The Power of Quantum Fourier Sampling

Bill Fefferman

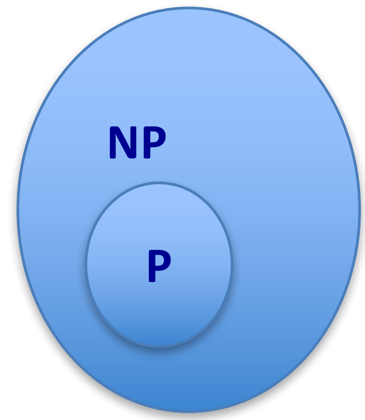
QuICS, University of Maryland/NIST

Joint work with Chris Umans (Caltech)

Based on arxiv:1507.05592

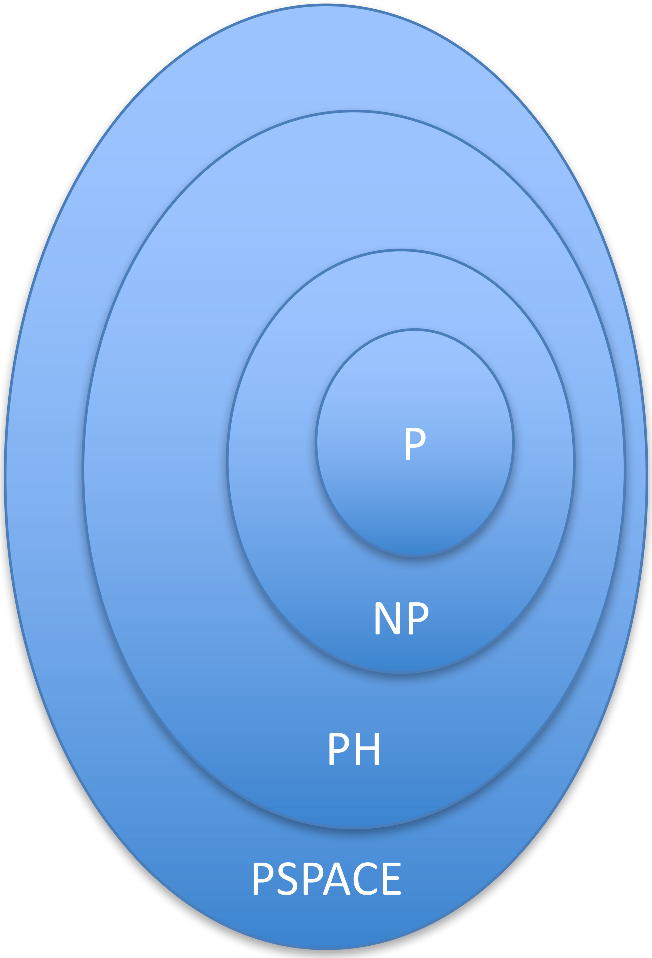
Classical Complexity Theory

- **P**
  - Class of problems efficiently solved on classical computer
- **NP**
  - Class of problems with efficiently checkable solutions
  - Characterized by **SAT**
    - Input: $\Psi:\{0,1\}^n \rightarrow \{0,1\}$
      - n-variable boolean formula
        - » E.g., $(x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee -x_2 \vee x_6) \wedge \ldots$
    - Problem: $\exists\, x_1, x_2, \ldots, x_n$ so that $\Psi(x)=1$?
  - **SAT** is **NP**-complete



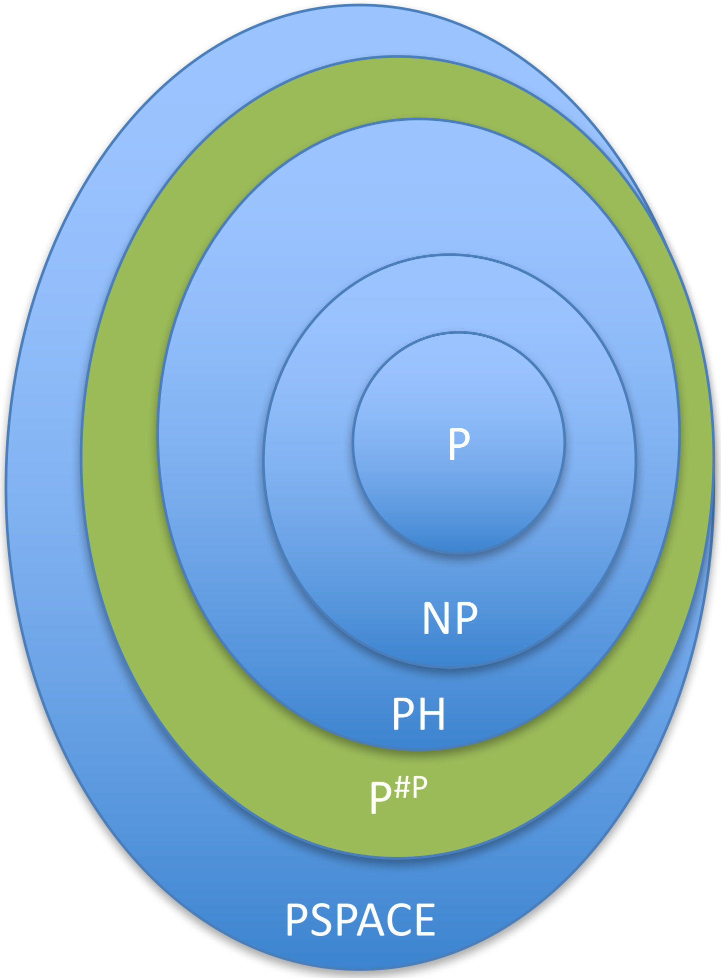
Beyond **NP**

- **Tautology**
  - Input: $\Psi:\{0,1\}^n \rightarrow \{0,1\}$
  - $\forall x\ \Psi(x)=1$?
  - Complete for **coNP**
  - Don't believe that **coNP**=**NP**
- Generalize **SAT** and **Tautology** by adding quantifiers:
  - **$QSAT_2$** is the version of the **SAT** problem with 2 quantifiers
  - E.g., $\exists x_1 x_2 x_{3\ldots} x_{n/2} \forall x_{n/2+1} x_{n/2+2,\ldots,} x_n$ so that $\Psi(x)=1$?
  - Consider problems **$QSAT_3$,$QSAT_4$,$QSAT_5$...$QSAT_n$**
  - Conjectured to get strictly harder with increasing number of quantifiers (or else there's a *collapse*!)
- **Σ_k** is class of problems solvable with a **$QSAT_k$** box
- **PH** is class of problems solvable with a **$QSAT_{O(1)}$** box
- **PSPACE** is class of problems solvable with a **$QSAT_n$** box



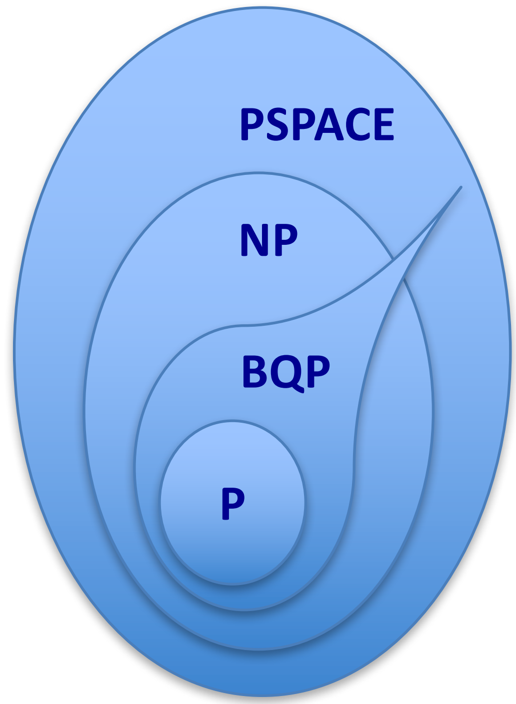
Complexity of *Counting*

- **#SAT**
  - Input: $\Psi:\{0,1\}^n \rightarrow \{0,1\}$
  - Problem: How many satisfying assignments to Ψ?
- **#SAT** is complete for **#P**
- **PH** $\subseteq$ **P**$^{\#P}$ [Toda'91]
- $\mathbf{Permanent}[X] = \sum_{\sigma \in S_n} \prod_{i=1}^{n} X_{i,\sigma(i)}$ is **#P**-hard



How powerful are quantum computers?

- **BQP**: The class of *decision* problems solvable by quantum computers in polynomial time
- Certainly **P**$\subseteq$**BQP**
- But why should **BQP**$\not\subseteq$**P** (or **NP** or **PH**)?
  - Shor's algorithm: Factoring$\in$**BQP**
    - But little reason to believe Factoring is not in **P**
    - In fact, if Factoring is **NP**-hard then **PH** collapses
  - Oracle separations, see [e.g., Aaronson'10, F., Umans'11]
  - In short, not much is known!



Separations from sampling problems

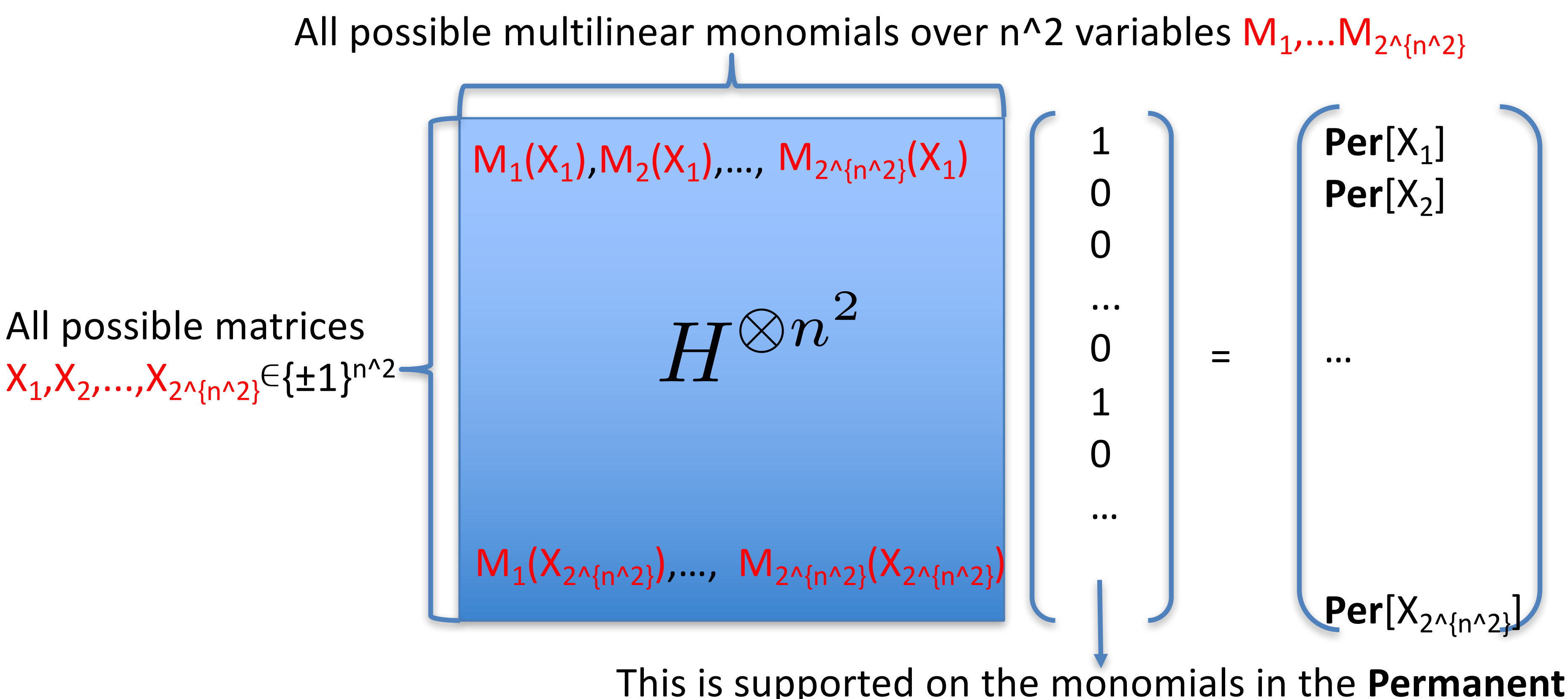
- Starting with [DT'02][BJS'10] we know that there are *distributions* that can be sampled quantumly that cannot be sampled *exactly* classically (unless **PH** collapse)
  - *Quantumly*: Efficiently prepare a quantum state on n qubits and measure in standard basis
    - Distribution is over measurement outcomes
  - *Classically*: No efficient classical randomized algorithm can sample from *exactly* the same distribution
- *Our focus*: "Approximate sampling" hardness result
  - Want a hardness result even if the classical sampler samples from distribution 1/poly(n) close in total variation distance from quantum distribution
  - Why are we interested in this?
    - "To model experimental error"
    - Other complexity separations would follow (i.e., **fBQP**$\not\subset$**fBPP** [Aaronson'10])

Construction of quantumly sampleable distribution $\mathbf{D}_{\mathbf{PER}}$

- *Goal*: efficiently prepare a quantum state in which *each* amplitude is proportional to the **Permanent** of a different matrix
- *Sketch of procedure*:
  1. Prepare the "permutation matrix state"
     - Quantum state on n^2 qubits uniformly supported only on those $n!$ permutation matrices
  2. Apply a quantum Fourier transform $H^{\otimes n^2}$
     - i.e., apply Hadamard on each of n^2 qubits
  3. Measure in standard basis to sample
- *Claim*: Each amplitude is proportional to the **Permanent** of a different $\{\pm 1\}^{n \times n}$ matrix

What's happening?

- Recall, **Permanent**($x_1,x_2,\ldots,x_{n^2}$) is a multilinear polynomial of degree n
- Our quantum sampling algorithm (*omitting normalization*):



Sketch of classical hardness proof

- *Recall*: $\mathbf{D_{PER}}$ is a distribution over all $\{\pm 1\}^{n \times n}$ matrices X with probabilities proportional to $\mathbf{Permanent^2}$[X]
- Assume there's a classical algorithm that samples from distribution close in total variation distance to $\mathbf{D_{PER}}$
- *Key tool*: Stockmeyer's algorithm
  - *Input*: Classical sampler and an outcome
  - *Output*: A $(1 \pm \varepsilon)$-*multiplicative estimate* to the probability of this outcome in time poly(n,1/ε) with an **NP** oracle
    - i.e., for ε=1/poly(n), this is in $\mathbf{BPP^{NP}} \subseteq \mathbf{\Sigma_3}$
- *Our strategy*: Chose a random $\{\pm 1\}^{n \times n}$ matrix X and use Stockmeyer's algorithm to estimate outcome probability of X ≈ $\mathbf{Permanent^2}$[X]
  - Since our sampler is *approximate*, can't trust it on any single outcome probability
  - Markov inequality: *Most* of the probabilities must be *additively close* to the true probabilities
  - So we end with a $\mathbf{BPP^{NP}}$ algorithm for *additively estimating* the $\mathbf{Permanent^2}$ of *most* matrices
- Is estimation task **#P**-hard? If so then $\mathbf{P^{\#P}} \subseteq \mathbf{BPP^{NP}} \subseteq \mathbf{\Sigma_3}$
  - But we know that $\mathbf{PH} \subseteq \mathbf{P^{\#P}}$ by Toda's theorem
  - So $\mathbf{PH} \subseteq \mathbf{\Sigma_3}$ (Collapse!)

Relating Additive to Multiplicative error

- *Main result*: If there's a *classical* approximate sampler, then:
  - Can compute $\mathbf{Per^2}[X] \pm \epsilon n!$ with probability $1-\delta$ over X in $\mathrm{poly}(n, 1/\epsilon, 1/\delta)$ time with **NP** oracle
- This is unnatural! Would like multiplicative error:
  - $(1-\epsilon)\mathbf{Per^2}[X] \leq \alpha \leq (1+\epsilon)\mathbf{Per^2}[X]$ with probability $1-\delta$ in $\mathrm{poly}(n, 1/\epsilon, 1/\delta)$ time with **NP** oracle
- Can we get *multiplicative* error using our procedure?
  - "Permanent Anti-concentration conjecture" [AA'11]
    - Need: exists polynomial p so that for all n and δ
      - $\Pr_X[|\mathrm{Per}(X)| < \sqrt{n!}/p(n, 1/\delta)] < \delta$
    - Have evidence that this is true:
      - For Bernoulli distributed $\{-1,+1\}^{n \times n}$ matrices:
        - $\forall \varepsilon > 0 \ \Pr_X[|\mathrm{Per}[X]|^2 < n!/n^{\varepsilon n}] < 1/n^{0.1}$ [Tao & Vu '08]

How hard is "Approximating" the Permanent?

- *Scenario* 1:
  - Suppose I had a box that:
    - "Solves all the Permanents approximately"
    - Input: ϵ>0 and matrix X$\in${-1,+1}$^{n \times n}$
    - Output: α so that:

      $$(1-\epsilon)\mathsf{Per}^2(\mathsf{X}) \leq \alpha \leq (1+\epsilon)\mathsf{Per}^2(\mathsf{X})$$

    - In time poly(n,1/ϵ)
  - This is **#P**-hard!
- *Scenario* 2:
  - Suppose I had a box that:
    - "Solves most of the Permanents exactly"

      $$\Pr_X[\alpha = \mathsf{Per}^2[\mathsf{X}]] > 1-\delta$$

    - For δ=1/poly(n)
  - This is **#P**-hard!
- Our "solution" has weakness of both Scenario 1 and 2
  - Hardness proofs break-down!
  - This is exactly the same reason other two "approximate" sampling results need conjectures…

Generalizing the argument

- Unlike the results of [Aaronson & Arkhipov ’12] and [Bremner, Montanaro & Shepherd ’16] we can generalize our argument to rely on alternative hardness conjectures
  - Can generalize the **Permanent** to any “*efficiently specifiable* polynomial”
    - By changing permutation matrix state
    - For instance: Hamiltonian cycle polynomial, others…
  - Can generalize the entries of the matrices and the distribution over matrices (e.g., iid Gaussian instead of random sign matrix)
- If any of these conjectures are true, we show the desired “approximate sampling” separation

Thanks!