The Bill Tutte Memorial Fund

How Bill Tutte Won the War

(or at least helped to shorten it by two years)

Introduction

Many readers will be familiar with the work of Professor William "Bill" Tutte of Waterloo University, Ontario, whose pioneering studies in graph and matroid theory led to his pre-eminence in the field of Combinatorics. Fewer will be aware that he was also responsible for one of the greatest intellectual feats of World War 2.[1]

History has credited him with shortening the war in Europe by two years, saving the lives of millions, but he never received the public recognition or acclaim that he deserved.[2] In fact, it was not until a few years before his death in 2002 that he was able to speak about it, and then only with his usual modesty.

Early Days

Bill Tutte was born in Newmarket, Suffolk, on 14 May 1917 into humble circumstances; his father was a jobbing gardener and his mother a housekeeper. He was educated at Cheveley village school where the headmaster soon recognised his potential and encouraged him in his studies; Tutte later recalled frequently consulting the school's copy of The Children's Encyclopaedia.

He passed the scholarship examination (11+) to the Cambridge and County High School, which required him to travel over 16 miles each way by bicycle and train daily; when the weather was fine or his parents could not afford the train fare he would cycle the whole way on a bike donated by a local charity.

He continued to excel at school and in 1935 was awarded a scholarship to Trinity College, Cambridge, to read Natural Sciences, specialising in Chemistry. Tutte soon joined a small group of undergraduates in the Trinity Mathematical Society who shared his love of mathematical puzzles.

With his friends Leonard Brooks, Cedric Smith and Arthur Stone, and writing under the pseudonym Blanche Descartes derived from the initial letters of their first names, Tutte published a solution to the problem of squaring a square with tiles of different sizes; their solution was novel in that it compared the square with an electrical circuit and used Kirchhoff's Laws in the analysis. (The squared square is still the logo of Trinity Mathematical Society.)

It was this interest in mathematical puzzles that led in 1941 to him being invited to join the Government Code and Cypher School at Bletchley Park. During the First World War it had been linguists who were in demand as code breakers but by the 1940s codes and ciphers were largely mathematically based.

[1] Citation for the award of Officer of the Order of Canada in 2001.

[2] This analysis of Tutte's contribution has been attributed to General Eisenhower by Captain Jerry Roberts, one of the last surviving members of Major Ralph Tester's team ("The Testery") at Bletchley Park

Bletchley Park and Lorenz

At Bletchley Park Tutte was interviewed by Alan Turing, then heavily involved in the Enigma code breaking for which he later became famous, but did not join Turing's team. Instead Tutte joined the renowned cryptanalyst Colonel John Tiltman's research team, who were grappling with a new code, nicknamed Tunny (one of the Fish series of codes), which was vastly more complex than Enigma and, as it turned out, strategically much more important.

Tunny, or as we now know it Lorenz, encrypted messages that were sent by radio teleprinter using Baudot code, whereas Enigma used Morse code and the 26 letter alphabet.

Lorenz was an enciphering attachment to teleprinter machines using punched paper tape that had been introduced by Hitler for strategic communications between himself and his top level commanders and their headquarters, while Enigma was used for tactical messages between individual formations and units, notably ships and submarines. Hitler called Lorenz his "Secrets Writer" (Geheimschreiber) and considered it unbreakable, entrusting it with the most sensitive information.

After months of unsuccessful attempts to decipher Lorenz messages that had been intercepted at the "Y Stations" around Britain, the code breakers at Bletchley Park ("Station X") were gifted an opportunity on 30 August 1941 when a German operator sent the same long message twice but, contrary to all regulations, with the same Lorenz settings.

Crucially, in the second message the operator used abbreviations for a number of common words, for instance Nr for Nummer (number), and changed the punctuation. In just ten days Tiltman had deciphered the message. However, this in itself did not reveal the mechanism by which the messages had been enciphered. That task was given to Bill Tutte.

Studying the broken code in detail, Tutte noticed a repeat pattern of 41 characters and deduced that the first wheel or rotor in the Lorenz machine must have 41 teeth. Over a period of weeks, by intellect and intuition alone, he went on to accurately describe all 12 rotors, without ever having seen a Lorenz machine.

By contrast, Enigma used only 3 (Army and Air Force) or 4 (Navy) rotors and Turing had access to captured machines and help from the Poles who had worked on the machine before the war to assist him in cracking the code. A new team under Major Ralph Tester ("The Testery") was set up to exploit Tutte's breakthrough.

Subsequently a GPO engineer, Tommy Flowers, designed and built Colossus, the world's first programmable electronic computer, to run the algorithms that Tutte created to read intercepted Lorenz encoded messages, giving allied intelligence services invaluable information on German strategic intentions and capabilities.

Consequences

After the entry of the USA into the war against Hitler in December 1941, many believed that eventual victory was inevitable; however, what was far from certain was when that would be. Churchill even feared that it could take until 1950.

He knew that it would take years for the huge American economy and industrial capability to transform onto a war footing, and he was fearful of a premature engagement in Europe that could result in defeat by the battle-hardened German armies.

The Battle of Kasserine Pass in February 1943 when Rommel's Afrika Korps routed poorly led and untested American troops in Tunisia proved his point. Similarly, the disastrous Dieppe landings in August 1942 had shown how inadequate forces could not hope to land on strongly defended coastal positions.

Churchill and Roosevelt had realised at an early stage that Russia held the key to defeating Hitler and, as well as providing the Russians with prodigious amounts of war equipment, the supply of strategic information obtained from intercepted Lorenz messages was critical.

The surrender of German forces at Stalingrad in the winter of 1942/3 allowed the Russians to move onto the offensive. Hitler was determined to crush them and to avenge the defeat at Stalingrad. In July 1943, 3000 German tanks faced almost twice that number of Soviet heavy armour at Kursk, 280 miles South West of Moscow, in the largest engagement of armour ever to have taken place. Although heavily outnumbered, the German tanks were far superior in armour and fire power.

However, delays in German arrivals allowed the Russians to prepare formidable defences and to concentrate their forces. Moreover, German misgivings about the forthcoming battle led to much signals traffic using the supposedly unbreakable Lorenz code machines. Thanks to Bill Tutte, the British were able to read this traffic. (British radio technology was far ahead of that of both the Germans and Russians, neither of whom could believe signals traffic in Russia could be intercepted in Britain.)

The British were able to give their Russian allies almost the complete German order of battle, leading to a stunning Russian victory which they rightly called the Turning of the Tide. General Zhukov, the Russian commander, was so impressed with the information he had been given that he thought the British must have had a mole in the German army headquarters, which in effect we did.

Afterwards, the Russian advance into Germany and eventually to Berlin was unstoppable, but it did ensure the engagement of up to 100 Divisions of crack German troops with countless tanks and aircraft on the Eastern front for the rest of the war. This massive diversion of German resources allowed the successful Allied invasion of Normandy in June 1944, but only after intercepted Lorenz traffic had satisfied General Eisenhower that Hitler was convinced that the invasion would come at the Pas de Calais.

The final defeat of Nazi Germany in May 1945 can be linked directly to the work of Bill Tutte. Had the Germans defeated the Russians at Kursk, the war in the West would have been very different indeed.

While the end result may well have been the same, without Bill Tutte's cracking of the Lorenz code the war could have gone on for many years longer. Alan Turing may have saved Britain from defeat in the Battle of the Atlantic in 1941 when we stood alone, but Bill Tutte shortened the war in Europe by some two years, saving countless lives.

Ironically, it was British mistrust of the Russians that led to Bill Tutte receiving no recognition or award for his war winning achievement. We never admitted to the Russians that we had cracked the Lorenz code.

After the defeat of Germany, the Russians used captured Lorenz machines for their own coded messages throughout the early days of the Cold War, without realising that British security services could read the traffic.

To have recognised Bill Tutte's achievement would have given the game away. It was not until nearly 50 years later that Tutte's story came out, but by then the history of Bletchley Park was dominated by the story of Alan Turing, largely as a result of the tragic circumstances of his death.

Even now, much remains secret about Bill Tutte's wartime achievements.

Later Life

After the war Bill Tutte returned to Trinity College to complete a doctorate in mathematics before emigrating to Canada, where he enjoyed a distinguished academic career at Toronto and later Waterloo Universities.

He was made a Fellow of the Royal Society in 1987 and an Officer in the Order of Canada in 2001, shortly before he died in 2002. Stories about his activities at Bletchley Park began to emerge in the mid-1990s during a project to rebuild the Colossus computer. (Tommy Flowers' work had also been kept secret, leading the Americans mistakenly to claim the world's first electronic programmable computer.)

In 2011 a BBC TV documentary programme "The Lost Heroes of Bletchley Park" drew public attention to Tutte and Flowers for the first time and, following a campaign by the local newspaper in Newmarket, in 2012 the Prime Minister, David Cameron, wrote to Tutte's remaining family in the town to express the nation's belated gratitude to him.

Memorial

Newmarket Town Council has now resolved to commemorate Bill Tutte with a memorial in the town centre and to endow a school scholarship or prize fund in his name to encourage local young people, particularly those from humble backgrounds as Tutte himself was, to study and excel in mathematics or computer science.

The proposed cryptic memorial by the acclaimed sculptor Harry Gray features pierced steel panels to represent the punched paper tape on which Lorenz messages were transmitted, a squared square and a 41-toothed wheel. Further information may be found at www.billtuttememorial.org.uk, together with details of how to subscribe to the memorial fund.

Richard Fletcher

Secretary, Bill Tutte Memorial Fund

(For further reading see C.J. Budd, 'Bill Tutte: Unsung Bletchley Hero', in S. Parc (ed.), *50 visions of Mathematics*, Oxford: Oxford University Press, forthcoming.)