exist.

i.e. $\exists$ a relativized world s.t.

any computationally secure crypto must use quant. communication

quick pre-requisites.

§2.3 Quantum Information

diamond norm: $\|A\|_\diamond := \sup_{\mathrm{tr}(\rho)=1,\ \rho\geq 0} \|(A\otimes I)(\rho)\|_1$.

$$\|M\|_F := \sqrt{\mathrm{tr}(M^\dagger M)}.$$

Fact 7. Let A & B be quantum channels & ρ be a density matrix.

Then,

$$TD(A(\rho), B(\rho)) \leq \frac{1}{2}\|A-B\|_\diamond.$$

skip for now

Fact 8 ([AKN98]). Let U & V be unitary matrices, and suppose d is the distance b/w 0 & the polygon in the complex plane whose vertices are the eigenvalues of $UV^\dagger$.

(Aharonov Kitaev Nisan)

Then, $\|U(\cdot)U^\dagger - V(\cdot)V^\dagger\|_\diamond = 2\sqrt{1-d^2}$

Lemma 9. Let U, V be $N\times N$ unitary matrices.

Then $\|U(\cdot)U^\dagger - V(\cdot)V^\dagger\|_\diamond \leq 2\|U-V\|_F$

(proof skipped)

Notn: $U(\cdot)U^\dagger$ or $U\cdot U^\dagger$ is the operator that maps ρ to $U\rho U^\dagger$.

for Hermitian matrices A, B, $A\leq B$ means $B-A$ is PSD

for superoperators A, B, $A\leq B$ means $B-A$ is completely positive

i.e. for any $\mathbb{1}$ & positive matrix ρ,

$(\Lambda \otimes \mathbb{1})(\rho)$ is PSD.

NB [BHH'16]: (Brandão, Harrow, Horodecki) If Λ has input dim. N, a criterion equivalent to complete positivity is

$$(\Lambda \otimes \mathbb{1}_N)(|\Phi_N\rangle\langle\Phi_N|) \geq 0$$

/

$$|\Phi_N\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |ii\rangle$$

---

§ 2.4 Haar measure & concentration.

Notation: $\mathbb{S}(N)$: N-dim pure states

$\mathbb{U}(N)$: group of $N \times N$ unitary matrices

$\downarrow = 2^n$.

σ_N: Haar measure on $\mathbb{S}(N)$

μ_N: Haar measure on $\mathbb{U}(N)$.

: $\mathbb{U}(N)^M$: space of $MN \times MN$ block diag. unitary matrices (each block has size $N \times N$).

: also, (equiv.) M-tuples of $N \times N$ unitary matrices

μ_N^M: the product measure

$$\mu_N^M(U_1 \dots U_M) := \mu_N(U_1) \cdots \mu_N(U_M)$$

on $\mathbb{U}(N)^M$

(which is interpreted as a distⁿ on a direct sum $U_1 \oplus \dots \oplus U_M$ of matrices)

Story:
Thm 10 ([Mec19, Thm 5.17]) stated below, is a concentration inequality on the Haar measure, stated in terms of Lipschitz continuous functions.

Elizabeth Meckes
The Random Matrix Theory of Classical Compact Groups

Def^: L-Lipschitz: For a metric space M with metric d, a function $f: M \to \mathbb{R}$ is L-Lipschitz if for all $x, y \in M$,
$$|f(x) - f(y)| \leq L \cdot d(x, y)$$

Thm 10. Given $N_1 \dots N_K \in \mathbb{N}$,
let $X = \mathbb{U}(N_1) \oplus \dots \oplus \mathbb{U}(N_K)$
be the space of block-diagonal unitary matrices w/ blocks of size $N_1 \dots N_K$.

Let $\mu = \mu_{N_1} \times \dots \times \mu_{N_K}$ be the product of Haar measures on X.

Suppose, $f: X \to \mathbb{R}$ is L-Lipschitz in the Frobenius norm.

Then, for each $t > 0$:
$$\Pr_{U \leftarrow \mu}\left[f(U) \geq \mathop{\mathbb{E}}_{V \leftarrow \mu}[f(V)] + t\right] \leq \exp\left(-\frac{(N-2)t^2}{24L^2}\right)$$
where $N = \min\{N_1, \dots, N_K\}$

§2.5 Complexity theory

Def^n: Language := A function $L: \{0,1\}^* \to \{0,1\}$

Promise problem := A function $\Pi: \{0,1\}^* \to \{0,1,\perp\}$.

$\mathrm{Dom}(\Pi) := \{x \in \{0,1\}^* : \Pi(x) \in \{0,1\}\}$

domain of a promise problem

Def^n 11 (Promise BQP). A promise problem $\Pi: \{0,1\}^* \to \{0,1,\perp\}$ is in Promise BQP if

$\exists$ a randomised poly-time quant. algorithm $A(x)$ s.t.

(i) if $\Pi(x)=1$, then $\Pr[1 \leftarrow A(x)] \geq 2/3$

(ii) if $\Pi(x)=0$, then $\Pr[1 \leftarrow A(x)] \leq \frac{1}{3}$

BQP is defined as the set of languages in Promise BQP.

(special case of a promise problem where $\mathrm{dom}(\Pi) = \{0,1\}^*$).

Def^n 12 (Promise QMA). A promise problem $\Pi: \{0,1\}^* \to \{0,1,\perp\}$ is in Promise QMA if

$\exists$ a poly-time quant. alg. $V(x, |\psi\rangle)$ called a verifier & a polynomial p s.t.

(i) (completeness) if $\Pi(x)=1$,

$\exists$ a quantum state $|\psi\rangle$ on $p(|x|)$ qubits (called a witness or a proof)

s.t. $\Pr[\nu(x,|\psi\rangle)=1] \geq \frac{2}{3}$

(ii) (soundness) if $\neg(x)=0$,
then $\forall$ state $|\psi\rangle$ on $p(|x|)$ qubits,
$\Pr[\nu(x,|\psi\rangle)=1] \leq \frac{1}{3}$.

QMA is defined as the set $\forall$ languages in Promise QMA.

[skipped: Promise PostBQP
Promise PP was assumed
]

§ 2.6 Quantum Oracles

convention: We define queries to a unitary matrix U [*]
to mean a single application $\forall$
U, U^+, controlled-U (i.e. $\mathbb{I}\oplus U$ (same dim as U))
or, controlled-U^+ (i.e. $1\oplus U^+$)

: superscripts for algorithms the query oracles, e.g. $A^U(x,|\psi\rangle)$

: Variants $\forall$ Promise BQP, Promise QMA
w/ quantum oracles —
(i) where the algorithm can apply unitaries from (or for Promise QMA, the verifier) a sequence $\mathcal{U}=\{U_n\}_{n\in\mathbb{N}}$
(ii) the algorithm incurs a cost of n to query U_n.
(thus, a polytime alg. on input x can query U_n

for any $n \leq \text{poly}(|x|)$.
(where a "query to U_n" is as in [*])

NB: classical oracles are a special case of quantum oracles.

Convention: For a language L, a query to L
is implemented via the unitary U that
acts as $U|x\rangle|b\rangle = |x\rangle|b \oplus L(x)\rangle$.

§ 2.7 Cryptography

Def^n 15 (Pseudorandom (quantum) states).

Def^n 16 (Pseudorandom unitary transform^n s)
[J LS '18]

Let • $\kappa \in \mathbb{N}$ be the security parameter
• $n(\kappa)$ be the # qubits in the quantum system.

A keyed family of n-qubit unitary transformations
$\{U_k\}_{k \in \{0,1\}^\kappa}$
is pseudorandom if
the following two conditions hold:

(1) (Efficient computation) There is a poly-time
quantum algorithm G that
implements U_k on input k,
i.e. for any n-qubit $|\psi\rangle$,
$G(k, |\psi\rangle) = U_k|\psi\rangle$.

(2) (computationally indistinguishability).

For any poly-time quantum algorithm $\mathcal{A}^U$ that queries n-qubit U, it holds that

$$\left| \Pr_{k \leftarrow \{0,1\}^\kappa} \left[\mathcal{A}^{U_k}(1^\kappa) = 1 \right] - \Pr_{U \leftarrow H_{2^n}} \left[\mathcal{A}^{U}(1^\kappa) = 1 \right] \right| \leq \mathrm{negl}(\kappa)$$

Remarks (quickened): (i) In this work, we take $n(\kappa) = \omega(\log \kappa)$ (even though the original def^ did not impose this), it turns out that $O(\log \kappa)$-gPRUs are more like classical output cryptographic objects: one can perform [BS20, AQY22, BEM24] tomography on them.

(also called "short PRUs")

(ii) Type of adversary $\mathcal{A}$ in Def^ 15 & 16

we consider non-uniform quant. alg. w/ classical advice.

i.e. a uniform poly(κ)-time q.alg. $\mathcal{A}(1^\kappa, x)$ where $x \in \{0,1\}^{\mathrm{poly}(\kappa)}$ is an advice string depending only on κ.

§ 2.2 Probability

Lemma 5 (Bayes decision rule). Let

can't do better than Bayes for guessing

Let X be a $\{0,1\}$-valued random variable, Y be a random variable (could depend on X) with domain D &

$f : D \to \{0,1\}$.

Then,

$$\Pr[f(Y) = X] \leq \Pr\left[\arg\max_x \Pr[X = x \mid Y] = X\right].$$

Lemma 6 (Borel-Cantelli [Bor 09, Can17])

Let $\{X_n\}_{n \in \mathbb{N}}$ be a sequence of (not necessarily independent) random variables w/ values in $\{0,1\}$.

If $$\sum_{n=1}^{\infty} \mathbb{E}[X_n] < \infty,$$

then $$\Pr\left[\sum_{n=1}^{\infty} X_n = \infty\right] = 0.$$

↗ A criterion under which at most finitely many of the events occur, w.p. 1.

§5 Pseudorandomness from a quantum oracle.

Story: We construct a quantum oracle $(\mathcal{U}, \mathcal{C})$
relative to which, Promise BQP = Promise QMA
&
PRUs exist.

We first describe the oracle
(divided into two parts)
$\mathcal{U}$: quantum oracle — $\mathcal{C}$: classical oracle (i.e. a language)

§5.1 Definition of the oracle

Oracle $\mathcal{U} := \{U_n\}_{n \in \mathbb{N}}$ where for each n,
$U_n \leftarrow M_{2^n}^{2^n}$
(i.e. U_n is a direct sum of 2^n different
n-qubit Haar random unitaries)

Language $\mathcal{C}$:
(Story: $\mathcal{C}$ is defined deterministically & independently of $\mathcal{U}$).
(Story: $\mathcal{C}$ is defined in stages: first we define $\mathcal{C}_4$ behaviour
on 1-bit strings,
then on 2-bit strings &
so on)

For a string x,
define $\mathcal{C}(x) = 1$ if all the following hold:

(1) x is a description of a quantum oracle circuit $V^{\bar{U},\mathcal{E}}(|\psi\rangle)$ that takes as input a quantum state $|\psi\rangle$, & makes queries to a quantum oracle $\bar{U}$ & the classical oracle $\mathcal{E}$.

(NB: $|\psi\rangle$ & $\bar{U}$ are not part of the description of V; they are aux inputs).

(2) V runs in time at most $|x|-1$.

(NB: This means $\mathcal{E}$ queries $\mathcal{E}$ on inputs of length at most $|x|-1$).

(3) the average acceptance prob. of V (viewed as a QMA verifier) is greater than $\frac{1}{2}$ (when averaged over $\bar{U} \leftarrow \Delta$), i.e.

$$\mathop{E}_{\bar{U}\leftarrow\Delta}\left[\max_{|\psi\rangle} \Pr\left[1 \leftarrow V^{\bar{U},\mathcal{E}}(|\psi\rangle)\right]\right] > \frac{1}{2}$$

NB1: Condition (2) guarantees that $\mathcal{E}$ is not defined circularly. ∵ Condition (3) ensures that the quantity in condition (3) depends only the previously constructed parts of the oracle $\mathcal{E}$.

NB2: We used $\bar{U}$ in our notation to emphasise that $\bar{U}$ is only used to take an average in the definition of $\mathcal{E}$ & is not the same as U.

§ 5.2 Promise BQP = Promise QMA relative to $(\mathcal{U}, e)$.

Story: We start with a lemma that says that
the acceptance prob. of a quantum query alg.
viewed as a function of the unitary matrix U
used in the query,
is Lipschitz.

Lemma 28. Let A^U be a quantum algorithm that
makes T queries to $U \in \mathbb{U}(D)$.

Define $f: \mathbb{U}(D) \to \mathbb{R}$ by

$$f(U) := \Pr[1 \leftarrow A^U].$$

Then, f is T-Lipschitz in the Frobenius norm.

Proof. Suppose $\|U - V\|_F \leq d$

$$\Rightarrow \|I \oplus U - I \oplus V\|_F \leq d \quad \text{& also,}$$

$$\|I \otimes U^+ - I \otimes V^+\|_F \leq d$$

(recall that controlled-U is $I \oplus U$ etc.)

Lemma 9 says (since $\|U(\cdot)U^+ - V(\cdot)V^+\|_\diamond \leq 2\|U - V\|_F$) then that the diamond distance b/w
controlled-U & controlled-V is
at most $2d$
(similarly for controlled-U^+ & controlled-V^+).

By the sub-additivity of the diamond norm under compositions
$\Rightarrow$ as super-operators $\|A^U - A^V\|_\diamond \leq 2Td$.

$TD(\mathcal{A}(\rho), \mathcal{B}(\rho)) \leq \frac{1}{2} \| \mathcal{A}(\cdot) - \mathcal{B}(\cdot) \|_\diamond$

By Fact 7, it follows that

$$|f(U) - f(V)| \leq T\delta.$$

□

Story: The next lemma extends Lemma 28 to QMA verifiers:

think of V as a QMA verifier that

received a witness $|\psi\rangle$

in which case

the lemma says that

the max. acceptance prob. of V is Lipschitz

w.r.t the queried unitary.

Lemma 29. Let $V^U(|\psi\rangle)$ be a quant. alg that makes

T queries to $U \in \mathbb{U}(D)$ &

takes as input a quant. state $|\psi\rangle$

on some fixed (but arbitrary)

number of qubits.

Define $f : \mathbb{U}(D) \to \mathbb{R}$ by

$$f(U) := \max_{|\psi\rangle} \Pr[1 \leftarrow V^U(|\psi\rangle)]$$

Then, f is T-Lipschitz in the Frobenius norm.

[Proof.

TODO: double check

NB: f is well defined because of the extreme value thm.

Define $f_\psi : \mathbb{U}(D) \to \mathbb{R}$ as

$$f_\psi(U) := \Pr[1 \leftarrow V^U(|\psi\rangle)].$$

NB2: $f(U) = \max_{|\psi\rangle} f_\psi(U)$.

NB3: Lemma 28 $\Rightarrow$ f_ψ is T-Lipschitz for every $|\psi\rangle$.

Let: $U, V \in \mathbb{U}(D)$.

Suppose: $|\phi\rangle$ & $|\psi\rangle$ are such that $f(U) = f_\psi(U)$ &
$f(V) = f_\varphi(V)$.

Then:
$$\begin{aligned} |f(U) - f(V)| &= |f_\psi(U) - f_\varphi(V)| \\ &= \max\{f_\psi(U) - f_\varphi(V), \\ &\qquad f_\varphi(V) - f_\psi(U)\} \end{aligned}$$
($\because |a-b| = \max\{a-b, b-a\}$)

$$\leq \max\{f_\psi(U) - f_\psi(V), \; f_\varphi(V) - f_\varphi(U)\}$$
($\because f_\psi(V) \leq f_\varphi(V)$, $f_\varphi(U) \leq f_\psi(U)$)

$$\leq T\|U - V\|_F$$
($\because$ f_ψ & f_φ are T-Lipschitz)

□

Story: We are now ready to prove the first main result.

Theorem 30. With prob. 1 over $U \leftarrow \mathbb{D}$,
$\mathrm{PromiseBQP}^{\mathcal{U},\mathcal{C}} = \mathrm{PromiseQMA}^{\mathcal{U},\mathcal{C}}$.

Proof Let $\Pi \in \mathrm{PromiseQMA}^{\mathcal{U},\mathcal{C}}$.

NB: This means (by Def^ 12),
$\exists$ a poly-time verifier $V^{\mathcal{U},\mathcal{C}}(x, |\psi\rangle)$
with completeness $\frac{2}{3}$ &
soundness $\frac{1}{3}$.

NB2: W.l.o.g. one can amplify the completeness prob. of V to $\frac{11}{12}$ & & soundness (prob. of V) to $\frac{1}{12}$.

Let: $p(n)$ be a polynomial upper bound on the running time of V on inputs x of length n.

Story: We now describe a Promise$BQP^{\mathcal{U},\mathcal{E}}$ alg. $A^{\mathcal{U},\mathcal{E}}(x)$ s.t. w.p. 1 over $\mathcal{U}$, A computes Π on all but finitely many inputs $x \in Dom(\Pi)$.

Construction of $A^{\mathcal{U},\mathcal{E}}(x)$:

(1) Let $d := \lfloor \log_2 (3456\,|x|\,p(|x|)^2 + 2) \rfloor$.

For each $n \in [d]$,

A performs process tomography on each $\mathcal{U}_n$, producing estimates $\tilde{\mathcal{U}}_n$ s.t.

$$\| \tilde{U}_n(\cdot)\tilde{U}_n^\dagger - U_n(\cdot)U_n^\dagger \|_\diamond \leq \frac{1}{6p(|x|)} \quad \forall n$$

w.p. at least $2/3$ (over randomness of A).

Denote the collection of these estimates by

$$\tilde{\mathcal{U}} := \{\tilde{\mathcal{U}}_n\}_{n\in[d]}.$$

(2) A constructs a description of a quantum oracle circuit $W^{\bar{\mathcal{U}},\mathcal{E}}_{x,\tilde{\mathcal{U}}}(|\psi\rangle)$ where x & $\tilde{\mathcal{U}}$ are hardcoded into the circuit, $|\psi\rangle$ is the input & $\bar{\mathcal{U}}$ & $\mathcal{E}$ are accessed as oracles.

The circuit $W^{\vec{u},\vec{\tilde{u}},c}_{x,\vec{\tilde{u}}}(|\psi\rangle)$ is defined as:

$V^{u,c}(x,|\psi\rangle)$ except for each $n \in [d]$, queries to u_n are replaced by $\tilde{u}_n$ & for each $n \in [p(|x|)] \setminus [d]$, queries to u_n are replaced by (those to) $\bar{u}_n$.

(3) A queries $C(x)$ & outputs the result.

Claim: We now show that for any $x \in Dom(\Pi)$ w.h.p. over u, A correctly decides Π on x i.e. $\Pr[A^{u,c}(x) = \Pi(x)] \geq 2/3$.

Not^n $(f(\vec{\tilde{u}}, \vec{\bar{u}}))$. Fix
- a fixed x,
- sequence of unitaries $\vec{\tilde{u}} = \{\tilde{u}_n\}_{n \in [d]}$ & $\vec{\bar{u}} = \{\bar{u}_n\}_{n \in [c(|x|)] \setminus [d]}$

$$f(\vec{\tilde{u}}, \vec{\bar{u}}) := \max_{|\psi\rangle} \Pr[W^{\vec{\bar{u}},c}(x, \vec{\tilde{u}}; |\psi\rangle) = 1].$$

NB: Using this not^n, A outputs 1 iff

$$\mathop{\mathbb{E}}_{\vec{\bar{u}} \leftarrow \mathcal{D}}[f(\vec{\tilde{u}}, \vec{\bar{u}})] > \frac{1}{2} \qquad [2]$$

(by how c was defined).

NB 2: The "QMA acceptance prob" of v clearly is (in this not^n)

$$f(u,u) = \max_{|\psi\rangle} \Pr[V^{u,c}(x,|\psi\rangle) = 1]. \quad [3]$$

Story: In effect, our goal is to show that Eq (2) is a good estimator for Eq (3).

: We do this in two steps

(i) replacing U in f's second argument with an arg over $\overline{U}$ approximately preserves the QMA acceptance prob.

(ii) we argue similarly when replacing U by its estimate $\widetilde{U}$ in f's first argument.

NB: By Lemma 29, f is $p(|x|)$-Lipschitz wrt the second argument $\overline{U}$ viewed as a direct sum of matrices

$$\overline{U} \equiv \bigoplus_{r=a+1}^{p(|x|)} \overline{U}_r$$

size of unitary matrices in each direct summand

NB2: Thm 10, w/ $N = 3456|x|p(|x|)^2 + 2$,

$L = p(|x|)$ — L-Lipschitz

$t = \frac{1}{12}$ — # direct summ.

applied to f yields that

$$\Pr_{U \leftarrow \Delta}\left[\left| f(U,U) - \mathop{\mathbb{E}}_{\overline{U} \leftarrow \Delta}\left[f(U,\overline{U})\right]\right| \geq \frac{1}{12}\right] \leq 2e^{\left(-\frac{(N-2)\,t^2}{24L^2}\right)}$$

$$= 2^{e^{-\frac{3456|x|p(|x|)^2 \cdot \frac{1}{144}}{24\,p(|x|)^2}}}$$

$$= 2e^{-|x|} \qquad [4]$$

(The factor of 2 appears: Thm 10 applies to one-sided error; here, we must use two sided errors $\therefore$ abs. value)

NB3: $\because$ W calls $\tilde{U}$ at most $p(|x|)$ times &

$\because$ diamond dist. b/w unitary channels is preserved under taking inverses,

Fact 7 implies that for any $|\psi\rangle$

$$\left| \Pr\left[1 \leftarrow W^{\tilde{U},\varepsilon}_{x,\tilde{U}}(|\psi\rangle)\right] - \Pr\left[1 \leftarrow W^{U,\varepsilon}_{x,U}(|\psi\rangle)\right] \right| \leq \frac{p(|x|)}{2} \left\| \tilde{U}_x(\cdot)\tilde{U}_n^\dagger - U_n(\cdot)U_n^\dagger \right\|_\diamond$$

NB4: $\left| f(\tilde{U},\bar{U}) - f(U,\bar{U}) \right| = \left| \max_{|\psi\rangle} \Pr\left[1 \leftarrow W^{\bar{U},\varepsilon}_{x,\tilde{U}}(|\psi\rangle)\right] - \max_{|\psi\rangle} \Pr\left[1 \leftarrow W^{\bar{U},\varepsilon}_{x,U}(|\psi\rangle)\right] \right|$

($\because$ $|\max_\psi a(\psi) - \max_\psi b(\psi)| \leq \max_\psi |a(\psi) - b(\psi)|$.

Suppose: $a(\psi_a) \geq b(\psi_b)$ where ψ_a, ψ_b are argmaxs.

Then: $a(\psi_a) - b(\psi_b) \leq a(\psi_a) - b(\psi_a)$

$\leq \max_\psi |a(\psi) - b(\psi)|$

Similarly: if $b(\psi_b) \geq a(\psi_a)$ an argument analogously.)

$$\leq \frac{p(|x|)}{2} \left\| \tilde{U}_x(\cdot)\tilde{U}_n^\dagger - U_n(\cdot)U_n^\dagger \right\|_\diamond$$

& thus, by Jensen's inequality,

$$\left| \mathop{\mathbb{E}}_{\tilde{U}\leftarrow\mathcal{D}} \left[f(\tilde{U},\bar{U}) \right] - \mathop{\mathbb{E}}_{U\leftarrow\mathcal{D}} \left[f(U,\bar{U}) \right] \right| \leq \frac{p(|x|)}{2} \left\| \tilde{U}_n(\cdot)\tilde{U}_n^\dagger - U_n(\cdot)U_n^\dagger \right\|_\diamond$$

Recall: The estimates $\tilde{U}_n$ satisfy $\left\| \tilde{U}_n(\cdot)\tilde{U}_n^\dagger - U_n(\cdot)U_n^\dagger \right\|_\diamond \leq \frac{1}{6p(|x|)}$

w.p. at least $\frac{2}{3}$ (over the randomness of $\mathcal{A}$)

NB5: $\Pr_{\mathcal{A}}\left[\left| \mathop{\mathbb{E}}_{\tilde{U}\leftarrow\mathcal{D}} \left[f(U,\bar{U}) \right] - \mathop{\mathbb{E}}_{U\leftarrow\mathcal{D}} \left[f(\tilde{U},\bar{U}) \right] \right| \geq \frac{1}{12} \right] \leq \frac{1}{3}.$

Recall: Eq [4]: $\Pr_{U\leftarrow\mathcal{D}}\left[\left| f(U,U) - \mathop{\mathbb{E}}_{U\leftarrow\mathcal{D}} \left[f(U,\bar{U}) \right] \right| \geq \frac{1}{12} \right] \leq 2e^{-|x|}$

Eq [2]: $\mathcal{A}$ outputs 1 iff $\mathop{\mathbb{E}}_{U\leftarrow\mathcal{D}} \left[f(\tilde{U},\bar{U}) \right] > \frac{1}{2}$

Conclusion: Except with prob. $2e^{-|x|}$ over $\mathcal{U}$,

$$\Pi(x)=1 \Rightarrow \left\{ f(\mathcal{U},\mathcal{U}) \geq \frac{11}{12} \Rightarrow \Pr\left[\mathcal{A}^{\mathcal{U},C}(x)=1\right] \geq \frac{2}{3} \right\}$$

$$\Pi(x)=0 \Rightarrow \left\{ f(\mathcal{U},\mathcal{U}) \leq \frac{1}{12} \Rightarrow \Pr\left[\mathcal{A}^{\mathcal{U},C}(x)=0\right] \geq \frac{2}{3} \right\}$$

$f(\mathcal{U},\mathcal{U}) \leq \frac{1}{12} \Rightarrow \left| \mathop{\mathbb{E}}_{\vec{\mathcal{U}}\to\mathcal{D}} f(\vec{u},\vec{u}) \right| \geq \frac{1}{6} - \frac{1}{12}$ w.p. $1/3$

$\geq \frac{1}{12}$ w.p. $1/3$

$|a-b| \geq c$

$\max\{(a-b),(b-a)\} \geq c$ $\leq \frac{1}{12}$, i.e. out 0 w.p. $2/3$

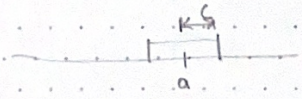
$\max\{a-b-c,\ b-a-c\} \geq 0$

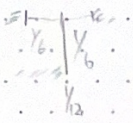
$\max\{(a-c)-b,\ b-(a+c)\} \geq 0$ $b \in [a-c, a+c]$; if $a \geq a^*$, $c \geq 0$

$f(\mathcal{U},\mathcal{U}) \geq \frac{11}{12}$ $b \geq \frac{1}{6} - \frac{1}{12}$ $b \geq a^* - c$

use negative

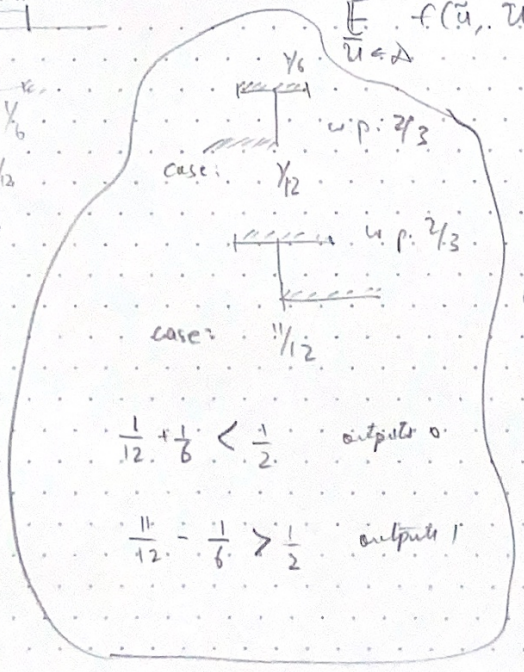
$$\Pr_{\mathcal{A}}\left[\left|f(\mathcal{U},\mathcal{U}) - \mathop{\mathbb{E}}_{\vec{\mathcal{U}}\to\mathcal{D}}\left[f(\vec{u},\vec{u})\right]\right| \leq \frac{1}{6}\right] \geq 2/3$$





case: $a \leq \frac{1}{12}$;

b



$\mathop{\mathbb{E}}_{\vec{\mathcal{U}}\to\mathcal{D}} f(\vec{u},\vec{u}) \leq \frac{1}{6} - \frac{11}{12}$

$\leq \frac{2}{12} - \frac{11}{12}$

if $a \leq a^*$, $c \geq 0$

$b \leq a^* + c$

$\leq \frac{11}{12} + \frac{1}{6}$

$=$

$b \geq \frac{11}{12} - \frac{1}{6}$

NB: By Borel-Cantelli (Lemma 6),

$$\sum_x \mathbb{E}[X_x] < \infty \quad \Rightarrow \quad \Pr\left[\sum_x X_x = \infty\right] = 0$$

(X_x indicates whether x was decided correctly by A)

$$\left(\because \sum_{i=1}^{\infty} 2^i \cdot 2e^{-i} = \frac{4}{e-2} < \infty \quad \text{(geometric series)}\right)$$

(2^i: # possible instances; $2e^{-i}$: failure)

i.e. A correctly decides $\Pi(x)$ for all but finitely many $x \in \mathrm{Dom}(\Pi)$ w.p. 1 over $\mathcal{U}$.

NB2: Thus, w.p. 1 over $\mathcal{U}$, A can turned into A' that agrees with Π on every $x \in \mathrm{Dom}(\Pi)$, by simply hard-coding those x's on which A & Π disagree.

NB3: $\because$ there are only countably many PromiseQMA$^{\mathcal{U},c}$ machines, one can union bound over all $\Pi \in$ PromiseQMA$^{\mathcal{U},c}$ to conclude that

$$\text{PromiseQMA}^{\mathcal{U},c} \subseteq \text{PromiseBQP}^{\mathcal{U},c}$$

w.p. 1.

(Q: why union bound is for the errors

$\Pr(\text{any one fails}) \leq \sum_{\Pi} \Pr[\text{fails on } \Pi]$

$\Big\Downarrow$

0)

□