Quantum property testing for sparse graphs

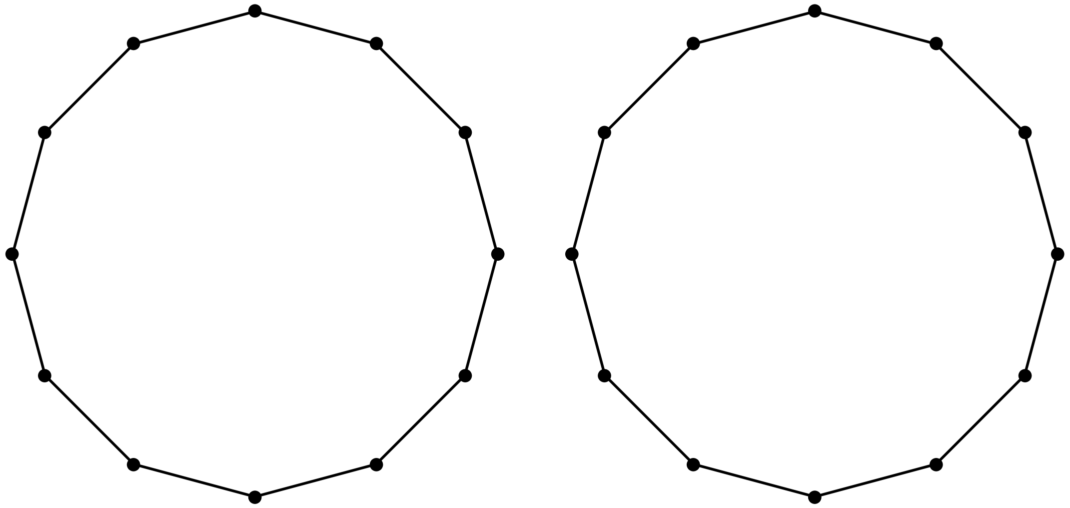
Andrew Childs
Waterloo

Yi-Kai Liu
Caltech

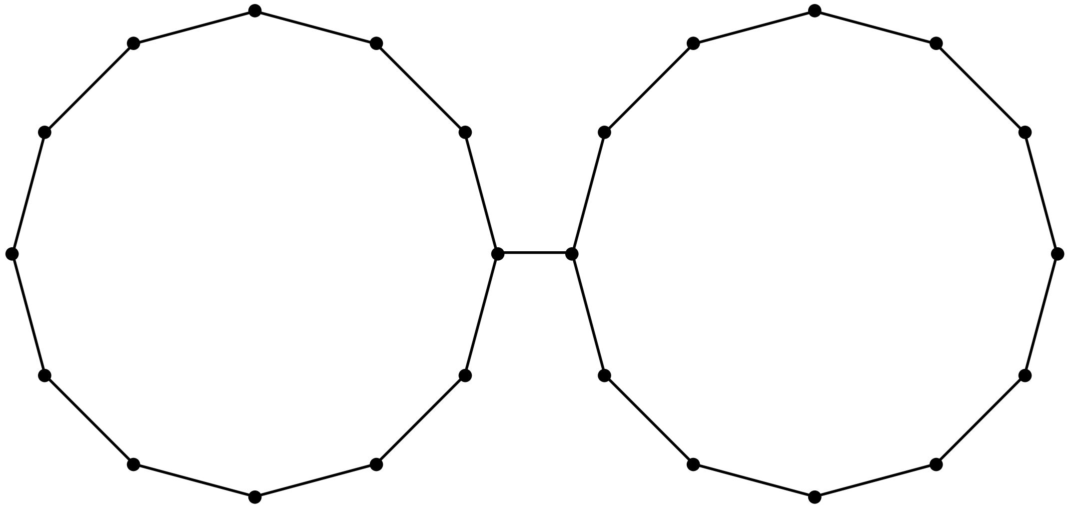
Deciding connectivity

Given an n-vertex graph G (in terms of a black box for its adjacency matrix), how hard is it to tell if G is connected?

Ex:



vs.



$\Omega(n^2)$ queries are required

Testing connectivity

Promise: Either G is connected or it is ϵ-far from connected.
(must change $\epsilon\binom{n}{2}$ edges to make it connected)

Trivial fact: for $\epsilon > (n-1)/\binom{n}{2}$, no graph is ϵ-far from connected.

So we can test connectivity in $\mathrm{poly}(1/\epsilon)$ queries.

Many natural graph properties can be tested in only $\mathrm{poly}(1/\epsilon)$ queries.

Ex (trivial): Eulerian, Hamiltonian, acyclicity, planarity, regularity, etc.

Ex (nontrivial): Bipartiteness, k-colorability, k-clique, etc.

[Goldreich, Goldwasser, Ron 95]

Quantum testing of graph properties

Can there be a significant quantum speedup for testing some graph property?

To say anything nontrivial, we need a property that can't be already be tested fast classically.

Can there be an exponential quantum speedup?

Outline

1. The model
2. Testing bipartiteness
3. Testing expansion
4. Open questions

Property testing

Given a black-box input $x \in \Sigma^N$
(equivalently, a function $f_x : \{1, \ldots, N\} \to \Sigma$)

Property $P \subseteq \Sigma^N$

Say x is ϵ-far from P if $\min\{\Delta(x, y) : y \in P\} > \epsilon N$

Hamming distance

Promise: either $x \in P$ or x is ϵ-far from P

Determine (with error probability at most $1/3$) which holds

Quantum property testing

- $O(1)$ quantum vs. $\Omega(\log N)$ classical [Buhrman, Fortnow, Newman, and Roehrig 03]
- Exponential separation between quantum and classical testing [BFNR 03]
- Some properties need $\Omega(N)$ quantum queries [BFNR 03]
- Testing juntas logarithmically faster than the best known classical tester [Atici and Servedio 07]
- Efficient quantum algorithm for testing solvability of a black box group [Inui and Le Gall 08]
- Quantum algorithms for testing uniformity/orthogonality of distributions [Bravyi, Harrow, Hassidim 09; Chakraborty, Fischer, Matsliah, de Wolf 09]
- ... but no work on testing graph properties

Sparse graphs

Fix a positive integer d.
Call a graph d-*sparse* if every vertex has degree at most d.

Black box description of a graph G (“adjacency-list model”):

$$f_G : V(G) \times \{1, \ldots, d\} \to V \cup \{*\}$$

$$f_G(v,i) = \begin{cases} w & \text{if } w \text{ is the } i\text{th neighbor of } v \text{ in } G \\ * & \text{if } v \text{ has fewer than } i \text{ neighbors} \end{cases}$$

Quantumly: $|v, i, z\rangle \mapsto |v, i, z \oplus f_G(v,i)\rangle$

ϵ-far means we must change $\epsilon n d$ edges

Note: Can still test connectivity in time $\mathrm{poly}(1/\epsilon)$ in this model [Goldreich and Ron 97].

Results

Quantum algorithms for

- ϵ-testing bipartiteness in time $O(n^{1/3}\mathrm{poly}(\log n, 1/\epsilon))$
- testing whether a graph is an α-vertex expander or ϵ-far from a $c\mu\alpha^2$-vertex expander in time $O(n^{\frac{1}{3}+3\mu}\mathrm{poly}(\log N, 1/\epsilon, 1/\alpha))$

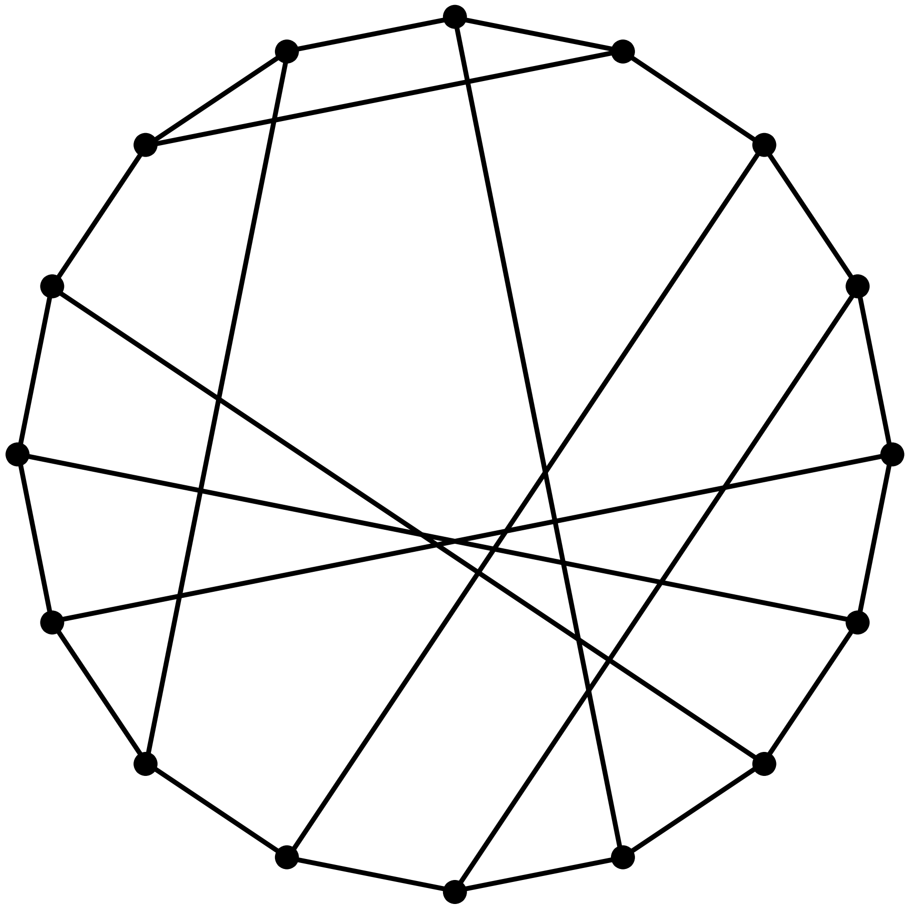
Both tasks require $\Omega(\sqrt{n})$ queries classically [Goldreich and Ron 97].

No nontrivial quantum lower bound!

Bipartiteness

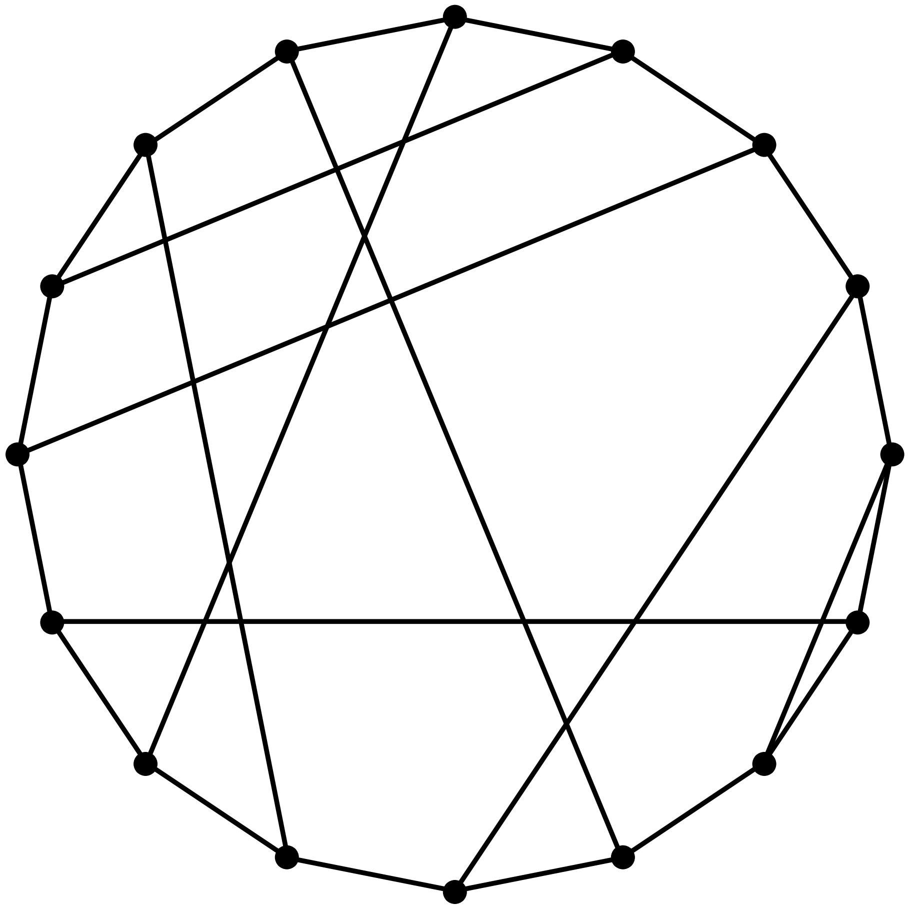
The problem

Given an adjacency-list black box for a d-sparse graph, decide whether the graph is



bipartite

or



ϵ-far from bipartite

Classical algorithm

Idea: Take many (short) random walks in G starting from a fixed vertex; look for a pair of walks that form an odd cycle.

Algorithm.

```
Repeat the following $O(1/\epsilon)$ times:
  Pick a random $v \in V(G)$.
  For $i$=$1$ to $K$, where $K = \sqrt{n}\,\mathrm{poly}(\log n, 1/\epsilon)$:
    Let $w_{i,0} = v$.
    Let $j = 1$.
    Repeat $L$ times, where $L = \mathrm{poly}(\log n, 1/\epsilon)$:
      With probability $1/2d$, let $w_{i,j}$ be the $k$th neighbor of $w_{i,j\text{-}1}$
      (assuming such a neighbor exists) and increment $j$.
  If $w_{i,j} = w_{i',j'}$ for some $i, i', j, j'$ with $j$ even and $j'$ odd, reject.
If no iteration rejected, accept.
```

Theorem [Goldreich and Ron 99]: This algorithm accepts when G is bipartite, rejects with constant probability when G is ϵ-far from bipartite, and runs in time $O(\sqrt{n}\,\mathrm{poly}(\log n, 1/\epsilon))$.

Element distinctness

Given a black-box input $x \in \Sigma^N$, are there distinct $i, j \in \{1, \ldots, N\}$ such that $x_i = x_j$ (a *collision*)?

Classical query complexity $\Theta(N)$.

There is a quantum algorithm that decides element distinctness using only $O(N^{2/3})$ queries [Ambainis 04].

Strategy: Quantum walk on the Johnson graph $J(N, N^{2/3})$, with vertices corresponding to subsets of $N^{2/3}$ indices.

When a collision exists, the algorithm returns one.

A quantum strategy

Fix a choice of random bits for the classical algorithm.

↖ $O(\sqrt{n}\,\mathrm{poly}(\log n, 1/\epsilon))$ of them

Search for an odd collision among the endpoints of the walks using the element distinctness algorithm.

Query complexity: $\left(\sqrt{n}\,\mathrm{poly}(\log n, 1/\epsilon)\right)^{2/3} = n^{1/3}\,\mathrm{poly}(\log n, 1/\epsilon)$

Caveat: Just flipping the coins takes time $\Omega(\sqrt{n})$, so the running time is significantly more than the query complexity.

Derandomization

We modify the classical tester to use significantly less randomess.

Idea: Replace the uniformly random bits by t-wise independent bits (where $t = \text{poly}(\log n, \log d, 1/\epsilon)$).

We call a set of random variables *t-wise independent* if the distribution is uniform for any subset of t or fewer random variables.

Theorem [Alon, Babai, Itai 86]: There is an algorithm to generate m bits that are t-wise independent in time $O(t \log m)$, using $O(t \log m)$ uniformly random bits.

By taking the random walk using t-wise independent random variables in place of uniformly random ones, we can give a classical bipartiteness testing algorithm whose running time is still $O(\sqrt{n}\, \text{poly}(\log n, 1/\epsilon))$, and that only uses $\text{poly}(\log n, \log d, 1/\epsilon)$ random bits.

Key idea: the analysis only depends on correlations among at most 4 random walks (and the walks are not very long).

The quantum algorithm

Algorithm.

Repeat the following $O(1/\epsilon)$ times:

Use the element distinctness algorithm to search for a "collision", where such an event is defined as an odd cycle obtained from a pair of pseudorandom walks executed as in the algorithm of Goldreich and Ron, but using $\mathrm{poly}(\log n, \log d, 1/\epsilon)$-wise independent random variables in place of uniformly random ones.

If a collision is found, reject.

If no iteration rejected, accept.

Theorem: This algorithm accepts when G is bipartite, rejects with constant probability when G is ϵ-far from bipartite, and runs in time $O(n^{1/3}\,\mathrm{poly}(\log n, 1/\epsilon))$.

Expansion

Expansion

Informally, expanders are graphs that are well-connected.

Definition. We say G is an α-expander if for every $U \subset V(G)$ with $|U| \leq |V(G)|/2$, $|\partial(U)| \geq \alpha|U|$.

vertex boundary of U: vertices in $V(G) \setminus U$ adjacent to some vertex in U

Many applications: Derandomization, PCP, hash functions, error correcting codes, network design, ...

How hard is it to test if a (d-sparse) graph is an α-expander or ϵ-far from an α-expander?

We'll actually consider something slightly weaker: either the graph is an α-expander or ϵ-far from a β-expander, where $\beta<\alpha$.

Even this weaker task requires $\Omega(\sqrt{n})$ classical queries [GR 97].

Classical algorithm

Idea: Random walks on expanders are rapidly mixing.
Take many (short) random walks in G starting from a fixed vertex; check whether there are more collisions between their endpoints than expected from a near-uniform distribution.

Algorithm(μ) [GR 00].

```
Repeat the following $O(1/\epsilon)$ times:
  Pick a random $v \in V(G)$.
  For $i=1$ to $n^{\frac{1}{2}+\mu}$:
    Let $w_i$ be the endpoint of a random walk of length $\frac{16d^2}{\alpha^2}\log n$
    starting from $v$, with steps taken as in the bipartiteness tester.
  If the number of pairwise collisions among the $w_i$ is more
  than $\frac{1}{2}n^{2\mu} + \frac{1}{128}n^{7\mu/4}$, reject.
If no iteration rejected, accept.
```

Theorem [Nachmias and Shapira 07]: If G is an α-expander, we accept with probability at least $2/3$. If G is ϵ-far from a $c\mu\alpha^2$-expander, where the constant c depends on d, we reject with probability at least $2/3$. The running time is $O(n^{\frac{1}{2}+\mu}\mathrm{poly}(\log n, 1/\epsilon, 1/\alpha))$.

Derandomization

As before, it is helpful to reduce the amount of randomness used by the classical algorithm.

One can show that it suffices to use t-wise independent random variables, where $t = \mathrm{poly}(\log n, d, 1/\epsilon, 1/\alpha)$.

The result is a classical algorithm using only $\mathrm{poly}(\log n, d, 1/\epsilon, 1/\alpha)$ random bits whose running time is still $O(n^{1/2+\mu}\mathrm{poly}(\log n, 1/\epsilon, 1/\alpha))$.

Counting collisions

The classical algorithm counts the collisions between walk endpoints.

In general, counting collisions is hard! ($\Omega(N)$ [Buhrman et al. 01])

But we only care of the number of collisions is above some small threshold M.

Strategy: Repeatedly find collisions, unmarking those found previously.

Claim. There is a bounded-error quantum algorithm to decide whether there are M or more collisions using $O(N^{2/3} M \log M)$ queries.

The quantum algorithm

Algorithm(μ).

Repeat the following $O(1/\epsilon)$ times:

Use the element distinctness algorithm to determine whether there are more than $\frac{1}{2}n^{2\mu} + \frac{1}{128}n^{7\mu/4}$ collisions among the endpoints of pseudorandom walks executed as in the classical expansion-testing algorithm, but using $\mathrm{poly}(\log n, d, 1/\epsilon, 1/\alpha)$-wise independent random variables in place of uniformly random ones.

If more collisions are found, reject.

If no iteration rejected, accept.

Theorem: If G is an α-expander, we accept with probability at least $2/3$. If G is ϵ-far from a $c\mu\alpha^2$-expander, where the constant c depends on d, we reject with probability at least $2/3$. The running time is $O(n^{\frac{1}{3}+3\mu}\mathrm{poly}(\log N, 1/\epsilon, 1/\alpha))$.

Results

Quantum algorithms for

- ϵ-testing bipartiteness in time $O(n^{1/3}\mathrm{poly}(\log n, 1/\epsilon))$
- testing whether a graph is an α-vertex expander or ϵ-far from a $c\mu\alpha^2$-vertex expander in time $O(n^{\frac{1}{3}+3\mu}\mathrm{poly}(\log N, 1/\epsilon, 1/\alpha))$

Both tasks require $\Omega(\sqrt{n})$ queries classically [Goldreich and Ron 97].

No nontrivial quantum lower bound!

Open questions

- Find any nontrivial quantum lower bound.
- Improve the algorithms? Quantum walk?
- Time-efficient quantum collision finding without derandomization?
- Quantum property testing of other graph properties: is there any example with an exponential speedup?