**Introduction**

* Speedups for problems like factoring are conjectural at present
* In black-box model, exponential and even larger speedups can be proved
* The speedup question - Within the black-box model, just how large of a quantum speedup is possible?
* Simon’s problem - root(N) and logN x log(logN) by Buhrman et. al

**Results**

1. **Maximal Quantum/Classical separation**

* In forrelation we are given access to two boolean functions f and g and our task is to estimate the amount of correlation between f and the Fourier transform of g
* One can give a quantum algorithm that could solve the forrelation problem with bounded probability of error using only 1 quantum error.
* **Theorem 1:** Any classical randomized algorithm for forrelation must make Ω(√N/ log N ) queries. Theorem 1 yields the largest quantum versus classical separation yet known in the quantum-query model (also largest property testing separation). This theorem is deduced as the consequence of a more general result i.e. a lower bound on the classical query complexity of a problem called Gaussian Distinguishing
* **Theorem 2:** Gaussian distinguishing requires Ω (1/ε log(M/ε)) classical randomized queries. Theorem 1 is just a special case of theorem 2 with M=2N and ε = 1/√N

1. **Proof of optimality**
   * Quantum/classical query complexity separation achieved is close to the maximum possible.
   * **Theorem 3:** Let Q be any quantum algorithm that makes t=O(1) queries to a N-bit string X. Then we can estimate Pr(Q accepts X), to constant additive error and with high probability, by making only O(N1-1/2t) classical randomized queries to X. This theorem answers the question raised by Buhrman et al in the negative that there doesn’t exist any problem with constant versus linear complexity gap. (Note that this theorem doesn’t rule out a logN vs N gap and they conjecture that this is indeed possible)
   * **Theorem 4:** Every degree-k real polynomial p : {-1,1}N->R that is
     1. Bounded in [-1,1] at every boolean point and
     2. “Block-multilinear” (the variable can be partitioned into k blocks such that each monomial is the product of one variable from each block)

can be approximated to within +-ε with high probability, by non-adaptively querying only O((N/ε2)1-1/k ) of the variables.

1. **K-fold forrelation**
   * Study k-fold forrelation and show that it captures the full power of quantum computation
   * **Theorem 5:**  If f1, f2, f3 are described explicitly and k = poly(n)then k-fold forrelation is a bqp complete promise problem
2. **Other Results**
   * Largest possible quantum/classical separations that are achievable for approximate sampling and relation problems.
   * There exists a sampling problem namely fourier sampling of a boolean sampling of a boolean function that is solvable in 1 quantum query but requires Ω(N/ log N) classical queries.
   * Every 1 query quantum algorithm can be simulated with O(√N) randomized query is generalized to show that every bounded degree 2 poly can be estimated using O(√N) randomized queries

**Techniques**

1. **Randomized lower Bound**
2. **Randomized upper bound**
3. **Other Results**

**Discussion**