Alan Turing, Marshall Hall, and the Alignment of WW2 Japanese Naval Intercepts

Peter W. Donovan

Marshall Hall Jr. (1910–1990) is deservedly well remembered for his role in constructing the simple group of order $604800 = 2^7 \times 3^3 \times 5^2 \times 7$ as well as numerous advances in combinatorics. A brief autobiography is on pages 367–374 of Duran, Askey, and Merzbach [5]. Hall notes that Howard Engstrom (1902–1962) gave him much help with his Ph.D. thesis at Yale in 1934–1936 and later urged him to work in Naval Intelligence (actually in the foreign communications unit Op-20-G).

> I was in a research division and got to see work in all areas, from the Japanese codes to the German Enigma machine which Alan Turing had begun to attack in England. I made significant results on both of these areas. During 1944 I spent six months at the British Headquarters in Bletchley. Here there was a galaxy of mathematical talent including Hugh Alexander the chess champion and Henry Whitehead the eminent topologist…

Burroughs, Lieberman, and Reeds [2] clarified the work of Op-20-G on the Enigma in a contribution to the obituary of Andrew Gleason (1921–2008). Unfortunately the surviving records scarcely allocate credit to individuals. Hall was one of about ten core members of a team of about thirty not far from being another galaxy of mathematical talent. See Christenson [3].

Peter Donovan is retired from the mathematics department of the University of New South Wales in Sydney, Australia. His email address is p.donovan@unsw.edu.au.

DOI: http://dx.doi.org/10.1090/noti1090

The statistician Edward Simpson led the JN-25 team ("party") at Bletchley Park from 1943 to 1945. His now declassified general history [12] of this activity noted that, in November 1943:

> [CDR Howard Engstrom, U.S.N.] gave us the first news we had heard of a method of testing the correctness of the relative setting of two messages using only the property of divisibility by three of the code groups [5-groups is the usage of this paper]. The method was known as Hall's weights and was a useful insurance policy just in case JN-25 ever became more difficult. He promised to send us a write-up of it.

The JN-25 series of ciphers, used by the Japanese Navy (I.J.N.) from 1939 to 1945, was the most important source of communications intelligence to the WW2 Allies in the Pacific.

Alan Turing's Work on Applied Probability

The centenary of the birth of Alan Turing (1912–1954) was extensively publicized in the popular and semipopular media. His contributions to applied probability theory and the central role this played in WW2 cryptology were substantially overlooked. In fact, Jack Good published two papers ([6] and [7]) which set out the technical aspects of his work. Good had been Turing's assistant for a while in his Bletchley Park years. Some analysis of the use made of this work in WW2 cryptology is now possible.

The greatest achievement of WW2 Allied cryptology was the breaking of the German encrypted teleprinter (teletype, teletypewriter), called *Tunny* by the cryptologists. Eventually this was handled

by the celebrated Colossus device, an (almost) electronic machine that replaced the optical punched tape-based Robinson. Good, Michie, and Timms [8] wrote a detailed account of this achievement in 1945. For present purposes the key sentence is:

> The fact that Tunny can be broken at all depends upon the fact that P, χ, Ψ', K and D have marked statistical, periodic or linguistic characteristics which distinguish them from random sequences of letters.

This report states elsewhere that the method involved, using logarithmic Bayesian "weights" and Turing's decibans, originated in the Naval Cryptology unit. Hugh Alexander in [1] leaves no doubt as to who was the dominant figure in work on Naval Enigma at Bletchley.

It is possible, but quite laborious, for anyone with appropriate skills to extract from [8] the substance of Turing's work on (Bayesian) probability being applied to cryptology. However, the recent declassification of his working paper [14] (circa August 1941) on the subject helps considerably. A useful commentary on this point has been written by Zabell [16].

Andrew Hodges records on page 243 of his well-known book [9] that, around December 1942, Gleason and Turing were eating in a Washington restaurant. They discussed:

> …statistical problems, such as that of how best to estimate the total number of taxicabs in a town, having seen a random selection of their licence numbers.

The theory needed for this "German tank" problem is Bayesian. One may speculate that this led to the initiative described by Ruggles and Brodie [10] in 1947:

> In early 1943 the Economic Warfare Division of the American Embassy in London started to analyse markings and serial numbers obtained from captured German equipment in order to obtain estimates of German war production and strength.

Ruggles and Brodie show that interest in this matter was developing in the United States independently of Turing. Gleason's role in this matter is not clear. In 1958–1960 I undertook the basic military training then commonly available for Australian boys aged fifteen to seventeen and was fascinated by the range of information engraved on the WW2 rifles used.

The statistician Edward Simpson was transferred to work on JN-25 at Bletchley Park in 1943. In 2010 he wrote an account [11] of this work, entitled *Bayes at Bletchley Park*. It explains the role of some of this material in decrypting Enigma traffic also.

The version of the Bayes Theorem needed for assessing whether a potential decryption should be accepted and also for Hall weights is as follows. Suppose that it is known that exactly one of the two hypotheses S and T is valid and independent runs are made of an experiment whose output is an element of a finite set K. It is known that, if S holds, then for $k \in K$ the probability of the outcome being k is σ_k, while if T holds the probability is τ_k. Suppose that the experiment is run $N = \sum_k n_k$ times with n_k occurrences of output k. Let p_0 denote the "prior" probability (before the experiments) that S holds. Likewise let p_N denote the "posterior" probability (after the results of the experiments are available) that S holds. Then

$$\log_\beta (p_N/(1-p_N)) = \log_\beta (p_0/(1-p_0)) + \sum_k n_k \log_\beta (\sigma_k/\tau_k)\,.$$

Here the logarithms can be taken to any convenient base $\beta > 1$. Once β is chosen, the $\log_\beta (\sigma_i/\tau_i)$ terms are known as "weights of evidence" or just "weights". Initially Turing advocated using logarithms to the base $\beta = \sqrt[10]{10}$ and named the dimensionless unit of weight the "deciban". These were rounded to the nearest half. Later Good pointed out that it was easier to take $\beta = \sqrt[20]{10}$ and so to work with the half deciban or "hdb". Another option is to take $\beta = \sqrt[100]{10}$ and thus use the "centiban". The lack of modern calculating devices at the time made some rounding of the logarithms essential.

In general it is clear from the formula that if p_0 is quite small, then quite a lot of strong evidence is needed to make p_N large enough so that S is highly likely.

Additive Ciphers. The JN-25 Systems

A description of the structure of the JN-25 cipher systems is needed in any explanation of the task faced by those trying to break them. The underlying algebraic structure of an abelian group $\mathcal{A}$ (here of order 100,000) and a subset S (here of order 33,334 and not invariant under all automorphisms of $\mathcal{A}$) is quite unorthodox.

The word "group" was used in the communications community in the sense of a string of letters or digits. These had a fixed standard length determined by the context. To avoid confusion, strings of 5 digits are here called 5-groups. The set $\mathcal{A}$ of 5-groups has an evident abelian group structure specified by what was then called "noncarrying" or "false" addition.

There is a natural way to use 5-groups as a reasonably secure communications system. A list of words and/or phrases intended for use is prepared. A different 5-group, the *code* 5-group, is allocated to each. A long random table (the "table of additives") of 50,000 (say) 5-groups is generated somehow and copied out on 500 serially

numbered pages with ten rows each of ten of these 5-groups on each page. (This note uses the word "random" loosely. All the underlying sample spaces are finite.) The message is written out in plain language on the first of four lines of a suitable form. The corresponding code 5-groups are written out on the line immediately below. A starting 5-group in the table of additives is randomly chosen. Consecutive 5-groups from the table beginning at the chosen 5-group are then written out on a third line, and the noncarrying sums ("code" + "additive") are then calculated and written on the fourth line. These were called GATs, or 5-Groups As Transmitted. The proposed recipient would need to be able to reverse this process and so needed to be able to recover the starting point. Information for this purpose was called the indicator or indicators and was sent as part of the message encoded, encrypted, or perhaps concealed among the GATs. Better still, two or all three of these methods of keeping the indicator secure would be superimposed.

The security of such a cipher system depends upon the indicators being unbreakable, the table of additives being replaced reasonably frequently, and the code book being replaced perhaps rather less often. The frequencies of occurrence of the common code 5-groups should be reduced by allocation of alternative code 5-groups to common words and/or phrases in use. Ideally there would be calculation of the maximum secure life of these systems. In practice, distribution of replacement cipher material presented problems. An army in retreat would sometimes allow its cryptographic material to be captured. Dice or suchlike were little used in the making of "random" choices, and so these choices were much less random than they should have been.

The allocation of code 5-groups is best done in a patternless or random way. The I.J.N. did not choose its JN-25 code 5-groups randomly but instead limited itself to *scannable* 5-groups. In the U.S.N. jargon of the day, a 5-group was said to be scannable if the sum of its digits was a multiple of three. The subset $\mathcal{S} \subset \mathcal{A}$ of scannable 5-groups has 33,334 elements. Simpson used the alternative phrase "divisible by three".

Initially we assume that the indicator system of the JN-25 cipher under attack can be decoded, decrypted, or located as may be necessary. (As this was the case in November 1943, the theory of Hall weights was just an "insurance policy" being kept in reserve.) It is then possible to have 1,000 large pieces of paper ("depth sheets") printed with fifty reasonably wide columns and perhaps thirty rows on each. This gives 50,000 columns, one for each 5-group in the table of additives. Intercepted messages can then be written out on a line with each GAT in the appropriate column. The task is now recovery of the additive involved.

The word "column" was sometimes replaced by "depth": the intercepted signals were then said to be "placed in depth". Confusingly, the word "depth" was also used for the number of different GATs in a column. A column would thus contain N distinct 5-groups $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_N$ where $\mathbf{x}_k = \mathbf{y}_k + \mathbf{a}$ and where $\mathbf{y}_k$ is scannable for $1 \le k \le N$ and $\mathbf{a}$ is an unknown 5-group. If d denotes the depth, then $N \le d$. Occasionally duplication (a "hit" or "click") occurred and then $N < d$.

A *potential decryption* is then any 5-group $\mathbf{b}$ such that $\mathbf{x}_k - \mathbf{b}$ is scannable for each k. Anachronistic large-scale random sampling shows that for various N (line 1 in the table below) the probability U_N that a column with N distinct GATs has a unique potential decryption, the average number A_N of potential decryptions, and the least number L_N such that 90% of samples have at most L_N potential decryptions are shown on lines two, three, and four respectively.

N	7	8	9	10	11	12	16	20
U_N	0%	0%	1%	3%	6%	11%	42%	68%
A_N	148	73.2	38.4	21.7	13.3	8.6	2.7	1.6
L_N	318	164	87	49	30	19	5	2

Hence only 68% of columns with twenty distinct GATs can be deciphered in isolation. However, what can be done in attacking a new JN-25 system is to examine those columns containing sixteen or more distinct GATs to identify which of these have unique decryptions. This gives provisional statistics on the frequency of occurrence of common code 5-groups to the cryptologists, who would have had some, admittedly imprecise, knowledge of the above table. Details on how to get started on a new JN-25 system are slurred over here. This phase would then work on the columns of greater depth to select potential decryptions $\mathbf{b}$ for which several of the "stripped" 5-groups $\mathbf{x}_i - \mathbf{b}$ are common.

Turing's 1941 exposition [14] on the use of probability theory in cryptanalysis compares the general task of finding the correct decryption to looking for a needle in a haystack. The limitation that all code 5-groups are scannable reduced the size of the haystack (if, for example, $N = 10$, the haystacks average 21.7 potential decryptions rather than 100,000) and so materially helped with the $\log_\beta (p_0/(1-p_0))$ term in the Bayes formula.

My paper [4] describes how, between August 1939 and February 1940, Turing and a few colleagues assisted in developing a method to discover potential decryptions of columns of smaller depth that contain common decrypted 5-groups $\mathbf{x}_i - \mathbf{b}$. In fact, there is another method which (usually) was more productive. Turing was involved in early 1940 in designing the first version of a special

purpose desk calculator for handling the search for potential decryptions. By December 1942 the U.S.N. had an elaborate powered version (the "fruit machine") being manufactured in Dayton, Ohio. The paper gives a contrived example of one use of such a device. The following text in a report (December 1942) was written by Turing and quoted in [4]:

> SUBTRACTOR MACHINE. At Dayton we also saw a machine for aiding one in the recovery of subtractor [5-]groups when messages have been set in depth. It enables one to set up all the cipher [5-]groups in a column of the material, and to add subtractor 5-groups to them all simultaneously. By having the digits coloured white, red or blue according to the remainders they leave on division by three it is possible to check quickly whether the resulting book [code] [5-]groups have digits adding up to a multiple of 3 as they should with the cipher to which they will apply it most. A rather similar machine was made by Letchworth for us in early 1940, and, although not nearly so convenient as this model, has been used quite a lot I believe.

The naval facility in Pensacola, Florida, has a display (small museum) which has one of these fruit machines. The words "I believe" here refer to work carried out in Singapore, later Manila, and later still elsewhere and so not readily accessible to Turing. Yet he was kept informed to some extent.

The admittedly minimal evidence of Turing's involvement is not restricted to this text. The senior cryptologist John Tiltman (1894–1982), heading the first team working on JN-25, did write up some reminiscences [13] for the internal use of the NSA. These include:

> I have no knowledge of higher mathematics and my grasp of probability is instinctive and quite unsound, but I am not too proud to ask for help and, when I have done so, have not often been misled.

Turing's report shows incidentally that the Bletchley Park mathematicians missed the use of colored background in speeding up the determination of divisibility by three. The aim is to arrange things so that the number of reds is congruent modulo 3 to the number of blues in each sum 5-group. This is somewhat reminiscent of the task of being given a graph drawn on a sphere with three edges meeting at each node, allocating a color (either red or blue) to each node so that the number of red nodes on the boundary of each face is congruent modulo 3 to the number of blue nodes. This task is a variant of the four-color theorem!

Photo by Joseph Maksin.

"Fruit machine" displayed in Pensacola, Florida.

Breaking a Cipher Piece by Piece

Turing's report [14] discusses in detail the breaking of a cipher piece by piece rather than attempting to get the full solution in one calculation. This is the strategy implicit in the device mentioned above. It uses pre-existing knowledge of the common code 5-groups. The cryptologist would attempt to recover the original code 5-groups by finding the additive for each column. The task of recovering the plain language corresponding to a given code 5-group would be carried out one by one.

Passing by the methods of finding reasonable potential decryptions, the question remains, when should a potential decryption of a column of depth $d = 10$ (say) be accepted? There was considerable urgency at the time. It was accepted that a (hopefully) modest proportion of decryptions would be wrong, but (hopefully) most of these would be corrected when further messages using that part of the additive table turned up. It seems that the clerical staff used simple *scoring systems* such as: "For depths of ten, accept any potential decryption that yields at least three points. Here a point is awarded for each of the one hundred most common code 5-groups appearing in the proposed decryption and for each piece of horizontal evidence obtained." In this reasoning the occasional duplicating GAT in a column is not disregarded but instead contributes to the calculated score.

A typical piece of "horizontal" evidence arises when the previous column has been decrypted with the common code 5-group 12345 being found. It is known that the common code 5-group 45678 often follows 12345 in signals. Hence a potential decryption in which 45678 occurs immediately to the right of 12345 is more likely to be correct.

One could argue that a better scoring system would award three points for any decrypted code 5-group in the most common twenty, two for any decrypted code group in the next twenty, one for common code 5-groups from forty-one to one hundred, and two for strong horizontal evidence. The word *weight* was used for a number of points in such a system. The threshold "at least three points" would then need adjustment. Any proposed scoring system for depths of (say) ten could be tested on the top ten GATs in columns with (say) sixteen or more GATs for which the correct decryption is known with high reliability.

Turing may well have sought rationality behind such scoring systems in 1940 and 1941, eventually producing the extremely important use ([11] and [14]) of Bayesian methods in cryptology. Of course any reconstruction of the thought processes that resulted in [14] is totally speculative. Quite independent work on sequential analysis was going on elsewhere. For example, Abraham Wald's 1945 paper [15] describes work carried out in 1943 and contains (page 121) the remarkable paragraph:

> Because of the substantial savings in the expected number of observations effected by the sequential probability ratio test, and because of the simplicity of this test in practical applications, the National Defense Research Committee considered these developments sufficiently useful for the war effort to make it desirable to keep these results out of the reach of the enemy, at least for a certain period of time. The author was, therefore, requested to submit his report in a restricted report which was dated September 1943. In this report the sequential probability ratio test is devised and its mathematical theory is developed.

The above discussion disregards the matter of getting started on a new JN-25 system. Here analysis of the initial traffic cannot be carried out piece by piece. One method is to accumulate depths which have unique decryptions and use them to get information on the common code 5-groups. It is in fact possible to use about seventy columns of depths at least thirteen to get an initial impression of what are the common code 5-groups. This depends upon the frequencies of occurrence being reasonably close to what happened historically. The details are not given here. Upgrading the statistics as more and more columns are decrypted must have been an essential part of the process.

Bayesian Methods in Decrypting JN-25 Columns

In this section K is the set of 33,334 scannable 5-groups. Hypothesis T is "the potential decryption is incorrect," and so the τ_k are all equal; indeed $\tau_k = 1/33334$ for all k. For the one hundred (or thereabouts) most frequently occurring code 5-groups k, the frequency σ_k is taken to be that obtained from decryptions already made. For other scannable 5-groups k the observed frequency would be a less reliable statistic. It was found easiest to just take $\sigma_k = 1/33334$ for such k: at least this avoided the need to calculate with negative weights.

General reference needs to be made to Edward Simpson's 2010 account [11] of work carried out at Bletchley Park in 1943–1945 decrypting columns of JN-25 with depths as low as six. In essence it used the above method of exploiting the available data.

The anonymous NARA archive RG0457, entry A1 9032, box 578, file 1391 of March 1945 gives information on the success in attacking various JN-25 systems. Code book B was used in conjunction with additive table 7 from August 1, 1941, to December 3, 1941, that is, in the four months leading up to the raid on the Pearl Harbor Naval and Air Force facilities. It is noted that this combination (JN-25B7) received quite heavy use. Joint work between the American naval unit "Cast" in the Philippines and the British unit FECB in Singapore managed to recover 35,761 additives out of 50,000. The report notes that some of the 35,761 would be incorrect. The combination JN-25B8 (December 4, 1941, to May 27, 1942) had been attacked by the unit at Hawaii as well, and so 47,340 additives had been recovered.

Hall Weights

The Hall weights originate in the observation that, if the *characteristic* $\chi(abcde)$ of the 5-group $abcde$ is defined to be $a+b+c+d+e$ interpreted modulo 10, then the proportions q_j of scannable 5-groups with characteristic j are far from equal. Indeed, careful calculation reveals that $q_9 = q_6 = 925/33334$, $q_2 = q_3 = 1780/33334$, $q_5 = q_0 = 3247/33334$, $q_8 = q_7 = 4840/33334$, $q_1 = q_4 = 5875/33334$. It is far from clear why Hall or anyone else thought that this was worth examining.

The real-valued function $j \mapsto q_j$ defined on the cyclic group of order 10 necessarily has a 10-term expansion in terms of sines and cosines. The functional equation $q_j = q_{5-j}$ implies that five of these terms are zero. Simple calculation yields the following, which is correct to five decimal places:

$$\begin{aligned} q_j \approx\ & .10000 - .00007\cos(2\pi j/5) \\ & - .00250\cos(4\pi j/5) - .00001\sin(\pi j/5) \\ & + .07808\sin(3\pi j/5). \end{aligned}$$

The approximate formula $q_j \approx .100 + .078\sin(3\pi j/5)$ is too attractive to be left out of this account.

Suppose d is reasonably large, say $d > 16$; $\mathbf{y}_k$, $1 \le k \le d$, are randomly chosen scannable 5-groups; and $\mathbf{a}$ is a randomly selected 5-group. Then the distribution of values of the $\chi(\mathbf{y}_k + \mathbf{a})$ may be calculated and expanded in terms of sines and cosines. The coefficients of $\cos(3\pi j/5)$ and $\sin(3\pi j/5)$ may then be used to indicate the most likely value(s) of $\chi(\mathbf{a})$. One can use a table of values of the inverse tangent function to assist in decryption!

The formula $\chi(\mathbf{x}+\mathbf{a}) - \chi(\mathbf{y}+\mathbf{a}) = \chi(\mathbf{x}) - \chi(\mathbf{y})$ motivates the calculation of the probability σ_k of the difference $\chi(\mathbf{x}) - \chi(\mathbf{y})$ being k as $\mathbf{x}$ and $\mathbf{y}$ vary over the $33,334^2$ possible pairs $(\mathbf{x}, \mathbf{y})$. These are rational numbers with denominator $33,334^2$ given as the sums $\sum_j q_j q_{k+j}$. The functional equation $\sigma_k = \sigma_{-k}$ is then implied by the earlier $q_n = q_{5-n}$. The values of σ_k are then given to six decimal places in the second column of either table below. In the previous notation S is the hypothesis that two intercepts are in alignment, while T is the hypothesis that they are not. The set K is now the set of ten digits and $\tau_k = 1/10$ for all k in the above logarithmic Bayes formula.

k= 0	0.130510	2.31288	2
1, 9	0.090556	-0.86162	-1
2, 8	0.075352	-2.45808	-2
3, 7	0.124667	1.91503	2
4, 6	0.109393	0.77980	1
5	0.069553	-3.15368	-3

The third column in this table gives the Hall weights $\log_\beta(10\sigma_k)$ in half decibans (so with $\beta = \sqrt[20]{10}$), while the fourth gives rounded values of these. These roundings lose quite a lot of precision.

k=0	0.130510	30.0009	30
1, 9	0.090556	-11.1762	-11
2, 8	0.075352	-31.8843	-32
3, 7	0.124667	24.8403	25
4, 6	0.109393	10.1148	10
5	0.069553	-40.9070	-41

In this table β is taken to be $\exp(3/338)$. The third column in the right-hand table gives instead $(338/3)\log(10\sigma_k)$, and the rounded values are given in the fourth column. Much less precision is lost. The choice $\beta = \exp(3/338)$ may be more aesthetic than historical.

Now suppose we are trying to test "the correctness of the relative setting of two messages using only the property of divisibility by three of the code 5-groups." So here the two messages are written out on successive lines of a form, one directly below the other. There are two hypotheses: S being that the relative setting is correct and T being that it is incorrect. If S holds, then the probability that $\chi((\mathbf{x}+\mathbf{a}) - (\mathbf{y}+\mathbf{a})) = \chi(\mathbf{x}) - \chi(\mathbf{y}) = k$ is σ_k, while otherwise—that is, if T holds—it is just $1/10$. At one stage in 1944 it was possible to work out the page part of the current JN-25 indicators but not the line or column part. Thus we now assume that the two messages which are being tested for correct alignment were encrypted starting on the same page of the table of additives. As there was a bias towards starting on the left half of the page and also a bias towards starting on the top half, the initial p_0 in the formula is about $2/100$ rather than $1/100$. Thus the logarithmic prior term is about $(338/3)\log((1/50)/(49/50)) \approx -438$, and so the Hall weight formula has the totally surprising Diophantine approximation

$$\begin{aligned}(338/3)\log(p_N/(1-p_N)) &\approx -438 + 30n_0 - 11(n_1+n_9) - 32(n_2+n_8)\\ &\quad + 25(n_3+n_7) + 10(n_4+n_6) - 41n_5.\end{aligned}$$

In practice the staff working with this formula would be given just a threshold, that is, a minimum acceptable value for the expression $30n_0 + \ldots - 41n_5$.

The initial deficit of -438 looks somewhat daunting, but the last paragraph glosses over the true situation. The aim is not to set two JN-25 messages in alignment, but rather at least six messages and hopefully at least seventeen if the decryption process is ever to get started. Another circumstance would be the discovery of two signals with "double hits", that is, the same pair of GATs occurring in each separated by the same number of other GATs. The Copperhead I device searched for double hits, which would make the "correctness of the relative setting" much more likely. This is not the place to develop a detailed account of the theory.

The operators handling JN-25 encryption in WW2 were instructed to *tail*, that is, to choose the starting point for the first signal in a new additive table randomly and then start each subsequent encryption immediately after the previous one finished. However, not all of them read the instructions. Once detected, this practice helped the cryptologists both with breaking indicator encryption systems and with getting long concatenations of intercepts to put in depth.

The reader seeking a challenge may wish to work out the appropriate modifications of these calculations if, instead of using only multiples of three, the I.J.N. had used only multiples of nine or multiples of eleven.

The Historical Significance

This note has avoided much historical detail about JN-25. For example, the 1945 report HW 43/34 on the system JN-25L53 in the British National Archives has over one hundred pages

and includes a glossary (of jargon). The authors were J. W. S. Cassels and E. H. Simpson. It has also slurred over the difference between Hall weights and the associated Shinn weights. However, much of the more important mathematical aspects are mentioned above.

The decryption and decoding of JN-25B in 1941–1942 undoubtedly turned around the naval war in the Pacific. Decryption of Enigma was extremely useful in the air battle over Britain and later in the Battle of the Atlantic. Also, the 1944 invasion of Normandy needed confirmation from high-level encrypted teleprinter traffic that the deception activities had in fact succeeded. Turing's work on Bayesian methods in cryptology permeated all of these activities.

Another well-known "insurance" discovery of the era did pay off handsomely. In February to April 1940 at Bletchley Park the talented mathematics student John Herivel developed a technique to recover likely settings of the Enigma encryption machine then used by the German Army and Air Force. This was not needed while an unsound indicator encryption practice was in use but came into its own in May 1940. The "bombe" device, designed by Turing and Gordon Welchman following an earlier Polish version, took over four months later. Meanwhile the Battle of Britain had to be fought.

The "insurance policy" of Hall weights became "useful" in 1944, and by then the U.S.N. had a massive preponderance on, under, and over the Pacific Ocean. Getting back into JN-25 without reading the indicators was very slow work. In general, JN-25 was much less productive as a source of intelligence in 1944–1945. However, Hall weights were an elegant method that did help in detecting alignments. Hall was justified in calling them a "significant contribution".

The Recordsearch facility of the National Archives of Australia may be used to locate and read online a report entitled *Japanese Naval Order of Battle* compiled in June 1944 by the Joint Intelligence Center Pacific Ocean Area, a predecessor of the NSA based in Hawaii. This document contains around ninety-five pages of information assembled by the center, mostly from intercepted radio communications.

Acknowledgment

This work depends much on a program of researching the communications intelligence aspects of the Pacific War jointly with John Mack.

References

[1] C. H. O'D. Alexander, *Cryptologic History of the German Naval Enigma*, British National Archives HW 25/7, GC&CS report, 1945.

[2] J. Burroughs, D. Lieberman, and J. Reeds, The secret life of Andrew Gleason, *Notices of the American Mathematical Society* **56** (November 2009), 1239–1243.

[3] C. Christensen, U.S. Naval cryptologic mathematicians during World War II, *Cryptologia* **35** (3) (2011), 267–276.

[4] Peter Donovan, The flaw in the JN-25 series of ciphers, *Cryptologia* **28** (4) (2004), 325–340.

[5] Peter Duren, Richard Askey, and Uta Merzbach, *A Century of Mathematics in America*, Vol. 1, American Mathematical Society, Providence, RI, 1989.

[6] I. Jack Good, A. M. Turing's statistical work in World War II, *Biometrika* **66** (1979), no. 2, 393–396.

[7] ———, Turing's anticipation of empirical Bayes in connection with the cryptanalysis of the naval Enigma, *Journal of Statistical Computation and Stimulation* **66** (2) (2000), 101–111.

[8] I. Jack Good, Donald Michie, and Geoffrey Timms, *General Report on Tunny*, British National Archives HW 25/4, GC&CS report, 1945.

[9] Andrew Hodges, *Alan Turing: The Enigma*, Burnett, 1983.

[10] Richard Ruggles and H. Brodie, An empirical approach to economic intelligence in WW2, *Journal of the American Statistical Association* **42** (March 1947), 72–91.

[11] Edward Simpson, Bayes at Bletchley Park, *Significance* **7** (2) (2010), 76–80.

[12] ———, *History of the Fleet General Purpose System (JN-25) Cryptographic Party*, British National Archives HW 8/149, GC&CS report, 1945.

[13] John Tiltman, *Reminiscences*, N.A.R.A. RG0457, entry A1 9032, box 1417, file 4632.

[14] Alan Turing, *The Applications of Probability to Cryptology*, British National Archives HW 25/37, GC&CS report, 1941.

[15] Abraham Wald, Sequential tests of statistical hypotheses, *Annals of Mathematical Statistics* **16** (2) (1945), 117–186.

[16] S. Zabell, Commentary on Alan M. Turing: The applications of probability to cryptography, *Cryptologia* **36** (3) (2012), 191–214.