V viewpoints

DOI:10.1145/3018994

Thomas Haigh

Historical Reflections
Colossal Genius: Tutte, Flowers, and a Bad Imitation of Turing

Reflections on pioneering code-breaking efforts.

MAY 14, 2017, will be the 100th anniversary of the birth of someone you might not have heard of: William Thomas ("Bill") Tutte. During the Second World War he made several crucial contributions to decrypting the Lorenz cipher used to protect the Nazi high command's most crucial radio communications. This work provided the statistical method implemented electronically by Tommy Flowers, a telecommunications engineer, in the Colossus machines, which pioneered many of the electronic engineering techniques later used to build digital computers and network equipment.[a]

A scene from the 2014 film ***The Imitation Game*** with actor Benedict Cumberbatch portraying Alan Turing.

PHOTO BY SNAP STILLS/REX/SHUTTERSTOCK

Myths of Bletchley Park

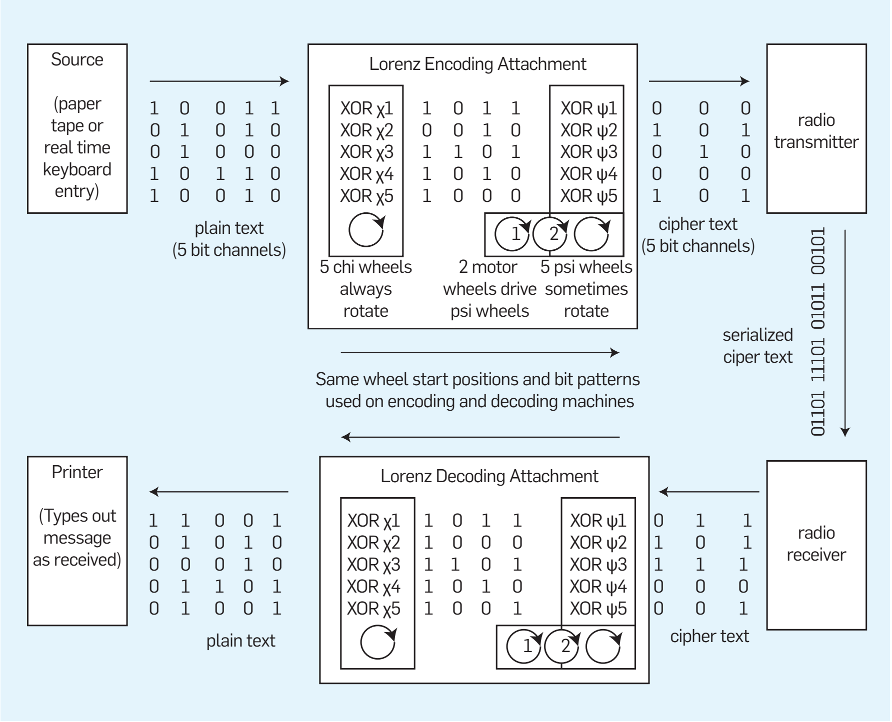
The British code-breaking effort of the Second World War, formerly secret, is now one of the most celebrated aspects of modern British history, an inspiring story in which a free society mobilized its intellectual resources against a terrible enemy. That's a powerful source of nostalgic pride for a country whose national identity and relationship with its neighbors are increasingly uncertain. Tutte's centennial gives a chance to consider the broader history of Bletchley Park, where the codebreakers worked, and the way in which it has been remembered. Some kinds of people, and work, have become famous and others have not.

Films reach more people than books. So statistically speaking, most of what you know about Bletchley Park probably comes from the Oscar-winning film *The Imitation Game*. This gives us a starting point: the film is a bad guide to reality but a useful summary of everything that the popular imagination gets wrong about Bletchley Park.

One myth is that Alan Turing won

a This column draws on a research project in progress I am conducting with Mark Priestley, supported by L.D. Rope's Second Charitable Settlement.

Figure 1. Logical representation of the action of the Lorenz machine, dubbed "Tunny" by the British. The gap of four characters shown between the chi and psi wheels is to symbolize the idea of two logically independent transformations applied to a five channel bitstream, rather than a representation of the actual inner working of the machine.



the war pretty much by himself. Benedict Cumberbatch played Turing as television's *Sherlock*: a humorless, asexual loner whose superhuman mental powers are compromised only by an almost autistic indifference to social norms. This combines the traditional focus of popular science writing on the lone genius who changes the world with the modern movie superhero narrative of a freak who must overcome his own flaws before he can save the world. (This is, I understand, exactly the same arc Cumberbatch follows in *Doctor Strange*, a literal superhero movie). A team of six bright young men arrive at Bletchley Park and are given the job of breaking the German Enigma code. After introducing himself as "the best mathematician in the world," Cumberbatch dismisses his fellow codebreakers, saying "I don't have time to explain myself as I go along, and I'm afraid these men would only slow me down." Over their objections, and the opposition of almost everyone else at Bletchley Park, he designs a machine called Christopher to beat Enigma.

The film struggles to shoehorn a complicated, nuanced, and tragic story into the generic template of a hero overcoming obstacles, facing disaster, and eventually triumphing. In reality, Turing was far from a marginal and despised figure at Bletchley Park, moving quickly to a leadership role. The obstacles Cumberbatch faces are mostly fictional and often absurd. His boss (in reality Turing's subordinate) Hugh Alexander tries to smash Christopher. Like all military men Alastair Denniston, the head of Bletchley Park, is a belligerent idiot. He smashes down the door, hoping to have Christopher destroyed. A little later Cumberbatch is blackmailed into passing secrets to a Soviet spy. Cumberbatch's growth is symbolized by his making friends with the other brilliant codebreakers, but they seem just as arrogant as he was. Fearful that Bletchley Park managers will get in the way, they pretend that Enigma is unbroken and instead run the Battle of the Atlantic from their machine room, deciding which convoys to save and which the U-boats should be allowed to sink.

Another myth is that code-breaking machines eliminated human labor and code-breaking skill. At first Christopher spins uselessly, producing dramatic tension but no Enigma settings. At the last minute, Cumberbatch thinks of looking for the common phrases, such as "Heil Hitler," to detect when the correct settings have been found. Enigma is broken! In reality this was not something that occurred to Turing only after he had finished building a completely pointless machine, but basic cryptanalytic practice already used to break Enigma manually.

Even with the Bombe, breaking Enigma continued to rely on a mix of human skill, manual methods, and machine power. Each Bombe was tended by a team of female operators, and in recent years a lot of attention has been paid to the experiences of these women. The Bombe operators and Enigma decrypters worked in factory-like conditions, in a massive operation pioneered by Gordon Welchman for the group attacking Air Force Enigma. Welchman had made his own vital contribution to the Bombe's design, a "diagonal board," but after the machines arrived shifted to overseeing their use. In contrast, once logistical challenges began to outweigh conceptual ones Turing drifted away from leadership of the corresponding group tackling Naval Enigma. There are many kinds of genius, and Turing's was not of the managerial variety.

By early 1945 more than 10,000 people worked directly on the British codebreaking effort. Most of them were women. The film directs some heavy-handed sexism at Joan Clarke, a rare female cryptanalyst, to give viewers a chance to feel superior to their grandparents. Word at Bletchley Park was indeed deeply stratified by class and gender, and cryptanalytic work of the kind done primarily by upper middle class men like Turing has traditionally been the most celebrated. Yet its own erasure of the work routinely done by women reflects a more modern sexism. A single giant machine, given by a superman, clunks without human intervention until the answer emerges.

That's silly. So is the myth that brilliant scientists need no help from engineers. Cumberbatch drew up the engineering blueprints for the one and only Bombe during a montage, then built it at Bletchley Park aided by a handful of briefly glimpsed assistants. In fact, approximately 200 Bombes were manufactured, none of them at Bletchley Park, with design and production work done primarily by the British Tabulating Machine Company, under the direction of its chief engineer Harold Keen. BTM had licensed IBM punched card technology for sale throughout the British Empire, giving it command of the necessary technologies and engineering methods.

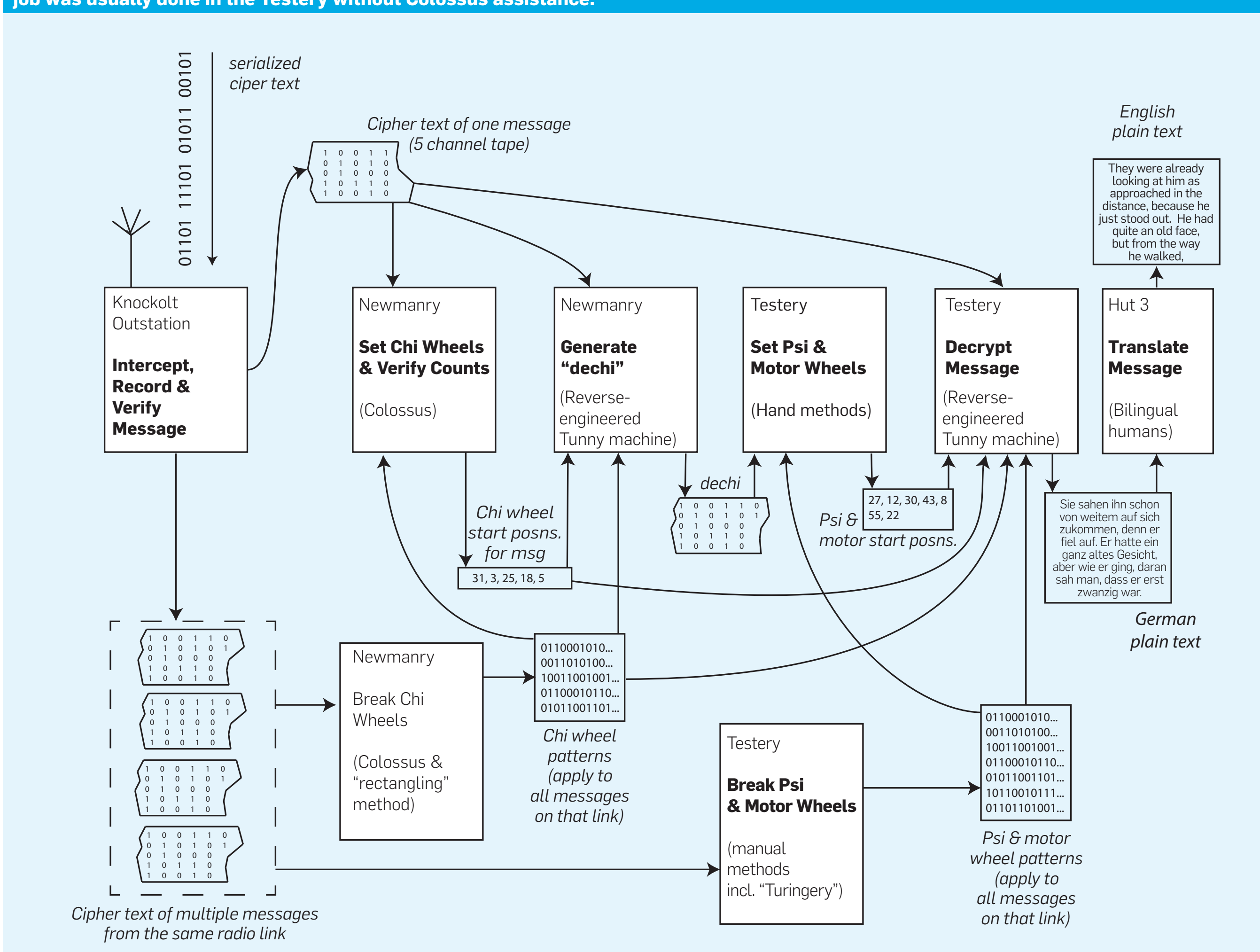
In this way, and countless others, technology transcended, rather than supplemented, human labor and bureaucracy. Perhaps nobody would pay to see a movie centered on heroic production engineers, brilliant Bombe operators, and inspirational government procurement specialists, but would it be so difficult to give walk-on parts to the people who actually designed, built, and operated the Bombes? It's not like leaving them out makes the firm particularly entertaining: political comedian John Oliver recently likened a hellish commute requiring three buses and two trains to "the length of the movie *The Imitation Game*—two wasted hours that feel like forever."

Tunny

There's another popular myth endorsed by the *The Imitation Game*: that the Enigma was the only significant German cipher broken at Bletchley Park. In reality another cipher, codenamed Tunny, was just as important. Enigma was used by the German military to communicate with forces in the field. Compact code boxes flashed up the appropriate letter of ciphertext each time a key was pushed. The encrypted version of the message was transmitted by a human using Morse code. Tunny was used by the German High Command to communicate with generals outside the reach of wired communication links, such as the divisions deep inside the USSR. Messages typed on a keyboard were encrypted, transmitted by radio, and automatically decrypted and printed at the other end. Enigma was declassified long before Tunny, with the result that early histories assumed that all intelligence delivered by Bletchley Park had come from Enigma.

The British knew nothing about the machine producing Tunny, working entirely on clues from the intercepted messages. In contrast, the team breaking Enigma had a number of resources to draw on. Enigma technology had been sold commercially since the 1920s, so its architecture was public. The German government specified modifications but Polish teams had broken earlier military versions. They passed their secrets, and the initial Bombe design, on to the British at the start of the war. Even the name "Bombe" came from the Polish "bomba kryptologiczna." Captured German personnel, code books, keys, and manuals provided more clues to changes in Enigma technology and practice.

Figure 2. The overall Tunny interception and decryption workflow process as of late 1944. While Colossus machines could also be used to tackle the Psi wheels, the increased pressure of work after the Germans began daily changes to wheel patterns meant that this part of the job was usually done in the Testery without Colossus assistance.



The first challenge was to figure out the structure of the machine that had produced the Tunny messages. This relied on operator error. In August 1941 a long message was sent twice, with minor alterations, using the same machine settings. Comparing the two messages let Brigadier John Tiltman piece together the original ("plain") text of each message and the encoding sequence ("key stream") with which each had been combined to yield its cipher text (see Figure 2). This nicely disproves the idea that Bletchley Park's experienced military men were there primarily to frustrate Turing.

Tutte's Breakthroughs

Tutte used these sequences to make the breakthrough. Shortly after the outbreak of war he had joined Bletchley Park's "Research Section," which had responsibility for investigating unfamiliar codes and devising methods that could be used to break them on a production basis. Like many of his colleagues he had a Cambridge degree, though as the son of a gardener his social background was unusually humble. His first degrees were in physical chemistry, but his interests were already shifting to mathematics.

Looking at the teleprinter tape five channels separately Tutte noticed a regularity every 41 characters in the key sequence. This gave the clue that a 41-character code wheel was involved. Step by step, Tutte's team worked out the full, complex structure of the Lorenz machine and its 12 code wheels (see Figure 1). Three kinds of information were needed to decrypt a Tunny message. Tutte had provided the first, by reverse engineering the Tunny machine's internal structure. From this the British built their own Tunny decrypting machines.

Two challenges remained. The second piece of information was the position of each of the wheels at the start of a message. Finding this was called "wheel setting," and had to be done for each message. The third was the bit pattern set up on each of the wheels. These were regularly changed by flipping tiny pins. Finding these sequences was called "wheel breaking," and was performed less frequently as most changed only monthly or quarterly.

After Tutte cracked the structure of the Tunny machine a new group, named the Testery after its head, Major Ralph Tester, went to work breaking its messages. While seconded to the research section, Turing came up with a method for figuring out the bit patterns on the coding wheels once the keystream had been successfully isolated. The cryptanalyst formed and tested hypotheses to gradually extend the known portion of the wheel pattern. "Turingery," described by Tutte as "more artistic than mathematical" made wheel breaking feasible, if arduous.

Both wheel setting and wheel breaking depended on luck, ingenuity, and German errors, but because wheel setting had to be done for each message it proved the biggest constraint. Until October 1942 the German operators were kind enough to precede each message with a series of 12 unencrypted letters, each coding the position for one of the wheels. Clues of this kind made the work of the codebreakers much easier, as hints obtained from decrypted messages were applied to others sent on the same link. Their results were sporadically impressive, but improvements in German practice threatened to close the door entirely.

At this point Tutte made his second huge contribution. When setting wheels it was easy to determine statistically whether a particular combination yielded natural language or random noise. Trying every possible combination of positions across the 12 wheels was clearly impossible: the war would be over, and the Earth swallowed up by the sun, long before the job was finished. But flaws in the design of the Lorenz machine made it possible to break the job into tractable steps. Each channel was encrypted by the successive action of two code wheels. The first set, known at Bletchley Park as the chi wheels, rotated to the next position each time a character was read, whereas the second set, the psi wheels, turned only when directed to do so by two "motor wheels." Decrypting a Tunny message posed two main challenges. First to set the chi wheels, using this information to generate "dechi," text encrypted only by the psi wheels. Then to set the psi and motor wheels, using this information to generate plain text.

Another myth is that code-breaking machines eliminated human labor and code-breaking skill.

Because the psi wheels did not always rotate, their contribution to the cipher text often repeated from one character to the next. This, Tutte realized, gave a statistical method to set the chi wheels without making any assumptions about the psi wheels. Whether the wheels moved or not they still masked the distinctive character distributions of German text. But whenever the psi wheels did not rotate, the deltas between successive characters would pass through them unchanged.

Analyzing a sample of decrypted messages showed him that the distribution of deltas was far from random. For example, in German "ei" is a very common string. E is (1,0,0,0,0) and I is (0,1,1,0,0). Their delta, (1,1,1,0,0) had a frequency of 5.9%—almost twice as common as in a random distribution. The delta between two repeated characters, (0,0,0,0,0), occurred 4.6% of the time. German has many double "s" characters, and teleprinter operators often pushed the shift and unshift keys, encoded as their own characters, twice to make sure that they were received.

When the distribution of deltas in successfully dechied text was plotted the same tell-tale "bulges" in the distributions of deltas appeared. If the psi wheels moved about half the time the peaks and valleys would be half as tall but follow the same pattern. However, if dechi was produced with the wrong wheel settings the distribution of deltas should be close to random, with all combinations occurring about 3.1% of the time.

Setting chi wheels meant generating dechi with different wheel combinations and looking for a non-random distribution of deltas. The five chi wheels could take 22 million combinations, but because each acted on only one of the five bit channels that encoded each character there was no need to consider all wheels simultaneously. The five most common deltas were (1,1,0,1,1), (1,1,1,0,0), (0,0,0,1,0), (1,1,1,1,1), and (0,0,0,0,0). In each case first two channels were either (1,1) or (0,0) and so added to 0. Maybe your school didn't teach you that 1+1=0, but in this context "addition" meant the logical operator XOR. Tutte devised a very simple method: (a) use all 1,271 possible wheel start positions to generate dechi for channels 1 and 2, (b) for each dechi stream count the number of positions where deltas for channels 1 and 2 add to 0, (c) take the wheel settings with the highest count. Once settings for the first two wheels were found the process was repeated to identify the others. If everything went well, this would set all five wheels by processing the encrypted message about 2,400 times.

Here, at last, was a way of breaking Tunny messages that did not depend on German laxity. It was possible to verify Tutte's method with hand calculation, but no manual method that involved comparing lengthy sequences so many times would ever be practical for production use. The success of the Bombes against Enigma made mechanization the obvious solution. Max Newman, a Cambridge mathematics lecturer, was put in charge of a small group exploring machine methods for Tunny.

Flowers and Colossus

Enter our third major protagonist, Tommy Flowers. Flowers came from a working class background, earning a degree in night school while working as an apprentice. He rose through the engineering ranks of the General Post Office, the government monopoly responsible for telephone and telegraph service as well as mail delivery. By the time the war began he was the leading electronics specialist at the Post Office's Dollis Hill research station. In January or February 1943, Newman arranged for a contract with Dollis Hill to build parts of a prototype machine able to apply Tutte's statistical method. Flowers, and others at Dollis Hill, had already been working with Bletchley Park to explore the application of electronic, rather than mechanical, sensing units to the next generation of Bombes.

Nicknamed "Heath Robinson," after a British cartoonist known for drawing improbably complex machines, the prototype read two looped paper tapes. When implementing Tutte's method one would hold the message text and one the coding key series produced by a particular pair of chi wheels. Dollis Hill's experience with telegraphic equipment, and Flowers' personal enthusiasm for electronic signal processing, came together in an optical sensing system, able to coordinate the two tapes at up to 2,000 characters per second. This allowed it to evaluate all possible combinations for the first two chi wheels in about half an hour. After the prototype proved itself, during testing in mid-1943, Dollis Hill built several more Robinsons.

Technology transcended, rather than supplemented, human labor and bureaucracy.

Back in March 1943, Flowers had also persuaded Newman to endorse experimental work on a machine able to simulate Tunny code wheels electronically rather than read them from tape. With no need to synchronize two tapes the message could be run at 5,000 characters per second. More importantly, it became much easier to change bit patterns or set new combinations of wheels. This reduced set up time between runs, and opened the door to new analytical tactics. As well as cramming electronic vacuum tubes into the simulated code wheels, Flowers used them liberally in its counters and in the logic circuits used to combine inputs in different ways. The first Colossus, delivered to Bletchley Park in January 1944, had approximately 1,500 tubes, a huge number by the standards of the day, but Flowers later said he knew it could run reliably because of his prewar experiments with a prototype electronic telephone exchange.

Colossus delivered a huge productivity boost. In February Newman's section was setting only four or five messages a day, but by March, with the first Colossus still not fully operational, this had already risen to 20. More machines were ordered. Here too work was segregated: cryptographers (overwhelmingly male and upper middle class) directed female Colossus operators. Once chi wheel settings were known then psi and motor wheel settings were usually performed in the Testery. Using linguistic knowledge and craft skills, rather than mechanical aids, it took about an hour to identify the correct settings for a message if things went well. Bletchley Park had, after all, deliberately recruited champion crossword solvers. Colossus could handle this job, but usually helped out only when spare machine time was available. Once all settings were known women, mostly from working class backgrounds, operated machines to decrypt the messages. The Tunny messages were translated by a mixed-gender group of middle class university graduates, analyzed by male intelligence specialists, and filed by women in a massive repository indexed with punched cards.[b]

Tutte realized that his statistical method could also, given a sufficiently long message, be used to break wheels. The technique was called "rectangling" because it involved making a large table tabulating every possible position of two wheels. The first two chi wheels repeated themselves every 1,271 characters, meaning a very long message might contain a dozen or more characters encoded with each possible wheel combination. Whenever the psi wheels did not rotate, the sum of the deltas from the encrypted message would be the same as the sum of the deltas on the corresponding channel of the chi wheel sequence and the plain text. Because the deltas of the first two channels of plain text were disproportionately likely to sum to zero, this exposed information about the wheel patterns. The encrypted message deltas tallied in each cell of the table gave clues about the sum of the deltas of the two corresponding code wheels. A high score

b The gender and class background of the different jobs is taken from Christopher Smith, *The Hidden History of Bletchley Park*, Palgrave, 2015. The work of Colossus operators is discussed in Abbate, J. *Recoding Gender: Women's Changing Participation in Computing.* MIT Press, Cambridge, MA, 2012.

pointed to a delta total of one, a low score to a total of zero. Codebreakers worked from estimates of the delta totals back to the separate deltas on each wheel, using a technique similar to the solving of a "magic rectangle." These candidate wheel deltas were then set up on Colossus, and varied over many runs to maximize fit with other messages using the same wheel patterns. Later versions of Colossus included an extra control panel, making it easier to set up and test candidate wheel patterns without going around to the back of the machine. Once the deltas for each wheel were established deriving the raw wheel patterns was trivial in comparison. Wheel breaking, like wheel setting, no longer relied on slips by the German operators. This was just as well, because in July 1944 they started changing all wheel patterns daily.

Colossus in Context

Turing is often misidentified by journalists as the creator of Colossus. As I discussed in a previous column, the "Matthew Effect" means that all the credit for any technical achievement tends to go to the most famous person tangentially associated with it. *The Imitation Game* further confuses this: "I want Christopher to be … a digital computer" Cumberbatch says of his Bombe, after being asked whether he is trying to build a Turing machine.

This seems to deliberately blur the Bombe with Colossus, which has often been called "the first programmable electronic computer," though Flowers himself was ambivalent about calling it a computer in his talks and articles. He saw it as a "processor," part of the evolution of digital bit stream manipulation toward his dream of a fully electronic telephone exchange. After working with Mark Priestley on a detailed analysis of Colossus I agree with Flowers. Colossus could be set up to combine input bitsteams from tape and the simulated code wheels in many different ways, running the selected inputs through a network of logic gates. This gave it the flexibility to carry out many different Tunny-related attacks. Because it did not include any hardware for arithmetic calling it a computer confuses things, whether we go by today's meaning of the word or 1940s definitions. Its configurable logic was stateless, used only to combine the current set of inputs to increment, or not increment, each of its five counters. The counters retained state from one tape character to the next, but the logic networks could not access this information. Neither was it programmable, as its basic sequence of operations was fixed (though many parameters could be set with switches). Colossus was a milestone in the development of digital electronics, incorporating many of the circuits and hardware features later used to build computers. But it had a quite different purpose, and different architecture, from an electronic computer.

Newly declassified information gives us a better sense of just how impressive Colossus was.

Newly declassified information gives us a better sense of just how impressive Colossus was. During the war the U.S. commissioned dozens of different specialized code-breaking machines from prominent companies and research centers such as IBM, NCR, Bell Labs, and MIT. Almost without exception the most technologically ambitious projects, such as microfilm and electronic memories, were late, abandoned before completion, or proved so unreliable as to be useless. Even some of the more technologically conservative projects, such as a million-dollar giant Bombe built by Bell Labs, fizzled in use because they were constructed without a good grasp of code-breaking practice.[c] Likewise, pretty much all post-war electronic computers, which like Colossus depended on making thousands of vacuum tubes work together, were plagued by reliability problems and took far longer to finish than expected. The more I look at those other projects of the 1940s the more amazed I am that the Dollis Hill team had the first Colossus installed and working at Bletchely Park less than a year after pitching it to Newman.

c These projects are described in Burke, C.B. *It Wasn't All Magic: The Early Struggle to Automate Cryptanalysis, 1930s–1960s.* National Security Agency, 2002.

Remembering and Forgetting

Back to *The Imitation Game*, which never mentions Tunny, Flowers, Colossus, or Tutte. The end of the movie takes place several years after the war. Cumberbatch's Turing is coming apart mentally after being sentenced to compulsory hormone treatments intended to contain his homosexual urges. He bumbles around his house in a bathrobe, drifting toward suicide, distracting himself only by building another Christopher. To send the audience out on a more cheerful note, Joan Clarke, his friend and former fiancée, visits to point out that she had "just taken a train through a city that would not exist if it wasn't for you. I bought a ticket from a man who would likely be dead if it wasn't for you."

When victory was declared, Cumberbatch boasted that "the war was really just a half-dozen crossword enthusiasts in a tiny village in the south of England. Was I God? No. Because God didn't win the war." I'm sure that the real Turing never dismissed the millions who fought and died in this way. He wasn't an idiot. But beneath the film's sepia nostalgia lies a very modern delusion: established institutions (such as government and the military) are so dysfunctional, and ordinary people so irrelevant, that tech geniuses must secretly seize power. To put that another way, Turing wasn't Peter Thiel.

Tutte made the same kind of dazzling intellectual contributions as Turing to the success of Bletchley Park. But brilliance alone does not win one the kind of fame that culminates in a glossy scientific biopic—an extremely rare honor. After earning his Ph.D. in 1948 Tutte followed the trajectory of his wartime work into a distinguished mathematical career focused on graphs and matroids. He is well remembered in those fields, and his wartime contribution is documented, for those who care, in several histories of Bletchley Park. Tragedy and drama attracted Hollywood to the lives of Alan Turing, Stephen Hawking (*The Theory* *of Everything*), and John Nash (*A Beautiful Mind*). Contentment is not as exciting to watch as tragedy, but most of us would prefer it for ourselves. I don't think Tutte minded this relative neglect—he appears to have lived a long, happy, and active life full of scholarly accomplishments and recognition, including appointment as a Fellow of the Royal Society and even the posthumous naming of an asteroid.

Flowers was less satisfied than Tutte with his career, never entirely realizing his vision for a fully electronic telephone exchange. His relative obscurity reflects a larger tendency to remember conceptual breakthroughs and ideas, which fit the stereotype of individual genius, rather than system building accomplishments, which are inherently team based. He lived to experience a small measure of fame for his work on Colossus, but seemed bitter, complaining that his career was over before he could benefit from this newfound respect. His reputation has continued to grow, and in the past few years a postage stamp and a display in the Science Museum in London have celebrated Colossus as a founding contribution to digital technology.

The real story of Bletchley Park is one of teamwork on a massive scale, in which good management and effective procurement were just as important as individual scientific genius. Tutte and Flowers did not win the war by themselves, any more than Turing did. But, whether or not the Colossus story ever makes it to the big screen, each played an outsize role in the defeat of fascism. C

Further reading

Copeland, Jack.
Colossus: The First Electronic Computer. **Oxford University Press, New York, 2006. A compendium of analysis, reprinted historical documents and memoir. Contains Tutte's own description of his breakthroughs against Tunny.**

Gannon, Paul.
Colossus: Bletchley Park's Greatest Secret **(Atlantic Books, 2006). The clearest overall history of Colossus.**

Hodges, Andrew.
Alan Turing: The Enigma. **Princeton University Press, Princeton, NJ, 2014. *The Imitation Game* was nominally based on Hodges' landmark biography of Turing, but don't let that put you off. He's maintained a tactful silence about the movie.**

McKay, Sinclair.
The Secret Lives of Codebreakers: The Men and Women Who Cracked the Enigma Code at Bletchley Park. **Gives a fascinating window onto the social history of Bletchley Park and the experiences of the people who worked there.**

Randell, Brian.
"The Colossus." In Metropolis, N., Howlett, J. and Rota, G.-C. eds., Academic Press, New York, 1980, 47-92. This paper broke the public silence surrounding Colossus, at a time when the British government was still actively suppressing the release of information.

Welchman, Gordon.
The Hut Six Story: Breaking the Enigma Codes **(McGraw Hill, 1982). The most substantial first person account of Bletchley Park, focused on Enigma rather than Colossus.**

Thomas Haigh (thomas.haigh@gmail.com) is a Visiting Professor at Siegen University and an Associate Professor at the University of Wisconsin—Milwaukee. He is the primary author of *ENIAC In Action* (MIT Press, 2016). Read more at http://www.tomandmaria.com/tom