Why quantum computers cannot work

Gil Kalai from Einstein Institute of Mathematics, Hebrew University of Jerusalem

Quantum computers are hypothetical devices based on quantum physics that can out-perform classical computers. A famous algorithm by Peter Shor shows that quantum computers can factor an n-digit integer in $n^3$ steps, exponentially better than the number of steps required by the best known classical algorithms. The question of whether quantum computers are realistic is one of the most fascinating and clear-cut scientific problems of our time.

What makes it hard to believe that superior quantum computers *can* be built is that building them represents a completely new reality in terms of controlled and observed quantum evolutions, and also a new computational complexity reality. What makes it hard to believe that quantum computers *cannot* be built is that this may require profoundly new insights into the understanding of quantum mechanical systems.

My work is geared toward a negative answer, and I offer an explanation within the framework of quantum mechanics, for why quantum computers cannot be built.

I will also mention some highlights from a scientific debate on the matter between myself and Aram Harrow (started here).

Related Links:
Pacific Institute for the Mathematical Sciences