The Military Use of Alan Turing

Andrew Hodges*

Alan Turing (1912-1954), British mathematician, was critical in the Anglo-American decipherment of German communications in the Second World War. This experience enabled him to formulate an original plan for the digital computer in 1945, based on his own 1936 concept of the universal machine. He went on to found the program of Artificial Intelligence research. This article discusses the relationship between these developments, and more general questions of mathematics and war illustrated by Alan Turing's life and work.

The British mathematician, Alan M. Turing (1912–1954) played a critical role in the Second World War, as the chief scientific figure in the Anglo-American decipherment of German military communications. Furthermore, his work was central to the emergence of the digital computer in its full modern sense in 1945. However, the secrecy surrounding his work was so intense that until the 1970s only hints of it were published. This secrecy was enhanced by the mystery of his sudden death in 1954 and the effective taboo, which prevailed for twenty years, on any public mention of his homosexuality. To those interested in the true history of the computer, Alan Turing's role remained as elusive as the myth of Atlantis. This secrecy has now almost completely been dispelled, partly through this author's work (Hodges 1983), but only to reveal a much deeper enigma of Alan Turing, who gave himself first to the purest and most timeless mathematics, but then applied himself to its most urgent and timely practice. What did Alan Turing think of his intellectual and moral involvement in the world crisis? And what is the true assessment of the impact of the war on his scientific work?

This article will review Alan Turing's mathematical work in the Second World War, discuss how this relates to the history and philosophy of computing, and then raise the wider question of his place in mathematics and war.

Turing's role in the Second World War was largely dominated by the particular form of the Enigma ciphering machine as elaborated for military and naval purposes by the German authorities. For a recent complete description of the Enigma see (Bauer 2000). Essentially, it was Turing who picked up the relay baton when the Polish mathematicians shared their brilliant cryptanalytic work with Britain and France. It then fell to him to pass on the baton, by sharing British achievements with the United States.

* Wadham College Oxford University OX1 3PN, UK. Email: andrew@synth.co.uk

B. Booß-Bavnbek et al. (eds.), *Mathematics and War*

Alan Turing's primary role stemmed partly from the fact that he was the first scientific figure to join the British cryptanalytic department, the so-called 'Government Code and Cypher School,' which until 1938 was staffed essentially by the language-based analysts of the First World War. (One reason for Turing's recruitment may have been that he had, through his Fellowship of King's College, Cambridge, personal connections with that older British generation; in particular J. M. Keynes may well have formed an important link.) Turing was brought into the work on a part-time basis at the Munich crisis period, and joined full-time immediately on declaration of war. Meanwhile an Oxford mathematics graduate, Peter Twinn, was recruited through open advertisement in 1938, and this belated acceptance of the modern world was shown also in the development of a modern communications infrastructure for the new headquarters at Bletchley Park, Buckinghamshire. Nevertheless, the Polish mathematicians were well in advance at the time of the now famous meeting in July 1939. They had used group-theoretic algebra to deduce the Enigma rotor wirings from information obtained by spying; they had noticed and used other group-theoretic methods and mechanical methods to exploit certain simple forms of indicator system that were then in use by the German forces. It is not clear to what extent Turing had discovered these independently in early 1939 – his report (Turing 1940) does not say – but in any case the Polish group had successfully made an all-important guess which had eluded the British: this was the order in which the keyboard letters were connected to the first rotor. They were in fact in the simple order ABCD.... This almost absurdly simple fact was the most critical piece of information imparted by the Poles.

In late 1939, Turing initiated the two most decisive new developments: he saw the 'simultaneous scanning' principle of what became the British 'Bombe', and he deduced the form of the more sophisticated indicator system that was being used for the German Naval communications.

Turing's 'Bombe' was an electromechanical machine of great logical and technical sophistication. Its property was this: given a stretch of ciphertext and the corresponding plaintext, it could search through all possible settings of the military Enigma and detect those which could possibly have been responsible for the encipherment. It is not difficult to see, from simple counting arguments, that a 'crib' of about 20 letters will generally serve to identify such a setting. (The reader may take it that, once some penetration into cipher traffic has been made, such a 'crib' is not impossible to find.) It is much harder to see that this theoretical possibility can be matched by any practical method. In particular, the Stecker or plugboard complication introduced in the military Enigma had so many possible settings that serial trial was impossible. In fact serial trial was indeed necessary for searching through the possible positions of the rotors. But Turing's great discovery was that the huge number of plugboard possibilities could effectively be tested in parallel, and virtually instantaneously. His idea was this: suppose we are testing, in the serial sequence, a particular rotor setting. A plugboard setting consists of a number of pairs like (AJ), (UY), representing the swapping of letters performed by the plugboard on entry to, and on exit from, the rotors. There are 150,738,274,937,250 possible settings consisting of ten such pairs, the choice normally made. However there is no need to work through such a number of possibilities. Instead, consider