

# Re: Help with quantum computing project

---

*Source:* <http://sci.tech-archive.net/Archive/sci.physics/2005-11/msg00657.html>

---

- *From:* Ben Rudiak-Gould <br276deleteme@xxxxxxxxxx>
  - *Date:* Thu, 10 Nov 2005 16:10:36 +0000
- 

kenfitz3@xxxxxxxxxx wrote:

Would anyone be able to give me a rough outline of topics to address in doing a presentation on Quantum Computing?

Quantum computing is a small field, but even so there's no way you can even begin to cover it in only 30 minutes. You'll have to focus on something. If this were for a hardware design course or a complexity-theory course, that would give you an area to focus on, but I don't know what makes sense for an operating-systems course. I can't see any connection between operating systems and quantum computing as it now stands.

One approach you could take is to talk only about the mathematical theory. There's far too much of this to cover in 30 minutes, but maybe you could whet people's appetites.

Or you could skip the mathematics entirely and give an executive summary, i.e. why-should-I-care. The problem is that it's not clear at this stage that Joe User actually should care. The stuff about exponential speedup and parallel universes is mostly hype. Quantum computers won't make the internet any faster, or speed up ray tracing or 3D games. The main impact on Joe is negative: quantum computers can break most or all public key algorithms, so e-commerce isn't safe any more (whether or not he personally owns a quantum computer).

If your audience is researchers or researchers-to-be, you could talk about open problems. One interesting open problem is actually building quantum hardware that works. Another is finding high-level notions of quantum computing suitable for high-level quantum programming languages. Another is expanding or theoretically constraining the space of "interesting" quantum algorithms. Only three interesting algorithms are known currently: order finding (Shor), SAT solving (aka "database search") (Grover), and efficient simulation of quantum systems. My guess is that the space of interesting algorithms is small.

-- Ben  
.