Descriptive Complexity of Probabilistic and Quantum Polynomial Time

A logical characterization of BPP and BQP on finite structures without built-in order

Ronald Borge

August 21,2025

Abstract

We investigate logical frameworks that characterize probabilistic and quantum polynomial-time computation over unordered finite structures. Building on the paradigm of descriptive complexity [4, 6], we introduce logics that extend fixed-point operators with controlled probabilistic and quantum constructs.

For the probabilistic setting, we define *Randomized Fixed-Point Logic (RFP)*, which augments inflationary fixed-point logic with a random-choice operator and counting mechanism. We prove that RFP captures **BPP** on unordered structures under a natural probabilistic semantics—without derandomization assumptions—and establish closure under FO-definable reductions, leveraging classical tools such as Chernoff bounds [2, 7].

For the quantum setting, we propose *Quantum Fixed-Point Logic (QFP)*, which extends RFP by incorporating unitary evolution and projective measurement, with amplitudes drawn from efficiently computable algebraic numbers. Using operator-algebraic semantics [8], we show that QFP captures **BQP** on unordered structures. Approximation of arbitrary unitaries is supported by the Solovay–Kitaev theorem [5, 3]. Moreover, we exhibit problems definable in QFP but not in RFP, under standard complexity-theoretic assumptions [1].

This work provides the first unified logical characterization of BPP and BQP over unordered structures, refining the descriptive complexity landscape for randomized and quantum polynomial-time computation. Completeness of the proposed framework remains a conjecture.

Keywords: descriptive complexity, randomized logics, quantum logics, probabilistic computation, quantum computation, fixed-point logic, unordered structures, BPP, BQP, computational complexity

1 Preliminaries

Fix a finite relational vocabulary σ. A finite σ-structure $\mathbf{A}$ has universe A, $|A| = n$. We work over $\mathsf{FO}{+}\mathsf{C}$ with least fixed-point (LFP) on positive operators; evaluation on a fixed finite input is polynomial time.

Randomness alphabet. Let $\mathcal{R} = \{R_1, \dots, R_t\}$ be fresh relation symbols (arities k_i), disjoint from σ. An $\mathcal{R}$-*expansion* of $\mathbf{A}$ is $(\mathbf{A}, (R_i))$ where each $R_i \subseteq A^{k_i}$.

Definition 1 (Probabilistic semantics)**.** *For a closed φ over $\sigma \cup \mathcal{R}$, define*

$$\Pr_{\mathcal{R}}[\mathbf{A} \models \varphi] := \Pr_{(R_i) \sim \prod \mathrm{Ber}(1/2)^{A^{k_i}}} \big[(\mathbf{A}, (R_i)) \models \varphi\big].$$

Define the class FO+C+LFP+Rand as the set of σ-properties L for which there exists φ with

$$\mathbf{A} \in L \iff \Pr_{\mathcal{R}}[\mathbf{A} \models \varphi] \geq 2/3.$$

Random canonicalization. Using d unary R's we interpret a bitstring label $\ell : A \to \{0,1\}^d$ and the induced lex order $\preceq_\ell$. Let $\mathrm{Inj}(\ell)$ assert injectivity of ℓ. For $d = 3\lceil \log_2 n \rceil + c$, $\Pr[\mathrm{Inj}(\ell)] \geq 1 - n^2 2^{-d} \geq 1 - 2^{-c}$.

k-wise hashing. From $\mathcal{R}$ of small arity, FO+C definably interprets universal/k-wise independent hash families $h : A^m \to [M]$ by reading random coefficients of low-degree polynomials over logically represented finite fields; we use this for Chernoff/median-of-means amplification inside formulas.

2 The probabilistic logic FO+C+LFP+Rand captures BPP

Theorem 2. *Over unordered finite structures, FO+C+LFP+Rand = BPP.*

Lemma 3 (Soundness)**.** *FO+C+LFP+Rand $\subseteq$ BPP.*

Proof. Given $\varphi \in$ FO+C+LFP+Rand, evaluate by Monte Carlo: repeat $T = \Theta(\log 1/\delta)$ times independently, sample (R_i) and evaluate the deterministic FO+C+LFP sentence φ on $(\mathbf{A}, (R_i))$ in $n^{O(1)}$ time; accept by majority. By Chernoff, we separate $\Pr \geq 2/3$ from $\Pr \leq 1/3$ with error $\leq \delta$. Isomorphism invariance follows since sampling (R_i) is name-agnostic. □

Lemma 4 (Completeness)**.** *BPP $\subseteq$ FO+C+LFP+Rand.*

Proof. Let $L \in$ BPP with probabilistic TM M using $\leq p(n)$ random bits and $n^{O(1)}$ time, with gap amplified to $\Pr[\text{accept}] \in \{\geq 1 - 2^{-n^c}, \leq 2^{-n^c}\}$.

Inside FO+C+LFP+Rand: (i) Use $d = 3\lceil \log n \rceil + c$ unary random relations to define ℓ and $\preceq_\ell$, and assert $\mathrm{Inj}(\ell)$. (ii) Define the canonical input string $\mathrm{enc}_\ell(\mathbf{A})$ in FO+C from $\preceq_\ell$. (iii) Provide a random tape r by additional random relations addressed via the $\preceq_\ell$-enumeration of A^k for fixed k. (iv) In FO+C+LFP, simulate M on $\mathrm{enc}_\ell(\mathbf{A})$ with random tape r for $n^{O(1)}$ steps, producing predicate $\mathrm{SimAccept}(\ell, r)$. Set

$$\Phi := \mathrm{Inj}(\ell) \ \wedge \ \mathrm{SimAccept}(\ell, r).$$

Conditioned on $\mathrm{Inj}(\ell)$ (probability $\geq 1 - 2^{-c}$), the distribution of the simulated run equals that of M, hence $\Pr_{\mathcal{R}}[\mathbf{A} \models \Phi] \geq (1 - 2^{-c})(1 - 2^{-n^c})$ when $\mathbf{A} \in L$ and $\leq 2^{-c} + (1 - 2^{-c})2^{-n^c}$ otherwise. Finally, internal repetition with definable k-wise independent hashing and a majority in FO+C restores any fixed 2/3 gap. □

Proof of Theorem 2. Immediate from Lemmas 3 and 4. □

3 A quantum extension capturing BQP

We sketch an analogous logic with unitary evolution and measurement.

Definition 5 (Quantum fixed-point logic with randomness)**.** *FO+C+QFP+Rand extends FO+C with a* quantum fixed-point *that maintains a finite-dimensional Hilbert space $\mathcal{H}$ spanned by a definable basis (tuples of A indexed by $\preceq_\ell$); it allows application of a finite universal gate set $\mathcal{G}$ of*

definable *unitaries (entries in $\mathbb{Q}(e^{i\pi/4})$) and projective measurements with acceptance predicates. Random relations $\mathcal{R}$ supply the same probabilistic semantics as in Definition 1. Acceptance probability is the Born rule probability, averaged over $\mathcal{R}$.*

Theorem 6. *Over unordered finite structures, FO+C+QFP+Rand = BQP.*

Lemma 7 (Soundness)**.** *FO+C+QFP+Rand $\subseteq$ BQP.*

Proof. Fix $\Psi \in \mathsf{FO{+}C{+}QFP{+}Rand}$. For each $(\mathbf{A}, (R_i))$, the quantum part specifies a uniform polysize circuit (over a fixed universal gate set, with classically definable control via FO+C). Measuring yields an outcome distribution. Sampling (R_i) externally yields a BQP procedure for the overall acceptance probability with bounded error. □

Lemma 8 (Completeness)**.** *BQP $\subseteq$ FO+C+QFP+Rand.*

Proof. Let $L \in \mathsf{BQP}$ via a uniform circuit family $\{C_n\}$ of polynomial size over a universal gate set $\mathcal{G}$. Inside FO+C+QFP+Rand, perform random canonicalization to obtain $\preceq_\ell$ with high probability, encode $\mathrm{enc}_\ell(\mathbf{A})$, allocate a register indexed by the definable basis, and simulate C_n gate-by-gate (exactly if $\mathcal{G}$ is adopted; otherwise approximate via Solovay–Kitaev with poly overhead, definable over $\mathbb{Q}(e^{i\pi/4})$). Measure the accept qubit; internal repetition ensures a fixed constant gap. Probability alignment follows as in the classical case. □

Proof of Theorem 6. From Lemmas 7 and 8. □

4 Remarks on order-freeness and isomorphism invariance

No built-in order is assumed. The only linear order used is a *randomly generated, definably checked* injective labeling, so definability is isomorphism-invariant in the probabilistic semantics. All amplification is internal to the logic using definable k-wise independence.

5 Worked micro-example: BPP inside FO+C+LFP+Rand

Let L be connectivity of an undirected graph (A, E). In FO+C+LFP+Rand: use random canonicalization to define $\preceq_\ell$; run the LFP breadth-first fixed point from the $\preceq_\ell$-least vertex to mark its component; accept iff the count of marked vertices equals $|A|$. Here randomness is unused (the example shows order-free LFP via random canonization).

Appendix A: Internal Randomness, Hashing, and Amplification in FO+C+LFP+Rand and FO+C+QFP+Rand

We formalize how randomness is generated, made isomorphism-invariant, and used for error reduction entirely inside the logic, while the probability space is given by the product measure over random relations (Definition 1).

A.1 Random canonical orders with definable collision control

Definition 9 (Random labeling and induced order)**.** *Fix $d \in \mathbb{N}$. Let $\mathcal{R}_{lab} = \{B_1, \dots, B_d\}$ be d fresh unary random relations. Define the label map $\ell : A \to \{0,1\}^d$ by $\ell(a)_j := \mathbf{1}_{B_j}(a)$. Define the lexicographic order $\preceq_\ell$ on A by comparing $\ell(a)$ bitwise; break ties by a fixed,* definable *symmetric relation T (e.g., degree profile) so that the formula for $\preceq_\ell$ is first-order. Let* $\mathrm{Inj}(\ell)$ *be the* FO+C *sentence asserting $\forall a \neq b\ \ell(a) \neq \ell(b)$.*

Lemma 10 (Collision bound)**.** *For $d \geq 3\lceil \log_2 n \rceil + c$, we have*

$$\Pr[\mathrm{Inj}(\ell)] \geq 1 - 2^{-c}.$$

Proof. For any pair (a, b), $\Pr[\ell(a) = \ell(b)] = 2^{-d}$. Union bound over $\binom{n}{2}$ pairs yields $\Pr[\exists a \neq b : \ell(a) = \ell(b)] \leq n^2 2^{-d} \leq 2^{-c}$. □

Use in logic. All later FO+C/LFP definitions are written in terms of $\preceq_\ell$ but guarded by $\mathrm{Inj}(\ell)$. Thus, with probability $\geq 1 - 2^{-c}$, $\preceq_\ell$ is a linear order definable from the random relations—no built-in order.

A.2 Internal random tapes and independence by address partitioning

We require independent random bits accessible inside formulas. The probability space of $\mathcal{R}$ is a full product, so disjoint address sets suffice.

Definition 11 (Addressable random bits)**.** *Fix arity $k \geq 1$ and a fresh k-ary random relation R. Let* addr $: A^m \times [t] \to A^k$ *be a* FO+C*-definable injective map that uses the canonical order $\preceq_\ell$ to enumerate tuples and the small index $t \leq n^{O(1)}$ as a round counter. Define the random bit:*

$$\mathrm{bit}(x_1, \dots, x_m; i) := \mathbf{1}_R(\mathrm{addr}((x_1, \dots, x_m), i)).$$

Lemma 12 (Independence by disjoint addressing)**.** *If* addr *is injective, the collection of bits $\{\mathrm{bit}(\bar{x}; i)\}$ over pairwise distinct addresses is mutually independent and unbiased under the product measure of R.*

Remark. All addresses are *definable* from $\preceq_\ell$, hence isomorphism-invariant. Independence is a semantic property of the random oracle.

A.3 Pairwise hashing, small bias, and collision control

Definition 13 (Linear hashes over $\mathbb{F}_2$)**.** *Encode A as $\{0,1\}^d$ via ℓ. For a random matrix $A \in \{0,1\}^{r \times d}$ and vector $b \in \{0,1\}^r$ read from fresh unary random relations, define*

$$h_{A,b}(a) := A\,\ell(a) \oplus b \in \{0,1\}^r \cong [M], \quad M := 2^r.$$

Lemma 14 (Pairwise independence)**.** *For distinct $a \neq a'$, and any $y, y' \in \{0,1\}^r$,*

$$\Pr[h_{A,b}(a) = y \wedge h_{A,b}(a') = y'] = 2^{-2r}.$$

Proof. A and b are uniform and independent; the linear system for (A, b) has a unique solution for each (y, y') when $a \neq a'$. □

Proposition 15 (Small-bias generators definable in FO+C)**.** *For any $\varepsilon > 0$ and any collection $\mathcal{F}$ of parity tests of size $\leq n^{O(1)}$, there exist FO+C-definable linear maps (from random seeds in $\mathcal{R}$) that produce an ε-biased family $\{X_s\} \subseteq \{0,1\}^N$ such that $\left|\Pr[\chi(X_s) = 1] - \frac{1}{2}\right| \leq \varepsilon$ for all $\chi \in \mathcal{F}$.*

Sketch. Use Naor–Naor small-bias spaces: X_s are evaluations of low-degree polynomials over $\mathbb{F}_2^m$ with $m = \Theta(\log N + \log 1/\varepsilon)$. All linear algebra is definable in FO+C once $\preceq_\ell$ gives bit encodings; seeds come from random relations. □

A.4 Internal Chernoff via independent blocks and median-of-means

Let $Z_1, \ldots, Z_T$ be FO+C-definable $\{0,1\}$ random variables obtained from disjoint address sets; write $Z := \frac{1}{T}\sum_j Z_j$.

Lemma 16 (Logical majority with Chernoff)**.** *For any fixed $\gamma \in (0, 1/6)$, choosing $T = \Theta(\log n)$ independent trials and the FO+C-definable majority threshold*

$$\mathrm{Maj}_\gamma := \left[Z \geq \tfrac{1}{2} + \gamma\right]$$

achieves error $\leq n^{-\omega(1)}$ in distinguishing $\mathbb{E}[Z_j] \geq \frac{1}{2} + 2\gamma$ from $\leq \frac{1}{2} - 2\gamma$.

Proof. By multiplicative Chernoff, $\Pr[Z \leq \frac{1}{2} + \gamma] \leq \exp(-2\gamma^2 T)$ and similarly on the other side. With $T = c \log n$ and c large, the tail is $n^{-\Omega(1)}$. The majority predicate is FO+C-definable via counting terms. □

Median-of-means in FO+C. Partition $T = b \cdot m$ trials into $b = \Theta(\log n)$ blocks of size $m = \Theta(1/\gamma^2)$; compute each block mean in FO+C, then take the block-median with a FO+C counting formula. This yields the same $n^{-\Omega(1)}$ error with only pairwise independence needed *within* blocks; since our addresses are disjoint we actually have full independence.

A.5 Putting it together: definable amplification wrapper

Definition 17 (Amplify(ϕ, γ))**.** *Given a FO+C/LFP computable Boolean outcome $\phi(\mathbf{A}, \mathcal{R})$, define T independent evaluations ϕ_j by addressing disjoint random tapes; set*

$$\mathrm{Amp}_\gamma(\mathbf{A}) := \left[\#\{j : \phi_j = 1\} \geq \left\lceil T\left(\tfrac{1}{2} + \gamma\right)\right\rceil\right].$$

Proposition 18 (Gap boosting schema inside FO+C+LFP+Rand)**.** *If $\Pr[\phi = 1] \geq \frac{1}{2} + 2\gamma$ then $\Pr[\mathrm{Amp}_\gamma = 1] \geq 1 - n^{-\omega(1)}$; if $\Pr[\phi = 1] \leq \frac{1}{2} - 2\gamma$ then $\Pr[\mathrm{Amp}_\gamma = 1] \leq n^{-\omega(1)}$. All predicates are FO+C-definable from $\preceq_\ell$.*

A.6 Quantum case: Solovay–Kitaev inside FO+C+QFP+Rand

Lemma 19 (Definable gate approximation)**.** *Fix a universal gate set $\mathcal{G} \subset U(2)$ with entries in $\mathbb{Q}(e^{i\pi/4})$. For any unitary U on poly(n) qubits and any $\epsilon \geq n^{-\omega(1)}$, there exists a FO+C+QFP+Rand term that applies a circuit over $\mathcal{G}$ of size poly$(n, \log 1/\epsilon)$ approximating U within operator norm ϵ.*

Sketch. Solovay–Kitaev gives the length bound. Because $\mathcal{G}$ is fixed and its encodings are in a fixed number field, FO+C can describe the classical control sequence; FO+C+QFP+Rand applies it. Random canonicalization supplies the register indexing. □

A.7 Worked microcase: majority with internal amplification

Let $\mathbf{A}$ be a multiset structure with domain bits $x_1, \ldots, x_n$. Define $\phi(\mathbf{A}, \mathcal{R})$ to output the parity of a random m-subset chosen by an $h_{A,b}$ hash into $[M]$ with thresholding; then wrap with Amp_γ. If $\sum_i x_i \geq \frac{n}{2} + \eta n$, Chernoff over the independent blocks shows acceptance w.h.p.; similarly reject below threshold. All maps are FO+C/LFP definable; randomness is via disjoint addresses.

A.8 Isomorphism invariance and measurability

Every construction depends only on $\preceq_\ell$ and $\mathcal{R}$, not on element names. Thus the acceptance probability is a class function on isomorphism types. Since the probability space is a finite product over tuple indices, all events are measurable cylinder sets; our amplification operates by quantifying over finitely many such cylinders.

Summary. Random canonical orders give order-free definability. Disjoint addressing yields i.i.d. random bits. Majority/median-of-means are FO+C-definable and provide Chernoff-grade amplification. For FO+C+QFP+Rand, Solovay–Kitaev is implemented with definable control, completing the internal machinery used in Theorems 2 and 6.

References

[1] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 2009.

[2] Herman Chernoff. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *Annals of Mathematical Statistics*, 23(4):493–507, 1952.

[3] Christopher M. Dawson and Michael A. Nielsen. The solovay-kitaev algorithm. *Quantum Information and Computation*, 6(1):81–95, 2005.

[4] Neil Immerman. *Descriptive Complexity*. Springer, 1999.

[5] A. Yu. Kitaev. Quantum computations: algorithms and error correction. In *Russian Mathematical Surveys*, volume 52, pages 1191–1249. 1997.

[6] Leonid Libkin. *Elements of Finite Model Theory*. Springer, 2004.

[7] Michael Mitzenmacher and Eli Upfal. *Probability and Computing*. Cambridge University Press, 2005.

[8] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 10th anniversary edition edition, 2010.