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

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

the smaller number of 325 basic pair-possibilities: (AA), (AB), (AC) ... (ZZ), where '(AA)' represents the letter A being left unchanged by the plugboard. Now, given any one basic pair-possibility, e.g., (AA), knowledge of the plaintext, ciphertext, and rotor setting will imply various other pair-possibilities, and these in turn yet more. Turing saw first, that finding a single 'contradiction' serves to eliminate a possibility: that is, if by following the implications (AA) can be shown to imply (AE), then (AA) must be false. He saw the less obvious point that by allowing the logical deductions to continue, (AA) would generally imply all of (AB) ... (AZ); hence all must be false; hence the rotor position being tested could not possibly be correct. Turing was proud of this counter-intuitive idea, of continuing to follow through the consequences of what must be false propositions. He said it was akin to the principle in mathematical logic that 'a false proposition implies any proposition.'

Turing also saw how to embody these 'deductions' simply in wired connections between rotors and terminals, so that the flow of implications would take place at the speed of electric current. (But it took another Cambridge mathematician, W. G. Welchman, to improve the circuitry with the 'diagonal board' which automatically identified (AB) with (BA), and so on; it is curious fact that Turing missed this simple idea.) Finally, it was essential that the machine could be equipped to detect the possibility of a correct rotor position, with logical switching capable of recognising an incomplete bank of pair-possibilities. With this achieved by the engineers of the British Tabulating Machinery company, Turing's Bombe yielded the central process on which Enigma decryption rested throughout the War. Its principle was highly non-trivial, and it apparently went unnoticed by G. Hasenjäger, the young German logician who was Turing's unseen opponent in this war of logic (Bauer, 2000).

As already noted above, in the business of searching through the 26^3 possible rotor positions, no improvement was possible on serial trial using the equivalent of moving Enigma rotors, so that improvements rested on having ever faster, more reliable machines produced in larger numbers. For the question of the choice of rotors and their order, however, which was particularly relevant for the Naval Enigma problem, Turing developed a method called 'Banburismus' which, particularly in 1941, much improved upon the simple trial of the possibilities. This method rested on the logical details of the turnover positions of the different rotors, but also on assessing the statistical identification of likely 'depths' – two different stretches of message, both sent on the same Enigma settings. For detecting depths objectively, giving a reliable probability measure to them, Turing developed a theory of Bayesian inference. The most striking feature of his theory was his measurement of the weight of evidence by the logarithm of conditional probabilities. This was essentially the same as Shannon's measure of information, developed at the same time. This theory was developed into sophisticated methodology (Good 1979, 2000). Whilst the logical principle of the Bombe, and its amazingly effective application, was perhaps Turing's most brilliant single idea, his statistical techniques were more general and far-reaching. In particular, they were also applied to the quite different Lorenz cipher system employed by Germany for high-level strategic messages. Thus it was Turing's theory of probability estimation that underlay

the methods mechanised by the large electronic 'Colossus' built in 1943–45 to decipher this type of traffic.

The latter half of the war saw the relay baton pass on to the USA. Turing himself had to cross the Atlantic, at the height of the battle, in connection with naval Enigma crisis of 1942 and the building of American Bombes at Dayton, Ohio. Besides transferring British expertise in Enigma-breaking to the United States, he also had a new top-level role in inspecting and reporting on the American equipment for speech encipherment (to be used by Roosevelt and Churchill), and became fully acquainted with the use of information sampling theory as well as the electronic technology involved. It is fair to say that Turing most enjoyed a pioneering period of breaking into the unknown, and flourished best in such settings; he was not so happy at detailed follow-up or development. After 1943 he spent much of his time on a freshly self-imposed problem: the design of an advanced electronic speech scrambler of a much more compact form than the American equipment he had inspected (Hodges 1983, p. 273).

Sometimes it is blithely asserted that what one mathematician can do, another can undo. Not so: the possibilities of cryptanalysis are highly contingent on details; and even if a system is breakable in the long term, short term considerations may be of the essence. The German military adaptation of the Enigma might have made it unbreakable; the British version of the Enigma, which has attracted far less attention, had more rotors and a non-reciprocal plugboard, and was apparently invulnerable to German attack. The successful continuation of the Polish work may very well have depended critically on Turing as an individual. It was not that Turing merely played the expert part expected of him. Rather, it was at a time when a distinctly pessimistic attitude prevailed, that Turing took on the Naval Enigma problem precisely because no-one else thought it tractable, and so he could have it to himself. This individualistic approach was also necessary in developing from scratch a suitable statistical theory. Thus, it can well be maintained that the Anglo-American command of the Atlantic battle, crucial in the central strategy of the Western war, was owed to Alan Turing's work.

Turing did not create great new fundamental mathematics in this work, but he brought to bear the insights of a deep thinker. The Bletchley Park analysts compared their work with chess problems, and G. H. Hardy had famously called chess problems the hymn tunes of mathematics, as distinct from serious, interesting problems (Hardy 1940). Yet unusually these military hymns had some beauty. In a remarkable comment on an episode in mathematics and war, the contemporary chronicler of the Naval Enigma section ended by saying (Mahon 1945). In finishing this account of Hut 8's activities I think that it should be said that while we broke German Naval Cyphers because it was our job to do so and because we believed it to be worthwhile, we also broke them because the problem was an interesting and amusing one. The work of Hut 8 combined to a remarkable extent a sense of urgency and importance with the pleasure of playing an intellectual game.

It can, however, be argued that more important than the direct application of new mathematics was the influence of his wartime experience in leading Turing from being a pure theorist of computation to being the leading expositor of an

actual electronic design for a modern computer. At the age of twenty-four, Turing had published what is now his most celebrated work, defining computability (Turing 1936–1937). Its motivation lay in pure mathematical logic, clarifying the nature of an 'effective method' with the Turing machine concept. It did not set out to assist practical computation in any way. Yet it did produce the constructive and highly suggestive idea of the universal Turing machine, and in fact Alan Turing was never entirely 'pure' in his approach: bringing 'paper tape' into the foundations of mathematics was itself a striking breach of the conventional culture. As we shall see, he took an interest in the practical application of his ideas even in 1936. But Turing's harmonious collaboration with the engineers of the Bombe took him very much further towards practicality, indeed into the most advanced practical engineering of 1940. Then his acquaintance with the world-leading technology of the Colossus showed him the viability of an electronic digital machine capable of embodying the idea of the universal machine – in modern terms, a computer with modifiable stored program. Turing was able to write a detailed proposal for such a computer, the ACE, in 1945–1946, and was able to survey from a position of considerable strength all the possible forms of data storage available at that point (Turing 1946).

In discussions of the origin of the computer there is an inevitable rivalry between the claims of mathematics and engineering. Engineers, often overlooked and accorded a low social status, do not take kindly to being treated as mere technical assistants when in fact they have contributed immensely skilled and creative solutions. Nevertheless, whether we speak of the computer, or of machines such as the Bombe or Colossus, no engineer originally conceived the nature and purpose of the machine: the conception was that of mathematicians. The point of the Bombe was to implement Turing's brilliant logic; the point of the Colossus was to implement ingenious developments of his statistical theory. The point of the modern computer is that it implements Turing's universal machine, on which instructions can be stored and manipulated in exactly the same way as data. It is usually said that von Neumann, in formulating the EDVAC plan in 1945, played the same mathematical role independently, but Martin Davis has recently argued that von Neumann could not have played this part without learning of Turing's work before the war (Davis 2000).

However, Turing was unusual in wishing to dominate every aspect of the computer design: not only its central principle and purpose, but the applications for which it would be used, and the details of its design. His report (Turing 1946) for the National Physical Laboratory, London, covered all of these. In every way it reflected the influence of his war work, but there was an irony. Official secrecy about the wartime success was total and prevented Turing from arguing from his extensive experience to establish some influence over the engineering side of the problem. So although his report alluded to important military applications in the solution of combinatorial problems, showed other influences of non-numerical Bletchley Park work, and claimed Foreign Office support, the NPL management continued to regard mathematics and engineering as belonging to two distinct planets and blocked Turing's efforts to argue otherwise.

Turing was particularly frustrated over the inability to command the necessary technology, because although vital for the trying out of a practical form of a universal machine, the actual form of the implementation was essentially a secondary matter. Turing correctly saw his ACE plan as necessarily obsolescent, leading the way to better machines, built using faster control circuits and larger storage systems. Of far greater significance, in Turing's plans, was the scope of what a practical universal machine would be doing: namely, implementing an open-ended array of software or as he called it, instruction tables.

In that first report he wrote a number of key remarks about the potential of the universal machine:

> It is intended that the setting up of the machine for new problems shall be virtually only a matter of paper work... There will be positively no internal alterations to be made even if we wish suddenly from calculating the energy levels of the neon atom to the enumeration of groups of order 720. Instruction tables will have to be made up by mathematicians with computing experience and perhaps a certain puzzle-solving ability. There will probably be a great deal of work of this kind to be done, for every known process has got to be translated into instruction table form at some stage. The process of constructing instruction tables should be every fascinating. There need be no real danger of it ever becoming a drudge, for any processes that are quite mechanical may be turned over to the machine itself.

In (Turing 1947) he elaborated on the potential for computer languages opened up by this last remark:

> Actually one could communicate with these machines in any language provided it was an exact language, i.e. in principle one should be able to communicate in any symbolic logic, provided that the machine were given instruction tables which would allow it to interpret that logical system...

These and other observations mapped out the scope of the computing industry of the future (although Turing did remarkably little to implement his prophetic ideas for computer languages). But, at a more profound level still, even this software manifesto was also secondary. He was, he said, building a brain: embarking on an experimental programme for what he called 'intelligent machinery', or what would now be called 'artificial intelligence.'

This deeper scientific programme was also influenced by his war experience. Before the war Turing had, in his work on ordinal logics, apparently accepted the standpoint of Gödel in which the mathematician does something beyond the scope of rule-following when seeing the truth of a Gödel sentence. It has been argued by the author (Hodges 1997, 2002), that Turing must have had a change of mind, or at least a definite clarification of mind, in about 1941. By that time the spectacle of the Bombes and of the mechanisation of human guessing and judgment by Bayesian statistical methods had supplied a vivid argument to the effect that the concept of being 'merely' mechanical was misleading. To capture the spirit of the time, it is worth noting from a recently declassified document (Good et al. 1945) the vivid

impression that the beginning of the electronic information technology age made on its beholders:

> It is regretted that it is not possible to give an adequate idea of the fascination of a Colossus at work [...] the fantastic speed of thin paper tape around the glittering pulleys [...] the wizardry of purely mechanical decoding letter by letter (one novice thought she was being hoaxed); the uncanny action of the typewriter in printing the correct scores without and beyond human aid [...].

Turing, even though he perfectly understood what was going on, was doubtless also influenced by this magical power of the purely mechanical. Possibly, Turing was also encouraged by exposure to intellectual currents which suggested thinking of the nervous system in behaviourist terms.

In any case, it is clear that by 1945 Turing had decided that the brain did not actually perform any uncomputable operations of the kind suggested by Gödel's theorem. He had formulated his 'mistakes' argument: that in assessing mathematical proofs the brain will sometimes make mistakes, and that accordingly Gödel's theorem does not have any force. His guiding thought was that the brain must be effectively a finite machine and therefore performs operations which can, at least in principle, be run on a universal machine, the computer. A further report (Turing 1948) explored the question of how a machine could be led to perform actions which appear not to be of a 'mechanical' nature, as understood in common parlance. Turing discussed program self-modification, networks of logical elements as models of neuronal systems, the idea of 'genetical search.' His ideas for emulating human 'education' combined what would now be called top-down and bottom-up approaches to Artificial Intelligence. This report was the basis of his more famous philosophical paper (Turing 1950).

Turing spent a year at Cambridge to do this theoretical work in 1948, because the National Physical Laboratory was making such desultory progress with implementing his computer plan. While he was there, another opportunity appeared to open. The key figure was the topologist M. H. A. Newman, the Cambridge lecturer who had introduced Turing to the frontier of mathematical logic in 1935, the first reader of Turing's consequent logical discoveries, and indeed to some extent Turing's collaborator in logic. Newman took the idea of the universal machine with him when he went to Manchester University as professor of pure mathematics in 1945. He also took an acquaintance with electronics, since he had directed the development of the Colossus as applied to the Lorenz cipher problem at Bletchley. In fact, he was equipped with all the force of Turing's ideas except that he had none of Turing's interest in mastering electronics for himself.

Newman's fervent desire was that the concentration and investment of scientific resources that had been shown possible in the emergency of the war, should now be dedicated to pure science. He rapidly made a proposal to the Royal Society, and was successful in getting a large grant for a computer on which to do research in mathematics (including for instance the Four-Colour Theorem), on an ambitious and long-term scale. Newman was able to recruit for his project the leading electronic engineers who came to Manchester from wartime radar development work, and he imparted to them the essential stored-program ideas that had to be implemented.

Newman offered Turing the role of running this emergent Computing Laboratory. Turing accepted. But even before he arrived, the success in June 1948 of the engineers' prototype meant that it was demanded for the British atomic bomb development. The government contract went to the engineers, not to Newman; the Royal Society connection was abandoned. Turing was sidelined along with Newman himself, and had to relaunch himself with quite new work: his mathematical theory of morphogenesis. By 1950 it was the end of the road for the synthesis and collaboration achieved in the Second World War. What is now the engineering discipline of 'computer science' took on a life of its own and the connection with mathematics was largely lost, Turing's legacy being abandoned with it.

There is, however, an important caveat to be made here: we do not know what Turing did as secret work for GCHQ after 1948. This Cold War question is still as secret now as the Second World War operations were in 1970. And it opens an aspect of the subject of Mathematics and War where all is speculation, an unresolved enigma. Perhaps the most extraordinary aspect of Alan Turing's story is his role as a great innocent figure of pure science, yet at the heart of the most urgent world crisis. It is a magical picture, but this sequel to it is still incomplete and obscure.

Was he involved in the Venona problem, which involved tracking KGB messages to and from its western agents? If so, was he eager for participation in the work against Soviet influence? Or was he only responding to a strong personal plea from Hugh Alexander, who from being Turing's deputy in 1941 had risen to become director of GCHQ in 1952? Or was it more the challenge of another 'interesting and amusing' mathematical problem? What were the inner springs? We do not know. I turn now to those more general questions about the setting of Turing's mind in the world of war.

There is a common joke about Military Intelligence being a contradiction in terms, and the concept of the 'military use of mathematics' has a similar problem, for mathematics is not just used: it has to be created by awkward, non-standard, individual mathematicians. A subordinate cannot simply be ordered to do something extraordinary, unexpected and innovative, such as breaking a cipher system that is supposed to be unbreakable. Anyone approaching such work in the spirit of carrying out an order, is unlikely to be inspired. Turing exercised a wilful initiative and went against prevailing wisdom to attack the naval Enigma systems. Such an unorthodox success, however welcome in the desperate situation of 1940, clearly signified a certain danger for government control: if people act from self-willed initiative, rather than following orders and duty, they may progress to some other self-willed initiative less to the taste of the State. As later became well known, some of those who decided for themselves to fight Germany, also chose with equal force to assist the USSR. In the postwar period the emergent idea of 'security' had to take this into account, and after 1948 Turing was bound to find that the wartime personal networks, class-based trust and easy acceptance of his eccentricity no longer applied in state affairs.

What makes this particularly interesting and piquant in discussing Turing's biography, is that the interplay of rule-following Duty and creative Will was central to Turing's own theory of mind and machine. In his 1948 report on machine

intelligence he described the problems to be addressed in terms of 'discipline' and 'initiative,' the latter being necessary to anything that could genuinely be called 'intelligence'. In his discussion of machine intelligence, a dialogue between mechanical and creative, obedience and surprise, runs throughout. It is a striking fact that he came down so strongly on the side of saying computers would be able to show intelligence, when he of all people knew the significance of creative originality. But this dialogue of compliance and rebellion – and resolving it by standing aside, withdrawing – ran through his life. In his 1950 paper, Turing made a joking reference to Casabianca, the boy on the burning deck who carries out his orders relentlessly as a computer, oblivious to common sense, and this image of military duty went back to his childhood learning of the poem at preparatory school, still within a First World War world. Even as a child he had known the limitations of rule-following, and had found the precepts of his class largely incomprehensible.

Yet Alan Turing had not been a rebel against his class or his school. In his upper-middle-class environment, dominated by the suffocating ideology of the Public School, he had neither complied nor rebelled; he had largely withdrawn into a scientific world of his own. There was, however, a moment in 1933 when the Anti-War student movement at Cambridge articulated the change that had taken place since the world of Duty plunged to disaster in 1914, and at twenty-one, Turing joined it and placed himself clearly on the modernist side. His contemporaries were insisting on deciding for themselves what to fight for, and the emergent left-liberal side decided not to fight for that old chant of Duty: 'King and Country.' 'Blatant militarist propaganda', Turing called a cinema recruiting film called 'Our Fighting Navy.' Ten years later, Alan Turing was to be seen by his WRNS assistants 'prancing' in his Bletchley Park hut at the news of the sinking of the Scharnhorst by that very Navy. Of course, the 1933 enlightenment had coincided with the one development that made war justifiable to the enlightened: the transformation of Europe's strongest industrial power into the aggressive engine of murderous fascism.

The young Alan Turing was well aware of the shock of Nazi Germany, and it was obvious where his sympathies lay. When visiting Germany in 1934, Turing's travelling companion was surprised to see how naturally a German socialist seemed to confide in him. Later, he was immediate in his response to the 1938 wave of persecution, and sponsored a young Jewish refugee. But in the intellectual context of the 1930s, dominated by the question of Communist party policy, Alan Turing's 1933 political engagement was short-lived; he was regarded as 'not a political person.' Alister Watson, who introduced him to Wittgenstein, was a Communist party member, as was also the young Robin Gandy who later became his student and closest friend. Others of Alan Turing's friends were fully engaged with political and economic issues. But for Alan Turing, it was the 'phoney' that attracted his scorn rather than political opposition; the compromises and alliances of political action were alien to him.

In temperament he was closer to his first lover, James Atkins, another mathematics student of his year, who was and remained a pacifist while becoming a professional musician. But Alan Turing found in the music of mathematics the means to undermine Nazi Germany. In 1936, just after he had completed his famous paper on computable numbers, and had arrived in Princeton, Alan Turing wrote to his mother, who was apt to ask him 'but what use is it':

> I have just discovered a possible application of the kind of thing I am working on at present. It answers the question 'What is the most general kind of code or cipher possible' and at the same time (rather naturally) enables me to construct a lot of particular and interesting codes. One of them is pretty well impossible to decode without the key, and very quick to encode. I expect I could sell them to H. M. Government for quite a substantial sum, but am rather doubtful about the morality of such things. What do you think? (Turing 1936)

What theory of a 'most general' cipher he had in mind, what was his theory of cipher security, and and what were the interesting codes, remain unknown. Nor, in Turing's reference to the question of 'morality of such things', is it clear whether he means the morality of selling his work, or the morality of doing military work. However, whatever moral consideration Turing found most perplexing, the fact is that at Princeton in 1937 he proceeded with a cryptographic idea embodied in an electromagnetic relay device, and saw it specifically as relevant to looming war with Germany. It is very possible that this device was indeed offered to the British government, and was the reason why he became the first scientific officer at the Government Code and Cypher School. He received a salary, and later some special payments, but what was more important, he paid a moral price: he sacrificed the freedom of his mind.

Freedom, to Alan Turing, was more important than questions of money. He waxed more eloquent over the Abdication crisis than over any other issue, expressing, perhaps naively, a support for the King's freedom to marry, and deploring the 'hypocrisy' of the Archbishop of Canterbury. But tellingly, he deprecated the indiscretion of the ex-King in allowing state papers to be seen by Mrs. Simpson. (Hodges 1983, p. 122) Soon afterwards, he had to promise to keep State secrets himself. But no doubt he found it exciting to be let into government's innermost secrets, and perhaps too the technical challenge of the Enigma problem became immediately and addictively fascinating.

The Abdication issue was an anticipation of his own quandary after his arrest as a homosexual in 1952. For in 1952 he showed himself the most devoted to personal freedom, but at the same time, as his friends did not know, he was the most tightly bound by secrecy at the highest level in the Anglo-American alliance. He was ahead of his time, as with all things, in an open insistence on his sexual identity, and his response to his trial and punishment (with hormone injections) in England was to travel over Europe. News of the Forbundet af 1948 organisation in Denmark and Norway, essentially the first open European gay movement, was a particular attraction.

It has yet to be disclosed what the security officials of Britain and the United States made of his priorities, but at a time when American commentators tended to place homosexuality on a level with communism as a danger to American interests it is not surprising that Turing was watched closely in 1953 when a young Norwegian tried to visit him. He was probably naive on such questions, for homosexuality had not been in itself a well-defined 'security' issue in 1939–1945. As Donald Michie has emphasised, there were gay men at Bletchley Park even more open

than Alan Turing. The change towards explicit 'vetting' for homosexuality, and the explicit exclusion of homosexuals, came only after 1948, and possibly Turing was unaware of the position in which he had placed himself. So in 1952 he was shocked to be excluded from secret work, and in 1953 highly indignant to be the object of police surveillance. It was this 'security' development which for society generally, as individually for Turing, created a change of consciousness, politicising a hitherto 'personal' issue.

In assessing Alan Turing's place in mathematics and war, we cannot overlook the culture of mathematics itself, of which he was part. It was and is a reticent and quiet culture. The introduction to this article mentioned a double secrecy surrounding Alan Turing's life: the official secrecy surrounding cryptology, and the social taboo about his sexuality. But it is a general reality for mathematicians that the very nature of their subject attracts almost as great an enforced silence. Very recently, mathematical culture has dipped its toe in the business of fortune and celebrity, but in the long aftermath of the Second World War it had no such profile. The contrast with the prestige of physics after the open and visible atomic bomb is particularly notable. The Second World War lesson was well learnt, and the National Security Agency and its British counterpart GCHQ became major employers of mathematical graduates, so that the postwar flowering of mathematics has to some extent rested upon the demands of the most secret government work. But the near-invisibility of mathematics combines easily with the total secrecy to make this alliance one incapable of arousing public interest.

Gauss called mathematics the queen of the sciences, who sometimes condescends to serve. The priorities of self-effacing mathematical culture are well illustrated by Newman, who was faced with the very difficult task of writing a Biographical Memoir of Turing immediately after his dramatic suicide in June 1954. Turing had been elected a Fellow of the Royal Society in 1951 and as such called for such a detailed Memoir, which appeared as (Newman 1955).

Alan Turing had died at the height of his powers in 1954, wrote Newman, who interestingly did not say that his apex lay either before or in the Second World War. Because of its secrecy, Newman could say nothing of significance about the wartime work, but even allowing for this constraint, he severely understated Turing's contribution with bland expressions such as 'a mild routine' and 'congenial set of fellow-workers.' Newman also understated Turing's role in the emergence of the computer. He stated that Turing's theory of the universal machine was not known by the designers of post-war digital computers, and omitted Turing's own design (Turing 1946) from his list of Turing's works. Newman gave far more attention in his Memoir to Turing's very abstract and difficult work on ordinal logics (Turing 1939). Above all, he portrayed the Second World War not as allowing Turing to turn the logical theory into practical application, but as interrupting Turing in his work on the logic of the uncomputable and the Riemann Hypothesis, preventing him from settling into a 'serious' problem. Thus subtly, perhaps unconsciously, he put an Anti-War impetus into his assessment – discounting those subjects that the war had accelerated, emphasising those that it had interrupted. His priorities were essentially the reverse of those that modern computer science would expect.

Newman was perfectly aware of the importance of Turing's work to worldly affairs. Newman knew it at first hand, and in no way dissented from the common agreement that Turing was the leading figure in the wartime work. In 1946 Newman wanted to reject the formal decoration he was offered by the government because he considered the rank of OBE that had been awarded to Turing to be so absurd an undervaluation. But Newman had been repelled from the emergent world of the computer, and it seems that by 1955 he considered both war and computation, however important politically and economically, to be secondary, transitory, matters compared with the timeless mathematics that it was his task to assess. Perhaps he was right: the queen of the sciences sometimes sees far ahead of her subjects. It is a point of view that Turing would have respected: in his last period he probably drew as much strength as he could from the Platonic qualities of the mathematical sciences, as counter to the harsh ironies of the world.

In 1953/4 Turing wrote a last semi-popular article on undecidable problems (Turing 1954a) and studied the axioms of quantum mechanics: topics that owed nothing to his Second World War experience. It seems that he wanted to go back to what he had learnt in 1932 from von Neumann's axioms of quantum mechanics, and to think out for himself a new quantum mechanical theory, focussing on the problem of when and how wave-function 'reduction' is supposed to take place (Gandy 1954). Since the 1980s, Roger Penrose's views on logic, complex analysis and physics (Penrose 1989, 1994) have made this late development particularly intriguing. Penrose's views stand as the most radical contradiction of Turing's on the possibility of machine intelligence, but are based on the same materialist ground and focus on the very topics that perplexed Turing most: the interpretation of Gödel's theorem and the reality of a quantum-mechanical infrastructure to the brain. In particular (Penrose 1994) offers a detailed mathematical critique of Turing's 'mistakes' argument, as well as concentrating on the puzzle of the 'reduction' process. Had Turing followed his late interests further, and combined them with his knowledge of computability, he might have seen something much deeper connecting logic, space-time and quantum mechanics, than anything he did for computers. We cannot know.

The Second World War obviously stimulated progress in significant areas of mathematics and science. But maybe it stunted the growth of more subtle things that might have been. It is perhaps too soon to assess the balance. Many mathematicians might feel, though would perhaps not say openly, that the principle of the computer is a trivial matter compared with the serious problems of mathematics. Newman probably took this view in 1955; it is hard to imagine what Turing really thought, for he was no typical mathematician and had a vision that only partially overlapped with that of the classical discipline.

At the end, Alan Turing wrote in March 1954 a cryptic joke about quantum mechanics to his friend Robin Gandy, on a postcard (Turing 1954b) headed 'Messages from the Unseen World':

> The exclusion principle is laid down purely for benefit of the electrons themselves, who might be corrupted (and become dragons or demons) if allowed to associate too freely.

Free association was, of course, just what the State had forbidden to him. But this dialogue of acquiescence and dissent; of seriousness and humour; of self-assertion and withdrawal; abstraction and concreteness – these last words were typical of Alan Turing in mathematics and in war.

References

Bauer, F. L. (2000): *Decrypted Secrets* (new edition), New York: Springer 2000.

Davis, M. (2000): *The Universal Computer,* New York: Norton 2000.

Gandy, R. O. (1954): Letter to M. H. A. Newman, in King's College archive, published in volume 4 of The Collected Works of A. M. Turing, eds. R. O. Gandy and C. E. M. Yates, Amsterdam: North-Holland 2001.

Good, I. J., Michie, D., et al. (1945): General report on Tunny, p. 327. This document became available at the Public Record Office, London in 2000.

Good, I. J. (1979): Studies in the History of Probability and Statistics. XXXVII. A. M. Turing's statistical work in World War II, *Biometrika* 66 (1979), 2, pp. 393-396.

Good, I. J. (2000): Turing's anticipation of Empirical Bayes in connection with the cryptanalysis of the Naval Enigma, *J. Stats. Comp. & Simul*. 66, pp. 101-111, and in volume 4 of The Collected Works of A. M. Turing, eds. R. O. Gandy and C. E. M. Yates, Amsterdam: North-Holland 2001.

Hardy, G. H. (1940): *A Mathematician's Apology,* Cambridge: Cambridge University Press 1940.

Hodges, A. (1983): *Alan Turing: the Enigma,* London: Burnett, New York: Simon & Schuster; new editions London: Vintage 1992, New York: Walker 2000.

Hodges, A. (1997): *Turing, a natural philosopher,* London: Phoenix; also New York: Routledge 1999. Included in: *The Great Philosophers* (eds. R. Monk and F. Raphael), London: Weidenfeld and Nicolson 2000.

Hodges, A. (2002): Alan M. Turing, in: E. N. Zalta (ed.), *Stanford Encyclopedia of Philosophy,* http://plato.stanford.edu.

Mahon, A. P. (1945): *The History of Hut Eight*, Public Record Office, London 1945, HW 25/3.

Newman, M. H. A. (1955): *Alan M. Turing*, Biographical memoirs of the Royal Society 1955, p. 253.

Penrose, R. (1989): *The Emperor's New Mind,* Oxford, New York: Oxford University Press 1989.

Penrose, R. (1994): *Shadows of the Mind,* Oxford, New York: Oxford University Press 1994.

Turing, A. M. (1936): Letter to Sara Turing, in Kings College Archive; see also Hodges 1983, p. 120.

Turing, A. M. (1936-37): On computable numbers with an application to the Entscheidungsproblem, *Proc. London Maths. Soc.*, ser. 2, 42 (1936-37), pp. 230–265; also in volume 4 of The Collected Works of A. M. Turing, eds. R. O. Gandy and C. E. M. Yates, Amsterdam: North-Holland 2001.

Turing, A. M. (1939): Systems of Logic defined by Ordinals, *Proc. Lond. Math. Soc.*, ser. 2, 45 (1939), pp. 161–228; also in volume 4 of The Collected Works of A. M. Turing, eds. R. O. Gandy and C. E. M. Yates, Amsterdam: North-Holland 2001.

Turing, A. M. (1940): *Mathematical theory of ENIGMA machine*, Public Record Office, London 1940, HW25/3.

Turing, A. M. (1946): Proposed Electronic Calculator, report for National Physical Laboratory, Teddington; published in: *A. M. Turing's ACE Report of 1946 and Other Papers* (eds. B. E. Carpenter and R. W. Doran), Cambridge, Mass.: MIT Press 1986; and in Volume 3 of The Collected Works of A. M. Turing (ed. D. C. Ince), Amsterdam: North-Holland 1992.

Turing, A. M. (1947): Lecture to the London Mathematical Society, typescript in King's College, Cambridge, published in. *A. M. Turing's ACE Report of 1946 and Other Papers* (eds. B. E. Carpenter and R. W. Doran), Cambridge, Mass.: MIT Press 1986; and in Volume 3 of The Collected Works of A. M. Turing (ed. D. C. Ince), Amsterdam: North-Holland 1992.

Turing A. M. (1948): Intelligent machinery, unpublished report for National Physical Laboratory; published (ed. D. Michie) in *Machine Intelligence* 7 (1969), and in Volume 3 of The Collected Works of A. M. Turing (ed. D. C. Ince), Amsterdam: North-Holland 1992.

Turing A. M. (1950): Computing machinery and intelligence, *Mind* 49 (1950), pp. 433-460.

Turing A. M. (1954a): *Solvable and Unsolvable Problems*, Penguin Science News 31 (1954).

Turing, A. M. (1954b): Postcard, quoted in volume 4 of The Collected Works of A. M. Turing, eds. R. O. Gandy and C. E. M. Yates, Amsterdam: North-Holland 2001); reproduced in Hodges 1983, p. 513.

http://www.springer.com/978-3-7643-1634-1

Mathematics and War
Booß-Bavnbek, B.; Høyrup, J. (Eds.)
2003, VIII, 420 p. 79 illus., Softcover
ISBN: 978-3-7643-1634-1
A product of Birkhäuser Basel