Peter J. Hilton received his D.Phil. from Oxford University in 1950, working under the supervision of his war-time friend J. H. C. Whitehead. He also received a Ph.D. from Cambridge University in 1952, and an honorary D.Sc. from Memorial University in 1983. He has held positions in this country at Cornell University, the University of Washington, Case Western Reserve University, and the State University of New York at Binghamton. He has published extensively in the areas of algebraic topology, categorical algebra, homological algebra, and mathematical education. Among his numerous books are An Introduction to Homotopy Theory, *(with S. Wylie)* Homology Theory: An Introduction to Algebraic Topology, *and (with Urs Stammbach)* A Course in Homological Algebra.

Reminiscences of Bletchley Park, 1942–1945

PETER HILTON

1. Introduction

In October 1941, a letter written by Stuart Milner-Barry (now a 'Treasury Knight'), Hugh Alexander (sometime British chess champion), Gordon Welchman (Cambridge mathematician), and Alan Turing, and addressed to Winston Churchill, was handed in at 10 Downing Street. The letter, whose full text appears as an appendix to **[Hinsley]**, requested Churchill to order a substantial increase in the Bletchley Park staff of cryptanalysts working on high-grade German ciphers. Bletchley Park was the wartime headquarters of the Government Code and Cipher School, and these four men had already been inducted, from their more sheltered peacetime habitats, into service with GCCS (now known as Government Communication Headquarters, or GCHQ).

To his great credit, Churchill ignored the unorthodoxy of the approach, bypassing "normal channels," and initialed a minute to General Ismay demanding immediate action. This minute led eventually to the recruitment of a very fine team of young — and not so young — mathematicians to Bletchley Park, to work on decoding messages enciphered on the Enigma machine and its very sophisticated successor, which we called Fish ("Geheimschreiber" being too much of a mouthful). However, the immediate effects of Churchill's minute were less spectacular. An interviewing team arrived at Oxford in November, seeking to recruit a mathematician with a knowledge of modern European languages. There did not exist in Oxford at that time a member of this rare species (the interviewers were not to realize that a linguistic background was largely superfluous, since the requirements of security did not allow them to know the nature of the work the successful candidate would be doing); the best approximation to be found there was myself, certainly not a mathematician but only an undergraduate student in his second year, and one whose knowledge of German was confined to a year of self-instruction at St. Paul's School in 1939/40, leading to a pass in the School Certificate A level (subsidiary) examination. The recruiters had to be content with this very modest outcome of their search, and I was offered the position, provided I was willing to start on January 10, 1942. For me, the alternative was to stay at Oxford till the summer of 1942 and then enter the Royal Artillery. Experience in training for the RA in the Officer Cadet Training Unit at Oxford had convinced me that, if I joined the RA, I would be in grave danger of early death — from boredom — so I did not hesitate to accept. Thus I embarked on this mysterious enterprise, and received a letter of appointment, at the princely salary of £200 per annum, signed "Your obedient servant, Mr. Secretary Eden." On January 10, 1942, I presented myself at the gates of Bletchley Park, to be greeted by a somewhat strange individual whose first question was "Do you play chess?." The questioner was none other than Alan Turing. Fortunately, I was able to answer "Yes," and much of my first day of war service was spent in helping Turing to solve a chess problem which was intriguing him. I like to think that this minor success contributed to the pleasant, and, for me, invaluable relationship which I enjoyed with Alan Turing from that day till the time of his death in 1954. I will be paying my tribute to his memory in the course of these reminiscences.

I would have wished that I could write in some detail of the nature of our work in those wonderfully exciting days. For we were regularly reading the highest grade ciphered messages passing between the German High Command and the senior echelons of the German army, the German navy (including the U-boat fleet) and the Luftwaffe; moreover, we were reading those messages within a few hours of their original transmission. We were thus able to provide as perfect and complete a picture of the enemy's plans and dispositions as any nation at war has ever had at its disposal — not lightly did Churchill describe our work as his "secret weapon," far more potent than anything that Werner von Braun could deploy against us. Unfortunately, the British government currently is behaving in a remarkably paranoid fashion with respect to the revelation of "secrets" by those who have at some time (as, of course, I had to do) taken an oath of confidentiality. Their dogged pursuit through the courts of those thoroughly respectable British newspapers who have sought to publish excerpts from Peter Wright's book *Spycatcher*, even though the book has been published in the US and though it is perfectly legal for individuals to bring copies into the UK, indicates that it is not even safe for me to reproduce information freely available in this country. I must therefore, very regretfully, confine myself, in my technical description of our work, to material which has already been published in the UK. I must add that I find it inconceivable that any information I could reveal about our methods over forty years ago could be of the smallest value to a potential enemy today or in the future — but that would be no defence if I were arrested for breach of the Official Secrets Act on stepping onto British soil.

2. "Breaking The Code"

The German Fish machine consisted of 12 wheels producing a *key* which, when "added" to the German text (called the *clear*), produced the encoded text (called the *cipher*). The "alphabet" is the teleprinter alphabet, consisting of $32(=2^5)$ characters, that is, the 26 letters of the usual alphabet and six other symbols. "Addition" is mod 2 addition at each of the five places on the tape; that is, the characters are the elements of a 5-dimensional vector space over $\mathbf{Z}/2$. Of course, in this system, addition and subtraction are the same, so that, while the transmitter adds key to clear to obtain cipher, the receiver adds key to cipher to obtain clear.

The task of our team of cryptanalysts was two-fold. First, we had to determine the pattern (of 1's and 0's) on each wheel for each of the groupings using the Fish system. These patterns changed regularly and, in the latter and most crucial part of the European war, were changing daily. Second, we had to determine the starting place on each wheel for each individual message. Of course, the actual interception of the messages and their accurate reproduction were also tasks demanding great skill and we were fortunate to be able to count on the excellent cooperation of those responsible for this crucial aspect of the overall enterprise.

In general, we had to rely on small statistical biases in the German language to eliminate most of the myriad possibilities; and then we used "hand methods" to make the final determinations. It was Alan Turing who first appreciated the essential role which could be played in the elimination phase of the process by high-speed electronic machines, and who was, in fact, — and quite consciously and deliberately — inventing the computer as he designed first the "Bombe" and then the "Colossus" for our cryptanalytical purposes. This is very well described in **[Good]** and **[Randell]**.

Before saying more about the role of Turing and others in this astonishingly successful operation, I should refer to two factors which were very much in our favor in dealing with our particular antagonist. First, we benefited greatly from a combination of Nazi bombast and German methodicalness. Nazi conceit dictated that great military successes should be announced to every German military unit everywhere[1]; and the passion of the German military mind for good order and discipline dictated that these announcements should be made in exactly the same words and sent out at exactly the same time over all channels. The effect is obvious: the clear could be obtained by reading some low-grade cipher and then, by adding the clear to the cipher, we would obtain a number of stretches of key to analyse into the constituent patterns on the wheels. Second, we also benefited greatly from German procedural errors. Thus, for example, it might well happen by inadvertence that two messages were both encoded using the same key — and we had means of making informed guesses as to when this occurred. Notice that we then have

$$C_i = K + \Gamma_i, i = 1, 2,$$

where C_i is the cipher and Γ_i the clear of the ith message. It follows that

$$C_1 + C_2 = \Gamma_1 + \Gamma_2;$$

this means that, by adding the ciphers, we obtain the sum of the clears. The reader will readily believe that it was a fascinating, if somewhat intricate, process to break up the sequence of characters C_1+C_2 into two clear messages. Once this was — even partially — accomplished, we would have a substantial length of key to analyse. (Here I oversimplify — it would be impossible to say which clear was Γ_1 and which Γ_2, so that there would be two candidates for K. So two analysts would get to work; one would be frustrated and the other triumphant.)

The picture I have drawn of our work at Bletchley Park, though woefully incomplete, is accurate so far as it goes, and gives, I believe, the flavor of our lives during those heady days when we were helping to win the war in a very exciting and uniquely stimulating way. A play by Hugh Whitemore, entitled "Breaking The Code," which purports to be a biographical sketch of Turing's life, including his work at Bletchley Park, and which featured Derek Jacobi in the principal role, gained a considerable vogue during its London and Broadway runs, and has thus given many people the impression that they now know something of Turing's life at that time, of his thoughts on many topics, and of the work we were doing at Bletchley Park. Unfortunately, the play, however dramatically coherent, is a work of fiction and is seriously misleading with regard to Turing's life and thought and with respect to our cryptanalytical work. Let me, therefore, say something about my own personal contact with Turing, and about Turing's unique contribution, in order to set the record straight.

[1]And Nazi dishonesty increased the frequency of such 'successes'!

3. Impressions of Alan Turing

It is a rare experience to meet an authentic genius. Those of us privileged to inhabit the world of scholarship are familiar with the intellectual stimulation furnished by talented colleagues. We can admire the ideas they share with us and are usually able to understand their source; we may even often believe that we ourselves could have created such concepts and originated such thoughts. However, the experience of sharing the intellectual life of a genius is entirely different; one realizes that one is in the presence of an intelligence, a sensitivity of such profundity and originality that one is filled with wonder and excitement.

Alan Turing was such a genius, and those, like myself, who had the astonishing and unexpected opportunity, created by the strange exigencies of the Second World War, to be able to count Turing as colleague and friend will never forget that experience, nor can we ever lose its immense benefit to us.

Turing was a mathematician, a logician, a scientist, a philosopher — in short, a thinker. It is not possible to convey the full, rich flavor of his thought in all these varied domains, but the skilled expositor can, with care, explain the nature of the ideas without stooping to vulgarization. Such a comprehensive exposition is now available to us in the fine biography by Andrew Hodges. Nevertheless, the phase of Turing's creative life that will most appeal to the reader's curiosity must be that in which he was making a unique and absolutely fundamental contribution to the winning of World War II by developing and establishing the basic methods of deciphering enemy codes.

Much has been written in recent years of the astonishing success of "Britain's secret weapon," but Hodges' is the first book to do justice to Turing's part in that great story. Others of us shared the excitement of successful achievement; some, like the mathematician Max Newman, deserved great credit for providing the organizational framework — not to be confused with its antithesis of bureaucratic structure — essential to the full exploitation of that success; but Turing stood alone in his total comprehension of the nature of the problem and in devising its solution — essentially by inventing the computer. (Of course, the process of invention was also occurring independently elsewhere; one must cite the pioneering work of John von Neumann in the USA.)

After the war, Turing continued his work on the development of a computer, first at the National Physical Laboratory (NPL) and then at Manchester University. Max Newman had gone from Bletchley Park to be head of the department of mathematics at Manchester University, and he invited Turing to take a readership in the department and to work with him on the design of a computer to be built by Ferranti. (I was also fortunate to be invited by Newman to take a junior position in the department in 1948.) Turing, who had been frustrated by bureaucratic obstructions at the NPL, was happy to accept, and the collaboration with Newman was crowned with success.

Unfortunately, the story of Turing's life is more the stuff of tragedy than of triumph. Turing was a homosexual. He was, characteristically, wholly honest about this and not ashamed, though he was never ostentatious about his preference. But, after the war, the law against the expression of male homosexuality was upheld with rigorous fervor in Britain, and in January 1952, Turing, then a reader at Manchester University and a Fellow of the Royal Society, was arrested and charged with committing "an act of gross indecency" with his friend, Arnold Murray. Of course, he didn't deny the charge, but he did not agree that he had done anything wrong. He was bound over on condition that he submit to hormonal treatment designed to diminish his libido; the only obvious effect was that he developed breasts. He was placed on probation till April 1953; as a byproduct of his plea of guilty, he was no longer permitted to work as a consultant to Government Communications Headquarters (GCHQ), Cheltenham, where the codebreakers worked, nor to visit the United States. It is a tragic irony that British security services should have been mobilized to exclude Turing, whose contribution to the work of GCHQ was of such inestimable value during the war, but should have failed so conspicuously to detect the activities of the mole Geoffrey Prime. I. J. Good, a wartime colleague and friend, has so aptly remarked that it is fortunate that the authorities did not know during the war that Turing was a homosexual; otherwise, the Allies might have lost the war (see [**Good**]).

On 7 June 1954, just short of his forty-second birthday, Turing committed suicide by swallowing cyanide. He left no note, and it is generally supposed that, in the words of his friend and executor, Nick Furlong, "he planned for the possibility, but in the end acted impulsively." [**Hodges**] has told the story of Turing's life and death with honesty and candor and a fine sense of balance. We are in his debt for bringing us closer to a marvelous person and for chastening our intolerant society.

However, I must make one point clear in the interests of historical accuracy and in view of the false impression created by the play "Breaking The Code." As Jack Good has pointed out, we did not know during the war that Turing was a homosexual. This was not because Turing took elaborate steps to conceal his predilections; it was because such a matter wasn't an issue with us — the thought never entered our heads. It is an anachronism to write as if today's obsession with people's sexual preferences and behavior was already afflicting us forty five years ago.

4. Meeting the Great

Among the unexpected advantages for me, as a young man, of working at Bletchley Park during the war was the opportunity it provided me to become friendly with some of the great mathematicians of the time and with some of those destined to be counted among the great. I have referred to my friendship with Alan Turing; important as this was to me, it was nothing like as significant as my very close relationship with J. H. C. (Henry) Whitehead, the outstanding British algebraic topologist. Since Henry was considerably older than I, he was not required to give up his academic work at Oxford and undertake war service until considerably after my own arrival at Bletchley Park at the beginning of 1942. Thus it came about, quite astonishingly, that I actually taught Henry several of the techniques of our work — and we were colleagues where our peacetime levels would have dictated an almost unbridgeable gap. We were colleagues who shared many common interests outside mathematics and the winning of the war — principally politics, cricket, and the drinking of beer; and thus we became firm friends. After the war, Henry was appointed to a chair at Oxford University and invited me to return to Oxford as his research student, although I had not completed the Oxford undergraduate program.[2] I thus became his first post-war D.Phil. student. Moreover, I even had the wonderful privilege of living in his home in Charlbury Road, N. Oxford, as a member of the family, getting to know his lovely, talented wife Barbara and their two sons. I became an algebraic topologist solely out of a desire to work with Henry — my decision to work in this area substantially antedated my discovery of what algebraic topology was. Henry's untimely death in 1960 was a deep personal and professional loss to me, and to the many mathematicians who owe so much to his inspiration.

Another contact of great significance which I made at Bletchley Park was with the British topologist and logician M. H. A. (Max) Newman, of whom I have written elsewhere **[Hilton]**. Max was the head of the "Newmanry," the section responsible for the use of the Colossus machines in the process of decoding Fish signals. No one could have done this vital work better. After the war, Newman was appointed Fielden Professor of Mathematics at the University of Manchester. He attracted to his department not only Alan Turing as Reader but also a galaxy of outstanding talent, which included Bernhard Neumann, Graham Higman, J. W. S. (Ian) Cassels, David Rees, I. J. (Jack) Good, Paul Cohn, Walter Ledermann, Arthur Stone and many others. I, too, as I have already indicated, was offered a junior appointment

[2]My studies in 1940/41 entitled me to a wartime B.A. degree, even though I only completed four terms out of the statutory nine.

in his department and was there from 1948 to 1952, returning in 1956, after a spell as Lecturer at Cambridge University, to the position of Senior Lecturer. Max was a person of profound culture and formidable intelligence; he was a beautiful pianist; and it is not surprising to those who appreciated the subtlety of his mathematical work that some of his ideas in combinatorial logic are today of fundamental importance in theoretical computer science.

Many other great mathematicians worked during the war at Bletchley Park and so became well-known to me; it is no coincidence that the list overlaps substantially with that of the mathematicians whom Max Newman attracted to Manchester University after the war. Thus David Rees, Jack Good, and J. A. (Sandy) Green were colleagues in the Newmanry; while Ian Cassels, W. T. (Bill) Tutte and Philip Hall also figure among Bletchley's distinguished alumni. I would also like to pay my own personal tribute to the value of my friendship at that time, persisting down to the present day, with the Cambridge topologist Shaun Wylie, who helped me greatly in my career and exercised a very beneficial influence on my mathematical taste and my powers as an expositor of mathematics. (We wrote together a textbook on algebraic topology, called *Homology Theory*, which was the first of its kind and enjoyed some popularity for many years, in spite of certain terminological and notational idiosyncrasies.)

We also liaised with several American cryptanalysts and enjoyed a happy and relaxed cooperation with them. Among them I particularly remember Howard Campaigne, A. H. (Al) Clifford, Arthur Levinson, and Walter Jacobs. Campaigne, Levinson, and Jacobs remained in the business after the war; Walter Jacobs, however, played his part as a mathematician, being an active member of the AMS; and Howard Campaigne, on retiring from US Government service, took up an academic career as chairman of the mathematics department at Slippery Rock State College. Our paths crossed again at meetings of the AMS and I was delighted when he invited me to Slippery Rock to give a colloquium talk.

5. Conclusions

This article is more than anything a personal reminiscence, and an expression of gratitude to fate[3] for creating circumstances which afforded me the privilege of meeting, on terms of apparent equality, many great senior mathematicians at a time when I was the merest tyro. However, I believe there is one important lesson of universal significance for the study of mathematics to be learned from our war-time experience at Bletchley Park and the astounding success of our enterprise.

[3] I continue, however, to feel guilty that my amazing good fortune coincided with the appalling misery of countless others.

For it cannot be doubted that our success was astounding. German Intelligence (Abwehr) continued to believe right up to the end of the war that their ciphers were absolutely secure. And, despite the genius of Turing and his unique contribution, it must be understood that we could not have been successful without the effective cooperation of each member of the team of mathematicians brought to Bletchley Park for the purpose of analysing German signals enciphered on their highest grade codes. Why were we so successful?

The relevant facts are these. Gathered together at Bletchley Park was a group of mathematicians, each of whom would be described as quintessentially "pure." Each of them occupied a position in the academic world or aspired to such a position after the war. None of them had any experience in industry or in applying mathematics to problems in the real world, although all had, as undergraduates, taken courses in the classical areas of applied mathematics — statics, dynamics, and continuous mechanics. Each of them (modesty compels me to admit the possibility of an exception) was a good mathematician, but none was a specialist in statistics or probability theory.[4] All were strongly motivated by a determination to do everything possible to win the war as quickly as possible. Remember that World War II was perceived as the last "good" war, in which right was unquestionably on one side and wrong on the other, without qualification. This fact would not have been held by my colleagues to justify the use of any means (for example, nuclear weapons) to win the war, but fortunately, our success would contribute significantly to victory without increasing human suffering. Finally, we were amazingly successful; despite Turing's enormous contribution, this effort was no "one man show," and it is impossible to imagine how we could have been more successful.

Given these facts, then, what are the hypotheses that might explain them? So far as I am concerned, they are these. To get people effectively to apply mathematics, the essential ingredients are (1) a strong education in mathematics; (2) the ability to think mathematically, to understand how to formulate a problem in precise mathematical terms (what Speiser called "Mathematische Denkweise," or "mathematical way of thinking"), and (3) a strong motivation to solve a given problem or problems. That these ingredients are necessary would, I believe, be denied by only few. That they are sufficient is less obvious and would be denied by many. For it is claimed that to create an appetite and an ability for applied mathematics, it is also necessary to train an individual in the actual practice of applying mathematics and to teach that individual some science to such a depth of understanding that he or she really understands what is involved in making progress in a scientific or engineering discipline by the use of mathematical methods. Moreover, those who put forward this point of view usually rate these two requirements so highly

[4] Jack Good subsequently became one.

that they advocate curricula in which exigencies of time, if not inclination, and often both, compel them to reduce the mathematical content and to pay very limited attention to the need to develop understanding rather than mere skill. Thus, in effect, by apportioning priorities to take account of limited resources of time, these advocates actually recommend programs that pay insufficient respect to the first two ingredients listed earlier.

The facts might appear at first sight to support the idea that courses in "applied mathematics" are necessary to subsequent success in applying mathematics. Certainly I would not deny that such courses, properly designed, are highly desirable, but the evidence from our wartime experience does not suggest that they are necessary. In my judgment, the traditional courses to which we had been exposed had not been properly designed — they tended to be cookbook courses in which certain mechanical principles (e.g., laws of conservation or conditions of equilibrium) were mechanically applied to create standard mathematical problems of no particular interest. I am convinced that not one of us at Bletchley Park would have attributed our success to such courses. Moreover, I would argue, and have indeed argued elsewhere **[Hilton and Young]**, that so-called pure mathematics offers many opportunities to develop a familiarity with the procedures of mathematical modeling, including numerical analysis and experimentation with special cases, which have often been regarded as the exclusive preserve of the applied mathematician.

If we now assume the truth of our hypotheses, what conclusions can we draw about the mathematical curriculum at the undergraduate and precollege levels? In the main, these conclusions are obvious. Our mathematics courses must be rich in content; we must teach them so that understanding will result — this approach does not deny the importance of skill but views it more as a by-product than as the purpose of the major educational thrust; and we must inculcate an appetite for solving real-world problems. The second and third objectives certainly need elaboration if we wish to translate them into actual curricular recommendations.

This is not the place for such elaboration. Nevertheless, it does seem pertinent to conclude with three lessons which I derived from those Bletchley days. First, mathematics is a single discipline, an integrated whole. Its subdivision into artificial watertight compartments is, at best, an administrative convenience, at worst an inhibiting straitjacket. Second, the distinction between pure and applied mathematics has been grossly exaggerated and should be allowed, indeed encouraged, to lapse. And, third, no mathematical activity can be successful unless it is undertaken with a combination of real enthusiasm and extensive knowledge and skill. I tend to think that our work at Bletchley Park marked the zenith of the golden age of cryptanalysis and that this age will never return. But, while the effects of that work were of great significance for the future of mankind, they were by no means confined — at least, potentially — to the winning of the war.

References

[Good] I. J. Good, Early Work on Computers at Bletchley, NPL Report **82** (1976), No. 1 (reproduced in *Annals of the History of Computing*).

[Hilton] Peter Hilton, M. H. A. Newman obituary, *Bull. London Math. Soc.*, **18** (1986), 67–72.

[Hilton-Young] Peter Hilton and Gail Young, Jr., eds. *New Directions in Applied Mathematics*, Springer, New York, 1982.

[Hinsley] F. H. Hinsley (with E. E. Thomas, C. F. G. Ransom and R. C. Knight), *British Intelligence in the Second World War*, Vol. II, HMSO, 1981.

[Hodges] Andrew Hodges, *Alan Turing: The Enigma*, Simon and Schuster, New York, 1983.

[Randell] B. Randell, The Colossus, Univ. of Newcastle Computing Laboratory Report **90** (1976) (reproduced in *Proceedings of International Conference on the History of Computing*, Los Alamos Scientific Laboratory).