CONJURA · OPEN PROBLEM

Polynomial Compatibility for Low-Degree, Low-Influence Distributions

The inverse-polynomial influence regime, over some finite abelian group

Status. Statement: AI-written from Kai-Min Chung, Yao-Ting Lin, Mohammad Mahmoody, *Black-Box Separations for Non-Interactive Commitments in a Quantum World*, Cryptology ePrint Archive, Report 2023/570, 2023, not yet checked by a human. The analogous statement with exponentially small influences, $\delta(d) = \exp(-d)$, is proved in the work of Austrin et al. that introduced the conjecture, while the inverse-polynomial regime $\delta(d) = 1/\mathrm{poly}(d)$ recorded here is open; since the group is existentially quantified, a proof for any one finite abelian group (for instance $\mathbb{Z}_2$) settles it affirmatively, whereas a refutation must rule out every finite abelian group.

Category. *Quantum Cryptography.*

Conjecture (informal). *Fix a finite abelian group and look at complex-valued functions on N-tuples of its elements, normalized so that the average squared magnitude is one. Every such function expands uniquely in the characters of the group; its degree is the largest number of coordinates that any character with a non-zero coefficient actually depends on, and the influence of a coordinate is the total Fourier weight sitting on characters that touch that coordinate. Now take two probability distributions over such functions, both supported only on normalized functions of degree at most d, and both so spread out that every single coordinate carries influence at most δ on average over the distribution. The conjecture asserts that for some finite abelian group there is a threshold δ that is only inverse-polynomially small in d — crucially, independent of the number of coordinates N — beyond which the two distributions must be compatible: you can pick one function from the support of each and a single input point at which both are non-zero. Equivalently, low degree together with low average influence prevents two distributions of functions from having systematically interlocking zero sets. The exponentially-small-influence version of this is known; the inverse-polynomial version is what is open, and it is exactly what several black-box impossibility results in quantum cryptography currently rest on, including the impossibility of building non-interactive commitments from one-way functions when communication is classical.*

1 The setting

Black-box separations in the quantum setting are proved by exhibiting an oracle relative to which the assumed primitive survives but the target primitive is broken by a polynomial-query adversary. In the classical setting, the separation of non-interactive commitments from one-way functions [MP12] plays two oracle distributions against each other: either a cheating receiver learns enough ε-heavy queries of the sender to guess the committed bit, or one can fix a partial oracle consistent with two openings $\mathsf{dec}_0, \mathsf{dec}_1$ of the same commitment, and partially fixed random oracles are still one-way.

Moving to quantum senders breaks the second step: one cannot record a superposition query, so "the set of oracle positions the sender asked" is no longer a partial function. The route found by

Austrin, Chung, Chung, Fu, Lin and Mahmoody [ACC22] is to work with the purified view of the honest party in the quantum random oracle model and to represent the oracle register in the Fourier basis, following Zhandry's compressed-oracle technique [Zha19]. A d-query algorithm then has a sparse Fourier representation, and each branch of the purified sender turns into a *distribution over degree-d, unit-norm, low-influence functions* on the oracle domain; "heavy" queries are exactly those carrying non-negligible Fourier weight, and after learning all of them the remaining influences are small. Two openings of the same commitment are simultaneously realisable precisely when one can find a function in the support of each branch's distribution together with a point where both are non-zero. That combinatorial statement is the Polynomial Compatibility Conjecture, and [ACC22] isolated it and proved it in the regime of exponentially small influences.

The present paper [CLM23] uses the conjecture to rule out quantum black-box constructions of non-interactive commitments from post-quantum one-way functions in the quantum-computation classical-communication model, and in fact in the stronger classical-commitment quantum-decommitment model, for perfectly complete schemes and for a very weak notion of binding. Boosting a single compatible oracle to a large *set* of compatible oracles is done with the Donoho–Stark support-size uncertainty principle [DS89] in place of Schwartz–Zippel, and the resulting set is shown one-way against quantum-advice adversaries by adapting the multi-instance time–space tradeoff machinery of [CGLQ20]. The consequences are sharp: since injective one-way functions imply non-interactive commitments in a black-box way [GL89], the result yields a separation of injective one-way functions from one-way functions with fully quantum constructions, improving [CX21] which allowed only the security reduction to be quantum, and it complements the positive result of [BB21] that a *quantum* commitment with a classical decommitment does follow from post-quantum one-way functions. All of this is conditional. The conjecture stated here is the condition, and its inverse-polynomial regime remains unproved; the paper notes its kinship with the Aaronson–Ambainis conjecture [AA09], which is also known only for exponentially small influences, and quantum black-box separations of this shape go back to [HY20].

Progress to date. The originating work proves the conjecture

when the average-influence bound is exponentially small in the degree, $\delta(d) = \exp(-d)$, and the present paper reports this as the evidence for the conjecture's validity. The paper also records that the conjecture is close in spirit to the Aaronson–Ambainis conjecture on low-degree low-influence polynomials, which is likewise only known for exponentially small influences. The present paper makes no attempt on the conjecture itself; it consumes it (via an equivalent formulation in terms of $(\mathcal{Y}, \delta, d, N)$-quantum states and a conversion lemma) and independently proves the unconditional half of its argument, namely that oracles sampled from sufficiently large sets of functions are one-way against polynomial-query quantum adversaries holding polynomial-size quantum advice.

Why it matters. This single Fourier-analytic statement is the only thing standing between a family of quantum black-box separations and unconditional status. If it is true: there is no quantum black-box construction of non-interactive commitments from post-quantum one-way functions when the commitment message is classical (even allowing a quantum decommitment), hence no black-box construction of injective one-way functions from general one-way functions even with fully quantum constructions, hence a separation between non-interactive commitments and pseudorandom states in the classical-commitment/quantum-decommitment model; and, from the originating work, no perfectly complete key agreement in the quantum-computation classical-communication model from one-way functions. If it is false, all of those attacks lose their combinatorial engine, and the pressing question becomes whether the QCCC constructions the separations rule out actually exist. Either resolution changes what is known, and the statement itself is a clean question about discrete Fourier analysis that is refutable by an explicit pair of distributions.

2 Notation and parameters

- $\mathcal{Y}$ is a finite abelian group, and $\widehat{\mathcal{Y}}$ is its dual group, whose elements are the characters $\chi : \mathcal{Y} \to \mathbb{C}^{\times}$; the trivial character is written $\hat{0}$.
- $N \in \mathbb{N}$ is the number of coordinates, $[N] = \{1, \ldots, N\}$, and an input is $x = (x_1, \ldots, x_N) \in \mathcal{Y}^N$.

- For $\chi = (\chi_1, \ldots, \chi_N) \in \widehat{\mathcal{Y}^N}$ we write $\chi(x) := \prod_{i=1}^{N} \chi_i(x_i)$. These $|\mathcal{Y}|^N$ functions form an orthonormal basis for the space of functions $\mathcal{Y}^N \to \mathbb{C}$ under the inner product $\langle f, g \rangle := \mathbb{E}_{x \leftarrow \mathcal{Y}^N}[f(x)\overline{g(x)}]$, so every $f : \mathcal{Y}^N \to \mathbb{C}$ has a unique Fourier expansion $f = \sum_{\chi \in \widehat{\mathcal{Y}^N}} \hat{f}(\chi)\,\chi$ with coefficients $\hat{f}(\chi) \in \mathbb{C}$.

- $\|f\|_2 := \left(\mathbb{E}_{x \leftarrow \mathcal{Y}^N} |f(x)|^2\right)^{1/2}$, the ℓ_2-norm with respect to the uniform distribution on $\mathcal{Y}^N$.

- $d \in \mathbb{N}$ is a degree bound and $\delta \in (0, 1]$ an influence bound; $\deg(\cdot)$ and $\mathrm{Inf}_i(\cdot)$ are as in Definition 1 below.

- $\mathbf{F}, \mathbf{G}$ denote probability distributions over functions $\mathcal{Y}^N \to \mathbb{C}$, and $\mathrm{supp}(\mathbf{F})$ denotes the support of $\mathbf{F}$, i.e. the set of functions to which $\mathbf{F}$ assigns non-zero probability. Expectations $\mathbb{E}_{f \leftarrow \mathbf{F}}[\cdot]$ are over f drawn from $\mathbf{F}$.

Parameters.

- $\mathcal{Y}$ — the finite abelian group over which the functions are defined. Existentially quantified: a single group suffices. The paper's own application is presented for $\mathcal{Y} = \mathbb{Z}_2$ but goes through for whichever group witnesses the conjecture.

- N — the number of coordinates (the ambient dimension). Universally quantified, and the influence threshold must not depend on it — this is the crux of the difficulty.

- d — the degree bound on every function in the support of both distributions. In the intended application d is governed by the number of quantum oracle queries made by the honest party, hence polynomial in the security parameter.

- $\delta(d)$ — the threshold on the average influence of each coordinate. The open regime is $\delta(d) = 1/\mathrm{poly}(d)$; the case $\delta(d) = \exp(-d)$ is already proved in the prior work that introduced the conjecture.

- $\mathbf{F}, \mathbf{G}$ — the two distributions over functions. In the application they arise as state polynomial distributions of the two branches (committing to 0 and to 1) of a purified honest sender in the quantum random oracle model.

3 The conjecture

Definition 1 (degree and influence over a finite abelian group). Let $\mathcal{Y}$ be a finite abelian group and let $f : \mathcal{Y}^N \to \mathbb{C}$ have Fourier expansion $f = \sum_{\chi \in \widehat{\mathcal{Y}}^N} \hat{f}(\chi)\,\chi$.

- The *degree* of a character $\chi = (\chi_1, \ldots, \chi_N) \in \widehat{\mathcal{Y}}^N$ is $\deg(\chi) := \big|\{i \in [N] \;:\; \chi_i \neq \hat{0}\}\big|$, and the *degree* of f is

$$\deg(f) := \max\big\{\deg(\chi) \;:\; \hat{f}(\chi) \neq 0\big\},$$

  with $\deg(f) := 0$ when f is identically zero.

- The *influence* of coordinate $i \in [N]$ on f is

$$\mathrm{Inf}_i(f) := \sum_{\substack{\chi \in \widehat{\mathcal{Y}}^N \\ \chi_i \neq \hat{0}}} \big|\hat{f}(\chi)\big|^2.$$

For $\mathcal{Y} = \mathbb{Z}_2$ these specialise to the usual notions for multilinear polynomials $f = \sum_{S \subseteq [N]} \alpha_S \prod_{i \in S} x_i$ over variables $x_i \in \{\pm 1\}$, namely $\deg(f) = \max_{\alpha_S \neq 0} |S|$ and $\mathrm{Inf}_i(f) = \sum_{S \ni i} \alpha_S^2$.

Conjecture 1 (polynomial compatibility). *There exist a finite abelian group $\mathcal{Y}$, constants $c_1 \in (0,1]$ and $c_2 > 0$, and a function $\delta : \mathbb{N} \to (0,1]$ satisfying $\delta(d) \geq c_1\, d^{-c_2}$ for all $d \geq 1$ — equivalently, $\delta(d) \geq 1/p(d)$ for some polynomial p — such that for every $d \in \mathbb{N}$ and every $N \in \mathbb{N}$ the following holds.*
Let $\mathbf{F}$ and $\mathbf{G}$ be any two probability distributions over functions $\mathcal{Y}^N \to \mathbb{C}$ such that:

- unit ℓ_2 norm: $\|f\|_2 = 1$ *for every* $f \in \mathrm{supp}(\mathbf{F})$ *and* $\|g\|_2 = 1$ *for every* $g \in \mathrm{supp}(\mathbf{G})$*;*

- degree at most d: $\deg(f) \leq d$ *for every* $f \in \mathrm{supp}(\mathbf{F})$ *and* $\deg(g) \leq d$ *for every* $g \in \mathrm{supp}(\mathbf{G})$*;*

- δ-influences on average: *for every* $i \in [N]$,

$$\mathop{\mathbb{E}}_{f \leftarrow \mathbf{F}}\left[\mathrm{Inf}_i(f)\right] \leq \delta(d) \quad \textit{and}$$
$$\mathop{\mathbb{E}}_{g \leftarrow \mathbf{G}}\left[\mathrm{Inf}_i(g)\right] \leq \delta(d).$$

Then there exist $f \in \mathrm{supp}(\mathbf{F})$, $g \in \mathrm{supp}(\mathbf{G})$, *and* $x \in \mathcal{Y}^N$ *such that*

$$f(x) \cdot g(x) \neq 0.$$

Remark 1 (what the quantifiers do and do not allow). Note that δ is allowed to depend on d but not on N, and that the group $\mathcal{Y}$ is existentially quantified: exhibiting a single finite abelian group for which the above holds settles the conjecture affirmatively.

4 Bibliography

[AA09] S. Aaronson, A. Ambainis. *The need for structure in quantum speedups.* arXiv preprint arXiv:0911.0996, 2009.

[ACC22] P. Austrin, H. Chung, K.-M. Chung, S. Fu, Y.-T. Lin, M. Mahmoody. *On the impossibility of key agreements from quantum random oracles.* Annual International Cryptology Conference (CRYPTO), 2022.

[BB21] N. Bitansky, Z. Brakerski. *Classical binding for quantum commitments.* Theory of Cryptography Conference, pages 273–298, Springer, 2021.

[CGLQ20] K.-M. Chung, S. Guo, Q. Liu, L. Qian. *Tight quantum time-space tradeoffs for function inversion.* 61st Annual Symposium on Foundations of Computer Science (FOCS), pages 673–684, IEEE Computer Society Press, 2020.

[CLM23] K.-M. Chung, Y.-T. Lin, M. Mahmoody. *Black-Box Separations for Non-Interactive Commitments in a Quantum World.* Cryptology ePrint Archive, Report 2023/570, 2023 (report number and year taken from the harvested filename, not printed on the page). [UNVERIFIED]

[CX21] S. Cao, R. Xue. *Being a permutation is also orthogonal to one-wayness in quantum world: Impossibilities of quantum one-way permutations from one-wayness primitives.* Theoretical Computer Science, 855:16–42, 2021.

[DS89] D. L. Donoho, P. B. Stark. *Uncertainty principles and signal recovery.* SIAM Journal on Applied Mathematics, 49(3):906–931, 1989.

[GL89] O. Goldreich, L. A. Levin. *A hard-core predicate for all one-way functions.* 21st Annual ACM Symposium on Theory of Computing (STOC), pages 25–32, ACM Press, 1989.

[HY20] A. Hosoyamada, T. Yamakawa. *Finding collisions in a quantum world: Quantum black-box separation of collision-resistance and one-wayness.* Advances in Cryptology — ASIACRYPT 2020, Part I, volume 12491 of LNCS, pages 3–32, Springer, 2020.

[MP12] M. Mahmoody, R. Pass. *The curious case of non-interactive commitments — on the power of black-box vs. non-black-box use of primitives.* Advances in Cryptology — CRYPTO 2012, volume 7417 of LNCS, pages 701–718, Springer, 2012.

[Zha19] M. Zhandry. *How to record quantum queries, and applications to quantum indifferentiability.* Advances in Cryptology — CRYPTO 2019, Part II, volume 11693 of LNCS, pages 239–268, Springer, 2019.