Tutte's Colossus Method Beginning of Modern Computation

Steve Meyer

Tachyon Design Automation
San Francisco, CA 94111
smeyer@tdl.com

Presented April 28, 2015 Eurocrypt Sophia Bulgaria

Introduction

- I think William Tutte should get more credit as the real pioneer of combinatorial code breaking and modern computing.
- Turing method of logic formula substitution was unable to deal with later German codes. Method was Hilbert's logic as repeated giant array formula substitution.
- Tutte in **Fish and I** lecture (on web) p. 6 explains Turing formula substitution as opposed to modern Von Neumann machine style computation.
- **"Turing would assume the first two symbol in the X1 pattern . . . And so on making as few corrections as were necessary for consistency. It is a method requiring great artistry. I never used it successfully myself."**

Colossus computational method

- Starting question given a wheel pattern and a message find wheel setting to decipher message. After Tutte's method was programmed on Colossus plus with help from statisticians exact initial wheel settings were not needed (pp. 7-8).
- Tutte writes **"...try all 1271 possible relative positions and pick the one with the best agreement"** (p. 7).
- **"Post Office engineers with applied mathematicians mechanized the process."**
- **"It occurred to me that with a sufficiently long message, this statistical method could be strengthened to find unknown wheel patterns."**

Tutte Colossus –physics view of the history

- Parallel events to Tutte cryptography is 1950s rejection of Von Neumann's 1920s quantum logic (QL) (original 1920s arguments due to Grete Hermann).
- Einstein and Bohr convinced Von Neumann that his formalized Quantum mechanics as axiomatized Hilbert logic was wrong leading, I think, to the Von Neumann computing machine definition.
- Computing is iterative computation not logic formula substitution.
- Reference **Blackett's War** by S. Budiansky.

Modern consequences

- 1950s physicists abandoned quantum logic (see Karl Popper Archive) but history rewritten so Quantum computers buildable from Von Neumann's 1920s QL axiomatization.
- Competition between methods no longer happens.
- P=NP still stuck in world of Hilbert and Turing repeated unbounded giant array substitution (proven 'equivalent" but proof abstracts out wrong properties).