Colossus: Its Origins and Originators

B. Jack Copeland
University of Canterbury

The British Colossus computer was one of the most important tools in the wartime effort to break German codes. Based on interviews and on recently declassified documents, this article clarifies the roles played by Thomas Flowers, Alan Turing, William Tutte, and Max Newman in the events leading to the installation of the first Colossus at Bletchley Park, Britain's wartime code-breaking establishment, in December 1943.

Colossus, the large-scale special-purpose electronic computer used for code breaking in the 1939–1945 war with Germany, completed its first trial runs in December 1943 (two years before the first comparable US computer, the ENIAC, was operational).[1] From February 1944, cryptanalysts used Colossus to read the priceless German traffic code-named "Tunny" by the British. The exact timing of the D-Day landings in June 1944 was based on intelligence produced by Colossus.

Traditional histories point to Alan Turing as the key figure in the design of Colossus. Yet the recently declassified official history of the attack on Tunny states: "Colossus was entirely the idea of Mr. Flowers."[2]

Biographical background

Thomas H. Flowers (1905–1998) joined the Telephone Branch of the Post Office in 1926, after an apprenticeship at the Royal Arsenal in Woolwich (well-known for its precision engineering). Flowers entered the Research Branch of the Post Office at Dollis Hill in North London in 1930, achieving rapid promotion and establishing his reputation as a brilliant and innovative engineer. At Dollis Hill, Flowers pioneered the use of electronics on a large scale. In 1934, he employed 3,000 to 4,000 valves (vacuum tubes) in an experimental installation for controlling connections between telephone exchanges by means of voice-frequency tones (1,000 telephone lines were controlled, each line having three to four valves attached to its end). Flowers' design was accepted by the Post Office, and the equipment went into limited operation in 1939. During 1938–1939, Flowers worked on an experimental, electronic high-speed digital data store for use in telephone exchanges. Flowers was first summoned to Bletchley Park to assist Turing in the attack on Enigma but he soon became involved in work on Tunny. After the war, Flowers pursued his dream of an all-electronic telephone exchange and was closely involved with the groundbreaking Highgate Wood exchange in London, which was the first all-electronic exchange in Europe.

Max H.A. Newman (1897–1984) was a leading topologist as well as a pioneer of electronic digital computing. A Fellow of St. John's College, Cambridge, from 1923, Newman lectured Turing on mathematical logic in 1935, launching Turing on the research that led to the universal Turing machine.[3]

Newman assisted Turing with the final drafting of the latter's 1936 paper "On Computable Numbers, with an Application to the Entscheidungsproblem."[4] At the end of August 1942, Newman left Cambridge for Bletchley Park, joining the Research Section and entering the fight against Tunny. In 1943, Newman became head of a new section known simply as the Newmanry, home first to the experimental Heath Robinson machine and subsequently to Colossus. By April 1945, there were 10 Colossi working round the clock in the Newmanry. In September 1945, Newman took up the Fielden Chair of Mathematics at the University of Manchester and, inspired both by Colossus and by the abstract universal stored-program computer described in Turing's "On Computable Numbers," lost no time in establishing a facility to build an electronic stored-program computer. Newman was soon joined by the engineers Freddie Williams and Tom Kilburn, and on 21 June 1948, in Newman's Computing Machine Laboratory, the world's first electronic stored-program digital computer, the Manchester "Baby," ran its first program.

Alan M. Turing (1912–1954) was in 1935 elected a Fellow of King's College, Cambridge, at the age of only 22.[5] "On Computable Numbers," published the following year, was

 Published by the IEEE Computer Society 1058-6180/04/$20.00

his most important theoretical work. It is often said that all modern computers are Turing machines in hardware. In a single article, Turing ushered in both the modern computer and the mathematical study of the uncomputable. During the early stages of World War II, Turing broke German Naval Enigma and produced the logical design of the Bombe, an electromechanical code-breaking machine. Hundreds of Bombes formed the basis of Bletchley Park's factory-style attack on Enigma. In 1945, inspired by his knowledge of Colossus, Turing designed an electronic stored-program digital computer, the Automatic Computing Engine (ACE). Turing's design became the basis for the very successful Digital Electronic Universal Computing Engine (DEUCE) computers, which were a cornerstone of the fledgling British computer industry and remained in use until about 1970.[6] At Bletchley Park, and subsequently, Turing pioneered artificial intelligence. He also pioneered the discipline now known as artificial life, using the Ferranti Mark I computer at Manchester University.

William T. Tutte (1917–2002) specialized in chemistry in his undergraduate work at Trinity College, Cambridge, but was soon attracted to mathematics. He was recruited to Bletchley Park early in 1941, joining the Research Section. Tutte worked first on the Hagelin cipher machine and in October 1941 was introduced to Tunny. Tutte's work on Tunny, which included deducing the Tunny machine's structure, can be likened in importance to Turing's earlier work on Enigma. At the end of the war, Tutte was elected to a Fellowship in mathematics at Trinity; he went on to found the area of mathematics now called graph theory.

The Tunny machine

Tunny, quite distinct from Enigma, was a system of teleprinter (the North American term is *teletypewriter*) encryption. (Colossus is sometimes incorrectly stated to have been used against Enigma.) Technologically more sophisticated than Enigma, Tunny carried the highest grade of intelligence. From 1941 onward, Hitler and the German High Command relied on Tunny to protect their communications with Army Group commanders across Europe.[7] Tunny messages sent by radio were first intercepted by the British in June 1941. After a yearlong struggle with the new cipher, Bletchley Park had its first successes against Tunny in 1942. Tunny decrypts contained intelligence that changed the course of the war in Europe, saving an incalculable number of lives.

To clarify the contributions made by Flowers, Newman, Turing, and Tutte to the attack on Tunny, it is necessary to outline the workings of the Tunny cipher machine.[8] The Tunny machine (which measured 19″ × 15-1/2″ × 17″ high) was a cipher *attachment*, automatically encrypting the outgoing stream of pulses generated by the teleprinter to which it was attached, or automatically decrypting incoming messages before they were printed. At the sending end, the operator typed plaintext at the teleprinter keyboard, and at the receiving end the plaintext was printed out automatically by another teleprinter (usually onto paper strip, resembling a telegram). The transmitted ciphertext was never seen by the German operators. In batch mode, many long messages could be sent one after another: The plaintext was fed into the teleprinter equipment on prepunched paper tape and was encrypted and broadcast at high speed.

Enigma was clumsy by comparison. The cipher clerk typed the plaintext at the keyboard of an Enigma machine while an assistant painstakingly noted down the letters of the ciphertext as they appeared one by one at the machine's lamp-board. Once the ciphertext was complete, it was passed to a radio operator for transmission in Morse code. In Tunny, Morse was not used: The Tunny machine's output—encrypted teleprinter code—went directly to air.

International teleprinter code assigns a pattern of five pulses and pauses to each character; using the Bletchley convention of representing a pulse by a cross and no pulse by a dot, the letter L, for example, is •x••x, M is ••xxx, N is ••xx• (in modern notation: 01001, 00111, and 00110, respectively). The plaintext entered Tunny in the form of teleprinter code and was encrypted by means of the bitwise addition of a further stream of dots and crosses, generated automatically by the Tunny and known as *key*. Dot-and-cross addition is Boolean XOR: Dot plus dot is dot, cross plus cross is dot, dot plus cross is cross, cross plus dot is cross. For example, if the plaintext message is simply JA, and the key for this message is MT, then the ciphertext is QW. J + M = Q and A + T = W:

J		A				
xx•x•		xx•••			Q	W
+		+		=	xxx•x	xx••x
••xxx		••••x				
M		T				

The obscuring key was generated by the internal wheels of the Tunny machine. Each time a letter entered the encryption mechanism, some (or all) of the wheels would move forward one step. The wheels had adjustable

metal cams around the circumference. Each time a wheel moved forward a step, a different cam reached a stationary switch, producing either a cross (that is, a pulse) or a dot. A cam in the so-called operative condition produced a cross, and in the inoperative condition, where the operator had moved the cam to one side, a dot.

Each wheel (there were 12) had a different number of cams, varying from 23 to 61. The arrangement of the cams, operative or inoperative, was identical in the sending and receiving Tunny. The Germans left the arrangement unchanged over many messages.

Two groups of five wheels produced the key. Each wheel in a group contributed one bit, dot or cross; the group as a whole contributed a single character. The character contributed by one group was added to the character contributed by the other to produce one character of key. For example, if one group contributes **xxx••** (U) and the second **xxx•x** (Q), the character of key is **••••x** (T): U + Q = T. The two groups of wheels were known at Bletchley as the χ-wheels and the ψ-wheels, respectively. (The remaining two wheels, the motor or μ-wheels, served to create irregularities in the movement of the ψ-wheels. The χ-wheels, on the other hand, moved regularly, rotating every time a letter entered the Tunny.)

Decryption relied on the fact that adding any characters x and y and then adding x again a second time retrieves y: $(x + y) + x = y$. The receiving Tunny generated the same characters of key as the sending Tunny and added them to the ciphertext in order to reveal the plaintext.

As with Enigma, the sending and receiving operators would rotate the wheels of their machines to the same numbered positions before the encryption (and decryption) of a message began, thus causing the same key to be produced. From October 1942, the 12 numbers specifying the positions were obtained from a book that was issued to the operators at each end of the Tunny link. Each book listed 100 or more different sequences of 12 numbers; after each sequence had been used once, the book was discarded, and the operators moved on to the next.

The structure of the Tunny machine was deduced in January 1942 by Tutte, with some assistance from other members of Bletchley Park's Research Section, on the basis of a pair of intercepted messages—a remarkable feat, to say the least. It was not until the very end of the war that the code breakers saw a captured Tunny machine.

Misconceptions about the history of Colossus

Martin Davis offers the following account of the British attack on Tunny:

> Some of the methods … used were playfully called *turingismus* indicating their source. But turingismus required the processing of lots of data and for the decryption be [sic] of any use, the processing had to be done very quickly… In March 1943, Alan Turing sailed home from a visit of several months in the United States … He whiled away the time during his Atlantic passage by studying [an] RCA catalog, for it had been found that vacuum tubes could carry out the kind of logical switching previously done by electric relays. And the tubes were fast … Vacuum tube circuits had in fact been used experimentally for telephone switching, and Turing had made contact with the gifted engineer, T. Flowers, who had spearheaded this research. Under the direction of Flowers and Newman, a machine, essentially a physical embodiment of turingismus, was rapidly brought into being. Dubbed the Colossus and an engineering marvel, this machine contained 1500 vacuum tubes.[9]

This account of matters is garbled. Other prominent accounts are also in error; for example, J.A.N. Lee, in a biographical article on Turing, says that "his [Turing's] influence on the development of Colossus is well known," and in an article on Flowers, Lee refers to Colossus as "the cryptanalytical machine designed by Alan Turing and others."[10] Lee states:

> Newman fully appreciated the significance of Turing's ideas for the design of high-speed electronic machines for searching for wheel patterns and placings on the highest-grade German enciphering machines, and the result was the invention of the 'Colossus'.[11]

Even a book sold at the Bletchley Park Museum states that at Bletchley Park "Turing worked … on what we now know was computer research" which led to "the world's first electronic, programmable computer, 'Colossus'."[12]

Turingery and Tuttery

In July 1942, Turing—on loan, for a period of a few weeks, from the Naval Enigma section to the group researching Tunny—devised a method of attack officially named *Turingery*.[13,14] An unofficial slang term for this method, *Turingismus*, was coined subsequently. (Leading Tunny-breaker Donald Michie recalled:

> [T]hree of us (Peter Ericsson, Peter Hilton and I) coined and used in playful style various fake-German slang terms for everything under the sun, including occasionally something encountered in the working environment. Turingismus was a case of the latter. (Personal communication, July 2001.))

I will use the official term *Turingery* in preference to the slang term for the method. Turingery was a hand method, involving paper, pencil, and eraser. Its function was *wheel breaking*, starting from a stretch of key.[15,16] Wheel breaking is the finding of the arrangement of the cams—operative or inoperative—around the wheels. Once gained by Turingery, this information remained current over the course of many messages. (At first the Germans changed the cam patterns of the χ-wheels once a month and of the ψ-wheels quarterly; from October 1942, the ψ-wheel patterns were also changed monthly. From August 1944, all wheel patterns were changed daily; although by that time new methods of wheel breaking were used in preference to Turingery.)

Turingery was used in conjunction with *depths*—two or more messages enciphered at the same starting positions of the wheels, an egregious breach of secure cipher practice. It was from depths that the stretch of key necessary for the application of Turingery was obtained (also by hand). Turingery extracted from the key the contribution of the χ-wheels. From this, the cam patterns of the individual χ-wheels could be deduced; further deductions led to the cam patterns of the ψ- and motor wheels.

Given successful wheel breaking from depths, the next hurdle was to find the starting positions of the wheels for each individual Tunny message (not just the few messages that were in depth). This process was known as *wheel setting*. After setting, the messages could be read. Tutte invented a procedure for wheel setting in November 1942[13] that became known as the Statistical Method.

Both Turingery and the Statistical Method used a process of sideways bitwise addition known as *differencing*. Differencing **•x••x**…, for example, produces **xx•x**… (dot plus cross, cross plus dot, dot plus dot, and so on). Differencing tracks changes in the original stream of dot and cross. If a dot follows a dot or a cross follows a cross, then the corresponding point in the differenced stream has a dot; if cross follows dot or dot follows cross, then the differenced stream has a cross. A dot in the differenced stream means no change, and a cross means change. Turing introduced differencing in July 1942: He made the fundamental observation that differenced key "could yield information unobtainable from ordinary key."[17] Turingery worked on the differenced key to produce the differenced contribution of the χ-wheels. Tutte discovered, a few months later, that differencing was the clue to wheel setting.

Tutte's Statistical Method is as follows.[14] Let attention be focused on the first two χ-wheels, χ_1 and χ_2. As each rotates through all its possible positions, it produces a stream of dot and cross which—assuming that the wheels have been broken—is known to the cryptanalyst. If the two streams are added and their sum differenced, the result is a periodic sequence; the period is $41 \times 31 = 1{,}271$, since there are 41 cams around χ_1 and 31 around χ_2. One of these 1,271 places in the sequence represents the position of the two wheels at the start of enciphering the message. The problem is to find it. The first step is to prepare the intercepted ciphertext in a certain way. At Bletchley, each of the five streams of dot and cross making up the ciphertext was called an *impulse*. For example, if the ciphertext is QW, as in the previous example, the first and second impulses are both **xx**, the third **x•**, and so on:

Q	W
x	x
x	x
x	•
•	•
x	x

The first and second impulses of the ciphertext (written c_1 and c_2) are added and the result differenced. (A message of about 1,000 characters or more is required.) The differenced $c_1 + c_2$ is then laid against the differenced $\chi_1 + \chi_2$ in each of the possible 1,271 positions, and at each position the number of times that the two streams agree—that is, have a dot or a cross in the same place—is counted. The position with the highest score is, Tutte showed, likely to be the start position of the two wheels.

Further applications of Tutte's method reveal the start positions of other χ-wheels. The start positions of the ψ- and μ-wheels can then be found by less computationally intensive methods.

The small statistical bulge at the correct start position, on which Tutte's method depends, is the result of the pattern of movement of the ψ-wheels—the great weakness of the Tunny machine. Each time a letter entered the encryption mechanism, the ψ-wheels would either all

step forward (like the chis) or all remain still, depending on the position of the motor wheels. (The motion of the psis was described as *staggering* at Bletchley Park.) While the psis remained stationary, they continued to contribute the same letter to the key. So, since differencing tracks change, the differenced ψ-stream contained more dots than crosses. The effect was boosted by the fact that the differenced plaintext also contained more dots than crosses, thanks both to the statistical properties of the German language and the practices of Tunny operators, who habitually repeated certain characters. The result was that at the correct start position, the differenced $\chi_1 + \chi_2$ would agree with the differenced $c_1 + c_2$ more often than not.[18] When the two were correctly aligned, counting the number of times that they had a dot or cross in the same place usually produced a result that was higher than chance—not much higher, but any regularity is the cryptanalyst's friend. If, instead of the ψ-wheels either all moving together or all standing still, the designer had arranged for them to move independently (or even to move regularly like the chis), then the chink that let Tutte in would not have existed.

Turing's method of wheel breaking from depths and Tutte's method of wheel setting were distant relatives, in that both used differencing. But there the similarity ended. (Turingery, Tutte said, seemed to him "more artistic than mathematical"; in applying the method you had to rely on what "you felt in your bones."[14]) In the quotation given above, Davis conflates Turingery and Tutte's Statistical Method. It was the latter that "required the processing of lots of data"—so much, indeed, that carrying out the method by hand was completely impractical. It was Tutte's method, not Turingery, that was implemented in Colossus and in its precursor, the Heath Robinson.[19]

I hope that Michie's words will eliminate the myth that Turingery was implemented in Colossus before it becomes set in stone: "Turingery was not used in either breaking or setting by any valve [vacuum tube] machine of any kind" (personal communication, November 2001).

Tutte has never received full credit for his great achievement, which was the sine qua non of the ensuing highly successful machine-based decryption of Tunny traffic. His method is sometimes attributed to Turing and sometimes to Newman. This is Tutte's own description of his discovery:

> Here was a method of wheel-setting! … The procedure was not to be recommended as a hand method but no doubt our electrical engineers could find a way of mechanizing it. … I went into Gerry Morgan's office [in the Research Section, of which both Tutte and Newman were members] to tell of these results. Max Newman was there. They began to tell me, enthusiastically, about the current state of their own investigations. When I had an opportunity to speak I said, rather brashly, 'Now my method is much simpler'. They demanded a description. I must say they were rapidly converted. The Research Section urged the adoption of the 'Statistical Method' of wheel-setting.[14]

Flowers, Turing, and Newman

Davis's claim, quoted above, that Colossus was "essentially a physical embodiment of turingismus" is one of the ways in which he conveys the impression that Turing played a leading role in Colossus. Another is his reference to Turing's interest in the RCA catalogue in March 1943 and the juxtaposition of this with remarks introducing Flowers. The view that Turing's interest in electronics contributed to the inspiration for Colossus is indeed common. The claim is enshrined in more than one leading museum; and in *IEEE Annals of the History of Computing*, Lee and Holtzman have stated that Turing "conceived of the construction and usage of high-speed electronic devices; these ideas were implemented as the 'Colossus' machines."[20]

By 1943, electronics had been Flowers' driving passion for more than a decade, and he needed no help from Turing. As I mentioned, a definitive contemporary account recorded that "Colossus was entirely the idea of Mr. Flowers."[2] Flowers emphasized in an interview with me that Turing "made no contribution" to the design of Colossus, saying: "I invented the Colossus. No one else was capable of doing it."[21]

Work on Colossus began early in 1943. (Turing was absent in the US; he left Bletchley Park for the US in November 1942.[22]) It took Flowers and his team at the Post Office Research Station 10 months to complete the machine, working day and night, pushing themselves until (as Flowers said) their "eyes dropped out." Colossus I successfully completed its first trial runs on 8 December 1943.

At the Post Office Research Station before the war, Flowers had explored the feasibility of using valves (vacuum tubes) as digital switches on a large scale in telephone equipment. His work in this area was, it appears, the earliest large-scale use of valves as devices for generating and using binary pulses.[23] At this time, the common wis-

dom was that valves could never be used satisfactorily in large numbers, for they were unreliable, and in a large installation too many would fail in too short a time. However, this opinion was based on experience with radio receivers and the like, which were switched on and off frequently. What Flowers discovered was that, so long as valves were left on, they could operate reliably for very long periods. As Flowers remarked, at the outbreak of war with Germany he was possibly the only person in Britain who realized that valves could be used on a large scale for high-speed digital computing.[24]

Once Tutte had explained his Statistical Method to Newman, Newman suggested using high-speed electronic counters to cope with the huge amount of counting of binary coincidences that the method demanded.[25] It was a brilliant idea, inspired by Newman's knowledge of C.E. Wynn-Williams' prewar work at Cambridge on the electronic counting of α-particle emissions.[23] Turing's contribution, in his role as a scientific policy advisor, was to persuade the Bletchley Park authorities that the machine envisaged by Newman should be built.[26] In December 1942, Newman was given the job of developing the requisite machinery.[27] The result was the Heath Robinson, installed at Bletchley Park in June 1943. Although the counters were electronic, Heath Robinson was largely electromechanical; the machine was effective, but slow and unreliable. Newman was sufficiently encouraged to place an order for more Robinsons with the Post Office.

During the design phase of Heath Robinson there were difficulties with the logic unit—the "combining unit" in the terminology of 1942. The job had been given to F.O. Morrell's telegraph section at Dollis Hill, and it was proposed to implement XOR by means of a frequency modulator of a type used for voice-frequency telegraph signals.[28] Because this device was analog, small variations would add up; wrong answers would often result.[28] At Turing's suggestion, Newman approached Flowers for help. Turing and Flowers had worked together previously in connection with a relay-based machine for use against Enigma (this was not the Bombe itself but a machine for automatically decrypting Enigma messages once the settings were known). Flowers and his switching group improved the design of the combining unit and manufactured it.[29]

Flowers did not think much of the Robinson, however. The basic design had been settled before he was called in, and he was skeptical as soon as Morrell (from whom he first learned of the Robinson) told him about it.[30]

Work on Colossus began early in 1943. It took Flowers and his team at the Post Office Research Station 10 months to complete the machine, working day and night, pushing themselves until (as Flowers said) their "eyes dropped out."

The Robinson depended on keeping two paper tapes, the message tape and the χ-tape, in perfect synchronism as they were driven on pulleys past a photoelectric reader at 1,000–2,000 characters per second. Flowers doubted that the Robinson would work properly, and in February 1943 he presented Newman with the alternative of a fully electronic machine able to generate the χ-stream (and ψ- and μ-streams) internally.[31] Opinion at Bletchley was that a machine containing the number of valves that Flowers was proposing could not work reliably. Newman pressed ahead with the two-tape machine, leaving Flowers to do as he wished regarding his alternative proposal. On his own initiative, working independently at Dollis Hill, Flowers began building the fully electronic machine that he could see was necessary. He embarked on Colossus "in the face of scepticism" from Bletchley Park and "without the concurrence of B.P."[31]

Colossus was not built "under the direction of Flowers and Newman" (as Davis, and folklore, assert). "B.P. weren't interested until they saw it [Colossus] working," said Flowers.[31] Flowers stated in an interview given in 1977:

> I don't think they [Newman et al.] really understood what I was saying in detail—I am sure they didn't—because when the first machine was constructed and working, they obviously were taken aback. They just couldn't believe it! … I don't think they understood very clearly what I was proposing until they actually had the machine.[32]

Not long before his death in 1998, Flowers

spoke with sadness about the fact that credit for Colossus was often given to Turing and to Newman. It is regrettable that erroneous accounts continue to appear.

Acknowledgment

I am grateful to Diane Proudfoot, four anonymous referees, and the editor, for comments and advice.

References and notes

1. Colossus is described in T.H. Flowers, "The Design of Colossus," *IEEE Annals of the History of Computing*, vol. 5, no. 3, July–Sept. 1983, pp. 239-252.
2. J. Good, D. Michie, and G. Timms, *General Report on Tunny, With Emphasis on Statistical Methods*; in the National Archives (Kew, Richmond, Surrey), document reference HW 25/4 (vol. 1), HW 25/5 (vol. 2), 1945, p. 35. A digital facsimile of *General Report on Tunny* is in The Turing Archive for the History of Computing; see http://www.AlanTuring.net/tunny_report.
3. B.J. Copeland, ed., "Letters on Logic to Max Newman," *The Essential Turing*, Oxford Univ. Press, 2004, pp. 204-216.
4. A.M. Turing, "On Computable Numbers, with an Application to the Entscheidungsproblem," *Proc. London Mathematical Soc.*, Series 2, vol. 42, 1936–1937, pp. 230-265.
5. For an account of Turing's life and work, see B.J. Copeland, ed., *The Essential Turing*, Oxford Univ. Press, 2004.
6. For more information about the ACE and the DEUCE, see B.J. Copeland, ed., *Alan Turing's Automatic Computing Engine*, Oxford Univ. Press, 2004.
7. The story of Tunny and the Bletchley attack is revealed in the recently declassified (2000) *General Report on Tunny* in Ref. 2. A digital facsimile of the complete report is available on the author's Web site at http://www.AlanTuring.net/tunny_report.
8. The Tunny machine was manufactured by the Lorenz company, the first model bearing the designation SZ40 ("SZ" stood for "Schlüsselzusatzgerät," meaning "cipher attachment"). A later version, the SZ42A, was introduced in February 1943, followed by the SZ42B in June 1944 ("40" and "42" perhaps refer to years). The physical machine is described in section 11 of the *General Report on Tunny* and in D. Davies, "The Lorenz Cipher Machine SZ42," *Cryptologia*, vol. 19, 1995, pp. 517-539; the machine's function and use is described in sections 11, 94, et passim, *General Report on Tunny*.
9. M. Davis, *The Universal Computer: The Road from Leibniz to Turing*, Norton, 2000, pp. 174-175.
10. J.A.N. Lee, *Computer Pioneers*, IEEE CS Press, 1995, pp. 306, 671.
11. Ibid, p. 492.
12. E. Enever, *Britain's Best Kept Secret: Ultra's Base at Bletchley Park*, 2nd ed., Alan Sutton, 1994, pp. 36-37.
13. J. Good, D. Michie, and G. Timms, *General Report on Tunny,* 1945, p. 458.
14. W.T. Tutte, "My Work at Bletchley Park," 2000. To appear in *Colossus: The First Electronic Computer*, B.J. Copeland, ed., Oxford Univ. Press, 2005.
15. J. Good, D. Michie, and G. Timms, *General Report on Tunny,* 1945, pp. 313-315.
16. *A Cryptographic Dictionary*, Government Code and Cypher School, Bletchley Park; in the US National Archives and Records Administration (College Park, Maryland), document reference RG 457, Historic Cryptographic Collection, box 1413, NR 4559, p. 89. A digital facsimile of *A Cryptographic Dictionary* is in The Turing Archive for the History of Computing; see http://www.AlanTuring.net/crypt_dic_1944.
17. J. Good, D. Michie, and G. Timms, *General Report on Tunny,* 1945, p. 313.
18. The reasoning is as follows. Let p_1 and p_2 be the first and second impulses of the plaintext and let $\Delta(p_1 + p_2)$ mean "the result of differencing $(p_1 + p_2)$." Then the above account of the workings of the Tunny machine implies that $\Delta(c_1 + c_2) = \Delta(p_1 + p_2) + \Delta(\chi_1 + \chi_2) + \Delta(\psi_1 + \psi_2)$. Tunny addition has the property that $x + \bullet = x$ for either value of x, dot or cross. So, since $\Delta(p_1 + p_2)$ and $\Delta(\psi_1 + \psi_2)$ are predominantly dot, $\Delta(c_1 + c_2)$ and $\Delta(\chi_1 + \chi_2)$ must agree with one another more often than not.
19. See further B.J. Copeland, "Colossus and the Dawning of the Computer Age," *Action This Day*, R. Erskine and M. Smith, eds., Bantam, 2001, pp. 342-369.
20. J.A.N. Lee and G. Holtzman, "50 Years After Breaking the Codes," *IEEE Annals of the History of Computing*, vol. 17, no. 2, Spring 1995, pp. 32-43. The quotation is from p. 33.
21. Flowers in interview with Copeland, July 1996. Except where indicated otherwise, all material in this article relating directly to Flowers derives from Flowers in interviews with Copeland, 1996–1998; and Flowers in interview with Christopher Evans in 1977 ("The Pioneers of Computing: An Oral History of Computing," Science Museum, London).
22. S. Turing, *Alan M. Turing*, Heffer, 1959, p. 71.
23. C.E. Wynn-Williams was among the first to suggest that electronic valves be used in place of relays, in connection with the counting of α-particle emissions; see C.E. Wynn-Williams, "The Use of Thyratrons for High Speed Automatic Counting of Physical Phenomena," *Proc. Royal Soc.*, Series A, vol. 132, 1931, pp. 295-310. (See also A.W. Hull,

"Hot-cathode Thyratrons," *General Electric Rev.*, vol. 32, 1929, pp. 390-399; and N.A. de Bruyne and H.C. Webster, "Note on the Use of a Thyratron with a Geiger Counter," *Proc. Cambridge Philosophical Soc.*, vol. 27, 1931, pp. 113-115.)

In 1931, Wynn-Williams reported (p. 302) that rings of three and four valves had been tried out experimentally. In contrast, Colossus I contained approximately 1,600 valves and the later Colossi approximately 2,400.

24. Flowers in interview with Copeland, July 1996.
25. J. Good, D. Michie, and G. Timms, *General Report on Tunny,* 1945, pp. 33, 458.
26. D. Horwood in interview with Copeland, October 2001.
27. J. Good, D. Michie, and G. Timms, *General Report on Tunny,* 1945, pp. 28, 33.
28. H. Fensom, "How the Codebreaking Colossus Was Conceived, Built and Operated: One of its Engineers Reveals its Secrets," 2001. To appear in *Colossus: The First Electronic Computer,* B.J. Copeland, ed., Oxford Univ. Press, 2005.
29. Flowers in interview with Copeland, July 1996; see also J. Good, D. Michie, and G. Timms, *General Report on Tunny*, 1945, p. 33.
30. Flowers in interview with Copeland, July 1998.
31. Flowers in interview with Copeland, July 1996.
32. Flowers in interview with Christopher Evans, 1977.

Jack Copeland is a full professor of philosophy and mathematical logic at the University of Canterbury, New Zealand, and director of The Turing Archive for the History of Computing. He studied mathematical logic at the University of Oxford under Turing's student Robin Gandy. He has published numerous journal articles, and his books include *Artificial Intelligence: A Philosophical Introduction* (Oxford: Blackwell, 1993, second edition forthcoming). He is editing three books for Oxford University Press: *The Essential Turing* (2004), *Alan Turing's Automatic Computing Engine* (2004) and *Colossus: The First Electronic Computer* (2005). He has held university positions in Britain, Australia, and New Zealand, and visiting positions in the US and Denmark.

Readers may contact Jack Copeland at The Turing Archive for the History of Computing (www.AlanTuring.net), Univ. of Canterbury, Private Bag 4800, Christchurch, New Zealand; jack.copeland@canterbury.ac.nz.

For further information on this or any other computing topic, please visit our Digital Library at http://computer.org/publications/dlib.