Late breaking - QCs are just imprecise analog computers - connects back to von Neumann

Steven Meyer

Tachyon Design Automation, Boston, MA 02111
smeyer@tdl.com

Presented May 21, 2019 at Eurocrypt Rump Session Darmstadt Germany

Slides and annotated references posted on my web page www.tdl.com/˜smeyer

Cold Atom physicist Chis Monroe's QC building

1. Chris Monroe studied atomic clocks. He is a Maryland professor and founder of best funded IonQ start up. Best entry to Monroe's non hype results is to listen to his videos.
2. According to Monroe up to minor engineering advantages, there is nothing better than trapped ion quantum computers (QC).
3. A QC is basically a row of pendulums (harmonic oscillators) that are controlled by and values sensed using lasers from single atom sensors and actuators.
4. Best current accuracy of exponential entanglement is 1-2 percent for current 10-20 qbit and other gates QCs. Monroe hopes accuracy can be held and improved with cooling.
5. The problem with expecting better than a few percent accuracy is that it violates Niels Bohr's complementarity principle. Inside atom calculations must be quantum. Macro machine level calculations are classical.

Inherent QC inaccuracy is reason analog computers abandoned

1. Paul Feyerabend (from Richard von Weizacker) in his Philosophical Papers Vol. 4 explains Bohr's conceptual first then electron state calculations next Bohr interpretation that is widely accepted by physicists but misinterpreted.
2. Bohr thought that Heisenberg's formal version of complimentarity as his uncertainty principle simplified atomic behavior too much because it assumed the formal theory is the same as the conceptual physics.
3. Bohr's Complimentary principle implies that atomic and macro calculations are not identical.
4. In Monroe's criticism of error correcting qbits, he argues that processing speed will be no faster than sequential von Neumann architectures computers (called VNCs here) or require an exponential number of qbits and auxiliary gates.

Consequences for crypto and CS of QMs as analog computers

1. QCs will be useless in symbolic code breaking applications.
2. QCs may be useful for quantum entangled communication, but the few percent inaccuracy is probably inherent.
3. QCs may be very useful for simulating molecular function where required approximations from state calculation complexity on VNCs are worse than QC simulation.
4. The advances used in QC research may be useful in building better versions of Shamir and Tomer's Twinkle and Twirl. The connection to Weizman Institute is through Chaim Leib Pekeris builder of Weizac in 1954 who worked at the Princeton Institute for Advanced study with John von Neumann and Wolfgang Pauli.

Connection to von Neumann's rejection of QM logic and TMs

1. CS has suppressed history by attempting to replace computation complexity with Hilbert's programme (church-Turing TM complexity) and physics with digital quantum logic.
2. Suggests there will be no future replacements to current number theory crypto algorithms.
3. In his development in the late 1940s and early 1950s of the first computer, Neumann rejected not just Hilbert's programme that all knowledge can be expressed as predicate calculus but also Turing's TM model replacing it with the MRAM model for VNCs.
4. For MRAMs there is no separate NP class.
5. Closest theoretical model for Neumann's VNCs is MRAMs studied by Hartmanis and Simon ('On the Structure of Feasible Computations', Lecture Notes in CS vol 26, 1-49).

Consequences of Neumann's view of computation

1. In Neumann architecture machines have a fixed number of unbounded binary coded memory cells for which multiplication, indexing and selecting are unit operations.
2. TMs are weak and therefore not a good model for computational difficulty because although they are universal in the Church Turing sense, they use unary encoding and require searching or guessing. Index don't guess or enumerate.
3. Neumann was explicit that computers must be constructed big enough so problem fits. I think for future situations where a code must be broken with no budget limit, response will be to build very large wide VNCs.
4. To show why Neumann rejected linguistic formula based theory consider the yes no question that is computable but outside NP: 'Are two regular expressions equivalent?'
5. Many QC algorithms use the TM world assumptions where NP problems are more difficult than those in P.

Neumann on language formulas

“The insight that a formal neuron network can do anything which you can describe in words is a very important insight and simplifies matters enormously at low complication levels. It is by no means certain that it is a simplification on high complication levels. It is perfectly possible that on high complication levels the value of the theorem is in the reverse direction, namely, that you can express logics in terms of these efforts and the converse may not be true (Aspray[1990], note 94, p. 321)”

Neumann on genetic algorithms

“He (Neumann) led the biologist to the window of his study and said: ’Can you see the beautiful white villa over there on the hill? It arose by pure chance. It took millions of years for the hill to be formed; trees grew, decayed and grew again, then the wind covered the top of the hill with sand, stones were probably deposited on it by a volcanic process, and accident decreed that they should come to lie on top of one another. And so it went on. I know, of course, that accidental processes through the eons generally produce quite different results. But on this one occasion they led to the appearance of this country house, and people moved in and live there at this very moment’(Heisenberg[1971] p. 111). ”