TOP SECRET

19 April 1945

ENIGMA WIRING RECOVERY FROM THE READING OF A DEPTH

1.1 Statement of the Problem. Suppose that a depth of from 15 to 20 messages (extending for 104 letters say) has been enciphered on an enigma machine. Suppose further that statistical tests on the cipher text have indicated enigma type encipherment, and that past experience with enemy plain text has enabled the solution of the depth by cribbing. Then a method for cryptanalytically obtaining the input sequence, the wiring of some or all of the moving wheels, the notch patterns on some or all of the wheels, and the wiring of the reflector is certainly desired. This paper discusses a method for obtaining some of these desired items.

1.2 Past Experience of U. S. Navy Units with this type of Problem. For the most part, U. S. Navy units have had little or no experience with actual enigma wiring recoveries. In the late thirties, the U. S. Coast Guard cryptanalytic unit recovered the wiring from an 80 odd message depth of quite some length. This wiring was found to be the same as that in the old commercial enigma machine. A write-up of their work, entitled "Swiss Navy Maneuvers" is in the Navy general cryptographic library. However, present techniques are so much more powerful than those used by the Coast Guard that a new and more complete write-up seems desirable. From time to time the Swiss have rewired their wheels, and the U. S. Army has recovered a new wiring from a long crib. Several types of enigma machines have been used by the German Agent System, and the Spaniards are known to have used two different enigma wirings. For the most part, the wirings of these machines were recovered by the British cryptographic unit and sent to those interested in the U. S. (The Coast Guard and the Minor European Section in the U. S. Navy cryptanalytic unit.) Most of these wirings were recovered with twists and reletterings. The presence of these is a necessary evil to the method of cryptanalytic recovery; a separate paper "On The Elimination Of 'Twists' in Wired Wheels", dated 2 January 1945, has been prepared, giving a procedure for removing twists and reletterings when additional information is available to the cryptanalyst.

1.3 Preparation Expected of the Reader. A general familiarity with enigma machine terminology is expected of the reader. In addition, the idea of a molecular structure or "menu" showing the relation between the 26 (or fewer) letters of the alphabet

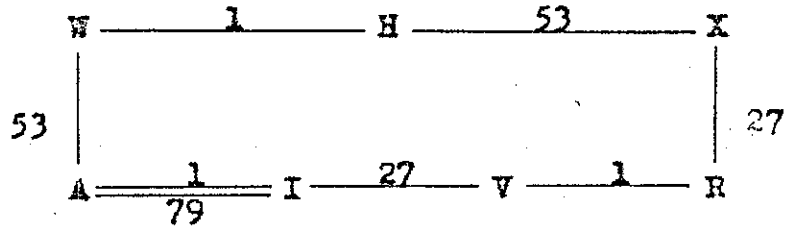
will be used in this report. This is merely a pictorial representation of a number of plain-text cipher-text alphabetic pairings. Finally, a group-theoretic approach to the enigma encipherments will be used. This is a fairly sophisticated mathematical tool, but to a mathematician, at least, the group theory structure shows the way to a quicker solution of the problem. However, the necessary mathematical explanations will be given in the body of the report to enable non-mathematical readers to follow the argument.

2.1 Encipherment and Solution of the Depth. In the summer of 1944 a new type of enigma machine, marked "T" by the manufacturers, was captured in a warehouse in Normandy where some of the machines were awaiting shipment to the Japanese. The machine was very similar to the old three-wheel one-movable-reflector commercial machine, except that it had a different input sequence and that there were eight wheels from which to choose the three wheels. Also each wheel had five notches instead of the single notch on the commercial wheels. It seemed desirable to study this new machine, since cryptographic personnel familiar with the Japanese systems were unfamiliar with the enigma machine. A set of English naval text messages in depth were enciphered on the T machine. Later this cipher text and the fact that the underlying text was English naval text was given to a group of cryptanalysts. For the purposes of this report, a depth of 20 will be used. Actually the messages can be read for depths less than 20, but the recovery of the wiring in these cases is a very tiresome procedure. The depth was read, and yielded the tabulated information. Only a partial tabulation of the recovered alphabets is given herewith.

2.2 Alphabetic Recoveries From Depth of 20.

Position Number	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	I	M	G	Q		K	C	W	A	S	F		B			U	D	V	J		P	R	H			
2	Z				Q	I		T	F		O			R	K	X	E	N		H				P		A
3	I	T	Y	J	O	M	U		A	D			F	S	E			V	N	B	G	R			C	
4	B	A	O		W	H		F	P	U			T	R	C	I		N		M	J		E			
5	Q	V		E	D	O	J	M	L	G		I	H	W	F	Y	A	T		R		B	N		P	
27	C		A		J	L	U	N	V	E		F		H			T	X	Y	Q	G	I		R	S	
28	G	E	S	X	B		A		R			Z			U			I	C	V	O	T	Y	D	W	L
29			O	U	T	N		L	J	I		H	R	F	C	S		M	P	E	D		Y		W	
30	C	O	A	T	L	Q	U		V			E	S	W	B		F		N	D	G	I	N		Z	Y
31	T	F	O			B	U	I	H			V		R	C	X	S	N	Q	A	G	L		P		
53	W			T	Y	O		X	S	N			Z	J	F				I	D			A	H	E	M
54	R	T		Y	W	U			N	P		O	V	I	L	J	S	A	Q	B	F	M	E		D	
55	F		I		N	A	X		C			Z		E	V	R		P	Y	W		O	T	G	S	L
56	O				J	I		S	F	E	Y			U	A			T	H	R	N				K	
57	T	O	R		J	U	N			E	S		X	G	B			C	K	A	F			M		
79	I	T	R	S	K				A	P	E	V		Z	Q	J	O	C	D	B		L				N
80	Q	G	M	K	O	R	B		S		D		C	T	E	U	A	F	I	N	P					
81	K		T	O	Z	G	F	P	U		A			S	D	H	Y	V	N	C	I	R			Q	E
82	Q			S	O		Y		L		R	I	P	V	E	M	A	K	D	U	T	N			G	
83	W		S	V	Z	T	X		J	I	R		O		M	Y		K	C	F		D	A	G	P	R

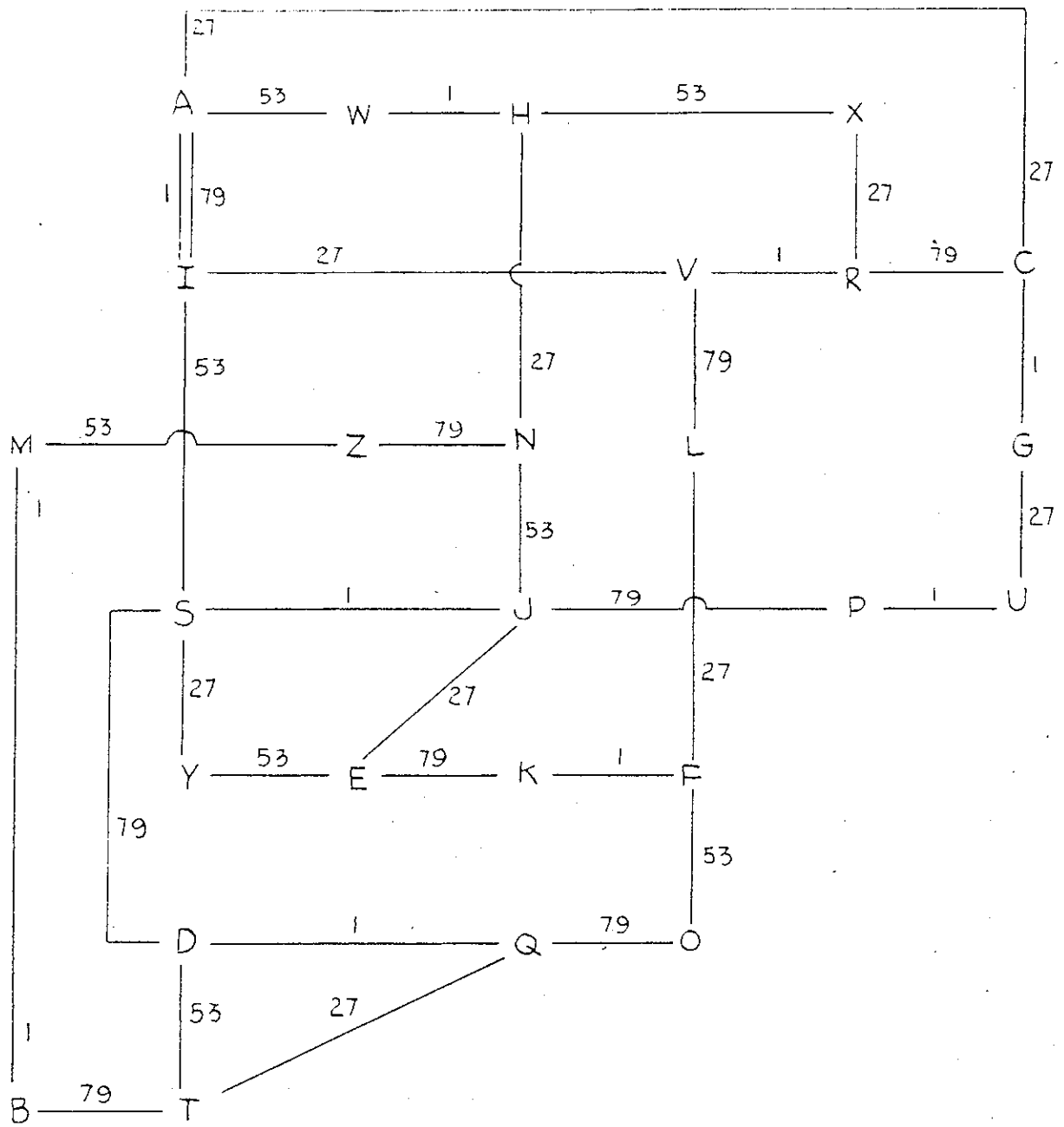
2.3 Structure of Molecules. Consider alphabets 1, 27, 53 and 79. The fast wheel of the enigma machine is in the same position for each of these enciphering positions. But the remainder of the machine, called the combined reflector, is in different relative positions for each of these enciphering positions. For position #1, there are 13 combined reflector links of which only 9 have been recovered. For position #27, there is another set of 13 links of which only 9 have been recovered. Similar statements hold for the other enciphering positions. A partial structure for the combined molecule for positions 1, 27, 53 and 79 can be built up as follows: W is linked to H by alphabet #1, H is linked to X by alphabet #53, X to R by #27, R to V by #1, V to I by #27, I to A by both #1 and #79, and A to W by #53. This gives a closure, as pictured below:



If all the available links are used, the molecule is much larger, and may use all 26 letters. Four molecules or menus have been built up from the data of 2.2.

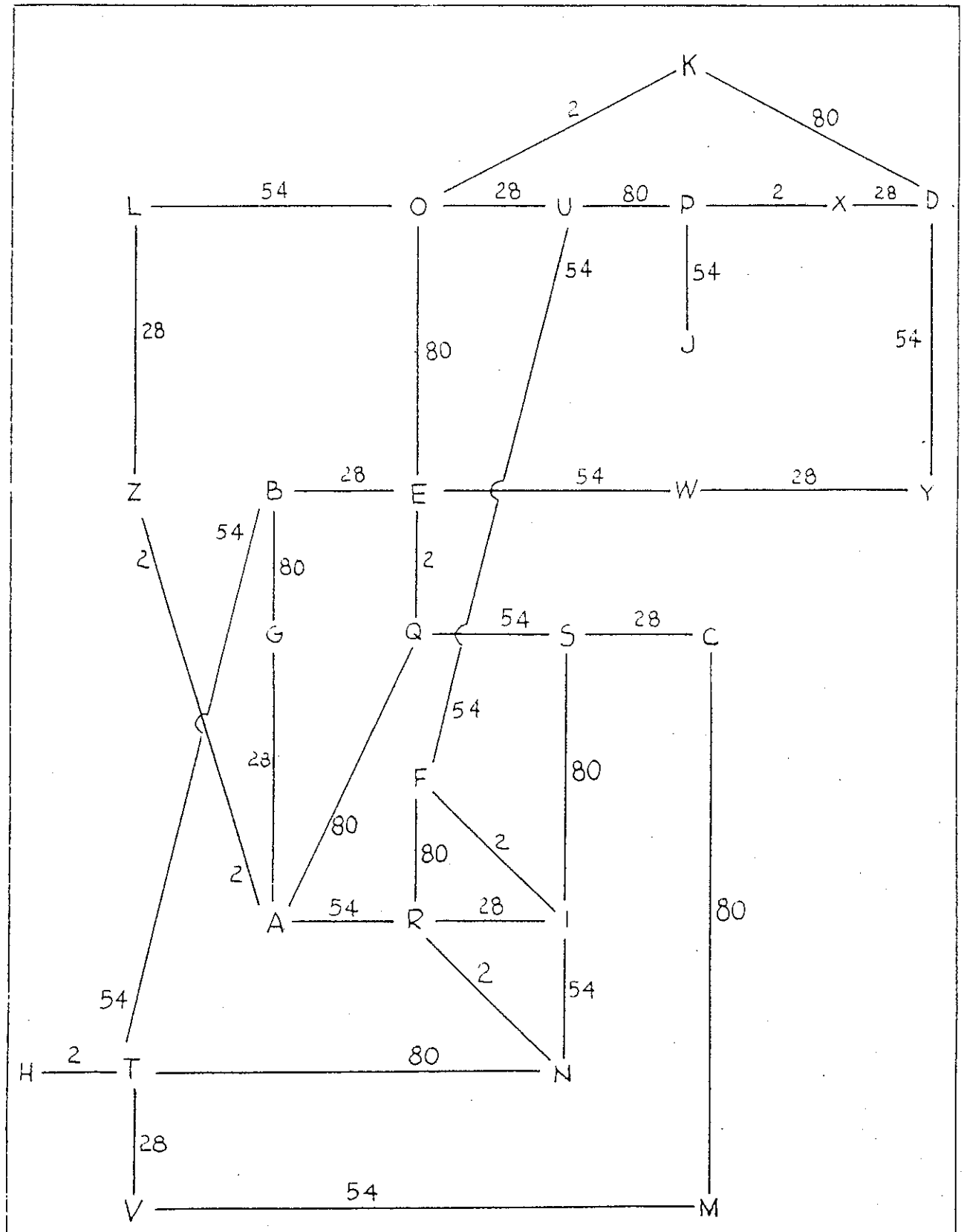
Menu #1	uses	alphabets	1, 27, 53, 79
Menu #2	"	"	2, 28, 54, 80
Menu #3	"	"	3, 29, 55, 81
Menu #4	"	"	4, 30, 56, 82

The reader who is an experimenter at heart will build up Menu #5 from alphabets 5, 31, 57, and 83.



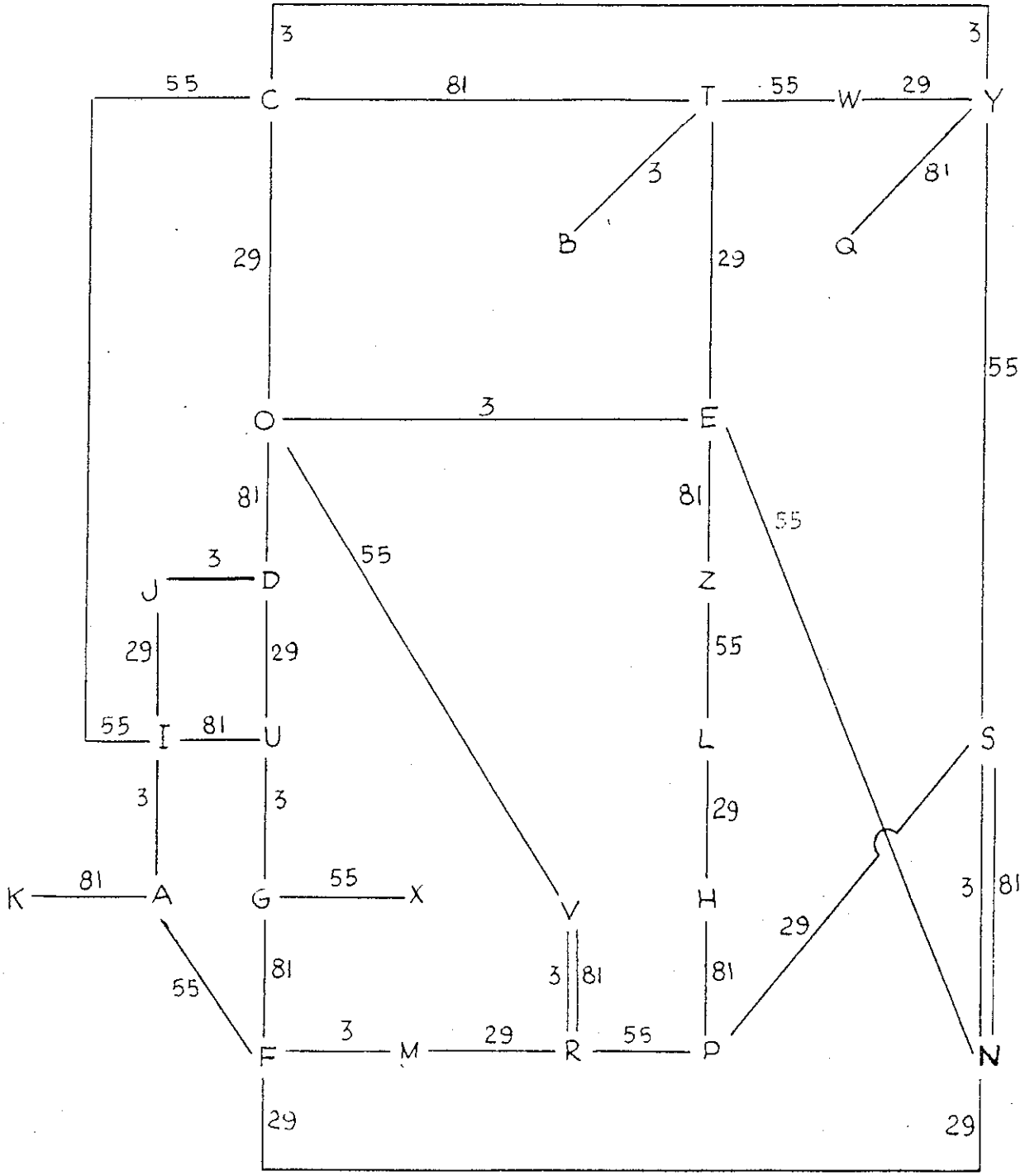
MENU #1

TOP SECRET



MENU #2

~~TOP SECRET~~



MENU #3

~~TOP SECRET~~

2.4 Combinations of Menus. If there is no turnover between alphabets 1 and 2, then there will be no simple turnover between 27 and 28, 53 and 54, and 79 and 80. If there is no notch on the fast wheel for the interval between alphabets 26 and 27, then there can be no double turnover at any of the above positions. Remark - a double turnover must be preceeded by a single turnover in an enigma (non-cyclometric) stepping machine. Assuming no turnover for the moment, what effect will there be on menus #1 and #2? Since the fast wheel is in the same position for each letter on menu #1, and since we are assuming the same internal combined reflector links for 1 and 2, 27 and 28, 53 and 54, and 79 and 80, and since the fast wheel is in the same position for each letter on menu #2, the only difference between menus #1 and #2 is a difference in the identity of the letters. In other words, the molecular structure or linkage structure must be the same for menus #1 and #2. Conversely, if the menus #1 and #2 do not have the same linkage structure (or are not isomorphic to use a mathematical term), there must have been a turn between 1 and 2, or 27 and 28, or 53 and 54, or 79 and 80, or perhaps badly garbled cipher text, or improperly decrypted plain text. In the case of corrupted text, efforts can be made to improve the text. In the case of a turn between enciphering alphabets 1 and 2, one would examine menus #2 and #3, or menus #3 and #4, etc.

Of course if there is no notch to cause a turn between enciphering positions 1 and 2, and also between 2 and 3, and if no double turnovers occur, then menus #1, #2 and #3 should all be isomorphic. Now in menu #1 there is a pair of letters connected by a double bond:

$$A \overset{1}{=\!=} I$$
$$79$$

This means that A enciphers to I in both alphabets 1 and 79. Hence it must be possible to place double bonds in menus #2 and #3 if all three menus are isomorphic. Due to incomplete alphabetic recoveries, a double bond is not present in menu #2, but there are certainly possibilities for the double bond. In menu #3 there are two double bonds, given by

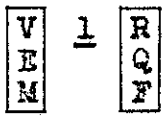
$$V \overset{3}{=\!=} R \qquad \text{and} \qquad N \overset{3}{=\!=} S$$
$$81 \qquad\qquad 81$$

Hence if menus #1, #2, and #3 are isomorphic, all menus must contain at least two double bond structures similar to the above. If only two are possible, then the double bond already found in menu #1 must correspond to one of the two above in menu #3.

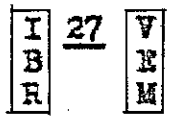
supposed isomorphism between menus #1, #2, and #3. Indeed, the data from menus #2 and #3 can be entered on menu #1, as is shown on the combined menu sheet. On this sheet, a block of four deep is provided for each of the 26 positions.

1 2 3 4	An entry in the top or space marked 1 is from menu #1, one from the second or 2 space is from menu #2, etc.

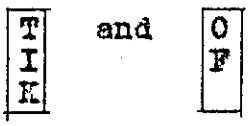
Solid lines connecting the 26 blocks are those which appear on menu #1. A line marked 1, such as



is to be interpreted as meaning that V—1—R, E—2—Q, M—3—F. And a line marked 27, such as

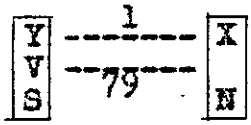


is to be interpreted as meaning that I—27—V, B—28—E, R—29—M. Now all of these alphabetic recoveries were already known, but consider



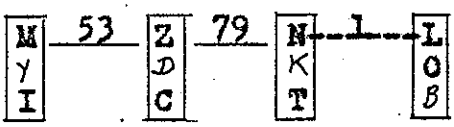
These are not connected by a solid line, but in menu #2, there is a connection I—2—F. Hence, assuming the correctness of our placements, T—1—O is required, and a line may be drawn connecting these blocks. Such lines not present in menu #1, will be drawn as dotted lines.

In addition, a double bond may be drawn between the blocks



since S—3—N is a part of our original data on menu #3. Because of the complexity of drawing all lines on the combined menu chart, these two connections have not been shown.

Also, C—3—Y gives Z—#1—E. If now these values are entered into the alphabetic recovery table, there are only two values in alphabet 1 not used. These two must be connected, that is N—1—L is also required and this line is drawn on the combined menu sheet as a dotted line. Indeed, from



we may fill in the inked values as shown.

The filling in of the remaining values may be done in several ways. A search may be made for other missing links (no pun

intended) which are implied but have not been entered on the combined menu. The placement of these links and their consequences will place other letters in the combined menu. Or a second method consists in selecting a letter in either menu #2 or #3 which has not been placed and trying this letter in turn in each of the vacant positions in the combined menu. Perhaps all but one of the positions will lead to contradictions. A third method is based on the cyclic structure. This will be discussed later, but it can be stated here that the cyclic structure of the isomorphism from menu #1 to #2 must be the same as that from menu #2 to #3. If a cycle of 5 is recovered in one isomorphism, there must be a cycle of 5 in the other. This device is useful near the end of the isomorphism recovery, and is quite helpful when there may be a missing letter in one or more menus.

By certain processes, generally devious rather than straightforward, all letters can be placed and the complete isomorphism between menus #1, #2 and #3 can then be established. The careful reader will work out the complete isomorphism, which can be checked against the one given later in section 3.3. He may also try to place menu #4 and menu #5 in the chart above. Menu #4 can be placed, but menu #5 can not be placed. This fact, when established, would suggest that there has been a turn in the position of the middle wheel between enciphering positions 4 and 5.

2.5 General Remarks on Menu Matching. If complete alphabets are given at the start, then a menu based on four enciphering alphabets will be rather hard to draw up neatly (due to the multiplicity of links involved) and will have available far more information than is needed to solve the problem.

If the depth is only 17 deep, instead of 20, the alphabets will probably not be as complete as they are for our example, and it will be a much harder job to match the menus. The technique is the same, but the work required to exhaust all the wrong cases is considerably increased.

If the depth is only 12 or 14 deep, it would be advisable to bring in, if possible, alphabetic recoveries from alphabets 105, 106, 107, 108, etc.

The reader may wonder why so much is left to the reader. A book on swimming strokes may be nice to read, but one must practice the strokes while actually in the water before one can claim to be a swimmer. So if the reader desires to actually possess the knowledge for recovering wiring from a depth, let the reader get his paper and pencils, using perhaps four colors to avoid confusion in the connecting links, and go to work.

A word or two about the Coast Guard recovery job may be in order. For the single notch wheels which they used, and for the 80 odd depth, it would be possible to establish isomorphisms between 26 (or perhaps only 25) menus, each menu being built up from almost complete alphabets. But the Coast Guard in those early days relied on double bond structures for the most part, and so in effect used only a small part of their available data. The present method, of course, is much more powerful since it can be used on a much smaller amount of data.

3.1 Group Theory Notation. Consider the group of alphabetic substitutions, and let capital letters denote the operation which effects the alphabetic substitution, and let small letters denote the 26 letters of the alphabet. Then if A_1 is substitution alphabet 1 of the recovery, it can be seen that

$$\begin{Bmatrix} a \\ b \\ c \\ . \\ . \\ \text{etc} \end{Bmatrix} \cdot A_1 = \begin{Bmatrix} i \\ m \\ g \\ . \\ . \\ \text{etc} \end{Bmatrix}$$

where 26 equations are involved in the above symbolic equation, such as $a \cdot A_1 = i$, $b \cdot A_1 = m$, $c \cdot A_1 = g$, etc. Since each alphabet is reciprocal, $a \cdot A_1 \cdot A_1 = a$, $b \cdot A_1 \cdot A_1 = b$, etc, or $A_1 = A_1^{-1}$, using the standard notation for the inverse operation. All enigma enciphering alphabets are reciprocal, so that all symbolic operations representing such substitutions must be their own inverses.

However, the operation A_1 can be regarded as the product of simpler operations. For the purposes of this report, certain simplifying assumptions will be made as to the nature of the enigma encipherment. The process of encipherment may be thought of as consisting of the five steps described below:

1. The operation of "steckering" the input letter. This will be represented by the symbol S. Some enigma machines with a built in input sequence have a constant stecker, others have a pluggable stecker which can be varied by the enciphering clerk. This operation is the same for all positions of encipherment.

2. The operation occuring when the steckered input letter goes through the fast wheel. This operation will be the same for alphabets 1, 27, 53, 79, etc. A different operation will be in effect for alphabets 2, 28, 54, and 80. Later

posite menu. Thus R_1 is the operator for step 3 for alphabets 1, 2, 3 and 4.

To determine the effect of the fast wheel at position 2, it is convenient to introduce another operator, the Caesar substitution operator. Let C be operation which carries a into b, b into c, etc. Then, due to the movement of the fast wheel through one position, the effect of the fast wheel at position 2 is given by

$$C\ W\ C^{-1}$$

The reader unfamiliar with group theory will undoubtedly desire to check this statement by actually tracing the path on a paper model of an enigma machine and comparing with the substitutions involved above. At the same time, it would be well to check the statement that

$$C^2\ W\ C^{-2}$$

gives the substitution from one side of the fast wheel to the other side when the wheel is two positions ahead of the basic position for which W is the operator. In the reverse direction, the operators will be the inverses of these just determined. Due to a general theorem

$$(ABC)^{-1} = C^{-1}B^{-1}A^{-1}$$

so that the operators for step 4 are easily determined from those in step #2.

Collecting all of this information (and drawing on our intuition for details stated but not proved and used but not stated), there results the following equations for the first four enciphering alphabets

$$\begin{aligned} A_1 &= S\ W\ R_1\ W^{-1}\ S^{-1} \\ A_2 &= S\ C\ W\ C^{-1}\ R_1\ C\ W^{-1}\ C^{-1}\ S^{-1} \\ A_3 &= S\ C^2\ W\ C^{-2}\ R_1\ C^2\ W^{-1} C^{-2}\ S^{-1} \\ A_4 &= S\ C^3\ W\ C^{-3}\ R_1\ C^3\ W^{-1}\ C^{-3}\ S^{-1} \end{aligned}$$

A similar set, but with a different reflector combination and hence a different operator symbol, say R_2, holds for A_{27}, A_{28}, A_{29} and A_{30}.

$$\begin{aligned} A_{27} &= S\ W\ R_2 W^{-1}\ S^{-1} \\ A_{28} &= S\ C\ W\ C^{-1}\ R_2\ C\ W^{-1}\ C^{-1}\ S^{-1} \\ A_{29} &= S\ C^2\ W\ C^{-2}\ R_2\ C^2\ W^{-1}\ C^{-2}\ S^{-1} \\ A_{30} &= S\ C^3\ W\ C^{-3}\ R_2\ C^3\ W^{-1}\ C^{-3}\ S^{-1} \end{aligned}$$

Also, other equations hold for A_{53}, A_{54}, A_{55}, and A_{56}, and for A_{79}, A_{80}, A_{81}, and A_{82}, with other reflector operators R_3 and R_4.

Now the single equation

$$A_2 = T_1^{-1} A_1 T_1$$

where A_2 and A_1 are known is not sufficient to determine T_1 uniquely. Indeed, where A_1 and A_2 consists of 13 pairs of substitutions, the number of possible values of T_1 is given by

$$26!! = 2^{13}\ 13!$$

an extremely large number of solutions.

However, T_1 must also be a solution of other equations, indeed

$$\begin{aligned} A_2 &= T_1^{-1} A_1 T_1 \\ A_{28} &= T_1^{-1} A_{27} T_1 \\ A_{54} &= T_1^{-1} A_{53} T_1 \\ A_{80} &= T_1^{-1} A_{79} T_1 \end{aligned}$$

With all of these restrictions on T_1, in general only one value of T_1 is possible, that is a unique solution to the four equations above is obtainable.

Assuming unique recovery of the T's, we can proceed to the next step. We may write

$$\begin{aligned} T_2 &= S\ C\ W\ C^{-1}C^{2}W^{-1}C^{-2}S^{-1} \\ &= S\ C\ S^{-1}\ (S\ W\ C\ W^{-1}C^{-1}S^{-1})\ S\ C^{-1}S^{-1} \\ &= (S\ C\ S^{-1})\ T_1\ (S\ C^{-1}S^{-1}) \\ &= (S\ C^{-1}S^{-1})^{-1}\ T_1\ (S\ C^{-1}S^{-1}) \end{aligned}$$

$$\begin{aligned} T_3 &= S\ C\ S^{-1}\ (S\ C\ W\ C^{-1}C^{2}W^{-1}C^{-2}S^{-1})\ S\ C^{-1}S^{-1} \\ &= (S\ C^{-1}S^{-1})^{-1}\ T_2\ (S\ C^{-1}S^{-1}) \end{aligned}$$

Thus T_2 is the same transform of T_1 that T_3 is of T_2. Now the number of solutions of

$$T_2 = (S\ C^{-1}S^{-1})^{-1}\ T_1\ (S\ C^{-1}S^{-1})$$

where T_1 and T_2 are known depends on the structure of the substitutions T_1 and T_2.

But if $(S\ C^{-1}S^{-1})$ is required to also be a solution of

$$T_3 = (S\ C^{-1}S^{-1})^{-1}\ T_2\ (S\ C^{-1}S^{-1})$$

there may be only one common solution to both sets of solutions, or a unique solution for $(S\ C^{-1}S^{-1})$. An added restriction on $(S\ C^{-1}S^{-1})$ is the fact that the substitution cycle for this operator (which is a transform of C^{-1} by S^{-1}) must have the same type of substitution cycle as C. Now C has a 26-cycle, hence $(S\ C^{-1}S^{-1})$ must also have a 26-cycle. If these two

$A_2 = T_1^{-1} A_1 T_1$ $\quad A_3 = T_2^{-1} A_2 T_2$ $\quad A_4 = T_3^{-1} A_3 T_3$

$A_{28} = T_1^{-1} A_{27} T_1$ $\quad A_{29} = T_2^{-1} A_{28} T_2$ $\quad A_{30} = T_3^{-1} A_{29} T_3$

$A_{54} = T_1^{-1} A_{53} T_1$ $\quad A_{55} = T_2^{-1} A_{54} T_2$ $\quad A_{56} = T_3^{-1} A_{55} T_3$

$A_{80} = T_1^{-1} A_{79} T_1$ $\quad A_{81} = T_2^{-1} A_{80} T_2$ $\quad A_{82} = T_3^{-1} A_{81} T_3$

If we had had only one equation in each set, unique solutions would have been impossible. If we had had only two equations in each set and full recoveries for all enciphering alphabets, there might have been unique solutions for T_1, T_2, and T_3. Actually, of course, we solved the system above with only two sets of four equations, and found T_1 and T_2. But to proceed from the equation,

$$T_2 = (S\ C^{-1} S^{-1})^{-1}\ T_1\ (S\ C^{-1} S^{-1})$$

to the solution of $S\ C^{-1} S^{-1}$ we have seen that we can not expect a unique solution. So we have gone back and added a fourth menu and another equation

$$T_3 = (S\ C^{-1} S^{-1})^{-1}\ T_2\ (S\ C^{-1} S^{-1})$$

to our working stock.

Indeed, using only one of the above equations to solve for $(S\ C^{-1} S^{-1})$ there are $(3!) \cdot 4^3 \cdot 2 \cdot 5 \cdot 7$ solutions. Fortunately, these two sets of $(3!) \cdot 4^3 \cdot 2 \cdot 5 \cdot 7$ solutions contain only one solution in common, hence a unique solution for $S\ C^{-1} S^{-1}$ results.

Now if T_2, is a transform of T_1, then a two cycle in T_2 must be paired with a two cycle in T_1. Start with the letter r in T_1. If we match r in T_1 with u in T_2, then we must also be able to match r in T_2 with u in T_3. But r in T_2 occurs in a four-cycle, and u in T_3 occurs in a five-cycle. Hence r in T_1 cannot be matched to u in T_2, and must be matched to z in T_2. Note that r in T_2 can be matched with z in T_3, since both these letters occur in four-cycles. If the pairings of r in T_2 with z in T_3 is established, the pairings x and d, o and r and b and g are also established. By continuing this procedure, the following cycle structure for $(S\ C^{-1} S^{-1})$ can be built up:

(e j c m n p f x d t s v w l b g i a y h q u o r z k)

There are 26 possible values of S in the solution of

$$P = S\ C^{-1}\ S^{-1}$$

where P is the above recovered operation whose cycle structure is the given 26-cycle, and where C^{-1} is the substitution $a \rightarrow z$, $b \rightarrow a$, $c \rightarrow b$, ---etc, which is also a 26-cycle. One value of S is the substitution which takes k into a, z into b, r into c, -----etc. Another value of S is the substitution which takes z into a, r into b, o into c, u into d, q int

Again, there are 26 possible starting points for the placement of the cycle for $W\ C\ W^{-1}$ under the normal alphabet.

Notice that there are two kinds of ambiguities in our specification for the wiring of the fast wheel. First, it was specified that W was the wiring in effect for the encipherment at positions 1, 27, 53 and 79. It would be just as logical to take positions 2, 28, 54 and 80. This choice of a position for W amounts to a relettering of the fast wheel. The second ambiguity results from the placement of the cycle for $W\ C\ W^{-1}$, and this operation is known as a twist. If one thinks of a wired wheel, a twist is a rotation of one side of the wheel relative to the other side, with the concept of elastic wires which will stretch to or contract down to the new positions. In general, twists and relettarings are not removable without additional information.

There are other methods for recovering the wiring of the fast wheel. Perhaps the following method will appeal to the experimenter. A paper strip model should be at hand for this approach. Assume one connection, or one wire. This amounts to the assumption of placing the sequence for $W\ C\ W^{-1}$ under a fixed point on the normal alphabet sequence. Assume, for example, a connection from A to A in wheel W. Then from A on the output side we can work back to K on the input sequence, when the wheel is in position 1. Now in position 2, the contact point A on the output side must be connected to the letter in menu #2 which is isomorphic to K in menu #1. This letter is C. So a connection must be drawn which connects A on the output side to the letter C on the input sequence while the strip is in position 2. This procedure can be followed through to give all the wiring specifications, or substitutions, necessary for wheel W.

4.2 General Remarks. After the stecker or input sequence and the fast wheel have been recovered, we can proceed to other steps. First, perhaps, would be the recovery of the notches on the fast wheel. The data given in this paper suggests a notch between positions 4 and 5, but since other data is lacking (alphabets 6, 7, 8,---etc.) we shall not recover the notch pattern.

To recover the wiring of the middle wheel, one procedure would be to remove the effect of the input sequence and the fast wheel. By grouping those alphabets for which there has been no turn on the middle wheel, it should be possible to obtain nearly complete alphabets for this stage. Also, the input sequence is now known, so that the group theory equations are simpler. This of course means that the recovery of the middle wheel is easier to carry out. Due to lack of data, this process will not be carried out in this report. This process involves a search for $W_2\ C\ W_2^{-1}$, much the same as the previous

search for $W_2 C W_2^{-1}$, where W_2 is the substitution operator for the middle wheel.

As long as there are moving elements with several different positions, the wiring can be recovered. But if the slow wheel and the reflector do not move, only their combined effect can be determined. For the reflector, the wiring must be reciprocal. So this condition cuts down greatly the number of possible positions for placing the reflector sequence under a normal alphabet. Since reciprocity and its use in eliminating some of the answers has been mentioned, it might be noted that in some usages the input sequence operation S is known to involve ten reciprocal pairs and six identity substitutions. So if this information is available, S can generally be uniquely determined.

The recovery of wiring from a depth can be a very interesting problem. Let the reader surround himself with pleasant working conditions and try it.

Robert E. Greenwood
Andrew M. Gleason
Agnes H. Clifford.
E. A. Hanson

etc. Thus the 26 values of S correspond to the 26 points at which the above sequence can be matched against the reversed normal alphabet. These 26 values of S cannot be reduced further without additional information. Indeed, this is one of the ambiguities resulting from cryptanalytic recovery.

4.1 Recovery of the Fast Wheel Wiring. If any one of the 26 possible substitutions S be used, the wiring of the fast wheel can be recovered from the equation

$$T_1 = S\ W\ C\ W^{-1} C^{-1} S^{-1}$$

since T_1 and C are known. Indeed,

$$W\ C\ W^{-1} = S^{-1}\ T_1\ S\ C$$

For convenience, choose one operational substitution S, the substitution which takes k into a, x into b, r into e, ---etc.

Let S, T_1, and C be represented pictorially as shown below:

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
	↓	↓	↓									↓	↓	↓	↓									↓	↓	↓
S	i	l	x	r	z	t	k	g	j	y	a	m	w	v	d	u	f	c	p	q	e	o	n	s	h	b
T_1	g	s	a	n	m	u	z	p	b	h	c	o	y	k	f	w	r	q	t	i	l	e	x	j	v	d
C	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a

Hence $S^{-1}\ T_1\ S\ C$ can be built up from equations such as

$$\begin{Bmatrix} a \\ b \end{Bmatrix} S^{-1} T_1 S\ C = \begin{Bmatrix} k \\ z \end{Bmatrix} T_1 S\ C = \begin{Bmatrix} c \\ d \end{Bmatrix} S\ C = \begin{Bmatrix} x \\ r \end{Bmatrix} C = \begin{Bmatrix} y \\ s \end{Bmatrix}$$

to give

WCW^{-1}	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
	↓	↓	↓									↓	↓	↓	↓									↓	↓	↓
	y	s	g	u	n	d	v	p	l	m	c	q	e	t	a	r	k	w	z	f	o	b	i	j	h	x

Written in the form of a cycle, there results

$W\ C\ W^{-1}$ (a y h p r w i l q k c g v b s z x j m e n t f d u o)

The reader should verify that if W is the substitution of the fast wheel, the cycle for $W\ C\ W^{-1}$ is the left hand sequence on the fast wheel in a paper strip model. Likewise the cycle for $S\ C^{-1} S^{-1}$ is the reversed input sequence.

equations and the restriction to a 26-cycle are not strong enough to limit our possible solutions of ($S\,C^{-1}S^{-1}$) to only one solution, we would then add other equations involving additional T's and thus still further limit the freedom in ($S\,C^{-1}S^{-1}$).

3.3 Actual Recovery of the Stecker Operator S. As a result of placing menus 1, 2, 3 and 4 on the combined menu sheet, the following isomorphisms were established.

Menu #1	ivrxhotbacgqdswyeupljkfmzn
Menu #2	beqjpfisgazrntxvmlwohcuydk
Menu #3	rmfnelkavguxhposydjbwqzict
Menu #4	gujhscoeyzxbaqkfirntvldwpm

This tabular arrangement is to be interpreted as follows: i in menu #1 occupies the same position as b in menu #2, r in menu #3 and g in menu #4. (Remember how alphabets letters are written as small letters to avoid confusion with the capital letters representing operations). Hence the operator T_1 which transforms A_1 into A_2 is of the nature

$$iT_1 = b,\ vT_1 = e,\ rT_1 = q,\ \text{---}\ \text{etc.}$$

A more convenient way of representing the operation T is to write out

T_1 (ibst) (myve) (lofu) (rq) (wxjhp) (gzdnkca)

with the understanding that $iT_1 = b$, $bT_1 = s$, $rT_1 = t$ and $tT_1 = i$, $mT_1 = y$, etc. Thus T_1 is seen to consist of three four-cycles and one two, one five, and one seven-cycle. The cycle structure for T_1, T_2, and T_3 can be written down as follows:

T_1	(ibst) (myve) (lofu) (rq) (wxjhp) (gzdnkca)
T_2	(rxob) (jnhw) (vsag) (uz) (qfldc) (ktpemyi)
T_3	(rgzd) (yiwv) (lcpq) (ko) (xbtmu) (aesfjnh)

To connect up this mathematical discussion with the practical aspects of the work, we started with incomplete alphabetic substitutions

$A_1, A_{27}, A_{53}, A_{79},$	in menu #1
$A_2, A_{28}, A_{54}, A_{80},$	in menu #2
$A_3, A_{29}, A_{55}, A_{81},$	in menu #3
$A_4, A_{30}, A_{56}, A_{82},$	in menu #4

and combined these into one composite menu. In other words, we solved the three sets of equations:

3.2 Theoretical Recovery of the Stecker or S Operator. Those gifted with a considerable amount of insight can determine that the known substitutions A_1, A_2, A_3, A_4, A_{27}, A_{28}, A_{29}, A_{30}, - - - and C are sufficient to determine S and W. The various mathematical steps will be traced out, however, since the casual reader can probably use assistance in this matter. Now

$$A_2 = S\ C\ W\ C^{-1}\ R_1\ C\ W^{-1}\ C^{-1}\ S^{-1}$$
$$= S\ C\ W\ C^{-1}\ (W^{-1}\ S^{-1}\ S\ W)\ R_1\ (W^{-1}S^{-1}S\ W)\ C\ W^{-1}C^{-1}S^{-1}$$
$$= S\ C\ W\ C^{-1}\ W^{-1}\ S^{-1}\ (S\ W\ R_1\ W^{-1}\ S^{-1})\ S\ W\ C\ W^{-1}\ C^{-1}\ S^{-1}$$

on grouping the terms slightly differently,

$$= S\ C\ W\ C^{-1}\ W^{-1}\ S^{-1}\ (A_1)\ S\ W\ C\ W^{-1}\ C^{-1}\ S^{-1}$$
$$= (S\ W\ C\ W^{-1}\ C^{-1}\ S^{-1})^{-1}\ (A_1)\ (S\ W\ C\ W^{-1}\ C^{-1}\ S^{-1})$$

Mathematically speaking, A_2 is the transform of A_1 by $S\ W\ C\ W^{-1}\ C^{-1}\ S^{-1}$, and A_1 is the transform of A_2 by $S\ C\ W\ C^{-1}W^{-1}S^{-1}=(S\ W\ C\ W^{-1}\ C^{-1}\ S^{-1})^{-1}$. Likewise

$$A_3 = (S\ C\ W\ C^{-1}C^{2}W^{-1}C^{-2}S^{-1})^{-1}\ (A_2)\ (S\ C\ W\ C^{-1}C^{2}W^{-1}C^{-2}S^{-1})$$

and

$$A_4 = (S\ C^{2}W\ C^{-2}C^{3}W^{-1}C^{-3}S^{-1})^{-1}\ (A_3)\ (S\ C^{2}W\ C^{-2}C^{3}W^{-1}C^{-3}S^{-1})$$

We have, therefore a sequence of equations and corresponding statements:

A_2 is the transform of A_1 by $S\ W\ C\ W^{-1}C^{-1}S^{-1}$
A_3 is the transform of A_2 by $S\ C\ W\ C^{-1}C^{2}W^{-1}C^{-2}S^{-1}$
A_4 is the transform of A_3 by $S\ C^{2}W\ C^{-2}C^{3}W^{-1}C^{-3}S^{-1}$

A_{28} is the transform of A_{27} by $S\ W\ C\ W^{-1}C^{-1}S^{-1}$
A_{29} is the transform of A_{28} by $S\ C\ W\ C^{-1}C^{2}W^{-1}C^{-2}S^{-1}$
A_{30} is the transform of A_{29} by $S\ C^{2}W\ C^{-2}C^{3}W^{-1}C^{-3}S^{-1}$
etc.

Note: The writing of $C^{-1}C^{2}$ instead of C^{1} is a whim of the writer. Please humor him to this extent.

Now introduce some simplifying notation.

Let
$$T_1 = S\ W\ C\ W^{-1}C^{-1}S^{-1}$$
$$T_2 = S\ C\ W\ C^{-1}C^{2}W^{-1}C^{-2}S^{-1}$$
$$T_3 = S\ C^{2}W\ C^{-2}C^{3}W^{-1}C^{-3}S^{-1}$$

so that
$$A_2 = T_1^{-1}\ A_1\ T_1$$
$$A_3 = T_2^{-1}\ A_2\ T_2$$
$$A_4 = T_3^{-1}\ A_3\ T_3$$

$$A_{28} = T_1^{-1}\ A_{27}\ T_1$$
$$A_{29} = T_2^{-1}\ A_{28}\ T_2$$
$$A_{30} = T_3^{-1}\ A_{29}\ T_3$$

etc.

the connection between these two operations will be studied. Let the symbol W denote the operation in effect for alphabets 1, 27, 53 and 79.

3. The operation occuring when the output of step number 2 above goes through the remaining wheels and reflector of the machine and returns. Since there is a reflector and since each wheel is used twice, once on incoming and once on outgoing, this operation is reciprocal. Let R_1 denote the operation in effect for alphabet #1. In reality R_1 can be specified by thirteen pairings or links.

4. The inverse operation to step number 2 above, which may be denoted by W^{-1} for alphabets 1, 27, 53 and 79.

5. The inverse steckering operation, which is inverse to the operation of step number 1, and may be denoted by S^{-1} for all positions of encipherments.

Thus, A_1 can be written as

$$\begin{Bmatrix} a \\ b \\ c \\ \cdot \\ \cdot \end{Bmatrix} A_1 = \begin{Bmatrix} a \\ b \\ c \\ \cdot \\ \cdot \end{Bmatrix} S\ W\ R_1\ W^{-1}\ S^{-1} = \begin{Bmatrix} i \\ m \\ g \\ \cdot \\ \cdot \end{Bmatrix}$$

Now A_1 is known, but none of the other operators S, W or R_1 is known at present.

Remark: Considerable confusion is frequently caused by not knowing the way in which the operators are to be applied. In this report (a) ABC will mean that the operation A is first carried out on the letter a, operation B is then applied to that result, and then C is applied to give the final answer.

Now substitution alphabet 2, denoted by A_2, is known, and if the operators for steps number 2, 3 and 4 in the five steps are determined, an operator equation can be written down for A_2. The operator for step 3 is easily determined. Indeed, it was assumed that there was no turn for any of the inside enciphering elements between alphabets 1, 2, and 3. This assumption was verified, since a consistent composite menu was built up for these three alphabets. Indeed, it has been shown that the same thirteen pairings or links were used for alphabets 1, 2, 3 and 4 since all four menus were assimilated into a com-

T O P S E C R E T
OP-20-G-4A/ac

TOP SECRET

26 February 1945.

Investigation of Wired Wheel Machines

From time to time, cipher machines of the wired wheel type are available for study before there is any traffic for exploitation. Such a case occurred when the TIRPITZ machine was captured in France in the summer of 1944. It seems advisable to get on record a number of significant cryptanalytic and cryptographic features of such machines. The following points should be observed in such cases.

1. Nature of the machine keyboard. In some cases, the letters on the keyboard serve as numbers also, and this correspondence should be noted.

2. Provision for a "stecker", and in particular the occurrence of the stecker in the cryptanalytic procedure of enciphering.

3. Wiring of the input plate.

4. Wiring diagrams of all wheels, notch patterns of all wheels, position at the window when the notch allows the kicking machanism to operate, movable rims, etc.

5. Type of reflector, i.e. pluggable, rotatable, etc.

6. Nature of the stepping mechanism, i.e. metric or enigma.

7. Bench mark levels, i.e. position on input plate which corresponds physically to window level. The position can be conveniently specified by the letter on the keyboard to which the input plate contact is wired in the absence of a stecker. Also, distinguishing marks on wheels which can be used as wheel bench marks.

If convenient, photographs should be taken of the complete machine and of certain component parts. This is particularly desirable when the machine may not be immediately available for inspection.

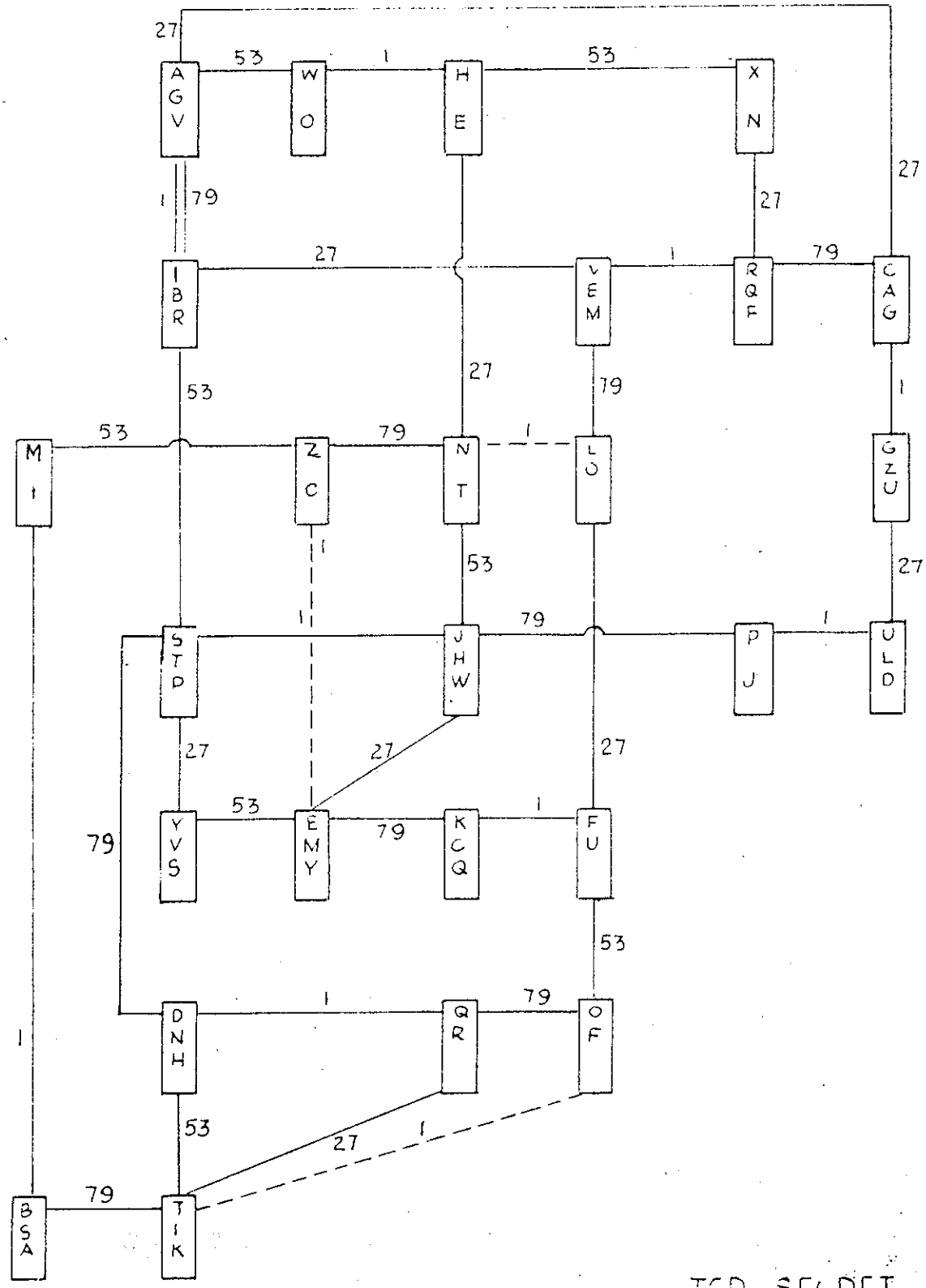
On the other hand, if one were turned loose in the enemy cryptographic spaces but without special equipment such as an ohmmeter to trace out wiring circuits, a different procedure must be adopted. In that case it seems advisable to use the machine to generate a large number of consecutive alphabets. From these the cryptographic features of all moving parts can be obtained.

TOP SECRET

COMBINED MENUS, 1,2,3 (INCOMPLETE)

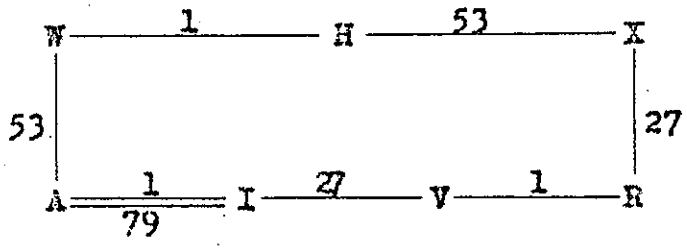
SOLID LINES ARE LINKS FROM MENU #1

BROKEN LINES REPRESENT ADDED VALUES OBTAINED FROM MENUS #2 & #3.

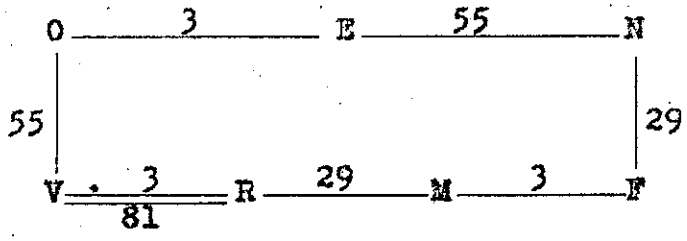


TOP SECRET

Recall the closure already mentioned in menu #1

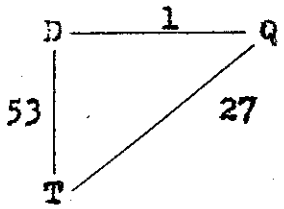


and note the closure in menu #3

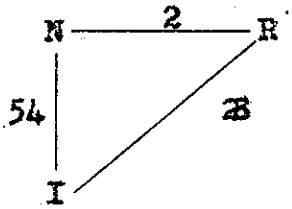


The fact that these two closures are isomorphic, involve a double bond combination and the fact that no contradictions arise in the remaining parts of the menus is sufficient justification for proceeding on the assumption that the above is correct.

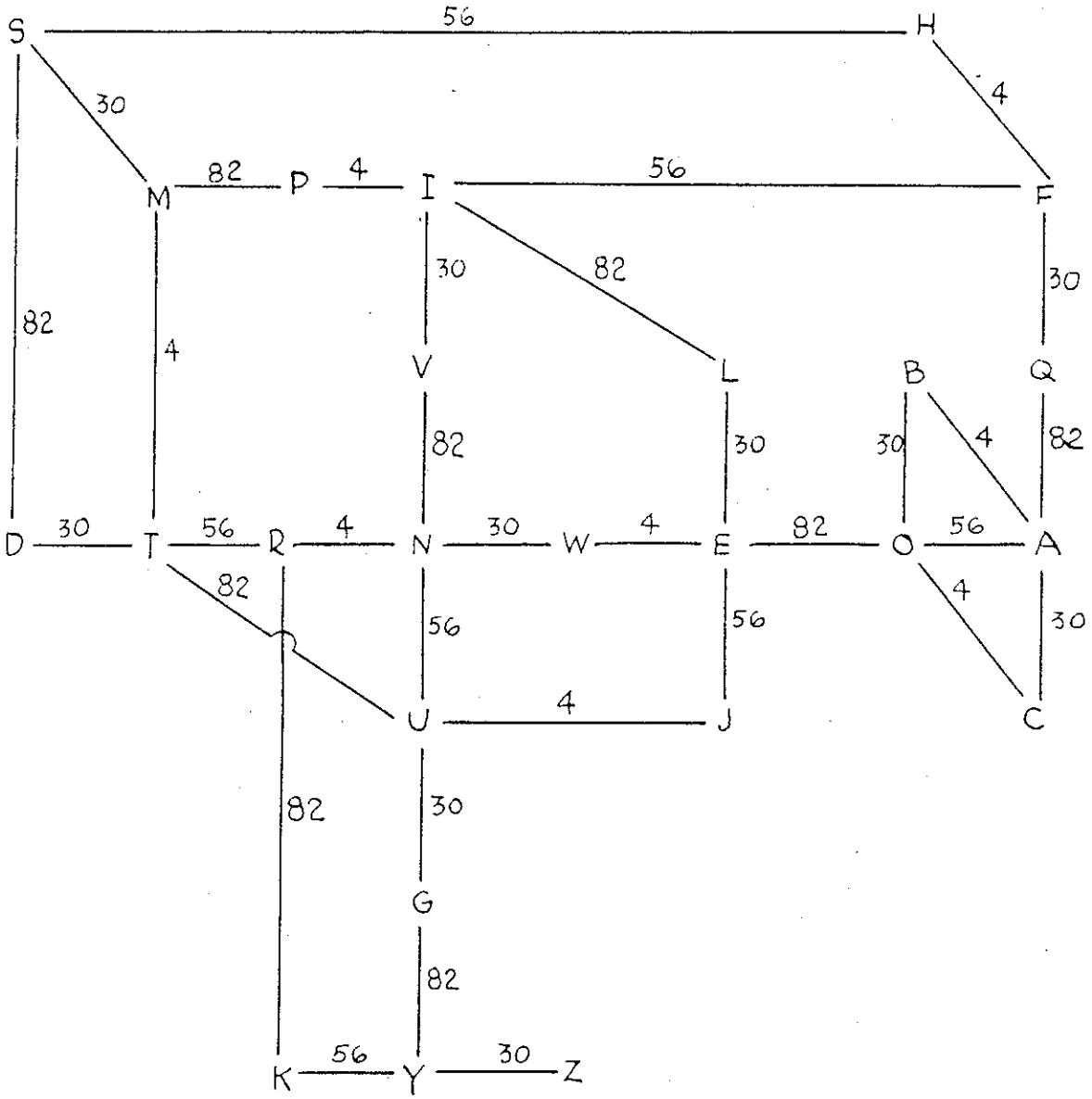
In menu #1 we have the triangular closure



and in menu #2 we have



If menus #1 and #3 are isomorphic, then menu #2 must also be isomorphic with #1 and with #3, and so it must be possible to match menus #1 and #2. The triangular closure is a good place to start from, although of course the fact that it looks good is no proof that it is right. However, assuming that this is correct, proceed with the matching of menus #1 and #2. A good part of menu #2 can be placed so as to partially establish the



MENU # 4

TOP SECRET