Turing’s Treatise on Enigma

Chapter 3

Dr. Alan M. Turing

Editors' Preface

This document was written by the late Dr. Alan M. Turing while he worked as a cryptanalyst at Bletchley Park during the Second World War. The document has been obtained from the US National Archives and permission has been obtained from the Controller of Her Majesty's Stationery Office to publish the paper on the personal Web Page of Frode Weierud. The document has been faithfully retyped by the three editors, Ralph Erskine, Philip Marks and Frode Weierud. The original document was typed and had the style and layout of a typewritten document of that period. To make the re-edited presentation more pleasing the document has been both left and right justified and a more modern type font has been used. Apart from these modifications to the layout the document has the appearance of the original.

Where there are obvious typing errors these have been corrected in square brackets. In a few cases a superfluous letter(s) has been removed by putting the letter(s) in square brackets preceded by a slash, e.g. [/s]. Longer and more detailed comments are in numbered footnotes.

The Editors,

Ralph Erskine,
Philip Marks,
Frode Weierud, © May 1999

Source:

National Archives and Records Administration (NARA), Record Group 457, NSA Historical Collection, Box 201, Nr. 964.

COPYRIGHT

Updated: 23 September 1999

[16]

Chapter III. Methods for finding the connections of a machine. Alphabets and boxes

For any position of the wheels of a machine the letters of the alphabet can be put into 13 pairs so that the result of enciphering one member of a pair is the other member. These pairs are usually written one under the other and called ‘the alphabet’ at the position in question. Thus the alphabet for the wheel order Green Red Purple and rod position 10 14 11 17 is

γ[1]	
M	S
V	L
Z	U
H	Y
J	E
T	R
O	G
I	F
X	D
K	C
A	Q
B	W
N	P

The order in which these are written is immaterial.

When we have two alphabets to deal with it is sometimes helpful to describe both alphabets simultaneously in the form of a `box'. Take for instance the two alphabets

α[2]		β	
V	M	V	U
Z	J	O	N
E	S	J	W
G	A	H	I
N	P	T	M
X	R	F	G
O	F	E	Z
H	I	L	R
L	B	Q	B
D	W	X	P
Y	T	Y	K
U	K	A	C
Q	C	S	D

To form a box from these we choose a letter at random, say T, and write it down with its partner in the first alphabet, Y, following it, thus TY; we then look for Y in the

[1] Editors’ Note: Turing has written KC and NP instead of KP and NC. It is likely to be an error, but it could also be Turing’s way of adapting the data to fit his example.

[2] Editors’ Note: This is the alphabet in column 6 of Fig. 13. Turing has written LB and QC instead of LC and QB.

second alphabet and find it in YK; we write the K diagonally downwards to the left from Y, thus $\begin{matrix}TY\\K\end{matrix}$; now we look for K in

[17]

the first and finding it in KU write $\begin{matrix}TY\\KU\end{matrix}$. From this we get to $\begin{matrix}TY\\KU\\V\end{matrix}$ and $\begin{matrix}TY\\KU\\VM\end{matrix}$, but if we were to continue the process we should get

T Y
K U
V M
T Y
K U
V M
T Y
. .
. .

We therefore draw a line, select a new letter, R say, and start again, writing our results below what we have already written. Thus we get

T Y
K U
V M

R X
P N
O F
G A
C Q
B L

Eventually when there are no letters left we stop with the completed ‘box’ (α ß box)

T Y
K U
V M

R X
P N
O F
G A
C Q
B L

S E
Z J
W D

H I

There are various remarks to be made about boxes. A box completely determines the alphabets from which it was made. Also it can be written in various forms depending on the choices of letter which are made during the process, but two different boxes made from the same alphabets can always be transformed into one another by a combination of the processes

[18]

i) Rearranging the order of the compartments

ii) Moving a number of lines from the top of the compartment to the bottom, the order of the lines remaining the same

iii) Rotating a compartment through 180° about its centre, and then rotating each letter of it through 180° about its centre.

At first sight it would seem possible that in making a box one might reach a state of affairs like this
AB
CD
E.

and that EA occurs in the first alphabet, and one would not then know what to do. This is not actually possible as EA in the first alphabet would contradict AB. For the same reason it is not possible to have E coupled with any other letter which has already occurred.

If we think of the columns in a compartment of a box we see that the effect of going down the left hand column of a compartment or up the right hand column gives the result of enciphering a letter with the first alphabet and then enciphering the result with the second. Consequently if instead of being given the alphabets we have the result of this double encipherment we shall almost have the box. We shall not know how much to slide the opposite sides of a compartment relative to one another, and in the case of compartments of equal size we shall not know how to pair off the sides.

The effect of enciphering first with α then with ß I shall call 'the permutation ßα', likewise the effect of enciphering with α then with ß then γ will be called γßα. For these permutations there is a notation similar to the boxes. However this kind of 'general box' does not enable one to recover the original alphabets. It is also more convenient to write them horizontally (the same applies to ordinary boxes, but the tradition there is firmly established). As an example of the notation

γβα = (GKLAIFP) (YSUH) (TCWMZB) (DEXVRN) (J) (O) (Q)[3]

[19]

This means that G enciphered at α (giving A), and then at ß (giving C) and then at γ gives K, likewise K enciphered with γβα gives L, P enciphered gives G, and J enciphered gives J. With the same notation the alphabet α could be expressed in the form (VM) (ZJ) (ES) (GA) (NP) (XR) (OF) (HI) (LB) (DW) (YT) (UK) (QC).

If the letters of a pair of alphabets are subjected to a substitution, and a new box is made up of the resulting alphabets the sizes of the compartments of this box will be the same as in the original box: in fact this box can be obtained from the first box by subjecting it to the same substitution (except possibly for order of compartments etc.): e.g. if we subject the alphabets α,ß to the substitution

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
Z D G Y T N B H F I K O L U E M S R Q C J A V X W P

[3] Editors' Note: The γβα box given in the original is (GKLAIYSUHFP) (TCWMZB) (DEXVRN) (J) (O) (Q) which is wrong.

(Z to replace A etc.) then we get the alphabets

α′	β′		α′β′
AL	AJ	and the box	CW
PI	EU		KJ
TQ	IV		AL
BZ	HF		RX
XR	NB		MU
EN	TP		EN
HF	OR		BZ
OD	SD		GS
YV	XM		DO
WC	WK		QT
JK	ZG		PI
SG	QY		VY
UM	[4]		HF

Conversely if we are given two pairs of alphabets λ,μ and ρ,σ such that the sizes of the compartments in the λμ box are the same as in the ρσ box, then it is possible to find a substitution which will transform λ into ρ and μ into σ (in fact usually a great many such substitutions). We have only to write the boxes in decreasing compartment size (say), and then a substitution with the required property will be the one which transforms letters in corresponding positions into one another.

[19a]

The size of the compartments in a box, and the lengths of the brackets (cycles) are important, as they remain the same if all the letters involved are subjected to the same substitution, (which might be a Steckering). If we write down the lengths of the cycles of a substitution in decreasing order we obtain what we call the 'class' or the 'shape' of the substitution, e.g. the class of γβα above is 7, 6, 6, 4, 1, 1, 1[5]; with boxes there are two ways of describing the shape, either by the lengths of the compartments or by the numbers of letters in them. It is always obvious enough which is being used.

The following information about frequencies of box shapes may be of interest.

26	25%
24,2	13%
22,4	7.3%
20,6	5.4%
18,8	4.5%
16,10	4.0%
14,12	3.9%
22,2,2	3.7%

[4] Editor's Note: This entry is crossed out in the original (XX). Boxing done by the editors gives the entry as CL.

[5] Editors' Note: The class given in the original is 11, 6, 6, 1, 1, 1 which corresponds to the faulty γβα box as used by Turing.

[20]

The phenomena involved

Before trying to explain the actual methods used in finding the connections of a machine it will be as well to shew the kind of phenomena on which the solution depends.

The most important of the phenomena is this. Suppose we are given the alphabets at the positions REA FKA WMA and also at REB FKB WMB then there is a substitution which will transform the alphabet REA into REB, FKA into FKB etc. The substitution is that which transforms letters of the column of the rod square corresponding to position A into the letters on the same rod in column B. When we are given complete alphabets we can box REA with FKA and REB with FKB, and the substitution will have to be one which transforms the first box into the second. As an example of this phenomenon we may take the alphabets and boxes

REA	REB	FKA	FKB	WMA	WMB	REA FKA	REB FKB	REA WMA	REB WMB
EX	RO	KH	ZJ	TW	XI	EX	RO	EX	RO
UL	FU	JQ	NP	QD	PG	UL	FU	UL	FU
HG	JM	NL	EU	ZF	HB	NK	EZ	KN	ZE
CD	AG	GC	MA	RN	VE	HG	JM	RT	VX
YV	KL	ZR	HV	VJ	LN	CD	AG	WI	ID
FS	BY	IO	DC	OC	CA	MQ	SP	PB	TW
RT	VX	PA	TQ	KL	ZU	JZ	NH	YV	KL
QM	PS	BW	WI	GS	MY	RT	VX	JZ	NH
WI	ID	TV	XL	BY	WK	VY	LK	FS	BY
BP	WT	SY	YK	IP	DT	SF	YB	GH	MJ
AO	QC	MD	SG	HM	JS	WI	ID	MQ	SP
JZ	NH	EF	RB	AU	QF	OA	CQ	DC	GA
NK	EZ	UX	FO	XE	OR	PB	TW	OA	CQ

The substitution which will transform REA into REB, FKA into FKB, WMA into WMB, the box REA/FKA into REB/FKB and REA/WMA into REB/WMB is

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
Q W A G R B M J D N Z U S E C T P V Y X F L I O K H

In this example the alphabets have been written out in such a way that a letter and the result of applying the substitution occupy corresponding positions. Of course if our alphabets were data from which the substitution was to be found this would not generally be the case. Our problem would be to arrange them or the boxes made from them, in such an order.

[21]

We might for instance [be] given the alphabets in the more or less alphabetical order

REA	REB	FKA	FKB	WMA	WMB	REA FKA	REB FKB	REA WMA	REB WMB
AO	AG	AP	AM	AU	AC	AO	AG	AO	AG
BP	BY	BW	BR	BY	BH	IW	SP	CD	PS
CD	CQ	CG	CD	CO	DT	BP	NH	QM	JM
EX	DI	DM	EU	DQ	EV	CD	VX	HG	YB
FS	EZ	EF	FO	EX	FQ	MQ	LK	SF	HN
GH	FU	HK	GS	FZ	GP	JZ	YB	ZJ	LK
IW	HN	IO	HV	GS	IX	RT	RO	VY	WT
JZ	JM	JQ	IW	HM	JS	VY	FU	BP	DI
KN	KL	LN	JZ	IP	KW	SF	EZ	IW	XV
LU	OR	RZ	KY	JV	LN	EX	JM	TR	EZ
MQ	PS	SY	LX	KL	MY	UL	CQ	NK	UF
RT	TW	TV	NP	NR	OR	NK	TW	LU	QC
VY	VX	UX	QT	TW	UZ	HG	ID	EX	OR

and then make from them the boxes on the right. From the right hand pair of boxes we see that E must become either O or R in the substitution, and we can try both hypotheses out by arranging the first two boxes correspondingly. If the first box is left as it is, the corresponding rearrangements of the second are

..	..
..	..
..	..
HN	AG
PS	SP
GA	NH
MJ	VX
ZE	LK
UF	YB
OR	RO
BY	FU
KL	EZ
XV	JM

The first of these rearrangements is impossible. It implies for instance that in the substitution C becomes H and M becomes P but in the third box C and M are on opposite sides of a compartment while in the fourth H and P are on the same side. Actually we have in the six alphabets rather an embarras de richesse. It would really be easier to work with say the first five alphabets and two constatations, AC and BH say of the remaining one. Since B and H occur three apart in the same column of $\frac{\text{REB}}{\text{FKB}}$ the pair of letters of WMA from which BH arises by the substitution must occur three apart in one of the columns of the large compartment of $\frac{\text{REA}}{\text{FKA}}$. The only possibility is that BH arises from FZ, and we can check & complete the result with the AC.

[22]

We make use of a third phenomenon when we have found some parts of the rod. Suppose we find the substitution which transforms the first column of the purple rods into the third

1	3	4	6[6]
Z	D	J	Y
D	K	W	P
G	E	C	A
Y	V	X	I
T	C	D	E
N	F	A	D
B	S	T	R
H	Z	G	C
F	H	Z	W
I	U	B	N
K	N	R	X
O	T	L	Z
L	Q	V	M
U	B	I	V
E	O	Q	J
M	W	N	S
S	N	P	T
R	Y	F	K
Q	G	U	H
C	I	Y	B
J	X	K	F
A	P	M	Q
V	L	H	U
X	J	E	O
W	R	O	G
P	A	S	L

It is (ZDKNFH) (GEOTCIUBSMWRYVLQ) (JX) (AP)

and the substitution which transforms the 4th[7] column into the 6th is

(JYBNSLZWPTRXIVMQ) (CADEOG) (HU) (FK)

These two substitutions are of the same ‘shape’, and if we write them like this

(YVLQGEOTCIUBSMWR) (NFHZDK) (PA) (JX)
(JYBNSLZWPTRXIVMQ) (CADEOG) (HU) (FK)

each letter in the lower line is below the letter which is three places further on along the (QWERTZU) diagonal. We can see that this must happen because if we replace the letters of the first and third columns of the rod square by those which are three places back along the diagonal and then move the result three places to the right and three upwards we get the fourth and sixth columns.

[6] Editors’ Note: Turing has circled the letter A in column 1 and the letter U in column 4 and joined the two together with a line. Similarly P in column 1 is joined to H in column 4, P in column 3 with H in column 6 and A in column 3 with U in column 6.

[7] Editors’ Note: Originally written as third and fourth and then changed by hand into 4th and 6th.

[23]

A rather similar phenomenon is useful when we know the diagonal of the machine. In such a case we can make a correction to our constatations transforming them into connections between the contacts on the right of the R.H.W. wheel instead of between contacts of the Eintrittwalze. The constatations when so transformed are described as ‘added up’ or ‘buttoned up’. The process can be carried out with two strips of cardboard with the diagonal written on them, and in one case repeated. As an example to make quite clear what this adding up process is take the fixed comic strips [in] Fig. 11. The alphabet for this position of the machine is

(CD) (FR) (TV) (XO) (JK) (WQ) (AG) (PY) (BS) (HM) (IL) (EN) (UZ)[8]

The added up alphabet can be obtained either by tracing through the wheels from the purple column on the right back to this column again, or by applying the substitution

Q W E R T Z U I O A S D F G H J K P Y X C V B N M L
Y X C V B N M L Q W E R T Z U I O A S D F G H J K P

to the ordinary alphabet. It is

(FR) (TV) (BG) (DQ) (IO) (XY) (WZ) (AS) (HE) (UK) (LP) (CJ) (MN)[9]

Instead of tracing the current through from the right hand purple column in Fig 11 we can of course trace it through from the left hand purple column back to this column again. This gives us a very simple picture of how the added up alphabets between turnovers are related; one is obtained from another simply by a slide on this left hand purple column, i.e. a slide on the last upright of the rod square. For instance if on the comic strips [in] Fig. 11 we move the R.H.W. to rod position 15 we have the added up alphabet

(EA) (RD) (VM) (IO) (PN) (UB) (LF) (GW) (YS) (CT) (QJ) (KZ) (HX)[10]

which can be obtained from the added up alphabet at rod position 18 by the substitution

T W V K S B C E Y U F H X Z M N J G O P A Q I R L D
R L D T W V K S B C E Y U F H X Z M N J G O P A Q I[11]

[24]

The saga

Suppose that one was left alone with an Enigma for half an hour, the lid being locked down and the Umkehrwalze not movable, what data would it be best to take down, and how would one use the data afterwards in order to find out the connections of the machine? Can one in this way find out all about the connections? This problem is

[8] Editors’ Note: Turing has written BZ and US instead of BS and UZ which can be found from Fig. 11.

[9] Editors’ Note: Turing has written HN and ME instead of HE and MN.

[10] Editors’ Note: Turing has written YX and HS instead of YS and HX.

[11] Editor’s Note: The last letter in the bottom row, I, is written as T in the original text, which is clearly wrong.

unfortunately one which one cannot often apply, but it helps to illustrate other more practical methods.

It is best to occupy most of one's half hour in taking down complete alphabets. At least nine of these are necessary as follows from this argument. If the solution is completely determined by the data the number of possible different data must be at least equal to the number of possible solutions. Now the number of possible different diagonals is 26!, the number of ways in which one can wire up a wheel is also 26!, and the number of ways in which one can wire an Umkehrwalze is approximately $(26!)^{1/2}$, so that the number of possible solutions is about $(26!)^{9/2}$. The number of possible variations of an alphabet is about $(26!)^{1/2}$, so that the number of possible variations of nine alphabets is about $(26!)^{9/2}$, which is the number of solutions.

The practical minimum amount of data is surprisingly close to this theoretical minimum. It is possible to find the connections with 9 properly chosen alphabets and 10 other constatations properly chosen. However, in order to shorten the work I shall take an example where we are given 11 alphabets and 10 constatations.

[25]

Data for saga

AAA	AAB	AAC	AAD	ABA	ABB	ABC	ACA	CAA	BAA	CAD	ACB	ADA	DAA	CAC	BAD
AL	AD	AI	AM	AK	AE	AW	AM	AS	AQ	AZ	SO	UQ	MJ	HX	MA
BS	BC	BY	BS	BO	BS	BV	BP	BO	BV	BN	ZJ	LB	IL	VS	IU
CE	EK	CT	CH	CF	CR	CZ	CE	CP	CH	CO					
DH	FV	DM	DR	DE	DQ	DX	DW	DJ	DU	DF					
FM	GZ	EV	EO	GQ	FL	EJ	FG	EU	EP	EI					
GR	HN	FN	FQ	HW	GV	FO	HL	FQ	FL	GL					
IK	IT	GX	GP	IX	HK	GU	IZ	GV	GM	HX					
JN	JY	HU	IJ	JP	IN	HI	JO	HY	IZ	JR					
OZ	LU	JO	KX	LS	JP	KR	KQ	IL	JO	KP					
PV	OQ	KZ	LT	MY	MO	LQ	NU	KT	KN	MY					
QW	PS	LW	UZ	NR	UY	MT	RS	MX	RW	QV					
TY	RX	PQ	VY	TZ	WZ	NS	TX	NR	ST	ST					
UX	MW	RS	NW	UV	TX	PY	VY	WZ	XY	UW					

There will be a substitution which transforms AAA into AAB, ABA into ABB and ACA into ACB. Following the method for finding such a substitution explained in the last paragraph[12] we form the boxes $\begin{matrix}AAA\\ABA\end{matrix}$, $\begin{matrix}AAB\\ABB\end{matrix}$ and also $\begin{matrix}AAC\\ABC\end{matrix}$ which will be needed later.

AAA ABA	AAB ABB	AAC[13] ABC	ACA	ACB	CAA	CAC
AL	AD	AI	AM	SO	AS	HX
SB	QO	HU	BP	ZJ	BO	VS
OZ	MW	GX	CE		CP	
TY	ZG	DM	DW		DJ	
MF	VF	TC	FG		EU	
CE	LU	ZK	HL		FQ	
DH	YJ	RS	IZ		GV	
WQ	PS	NF	JO		HY	
GR	BC	OJ	KQ		IL	
NJ	RX	EV	NU		KT	
PV	TI	BY	RS		MX	
UX	NH	PQ	TX		NR	
IK	KE	LW	VY		WZ	

We want to rearrange the box $\begin{matrix}AAB\\ABB\end{matrix}$ in the way that was done at the bottom of p. [21]. The substitution which transforms $\begin{matrix}AAA\\ABA\end{matrix}$ into $\begin{matrix}AAB\\ABB\end{matrix}$ must also transform two constatations of ACA into SO and ZJ. The only constatations of ACA from which SO could have arisen are LH, [&] VY. If OS arises from LH we should have to have a substitution which involves ZJ arising from OE in ACA, and this does not exist.

[26]

However, if we rearrange it so that OS arises from VY we find ZJ arising from IZ. We can similarly arrange $\begin{matrix}AAC\\ABC\end{matrix}$ to fit with them and agree with CAA and CAC, and fit $\begin{matrix}AAA\\CAA\end{matrix}$ to fit onto $\begin{matrix}AAD\\CAD\end{matrix}$ agreeing with BAA and BAD.

[12] Editors' Note: Turing wrote "last paragraph" while he probably referred to the last section.

[13] Editors' Note: In the two boxes AAA/ABA (column 1) and AAB/ABB (column 2) letters are circled and joined together by a line. The letter L in column 1 is joined to the letter O in column 2. Similarly O in column 1 is joined to Z in column 2, E in column 1 with J in column 2 and H in column 1 with S in column 2. Also the bigram HL in the box ACA is circled and joined with the bigram SO in the box ACB.

					Rearranged	
AAA	AAB	AAC	AAA	AAD	AAA	AAD
ABA	ABB	ABC	CAA	CAD	CAA	CAD
AL	VF	GX	AL	AM	AL	TL
SB	LU	DM	IK	YV	IK	GP
OZ	YJ	TC	TY	QF	TY	KX
TY	PS	ZK	HD	DR	HD	HC
MF	BC	RS	JN	JI	JN	OE
CE	RX	NF	RG	EO	RG	IJ
DH	TI	OJ	VP	CH	VP	RD
WQ	NH	EV	CE	XK	CE	FQ
GR	KE	BY	UX	PG	UX	VY
NJ	AD	PQ	MF	LT	MF	MA
PV	QO	LW	QW	SB	QW	ZU
UX	MW	AI	ZO	NW	ZO	WN
IK	ZG	HU	BS	UZ	BS	BS

We can now write down the parts of the rods which are in the columns corresponding to the window positions A, B, C, D though we do not know the correct order. They are

AVGT	YSKX	WNEU	UMAV
LFXL	MBRM	QHVZ	XWIY
SLDS	FCSA	GKBJ	IZHG
BUMB	CRNF	REYI	KGUP
OYTN	EXFQ	NAPE	JDQO[14]
ZJCW	DTOC	PQLD	
TPZK	HIJH	VOWR	

The substitution which transforms the letters in the first column of these rods into those on the same rods in the second column is

(AVOYSLFCREXWN) (BUM) (ZJDTPQHI) (GK)

That which transforms the second into the third is

(VGUMAPZH) (FX) (LDQ) (YTOWIJCSKBRNE)

and that which transforms the third into the fourth

(GTNFQOCWRMBJH) (XLDSAVZK) (EUP) (YI)

These three substitutions have now to be arranged one under the other in such a way that the substitution which transforms the third into the second is the same as that which transforms the second into the first, this substitution being a slide of one on the diagonal. Clearly (FX) in the second has to fit under either

(GK) or (KG) in the first: if F is under G we cannot fit the second and third together, for F occurs in a bracket of 13 in the third, and G in a bracket of 8 in the second. If F is under K we can fit the three together like this

[14] Editors' Note: JDQO should be placed between NAPE and PQLD.

(AVOYSLFCREXWN)(BUM)(ZJDTPQHI)(GK)
(SKBRNEYTOWIJC)(QLD)(VGUMAPZH)(XF)
(NFQOCWRMBJHGT)(PEU)(KXLDSAVZ)(IY)

The diagonal is

APQBORYFKVZHIXGJWELUDMTCNS

Of course we do not know where the diagonal 'starts', but with a hatted diagonal like this it does not matter. We can use the diagonal to put the rods in order and to give them names. There is likely to be an error in our naming, because we shall not know where to start naming either the rows or the columns. The difficult about naming the columns simply means that we do not know the Ringstellung or the absolute positions involved. If we have the columns correctly named but the rows wrongly we shall have the wheel right except that the plate contacts are rotated with respect to the spring contacts. It is very difficult to eradicate this. It can only be done if we have a great deal of information about actual window positions and Ringstellung, e.g. if there is a Herivelismus or if the letters of the Ringstellung are restricted to be all different and no two consecutive in the alphabet except Z and A.

[28]

Our set of rods is

IZHG	z
HIJH	h
XWIY	i
EXFQ	x
GKBJ	g
VOWR	j
REYI	w
LFXL	e
KGUP	l
JDQO	u
MBRM	d
OYTN	m
FCSA	t
NAPE	c
PQLD	n
BUMB	s
DTOC	a
CRNF	p
YSKX	q
AVGT	b
ZJCW	o
WNEU	r
SLDS	y
UMAV	f
TPZK	k
QHVZ	v

and we can transform all our data about other alphabets into the form of data about rod couplings[15]. The ones we need first are

AA	AB	AC	AD[16]
ah	ax	yw	fv
be	bl	eh	es
cu	cw	bd	
dt	dq	px	
fi	ey	gt	
gw	fj	ki	
jn	ko	zo	
kq	ms	vl	
lz	nu	ns	
mo	pt	um	
px	gv	jq	
rv	rh	fc	
sy	iz	ar	

From these we can get the upright of the middle wheel. The first step is of course to add up the alphabets. Here they are added up with Z as standard

AA*	AB*	AC*	AD*
pi	qj	vu	hx
ol	rd	dg	mb
nd	sl	yc	
mc	to	ow	
kx	uk	es	
je	ve	jh	
ws	zy	xf	
vb	cp	im	
uh	am	pq	
tr	bn	tn	
qg	wh	lr	
yz	fx	za	
af	gi	bk	

[15] Editors' Note: These rod couplings can be used to remove the effect of the R.H.W. The 1st column is used to transform alphabets where the R.H.W. is in position A, Like AAA, ABA, ACA, etc. The succeeding columns are used to transform alphabets where the R.H.W. is in position B, C and D respectively.

[16] Editors' Note: The rod coupling transformations have been applied to the alphabets on page 25. AA is the transformation of AAA, AB of ABB, AC of ACC and AD of ADD. ACC and ADD can be derived from ACA and ADA with the use of the transformations on page 26.

[29]

We now box AA^* with AB^* and AB^* with AC^*, and then rearrange $\begin{matrix}AB*\\AC*\end{matrix}$ so as to find the substitution which transforms $\begin{matrix}AA*\\AB*\end{matrix}$ into $\begin{matrix}AB*\\AC*\end{matrix}$ and AC^* into AD^*

AA^*	AB^*	AB^*	
AB^*	AC^*	AC^*	rearranged
pi	qj	jq	
gq	hw	pc	
je	ot	yz	
vb	nb	am	
nd	ku	ig	
rt	ve	dr	
ol	sl	ls	
sw	rd	ev	
hu	gi	uk	
kx	ma	bn	
fa	zy	to	
mc	cp	wh	
yz	xf	xf	

This substitution sends each letter of the upright of the middle wheel into the next on the upright; hence the upright is

lsezftrdgpjyxniqchukbmwvao

As we added up to position Z as standard this upright is the upright for position Z. We can make out part of the rod square from it, there being difficulties about where to begin as before

ZABCD	
LNJFB	z
SWKOL	h
EVRUP	i
ZYDQW	x
FMBEZ	g
TOLHC	j
RUINH	w
DXSIQ	e
GAXBV	l
PGOZD	u
JRHMK	d
YITVN	m
XCZSU	t
NHADF	c
IPMKJ	n
QTVWO	s
CZERS	a
HLYAE	p
UFPLI	q
KQUXR	b
BDGYT	o
MJFCA	r
WKNPG	y
VSQJM	f
ABWTX	k
OECGY	v

[30]

We can transfer our remaining data into information about couplings of the middle wheel rods. By sliding the diagonal up the side of the rod squares we can get the couplings immediately into added up form

A^*	B^*	C^*	D^*	A^* B^*	B^* C^*	B^* C^{*17}	rearranged
ra	as	ay	kd	ra	as	wl	
bt	bn	bi	ox	sl	gz	cr	
ce	cr	cl		wj	eq	do	
di	do	dr		kg	jk	vf	
fo	eq	ez		zv	tx	nb	
gk	fv	fn		fo	ph	iu	
hy	gz	gs		di	wl	my	
jw	hp	hw		un	cr	as	
ls	iu	xp		bt	do	gz	
mx	jk	jq		xm	vf	eq	
nu	lw	kt		yh	nb	jk	
pq	my	mu		pq	iu	tx	
vz	tx	vo		ec	my	ph	

The left hand wheel upright is

rwdmqxeptznschkvbgfiyjoual
zhixgjweludmtcnsapqboryfkv

[17] Editors' Note: The original has A^* here which clearly is wrong.

and under it has been written the diagonal. This serves to transform A or A^+ into the Umkehrwalze connections. They are

`yv,fs,ce,zw,oi,mu,rj,qx,pk,nd,ht,bg,al`[18]

[31]

'Adding up' method

Most practical methods of finding the connections of the machine depend on getting a long crib, either by 'reading on depth' (see Colonel Tiltman's paper [*long space*]) or by pinching. In many cases we expect the diagonal to have some special value, (e.g. qwertzu because the original commercial machine had such a diagonal). In this case the amount of crib is not very much. To estimate the amount of material that we have it is best to work out

(Length - 2.5) × square of average 'corrected depth'

Call this the 'material measure'. By corrected depth we mean the actual number of constatations, so that this can never exceed 13. As regards the amount of material necessary, it will almost always be impossible to get the wheel out with less than a measure of 90, from 90 to 140 it will be a matter of chance whether it comes out or not. From 140 onwards it will always come out, but with increasing ease as the material measure mounts up. With a material measure of [3?]00 it is so easy that the trouble of adding up further material would be more than would be gained in shortening the further work. The method is essentially the same as we used for finding the middle wheel in the case of the saga. Here however we have to do with partial alphabets or even single constatations instead of complete alphabets. We cannot therefore do any boxing. After we have added the material up we take some hypothesis about the upright, e.g. that F immediately follows K and work out its consequences. If for instance we find the (added up, I shall omit to mention this in future) constatations $\frac{K}{R}$ and $\frac{T}{F}$ immediately following one another we can infer that T immediately follows R on the upright. This we may express in the form

KF – RT

the dash denoting logical equivalence. We follow out the consequences until we reach a confirmation or a contradiction. When there is

Here KF means 'F follows K on the upright'. KF^2 would mean K & F are two apart [on the upright].[19]

[32]

plenty of material we do not usually work a hypothesis unless there is going to be an immediate confirmation, e.g. if TC implies RJ from two different parts of the crib.

[18] Editors' Note: We believe Turing made two errors when he derived the UKW connections and that the correct connections should be: es, ca, yu, zo, rp, jm, hq, ig, fv, nl, xw, bt, dk.

[19] Editors' Note: Turing's hand written note. The end of the last part is missing but we presume it is as we have indicated in the square brackets.

This will mean to say that the constatations $\begin{matrix}T\\R\end{matrix}$ and $\begin{matrix}J\\C\end{matrix}$ occur consecutively twice over. Alternatively we can say that $\begin{matrix}T\\R\end{matrix}$ occurs twice over at a certain distance and that $\begin{matrix}J\\C\end{matrix}$ also occurs twice over at the same distance. In order therefore to find these profitable hypotheses we have only to look for repetitions of constatations (half-bombes as they are rather absurdly called). For this reason and also because later we will want to be able to spot occurrences of a given letter at a glance, we put our material as we add it up into the form in Fig. 19.

Now to take a particular problem. We are given material six deep and 100 long, and we expect that the diagonal is qwertzu. Our material is

```
MYC..
NGJ..

RCA..
YID..

DAS..
TTV..

YON..
RMI..

OFL..
VQO..

MUX..
NJQ..
```

(I must apologise for it not making sense).

We decide to try out the hypothesis that there is no T.O. in the first seven columns, and therefore we add up the columns 1-7, 27-33, 53-59, getting

```
LCN..
MJY..

TBF..
XAH..

FDG..
ZUM..
 ...
```

[33]

	1	2	3	4	5	6	7	27	28	29	30	31	32	33	53	54	55	56	57	58	59
A	B	B				H	I	V	U		D	K	B	O	J			I			
B	A	A	R			Y	E			P	O		A	P	P			J	P		
C		J		N					Y		J		R			X					
D		U	E	Q					H		A			Z						L	
E		H	D			I	B												X		O
F	Z		H	H			Y			Y	Z			N		T	O		J	G	U
G			M				K	J	P			Y				V			V	F	
H		E	F	F	W	A			D								V				
I						E	D				M	N	P			U		A		X	Q
J		C						G			C				A			B	F	U	
K					M		G					A	T					T			
L	M											M	Z		O			Y		D	
M	L		G		K					Z	I	L			U		U			V	R
N			Y	C	Q					U		I		F							
O		P				X		S			B			A	L	P	F				E
P		O			T				G	B			I	B	B	O			B		W
Q		S	S	D	N			X				X				Z	X	U			I
R			B	U									C								M
S		Q	Q					O									Z		Z		
T	X				P					X			K			F		K		Y	
U		D		R					A	N			V		M	I	M	Q		J	F
V								A					U	X		G	H	X	G	M	
W					H										Y						P
X	T					O		Q		T		Q		V		C	Q	V	E	I	
Y			N			B	F		C	F		G			W			L		T	
Z	F									M	F		L	D		Q	S		S		

A	Q	
B	S	
C	U	?
D	X	
E	V	
F	P	
G	W	
H	T	
I	R	
J	G	Z
K	Y	
L	A	
M	B	
N	C	?
O	D	
P	E	
Q	F	
R	G	
S	H	
T	I	
U	J	
V	K	
W	K	
X	M	
Y	Q	N
Z	O	

Fig. 22

q	w	e	r	t	z	u	i	o	a	s	d	f	g	h	j	k	p	y	x	c	v	b	n	m	l
A	Q	F	P	E	V	K	Y	N	C	U	J	Z	O	D	X	M	Z	B	H	T	I	R	G	W	L
							m	l	q	u	?	?	f	?											
							W	L	A	Q	F	P	E	V											

Fig. 19

[34]

However we put the material directly into the form in Fig. 19. We see numerous half-bombes and do not need to make any more analysis of their lengths in order to find a profitable start. The half[-]bombes $\begin{matrix} Q \\ S \end{matrix}$ and $\begin{matrix} F \\ H \end{matrix}$ suggest the two possible starts QF=SH and QH=SF (the two strokes meaning a double implication, not equality!). The consequences of the second of these are shewn in Fig. 20. A contradiction is quickly reached. The consequences of QF [are shewn] in Fig. 21. The loop QF-ZO-MB-UJ-QF gives a second confirmation, and our hypothesis is now a virtual certainty. We now abandon the tree figure for an alphabet with consecutives written against them (Fig. 22). All goes smoothly except that there is clearly an error in our data as we have a few contradictions. We sort out the good from the bad by using pairs of letters two apart on the upright. Thus $JO^2 - AF^2$ confirming JZ, ZO, AQ, QF. When we have checked them all we can write out the upright of the R.H.W.

AQFPEVKYNCUJZODXMBSHTIRGWL

We then have to find the upright of the M.W. To do this we use the same process as we did with the saga. We have to find the added up couplings of the middle wheel. This can actually be done without either adding up separately or writing out the rod square, simply by having two movable strips with the upright and qwertzu written out on each, and sliding these above the (added up) crib till the constatations agree with pairs of letters on the strips directly above. We can then read off the coupling from the row of qwertzu letters, taking the pair of letters in column 1 for columns 1-7 of the crib [,] column 2 for 27-33 etc. Under Fig. 19 is shewn the strips as set for reading off one of the added up couplings for 53-59, viz. [aq]. The added up couplings that we get are

1–7	27–33	53–59	79–85	105–111
qp	hx	qa	jn	zm
wb	qs	wj	xv	ti
ef	wu	eg	tr	
ry	ek	th	fh	
tn	rn	rv	ql	
zu	tc	zx	up	
ix	zy	um	oy	
os	ia	io	ds	
ag	ov	sk	wb	
dm	dj	db	ci	
hv	fm	fy	gz	
jc	gb	pn	em	
kl	pl	cl	ka	

(some of these being supposed obtained from material not yet given)

[35]

Boxing these together we get

1–7	27–33	53–59
27–33	53–59	79–85
qp	hx	qa
lk	zy	ks
ef	fm	db
md	uw	wj
jc	jd	np
tn	bg	um
ry	ek	eg
zu	sq	zx
wb	ai	vr
ga	ov	th
ix	rn	fy
hv	pl	oi
os	ct	cl

When we fit these boxes together we fail miserably, and so we have to assume that there is a double T.O. somewhere, in spite of all the boxes turning out the same shape. We find that this is between the first and second alphabets, and that the remainder can be fitted together with the upright

wbnhcovrtixlyazqpgfkmsuedj

[36]

I will give a second example of the ‘adding up’ method for a case where it is only just possible to get the problem out. The material is given in Fig. 23 all ready added up. There are no ‘equidistances’ (half-bombes with equal distances) and so we have to make an analysis shewing all the consequences of any hypothesis that one letter follows another on the upright (Fig. 32). For instance from the analysis we see that AV, HT, NF, ZA [,] are all consequences of IM. The pencil letters round the outside were put in to help with the making of the analysis and were used in connection with columns 32, 33 of the material. Of course some of the consequences will be false owing to turnover, but as we are dealing only with distances of 1 we can hope to neglect this without harm. We now pick out squares with a large number of entries in them and follow out the further consequences of them[,] making trees as before, and hoping to find confirmations. When we get contradictions we leave the tree for the present but have to remember the T.O. possibility [(]Figs. 25–30[)]. When we get stuck we can sometimes continue using consequences which are of the form that two letters are at distance 2 on the upright. For this purpose an analysis of positions at which letters occur is useful (Fig. 24). In particular we need to do this at Fig. 30. Now VW and WY imply VY^2 and PR and RS imply PS^2 and these imply one another from columns 19, 21. We also get GL^2 which starts off another train of consequences involving another confirmation (Fig. 31). Eventually we get stuck with the bits of upright

```
      V W Y
N . Q   P R S
    U H J K
F G I L . O
      B . E
```

We might try putting in KA as a hypothesis, afterwards try KB etc. (KA appears at first to give confirmations, but these are bogus. The only reliable rule about confirmations is to try leaving a constatation out and then see if it can be inferred from the hypothesis). We might also try

[37]

putting in as many new constatations as possible which are consequences of those we have and our available information about the upright, and then start off afresh with some new distance on the upright, say 5. But there is a quicker road to success. Note the constatation $\begin{matrix}H\\J\end{matrix}$ in 1 and $\begin{matrix}G\\I\end{matrix}$ in 17. Since we have J following H and I following G on the upright it seems highly probable that we have HG^{10} and JI^{10}. If this is so we have this as part of the upright

FGIL.O....UHJK

hence OH^{6} which implies PK^{6} giving us this as upright

FGILNOQPRSUHJK

From this we get many confirmations and are able to fill in the whole of the upright (except X which goes in the one remaining place). Note that the T.O. which actually occurs between 24 and 25 has not troubled us at all.

[Pages 38 – 40 missing][20]

[41]

Clicks at twenty-six-distance

This is a method for finding the connections when we do not know the diagonal. It is very similar to the beginning of the saga, in principle. It depends on making hypotheses about pairs of letters being on the same rod, and drawing conclusions to the effect that other pairs of letters are on the same rod. Suppose for example that in our crib were the following constatations

5	6	31	32	57	58	83	84
A	E	F	E	T	U	P	U
F	G	T	R	P	R	A	G

We might make the hypothesis that on the rod which has A in column 5 there is G in column 6. We could then infer that there was another rod with F and E in columns 5, 6, and likewise rods TR, PU and this confirms our hypothesis that there was a rod AG.

[20] Editors' Note: The pages 38 to 40 are missing from the archive copy of the original.

Proceeding in this way we can with sufficient material find sufficiently much of some of the rods to be able to find the diagonal by the same method. The amount of the material needed is very great. We adopt a measure similar to the one for 'adding up' viz.

(length-39) × square of average corrected depth

I believe it is practically impossible to solve any problem with this measure less than 2000. It should be possible for 3000 but might sometimes a great deal of labour. With the example given here the measure is 4400.

When the material is sufficient we avoid taking hypotheses at random, and choose ones which we can see without very much analysis, to lead to a confirmation. This would be the case for example with these constatations

5	6		31	32
R	E		R	E
V	D		V	D

Either the hypothesis that E follows R or that D follows it on a rod would be immediately confirmed. In the absence of other information the probability that one or other of these

[42]

hypotheses is correct is about 79%. Our first job therefore is to look for such configurations of letters. All that we have to do is to analyse the constatations which have the same right hand wheel position, and ring round any repetitions. We then write out the ringed constatations on a separate sheet (Fig. 34). With the first occurrence of each constatation we give a number shewing how far on the other occurrence is. This plan also shews us where the T.O. is likely to be. It should be mentioned that in the case of this material there were two turnovers known to be 13 apart. The principle of spotting the turnover is this. Consider for example the constatations HE at b,II and b,X and JE at i,II and i,X.the first pair of these constatations shows that there must have been a pair in common between the coupling at b,II and b,X. Likewise there must be one in common between those at i,II and i,X. It is therefore fairly likely that there is no turnover between b,II and i,II, as if there had been it would have been quite likely that after the T.O. there would no longer have been a pair in common in the couplings. The evidence from a single such instance is rather slight, but with as much material as we have in our present problem we can fix it with no doubt at all, as occurring between z and a and between m and n.

It is worth while writing down all the favourable hypothesis under the pairs of columns of the rod squares involved (Fig. 35). We have done this only for the part a to m, and find that in five cases there are two favourable hypotheses viz. col. b with e, col. b with h, col. d with j, col. e with i, and col. g with j. We hope that in some of these cases the favourable hypotheses will imply one another, making them both virtually certain. The consequences of these hypotheses are shewn in Figs. 36–40. The notation is this. An expression like OF under the head ‘d into j’ means that the rod with o in col. d has F in col. j, and the strokes joining these mean that one can be deduced from the other. In the case of g into j the two hypotheses are essentially the same and we have an immediate

[43]

confirmation. With b into h we find that both of the first alternatives of the one hypothesis contradict both alternatives of the other. With d into j we manage to connect the two hypotheses together and with e into i we fail to connect but one of the hypotheses confirms itself. The information we have obtained about the rods from this is expressed in the Fig. 41a. In order to avoid bogus confirmations in what follows it is as well whenever we make a deduction to cross out one of the constatations used in the deduction. Up to this point the crossing out has been done with red strokes slanting up to the right. (Green vertical strokes were used to eliminate repetitions of a constatation, red vertical strokes to remove contradicted constatations). From now on for a time we will use similarly slanting green strokes.

Up to now we have simply been trying to ‘get a start’, and so long as we could get some fairly considerable bits of the rods square fixed we did not very much care what parts they were. But now we have got a fully adequate start, and we should consider a plan of campaign. In general what we want is to have most of the letters of the rods in columns p, p+q, p+r, p+q+r, t, t+u, t+r, t+u+r, of which any number may coincide, provided q, r, u are none of them 0. If we then find the permutation which transforms col. p into col. p+q expressed in cycles as on p. 18 or p. 26, and similarly for constatations p+r and constatations p+q+r. A slide of r on the diagonal will transform these into one another. We get further information about a slide of r on the diagonal by finding the substitutions that transform col. t into col. t+u, and col. t+r into col. t+u+r. Between the two sets of information we should have enough to reconstruct the diagonal (unless r=13 and as long as the bits of rod are not too incomplete).

[44]

In the present case we can take the columns c, d, f, g, j, k; giving them the numbers 3, 4, 6, 7, 10, 11 instead of the letters, this corresponds to p=3, q=3, t=6, u=4, r=1. In order to get these columns we look at Fig. 35 for suitable hypotheses to work in order to add in the extra columns. These hypotheses enable us to write in extra letters in the Fig. 41a and we continue to write in letters in this figure until we reach a confirmation or a contradiction. Until we reach a confirmation it is as well to differentiate the letters that are certain from the rest. The hypotheses that we actually used were: c into g IQ=SE: g into k XE=ND. After a considerable amount of work our rods look like Fig. 41b. The lines crossed out are ones that have been amalgamated with others. We now think we can start to look for the diagonal, and therefore make up the permutations transforming c into f, d into g, f into j and g into k. The notation is that of p. 19, except that we are mostly unable to complete the brackets, and leave dots.

c into f

```
...DCYQFVJZTAXHIN...SGOPR...KE...LUB...M...W...
```

d into g

```
...KWCM...ANSY...GLIJ...TUQ...DEBXOR...FPZV...H...
```

f into j

```
...QOTK...UHJNGR...BSZW...PFA...CXIM...YD...E...L...V...
```

g into k

```
...IND...(EX)...KF...TYHZ...MQBLJWURG...PA...C...S...O...V...
```

We have now to write the c into f permutation over the d into g permutation, and the f into j permutation over the g into k in such a way that a given letter in ‘c into f’ and in ‘f into j’ stands over the same letter in ‘d into g’ and ‘g into k’. To get a start on this observe the configuration of the ringed letters. This suggests that we arrange the permutations in this way

```
  D C Y Q F V J Z T A X H I N
D E B X O R
  ( Y D )
  ( X E )
```

[45]

This is further confirmed many times, and we get the permutations arranged like this

```
( D C Y Q F V J Z T A X H I N )       M S G O P R
( E B X O R A N S Y G L I J D )     K W C M T U Q

( Y D )   Q O T K     U H J N G R C X I M P F A
( E X )   O T Y H X     I N D M Q B L J W U R G
```

giving us the partial diagonal on a slide of 1

```
...BCSZ...EDNJIHK...LXYTOQRF...WMGAV...UP...
```

Z must be followed either by E, L, W or U. If it is U we get

```
  L U B
F P Z V
```

and the diagonal slide as

(BCSZUPLXYTOQRFEDNJIHKWMGAV)

If Z is followed by L we have the bits

```
 M S G O P R      K E          L U B     W
K W C M T U Q     H        F P Z V
```

to fit together, which we find can only be done like this

```
(KEMSGOPR) (BWUL)          (KEWLUBMSGOPR)
(HKWCMTUQ) (FPZV)  or like this  (HFPZVKWCMTUQ)
```

giving the diagonal slides

```
(EDNJIHK)(...)
(UP)
```

both of which are impossible. If Z is followed by W we have the bits

```
  M S G O P R  K E     W     L U B
K W C M T U Q  H   F P Z V
```

which fit together only as

```
(KEMSGOPR)     (LUBW)
(HKWCMTUQ)     (VFPZ)
```

and as before the $\frac{E}{K}$ configuration makes this impossible. We cannot have Z followed by E because of the impossibility of fitting $\frac{KE}{H}$ onto [FPZV] with E over Z. The diagonal is therefore

BCSZUPLXYTOQRFEDNJIHKWMGAV

[46]

After the previous examples that have been given it is hardly necessary to explain how to get the uprights of the various wheels after this point. The upright of the right hand wheel would be obtained by rearranging our bits of rod, and the middle wheel by the method described on p. 28. With luck we might find other messages on the same day with different L.H.W. positions and so find the L.H.W. upright. In the case that the Umkehrwalze is movable this may be rather tricky, but in such a case there are probably no Stecker, and we should be able to solve other days by single wheel processes, with the known wheels in the R.H.W. position, and hope for the unknown wheels to occur in the M.W. position.

In the example given above the diagonal is actually ABCD… with Stecker. We might have had a hatted fundamental diagonal with Stecker, and of course in such a case we could not have said what the fundamental diagonal was. We should then have had to proceed to try to solve other days keys by spider methods, without diagonal board, and assuming temporarily some arbitrary diagonal as fundamental diagonal, and non reciprocal steckering. With two or three such keys we should be able to find the actual fundamental diagonal by comparison of the steckered diagonal.

[Pages 47–59 missing][21]

[60]

Finding new wheels, Stecker knock-out

So far we have been dealing with the problem of getting out the connections of an entirely new machine, or one for which we know no more than the diagonal. There is another problem, that of finding the connections of some newly introduced wheels, the old wheels, or at any rate some of them, remaining as well; this includes the case of a change of Umkehrwalze.

The most hopeful case for getting out the new wheels is when one of the known wheels occurs in the R.H.W. position. If the machine has no Stecker there is no difficulty. We solve some messages by single wheel processes. This will be slightly more difficult than when we know the connections of the middle wheel, as we shall have to guess what is said in three or four different turnovers. However when the R.H.W. rod start has been found from a guess in one turnover it does not take any time to test a mot probable throughout the messages (the rods on which the various letters of the message occur can be written down once for all, and the mot probable punched out and run over the inverse oblong). For simplicity let us suppose that we have read the message right through. We then have the couplings in several consecutive positions of the middle wheel, and can apply the method of p. 28, 29 to find its upright.

In the case that the machine has Stecker we need rather more data, and very much more patience. The sort of data that one needs is a crib of length about 70, or else one of length 26 and depth 2. The trouble about cribs without any depth is that one uses up a great many of the constatations between each turnover in determining the coupling.

An example is shewn of a crib of length 18 and depth 2. This is to be regarded as one of greater length which has been cut down to allow for turnover. The text of the crib is shown at the top of Fig. 42. We are taking the worst case of 13 Stecker. There are several half-bombes in the crib, and we decide to work with TW. We have to make 17576 different hypotheses, (app) corresponding to the 26 different places on the R.H.W.

[21] Editors' Note: The pages 47 to 59 are missing from the archive copy of the original.

[61]

```
A N T R A N S P O R T C H E F S E E
F G N Y F Z J W I O W D U D L M H D

L I S T Y W E W A V O N W E W A Z E H N
T A D J S B U T U L C M A D T E F D K M
```

```
A |F  I        F |         U |        W |E         | A  G  3
B |               |W          |          |          | B  T  1
C |               |           |O  D      |          | C
D |     S         |           |   C    E |        E | D
E |               |   U       |          D | A  H  D | E  W  1
F |A          A   |           |            L |    Z    | F  O  8
G |   N           |           |          |          | G  A  3
H |               |           |     U    |    E     | H  V  7?
I |   A           |         O |          |          | I
J |       T       |   S       |          |          | J  L  11
K |               |           |          |          | K  M  6
L |T              |           |        V |        F | L  J  11
M |               |           |          |          | M  K  6
N |   G  T        |Z          |          |S         | N  S  4
O |               |         I  R|C         |          | O  F  8
P |               |       W   |          |          | P
Q |               |           |          |          | Q
R |         Y     |           |        O |          | R
S |       D   Y   |   J       |          |M         | S  N  4
T |L      N  J    |           |W         W|          | T  B  1
U |               |   E     A |        H |          | U
V |               |           |        L |          | V  H  7?
W |               |B     P    |T     A   T|          | W  E  1
X |               |           |          |          | X
Y |         R  S  |           |          |          | Y
Z |               |N          |          |    F     | Z
    1  2  3  4  5   6  7  8  9  10 11 12 13 14 15 16 17 18
```

```
M S F U O G L B F H E Y I J K R K M N W B E F H E L   o  1
Z A C Z G H N A P J B G W A C Z T D E F M F H I R W   j

L Q G K M J D N O P W P R S B G J K M J Q R X K Z T   t  1
A C D M R U V X U B C I V K E W B R V X U O Y Z A H   e

R H L N K E O P Q X Q S T C H K L N K R S Y L A U M   u  2  [10?]
Q N H R S T A T V W F K N O Q N U V B O D X P J K O   x

G Z B C L Q T U W T A B H U J D V A Q U W T N X Y Z   d  5  [9?]
O I S T U B U W X G L O P R O V W C P E Y Q V L P R   y
```

Fig. 42. Investigating a correct hypothesis in a Stecker knock-out

[62]

and the possible different ‘Stecker values’ of T and W. Any assumption as to the Stecker values of T and W implies two rod pairings, and when we have set these rods up we can look round and see if there are other Stecker which are consequences of the rod pairings and the Stecker we have already. Any new Stecker we find may allow us to set up more pairs of rods. So we go on until either no new consequences can be drawn (this may be rather frequently the case), or there is a contradiction. If there is confirmation and afterwards we can draw no further consequences it may be worth while bringing in extra hypotheses.

In the actual working it seems best to set the crib out as in Fig. 42, so that the occurrences of any letter can be spotted at once. We write the Stecker values of the letters in pencil on the right possibly on a separate sheet which slips underneath. In order to avoid bogus confirmations we cover up the constatations with shirt buttons as they are used. Fig. 42 shews the working for the correct hypothesis W/E, T/B. The ‘covered’ letters are shewn ringed. In order to shew how the working was done the steps have been numbered, the number being put against the constatation used and also against the Stecker values or rod pairing which resulted. The work as shown is not quite complete. It is possible to go further and get the Stecker values of all letters except D,X. There are six or more confirmations.

There are a number of other possibilities besides working from a half-bombe. It depends largely on the number of Stecker expected which will be the most profitable. When the number of Stecker is low (say 6) it is probably best to try half-bombes as unsteckered and to look for clicks which have all four letters unsteckered.

It seems unlikely that this method will ever be applied, partly because of the difficulty of obtaining the right kind of data. However much the same method could be applied to find a new Umkehrwalze with data of the kind that arises with the air Enigma. One may find the Ringstellung by Herivelismus, and also have a certain number of constatations at known window positions arising from CILLI’s.

[63]

The wheel order may also be known from CILLIs more or less accurately. We now make up rods giving, not the effect of going through the R.H.W. but through all three wheels, and with the columns not corresponding to all possible positions, but to the positions where there are known constatations, and use them instead of the ordinary rods: there is no difficulty about T.O.

[64]

Identification of wheels

When one has found the connections of a wheel one naturally wants to verify that it is not one of the wheels used in some other known machine. A convenient way of doing this is to find the class of substitution which transforms one column of the rod squares into the next (see p 19a). Thus the class of the wheel found on p 26 was 13,8,3,2. This ‘class’ is independent of what point of the rod square we take to be the top left hand corner, and so is an absolute characteristic of the wheel. It even remains the same if the

wheel is used in a machine with a different diagonal. In the case of an Umkehrwalze we can form the class of the substitution consisting of going through the U.K.W. and then sliding one position backwards on the diagonal. A list of characteristics for the known machines is given below.

K Enigma
I. 19,7
II. 14,12
III. 10,8,5,3
U.K.W. 15,9,1,1

Railway machine
I. 24,2; two apart 18,5,2,1
II. 12,8,4,2
III. 14,8,3,1
U.K.W. 24,2

Service machine
I. 13,6,4,3
II. 16,10
III. 7,7,6,6
IV. 11,11,2,2
V. 9,9,6,2
VI. 24,2; two apart 16,5,3,2
VII. 12,5,5,4
VIII. 24,2; two apart 22,4
U.K.W. A. 9,8,4,2,2,1
U.K.W. B. 10,8,7,1
U.K.W. C. 13,9,2,2

Commercial
I. 18,8
II. 19,7
III. 12,9,4,1
UKW. 22,2,1,1