Running head: Comparative Analysis of Mark1, Colossus and Zuse Z4.

A Comparative Analysis of Mark 1, Colossus and Zuse Z4.

Chris Collins

24th September 2006

Abstract

During WW2 three independent groups of researchers worked on the development of the first computer, which resulted in the systems Mark 1, COLOSSUS and Z4. This article discusses these computers, their architectures and the driving forces behind them.

.

Colossus

From 1939 until the end of the Second World War, Bletchley Park was the home to the Government Code and Cipher School (GC&CS). This was Britain's main intelligence agency during war time, and was tasked with breaking and decrypting encoded German and Japanese messages.

One of these encryption schemes, the Lorenz SZ 40/42 cipher was used by high level German officials for communication. The code breakers in Bletchley dubbed this family of ciphers "Fish", and the traffic generated by them "Tunny". The Lorenz machine was a teletype attachment which would automatically encrypt plaintext entered by it's operator and send the cyphertext over the wire. On the receiving end, the teleprinter had an identical Lorenz machine attached which could decrypt the cyphertext before printing out the plaintext on paper (Good et al., 1945).

The enciphering scheme used by these machines was one of letter subtraction. The plaintext letter was subtracted (a boolean XOR operation) from the next letter in the key stream in order to generate the cyphertext. In order to decrypt, the opposite action occurred, where the cyphertext was subtracted from the key stream to retrieve the plaintext.

Because of the particularities of how the Lorenz machine generated its key stream (Copeland, 2004), William T Tutte (Good et al, 1945) realised that a statistical analysis of the cyphertext could reveal the likely encrypting settings of the Lorenz machine. This involved differencing each letter of the cyphertext from the next, and comparing this to the 1,271 possible positions the machine could have been in to generate that character. A count was made of each time these matched, and as Tutte showed, the settings with the highest scores was the most likely to be the correct one, thus allowing a total decryption of the message.

Obviously, doing all this calculation by hand was a laborious process. Thomas Flowers had also been working on Tunny at Bletchley and given his background in electronics (Copeland, 2004) realised that he could build a machine which could carry out these calculations mechanically. He and his team began working on this in early 1943, and on 8 December 1943 the machine known as Colossus was built and had successfully passed its first trial runs.

Colossus was built using 1500 valves, much more than were ever used in any machine previously (Randell, 1980). It was programmable via a patch-panel and switches. These selected the logic circuits to be used during operation. It wasn't programmable in a general sense, as it wasn't designed to be a general purpose computer.

Input to the Colossus was via a stream of punched paper, containing the cyphertext to be analysed. This ran at a pace of 12m/s allowing the Colossus to analyse 5000 characters per second. Internally it generated the key stream for comparison, and output was via an attached teletype machine where the results were printed. Apart from the registers it used during computation, it had no storage capability.

Z4

The Z4 computer was the fourth in a line of progressively more sophisticated computers designed and built by Konrad Zuse. Zuse was born in Berlin, Germany in 1910 and qualified as a civil engineer in 1935. Up to this point he had shown no interest in computers, but from 1934 onwards he realised the number of calculations required of a civil engineer, and wished for a way to free engineers from them.

When he came to designing his computer, Zuse realised that it had to be general purpose, which its operator should be able to specify the algorithm it was to run, i.e. it should be freely programmable.

By 1938 he had designed and built his first computer, the Z1. This was a mechanical device driven by an electric motor, giving it a clock speed of one hertz. It could read programs from a punch tape, it calculated 22 bit binary floating point numbers, and had a 64 word memory. Uniquely, the memory was also mechanical, and relied on the positions of pins between two metal sheets. According to Zuse (2001) the machine also featured the following:

> A high performance binary floating point unit in the semi-logarithmic representation, which would allow him to calculate very small and very big numbers with sufficient precision.
>
> A high performance adder with a one-step carry-ahead and precise arithmetic exceptions handling.
>
> A memory in which each cell could be addressed by the punch tape and could store arbitrary data.
>
> A control unit that controlled the whole machine, and implemented input and output devices from the binary to the decimal number system and vice versa.

Between 1938 and 1942 Zuse continued to refine his computer, going through two revisions of the prototype. The Z2 was built using relays for the control unit, and arithmetic unit. The Z3 was build entirely from relays, apart from it's memory.

Z4 was the next generation of Zuse's computers, and was intended to become the prototype for a mass produced computer. Work began on Z4 in 1942, but shortly later it became

increasingly difficult to complete this work due to the Allied air raids on Berlin. Zuse was forced to flee the bombing, and all progress on the Z4 essentially ceased.

Progress on the prototype Z4 remained at a standstill until 1948 when Zuse met Eduard Stiefel (Zuse, 2001). Prof Stiefel was setting up an Institute for Applied Math in Zurich, and agreed to use the Z4 there. Immediately Zuse set about rebuilding and improving the Z4 for it's delivery to Zurich.

The Z4 was delivered to the Institute in Zurich on July 11 1950, and Zuse (2001) reports the specifications as such:

> The restored Z4 consisted of about ten relay cupboards containing 2,200 standard relays, plus 21 stepwise relays for the micro-sequencer. The Z4's memory was a mechanical one with 64 words, each containing 32 bits. The structure of the mechanical memory was similar to the memory of the Z1. However, while the Z1 had a word length of 22 bits, the word length of the Z4 was extended to 32 bits. Each word was directly addressable by the instructions on the punch tape.

Mark I

In many respects the development of the Harvard Mark I computer is similar to the inception of the Z1. It started in 1939 with Howard Aiken, who was doing a doctoral dissertation on the conductivity of vacuum tubes. This required the solution of a set of non-linear differential equations (Aspray, 2000). Like Zuse, Aiken realised the potential of a general computer for solving applied math problems like these.

Aiken set about writing the functional specifications of his computer, and in 1939, Harvard and IBM signed an agreement for IBM to construct and deliver the computer. This was

achieved by 1944, when Harvard took delivery of the "Aiken-IBM Automatic Sequence Controlled Calculator Mark I", though it was known most widely as the "Harvard Mark I".

This was an electromechanical machine driven by an electric motor, connected to a 50 ft. shaft which powered the other components. It would calculate using 23 digit decimal numbers. It had dials for setting up to 60 constants for use during calculation, and had a 72 word memory for storing intermediate values. It took it's programmed input via card reader and had an attached typewriter for outputting calculated solutions (IBM, 2002).

Aiken had been a Navy reserve officer, and in 1941 was called to active duty. He convinced the Navy that the computer could be of use to the war effort, and by 1944 had been transferred back to Harvard as the commander of the computer laboratory. The Mark I was used for strength-of-materials calculations for the Bureau of Ships; ray tracing, physics, and astronomy research of Harvard faculty; and a test calculation for John von Neumann on the design of the implosion device for the atomic bomb (Aspray, 2000).

Conclusion

When it comes to architectures, the Colossus comes closest to Von Neumann's stored program concept (Von Neumann, 1945). It was built with a very specific purpose, and had limited programmability, though nevertheless, it held it's program internally.

By comparison the Mark I was the opposite. It held its initial data internally via the 60 slots for constants, and it took it's programming via punch tape. The Mark I was however much more general purpose, though still designed and built specifically to solve applied math problems.

Similarly, the Z4 was designed to be general purpose and built to solve mathematical equations, though it was the first to be implemented to use binary.

References

Aspray William (2000). Was Early Entry a Competitive Advantage. IEEE Annals of the History of Computing. Vol. 22, No. 3, pp 42-87.

Copeland B Jack (2004). Colossus: It's Origins and Originators. IEEE Annals of the History of Computing. Vol. 26, No. 4, pp 38-45.

Good, Michie, & Timms (1945). General Report on Tunny. Retrieved on Aug. 30, 2006 from http://www.cs.usfca.edu/www.AlanTuring.net/turing_archive/archive/index/tunnyreportindex.html.

IBM Archives (2002). Feeds, Speeds and Specifications. Retrieved on Sept. 02, 2006 from http://www-03.ibm.com/ibm/history/exhibits/markI/markI_feeds.html

Randell B (1980). The COLOSSUS. Retrieved on Aug 31, 2006 from http://www.cs.ncl.ac.uk/research/pubs/books/papers/133.pdf

Von Neumann John (1945). First Draft of a Report on the EDVAC. IEEE Annals of the History of Computing. Vol. 15, No. 4, pp 27-75.

Zuse Horst (2001). The Life and Work of Konrad Zuse. Epe Magazine. Retrieved on Aug 31, 2006 from http://www.epemag.com/zuse/default.htm#index.