GENERAL REPORT ON TUNNY

With Emphasis on Statistical Methods.

TABLE OF CONTENTS

Part 0

01 Preface

Part 1 INTRODUCTION

11 German Tunny

12 Cryptographic Aspects

13 Machines

14 Organisation

15 Some Historical Notes

Part 2 METHODS OF SOLUTION

21 Some Probability Techniques

22 Statistical Foundations

23 Machine Settings

24 Rectangling

25 Chi-breaking (from Cipher)

GENERAL REPORT ON TUNNY

With Emphasis on Statistical Methods.

TABLE OF CONTENTS

Part 0

01 Preface

Part 1 INTRODUCTION

11 German Tunny
12 Cryptographic Aspects
13 Machines
14 Organisation
15 Some Historical Notes

Part 2 METHODS OF SOLUTION

21 Some Probability Techniques
22 Statistical Foundations
23 Machine Setting
24 Rectangling
25 Chi-breaking (from Cipher)
26 Wheel-breaking (from Key)
27 Cribs
28 Language Methods

Part 3 ORGANISATION

31 Mr.Newman's Section
32 Major Tester's Section
33 Knockholt
34 Registration and Circulation
35 Tape-making and Checking
36 Chi-breaking and Cribs
37 Machine Setting
38 Wheel-breaking (from Key)
39 Language Methods

Part 4 EARLY METHODS AND HISTORY

41 The First Break
42 Early Hand Methods
43 Testery Methods 1942-4
44 Hand Statistical Methods

Part 5 MACHINES

51 General Introduction
52 Development of Robinson and Colossus
53 Colossus
54 Robinson
55 Specialised Counting Machines
56 Copying Machines
57 Simple Machines
58 Photographs
(See also p 337
in section 5-3)

Part 6

61 Raw Materials and Production with Plans of Tunny Links

Part 7* REFERENCE

71 Glossary and Index
72 Notation
73 Bibliography
74 Chronology

Part 8

81 Conclusions

Part 9 APPENDICES

91 5202
92 Motor Rectangles
93 Thrasher
94 QEP Research
95 Mechanical Flags

01 PREFACE (SHOULD BE READ)

The 'General Report on Tunny' is an account of machine and statistical methods for breaking Tunny ciphers. Language methods are briefly described so that the report may be understood without previous knowledge. For a fuller account of language methods the reader should consult the report of Major Tester's Section.

This report is essentially cryptographic and is complementary to the electrical report prepared by Mr. Flowers. Most of the book concerns cryptographic methods in their prime, but there is also a little historical perspective. The plan of the book is as follows:

Part 1 gives a broad outline of the entire subject. This part should be well understood by the reader before he proceeds to the other parts which may then be read in any order.

In Part 2 all methods are described in some detail. The later section (W,X,Y,Z) of each chapter covers advanced theoretical aspects and involve a knowledge of mathematics of at least sixth form standard. These sections may be omitted on a first reading, but give valuable general examples of statistical cryptographic methods.

A description of the other parts is given in the table of contents. It is hoped that the 'Conclusions' may be of value in other sections of the Foreign Office.

The report contains a number of references to the Research Logs of Mr. Newman's Section, (labelled R0, R1, R2, R3, R4, R5) and that of Major Tester's Section (labelled R41). Those references which are not preceded by the word 'see' are intended to be of purely historical interest. The correlation of reference with date is given by the following list:

R0	p 1	15th August, 1943
	26	September
	59	October
	92	November
R1	13	December
	34	January, 1944
	78	February
R2	5	March
	37	April
	60	May
	90	June
R3	5	July
	38	August
	62	September
	83	October
	106	November
R4	35	December
	77	January, 1945
R5	1	February
	33	March
	73	April
	111	May

References to the report itself are of the form 36F(b) which means Part 3, Chapter 6, Section F, Paragraph (b). Formulae are numbered in Arabic numerals by sections (e.g. (26F4) for the 4th formula of Part 2, Chapter 6, Section F), and tables and exhibits are numbered in Roman numerals by chapters (e.g. 26(II)). Section headings are listed at the beginning of each chapter.

The authors wish to thank all who have helped them with the report, and in particular to acknowledge the help they have received from the reports of the Research Section, Major Tester's Section and Sixta which have in many places been quoted verbatim and without further acknowledgement.

PART 1 - INTRODUCTION

11 GERMAN TUNNY

11A Fish Machines
11B The Tunny Cipher Machine
11C Wheel Patterns
11D How Tunny is used
11E The Tunny Network

12 CRYPTOGRAPHIC ASPECTS

12A The Problem
12B Modern Strategy
12C Chi-breaking and Setting
12D Motor and Psi-breaking and Setting
12E Methods involving Key

13 MACHINES

13A Explanation of the Categories
13B Counting and Stepping Machines
13C Copying Machines
13D Miscellaneous Simple Machines

14 ORGANISATION

14A Expansion and Growth
14B The Two Sections in 1945
14C Circulation

15 SOME HISTORICAL NOTES

15A First Stages in Machine Development
15B Early Organisation and Difficulties
15C The Period of Expansion

11 - GERMAN TUNNY.

11A FISH MACHINES.

(a) The Teleprinter Alphabet

Two teleprinters in communication consist of two enlarged electromatic typewriters connected by cable, and constructed so that whatever is typed on either keyboard is printed on both typewriters. When a key is depressed by the sender, the enlarged typewriter sends along the cable one of 32 electrical signals. These signals consist of five consecutive impulses, each of which may be positive (known as DOT) or negative (known as CROSS) and they operate the appropriate key of the receiving typewriter. The 32 signals are known as 'LETTERS' and correspond to the keys on the teleprinter keyboard.

It is clear that the number of keys cannot be greater than 32, and it is in fact 31. However 29 out of 31 keys can have two meanings, one in figure shift and one in letter shift, the remaining two being used to operate the change to letter shift and the change to figure shift respectively.

The following table shows the construction and meanings of the letters in the teleprint alphabet - as laid down by international convention. Figure shift meanings are liable to variation when they have a purely national significance (e.g. £).The order of the letters is specially devised for cryptographic purposes and not conventional.

CONVENTIONAL NAME	IMPULSE 1 2 3 4 5	MEANING IN LETTER SHIFT	IN FIGURE SHIFT
/ occasionally 7	. . . . .	(no meaning)	
9	. . x . .	space	space
H	. . x . x	H	£
T	 x	T	5
O	. . . x x	O	9
M	. . x x x	M	full stop
N	. . x x .	N	comma
3	. . . x .	carriage return	carriage return
R	. x . x .	R	4
C	. x x x .	C	colon
V	. x x x x	V	equals
G	. x . x x	G	@
L	. x . . x	L	close bracket
P	. x x . x	P	0 (zero)
I	. x x . x	I	8
4	. x . . .	line feed	line feed
A	x x . . .	A	dash
U	x x x . .	U	7
Q	x x x . x	Q	1
W	x x . . x	W	2
5 or +	x x . x x	move to FIG shift	(none)
8 or -	x x x x x	(none)	move to LET. shift
K	x x x x .	K	open bracket
J	x x . x .	J	ring bell
D	x . . x .	D	who are you?
F	x . x x .	F	per cent
X	x . x x x	X	/
B	x . . x x	B	?
Z	x . . . x	Z	+
Y	x . x . x	Y	6
S	x . . x . .	S	apostrophe
E	x	E	3

It is worth noticing that the numerals 1,2,3,4,5,6,7,8,9,0 are associated with the keys of the top row of the typewriter keyboard, taken in order from Q (on the left) to P (on the right).

The conventional names 3 4 5 8 9 / have no connection with the meaning or ordinary occurrence of numerals and punctuation on the typewriter keyboard in figure shift, but are just names given to those keys and electrical signals which do not correspond to any of the 26 letters of the ordinary alphabet. For example the transmission by teleprinter of the phrase 'PRICE 3/6' would involve the following electrical signals being sent in order 9PRICE95EXY89. Similarly a full stop is sent as 5M89 and a comma as 5N89.

A teleprinter message can be thought of as a stream of "Letters" corresponding to the keys depressed and the electrical signals sent during transmission.

(b) Five-impulse Tape.

For speed and accuracy in transmission, long teleprinter messages can be 'perforated' in advance and transmitted automatically from five-impulse tape (AUTO) instead of by hand operation of the keyboard (HAND). The tape from which the transmission takes place is made of paper and gives the sequence of signals to be sent, each signal being represented vertically as a set of five impulses with a blank for every dot and a hole for every cross. The tape for 'PRICE 3/6' would look like this

```
                                      ___________________________
1st Impulse                                     o   o o o o o
2nd Impulse                              o o o o     o     o
Sprocket holes (used to drive tape)   . . . . . . . . . . . . . .
3rd Impulse                           o o   o o   o     o o o o
4th Impulse                                o   o     o   o   o
5th Impulse                              o     .     o   o o o
                                      ___________________________

                (conventional name)   9 P R I C E 9 5 E X Y 8 9
```

Similarly the receiving teleprinter can be made to punch a tape, instead of, or in addition to, printing the message when it arrives.

(c) The German Ciphered Teleprinter

During the war in Europe in 1940-5 the Signals Units (FUNKTRUPPEN) attached to German service authorities were issued with a novel type of WT and cipher equipment for communication with Berlin or other Headquarters stations. Receiving and sending teleprinter equipment were used but the electrical signals corresponding to the various teleprinter letters were not normally transmitted from sender to receiver by cable but sent out over the air in ciphered form. Cipher machines (SZ or SCHLUESSELZUSATZGERAETE) were therefore interposed between the sending teleprinter, which converted the message into a sequence of enciphered impulse-signals, and the transmitter which sent the ciphered sequence over the air, and similarly between the WT receiver and receiving teleprinter.

These cipher machines were given (by us) the general cover name of FISH and two particular features should be noticed

(i) the cipher was not directly applied to the message, which was reduced to teleprinter form before being enciphered

(ii) the cipher text was never seen by sending or receiving operator, as no recording device was interposed between cipher machine and WT transmitter or receiver.

(iii) the receiving teleprinter printed on to continuous sticky tape, so that not only / but also 3 (carriage return) and 4 (line feed) did not occur in the unciphered stream. There was no bell.

The equipment of a mobile FISH signal unit was housed in two trucks:

(a) The BETRIEBSWAGEN carried two cipher machines (for sending and for receiving) and teleprinter equipment for sending either from keyboard or from tape, and for receiving and printing. In addition, it carried a device for perforating five-impulse tape from a message by tapping it out on a keyboard.

(b) The SENDUNGSWAGEN carried the WT transmitter.

The WT Receiver was independent of both trucks but carried by them when the unit was not operating.

When in operation Sendungswagen and Receiver were usually placed about ½ mile from the Betriebswagen and connected to it by cable. On occasions when the teleprinters were connected by land line, the Betriebswagen was connected up directly to an exchange board.

At the Berlin end of Fish links and in some other fairly firmly established places (e.g. Paris in 1943), equipment was not arranged on a mobile basis but in a central station or exchange.

Three types of Fish machines are known:

STURGEON (used mainly by the German Air Force)
TUNNY (used mainly by the German Army) which forms the subject of this report.
THRASHER (which is dealt with in ch 9)

11B THE TUNNY CIPHER MACHINE

(a) Addition

FIG 11(I) THE ADDITION SQUARE

	/9HT	OMN3	RCVG	LPI4	AUQW	58KJ	DFXB	ZYSE
/	/9HT	OMN3	RCVG	LPI4	AUQW	58KJ	DFXB	ZYSE
9	9/TH	MO3N	CRGV	PL4I	UAWQ	85JK	FDBX	YZES
H	HT/9	N3OM	VGRC	I4LP	QWAU	KJ58	XBDF	SEZY
T	TH9/	3NMO	GVCR	4IPL	WQUA	JK85	BXFD	ESYZ
O	OMN3	/9HT	LPI4	RCVG	58KJ	AUQW	ZYSE	DFXB
M	MO3N	9/TH	PL4I	CRGV	85JK	UAWQ	YZES	FDBX
N	N3OM	HT/9	I4LP	VGRC	KJ58	QWAU	SEZY	XBDF
3	3NMO	TH9/	4IPL	GVCR	JK85	WQUA	ESYZ	BXFD
R	RCVG	LPI4	/9HT	OMN3	DFXB	ZYSE	AUQW	58KJ
C	CRGV	PL4I	9/TH	MO3N	FDBX	YZES	UAWQ	85JK
V	VGRC	I4LP	HT/9	N3OM	XBDF	SEZY	QWAU	KJ58
G	GVCR	4IPL	TH9/	3NMO	BXFD	ESYZ	WQUA	JK85
L	LPI4	RCVG	OMN3	/9HT	ZYSE	DFXB	58KJ	AUQW
P	PL4I	CRGV	MO3N	9/TH	YZES	FDBX	85JK	UAWQ
I	I4LP	VGRC	N3OM	HT/9	SEZY	XBDF	KJ58	QWAU
4	4IPL	GVCR	3NMO	TH9/	ESYZ	BXFD	JK85	WQUA
A	AUQW	58KJ	DFXB	ZYSE	/9HT	OMN3	RCVG	LPI4
U	UAWQ	85JK	FDBX	YZES	9/TH	MO3N	CRGV	PL4I
Q	QWAU	KJ58	XBDF	SEZY	HT/9	N3OM	VGRC	I4LP
W	WQUA	JK85	BXFD	ESYZ	TH9/	3NMO	GVCR	4IPL
5	58KJ	AUQW	ZYSE	DFXB	OMN3	/9HT	LPI4	RCVG
8	85JK	UAWQ	YZES	FDBX	MO3N	9/TH	PL4I	CRGV
K	KJ58	QWAU	SEZY	XBDF	N3OM	HT/9	I4LP	VGRC
J	JK85	WQUA	ESYZ	BXFD	3NMO	TH9/	4IPL	GVCR
D	DFXB	ZYSE	AUQW	58KJ	RCVG	LPI4	/9HT	OMN3
F	FDBX	YZES	UAWQ	85JK	CRGV	PL4I	9/TH	MO3N
X	XBDF	SEZY	QWAU	KJ58	VGRC	I4LP	HT/9	N3OM
B	BXFD	ESYZ	WQUA	JK85	GVCR	4IPL	TH9/	3NMO
Z	ZYSE	DFXB	58KJ	AUQW	LPI4	RCVG	OMN3	/9HT
Y	YZES	FDBX	85JK	UAWQ	PL4I	CRGV	MO3N	9/TH
S	SEZY	XBDF	KJ58	QWAU	I4LP	VGRC	N3OM	HT/9
E	ESYZ	BXFD	JK85	WQUA	4IPL	GVCR	3NMO	TH9/
	/9HT	OMN3	RCVG	LPI4	AUQW	58KJ	DFXB	ZYSE

Before considering in detail the operation of the Tunny machine it is necessary to define the addition of two teleprinter letters.

Teleprinter letters are added by summing corresponding impulses according to the rules

. plus . equals .
x plus x equals .
. plus x equals x
x plus . equals x

$$\text{Therefore } 9 + Y = \left\{\begin{array}{ccccc} . & & x & & x \\ . & & . & & . \\ x & \text{plus} & x & \text{equals} & . \\ . & & . & & . \\ . & & x & & x \end{array}\right\} = Z$$

From this example it is clear that not only 9 + Y = Z but also that 9 + Z = Y and Y + Z = 9. This is an important result which may be stated in the form of the theorem: Addition and Subtraction of teleprinter letters (or characters) is the same thing. (M1)

Any proof required is left to the reader.

Fig.11 (I) shows an addition square giving the sum of every pair of letters.

(b) Tunny Key

For each letter in turn of the unciphered stream of impulse signals, the Tunny machine makes up a key-letter (K) and adds it to the plain text (P) to get a ciphered letter (Z).

The P-stream can contain any letter of the teleprint alphabet except /, 3, or 4. Of the letters that do occur 9 (space), 5, 8, and E are particularly common . The K-stream, and therefore Z-stream, contains each letter of the teleprinter alphabet approximately an equal number of times.

Example	P-stream	9DIE9SCHOENE9JUNGFRAU9
	K-stream	Y/RAV8BUJL/3KSHV9AICIN
	Z-stream	ZIN4GGQWWWNDJCWLVCMFC3

(c) The Wheels

12 wheels are used to generate the key. Each wheel consists of a pattern of dots and crosses of a given length. Each character moves into the active position in turn, and when the wheel has gone round completely the pattern is repeated. The wheels are divided into three groups with the following names and lengths.

CHI (χ) Wheels	χ_1 length	41	characters
	χ_2	31	
	χ_3	29	
	χ_4	26	
	χ_5	23	
PSI (ψ) Wheels	ψ_1 length	43	characters
	ψ_2	47	
	ψ_3	51	
	ψ_4	53	
	ψ_5	59	
MOTOR or MU (μ) Wheels	μ_{61} length	61	characters
	μ_{37}	37	

The key-letter is the sum of the letter of chi-key (χ) formed by the five characters in the active positions of $\chi_1, \chi_2, \chi_3, \chi_4, \chi_5$, and the letter of psi-key (ψ') formed by the five characters in the active positions of $\psi'_1, \psi'_2, \psi_3, \psi_4, \psi_5$.

(d) <u>Chi-key</u>.

After each letter of the P-stream has been enciphered each chi moves on once. The pattern of characters added to each impulse of the P-stream has a period equal to the length of the corresponding chi-wheel, and since the lengths of these wheels are prime to each other, the stream of letters generated by the chis has a period of $41 \times 31 \times 29 \times 26 \times 23$.

(e) <u>Psi-key</u>.

The motion of the psis is irregular and determined by the motor. After a letter has been enciphered either (i) each psi wheel moves on once and a new letter of psi-key is used for ciphering the next letter or (ii) all five psis remain still and the same letter of psi-key is used again. When (ii) happens there is said to be an extension of the psi-stream. The term EXTENDED PSI (or ψ') stream is used for the actual sequence of letters added by the Psis to the P-stream, and the term ψ-stream for the sequence of letters that the psis would generate if there were no extensions.

<u>Example</u>	P-stream	9 D I E 9 S C H O E N E 9 J U N
	ψ-stream	F L D E Q / K H B 4
	ψ'-stream	F L L D E E E Q / K K H B 4 4 4
	$(P + \psi')$-stream	D 5 H 3 S 9 K A O C A Y X D S C

(f) <u>Motors</u>.

The dots and crosses arranged round the motor wheels do not mean the same as the symbols usually called dots and crosses.

A dot means STOP
A cross means GO.

Mu61 moves on once after each letter is enciphered. When mu61 has a cross in the active position (before moving) mu37 moves on once: when it has a dot in the active position (before moving) mu37 stays still. The character of mu37 in the earlier active position is the active character of the BASIC MOTOR (BM). In other words BM = Mu37 "extended by Mu61" = 'Mu37'.

<u>Example of finding Basic Motor</u>:

```
Mu61:   x . x x x . x x . x x x x x . x x
Mu37:   x . . x . . x x . x . x . . x x .
(a) Number the characters of Mu61 repeating numbers wherever there is a dot:
        x . x x x . x x . x x x x x . x x
        1 2 2 3 4 5 5 6 7 7 8 9 10 11 12 12 13
(b) Number the characters of Mu37 (without repeating)
        x . . x . . x x . x . x . . x x .
        1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
(c) Replace the sequence of numbers given in (a) by their equivalents given by (b).
        1 2 2 3 4 5 5 6 7 7 8 9 10 11 12 12 13
    BM: x . . . x . . . x x x . x . x x .
```

The active character of the Basic Motor - in conjunction with the active character of the LIMITATION determines the character of the TOTAL MOTOR and this regulates the motion of the psis.

The limitation consists of a sequence of dots and crosses such that when there is a Basic Motor dot <u>and</u> a limitation cross in the active position there is a Total Motor dot and the psis do not move. At all other places (e.g. where there is a Basic Motor cross or a Basic Motor dot and an limitation dot) there is a Total Motor cross and every psi moves on once.

<u>Example</u>:	Basic Motor	x . . . x . . . x x x . x . x x .
	Limitation	. x . x x . . x x x . . x x . . x
	Total Motor	x . x . x x x . x x x x x . x x .

(g) Limitations.

The sequence of characters defined in paragraph (f) as the LIMITATION is a byproduct of the other patterns on the machine or in the P-stream, and is not generated independently. Four different methods have been used to produce the limitation and the four different types are defined as follows:

(i) $\bar{\chi}_2$ limitation (known for short as χ_2 lim. or chi 2 lim).
The active character of the limitation at any position is given by the character of χ_2 which was active in the previous position. This is called chi 2 ONE BACK and written $\bar{\chi}_2$.
(NB $\bar{\bar{\chi}}_2$ means χ_2 two back, $\underline{\chi}_2$ means χ_2 one forward etc.)

(ii) $\bar{\chi}_2 + \bar{\psi}_1'$ limitation (known for short as ψ_1 lim or Psi 1 lim).
The active charater of the limitation is given by the sum of the characters of χ_2 and ψ_1' which were active in the previous position.

(iii) $\bar{\chi}_2 + \bar{\bar{P}}_5$ limitation (known for short as P_5 lim.)
The active character of the limitation is given by the sum of the character of χ_2 which was active in the previous position and the character of P_5 which was active two positions previously.

(iv) $\bar{\chi}_2 + \bar{\psi}_1' + \bar{\bar{P}}_5$ limitation (known for short as $\psi_1 P_5$ lim.)
The active character of the limitation is given by the sum of the characters of χ_2 and ψ_1' which were active in the previous position and the character of P_5 which was active two positions previously.

Limitations involving P_5 constitute an "autoclave" since the key stream becomes dependent on the Plain Language.

On the earliest model of the Tunny machine there was "No limitation". This was equivalent to a limitation stream consisting entirely of crosses, so that Total and Basic motors were the same.

(h) A General Example of Ciphering with $\bar{\chi}_2 + \bar{\psi}_1'$ limitation.

(i)	P:	9	I	M	9	K	A	M	P	F	9	G	E	G	E	N	9	(given)
(ii)	χ:	U	O	8	X	X	R	J	Y	W	C	R	/	E	Q	L	3	(given)
(iii)	ψ:	N	L	D	E	Q	/	K	H	B	4							(given)
(iv)	BM:	.	.	x	x	.	.	x	.	x	.	x	x	.	.	.	x	(given)
(v)	χ_2:	x	.	x	.	.	x	x	.	x	.	x	.	.	x	x	.	(from ii)
(vi)	$\chi_2+\psi_1'$:	x	.	x	x	x	.	.	x	x	x	.	.	x	x	x	.	(from v and x)
(vii)	$\bar{\chi}_2+\bar{\psi}_1'$:	.	x	.	x	x	x	.	.	x	x	x	.	.	x	x	x	(from vi)
(viii)	TM:	x	$\underline{.}$	x	x	$\underline{.}$	$\underline{.}$	x	x	x	$\underline{.}$	x	x	x	$\underline{.}$	$\underline{.}$	x	(from iv and vii)
(ix)	ψ':	N	$\underline{L}$	$\underline{L}$	D	$\underline{E}$	$\underline{E}$	$\underline{E}$	Q	/	$\underline{K}$	$\underline{K}$	H	B	$\underline{4}$	$\underline{4}$	$\underline{4}$	(from iii and viii)
(x)	ψ_1':	.	.	.	x	x	x	x	x	.	x	x	.	x	.	.	.	(from ix)
(xi)	$K = \chi+\psi'$	J	R	F	H	M	J	R	4	W	Q	S	H	C	Y	T	R	(from ii and ix)
(xii)	$Z = P+K$:	K	N	Z	T	W	3	P	H	V	W	8	Y	4	H	M	C	(from i and xi)

Note that the ψ'(ix) depends on (vi) which depends on a character in ψ' at a previous place. ψ' therefore depends on its own recent past and can only be constructed letter by letter. Only when the 4th letter of ψ' is known can we tell if there is an extension in the ψ from the 5th letter to the 6th, and so determine the 6th letter for certain. When this is known, and only then, can we start to find out if the ψ is extended from the 7th to the 8th letters, and so on.

The underlinings in the example show the relation between Total Motor dots and psi extensions.

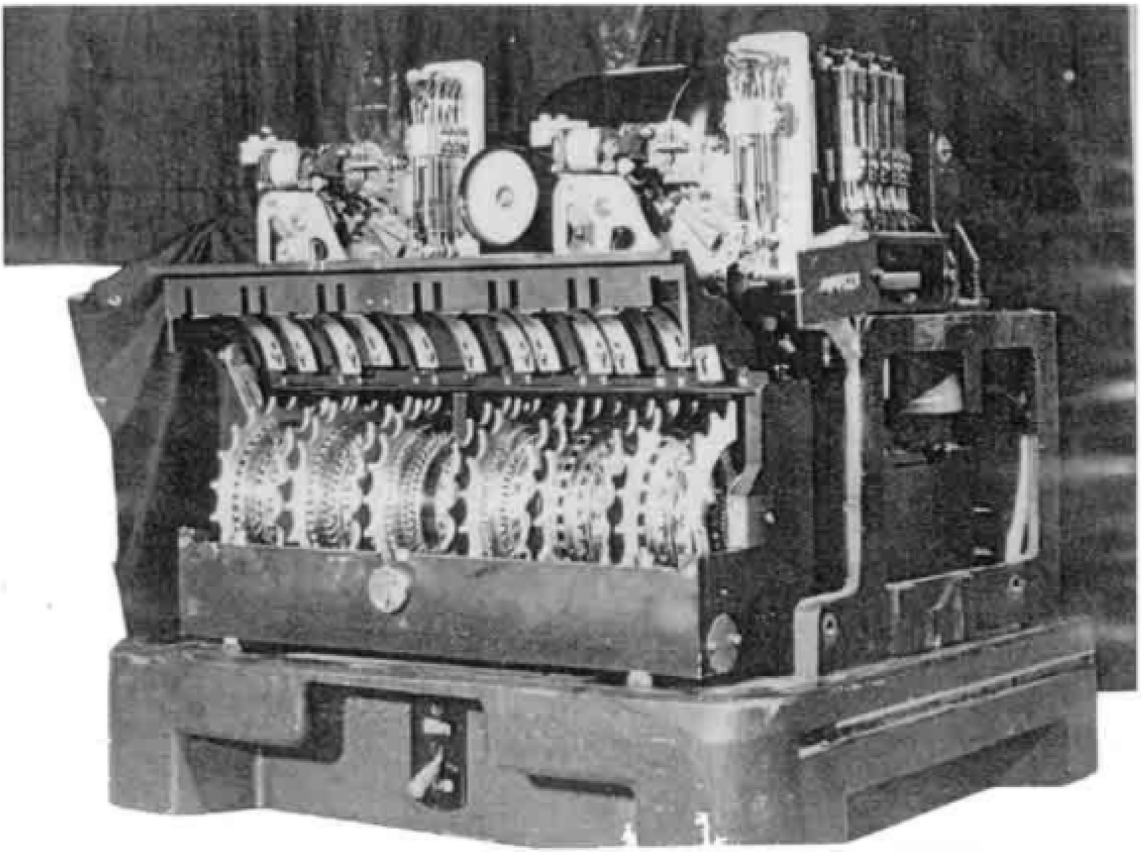
(i) Functional Summary

The action of the Tunny machine at any given position is most easily expressed by the formula

$$\left.\begin{aligned} Z &= P + K \\ K &= \chi + \psi' \end{aligned}\right\} \qquad (A2)$$

TUNNY MACHINE

Fig 11.(11)



It follows at once from (A1) that

$$K = P + Z$$
$$P = Z + K \qquad (A3)$$

and

$$Z + P + \chi + \psi' = / \qquad (A4)$$

This shows that ciphering and deciphering both involve adding the key, and are in fact the same process, as long as P_5 is not involved in the limitation. When P_5 is involved, the limitation must be taken from the output when enciphering and the input when deciphering.

(j) Mechanical Aspects.

Three models of the Tunny machine are known:

SZ 40 (1940) with no limitation
SZ 42A (1942) with χ_2 or $\chi_2 P_5$ lim.
SZ 42B (1942) with $\chi_2\psi_1$ or $\chi_2\psi_1 P_5$ lim.

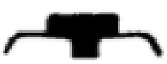
Apart from the limitation difference the models differ very little in construction.

Fig.11 (II) shows a photograph of a German Tunny machine captured after the surrender. The machine is shown without its metal covering, stands on a metal base of dimensions 19 inches x $15\frac{1}{2}$ inches, and has an overall height of 17 inches.

The 12 wheels appear in the picture with their German number painted above them. From left to right these wheels are

German name	1	2	3	4	5	6	7	8	9	10	11	12
British name	ψ_1	ψ_2	ψ_3	ψ_4	ψ_5	μ_{37}	μ_{61}	χ_1	χ_2	χ_3	χ_4	χ_5

The patterns of dots and crosses on each wheel is set up by means of a series of cams which may be either operative or non-operative, according to whether they are placed in a vertical position (NOCKE) or an oblique position (KEINE).



Operative
NOCKE

Non-operative
KEINE

In the photograph, the cams are most easily seen on χ_2 (Wheel 9) and χ_4 (Wheel 11).

On the front of each wheel can be seen a series of numbers, one of which (seen through a window which is not shown) denotes the wheel position. German wheel numbering and British wheel numbering are arranged in opposite direction so that successive active positions are numbered by the Germans in reverse order.

The addition of chis and psis is arranged electrically. The motorising is mechanical.

(k) Switching on and Switching off.

The machine can be switched in and out of the circuit by moving the switch at the bottom to EIN or AUS. When the switch is at AUS, the teleprinter mechanism is wired direct to the W/T transmitter or receiver. When the machine is switched on, the wheels are reset at positions which are used for ciphering the first letter of the transmission. Before the second letter is ciphered all wheels move on once (irrespective of motor and limitation) and between the ciphering of the second and third letters the psis move normally but μ_{37} always moves. After that, the machine moves in the normal way.

(a) German Precautions

Though the Germans never fully appreciated the weaknesses of the Tunny machine, they were alive to some of the more elementary pitfalls. In particular they took care to construct wheel patterns so that

(1) there were not too many extensions of the psis.

(2) there was an equal number of dots and crosses in each impulse of the chi-stream and the extended psi-stream.

(3) the sum of consecutive characters in each impulse of the chi-stream and the extended psi-stream was dot and cross with equal frequency.

(b) Differenced and Undifferenced Wheels.

The letter (or character) obtained by adding any letter (or character) to its successor is known as the differenced or delta (Δ) letter (or character) e.g.

$$\Delta P = P + \underline{P}$$

$$\Delta \chi = \chi + \underline{\chi}$$

$$\Delta \Psi_3' = \Psi_3' + \underline{\Psi_3'}$$

A differenced wheel pattern is obtained by adding each character in a wheel pattern to its successor, and will clearly have the same period as the undifferenced pattern:

```
 χ4 pattern :   ' . . x x . x . x x x . . x . . x x . . . x . . x x x
Δχ4 pattern :    . x . x x x x . . x . x x . x . x . . x x . x . . x
```

It will be readily seen that the number of crosses in the differenced wheel pattern is equal to twice the number of 'groups' of crosses (or dots) in the undifferenced pattern and is therefore even.

(c) Constructions of Wheel Patterns.

Conditions (2) and (3) above were fulfilled as far as the chi-stream was concerned by the rule that the number of crosses in each χ and $\Delta\chi$ pattern should be (as nearly as possible) half the length of the wheel.

The number of crosses in all undifferenced Ψ patterns was also made (as nearly as possible) half the length of the wheel. When the psi was extended, the extension produced additional dots or crosses and the proportion was preserved.

The case of the differenced Ψ patterns is different. At every extension, a letter of the Ψ' stream is repeated and therefore there is a stroke in the $\Delta\Psi$ stream. A dot is therefore added to each impulse of the $\Delta\Psi'$ stream at each extension, and therefore, in order to preserve an equal number of dots and crosses in each impulse of the $\Delta\Psi'$ stream (after extension) there must be a preponderance of crosses in each $\Delta\Psi$ pattern (before extension).

(d) The Law $ab = \frac{1}{2}$

The proportion of crosses in the TM stream is called a.
The proportion of crosses in each $\Delta\Psi$ pattern is called b.

The Germans wished to ensure that the proportion of dots and crosses in each impulse of the $\Delta\Psi'$ stream was (if possible) equal to $\frac{1}{2}$.

Now, at TM dots, there is an extension in the $\Delta\Psi'$ and therefore a stroke. So a cross in any impulse of $\Delta\Psi'$ must occur against a TM cross.

In each impulse, TM crosses occur a proportion a of the time, and at a proportion b of TM cross positions there is a $\Delta\Psi$ cross. Therefore proportion of crosses in each impulse of $\Delta\Psi'$ stream = ab.

By choosing suitable patterns for psis and motors it can always be arranged (and after March 1942 nearly always was arranged) that ab was as nearly as possible $\frac{1}{2}$ in each impulse.

(e) Dottage

The dottage (d) is defined as the number of dots in the pattern of μ_{37}.

Then proportion of dots in $\mu_{37} = d/37$. This proportion will be unchanged by the extension of μ_{37} by μ_{61}.

Therefore proportion of dots in BM = d/37

But proportion of crosses in limitation = $\frac{1}{2}$ (approx)

Therefore proportion of dots in TM = d/74

Therefore a = proportion of crosses in TM = $\frac{74 - d}{74}$

$$b = \frac{1}{2} \times \frac{74}{74 - d} \qquad = \frac{37}{74 - d}$$

The $\Delta\Psi_1$ pattern must therefore be constructed with the nearest even number to $\frac{43.37}{74 - d}$ crosses (and so on.)

For SZ 40 with no limitation the calculation is slightly different and left to the reader.

(f) Values of a, b, d

In known wheel patterns (for SZ 42A and SZ 42B)

d varies from 14 to 28
a varies from .81 to .62
b varies from .62 to .81 so that psi extensions occur from 2/5 to 4/5 of the time.

(Wheel characteristics are discussed more fully in Chapter 22)

11D HOW TUNNY IS USED.

(a) Fish Links

Tunny machines worked in pairs, and each pair formed a link which was given (by us) the name of a fish e.g. in May,1944:

JELLYFISH connected STRAUSBERG exchange (near BERLIN), with HEERESGRUPPE D and [redacted] WEST at PARIS.

WHITING connected KOENIGSBERG exchange with HEERESGRUPPE NORD at RIGA

The units to which links were connected remained pretty stable, but the position first of the army groups and later of the exchanges became increasingly mobile after the invasion. This aspect of Tunny is discussed in 11E

It is obvious that two Tunny machines transmitting to each other must generate identical key streams and must therefore

(i) have the same pattern of dots and crosses round their wheels

(ii) have the patterns set in the same position at the start of each transmission. After this the motors and limitation will act identically at both ends and the machines should always be in step, their motion being synchronised by electrical signals transmitted before and after each teleprinter letter.

Different sets of wheel patterns (GRUNDSCHLUESSEL) and different books of settings (SPRUCHSCHLUESSELSAETZE) were used on each link.

It was usual (though not invariable) for all four machines used on a given fish link to be of the same type. The rule was broken particularly when spare machines were brought into use. For a long time for example on Gurnard

Berlin transmitted and Zagreb received on SZ 42B (psi 1 lim.)
Zagreb transmitted and Berlin received on SZ 42A (chi 2 lim).

(b) Transmissions

Tunny operators can transmit to each other either in cipher or in clear according to whether the Tunny machine is switched IN or OUT, and either in HAND or in AUTO. If sending and receiving machines were working simultaneously, transmission is described as DUPLEX, otherwise as SIMPLEX.

After Oct.1942 the normal routine was somewhat as follows: The operator sits at the keyboard of the sending teleprinter with the printer of the receiving teleprinter directly in front of him. He makes contact with the operator at the other end by hand transmission in clear, and may carry on a brief conversation in Q-code to ensure that conditions are satisfactory for cipher transmission.

Before the Tunny machine is switched in, the operator sets the wheels to the settings opposite the next number in the QEP book and transmits QEP followed by the last 2 figures of the number. Just before switching in he transmits UMUM in clear.

After the machine is switched in, all outgoing transmission is in cipher. Further chat by the operator may be answered in clear, or, if the receiving Tunny is also switched in, in cipher. The text of the operator's chat (clear or cipher) is received on the printer but not preserved.

As soon as the operator is ready to transmit his message (which should have been previously perforated) he switches in the auto transmitter and ceases to operate the keyboard. The message starts with an address and serial number and as it is received it is stuck on a message form by the receiving operator.

The transmission of a complete tape is usually followed by operators' chat in hand and then mixed hand and auto transmission while the sender tries to discover if the message has arrived in comprehensible form, makes any necessary corrections, or retransmits any part of the tape. When the receiver is satisfied, he sends a receipt in clear or cipher according to whether his outgoing Tunny is switched in or not.

After the receipt, the sender may switch off or send another message before resetting. One transmission therefore may contain several serial messages. On the other hand, very long message tapes may be transmitted partly in one QEP and partly in the next, and resetting may also take place during a message if something goes wrong.

(c) Repetition of P

Hand transmission is by no means continuous and a PAUSE implies that the operator has stopped to think or is waiting for the other operator to reply.

Pauses in auto may also occur. Sometimes two tapes are transmitted without any intervening hand transmission, and there is a pause while the new tape is inserted. More frequently, something goes wrong and auto transmission has to be stopped and restarted. When this happens the tape is moved back so that the last 100 letters are retransmitted. In the decode, therefore, 100 letters or so will be repeated. This repeat of P is known as a GO-BACK.

When the pause is accompanied by the resetting of the wheels and the transmission of a new QEP number, the tape is still set back so that the last 100 letters or so of the P of one transmission are reciphered at the beginning of its successor. This is know as an OVERLAP.

(d) Depths

Each QEP number, and each QEP list, should only be used once. However sometimes the same QEP number and settings are used for two (usually consecutive) transmissions. As long as a limitation involving P_5 is not being used the key generated will be the same for both transmissions and they will be in DEPTH.

If the Tunny machine is switched out and a new transmission started without resetting, there is said to be a FOLLOW-ON. 11B (k) shows that the decodes of the two parts of a follow-on will be divided by two blanks for which nothing will have been transmitted.

(e) Change of keys

Once a day (usually between 0600 and 1200), some or all of the wheel patterns are changed. The sender sends out QZZ (usually in clear) and this tells the receiver that he is changing over to the new day's patterns, and that the receiver's incoming Tunny must also be changed.

Before Summer 1944 motor patterns were changed daily but chi patterns were changed monthly and psi patterns monthly or quarterly (see 11E(a)). During the summer changes became more frequent, and after August 1st there was a daily change of all wheel patterns on all links.

Wheel patterns were issued for a month at a time. A day's wheel patterns - as issued - are shown in Fig.11 (III) where + = Nocke and O = Keine.

11E THE TUNNY NETWORK

(a) The period of experiment.

The Tunny machine (SZ40 with no limitation) made a first and experimental appearance in June 1941 on the link Berlin - Athens - Saloniki. At first it was used crudely enough.

(i) Wheel patterns were not chosen so that ab = ½, and there was a regular excess of dots over crosses in the $\Delta\Psi'$ stream.

(ii) The QEP indicating system had not been introduced and wheel settings were chosen by the sender, and sent out in a simple substitution of letters for settings which changed every month and was different for each wheel.

(iii) Motor patterns were changed daily, chi patterns monthly, and psi patterns every three months.

(iv) The machine was not wired to a tone transmitter, but the cipher text was recorded and sent by facsimile (Hellschreiber).

Until October, 1942 there was still only one Tunny link, but the procedure gradually improved with the introduction of ab = ½ and of Tone Transmission before March, 1942.

The replacement of the single link by two links - Codfish from Berlin to Saloniki, and Octopus from Koenigsberg to South Russia - using the QEP system and with monthly change of chi and psi patterns signified the end of the German experimental period and the start of the general expansion of the Tunny system.

(b) The period of expansion

SZ42A was first introduced on Codfish in February 1943, and gradually replaced SZ40 on all links.

SZ42A was fitted with a P_5 attachment which was used experimentally on Herring (Rome-Tunis) in March 1943, but only made a general appearance after December 1943 on Western European links.

At the time of the allied invasion of the continent in 1944, Tunny had reached its most widespread and stable level of organisation. There were 26 links and two main central exchanges.

STRAUSSBERG near Berlin - the terminus for the 9 Western links and KOENIGSBERG the terminus for the 10 Eastern links.

The exchanges were connected by a further link (DACE) and there were 6 cross country links.

(c) The period of Flux

From July 1944 - May 1945, the organisation of the Tunny network became increasingly disorganised as German Army units and even German Headquarters stations moved to new positions. Nearly all links had their terminus moved to new exchanges as Zossen near Berlin between July 1944 and October 1944. When Berlin was threatened part of these exchanges moved first to Erfurt then back to Berlin, and ultimately (by the end of the war) to Salzburg. Charts showing the Tunny network at various times in 1944-5 are given in Part 6.

Cipher security was tightened up in the summer of 1944 and by August 1st a daily change of all wheel patterns had been introduced on each link. SZ42B was first used on Codfish in June 1944 and about half the Tunny links were issued with this machine. At first it was used (=SZ42A was then used) with the P_5 limitation switched in (i.e. on Ψ_1, P_5 lim) but later it was decided that the P_5 attachment on both machines gave more trouble than it was worth, and it dropped out of use from September 1944 onwards.

By May 1945 the German Army was in a state of complete disorganisation and the last Tunny message was sent on 8th May, 1945

For practical, if not logical, simplicity it will be found that P, K, Ψ', D and Z are sometimes used to refer not to any specific letter in the active position but to the whole of the stream concerned.

Further, now that the distinction between a message and a transmission has been carefully drawn, it will be convenient to refer to each of these as a message. This practice is in accordance with traditional usage and agrees with that found in the Research Logs and other contemporary Tunny documents. The exact meaning will usually be clear from the context.

(b) Wheel-breaking and Setting.

Cryptographic work on Tunny falls into two parts

(i) The recovery of wheel patterns or WHEEL-BREAKING
(ii) The recovery of message settings or SETTING.

The theoretical basis of wheel-breaking and setting is very similar, and for every method of setting there is a corresponding method of wheel-breaking which uses more traffic and more information.

Normal practice is therefore to select the most promising material enciphered on a given set of wheel patterns and to use this for wheel-breaking. When the wheel patterns are known, they can then be used for setting other messages enciphered on them.

It will be noticed that it is possible to determine

(i) relative but not absolute settings
(ii) wheel patterns of corresponding chis and psis (e.g. χ_4 Ψ_4) only with the proviso that dots and crosses may be interchanged on both wheels. This does not apply if one of the wheels is involved in the limitation.

(c) Weaknesses of Tunny.

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

12 CRYPTOGRAPHIC ASPECTS.

12A THE PROBLEM

(a) Formulae and Notation.

In Chapter 11 we have defined P, K, χ, Ψ', and Z as the letter of plain language, key, chi, extended psi and cipher streams in the active position, P and so on as their predecessors, $\underline{P}$ and so on as their successors and $\Delta P = P + \underline{P}$ etc.

Before discussing the cryptographic aspects of the Tunny machine it is necessary to restate the formula of the machine.

$$Z = P + K$$
$$K = \chi + \Psi'$$

and to list the following relevant variants, D (or DE-CHI) being defined as the sum of Z and χ streams.

$$Z = P + K = D + \chi$$
$$K = P + Z = \chi + \Psi'$$
$$D = Z + \chi = P + \Psi'$$

For practical, if not logical, simplicity it will be found that P, K, Ψ', D and Z are sometimes used to refer not to any specific letter in the active position but to the whole of the stream concerned.

Further, now that the distinction between a message and a transmission has been carefully drawn, it will be convenient to refer to each of these as a message. This practice is in accordance with traditional usage and agrees with that found in the Research Logs and other contemporary Tunny documents. The exact meaning will usually be clear from the context.

(b) Wheel-breaking and Setting.

Cryptographic work on Tunny falls into two parts

(i) The recovery of wheel patterns or WHEEL-BREAKING
(ii) The recovery of message settings or SETTING.

The theoretical basis of wheel-breaking and setting is very similar, and for every method of setting there is a corresponding method of wheel-breaking which uses more traffic and more information.

Normal practice is therefore to select the most promising material enciphered on a given set of wheel patterns and to use this for wheel-breaking. When the wheel patterns are known, they can then be used for setting other messages enciphered on them.

It will be noticed that it is possible to determine

(i) relative but not absolute settings
(ii) wheel patterns of corresponding chis and psis (e.g. χ_4, Ψ_4) only with the proviso that dots and crosses may be interchanged on both wheels. This does not apply if one of the wheels is involved in the limitation.

(c) Weaknesses of Tunny.

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

A typical operation in Tunny breaking consists in using these characteristics to separate out a stream of letters (such as a K-stream) into its component streams (e.g. χ and Ψ'). This may be described as the solution of an equation; in the example quoted the equation is $K = \chi + \Psi'$.

Several equations of this form are soluble given streams of sufficient length. In some cases the solution is a job for a linguist, in others for statistician, and mechanical aid may or may not be required.

(d) Early methods.

In the early days comparatively simple hand methods of analysis were possible. Before the QEP system was introduced indicators could be used not only to set messages on one or more wheels (when the substitution equivalents were known) but also to recognise depths and near-depths (messages with common settings on nearly all wheels) and even to break wheel patterns. With depths, near depths and partly set messages, the plain language could sometimes be inferred and a stretch of key obtained.

This key could be easily analysed as long as $ab \neq \frac{1}{2}$

$$K = \chi + \Psi'$$
$$\therefore \Delta K = \Delta\chi + \Delta\Psi'$$

For when, $ab \neq \frac{1}{2}$ there is a surplus of dots over crosses in each impulse of $\Delta\Psi'$, and therefore it is immediately possible to deduce the pattern (or setting) of any $\Delta\chi$ from a long enough stretch of that impulse of Δkey.

These methods are described in some detail in Part 4, but the bulk of this report is designed to show the more complex methods required when wheels and indicating system were constructed so as to invalidate the more simple-minded approaches. In the pages that follow it is assumed that $ab = \frac{1}{2}$, and that indicators give no information about the settings used. All methods described, apply to the Tunny machine with limitation; the only simplifications which are possible for Tunny with no limitation are trivial and easily deduceable.

12B MODERN STRATEGY

There are three main methods of Tunny analysis each of which can (in suitable cirumstances) be used for wheel-breaking or setting. The stages by which Z is broken down into χ, Ψ', P and Motors in each method are shown diagramatically in fig.12(I) and listed below.

(a) 1st Method.

Stage I. Solution of $Z = \chi + D$. Various χ-patterns (or settings) are tried mechanically and the correct one is distinguished by the statistical properties of ΔD.

Stage II. Solution of $D = P + \Psi'$. This is a hand job for a cryptographer who can recognise plain language and extended psi stream. Ψ - patterns (or settings) follow at once from the Ψ' stream.

Stage III. Solution of motor patterns (or settings), by hand from the extended psi-stream.

This method is the general method of wheel-breaking and setting when the motors are not known and Stage III is still in progress. The use of the method is limited by the minimum length required to obtain reliable chi-patterns or settings in Stage I. For chi-breaking the minimum length is about 4,000 and for chi setting about 1000 letters

(b) <u>2nd Method.</u>

Stage I. Mechanical solution of $Z = \chi + D$ as in 1st method.

Stage II. Solution of motor patterns (or settings) from ΔD stream by statistical and mechanical means.

Stage III. Solution of $D = P + \Psi'$. Ψ' streams corresponding to the various possible Ψ patterns (or settings) are tried mechanically, the correct one being distinguished by the statistical recognition of P. It will be noticed that this is only possible after the motors have been broken (or set).

This method is entirely mechanical and, as soon as there were sufficient machines available, it became the general method of setting as soon as the motor patterns were found. This method was used for wheel-breaking, but only experimentally. For this reason the statistical breaking of motor patterns from ΔD is discussed in the Appendix (92) and not in Part 2. The minimum length required for wheel-breaking and setting is rather greater than that required in the first method.

(c) <u>3rd Method.</u>

Stage I. Solution of $Z = K + P$ by means of depth or crib. Plain language for two messages in depth found by hand or a predetermined stretch of P is mechanically tried in various positions of Z and the correct position distinguished by the statistical properties of ΔK.

Stage II. Solution of $K = \chi + \Psi'$. Various χ-patterns (or settings) are tried by hand or mechanically and the correct one is distinguished by the statistical properties of $\Delta\Psi'$.

Stage III. Solution of motor from Ψ' as in 1st method.

This method (as far as depths are concerned) is the only method needing no machine help. Before the introduction of autoclave and the arrival of machines it was the general method of wheel-breaking and setting. Depths remained an important method of wheel-breaking on links without autoclave, though depths for setting became increasingly rare. Cribs provided a useful subsidiary method of wheel-breaking on all links. At least 100 letters of key were required for wheel-breaking.

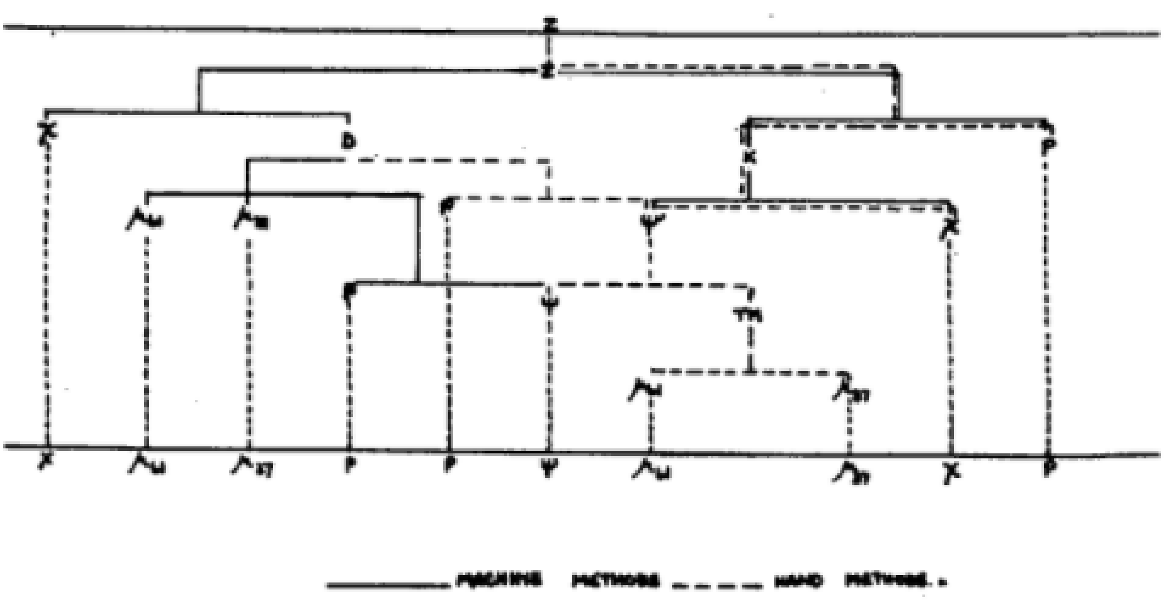


Fig 12(I).

12C CHI BREAKING AND SETTING Solution of $Z = \chi + D$.

(a) Frequency of letters in $\Delta\Psi'$

The precautions taken by the Germans in the construction of wheel patterns produce χ, $\Delta\chi$, and Ψ' streams in which each letter occurs an approximately equal number of times. But though the arrangements for $\Delta\Psi'$ produce an even distribution of dots and crosses in each impulse separately, the fact that there is a dot on every impulse wherever there is an extension and a preponderance of crosses in other places, produces a $\Delta\Psi'$ stream in which

wherever there is a TM dot there is a stroke

wherever there is a TM cross the frequency of the various letters in $\Delta\Psi$ depend on the number of crosses in them.

It can easily be seen that the proportion of TM dots (which = 1-a) and the frequency of crosses in each impulse at TM cross positions (which = b) both increase with the dottage. Fig.12(II) gives a $\Delta\Psi'$ count on a day with 26 dots in μ_{37}.

(b) Frequency of letters in ΔP.

The number of occurrences of each letter in ΔP are by no means equal. The frequent repetition in P of groups of letters common in punctuation or German language like 59M889 or 9M89 (full stop) EI, EN N9, SCH and so on naturally implies the frequent repetition in ΔP of their differenced equivalents /UA/5, UA5, U, P,3, JG. Therefore letters like 5 and U which come from popular bigrams in P are frequent in ΔP. Typical P and ΔP counts are given in fig.12(II).

(c) Frequency of letters in ΔD.

We now consider what happens in $\Delta D = \Delta P + \Delta\Psi'$. Wherever $\Delta\Psi'$ is a stroke, ΔP will be reproduced in ΔD, since any letter added to stroke is unchanged. Therefore the shape of the ΔD count at those places where there are TM dots is identical with the shape of the count of ΔP. In other places every letter in ΔD will occur an approximately equal number of times (though the combination of letters common in ΔP and in $\Delta\Psi'$ against BM crosses will make some letters rather stronger than the others). A ΔD count can therefore be regarded as a watered down version of the ΔP count at the back of it.

```
Example     P:  9 I M 9 K A M P P 9 G E G E N 9
           ΔP:  4 G O J N 8 R 5 D V 5 5 5 P 3
           ΔΨ': 8 7 5 3 7 7 P Q K / 5 7 7 V 7
           ΔD:  X G A A N 8 M N I V / 5 5 W 3
```

As the μ_{37} dottage increases and therefore also the proportion of strokes in $\Delta\Psi'$, the proportion of ΔD count derived directly from ΔP count increases, and the ΔD count from a given ΔP count will be correspondingly stronger.

(d) Chi Setting.

It has been shown that ΔD = not only $\Delta P + \Delta\Psi'$ but also $\Delta Z + \Delta\chi$. If we know the wheel-patterns, we can (in theory) set the chi wheels to every possible combination of settings in turn and generate all the $\Delta\chi$ sequences corresponding to the χ streams with which the transmission could have been enciphered. These can be added to the ΔZ and all possible ΔD's obtained. The counts of letter frequency in all these possible dechis will be more or less level, except the counts of the correct dechi which will follow the pattern described in the last paragraph. If the correct count shows the characteristics of a ΔD count strongly, it will be easily identified, and the chi settings will be found without any doubt even though the original chance that any particular set of settings is correct is as small as 1 in 41x31x29x26x23, that is 1 in 22 million.

Fortunately it is not necessary to try out every combination of chi settings individually. We can count the combined frequency of O and M say, without knowing (or bothering) where chi 3 is set, by counting the number of positions where ΔD1 is a dot, ΔD2 a dot, ΔD4 a cross, and ΔD5 a cross. Therefore using the combined counts of O and M and of other pairs of letters differing from each other only on the third impulse we can set chi 1, chi 2, chi 4, and chi 5, and then go back later to chi 3.

When attempting to set a message we normally start with the '1+2 BREAK IN'. We count the ΔD1 + ΔD2 = dot, that is the combined frequency of the letters /9HT OMN3 AUQW 58KJ, most of which occur frequently in ΔD. On a correct de-chi the count of these 16 letters should be well above the count of the other 16 letters for which ΔD1 + ΔD2 = x. On a de-chi at incorrect settings the combined frequency of any 16 letters should be about half the total number of letters counted. So by counting possible de-chis on the first two impulses only, at the 41x31 = 1271 possible settings for chi 1 and chi 2, we can probably set these wheels. Then, by counting the frequency of other suitably chosen sets of letters we can set the other chis in turn (either singly or in pairs). It is not necessary to set all chis simultaneously.

Even so, the counting of the 1271 possible Δ de-chis on the first two impulses and other similar operations are not jobs which could be undertaken by hand. The COLOSSUS is a machine which has been devised to do these jobs at high speeds. It can be made to record the answers only at such settings as are likely to be correct. A ROBINSON is a more general machine which can be used for the same purpose.

If a transmission is too short then the correct ΔD count will not stand out sufficiently from the others to make the settings certain. When the language is moderately good the minimum length required are very roughly as shown in the following table (d is the dottage of Λ_{st}).

d	15	18	21	24	27
Rough minimum	6200	4000	2400	1700	1200

*These figures have a very large probable error.

(e) Chi Breaking.

If there is a very strong ΔD count for a given transmission it is possible not only to select the settings used for making the correct $\Delta\chi$ stream if the wheel patterns are known, but to determine the patterns of the wheels themselves if they are not known. This is equivalent to selecting the correct ΔD count from the series of letter counts made with ALL POSSIBLE wheel patterns, and can often be done even though the original chance that any set of wheel patterns is correct is 1 in 2 to the power of (41+31+29+26+23) = 1 in 2^{150} = 1 in 10^{45}. (in fact the figure 10^{45} is an overstatement, as the Germans impose restrictions on themselves in the choice of wheel patterns which reduce the figure to about 10^{38}. (See 25X)

The 1+2 RECTANGLE which is made on Colossus or Garbo and CONVERGED by hand is a means of finding the patterns of $\Delta\chi_1$ and $\Delta\chi_2$ which maximise the number of letters of ΔD in which ΔD1 + ΔD2 = dot. The extent to which this frequency can be made to exceed $\frac{1}{2}$ when the optimum patterns have been chosen, determines (a) how much relation the optimum patterns are likely to have to those really used and (b) whether it is worth while to attempt to use the most reliable characters in the optimum pattern for setting other messages enciphered on the same wheel patterns or as a start for COLOSSUS WHEEL-BREAKING. In Colossus-wheelbreaking attempts are made to find the deltaed patterns of all the chis which will lead to the strongest ΔD count.

Unless there is a transmission of over 4000 letters it is unlikely that the optimum $\Delta\chi_1$ and $\Delta\chi_2$ will be strong enough to be in any way significant and therefore chi-breaking by means of the rectangle will be impossible.

Fig 12 (II) Some Typical letter counts.

	P	ΔP	Ψ′	ΔΨ′	ΔD	χ	Z	
/	4(a)	91	118	1159	128	98	110	/
9	544	78	107	4	127	99	81	9
H	67	82	97	17	128	99	94	H
T	123	56	108	4	98	101	124	T
O	89	121	107	18	128	101	108	O
M	180	69	100	47	105	106	89	M
N	212	66	98	7	78	95	95	N
3	1(a)	157	99	2	118	101	114	3
R	159	77	87	11	87	105	110	R
C	44	73	84	53	84	98	105	C
V	21	64	100	153	80	99	89	V
G	94	127	109	32	125	114	93	G
L	87	76	85	17	98	118	104	L
P	51	90	116	47	99	110	123	P
I	137	50	121	10	94	89	87	I
4	3(a)	52	79	5	71	105	93	4
A	161	136	96	13	96	90	82	A
U	81	224	109	52	148	103	99	U
Q	23(b)	79	103	186	92	97	88	Q
W	38	67	108	52	70	114	104	W
5	200	326	106	160	170	108	106	5
8	197	144	75	572	101	107	112	8
K	60	45	106	154	66	99	95	K
J	6	194	96	46	115	96	77	J
D	71	83	91	14	71	91	85	D
F	42	156	103	56	107	83	104	F
X	1	83	79	168	87	93	106	X
B	57	32	111	47	55	104	101	B
Z	26	65	81	13	81	103	108	Z
Y	7	84	94	62	88	95	106	Y
S	110	90	121	14	109	75	110	S
E	304	63	106	5	96	104	98	E
Total	3200	3200	3200	3200	3200	3200	3200	

Notes.

All counts are taken from the same message ciphered on the keys of Grilse Jan. 10th 1945. (26 dots in μ_{37}).

The bulges in the counts of P, ΔP, ΔΨ′, ΔD have been explained. Ψ′, χ, Z show (for all practical purposes) typical random count in which every letter occurs an approximately equal number of times. The counts of D, K, Δχ, ΔZ must also be flat.

(a) /34 should not occur in P. Their occurrence is due to corruption.

(b) Q rarely occurs in 'letter-shift', but is quite frequent in figure-shift, where it corresponds to 1 (one).

(c) Note how the frequency of letters other than / depends on the number of crosses in them. For 26 dots in μ_{37} a = ·65 b = ·77.

12D MOTOR AND PSI BREAKING AND SETTING Solution of D = P + Ψ'.

(a) Psi-breaking and setting by hand.

When chi-wheels and settings for a message are known the chi stream and Z stream can be added together and de-chi stream found. A stretch of de-chi can be converted by eye into the sum of P and psi by a skilled cryptographer with knowledge of "Tunny-German" and the power of instantaneous mental addition of letters of the Teleprint alphabet.

A start can be made as follows : it is very likely that somewhere in every message a full-stop (say 5M89) in P will occur at the same place as a long extension of the psis (say TTT). Experienced men know at sight that

JNKH = 5M89 + TTTT

NJ3W = 5M89 + QQQQ and so on, so that the identification of a 'stop' often provides an initial break from which further P and Ψ' can be determined.

Example : Part of de-chi stream (data) : C Q P Q V B G Q F F Y J E B 4 L T
P stream (inferred) : 9 I N F 5 M 8 9 D I V 5 M 8 9
Ψ' stream (inferred) : R Z G G S S S W 9 J J T X I I

From Ψ' obtained in this way the unextended psi is easily found. If there are 59 letters of it, the sequence will give us the complete pattern of dots and crosses on psi 5 (unconfirmed) and a complete pattern (partly confirmed) on the other psis. Fewer letters of psi (about 10) are required to find the <u>settings</u> of wheels whose patterns are already known.

As the dottage and number of extensions increases, reading a de-chi becomes correspondingly easier although more letters of Ψ' are required to give an adequate stretch of psi.

(b) Motor-breaking and setting given ΔΨ'

When the psi patterns (or settings) for some point in a message have been found, it is necessary

(i) To find the psi settings for the start of the message.

(ii) To recover a sufficiently long stretch of Ψ' to enable the motor patterns (or settings) to be determined.

In order that motor settings for the beginning of the message may be found directly, these two jobs are usually done in unison. The approximate psi settings for the start of the message may be calculated and the psi stream generated. This can be fitted on to the de-chi stream and used to separate into P and Ψ' a longish stretch of de-chi near the start - the psi being extended wherever this is required to make sense of the P.

When a longish stretch has been read the motor can be worked out. The Ψ' shows where the TM dots occur. There is a BM dot at all these places and a BM cross at every other place which has a limitation cross, the character of the limitation being determined since chi, psi and P are known.

Consequently, certain dots and crosses in the BM stream can be placed: when enough have been placed it is possible to find a unique pattern of motor wheels (or a unique position of motor wheels) which will fit these BM dots and crosses without contradiction.

The length of Ψ' required depends on the dottage; the normal minima are 300 letters for motor breaking and 120 letters for motor setting.

(c) Motor and psi-settings by machine.

It has already been shown that a ΔD count consists of the sum of the count against TM dots, where ΔD = ΔP, and the count against TM crosses which is nearly random. The strong letters in ΔD therefore derive a proportion of their strength from BM dots which is greater than the proportion of BM dots in the whole message. We can therefore- in favourable circumstances - select the correct motor settings by trying each pair of settings in turn and choosing those at which the frequency of the strongest ΔD letters against BM dots is a maximum.

With $\bar{\chi}_1$ limitation, the extended psi pattern corresponding to each possible settings of each psi is known as soon as the motors have been set, and the correct setting of each psi can be recognised by the marked characteristics $D + \Psi' = P$ in each impulse. For unlike ΔD, which has an equal number of dots and crosses in each impulse as longas $ab = \frac{1}{2}$, P_1, P_2, P_4, P_5 normally have an excess of dots and P_3 an excess of crosses sufficient for it to be possible to set at least one psi wheel independently of the others.

For psi 1 (or P_5) limitation a similar method can be used, provided psi 1 (or psi 5) are set first and no effort is made to set the other psis until the pattern of the Total Motor has been completely determined.

Colossus is designed to carry out both these jobs.

<u>12E METHODS INVOLVING KEY</u> <u>Solution of $Z = K + P$, and $K = \chi + \Psi'$.</u>

(a) <u>Obtaining of key from depths.</u>

As the key stream is the same for both messages(a and b) of a depth, we get

$$Z_a + P_a = K = Z_b + P_b$$

$$\therefore Z_a + Z_b = P_a + P_b$$

Z_a and Z_b are known. $Z_a + Z_b$ can be found by addition and a skilled cryptographer can separate this out into the sum of two stretches of plain language.

<u>Example</u> : Z_a = A O 9 V Y P B 8 S L K N 9 I I / P R 8 Y Q A H V 8
Z_b = N N R Z Y A P Q U P G L I N C 3 A 4 L P 8 / K 9 Z
$Z_a + Z_b$ = K H C K / Y K 3 4 8 Y V 4 R 3 3 Y 3 F A 3 A 5 G C
P_a = 5 Q M 8 9 E N G L 5 M 8 9 I N F 5 M 8 9 D I V 5 M
P_b = H A L T 9 H A L T 9 D E I N 9 S C H L U E S S E L

from Z_a and P_a the stretch of key is found by addition.

(b) <u>Obtaining of key from cribs.</u>

At certain times in the history of Tunny certain routine reports were sent out from the "Berlin" end of two or more different links from the same P-tape. It may be possible to identify retransmission of this type from serial receipts and other forms of unciphered operators' chat before either version has been decoded, and as soon as one version has been decoded it is comparatively easy to do so.

When the report has been decoded on one link it is possible to find the point in the Z of the undeciphered link at which the P from the known decode starts. This is done by trying the various possible positions (on a Robinson) and testing P + Z at each position for the statistical characteristics of ΔK.

(c) <u>Wheel-breaking from key.</u>

Chi-breaking from key is analagous to chi-breaking from Z, the method being to select the patterns of $\Delta\chi$ wheels which will give the strongest count for $\Delta\Psi'$. It is, in fact, equivalent to chi-breaking from Z when the P-stream consists entirely of strokes.

The comparative strength of a $\Delta\Psi'$ and a ΔD count can be seen in fig. 12 (II) and is such that whereas chis are rarely broken from under 4000 letters of $Z = \chi + D$, they can sometimes be broken from 100 letters of $K = \chi + \Psi'$. This means that the dimensions of the job make it quite practicable by hand though a Colossus may profitably be used if the stretch of key is sufficiently long.

Wheelbreaking from key on χ_2 limitation normally starts with a $\hat{\chi}_2$ count or run. Wheel-breaking from other kinds of key normally starts with KEY RECTANGLES and a COMBINED ($\Delta\chi_5$) FLAG. If this is significant the chi patterns obtained are used to complete the wheels by an improved form of TURINGERY (Turing's Method), or alternatively by Colossus wheel-breaking methods, if the key has more than about 300 letters.

Once the chi patterns have been found and the $\Delta\Psi'$ stream obtained, the recovery of the psi patterns is trivial.

13 - MACHINES

The machines used in Tunny-breaking may be classified as :-

(1). Counting and Stepping Machines.
(2) Copying Machines.
(3) Miscellaneous simple machines.

13A EXPLANATION OF THE CATEGORIES.

(a) Counting and stepping machines.

These machines are given two teleprinter patterns, combine them in some way and count the number of places of the combined pattern in which a certain condition is satisfied.

An essential feature is that these counts must be made with the two patterns in all possible relative positions i.e. one pattern must "step".

For example, chi-setting consists of adding $\Delta\chi + \Delta Z$ in all possible relative positions, and counting for each position the number of places in which a condition such as $\Delta\chi_1 + \Delta\chi_2 + \Delta Z_1 + \Delta Z_2 =$ dot is satisfied.

At each setting the answer is, of course, a number.

(b) Copying Machines

These combine one or more teleprinter patterns. They differ from "Counting and Stepping" machines in that

(i) there is no stepping.
(ii) the result is not a number, but a sequence of letters.

The sequence of letters may be either a punched tape or a print-out.

These machines vary greatly in complexity, from the hand-perforator in which a pattern tapped out on a keyboard letter by letter is reproduced on a tape, to the decoding machine in which Chi, Mu, Psi set up electrically are combined with Z to produce P.

Of all machines "Counting and Stepping" machines are by far the most spectacular: both cryptographically and electrically they are notable achievements. For producing results they are dependent on humbler machines, especially tape-making machines.

13B COUNTING AND STEPPING MACHINES.

There are three versatile machines: -

Colossus
Robinson
5202

The fundamental difference between Colossus and Robinson is that on Robinson all patterns are punched on tapes, whereas on Colossus only one pattern is on a tape, the other being represented electrically.

5202, the photographic machine, is essentially a Robinson, using film instead of tape, but working many times faster, first making an approximate count. For details see 91.

(a) Colossus

Colossus has a "bedstead" round which the Z tape is driven by pulleys so as to be scanned at 5000 letters per second; and "triggers" in which chi, Mu, Psi patterns may be set up.

The counts most commonly required are of $\Delta D = \Delta Z + \Delta \chi$ and $P = Z + \chi + \psi'$. For these there is a switch panel which imposes conditions on Q, where Q is, at choice, any sum, with or without deltaing, of Z, Chi, Psi.

The Q panel suffices to select almost any arbitrary group of letters, but is kept reasonably small by 'not' switches: "either A or B or C" is replaced by the equivalent "Not (not A, notB, not C)".

There is a plugboard for conditions not expressible in terms of Q. It has no "not".

The effective speed is increased fivefold by five separate counters which, in particular, can be used for counting at five different settings simultaneously (multiple test).

Specialised facilities include "not 99", for ignoring the 9's used to replace corruption; "spanning", for selecting a part of the text; "set total", for cancelling scores too small to be of interest.

On some Colossi there is an elaborate rectangling gadget; on others a wheel-breaking panel.

Scores are displayed and printed.

Colossus is the standard machine for wheel-setting and breaking: it is too large to replace hand work economically in all cases.

On Colossus only one pattern is arbitrary viz. the tape, the others being restricted by wheel periodicities. If two arbitrary patterns are to be compared Robinson is used.

(b) Robinson

In pre-Colossus days the old Robinson did much of the work now assigned to Colossus, and, considering its primitive character, did so with remarkable success.

The present 'Super Rob.' has four bedsteads, a plugboard rather more flexible than that of Colossus, a very meagre switchboard, "span" and "set total". It lacks the immense elaboration of facilities provided by Colossus.

Its advantage is that patterns punched on a tape are completely arbitrary; its disadvantage that they are difficult to change.

Since Colossus became generally available, Robinsons has been used mostly for cribs and for experimental work, occasionally for rectangling.

(c) Specialized Counting and Stepping Machines.

These are Dragon, for setting short cribs in de-chis; and two machines which arrived too late for operational use: Aquarius, for go-backs and Proteus for depths.

13D COPYING MACHINES

These machines are fed with tape, keyboard operation or electrically plugged patterns.

They produce either tape or printed letters.

It is convenient to describe them in tabular form.

INPUT	OUTPUT	NAME OF MACHINE	REMARKS
Keyboard	→ tape	Hand perforator	
Tape	→ tape	Angel Insert machine (or I.R.M.):	Special facilities for making corrections by hand.
Tape	→ print	Junior :	Has comprehensive steckering
		Garbo :	A Junior with Δ'ing.
Tape	→ tape	Miles :	Can add five tapes with impulse permutation, etc.
		Miles A :	Has also Δ'ing and is more flexible.
Plugged pattern and tape or keyboard	→ tape or print	Tunny : Decoding machine :	The plugged patterns are arbitrary Tunny key. These two machines differ principally in application.

All these machines make use of certain standard units: the simpler ones consist of little else:

1. Tape <u>Readers</u> (or transmitters, or auto-transmitters).
2. <u>Reperforators</u> (or punches).
3. <u>Electromatic</u> <u>Typewriters</u>.

The varieties names in brackets differ technically, not functionally.

13D MISCELLANEOUS SIMPLE MACHINES

These include:-

Slide-rules.
Adding machines.
Hand counters for measuring the length of tapes in terms of sprocket-holes.
"Stop and Start" for punching stop and start signs.
Stickers (h and c): a device used in joining tapes.

14 ORGANISATION

14A EXPANSION AND GROWTH

(a) General position.

In order that information sent out by the Germans in Tunny messages might become available to Allied authorities, four types of organisation had to be built up. These were all under the direction of G.C. and C.S. and concerned Interception, Cryptography, Traffic Analysis and Intelligence.

This report is concerned only with Cryptographic work on Tunny, and the sections at Station X concerned with this occupied an intermediate position between

GCWS KNOCKHOLT and ancilliary non-morse interception stations working on Fish Traffic, and

Intelligence sections at Station X to which Tunny decodes passed (Hut 3, Naval Section, 180S).

Traffic Analysis - undertaken by Sixta (Non-morse) - was often of cryptographic value, and several references to Sixta's work will be found in the chapters that follow.

(b) Three periods.

The history of cryptographic work on Tunny can be suitably divided into three periods - the Research period, the Testery period, and the combined period.

Tunny traffic was tackled by the Research section shortly after the first link was set up in June, 1941. The Research period lasted until July, 1942, by which time a stretch of key had been obtained from a depth (August, 1941), the workings of the machine deduced (January, 1942), and various hand methods of wheel-breaking and setting on the basis of the indicating system, depths, near depths and short cribs devised and used with success on the traffic of March to July, 1942. In July, current traffic was read for the first time.

In July, 1942 Major R.P. Tester formed a Tunny section (the "Testery" - consisting mainly of ex-members of the Research section) to tackle Tunny on an operational basis, and from July to October, 1942 nearly every message was read. In October, 1942, the expansion of the Tunny system started and the QEP system was introduced. After this, operational activity was restricted to wheel-breaking and setting from depths. Depths were frequent and produced many sets of wheels but covered only a fringe of the setting problem.

The Research section again set to work on Tunny and devised statistical and mechanical methods of setting which did not depend on depth. Mr. M.H.A. Newman was given the job of developing these operationally in December, 1942, and his section (the "Newmanry") with its first two machines was founded in June, 1943. The section was at first regarded by members of Major Tester's section with some amusement, but by October, techniques were improved and operational work had started.

With the introduction of P_5 limitation in December, 1943, depths disappeared. Mr. Newman's section became essential to all Tunny work and a new division of labour was effected. The section became responsible for chi-breaking and setting (which had to be done mechanically), and Major Tester's section for psis and motors which could be broken or set by hand. More and better machines were ordered, so that, when the daily wheel change was introduced in the summer of 1944, the combined sections took it in their stride. The main division of work remained unchanged to the end, though an increasing amount of wheel-breaking was done by Major Tester's section as P_5 was dropped and depths became more frequent, and an increasing amount of motor and psi setting was done by machine as soon as the number of Colossi made this possible.

(c) Combined operations.

In general Testery methods were hand methods based on language properties, and Newmanry methods were statistical and needed machines. But there were many contradictions. The computing of Rectangles is a statistical hand job undertaken by the Newmanry, and on the other hand Dragon is a machine designed to do a language job in the Testery. Hand analysis of key (by methods elaborated from that devised by TURING in 1942) is a statistical hand job involving probability techniques which was done by the Testery before (and after) the Newmanry was founded.

The decoding room grew up as part of Major Tester's section and remained so. A joint Registry was founded in January, 1944.

14B THE TWO SECTIONS IN 1945

The following brief notes show the general set up of the operational organisation in its final stage of development. Every department was staffed 24 hours a day.

(a) Control and registration.

The Control Officer maintained all contacts with Knockholt and Hut 3. In particular he was responsible for informing Knockholt which links were to be covered and which messages were required for wheel-breaking or setting.

Z-tapes for all messages required were prepared at Knockholt and teleprinted in the case of wheel-breaking tapes to Block H, and in the case of setting tapes to Room 11, Block F. Red forms were sent by bag.

The joint registry in Room 12 was responsible for arranging the circulation of these tapes and relevant documents to the Newmanry, the Testery cryptographic departments, and to the decoding room. The registry itself kept all material not in direct operational use, and arranged the disposal and storage of materials relevant to decoded and abandoned messages on which further work was unlikely. This arrangement was of great value in keeping the number of tapes and papers in operational rooms to a minimum. "Room 12" had two branches: the T-Registry in Block H for dealing with wheel-breaking tapes and the Main Registry in Room 12 itself for dealing with setting tapes.

(b) Mr. Newman's section.

Wheel-breaking activities took place in Block H under the direction of the Wheel Man, setting activities in Block F under the direction of the Duty Officer who also had general charge of the section's activities on his shift. Each Block contained a Registry, Tunny Room and Colossus Rooms.

The TUNNY ROOMS housed copying machines as described in the last chapter. Tunny Room (Block F) undertook the preparation and copying of tapes for setting and the making of printed de-chis (i.e. printed copies of the D-stream for sending to the Testery). Room D (Block H) undertook the preparation and copying of wheel-breaking and crib tapes and the making of printed rectangles.

COLOSSI in Block F were used for setting, those in Block H primarily for wheel-breaking and Rectangle-making and the residue for setting. When ROBINSONS were used for setting these were housed in Block F but improved ("Super") Robinsons - used mainly for Cribs - were installed in Block H.

Details of Tunny Room and Colossus jobs were left to the operators concerned but the jobs were ordered by the REGISTRARS and returned to them on completion. The OPS. REGISTRY in Block F (Ops.) consisted of the RUNS REGISTRARS who issued setting jobs to Colossi (previously to Robinsons), the TAPES REGISTRARS who issued jobs to the Tunny Room (Block F), and the LOGS REGISTRAR who kept in touch with Room 12 and kept track of all tapes sent up by them for setting. In Block H there was a single H-REGISTRY which kept track of all wheel-breaking tapes and ordered any Tunny Room or Colossus jobs.

In addition to these departments, Block H housed the computers and (Newmanry) Cribs section.

COMPUTERS, under the direction of the RECTANGLES REGISTRAR converged rectangles and did other paper work on Key Rectangles and Flags.

The (Newmanry) CRIBS Man and Registrar selected suitable messages for crib jobs with the help of Sixta and (Testery) Cribs Watch, and itself organised and ordered the necessary tape-making and Robinson Runs. In addition to this, they were responsible for any other (routine or experimental) Robinson jobs.

Maintenance of machines was the responsibility of the engineer in charge.

(c) Major Tester's Section.

ROOM 41 contained registrars, and cryptographers for psi-breaking and setting (by hand) from de-chis, reading of depths, and wheel-breaking from Key (by hand). DRAGON - though in a different room - was fed and operated by members of Room 41. The head of Room 41 was in general charge of all work in Major Tester's section on his shift.

De-chis on which psis were broken or set at some point in the message were passed to ROOM 40. ROOM 40 were responsible for Motor breaking and setting, and for finding settings for all wheels as near the start of the message as possible. It also dealt with decoding breakdowns.

Messages set on all wheels were passed to the supervisor of the Decoding Room who issued them to decoding machines as soon as possible, and checked them on return.

Decodes were read by the (Testery) CRIBS watch who routed them to the correct intelligence section and looked out for items of cryptographic importance or of wireless importance (for Sixta) and in particular for possible retransmissions which might serve as cribs.

(d) Sixta

SIXTA (non-morse) - Mr. Uzielli's section - read the unciphered chat between German Operators (which was intercepted at Knockholt), and studied Fish wireless procedure from the Logs of intercept stations and decodes. In particular Sixta supplied information about Retransmissions, daily times of QZZ, and any change of machine (and limitation) used.

14C CIRCULATION

This section gives four examples of the passage of a message through the two sections in various circumstances. The examples are typical but clearly not exhaustive. The methods referred to are defined in Section 12B.

(a) 1st method. Setting

The Tape arrives in Room 11; is passed to the Ops. Registry; sent by the Tapes Registrar to Tunny Room to be prepared for Colossus and returned; sent by the Runs Registrar to Colossus for chi-setting and returned. If set, a de-chi is ordered by the Tapes Registrar and returned. Tapes, de-chi, and chi-settings are then sent from the Ops. Registry to Room 12.

De-chi with RP and chi-settings is sent by Room12 to Room 41 for psi setting, passed onto Room 40 for motor settings, and on to the Decoding Room. The decode is passed to the Criba Watch who route it to the appropriate intelligence section via Room 12.

(b) 2nd method. Setting.

The tape arrives in Room 11; is passed to the Ops. Registry; sent by the Tapes Registrar to Tunny Room to be prepared for Colossus and returned. Sent by the Runs Registrar to Colossus for setting on all wheels and returned. If set, tapes and settings are sent to Room 12.

RP and settings are sent from Room 12 to the Decoding Room - then as in (a).

(c) 1st method. Wheel-breaking.

The tape arrives in Block H; is passed to H- Registry; thence it is EITHER sent to Room D for Rectangling on Carbo and returned, OR sent to Room D to be prepared for Colossus and then to Colossus for rectangling and returned. The rectangle is sent to the computers for convergence.

If significant, Tapes and Rectangle go to Colossus for chi-breaking and, if successful, tapes and chi patterns are sent to the Ops. Registry via the H-Registry. A de-chi is ordered from Tunny Room (F) by the Tapes Registrar and returned, and tapes, dechi and chi patterns sent from the Ops. Registry to Room 12.

De-chi with RP and chi patterns is sent by Room 12 to Room 41 for psi-breaking, passed on to Room 40 for motor-breaking, and on to the Decoding Room - then as in (a).

(d) 3rd method. Wheel-breaking from Depth.

Printed texts of the alleged depth are teleprinted to Room 11 and passed to Room 41. If the alleged depth is read successfully, wheel-breaking from Key starts at once by hand in Room 41, but the key is also sent to Block H where it is perforated and rectangled in Room D, a combined flag being then made by the computers. If significant the partial chis from the flag are passed to the key-breaker in Room 41.

If chis and psi patterns are broken successfully they are passed with Key and RF to Room 40 for Motor-breaking, then on to the Decoding Room and as in (a).

Tapes on which setting and wheel-breaking are abandoned are returned to Room 12 and T-Registry respectively.

15 SOME HISTORICAL NOTES

15A FIRST STAGES IN MACHINE DEVELOPMENT.

(a) Early development of Statistical methods.

The idea of breaking single Tunny messages without depth by statistical methods was first propounded in the autumn of 1942. The '1+2 - break-in' was invented by W. Tutte in November, 1942, and tested out with success by paper stencils. He also suggested at this time the breaking of chi-wheel patterns by means of the rectangle, and succeeded in finding the chis from a message 15,000 letters long.

Methods for setting motors and psi-wheels (by 'contracting' de-chis) and the rectangle-method for breaking motors, were suggested by others working in the Research section at that time.

(b) Proposals for the use of machinery.

The idea of using electronic counters to carry out these processes at a practically useful speed was put forward by M.H.A. Newman and in December, 1942 he was given the task of developing machine methods of setting TUNNY.

A number of schemes were considered, including that of sliding photographic plates over each other, a method later perfected in U.S. It was soon settled that the best machine for the early experimental stages was one which read a 'message-tape' and a 'wheel-tape' photo-electrically, and combined them electrically before counting. Emphasis was laid from the start on the need for flexibility, in order that the routines designed <u>in abstracto</u> might be able to be modified in the light of experience without changing the machine.

(c) Heath Robinson

The result of many discussions was the two-tape machine later called 'Robinson'. It consisted of a valve and relay counter, designed by Dr. Wynn-Williams, coupled to a tape-rack ('bedstead') and a "combining" unit, designed by Mr. Flowers of the Post Office Research Station, Dollis Hill. The Pilot model, Heath Robinson, was commissioned in January, 1943 and began working in June of the same year.

'Heath Robinson' amply satisfied the demands for flexibility, and there can be little doubt that the opportunities it gave for trying new techniques at this crucial stage played a decisive part in the later successes of Colossus.

(d) The first 'Tunny'.

The 'Robinson' machine for making counts was accompanied by what was called in the section the 'Tunny' machine, for preparing tapes. This was essentially a reproduction of the German machine in terms of relays and uniselectors, but with facilities for switching in only a selection of the wheels and impulses.

It is an important feature of all apparatus used in the section that it uses standard five impulse tape, without any special preliminary processing. Although this led to a good deal of trouble both in designing the apparatus and in the early days of operation, through stretching tapes, it was well worth while surmounting these troubles in order to be able to use ordinary commercially produced tapes and tape-making plants, (later including American (I.B.M.) Machinery).

(e) Automatic Recording

In the Robinson as originally designed the selected readings (those above the 'set-total') were shown on a screen, to be copied down by operators, who were then to cancel the reading by a switch. Shortly before the machine was finished Mr. Gifford, of TRE, suggested that he should design a printer which would print the settings and totals. The automatic recording to which this led proved to be an indispensable part of the process. For operations in which certain initial scores form the basis of complicated later runs, the extra hazards introduced by mistakes and fatigue of copying, and lack of uniformity in hand written dossiers, are great enough to reduce the proportion of success substantially. A rack for automatic recording was therefore made a part of Colossus, even though this entailed some weeks' delay in the arrival of Colossus I.

15B EARLY ORGANISATION AND DIFFICULTIES.

(a) The Initial Staff.

The initial staff of Mr. Newman's Section consisted of M.H.A.Newman, soon joined by D.Michie, with 16 Wren operators and two engineers, working first two shifts and then three, in a two-roomed hut (Hut 11.)

(b) Development of the system of checks.

The early difficulties were sufficiently severe to prevent more than three messages from being set in any week in the first three months of operation. They arose partly from machine faults, (incorrect tapes from Tunny and incorrect counts on Robinson), partly from operator's errors. The standard of accuracy needed before there was any possibility of success was very much higher than would ordinarily be required of this kind of apparatus, or of operators. A single letter omitted in a tape destroyed the value of the run and the ordinary length of a tape was about 3000 letters. A count missed at the beginning of a run on Robinson gave wheel settings bearing no simple relations to the true ones. In addition there were numerous opportunities for wrong plugging, switching, and tape-setting on both machines. An error which passed undetected through several stages of the work could take hours or even days to track down.

To remedy this state of affairs a system of checks was gradually evolved which made it a rare occurence for a mistake to persist through several operations. To achieve this very elaborate checks were necessary, and about half the operational time was occupied in carrying them out. It was made a principle that the design of a new routine must include all the checks required, and in estimating the merits of a proposed routine the nature of the checks required had always to be taken into account. It is for this reason that checks are described so fully in the chapters that follow.

15C PERIOD OF EXPANSION

(a) Mass production of Robinsons

Towards the end of 1943 the pressure for a large production by machine methods had grown, for two main reasons. The Tunny network had grown, the value of the contents had raised the traffic to the highest level, and the tightening up of German precautions against 'depths' had caused production by 'hand' setting methods to sink almost to zero. The introduction of the P_5 limitation of the end of 1943 made depth-reading impossible. A large programme of machine construction was therefore embarked on. Twelve Robinsons were ordered in the late summer of 1943, and the first factory model arrived in November, just in time for the move to more adequate quarters in Block F. The original Pilot model, which was by this time completely worn out, was thereupon abandoned. Some of the later Robinsons had four 'bedsteads' enabling complicated runs to be done without special tape-making.

(b) Colossus

Meanwhile Colossus I was delivered in February, 1944, and immediately sent up the output to more than twice its previous level. Colossus was entirely the idea of Mr. Flowers of Dollis Hill. His original scheme was to set up the message, as well as the wheels, on valves but this was given up when it was realised that messages of 5000 or more would be wanted. The combination of one tape, carrying the message, with wheel patterns set up electrically, gave nearly all the advantages of the pure valve machine with a great saving in valves and in setting time. The advantages of this machine over Robinson were (1) Its speed, a factor of 25/2 when 5 counters were available on all chi-runs: (2) The absence of inertia which enabled a run to be stopped at any moment and the wheels switched to assigned settings. (3) The great reliability resulting from the use of valves throughout, instead of relays and the abolition of synchronised tapes. A preliminary order for four further Colossi was placed in March, 1944, increased to twelve at the end of April. The order for Robinsons was curtailed. Great pressure was put on Dollis Hill to deliver the Colossi quickly and they promised on the 14th March to have Colossus 2 (i.e. the first production model) working by 1st June. This promise they fulfilled. Colossus 2 came into action on 1st June at 0800. The remaining Colossi followed at the rate of about 1 a month. A new building (Block H) was erected to house Colossi 5 to 11. Its plans were approved on 25th May, 1944 and it was ready for occupation on 17th September. Work on assembly of Colossus 11 had started on 8th May, 1945 and was stopped (before completion) a few days later.

(c) Staff expansion

The machine expansion was accompanied by an expansion of Newmanry staff which finally amounted to 272 Wrens and 27 men. The organisation had to be correspondingly elaborated, mainly by the multiplication of Registrars to keep track of tapes and jobs in their travels round the Newmanry, and to keep in touch with Major Tester's Section.

(d) Reallocation of work between the two sections.

The original paper schemes for machines processes proposed the setting of all 12 wheels by statistical methods carried out on Robinson. The Motor was to be set by running the motor-pattern against strokes of ΔD, and psi wheels could then be run against ΔD, 'contracted' by missing out letters opposite motor dots. The tunny machine had a special contrivance for making this contracted version.

This programme was actually carried out for some months, until it was realised that, given a de-chi, it is possible to set the motor and psis by 'language' methods. This work was done in Major Tester's section, and a convenient division of work and utilisation of available resources resulted. With the introduction of the P_5 limitation this division became a necessity, since, on the one hand, chis could no longer be set on depths, and on the other, de-chis could no longer be 'contracted' on Tunny. The division of work on chis and psis necessitated a close co-operation between the two sections, and an important step was the setting up of the joint registry. With the switch over to Colossus, complete setting on all 12 wheels by machine again became possible, and when at the end of 1944 Colossi began to be plentiful a large proportion of messages were completely set by machine methods.

(e) Wheel breaking

With the introduction of the P_5 limitation it became necessary to break the chi-wheel-patterns statistically from ΔD. As long as the wheels changed only once a month this could be done without seriously interfering with the normal setting organisation, and with the use of only about two Wrens a shift for computing. When a daily wheel change was introduced in July, 1944, wheel-breaking became a normal part of the Newmanry's work, and about 18 Wrens a shift were employed in computing and (eventually) 3 Colossi on the later wheel-breaking processes. 'Key-breaking', i.e. finding the wheels by statistical methods from key found from depths, was closely allied to ordinary wheel-breaking, and undertaken in collaboration with the Testery.

(f) Super-Robinson

'Cribbing' as a method of obtaining wheels, was begun in June, 1944. Since this required two message tapes to be run against each other, the use of Robinson was essential, and in view of the troubles on the old Robinson a new model was designed by DR. COOMBES and MR. CHANDLER of Dollis Hill; two of them had been completed by 8th May, 1945.

(g) Tape-making machinery

The prototypes of Garbo and Miles were introduced towards the end of 1943.

21 SOME PROBABILITY TECHNIQUES.

(a) Symbols used in symbolic logic

(b) Simple probability notations.

(c) Special values of p.

(d) Relationship of events

(e) The laws of probability

(f) Some theorems- (including Bayes' theorem)

(g) The deciban

(h) Methods of applying the above axioms

(i) Theorem of the weighted average of factors

(j) Theorem of the chain of witnesses

(k) Expected value, standard deviation, variance, distributions

(l) Some special distributions

(m) Some simple formulae of a non-analytic type, concerning proportional bulges

(n) The general formula for sigma in Tunny work

(o) The statistician's fallacy

(p) The principle of maximum likelihood

It is assumed that the reader has at any rate an elementary knowledge of probability theory. Therefore the account presented here does not contain many examples but is mainly a list of definitions, notations and theorems. Rigour is <u>deliberately</u> avoided when it would make the account more difficult to read.

(a) Symbols used in symbolic logic.

$\vee$ means 'or'

. means 'and', but the symbol . is often omitted, thus E.F can be written EF (E and F being propositions).

$\sim$ means 'not', but we shall write '$\widetilde{X}$' instead of the usual '$\sim X$'.

(b) Simple probability notations.

$P(E|H)$ means the probability of an event E given a hypothesis H. When H is taken for granted we write $P(E)$ simply.

The letter p represents a probability.

The letter o represents odds and is defined by the equation

$o = \frac{p}{1-p}$. The odds of an event E given an hypothesis H are written as $O(E|H)$. Sometimes odds are expressed as a ratio such as '3:2' or '3 to 2'. This means $o = 3/2$. The following phrases are equivalent.

'a:b', 'a:b on', $o = a/b$','a to b', 'b to a against' etc.

(c) Special values of p.

'Certainty'	$p = 1$ or $o = \infty$
'Impossibility'	$p = 0$ or $o = 0$
'Evens'	$p = \frac{1}{2}$ or $o = 1$.

(d) Relationship of Events.

Two events are 'mutually exclusive' if they cannot both happen. Two events are 'independent' if a knowledge that one is true does not affect the probability of the other one. A number of events is 'exhaustive' if it is certain that one or other of them will happen.

(e) The laws of probability.

(i) the law of addition of probability

$$P(E_1 \vee E_2|H) = P(E_1|H) + P(E_2|H)$$

if E_1 and E_2 are mutually exclusive.

(ii) the law of multiplication of probabilities

$$P(E_1E_2|H) = P(E_1|H)\ P(E_2|E_1H).$$

In particular, if E_1 and E_2 are independent

$$P(E_1E_2|H) = P(E_1|H)\ P(E_2|H).$$

(f) Some theorems.

(i) $P(E_1E_2 \ldots E_n|H)$

$$= P(E_1|H)P(E_2|E_1H)P(E_3|E_1E_2H) \ \ldots \ P(E_n|E_1 \ldots E_{n-1}H).$$

(ii) $P(E_1 \vee E_2 \vee \ldots \vee E_n|H)$

$$= \sum_r P(E_r|H) - \sum_{r,s} P(E_rE_s|H) + \sum_{r,s,t} P(E_rE_sE_t|H) - \ldots \text{ etc.},$$

and in particular if $E_1, E_2, \ldots, E_n$ are all mutually exclusive, the right hand side can be replaced by $\sum P(E_r|H)$. If $E_1 \vee \ldots \vee E_r$ is exhaustive the left hand side is 1. Therefore $P(\tilde{E}) = 1 - P(E)$.

(iii) Bayes' theorem.

For various hypotheses H_i $(i=1,2,\ldots)$

$$\frac{P(H_i|E)}{P(H_i)} \propto P(E|H_i)$$

The proof of this is simple. For by the law of multiplication of probabilities,

$$P(H_i|E)P(E) = P(EH_i) = P(E|H_i)P(H_i)$$

$$\therefore \frac{P(H_i|E)}{P(H_i)} = \frac{P(E|H_i)}{P(E)} \propto P(E|H_i).$$

A special case of Bayes' theorem, itself often referred to in the research logs as Bayes' theorem, is particularly important in cryptographic problems. Suppose we consider the hypotheses H and $\tilde{H}$. Then, by the theorem above

$$\frac{P(H|E)}{P(H)} \Big/ \frac{P(\tilde{H}|E)}{P(\tilde{H})} = \frac{P(E|H)}{P(E|\tilde{H})}.$$

$$\frac{O(H|E)}{O(H)} = \frac{P(E|H)}{P(E|\tilde{H})}$$

$P(E|H) / P(E|\tilde{H})$ is called the factor in favour of H given E, ~~one~~ and is seen to be the factor by which the 'prior odds' O(H) must be multiplied in order to get the 'posterior odds' O(H|E). In the more general form of Bayes' theorem any set of numbers proportional to $P(E|H_i)$ can be called the 'relative factors' in favour of the various hypotheses H_i and they are the ratios by which the prior probabilities may be multiplied, in order to get the correct ratios for the posterior probabilities. The special case of Bayes' theorem was first used in B.P. by A.M. Turing. (The fact that it was a special case of Bayes' theorem was pointed out by I.J. Good.)

(g) The deciban.

But Turing's great advance consisted in the invention and application of the 'deciban' (in Hut 8). (Deciban is abbreviated to 'd.b.'.)

This is defined simply as $10\log_{10} f$, where f is the factor as defined above. Simple though this idea is, it makes an enormous simplification in practical work. As an example let us suppose that a penny is tossed 20 times and that each time it comes down heads. Suppose that we have two theories (i) that the penny is unbiassed, (ii) that it is double headed, and suppose that the second hypothesis (H) has prior odds of one in ten thousand. If we call E the event that the coin comes down heads then $P(E|H) = 1$

$P(E|\tilde{H}) = \frac{1}{2}$

Therefore the factor in favour of H given E is 2, i.e. 3 decibans. So we gain $3 \times 20 = 60$ decibans from the whole series of experiments. The prior odds were $1/10^4$ i.e. 40 d.b. down and so the posterior odds are $60 - 40 = 20$ d.b. or 100:1 on. (Observe that we talk about the decibanage of 'Odds', meaning, of course, $10\log_{10} o$).

(h) Methods of applying the above axioms.

We assume that probability is a measure of the degree of belief that one ought to have, given certain evidence about an event, and that it satisfies the axioms given above. In order to apply the theory one must be able to judge that two events are equally probable, or at least sufficiently nearly so for all practical purposes. For example, if there was a barrel containing 10,000 ordinary pennies and one double-headed one, all thoroughly mixed up, we should judge that a coin chosen at random would have an equal probability of being any of the coins. Therefore by the law of addition it follows that the probability of drawing the double-headed coin is 1/(10,001), or odds of 10,000:1 against, i.e. 10^{-4}. In the example of decibanning given above the coin might have been chosen in this way. This is quite a good analogue of the sort of thing done in cryptographic problems, namely one looks for needles in haystacks and the object chosen has to have a large factor in favour of being a needle in order to overcome its prior odds. (It will be observed that one would take a long time to find the needle if one could not estimate the factor very quickly - hence the necessity of machines in such problem.)

Another thing that is often necessary in practice is to make a probability judgement of the type that a certain probability lies in a rather large interval. For example if a man produced a coin and began to toss it, you may be able to judge by his manner and some half-remembered facts that the probability of its being a double-headed coin must lie between 1/(million) and 1/(100). If no such judgement were possible you could never assert that you believed the coin to be double-headed, even if it came down heads 100 times running.

(i) Theorem of the weighted average of factors.

Suppose that a number of unreliable witnesses each says that a certain event E has happened but it is known that one and only one of them has in fact seen the evidence. Let the probabilities that the witnesses have seen the evidence be p_1, p_2, ... and the factors in favour of an hypothesis H be f_1, f_2, ... respectively. Then the resulting factor is $\Sigma\, p_i f_i$.

As a special case suppose that an experiment is done and it has a probability p of having been done correctly, in which case it contributes a factor f to a certain hypothesis. If it is done incorrectly it supplies no evidence, i.e. a factor of 1. Then the resulting factor is pf + 1-p. This special case is sometimes referred to as the theorem of corrected excess.

(j) Theorem of the chain of witnesses (and 'proportional bulges').

A proposition which can either be true or false is handed on through a chain of witnesses of 'reliabilities' $\frac{1}{2}(1 + \xi_i)$ $(i = 1,2,3,\ldots)$. (By reliability we mean here the probability of repeating what is heard instead of negating it.) Then the reliability of the chain as a whole is $\frac{1}{2}(1 + \prod_i \xi_i)$.

This theorem is the real reason why 'proportional bulges' were introduced. The 'Proportional bulge' or P.B., ξ, of a proposition is defined by saying that its probability is $p(1+\xi)$ where p is the probability that the proposition would have in certain conditions which in the applications can be described as a 'wrong case' or 'random case'. The theorem of multiplication of proportional bulges, given above, is true only when $p = \frac{1}{2}$. There is a tendency for P.B.'s to lead to a slight algebraic simplification even if $p \neq \frac{1}{2}$.

(k) Expected value, standard deviation, variance, distributions.

Let a variable or 'variate' x have probability $f(x_i)$ of being equal to x_i. Then its expected value is defined as $E(x) = \sum x_i f(x_i)$. This is also called the mean (value) of x or the mathematical expectation of x or the average (value) of x. The average of the sum of two independent variables is equal to the sum of the averages, and similarly for the product.

The 'variance' of a variable is defined as the mean value of the square of the deviation of x from its mean. The positive square root of the variants is called the 'standard deviation' (S.D.) of x and is usually denoted by σ. Thus, if $\bar{x}$ is the mean value of x, then

$$\sigma^2 = E\left\{(x - \bar{x})^2\right\}$$

When we write $x = \bar{x} \pm \sigma$ we mean $E(x) = \bar{x}$ and S.D. of x is σ. There is no difficulty in extending the definition of an average to the case of a continuous variable.

If

$$P(x_1 < x < x_1 + dx_1) = f(x_1)dx_1,$$

then

$$E(x) = \int tf(t)dt$$

f(x) is called the distribution function of x.

(l) Some special distributions.

Let n experiments be performed each with the probability p of success. Then the probability of exactly r successes is

$$\binom{n}{r} p^r (1-p)^{n-r}$$

This is the so-called binomial distribution.

If

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\bar{x})^2}{2\sigma^2}}$$

we say that x has a normal (or Gaussian) distribution. It is easy to see that the mean of x is $\bar{x}$ and its S.D. is σ. The factor $\frac{1}{\sigma\sqrt{2\pi}}$ is the so called normalising factor which makes $\int f(x)dx = 1$.

The integral of f(x) is called the error function. A convenient way of tabulating this is in a deciban form. A table of $\Psi(x)$ is given in R1,109 where

$$\Psi(x) = -10 \log_{10} \left(\frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{1}{2}t^2} dt \right).$$

The binomial distribution is closely approximated by the normal one for quite small values of n, if we take $\bar{x}$ = pn and $\sigma = \sqrt{np(1-p)}$. In Tunny theory this is the most frequent form for σ. The normal distribution is also a good approximation when a variable is the sum of a lot of small independent contributions.

If the probability of exactly n successes is $e^{-a}a^n/n!$, n is said to have a 'Poisson distribution'. The formula is easy to remember since $a^n/n!$ is a typical term of the expansion of e^a, so that

$$\sum_n e^{-a}a^n/n! = 1.$$

The average and variance of the distribution are both equal to <u>a.</u>

The binomial distribution is approximated by the Poisson distribution if n is fairly large but p is small, so that the average is much less than n. The Poisson distribution is approximated by the normal distribution when the number of successes minus <u>a</u> is small compared with a.

There is one other distribution used in the research logs, namely the 'χ^2 distribution'. Given n independent variables each with a normal distribution of mean o and S.D.1, let χ^2 be the sum of the squares of these variables.

Writing $\varphi(n) = P(\chi^2 > t)$, we have

$$\varphi(n) = \frac{e^{-t/2}(t/2)^{(n/2)-1}}{\left(\frac{n}{2}-1\right)!} + \varphi(n-2)$$

where $\varphi(2) = e^{-t/2}$, $\varphi(1) = \sqrt{\frac{2}{\pi}}\int_{\sqrt{t}}^\infty e^{-\frac{1}{2}x^2}dx$, $\frac{1}{2}! = \frac{1}{2}\sqrt{\pi}$.

This is the most convenient formula when t is a good deal larger than n, as it is in all our applications.

This distribution applies also to the sum of the squares of $(n+1)$ such variables whose sum is fixed.

(m) <u>Some simple formulae of a non-analytic type concerning proportional bulges.</u>

If P and Q are independent propositions

$$P.B.(P.Q.) = P.B.(P)P.B.(Q) + P.B.(P) + P.B.(Q)$$

If P_i $(i = 1,2,\ldots)$ are mutually exclusive and exhaustive propositions each with the same 'random probability' then

$$\sum P.B.(P_i) = 0.$$

If P_i $(i = 1,2,\ldots)$ are mutually exclusive propositions with the same random probability,

$$P.B.\ (P_1 \vee P_2 \vee P_3 \vee \cdots) = \underset{i}{\text{Average}}\ \{P.B.(P_i)\}$$

If P, Q, Ξ, Θ are teleprinter letters which have the same number of components, then

$$P.B.\ (P+Q = \Xi) = \underset{\Theta}{\text{Average}}\ \{P.B.(P=\Theta)P.B.(Q=\Xi+\Theta)\}$$

Here Ξ is a fixed teleprinter letter, P and Q are letters belonging to certain classes.

(n) <u>The general formula for sigma in Tunny work.</u>

Let two tapes be compared, one with a proportion p_i of letters A_i and the other with a proportion q_i of letters B_i $(i = 1,2,\ldots r)$. Let the overlap of the two tapes be N. Let the number of times A_i comes opposite B_i be ν_i. Let $\nu = \sum_{i=1} \nu_i$. Then the average of ν is $A = N\sum p_i q_i$ and $N^2\sigma^2 = A^2 + NA - N^2 \sum p_i q_i (p_i + q_i)$.

In particular, if $r = 1$

$$\sigma^2 = Np(1-p)q(1-q).$$

The proof of the general formula is best done by the method of characteristic functions. We do not describe this method here, but instead refer the reader to R4, 105-108.

(o) <u>The statistician's fallacy.</u>

A standard type of statistical experiment is exemplified by the following. A new fertiliser is tried and the amount of the crop produced is increased by 2σ. A deviation 2σ above the mean occurs about once in 40 experiments at random, assuming a normal distribution, and the result would probably be regarded as significantly good. As a conventional test of significance this is a useful method and one which is used in Tunny breaking also (as in the significance test for a short wheelbreaking run).

On the other hand it would be quite wrong to assume that it was 40:1 on that the new fertiliser was better than the usual type. This would be equivalent to neglecting the numerator in the special form of Bayes theorem, namely the probability of obtaining as good a result as the one obtained with a fertiliser known to be better than before. This may be hard to estimate but it is at any rate less than one. Another equally important criticism is that we are throwing away a lot of evidence if we say only that the result of the experiment is that a deviation of at least 2σ above the mean in obtained. The result is likely to be known more exactly, say that the deviation is between 2.0σ and 2.1σ, and in this case the factor in favour of the hypothesis would be less (with a normal distribution). These points are stressed because there is a prominent school of Statisticians who do not even accept Bayes theorem.

An example of this from our work is given by the score on a 1+2 break-in. Suppose the best score is 4σ without serious rivals. 4σ or better occurs at random once in 30,000 experiments so it would be natural to imagine that the odds of the setting given are 30,000 divided by 1271 or 23:1 on. In fact they are more like 3:1 on, (that is, even after a factor has been set against all the other settings due to the existance of no serious rival), though the odds depend to a reasonable extent on the particular link and length of tape and d. In the very early days of the section there was a tendency to continue with a message for some time if it gave a 4σ, since it was not believed that the odds could be much below 20:1 on. This was before the deciban had been brought over from Hut 8. (Later on the deciban exerted an influence on the work of the Testery also, due to the liaison between the two sections.)

<u>(p) The principle of maximum likelihood.</u>

If one has a continuous sequence of possible theories depending on a parameter x, it often happens that one has very little knowledge about the prior probabilities of the theories. If an experiment is done whose result has probability $f(x)$, then the numbers $f(x)$ are the relative factors of the various theories concerning the magnitude of x. $f(x)$ often has a maximum value at say $x = x_0$. Then x_0 is called the maximum likelihood solution for x. For a given value of ϵ it is more probable that x will lie in the interval $(x_0 - \epsilon, x_0 + \epsilon)$ than in any other interval of the same size, provided that the prior distribution is uniform. In this special case the maximum likelihood solution is equal to the 'most probable value'. Neither of these should be confused with the expected value.

22 STATISTICAL FOUNDATIONS

22A Introductory

22B The Chi Stream

22C The Motor Stream

22D The Psi Stream

22E The Sum of Two Streams

22F The Key Stream

22G The Plain Language Stream

22H The De-chi Stream

22J The Cipher Stream

22K Sampling Errors in Alphabetical Counts

22W Some further Streams

22X The Algebra of Proportional Bulges

22Y The Amount of Evidence derived from a Letter Count

22A INTRODUCTORY

Statistical methods of Tunny breaking are possible because (and only because) cipher, plain, key, chi, extended psi, de-chi and motor streams can - with suitable treatment- be made to exhibit marked characteristics which will distinguish them from a random sequence of letters. In this chapter we analyse these characteristics, and in subsequent chapters we show how they are exploited.

(a) Notation.

The letters Z, P, K, χ, ψ', D are used to denote the operative letters of the Cipher, Plain, Key, Chi, Extended psi and de-chi Streams at any given ciphering position. They are connected by the equations:

$$Z = P + K$$

$$K = \chi + \psi'$$

$$D = Z + \chi = P + \psi'$$

The suffixes 1, 2, 3, 4, 5 are used when a particular impulse is specified so that (using a generalised form) U_1 denotes the operative character of the i^{th} impulse of the U-stream at a given ciphering position.

L is used to denote the operative character of the limitation.

(b) <u>Some further definitions.</u>

The following symbols are generally used in Tunny-analysis and must be defined here :

$\bar{U}$ = letter preceding U

$\bar{U}_i$ = character preceding U_i

$\bar{\bar{U}}$ = letter preceding $\bar{U}$

$\underline{U}$ = letter following U

$\underline{\underline{U}}$ = letter following $\underline{U}$ and so on.

$\Delta U = U + \underline{U}$

$\Delta^2 U = \Delta(\Delta U)$

$\Delta^n U = \Delta(\Delta^{n-1} U)$

$\Delta_2 U = U + \underline{\underline{U}}$

$\Delta_3 U = U + \underline{\underline{\underline{U}}}$ and so on.

$\hat{\bar{U}} = \bar{U} + U + \underline{U} = \bar{\bar{U}} + \Delta U$

$U_{ij} = U_i + U_j$

$\tilde{U}_i = U_i$ + a cross

$U_i \rightarrow x \ : \ P(U_i = x) > \frac{1}{2}$

$U_i \rightarrow \cdot \ : \ P(U_i = \cdot) > \frac{1}{2}$

$U_i \xrightarrow[p]{} x \ : \ P(U_i = x) = p$ where $p > \frac{1}{2}$

$U_i \xrightarrow[p]{} \cdot \ : \ P(U_i = \cdot) = p$ where $p > \frac{1}{2}$

(c) <u>Two general theorems</u>

Theorem I : $\underline{\Delta(U + V) = \Delta U + \Delta V}$ (A1)

Theorem II: $\underline{\Delta^2 U = \Delta_2 U}$ (A2)

Proof : $\Delta^2 U = \Delta(\Delta U) = (U + \underline{U}) + (\underline{U} + \underline{\underline{U}}) = U + \underline{\underline{U}} = \Delta_2 U$

Theorem II is a special case of the general theorem :

$\Delta^n U = \Delta_n U$ if and only if $n = 2^r$. (See 25 p149)

<u>22B THE CHI-STREAM</u>

The chi-stream differs from a random sequence of letters in its periodicity in each impulse taken separately and in the deliberately arranged equality of dots and crosses in each impulse.

In order to prevent simple statistical recognition of the chi-stream each individual chi pattern is constructed with

(1) As nearly as possible an equal number of dots and crosses in the undifferenced and in the differenced wheel,

(2) No stretch of 5 or more identical consecutive characters in the undifferenced wheel. (See R5 p 4.)

Alleged chi patterns fulfilling these conditions are said to be 'legal'.

The conditions of legality are most obviously fulfilled by the pattern :

χ: . . x x . . x x . .

$\Delta\chi$: . x . x . x . x . x

A few of the patterns recovered consisted entirely of this pattern and were known as 'perfect wheels', e.g.

χ_r: . . x x . . x x . . x x . . x x . . x x . . x

$\Delta\chi_r$: . x . x . x . x . x . x . x . x . x . x . x x

In other cases the pattern was used over shorter stretches.

In the construction of chi patterns no attention was paid to the distribution of dots and crosses in the Δ^2 wheel. However, empirical evidence (see R3 p 18) shows that $\Delta^2\chi_i \xrightarrow[\cdot 4\frac{1}{2}]{} \times$ (6.1)

The fact that $\Delta^2\chi_i \rightarrow \times$ can be seen to be a natural result of the conditions of legality and the popularity of the pattern . . x x . . x x

The following table gives the conditions of legality in numerical terms:

Wheel	Length	No. of crosses in χ	No. of crosses in $\Delta\chi$	Av. no. of crosses in $\Delta^2\chi$
1	41	20 or 21	20	26
2	31	15 or 16	16	$19\frac{1}{2}$
3	29	14 or 15	14	19
4	26	13	12 or 14	$16\frac{1}{2}$
5	23	11 or 12	12	14

FIG. 22 (I)

The number of legal chis is discussed in §FX , and the frequency of various patterns 4 5 and 10 consecutive characters in R3 pp 125, 126.

22C THE MOTOR STREAM

(a) Definitions.

For a given set of wheel patterns we define

Number of dots in μ_{37} as	d
Proportion of dots in μ_{37} as	$D \equiv d/37$
Proportion of crosses in μ_{37} as	$a' \equiv 1-D$
Proportion of crosses in TM as	a
Number of crosses in μ_{61} as	k

(b) The motor wheels

μ_{61} is constructed so that $30 \leqslant k \leqslant 50$ and $k \not\equiv 37$ without more than so far as is known 5 consecutive dots or 15 consecutive crosses.

μ_{37} is constructed so that $14 \leqslant d \leqslant 28$ without more than, so far as is known, 5 consecutive dots or 6 consecutive crosses.

(c) The basic motor.

Theorem I. The BM has a period of $61 \times 37 = 2257$ (C1)

Proof After n complete revolutions of μ_{61}, μ_{37} has moved nk places. The initial position is reached when

$$nk \equiv 0 \text{ (modulo 37)}$$

Since $k \not\equiv 37$, n must be a multiple of 37, and the motor returns to its orginal position after 37 revolutions of μ_{61}.

Theorem II. Proportion of crosses in BM = a' (C2)

Proof. Since the period of the BM = 2257, each position of μ_{37} occurs with each position of μ_{61} once in each cycle. As each character of μ_{37} occurs 61 times per cycle, the proportion of crosses in μ_{37} is not changed by the extension.

(d) The total motor.

Assuming that the proportion of crosses in the limitation is $\frac{1}{2}$ - which is not strictly true for $\bar{\chi}_2$ or $\bar{\chi}_2\bar{P}_5$ limitation - we have:

Proportion of dots in TM = $\frac{1}{2}$ x proportion of dots in BM

$$\text{i.e.} \quad 1 - a = \tfrac{1}{2}(1 - a')$$

Proportion of crosses in TM is comprised of:

$$\text{Proportion of} \left.\begin{array}{ll} \text{BM dot lim dot} & \tfrac{1}{2}(1 - a') \\ \text{BM cross lim dot} & \tfrac{1}{2}a' \\ \text{BM cross lim cross} & \tfrac{1}{2}\,a' \end{array}\right\} \qquad \text{(C3)}$$

Summary

$$d/37 = D = 1 - a' = 2(1 - a) \qquad \text{(C4)}$$

(e) Double dots in BM.

The proportion of double dots in the BM is empirically $1.1(1-a')^2$(se

22D THE PSI STREAM

(a) Construction of psi patterns.

The psi patterns are constructed so that there are as nearly as possible an equal number of dots and crosses in each impulse of the Ψ' (extended psi) and $\Delta\Psi'$ streams. This implies that each Ψ wheel has

(1) as nearly as possible an equal number of crosses and dots in the undifferenced wheel, (actually one more cross than dot).

(2) a proportion b of crosses in each differenced (unextended Ψ) where $b = \frac{1}{2a} = \frac{1}{2}(1+\beta)$.

(b) A few identities.

$$\beta \equiv 2b - 1 \qquad \text{(D1)}$$

$$a \equiv \frac{1}{2b} \equiv \frac{1}{1+\beta} \qquad \text{(D2)}$$

$$1-a \equiv \frac{2b-1}{2b} \equiv \frac{\beta}{1+\beta} \qquad \text{(D3)}$$

$$1-a' \equiv \frac{2b-1}{b} \equiv \frac{2\beta}{1+\beta} \equiv D \equiv \frac{d}{37} \qquad \text{(D4)}$$

$$a' \equiv \frac{1-b}{b} \equiv \frac{1-\beta}{1+\beta} \qquad \text{(D5)}$$

(c) Corresponding values of d, a, b, β, and the number of crosses in each $\Delta\Psi$.

For all values of d:				Ψ_1	Ψ_2	Ψ_3	Ψ_4	Ψ_5	
Length				43	47	51	53	59	
No. of crosses in Ψ				22	24	26	27	30	
				Number of crosses in					
d	a	b	β	$\Delta\Psi_1$	$\Delta\Psi_2$	$\Delta\Psi_3$	$\Delta\Psi_4$	$\Delta\Psi_5$	d
14	·81	·62	·24	26	28	32	32	36	14
15	·80	·63	·26	26	30	32	34	38	15
16	·78	·64	·28	28	30	32	34	38	16
17	·77	·65	·30	28	30	32or34	34	38	17
18	·76	·66	·32	28	32	34	36	38	18
19	·74	·68	·35	28	32	34	36	40	19
20	·73	·69	·37	30	32	34or36	36	40	20
21	·72	·70	·40	30	32	36	38	42	21
22	·70	·71	·42	30	34	36	38	42	22
23	·69	·73	·45	32	34	38	38	42	23
24	·67	·75	·49	32	34	38	40	44	24
25	·66	·76	·51	32	36	38	40	44	25
26	·65	·77	·54	34	36	40	40	46	26
27	·64	·79	·58	34	36or38	40	42	46	27
28	·62	·81	·61	34	38	42	42	48	28

FIG 22 (II)

(d) <u>Frequency of letters in Ψ'.</u>

The number of dots and crosses in each impulse of the Ψ' stream are equal and their positions relatively independent. Therefore the frequency of every letter in the Ψ' stream is approximately equal.

(e) <u>Frequency of letters in $\Delta\Psi'$.</u>

In the $\Delta\Psi'$ stream, though there are an equal number of dots and crosses in each impulse, they are so placed that there is a dot in every impulse at each extension.

TM dot positions occur (1-a) of the time and at each of these there is a stroke in $\Delta\Psi'$.

The $\Delta\Psi'$ stream at TM cross positions is in fact the $\Delta\Psi$ stream (unextended) and the chance of a cross in any impulse is b. Therefore the frequency of various letters is as follows

/	0 crosses	$(1-a) + a(1-b)^5$
9T34E	1 cross	$ab(1-b)^4$
HONRLIADZS	2 crosses	$ab^2(1-b)^3$
MCGPUWJFBY	3 crosses	$ab^3(1-b)^2$
VQ5KX	4 crosses	$ab^4(1-b)$
8	5 crosses	ab^5

(D6)

(f) <u>$\Delta\Psi'_{ij}$</u>

$\Delta\Psi'_{ij}$ = dot, when TM = dot

When TM = cross $\qquad P(\Delta\Psi_{ij} = \text{dot}) = b^2 + (1-b)^2$
$= 2b^2 - 2b + 1$

$\therefore\ \Delta\Psi'_{ij} \longrightarrow \cdot$ with probability $(1-a) + a(2b^2 - 2b+1)$
$= 1-a + b - 1 + a = b$

$$\therefore\ \Delta\Psi'_{ij} \xrightarrow[b]{} \cdot \qquad \text{(D7)}$$

(g) <u>$\Delta\Psi'$ stream and limitation.</u>

In each impulse of $\Delta\Psi'$ stream and in limitation stream there are an equal number of dots and crosses.

Now at TM dot positions, $\Delta\Psi'_i$ = dot
L = cross.

Therefore the remaining $\Delta\Psi'_i$ dots, and the remaining lim x's form the same proportion of the TM cross positions.

Therefore at TM cross positions $\Delta\Psi'_i \xrightarrow[b]{}$ cross
L $\xrightarrow[b]{}$ dot

Consequently in any position,

$P(\Delta\Psi'_i = \text{dot}) = P(L+x = \text{dot})$

and for calculating the frequency of various letters in combination with limitation, (L+x) can be treated as $\Delta\Psi'_i$ - a stream of letters with a period of 31 for χ_2 limitation, and virtually non-periodic for other limitations.

The following table gives the frequency in $\Delta\Psi'$ of each '6-impulse letter'.

'Letters' with	Prop: ag: TM .	Prop: ag: TM x	Prop: in $\Delta\Psi'$
0 crosses	1	$(1-b)^6$	$(1-a)+a(1-b)^6$
1 crosses	-	$b(1-b)^5$	$ab(1-b)^5$
2 crosses	-	$b^2(1-b)^4$	$ab^2(1-b)^4$
3 crosses	-	$b^3(1-b)^3$	$ab^3(1-b)^3$
4 crosses	-	$b^4(1-b)^2$	$ab^4(1-b)^2$
5 crosses	-	$b^5(1-b)$	$ab^5(1-b)$
6 crosses	-	b^6	ab^6

FIG. 22(III)

From this table we see that $P(\Delta\Psi' = 9,\ L = .)$
$= P(\Delta\Psi' = M,\ L = x) = ab^2(1-b)^4$

Fig 22(V) shows $\Delta\Psi'$ letter counts for Ψ' streams corresponding to $d = 27, 24, 21, 18, 15$. $\Delta\Psi'$ counts are given separately for $\overline{\chi}_2$ lim and $\overline{\chi}_2\overline{\Psi}'_1$ lim, and in the case of $\overline{\chi}_2$ lim the counts of $\Delta\Psi'$ against L = x and L = . are given separately.

An immediate application of the $\Delta\Psi'_6$ principle to (D7) gives

$$\Delta\Psi'_i + L \xrightarrow[b]{} x \qquad \text{(D8)}$$

(h) <u>Proportional bulges of letters in $\Delta\Psi'$ stream.</u>

The proportional bulges of $(\Delta\Psi = \Theta)$, $(\Delta\Psi' = \Theta)$ where Θ is any letter, are denoted by β_Θ, β'_Θ and PB's $(\Delta\Psi_{ij} = \text{dot})$ and $(\Delta\Psi'_{ij} = \text{dot})$ by β_{ij}, β'_{ij}.

A table similar to Fig 22 (III) showing PB $(\Delta\Psi' = \Theta)$ for all values of Θ in terms of β is given in R5 p27.

$$P(\Delta\Psi'_{ij} = \text{dot}) = \tfrac{1}{2}(1 + \beta'_{ij}) = b = \tfrac{1}{2}(1 + \beta)$$

$$\therefore\ \beta'_{ij} = \beta \qquad \text{(D9)}$$

The idea of a PB and the introduction of β first occurs on R1 p 20.

(i) <u>Δ^2 characteristics.</u>

It is a fairly good approximation to accept the simple minded results

$\Delta^2\Psi_i \longrightarrow .$ with probability $b^2 + (1-b)^2 = 2b^2 - 2b + 1$

$\Delta^2\Psi'_i \longrightarrow .$ with probability $\frac{1}{2}$

$\Delta^2\Psi'_{ij} \longrightarrow .$ (See R3 p 22).

(j) <u>The sum of psi streams.</u>

It is sometimes useful to be able to recognise statistically the sum of 2 psi streams. This problem is dealt with in 22W(a).

22E THE SUM OF TWO STREAMS

(a) The Proportional Bulge.

In caculating the frequency of various letters or groups of letters in the sum of two streams whose letter frequencies are known, it is sometimes more convenient to consider the proportional bulges of the letters concerned and not their frequencies. The PB has been introduced in 21(j) and is normally denoted by a small Greek letter.

Consider a stream of letters (U) drawn from an alphabet of r letters, then $PB(U = \theta) = \zeta^{U}_{\theta}$

where $P(U = \theta) = \frac{1}{r}(1 + \zeta^{U}_{\theta})$

Summing over the r letters of the alphabet we get

$$\sum_{\theta} P(U = \theta) = 1$$

$$\sum_{\theta} \zeta^{U}_{\theta} = 0$$

(b) The Faltung theorem (a special form of a result stated in 21(m)).

In a stream of letters (U + V) which is the sum of two streams U and V it is clear that

$$P(U+V = \theta) = \sum_{\phi}\left\{P(U = \phi) . \quad P(V = \theta + \phi)\right\} \qquad \text{(E1)}$$

$$\therefore \frac{1}{r}(1 + \zeta^{U+V}_{\theta}) = \frac{1}{r^2}\sum_{\phi}\left\{(1 + \zeta^{U}_{\phi})(1 + \zeta^{V}_{\theta+\phi})\right\}$$

$$= \frac{1}{r^2}\sum_{\phi}\left\{1 + \zeta^{U}_{\phi} . \zeta^{V}_{\theta+\phi}\right\}$$

$$= \frac{1}{r^2}\left\{r + \sum_{\phi} \zeta^{U}_{\phi} . \zeta^{V}_{\theta+\phi}\right\}$$

$$\therefore \zeta^{U+V}_{\theta} = \frac{1}{r}\sum_{\phi}\left\{\zeta^{U}_{\phi} . \zeta^{V}_{\theta+\phi}\right\} \qquad \text{(E2)}$$

If every $\zeta^{U}_{\phi} = 0$, then $\zeta^{U+V}_{\theta} = 0$ (E3)

Therefore if two streams, one of which is random, are added together the resulting stream is random.

(c) Multiplication of PB's.

If we put r = 2 and consider the sum of two streams each consisting of dots and crosses, we get

$$\zeta^{U+V}_{\bullet} = \frac{1}{2}\left\{\zeta^{U}_{\bullet}\,\zeta^{V}_{\bullet} + \zeta^{U}_{\times}\,\zeta^{V}_{\times}\right\}$$

But $\zeta_{\bullet} + \zeta_{\times} = 0$

$$\therefore \zeta^{U+V}_{\bullet} = \zeta^{U}_{\bullet}\,\zeta^{V}_{\bullet}$$

This multiplication property is first mentioned in R1 p 20.

22F THE KEY STREAM

$$K = \chi + \Psi'$$

$$\therefore \Delta K = \Delta\chi + \Delta\Psi'$$

The undifferenced Ψ' stream is flat, therefore the undifferenced K stream is random and unrecognisable statistically [(R3)]

(a) Recognising key on any limitation.

$$\Delta\Psi'_{ij} \xrightarrow[\frac{1}{2}(1+\beta)]{} dot$$

$$\therefore \Delta\chi_{ij} + \Delta\Psi'_{ij} \xrightarrow[\frac{1}{2}(1+\beta)]{} \Delta\chi_{ij}$$

$$\therefore \Delta K_{ij} \xrightarrow[\frac{1}{2}(1+\beta)]{} \Delta\chi_{ij} \qquad (F1)$$

Differencing at distance w_i where w_i is the length of χ_i (R3 p 62)

$$\Delta_{w_i}(\Delta K_{ij}) \xrightarrow[\frac{1}{2}(1+\beta^2)]{} \Delta_{w_i}(\Delta\chi_{ij})$$

since we are in effect adding two streams in which $\Delta K_{ij} \rightarrow \Delta\chi_{ij}$ with proportional bulge β

Now $\Delta_{w_i}(\Delta\chi_i) = dot$

$$\therefore \Delta_{w_i}(\Delta K_{ij}) \xrightarrow[\frac{1}{2}(1+\beta^2)]{} \Delta_{w_i}(\Delta\chi_j) \qquad (F2)$$

Similarly, differencing at w_i w_j (e.g. 26 x 23 for χ_4 and χ_5)

$$\Delta_{w_i w_j}(\Delta K_{ij}) \xrightarrow[\frac{1}{2}(1+\beta^2)]{} dot \qquad (F3)$$

This result shows that all key maybe recognised by an excess of dots over crosses in $\Delta_{598}(\Delta K_{45})$. (R2 p 90)

(b) Recognising key on $\bar{\chi}_2$ limitation.

$$\Delta\Psi'_i + lim \xrightarrow[\frac{1}{2}(1+\beta)]{} x$$

$$\therefore \Delta K_i \xrightarrow[\frac{1}{2}(1+\beta)]{} \Delta\chi_i + lim + x$$

$$\therefore \Delta K_2 \xrightarrow[\frac{1}{2}(1+\beta)]{} \Delta\chi_2 + \bar{\chi}_2 + x$$

$$\therefore \Delta K_2 \xrightarrow[\frac{1}{2}(1+\beta)]{} \chi_2 + x \qquad (F4)$$

and differencing at 31 (R2 p. 70) we get

$$\Delta_{31}(\Delta K_2) \xrightarrow[\frac{1}{2}(1+\beta^2)]{} dot \qquad (F5)$$

(c) $\Delta^2 K$.

In cases where $\Delta^2\chi_i$ and $\Delta^2\chi_j$ each $\rightarrow$ x with high probability

$$\Delta^2\chi_{ij} \longrightarrow dot$$

Now $\Delta^2\Psi'_{ij} \longrightarrow dot$

and therefore $\Delta^2 K_{ij} \longrightarrow dot$ (F 6)

Key has once been recognised by this method (see R3 p 22) (R3 pp 15,76)

Further

$\Delta^2 \psi'$ = stroke at double dots in the TM

$\Delta^2 \chi \xrightarrow[.1]{} /$ since $\Delta^2 \chi_i \xrightarrow[.63]{} \times$

$\Delta^2 K \xrightarrow[.1]{} /$ at double dots in the TM (Ro p 53) (F7)

(d) <u>The sum of key streams.</u>

There are a few words on this topic in 22W(b).

22G THE PLAIN LANGUAGE STREAM

(a) <u>P and ΔP.</u>

Machine methods of work on Tunny make it important that we should be able to recognise plain language not only by its linguistic, but also by its statistical properties.

The statistical properties of the P stream are obvious enough, the frequency of the various letters ranging from that of 9 (space) which normally occurs once in every 6 or 7 letters to that of stroke, 3, and 4 which should not occur at all.

In Δ P the frequency of each letter depends on the frequency of the 32 bigrams which add up to it. The letter count is not as bulgy as that of P, but is of greater basic importance in view of its contribution to the count of ΔD.

Fig. 2 (IV) shows bigram frequencies and their contribution to the various letters of ΔP in a sample of 25,600 letters of Jellyfish June 1944.

The first references to ΔP counts are on Ro pp 21, 45 - 7 and to P counts on R2 pp 83, 110 - 2)

(b) <u>Heterogenous nature of P and ΔP.</u>

Fish messages consist of a mixture of three component types of P: German language (in letter shift), numerals (in figure shift), and punctuation (involving frequent shift changes). The P and ΔP counts for these components are strikingly different and, even within each type the form of the count depended on the operators spacing and punctuation

FIG. 22 (IV)

Frequency of Bigrams in 25,600 letters of Jellyfish traffic of June,1944. The bigrams are sorted by their difference and the no. of occurences of each ΔP letter occurs at the foot of each column.

//	-	/9	-	/H	-	/T	-
99	253	9/	-	9T	57	9H	59
HH	-	HT	51	H/	-	H9	96
TT	45	TH	7	T9	179	T/	-
OO	16	OM	43	ON	61	O3	-
MM	27	MO	26	M3	-	MN	-
NN	69	N3	-	NO	44	NM	2
33	-	3N	-	3M	-	3O	-
RR	30	RC	15	RV	2	RG	34
CC	7	CR	-	CG	-	CV	-
VV	7	VG	10	VR	3	VC	-
GG	4	GV	-	GC	-	GR	53
LL	52	LP	2	LI	40	L4	-
PP	19	PL	4	P4	-	PI	12
II	11	I4	-	IL	29	IP	-
44	-	4I	-	4P	-	4L	-
AA	223	AU	98	AQ	-	AW	-
UU	4	UA	-	UW	-	UQ	-
QQ	11	QW	9	QA	-	QU	17
WW	4	WQ	5	WU	19	WA	24
55	43	58	18	5K	43	5J	-
88	156	85	17	8J	-	8K	46
KK	-	KJ	-	K5	46	K8	29
JJ	-	JK	-	J8	-	J5	3
DD	2	DF	4	DX	-	DB	-
FF	64	FD	6	FB	-	FX	-
XX	-	XB	-	XD	-	XF	-
BB	-	BX	-	BF	2	BD	3
ZZ	8	ZY	-	ZS	-	ZE	43
YY	-	YZ	-	YE	-	YS	-
SS	79	SE	85	SZ	12	SY	-
EE	22	ES	166	EY	5	EZ	11
/	1156	9	566	H	542	T	432

/O	-	/M	-	/N	-	/3	-
9M	106	90	61	93	-	9N	154
HN	21	H3	-	HO	23	HM	20
T3	-	TN	2	TM	14	TO	24
O/	-	O9	76	OH	2	OT	25
M9	284	M/	-	MT	17	MH	-
NH	4	NT	47	N/	-	N9	346
3T	-	3H	-	39	-	3/	-
RL	19	RP	8	RI	81	R4	-
CP	-	CL	-	C4	-	CI	15
VI	23	V4	-	VL	-	VP	-
G4	-	GI	5	GP	-	GL	48
LR	5	LC	-	LV	3	LG	17
PC	-	PR	16	PG	-	PV	-
IV	17	IG	56	IR	18	IC	99
4G	-	4V	-	4C	-	4R	-
A5	48	A8	373	AK	15	AJ	5
U8	8	U5	10	UJ	-	UK	-
QK	-	QJ	-	Q5	-	Q8	18
WJ	-	WK	-	W8	25	W5	18
5A	284	5U	2	5Q	77	5W	70
8U	9	8A	82	8W	18	8Q	4
KQ	-	KW	5	KA	27	KU	5
JW	-	JQ	-	JU	-	JA	9
DZ	-	DY	-	DB	7	DE	170
FY	-	FZ	9	FE	85	FS	5
XS	-	XE	-	XZ	-	XY	16
BE	137	BS	17	BY	-	BZ	-
ZD	-	ZF	-	ZX	-	ZB	5
YF	-	YD	-	YB	-	YX	6
SX	-	SB	-	SD	6	SF	7
EB	36	EX	17	EF	33	ED	45
O	1001	M	786	N	451	3	1131

/R	-	/C	-	/V	-	/G	-
9C	41	9R	101	9G	90	9V	106
HV	-	HG	-	HR	50	HC	-
TG	2	TV	-	TC	-	TR	28
OL	31	OP	12	OI	4	O4	-
MP	8	ML	10	M4	-	MI	44
NI	47	N4	-	NL	2	NP	-
34	-	3I	-	3P	-	3L	-
R/	-	R9	204	RH	5	RT	48
C9	24	C/	-	CT	-	CH	268
VH	-	VT	-	V/	-	V9	28
GT	30	GH	7	G9	87	G/	-
LO	7	LM	9	LN	2	L3	-
PM	2	PO	10	P3	-	PN	-
IN	163	I3	-	IO	16	IM	49
43	-	4N	-	4M	-	4O	-
AD	10	AF	15	AX	-	AB	65
UF	50	UD	-	UB	3	UX	2
QX	6	QB	-	QD	-	QF	-
WB	-	WX	5	WF	-	WD	-
5Z	24	5Y	14	5S	22	5E	17
8Y	-	8Z	27	8E	24	8S	19
KS	-	KE	41	KZ	-	KY	-
JE	2	JS	-	JY	-	JZ	-
DA	42	DU	37	DQ	-	DW	2
FU	25	FA	34	FW	-	FQ	-
XQ	-	XW	2	XA	-	XU	-
BW	8	BQ	-	BU	8	BA	22
Z5	43	Z8	16	ZK	-	ZJ	-
Y8	10	Y5	2	YJ	-	YK	-
SK	2	SJ	-	S5	41	S8	21
EJ	-	EK	6	E8	26	E5	34
R	577	C	549	V	380	G	755

/L	-	/P	-	/I	-	/4	-
9P	54	9L	58	94	-	9I	136
HI	22	H4	-	HL	16	HP	2
T4	-	TI	47	TP	3	TL	29
OR	76	OC	17	OV	-	OG	7
MC	-	MR	14	MG	-	MV	22
NV	2	NG	153	NR	7	NC	4
3G	-	3V	-	3C	-	3R	-
RO	78	RM	33	RN	25	R3	-
CM	-	CO	13	C3	-	CN	4
VN	-	V3	-	VO	55	VM	-
G3	-	GN	4	GM	-	GO	-
L/	-	L9	107	LH	-	LT	23
P9	28	P/	-	PT	2	PH	-
IH	4	IT	104	I/	-	I9	58
4T	-	4H	-	49	-	4/	-
AZ	9	AY	2	AS	42	AE	61
UY	-	UZ	-	UE	97	US	34
QS	3	QE	7	QZ	-	QY	2
WE	94	WS	-	WY	-	WZ	-
5D	-	5F	-	5X	42	5B	5
8F	38	8D	29	8B	25	8X	-
KX	-	KB	-	KD	18	KF	-
JB	-	JX	-	JF	-	JD	-
D5	49	D8	4	DK	2	DJ	2
F8	6	F5	15	FJ	-	FK	7
XK	-	XJ	-	X5	19	X8	37
BJ	-	BK	2	B8	7	B5	21
ZA	9	ZU	47	ZQ	-	ZW	13
YU	2	YA	-	YW	-	YQ	-
SQ	-	SW	9	SA	18	SU	32
EW	16	EQ	-	EU	42	EA	-
L	490	P	665	I	420	4	479

22G Page 55.

FIG. 22 (IV) (Continued)

/A	-	/U	-	/Q	-	/W	-	/5	-	/8	-	/K	-	/J	-	/D	-	/P	-	/X	-	/B	-	/Z	-	/Y	-	/S	-	/E	-
9U	103	9A	218	9W	121	9Q	38	98	813	95	723	9J	7	9K	95	9P	96	9D	194	9B	162	9X	-	9Y	8	9Z	56	9R	124	98	198
HQ	-	NW	10	HA	24	HU	10	HK	-	HJ	-	H5	31	H3	2	HX	-	HB	-	HD	2	HP	-	H3	-	HE	94	HZ	2	HY	-
TW	13	TQ	-	TU	18	TA	75	TJ	-	TK	3	T8	21	T5	96	TB	-	TX	-	TF	-	TD	4	TK	188	TS	16	TI	-	TZ	51
O5	19	O8	6	OK	15	OJ	-	QA	-	OU	2	OQ	2	OW	2	OE	-	OI	-	O8	38	OB	66	OD	2	OF	12	OX	-	OB	32
MB	382	N5	38	MJ	-	MK	-	MU	6	MA	208	MY	2	MQ	-	MT	31	MX	-	MR	92	M8	7	MP	5	MD	-	MB	-	MX	-
HK	17	NJ	-	N5	78	N8	79	NQ	-	NW	17	NA	75	NU	11	NS	28	NK	84	NE	18	NY	-	NX	-	NB	10	ND	151	NF	22
3J	-	3K	-	3S	-	35	-	3W	-	3Q	-	3U	-	3A	-	3Z	-	38	-	3Y	-	3Z	-	3B	-	3X	-	3P	-	3D	-
HD	43	HP	21	RX	4	RB	12	RE	8	RT	-	R8	51	RR	98	RA	78	RU	36	RQ	10	RW	13	R5	52	R8	22	RK	26	RJ	-
GY	-	GD	-	GB	-	GX	-	OY	-	OZ	-	GR	2	O8	-	OU	3	GA	28	GW	-	OQ	-	O8	19	O5	27	GJ	-	OK	15
VI	-	VB	-	VD	-	VP	-	VB	-	VE	40	VZ	-	VY	-	VQ	-	VW	-	VA	7	VU	-	VK	-	VJ	-	V5	19	VB	41
GB	-	GI	-	GF	-	GD	-	GZ	190	G8	8	GY	-	GZ	-	GW	2	GQ	-	GU	21	GA	6	GJ	-	GK	8	G8	11	O5	30
LZ	2	LY	-	LS	17	LE	68	LD	28	LP	-	LX	-	L8	3	L6	42	L8	50	LK	-	LJ	-	LA	84	LU	22	LQ	-	LW	4
PY	-	PZ	4	PE	17	P8	-	PP	10	PD	-	P6	-	PX	-	P8	17	P5	16	PJ	-	PK	3	PU	6	PA	21	PW	2	PQ	2
IS	66	IR	107	IZ	-	II	-	IX	2	IB	6	ID	5	IF	27	IX	24	IJ	-	I5	23	I8	5	IQ	2	IW	-	IA	17	IU	4
4Z	-	4S	-	4T	-	4Z	-	4B	-	4X	-	4P	-	4D	-	4J	-	4K	-	48	-	45	-	4W	-	4Q	-	4U	-	4A	-
A/	-	A9	185	AM	22	AT	14	AO	3	AM	52	AN	202	A3	-	AR	47	AC	47	AV	10	AG	33	AL	55	AP	-	AI	4	A4	-
U9	31	U/	-	UT	15	UH	8	UM	53	UO	-	U3	-	UK	153	UD	18	UR	58	UG	19	UY	2	UP	9	UL	3	U4	-	UI	10
QE	-	QT	-	Q/	-	Q9	19	QN	-	Q3	-	QO	6	QM	8	QT	-	QG	-	QR	9	QO	-	QI	2	Q4	-	QL	5	QP	4
WT	11	WH	-	W9	63	W/	-	W3	-	WN	8	WM	18	WO	13	WG	-	WY	-	WC	-	WR	2	W4	-	WI	19	WP	12	WL	4
5O	9	5M	617	5N	62	53	-	5/	-	59	36	5H	-	5T	10	5L	63	5P	10	5I	11	54	-	5R	27	5C	61	5Y	38	5G	-
8M	20	8O	34	83	-	8N	21	89	1491	8/	-	8T	5	8H	7	8P	12	8L	4	84	-	8I	2	8O	7	8R	45	8G	31	8V	19
KN	3	K3	-	KD	16	KM	25	KH	13	KT	6	K/	-	K9	38	KI	-	K4	-	KL	17	KP	7	KY	2	KE	3	KR	25	KC	-
J3	-	JW	-	JM	3	JO	3	JT	-	JH	-	J9	-	J/	-	J4	-	JI	-	JP	-	JL	2	JG	-	JV	-	JO	-	JR	-
IR	8	DO	-	DW	-	DG	7	DL	26	DP	-	DI	55	D4	-	D/	-	D9	85	IH	-	DT	6	DO	29	IM	2	IM	-	D5	-
FO	-	FR	16	FG	6	FY	-	FP	3	FL	14	F4	-	FI	6	F9	65	P/	-	FT	16	FH	17	FM	-	FO	19	F5	-	FK	4
XV	-	XD	-	XR	4	XC	-	XI	-	XA	-	XL	-	XP	-	XH	-	XT	-	X/	-	X9	-	XN	-	X3	-	XD	-	XM	-
BG	4	BV	-	BC	-	HR	31	B4	-	BI	34	BP	-	BL	7	BT	21	BH	5	B9	18	V/	-	B3	-	BN	-	BM	-	BO	22
ZL	-	ZP	-	ZI	-	ZA	-	ZR	2	ZO	-	ZY	-	ZG	-	ZO	3	ZM	-	ZN	-	Z5	-	Z/	-	Z9	33	ZK	-	ZT	16
YP	-	YL	2	YA	-	YI	-	YC	-	YR	-	YG	-	YV	-	YM	42	YD	-	Y3	-	YN	-	Y9	19	Y/	-	YT	4	YH	-
8I	36	8A	-	8L	5	8P	4	8Y	-	8G	6	8R	-	8C	90	8K	2	83	-	8O	23	8K	-	8H	9	8E	188	S/	-	89	134
ZA	-	KI	214	XP	8	BL	90	BO	50	BY	5	RO	23	RR	383	R3	-	RN	374	RM	80	RQ	-	RT	96	RH	51	R9	224	E/	-
A	767	U	1472	Q	498	W	504	5	2698	8	1168	K	505	J	1049	D	594	P	991	X	576	B	175	Z	621	Y	712	S	695	E	612

22G Page 56

FIG. 22 (Y)

THE Ψ' STREAM

	DELTA Ψ'(X2 Lim.)											DELTA Ψ'					
	27		24		21		18		15			27	24	21	18	15	
	Lx	L.	Lx	L.	Lx	L.	Lx	L.	Lx	L.							
/	1155	0000	1017	0002	0867	0004	0746	0006	0646	0012	/	1120	1032	0871	0787	0678	/
9	0000	0003	0003	0010	0007	0012	0009	0015	0010	0024	9	0003	0009	0017	0021	0024	9
H	0005	0007	0007	0017	0015	0023	0010	0022	0014	0044	H	0008	0021	0032	0039	0060	H
T	0000	0005	0001	0003	0007	0005	0005	0017	0009	0018	T	0002	0007	0013	0020	0032	T
O	0004	0009	0002	0014	0009	0021	0014	0023	0017	0033	O	0016	0020	0030	0038	0057	O
M	0006	0043	0012	0058	0022	0061	0032	0054	0040	0066	M	0048	0066	0079	0086	0098	M
N	0002	0012	0003	0013	0012	0015	0010	0035	0021	0031	N	0017	0018	0032	0041	0046	N
3	0000	0006	0001	0007	0005	0009	0007	0016	0011	0014	3	0005	0012	0016	0020	0031	3
R	0002	0016	0008	0020	0011	0025	0017	0035	0024	0033	R	0011	0025	0032	0046	0055	R
C	0016	0040	0014	0039	0018	0056	0030	0059	0036	0058	C	0053	0056	0069	0098	0106	C
V	0037	0170	0041	0128	0040	0121	0065	0102	0054	0104	V	0209	0174	0185	0167	0153	V
G	0011	0045	0016	0046	0019	0060	0020	0061	0044	0064	G	0059	0049	0065	0076	0099	G
L	0003	0008	0003	0013	0008	0019	0013	0028	0027	0054	L	0013	0020	0032	0047	0060	L
P	0012	0043	0016	0036	0019	0053	0021	0068	0041	0051	P	0060	0054	0068	0067	0088	P
I	0001	0013	0006	0010	0003	0017	0013	0026	0019	0031	I	0020	0015	0018	0045	0050	I
4	0001	0005	0002	0004	0000	0008	0009	0011	0010	0017	4	0007	0006	0013	0025	0027	4
A	0002	0013	0003	0013	0005	0024	0016	0032	0015	0025	A	0014	0016	0024	0043	0040	A
U	0006	0041	0011	0041	0019	0041	0033	0061	0023	0059	U	0044	0053	0062	0088	0081	U
Q	0030	0128	0053	0115	0048	0115	0045	0085	0048	0099	Q	0157	0164	0168	0149	0145	Q
W	0013	0029	0015	0039	0024	0044	0027	0048	0030	0059	W	0040	0048	0060	0067	0090	W
5	0030	0141	0048	0117	0045	0117	0056	0098	0051	0098	5	0172	0177	0176	0156	0151	5
8	0105	0486	0106	0386	0122	0274	0108	0228	0090	0165	8	0600	0487	0375	0327	0259	8
K	0035	0129	0040	0139	0057	0118	0057	0115	0050	0091	K	0171	0173	0180	0158	0137	K
J	0012	0030	0009	0041	0015	0043	0029	0056	0029	0050	J	0051	0053	0063	0089	0083	J
D	0001	0008	0007	0021	0015	0018	0012	0032	0020	0040	D	0010	0024	0031	0044	0054	D
F	0007	0037	0012	0048	0016	0053	0018	0057	0021	0049	F	0042	0055	0064	0077	0075	F
X	0032	0110	0038	0140	0046	0142	0043	0102	0050	0094	X	0147	0181	0192	0145	0150	X
B	0007	0032	0023	0052	0024	0064	0033	0045	0031	0056	B	0037	0070	0088	0074	0079	B
Z	0002	0009	0004	0018	0005	0025	0010	0029	0019	0026	Z	0013	0019	0029	0040	0039	Z
Y	0009	0026	0017	0044	0029	0038	0023	0048	0024	0059	Y	0039	0064	0073	0062	0077	Y
S	0002	0010	0009	0013	0010	0024	0015	0028	0019	0018	S	0012	0026	0036	0045	0046	S
E	0000	0000	0001	0005	0006	0006	0002	0010	0008	0025	E	0000	0006	0009	0013	0032	E
	1548	1652	1548	1652	1548	1652	1548	1652	1548	1652		3200	3200	3200	3200	3200	
AVG.··	1405	1077	1331	1015	1279	923	1204	911	1104	893		2458	2356	2198	2129	2012	•

FIG. 22 (VI)

THE D-STREAM TYPE A (GAL 3110 8.4.45.)

Dottage

	P	ΔP		DELTA D (X2 lim.) 27 Lx	27 L.	24 Lx	24 L.	21 Lx	21 L.	18 Lx	18 L.	15 Lx	15 L.		DELTA D (X2+[illegible] lim.) 27	24	21	18	15	
/	0002	0560	/	0205	0063	0189	0049	0165	0043	0141	0052	0124	0046	/	0265	0259	0234	0208	0186	/
9	0529	0051	9	0039	0072	0042	0063	0050	0066	0039	0063	0045	0067	9	0104	0116	0094	0103	0102	9
H	0054	0061	H	0036	0045	0042	0059	0045	0059	0029	0069	0028	0063	H	0088	0091	0084	0085	0101	H
T	0096	0063	T	0040	0058	0045	0049	0035	0043	0038	0048	0045	0060	T	0081	0079	0098	0105	0093	T
O	0076	0096	O	0044	0072	0053	0060	0051	0051	0040	0054	0051	0051	O	0090	0106	0102	0110	0089	O
M	0210	0083	M	0035	0057	0038	0046	0049	0061	0052	0072	0050	0060	M	0096	0106	0105	0104	0092	M
N	0117	0051	N	0033	0045	0031	0058	0032	0050	0039	0054	0038	0038	N	0080	0077	0080	0087	0087	N
3	0082	0109	3	0061	0042	0064	0051	0063	0048	0050	0053	0046	0054	3	0100	0108	0089	0100	0098	3
R	0116	0068	R	0034	0043	0030	0041	0038	0044	0038	0055	0038	0047	R	0070	0065	0077	0084	0091	R
C	0037	0084	C	0051	0040	0045	0059	0041	0049	0057	0046	0045	0048	C	0085	0092	0105	0089	0094	C
V	0048	0044	V	0031	0076	0028	0075	0029	0069	0053	0065	0043	0048	V	0081	0105	0107	0101	0110	V
G	0066	0060	G	0036	0041	0033	0047	0033	0051	0036	0060	0042	0062	G	0070	0072	0069	0098	0097	G
L	0073	0052	L	0035	0036	0029	0037	0032	0041	0032	0055	0030	0056	L	0075	0075	0085	0093	0083	L
P	0046	0065	P	0029	0043	0048	0055	0038	0054	0044	0059	0057	0058	P	0072	0094	0086	0077	0101	P
I	0070	0064	I	0032	0045	0040	0053	0031	0045	0045	0060	0049	0056	I	0097	0078	0086	0094	0098	I
4	0001	0067	4	0042	0053	0039	0046	0036	0047	0034	0051	0041	0041	4	0083	0093	0075	0083	0094	4
A	0145	0125	A	0058	0044	0055	0042	0069	0041	0054	0048	0054	0045	A	0089	0080	0107	0098	0117	A
U	0074	0191	U	0081	0054	0088	0053	0078	0042	0084	0043	0070	0048	U	0133	0139	0108	0115	0119	U
Q	0027	0069	Q	0041	0055	0041	0053	0046	0066	0042	0045	0049	0056	Q	0103	0103	0105	0106	0099	Q
W	0043	0081	W	0038	0048	0035	0033	0046	0045	0044	0044	0049	0048	W	0084	0083	0076	0075	0082	W
5	0425	0275	5	0102	0057	0105	0048	0090	0063	0073	0041	0073	0051	5	0166	0165	0166	0119	0134	5
8	0465	0171	8	0087	0108	0073	0096	0086	0091	0088	0075	0065	0075	8	0212	0181	0157	0135	0132	8
K	0026	0065	K	0036	0055	0041	0066	0045	0058	0055	0035	0042	0044	K	0095	0078	0096	0088	0104	K
J	0088	0084	J	0040	0038	0031	0030	0037	0033	0034	0052	0037	0050	J	0103	0090	0074	0104	0088	J
D	0053	0084	D	0037	0043	0042	0049	0040	0039	0029	0034	0043	0058	D	0081	0077	0084	0087	0096	D
F	0042	0091	F	0042	0056	0047	0049	0039	0045	0052	0045	0048	0055	F	0096	0085	0099	0103	0102	F
X	0023	0074	X	0044	0064	0045	0055	0035	0073	0052	0051	0043	0051	X	0093	0110	0124	0100	0101	X
B	0031	0046	B	0029	0033	0037	0043	0031	0042	0038	0052	0041	0038	B	0073	0066	0076	0108	0093	B
Z	0030	0069	Z	0037	0044	0024	0046	0030	0049	0037	0043	0040	0043	Z	0077	0088	0082	0087	0087	Z
Y	0022	0079	Y	0036	0040	0034	0052	0042	0045	0035	0053	0042	0049	Y	0095	0093	0097	0091	0095	Y
S	0067	0059	S	0027	0042	0030	0046	0040	0057	0031	0041	0041	0047	S	0082	0078	0103	0069	0072	S
E	0176	0059	E	0033	0040	0024	0043	0026	0042	0033	0034	0039	0039	E	0081	0068	0070	0074	0063	E
	3200	3200		1548	1652	1548	1652	1548	1652	1548	1652	1548	1652		3200	3200	3200	3200	3200	
ΔD12 = .		2135		973	913	973	896	987	859	902	848	866	796		1889	1861	1775	1762	1723	

FIG 22(VII)

THE D-STREAM TYPE 6 (CEP [illegible] 9.4.44)

DELTA D ($\overline{X}_2$ lim.) | DELTA D ($\overline{X}_2$ $\overline{\Psi}_1$ lim.)

	P	ΔP		27 Lx	27 L.	24 Lx	24 L.	21 Lx	21 L.	18 Lx	18 L.	15 Lx	15 L.		27	24	21	18	15	
/	0008	0074	/	0050	0060	0046	0075	0046	0048	0052	0067	0045	0058	/	0089	0122	0110	0119	0101	/
9	0468	0069	9	0045	0083	0041	0085	0054	0055	0047	0065	0046	0057	9	0107	0130	0096	0106	0109	9
H	0056	0094	H	0054	0092	0058	0076	0045	0065	0062	0049	0051	0074	H	0104	0092	0127	0113	0104	H
T	0087	0056	T	0039	0042	0035	0060	0047	0058	0038	0056	0042	0057	T	0103	0089	0095	0101	0095	T
O	0061	0140	O	0057	0070	0056	0073	0070	0058	0048	0044	0044	0052	O	0133	0135	0144	0114	0129	O
M	0280	0098	M	0050	0066	0052	0060	0048	0052	0045	0045	0052	0063	M	0105	0105	0104	0100	0114	M
N.	0167	0077	N	0039	0043	0030	0042	0038	0053	0033	0056	0037	0064	N	0092	0094	0098	0092	0106	N
3	0001	0105	3	0053	0052	0055	0049	0056	0046	0056	0045	0060	0051	3	0101	0083	0106	0114	0115	3
R	0155	0088	R	0044	0035	0032	0042	0048	0048	0045	0050	0047	0034	R	0081	0086	0087	0086	0092	R
C	0041	0082	C	0043	0042	0038	0035	0037	0037	0043	0041	[illegible]	0047	C	0069	0082	0068	0077	0074	C
V	0042	0051	V	0031	0047	0031	0045	0026	0061	0043	0059	0037	0042	V	0076	0077	0084	0078	0076	V
G	0074	0111	G	0048	0050	0040	0059	0047	0059	0045	0049	0055	0046	G	0104	0095	0095	0097	0109	G
L	0086	0069	L	0033	0068	0044	0053	0040	0052	0085	0058	0051	0051	L	0102	0100	0106	0088	0091	L
P	0041	0086	P	0041	0067	0042	0052	0048	0060	0046	0051	0043	0052	P	0096	0112	0106	0110	0111	P
I	0177	0048	I	0021	0033	0032	0048	0038	0061	0040	0062	0038	0067	I	0089	0086	0094	0094	0103	I
4	0003	0069	4	0031	0040	0036	0045	0038	0055	0045	0062	0040	0049	4	0075	0077	0087	0083	0088	4
A	0164	0172	A	0069	0050	0074	0042	0064	0043	0059	0055	0066	0055	A	0139	0115	0131	0124	0114	A
U	0080	0246	U	0109	0050	0094	0053	0090	0063	0081	0067	0084	0055	U	0148	0178	0134	0129	0161	U
Q	0014	0069	Q	0037	0042	0051	0055	0039	0066	0046	0037	0037	0054	Q	0097	0095	0070	0101	0096	Q
W	0033	0058	W	0030	0052	0037	0042	0030	0060	0034	0044	0043	0039	W	0071	0089	0099	0095	0072	W
5	0260	0321	5	0128	0040	0122	0041	0099	0040	0103	0047	0074	0054	5	0171	0169	0156	0144	0113	5
8	0266	0174	8	0073	0038	0078	0041	0067	0055	0060	0056	0058	0055	8	0131	0112	0103	0098	0103	8
K	0068	0066	K	0033	0037	0034	0048	0036	0036	0037	0049	0042	0058	K	0078	0064	0089	0075	0074	K
J	0009	0153	J	0077	0039	0064	0035	0070	0037	0059	0047	0063	0047	J	0125	0110	0106	0098	0108	J
D	0083	0115	D	0057	0036	0056	0037	0045	0049	0047	0037	0046	0050	D	0109	0091	0087	0100	0097	D
F	0046	0121	F	0055	0040	0054	0045	0053	0046	0048	0055	0048	0069	F	0098	0088	0095	0102	0101	F
X	0014	0095	X	0040	0041	0049	0061	0045	0040	0052	0044	0052	0044	X	0098	0093	0096	0102	0100	X
B	0039	0030	B	0019	0053	0023	0037	0029	0047	0032	0055	0037	0045	B	0068	0069	0060	0078	0071	B
Z	0036	0053	Z	0025	0053	0038	0040	0034	0055	0026	0048	0046	0065	Z	0095	0081	0084	0086	0082	Z
Y	0005	0056	Y	0045	0067	0036	0074	0044	0042	0040	0049	0052	0031	Y	0067	0077	0079	0091	0098	Y
S	0074	0098	S	0045	0060	0036	0065	0041	0057	0050	0050	0041	0042	S	0111	0111	0121	0111	0097	S
E	0262	0056	E	0027	0064	0034	0037	0036	0045	0030	0053	0037	0045	E	0068	0085	0083	0094	0096	E
	3200	3200		1548	1652	1548	1652	1548	1652	1548	1652	1548	1652		3200	3200	3200	3200	3200	
[illegible]13*		1972		0943	0856	0927	0877	0899	0835	0860	0829	0844	0893		1794	1782	1768	1723	1714	

FIG. 22 (VIII)
THE D-STREAM TYPE C (JB 8347 20.3.45.)

	P	ΔP		27		DELTA D (X2 Lim.) 24		21		18		15			27	DELTA D (X2+ 1 lim.) 24	21	18	15
				Lx	L.	Lx	L.	Lx	L.	Lx	L.	Lx	L.						
/	0002	0100	/	0054	0043	0054	0055	0056	0061	0051	0049	0060	0057	/	0100	0095	0111	0090	0097
9	0428	0073	9	0035	0067	0035	0088	0050	0055	0041	0067	0043	0054	9	0082	0104	0078	0092	0105
H	0092	0088	H	0052	0053	0043	0058	0053	0060	0054	0046	0042	0068	H	0118	0102	0091	0099	0082
T	0173	0073	T	0044	0061	0042	0061	0042	0063	0048	0064	0041	0054	T	0101	0092	0093	0110	0099
O	0055	0093	O	0046	0048	0043	0060	0049	0032	0059	0050	0050	0054	O	0104	0098	0096	0105	0101
M	0094	0060	M	0041	0052	0039	0045	0036	0065	0035	0049	0042	0042	M	0087	0075	0102	0085	0117
N	0298	0080	N	0038	0049	0048	0045	0045	0074	0038	0052	0042	0063	N	0078	0083	0083	0088	0072
3	0003	0218	3	0088	0070	0075	0059	0075	0055	0088	0053	0067	0053	3	0130	0131	0126	0123	0135
R	0172	0091	R	0034	0059	0040	0043	0047	0046	0034	0053	0039	0045	R	0099	0113	0099	0101	0095
C	0074	0072	C	0042	0046	0032	0057	0041	0041	0041	0039	0042	0043	C	0075	0085	0080	0085	0095
V	0032	0053	V	0034	0052	0047	0046	0039	0049	0041	0063	0040	0045	V	0088	0102	0080	0092	0084
G	0083	0147	G	0068	0051	0068	0059	0076	0055	0055	0050	0070	0059	G	0128	0116	0132	0117	0113
L	0073	0066	L	0048	0080	0050	0059	0057	0056	0040	0055	0047	0051	L	0108	0105	0111	0107	0101
P	0045	0107	P	0044	0060	0053	0057	0048	0068	0055	0054	0053	0051	P	0104	0097	0107	0103	0110
I	0172	0076	I	0029	0034	0038	0054	0040	0051	0042	0043	0057	0043	I	0080	0087	0103	0071	0107
4	0001	0075	4	0034	0042	0035	0060	0038	0036	0049	0055	0043	0055	4	0081	0111	0084	0103	0093
A	0156	0072	A	0039	0040	0055	0038	0028	0043	0048	0051	0043	0041	A	0095	0090	0091	0094	0102
U	0107	0158	U	0091	0045	0084	0062	0076	0045	0073	0050	0072	0052	U	0108	0130	0128	0098	0099
Q	0014	0095	Q	0049	0073	0051	0057	0046	0060	0042	0063	0029	0058	Q	0129	0117	0120	0127	0103
W	0045	0074	W	0029	0042	0040	0053	0040	0052	0045	0044	0034	0060	W	0100	0112	0083	0104	0096
5	0086	0149	5	0055	0038	0044	0044	0052	0047	0052	0048	0050	0050	5	0119	0108	0103	0114	0112
8	0085	0095	8	0046	0048	0048	0051	0036	0059	0038	0057	0055	0055	8	0106	0095	0094	0098	0103
K	0042	0075	K	0033	0048	0036	0047	0042	0058	0033	0041	0036	0050	K	0076	0082	0078	0084	0100
J	0004	0167	J	0069	0053	0074	0046	0065	0042	0063	0049	0060	0066	J	0113	0096	0107	0122	0107
D	0105	0066	D	0034	0040	0026	0038	0043	0048	0043	0055	0049	0049	D	0092	0087	0099	0075	0104
F	0083	0220	F	0083	0042	0084	0046	0068	0037	0067	0039	0070	0040	F	0134	0134	0121	0120	0116
X	0008	0078	X	0049	0046	0041	0039	0050	0048	0040	0052	0038	0037	X	0071	0089	0098	0103	0091
B	0057	0026	B	0019	0060	0023	0046	0018	0045	0032	0052	0032	0049	B	0080	0068	0085	.0078	0078
Z	0053	0112	Z	0049	0049	0043	0047	0047	0046	0033	0045	0031	0048	Z	0092	0095	0101	0081	0100
Y	0008	0118	Y	0067	0056	0051	0048	0047	0062	0064	0066	0062	0054	Y	0113	0110	0119	0115	0099
S	0126	0119	S	0060	0058	0050	0036	0054	0050	0066	0055	0053	0046	S	0118	0109	0111	0132	0091
E	0424	0104	E	0045	0047	0056	0048	0044	0043	0038	0043	0056	0060	E	0091	0082	0086	0084	0093
	3200	3200		1548	1652	1548	1652	1548	1652	1548	1652	1548	1652		3200	3200	3200	3200	3200
$\Delta D_{34} = x$		1791		These figures are not entered as $\Delta D_{3+4} \times \Delta D_{1+2}$ are normally counted before X2 is set and limitation positions determined (See 23)											1717	1673	1704	1672	1641
$\Delta D_{12} = \bullet$		1821													1706	1727	1721	1733	1636

FIG 22 (IX)

Some further $\Delta P + \Delta D$ counts showing the main types combined in various proportions, and the characteristic features of some well defined, but less frequent types. Should be read in conjunction with more typical counts given in Figs 12 (II) and 22(VI - VIII).

	1	2	3	4	5	6
	ΔP	ΔD 26 dots JB	ΔD 28dots JB	ΔD 26 dots GDB	ΔD 26 dots C2Z	ΔD 20 dots JP
/	149	$\boxed{175}$	213	117	$\boxed{188}$	164
9	46	95	166	148	$\boxed{189}$	111
H	142	119	102	94	123	102
T	40	83	79	69	86	87
O	71	116	88	$\boxed{176}$	114	97
M	115	98	88	120	73	116
N	13	90	101	78	85	82
3	23	96	122	111	98	119
R	4	88	86	98	92	82
C	224	85	80	62	86	93
V	4	72	79	80	73	109
G	13	103	110	138	77	97
L	346	93	72	96	72	89
P	44	60	78	96	82	87
I	72	108	79	64	89	87
4	93	72	80	76	77	89
A	147	106	65	85	79	84
U	230	119	95	$\boxed{168}$	102	118
Q	324	129	96	95	77	108
W	275	57	90	95	88	93
5	32	$\boxed{183}$	161	126	$\boxed{224}$	136
8	112	132	$\boxed{255}$	110	$\boxed{189}$	106
K	15	70	63	80	92	93
J	41	134	110	130	92	120
D	1	80	71	86	73	72
F	26	116	92	114	76	121
X	27	101	70	94	68	103
B	52	72	60	55	66	70
Z	158	75	71	86	105	99
Y	13	111	82	86	76	116
S	286	108	90	94	98	72
E	62	54	106	73	91	89
COUNTS ARE NORMALISED TO	3200	3200	3200	3200	3200	3200
LENGTH OF SAMPLE	2480	1240	5249	1848	2191	5003
STANDARD DEVIATION (FOR THE RANDOM CASE) OF EACH ENTRY $100\sqrt{\frac{32}{N}}$	11•2	15•7	7•7	12•9	11•9	6•2

1. ΔP count described in 22G(c)(6). Numerals interspersed with 99. No letter shift at all.
2. Strong in / and 5 and in some language letters I is surprisingly high, P surprisingly low and W and E lower than would be normally expected.
3. See 22G(c)(4). 8 is strong enough in ΔP to dominate ΔD and to increase the frequency in ΔD of 9 and E to a higher level than usual.
4. Count dominated by U and O. A combination of strong language and 5M98 punctuation.
5. A typical Codfish Zagreb in which letters differing in the third impulse differ little in frequency. Hard to set on χ_3 for this reason.

habits.

Some messages consist entirely of German, of abbreviations and punctuation, or even of numerals, but in most messages there is a heterogeneous mixture of Hand patches (German language with irregular spacing)

Addresses (Abbreviations and punctuation)

Message content (Language usually with some abbreviations and numerals)

and occasional places where the tape sticks and the same letter of P is transmitted until the tape is adjusted. (RO p 67)

(c) <u>Component types of language</u>.

(1) German Language (Type C)

The P and ΔP counts for German Language with single 9 spacing vary little in shape, those given in Fig. 22 (VI) being a good example. In P, it will be noticed that the most popular language letter E is almost as frequent as 9, and that other good language letters N, R, I, A, S occur with frequency well above random. The message being largely in lettershift (except for incidental punctuation) the shift change letters 5 and 8 are both below random. Q, J, X, Y are rare.

In ΔP, the most significant letters are : F (= E + N), 3 (= N + 9) J (= E + R = U + N), U (= 5 + M = I + E), 5 (= 9 + 8), G and S which are all high, and B whose 13 contributing bigrams are all feeble. (R2 pp 97-100)

(2) <u>Single Punctuation</u> (Type B)

All punctuation signs are sent in figure shift, and unless punctuation follows or precedes numerals each sign must be preceded by a 5 and followed by an 8. The most common form of punctuation is the full stop, which occurs extensively in abbreviations and addresses, and has the basic form 5M89 or 5MA89.

Fig. 22 (VII) shows P and ΔP for a standard type of message consisting largely of German language abbreviated with 5M89. 9 which is frequent (in P) both for punctuation and for language is well ahead of any other letter. It is followed (at a distance) by the punctuation letters 5M8, and E at the head of the language group.

In ΔP, the German language letters are still strong (but in a part of the message only), and the lead is taken by 5 (= 9 + 8), U (= 5 + M = I + E), A (= M + 8) and 8 (= M + A = 5 + 9), 5 + U being especially strong in most cases.

(3) Double Punctuation (Type A)

In practice punctuation is often modified according to the habits of the operator perforating the tape. Many operators were trained to change from figure to letter shift and vice versa by depressing the shift keys twice (or more) to ensure that the shift change actually took place. These operators were mostly employed at the Königsberg exchange or on Rome Bream, but after the Königsberg exchange had moved to Berlin double punctuation made a general appearance in the West (see also R4 p 5).

Fig 22 (VIII) shows P and ΔP counts for a message with double punctuation. In the P count 5 and 8 are almost twice as frequent as they are in the single punctuation count [Fig 22 (VII)], and are almost as high as 9. Language naturally forms a small proportion of the message and the strength of language letters is reduced.

The main significance of double punctuation lies in the inflation of stroke in ΔP, so that strokes may occur with 3 - 6 times random frequency.

(4) Other operators habits (auto).

Certain other forms of punctuation are popular on particular links or with particular operators: they are given differenced and undifferenced so that their contribution to ΔP can be estimated

P:	5M98	ΔP:	U05
	5M989		U055
	5MMA89		U/8M5
	55KK889, 55LL889 (Brackets)		/H/T/5, /D/P/5 and so on.

In some messages 9 is inserted before all punctuation and 8 is the highest letter in ΔP. A few operators divide words with 89 or even 989 and this inflates 5 to a high level in ΔP even in German language messages with little punctuation.

(5) Operators habits (hand)

Spacing and punctuation in hand is erratic, and even the most improbable letters may be inflated by operators who tap out some pair of letters in turn while thinking, e.g. LALALALA

(6) Numerals

The most common letters in undifferenced numerals are P, Q, and W. In general, numerals are rarely sufficiently frequent to make much difference to the shape of P or ΔP counts.

Occasional examples of messages consisting entirely of numerals have occurred. A good example is a message giving a sheet of QEP numbers whose letter count is given in Fig 22 (IX). (R4 p 16.)

(7) Freaks.

It is unreliable to reject any letter count with significant bulges however oddly arranged these bulges appear to be. A few of the last German messages ever sent on Tunny gave some new wheel patterns and consisted almost entirely of the words NOCKE and KEINE separated by commas e.g.

P NOCKE5N89NOCKE5N89KEINE5N89
ΔP HPEOGQW53HPEOGQW5JCURFGQW5

(d) <u>P counts on 1-2 impulses.</u>

The best P_1 bulge is on P_3 = x for punctuation (single or double) and on P_5 = dot for language. Normally P_1, P_2, P_4, $P_5 \longrightarrow$ dot and $P_3 \longrightarrow$ x but if 5's and 8's in P are very strong, they may be sufficient to negative the bulges on P_1, P_2, P_4 and P_5.

Fig. 22 (X) shows the one and two impulse bulges for the 3 messages (type A, type B, type C) whose full counts are given in Figs. 22 (VI), 22 (VII), 22 (VIII), and average bulges for a set of messages described in R5 p 84.

	A	B	C	Crude av. of 57 messages
P_1 = .	1543	1747	1797	1660
P_2 = .	1530	1687	2009	1720
P_3 = x	1857	1837	1708	1800
P_4 = .	1455	1594	1919	1660
P_5 = .	1465	1806	2197	1720
P_{45} = .	2408	2272	1916	2240
P_{12} = .	2299	2022	1684	2100
P_{13} = x	1951	2074	2116	2080
P_{25} = .	2181	1925	1932	2060
P_{24} = .	2167	1881	1884	2040
ΔP_2 = .	1565	1863	1572	
ΔP_{12} = .	2135	1972	1670	
ΔP_{13} = .	1874	1637	1821	
ΔP_{34} = x	1461	1829	1791	
ΔP_{25} = .	1881	1654	1766	
ΔP_{45} = .	2025	1852	1478	

FIG 22 (X)

(e) <u>ΔP counts on 1 and 2 impulses.</u>

Bulges on ΔP_1 are of interest only in the case of ΔP_2 on messages with $\overline{\chi}_2$ limitation. $\Delta P_2 \rightarrow$ cross in messages strong in single punctuation. Double punctuation will normally cancel out the tendency for $\Delta P_2 \rightarrow$ x, but only rarely produces a comparable bulge on ΔP_2 = dot.

Except when a message consists almost exclusively of German language, the best ΔP_{ij} bulge is on $\Delta P_{12} \rightarrow$ dot. On German language, the bulge on $\Delta P_{12} \longrightarrow$ dot is weak (though usually positive) and the best bulges are on $\Delta P_{34} \rightarrow x$ and $\Delta P_{13} \longrightarrow$ dot. See Fig 22(x)

PB $(\Delta P_i =$ dot$)$ is defined as π_i
PB $(\Delta P = \Theta)$ is defined as π_Θ

<u>(f) $\Delta^2 P$</u>

A $\Delta^2 P$ letter count and the corresponding ΔP count is given in R3 p.86. The bulginess of $\Delta^2 P$ is the more marked, the frequency of U being about 8% and O 8 M 3 4 all occurring over 5 % of the time. (R0 p.50.)

<u>(g) Bigrams in P and Δ P.</u>

Fig 22 (IV) gives a table of Bigram frequency in P.

No statistics of Δ P bigrams were taken.

<u>(h) The sum of two P streams.</u>

By considering the frequency of letters in $Z_a + Z_b$ for two messages (a,b) alleged to be in depth it is sometimes possible to decide whether $Z_a + Z_b = P_a + P_b$ and the messages are infact in depth or not. A Scoring table for alleged depths is given in 22 V (c).

<u>22H THE DECHI STREAM</u>

$D = P + \Psi'$ $\qquad\qquad \therefore \quad \Delta D = \Delta P + \Delta\Psi'$

The undifferenced Ψ' stream is flat, therefore the undifferenced D stream is flat and unrecognisable statistically. [(E3)]

<u>(a) Frequency of letters in Δ D</u>

Applying (E1) and (E2) we get

$$P(\Delta D = \Theta) = \sum_{\Phi} \left\{ P(\Delta\Psi' = \Phi) . P(\Delta P = \Theta + \Phi) \right\} \qquad \text{(H1)}$$

$$\delta_\Theta = p\delta(\Delta D = \Theta) = \frac{1}{32} \sum_{\Phi} \left\{ \beta'_\Phi . \pi_{\Theta+\Phi} \right\} \qquad \text{(H2)}$$

The most important contribution to the frequency of any letter Θ in ΔD comes from the proportion of places in which there is a Θ in ΔP and a stroke in $\Delta\Psi'$. Now $P(\Delta\Psi' = /) = (1-a) + a(1-b)^5$ = approx. $(1-a)$, and $(1-a)$ varies in value from .18 when there are 14 dots to .38 when there are 28 dots.

As a result, 1/5 - 2/5 of the ΔP stream is reproduced exactly in the ΔD stream, and, assuming (as a first approximation) that ΔD is flat when $\Delta\Psi' \neq /$, we can see how ΔD count can be thought of as a ΔP count "watered down" by the addition of random material from the places where there is a T.M. x and no extension of the pais. As the dottage increases more and more of the ΔP stream is reproduced in ΔD, and the stronger is the ΔD count for a given ΔP count.

In fact, ΔD is not flat when $\Delta \Psi' \neq /$, for the frequency of 8 in $\Delta \Psi'$ (and even the frequency of V,X,5,Q,K) is sufficiently high to ensure that a high letter (Θ) in ΔP will make a considerable contribution to the frequency of (Θ + 8) and of (Θ + V) etc. in ΔD. Letters whose frequency in ΔD gets a substantial contribution in this way are known as "Good T.M.x letters" (RO p.57).

The relative importance of T.M.x contributions can be seen from the fact that $P(\Delta \Psi' = 8) = ab^5 + \frac{1}{2}b^4$ which equals .07 when there are 14 dots and .22 when there are 28 dots. It will be noticed that as the dottage increases, not only does the strength of the T.M. dot and T.M. cross components of $\Delta \Psi'$ increase, but that relative importance of T.M. cross components gradually increases.

To summarise we may say

$$\underline{P(\Delta D = \Theta) = (1-a).P(\Delta P = \Theta) + aP(\Delta D = \Theta \mid TMx)} \qquad (H3)$$

where the great part of the "bulginess" comes from the first term on the right hand side.

(b) ΔD, with limitation.

The T.M. dot positions are concentrated at places where there is a limitation cross, and using (H3) we may say

$$P(\Delta D = \Theta) = \left[(1-a)P(\Delta P = \Theta) + \tfrac{1}{2}a'P(\Delta D = \Theta \mid TMx)\right] + \left[\tfrac{1}{2}P(\Delta D = \Theta \mid TMx)\right]$$

where the square brackets cover lim cross and lim dot positions.

$$\therefore P(\Delta D = \Theta \mid L = \bullet) = P(\Delta D = \Theta \mid TMx) \qquad (H4)$$

$$\underline{P(\Delta D = \Theta \mid L = x) = \left\{(1-a')P(\Delta P = \Theta) + a'P(\Delta D = \Theta \mid TMx)\right\}} \qquad (H5)$$

since $(1-a') = 2(1-a)$.

This result demonstrates symbolically that the bulginess of a ΔD count against limitation cross is essentially greater than the bulginess of the total ΔD count, since what has been left out consists entirely of count against TMx, and the proportion of ΔP in the remainder has been doubled.

It might be noticed that the frequency of ΔD letters against limitation can be derived directly from (H1) by treating the limitation as $\Delta\Psi'_{6}$. Since $\Delta D_6 = \Delta\Psi'_6$, ΔP_6 must be regarded as a dot, and $P(\Delta P = \textcircled{8})$ put equal to zero, where $\textcircled{8}$ is a "letter" whose 6th impulse is a cross.

As a dechi is usually counted when Z and chis only are known, it is only possible to count against limitation dots and crosses when $\overline{\chi}_2$ lim is being used.

(c) Some ΔD counts

In practice it is arduous to obtain information about the frequency of letters in ΔD by means of ΔP counts and the relation (H2). The simplest way of obtaining information is by collecting ΔD counts from chi-setting messages or by combining ΔP and $\Delta\Psi'$ on a Robinson or Colossus. This was not at first realised (R1, 31,79; R2 37,51)

In Figs.22 (VI)(VII)(VIII) are shown ΔD counts corresponding to three different ΔP counts (Types A,B,C) and the $\Delta\Psi'$ counts given in Fig.22 (V). As with $\Delta\Psi'$, ΔD counts are given separately for $\overline{\chi}_2$ lim. and $\overline{\chi}_2\overline{\Psi}'_1$ lim, and in the case of $\overline{\chi}_2$ lim the counts of ΔD against L = x and L = . are given separately.

The counts show the gradual flattening of $\Delta\Psi'$ and ΔD as the dottage decreases, and also how this flattening is to some extent masked by random variations. The importance of good ~~Tbx~~ letters is shown particularly by the Type A figures. Here the ΔP (and ΔD) counts are dominated by one very powerful letter (/), with the result that 8 = (/ + 8) is the second highest letter in ΔD. The importance of 8,V,X,5,Q,K etc. is even more marked in the counts of ΔD against L = . as given for $\overline{\chi}_2$ limitation.

(d) ΔD counts with $\overline{\chi}_2\overline{P}_5$ limitation

With $\overline{\chi}_2\overline{P}_5$ limitation it is not possible (in practice) to count ΔD against lim dot and lim cross, but it is possible to count ΔD against $\overline{\chi}_2$ dot and $\overline{\chi}_2$ cross. (R3 p 56).

When P consists of German language $P_5 \longrightarrow$ dot (See 22G) and therefore L = $\overline{\chi}_2 + \overline{P}_5 \longrightarrow \overline{\chi}_2$. Therefore rather more than half the bulge on good language letters (3,U,F,J etc) in ΔD comes against $\overline{\chi}_2$ crosses.

The strength of 5 in ΔP is largely derived from P = 5M89, with ΔP = UA5. Now when 5 occurs in this way in ΔP, $\overline{P}$ = 5 and $\overline{P}_5 \longrightarrow$ x.

Therefore lim $\rightarrow \bar{\chi}_2 + x$, and most of the bulge of 5 in ΔD comes against $\bar{\chi}_2$ DOTS. These two facts are shown by the following count of a Gurnard message.

	$\bar{\chi}_2 = x$	$\bar{\chi}_2 = \cdot$
/	151	157
9	168	121
H	157	166
T	183	161
O	172	167
M	146	142
N	166	136
3	169	154
R	157	157
C	139	122
V	170	130
G	176	156
L	126	138
P	140	154
I	128	145
4	141	125
A	165	144
U	187	173
Q	137	130
W	135	142
5	155	239
8	163	149
K	127	126
J	181	142
D	126	140
F	176	149
X	129	138
B	134	107
Z	162	131
Y	186	137
S	172	134
E	126	131
Total	4950	4643

FIG 22 (XI)

for Statistics on a longish sample of language type messages see R3 p.87.

<u>(e) Δ D against B.M.</u>

By an argument similiar to that in (b) it can be seen that

$$P(\Delta D = \theta \mid BM = x) = P(\Delta D = \theta \mid TMx) \qquad (H6)$$

$$P(\Delta D = \theta \mid BM = \cdot\ ) = \left\{ \tfrac{1}{2}P(\Delta P = \theta) + \tfrac{1}{2}P(\Delta D = \theta \mid TMx) \right\} \qquad (H7)$$

and that the bulginess of a Δ D count against BM is essentially greater than the bulginess of the total Δ D count.

<u>(f) Δ D counts on 1 and 2 impulses</u>

From (E4) we get $\delta_{ij} = \dot{P}\sigma_{\omega}(\Delta D_{ij} = \omega) = \beta'_{ij} \cdot \pi_{ij}$

But $\beta'_{ij} = \beta$

$$\delta_{ij} = \pi_{ij} \cdot \beta \qquad (H8)$$

Putting $j = 6$ $\quad \delta_{i6} = \pi_{i6} \cdot \beta$

$\therefore$ PB (ΔD_i + lim = cross) = $\pi_i \cdot \beta$ [redacted]

$\therefore$ (for χ_2 = lim) PB (ΔD_2 [redacted] (H9)

Now $\left\{ \begin{array}{l} \text{[redacted]} \longrightarrow \text{dot (nearly always)} \\ \longrightarrow \text{cross (for punctuation)} \end{array} \right.$

$\therefore$ Δ [redacted] $\longrightarrow$ dot

ΔD_2 + Lim $\longrightarrow$ dot (R1 p.9) (H10)

Figs 22 (VI)(VII)(VIII) give scores [redacted] for the various Δ D counts shown.

The following table gives values for two impulse Δ D proportional bulges against limitation dots and crosses.

$\underline{\delta}_{..} \equiv$ PB (ΔD_i = . ΔD_j = . | L = .)

$\overline{\delta}_{..} \equiv$ PB (ΔD_i = . ΔD_j = . | L = x)

$\delta_{..} \equiv$ PB (ΔD_i = . ΔD_j = .) and so on.

$\underline{\delta}_{..}$	$\frac{\beta}{2}\{\beta(\pi_{..} + \pi_{xx}) - (\pi_{..} - \pi_{xx})\}$
$\underline{\delta}_{xx}$	$\frac{\beta}{2}\{\beta(\pi_{..} + \pi_{xx}) + (\pi_{..} - \pi_{xx})\}$
$\underline{\delta}_{x.}$	$\frac{\beta}{2}\{-\beta(\pi_{..} + \pi_{xx}) - (\pi_{x.} - \pi_{.x})\}$
$\underline{\delta}_{.x}$	$\frac{\beta}{2}\{-\beta(\pi_{..} + \pi_{xx}) + (\pi_{x.} - \pi_{.x})\}$
$\overline{\delta}_{..}$	$\frac{\beta}{2}(1+\beta)\{-\beta^2(\pi_{..} + \pi_{xx}) + 2\beta\pi_{..} + (3\pi_{..} + \pi_{xx})\}$
$\overline{\delta}_{xx}$	$\frac{\beta}{2}(1+\beta)\{-\beta^2(\pi_{..} + \pi_{xx}) + 2\beta\pi_{xx} + (3\pi_{xx} + \pi_{..})\}$
$\overline{\delta}_{x.}$	$\frac{\beta}{2}(1+\beta)\{+\beta^2(\pi_{..} + \pi_{xx}) + 2\beta\pi_{x.} + (3\pi_{x.} + \pi_{.x})\}$
$\overline{\delta}_{.x}$	$\frac{\beta}{2}(1+\beta)\{+\beta^2(\pi_{..} + \pi_{xx}) + 2\beta\pi_{.x} + (3\pi_{.x} + \pi_{x.})\}$
$\delta_{..}$	$+\frac{1}{2}\beta(\pi_{..} + \pi_{xx})$
δ_{xx}	$+\frac{1}{2}\beta(\pi_{..} + \pi_{xx})$
$\delta_{x.}$	$-\frac{1}{2}\beta(\pi_{..} + \pi_{xx})$
$\delta_{.x}$	$-\frac{1}{2}\beta(\pi_{..} + \pi_{xx})$

Fig. 22 (XII)

The workings are left to the reader (similar workings are given on R4 p.80)

Two results should be noticed.

(i) $\underline{\delta_{..} = \delta_{xx}}$ and $\underline{\delta_{x.} = \delta_{.x}}$. Whatever the relative values of $\pi_{..}$ and π_{xx}. This shows that the benefits of counting against χ_2 limitation increase as $|\pi_{..} - \pi_{xx}|$ increases (R2 p 96) (H11)

(ii) $\underline{\delta}_{ij} = \frac{1}{2}\{\underline{\delta}_{..} + \underline{\delta}_{xx}\} = \frac{1}{2}\beta^2(\pi_{..} + \pi_{xx}) = \beta^2\pi_{ij}$

But $\delta_{ij} = \frac{1}{2}\{\underline{\delta}_{ij} + \overline{\delta}_{ij}\} = \beta\pi_{ij}$ (from H6).

$$\therefore \overline{\delta}_{ij} = \pi_{ij}(2\beta - \beta^2) = \beta(2-\beta)\pi_{ij}$$

$$\therefore \overline{\delta}_{ij} / \underline{\delta}_{ij} = \frac{2-\beta}{\beta} \qquad \text{(H12)}$$

The following table gives value for $\Delta D_1 = \Delta D_2 =$ dot, L = x etc. for the messages considered in Figs 22, (VI)(VII)(VIII).

ΔD1	ΔD2	L	Type A	Type B	Type C
•	•	x	490	404	406
•	x	x	276	322	386
x	x	x	497	495	385
x	•	x	283	327	371
•	•	•	421	435	465
•	x	•	400	433	402
x	x	•	439	400	406
x	•	•	392	384	379

FIG 22 (XIII)

(g) $\Delta^2 D$

$$\Delta^2 D = \Delta^2 P + \Delta^2 \Psi'$$

It was several times suggested that methods involving use of $\Delta^2 D$ frequencies should be used. However counts taken showed that although the count of $\Delta^2 P$ was more bulgy than that of ΔP nevertheless the count of $\Delta^2 \Psi'$ was feeble compared with that of $\Delta\Psi'$. As a result the count of $\Delta^2 D$ has no statistical (or other) advantages over that of $\Delta \dot{D}$. (See R3 p 44 - 5, 52-3 and R4 p 131-3 for example of $\Delta^2 D$ counts) (First $\Delta^2 D$ count R1 p 82).

(h) Bigrams in ΔD

Little work was done on bigram frequencies. Some experiments, however showed that the frequency of $\Delta D_1 + \Delta D_2$ bigrams .., .x, xx, x. did not differ significantly from the estimated frequency assuming random juxtaposition (R3 p 63)

22J THE CIPHER STREAM

$$Z = \chi + D$$

$$\therefore \Delta Z = \Delta\chi + \Delta D$$

$\therefore$ Adapting (6a) and (6c) we get

$$\Delta Z_{ij} \xrightarrow{\frac{1}{2}(1+s_{ij})} \Delta\chi_{ij} \qquad \text{(J1)}$$

$$\Delta_{w_i w_j}(\Delta Z_{ij}) \xrightarrow{\frac{1}{2}(1+s_{ij})} \text{dot}, \qquad \text{(J2)}$$

and in particular $\Delta_{1271}(\Delta Z_{12}) \xrightarrow{\frac{1}{2}(1+s_{ij})} \text{dot}$. (J3)

This formula has been used as the basis of a formula for determining whether unidentified traffic is on Tunny, (See R3 p.77) and the discussion on Significance test Θ in Ch.24.

22K SAMPLING ERRORS IN ALPHABETICAL COUNTS

Our knowledge of alphabetical counts of ΔP and ΔD is essentially empirical. There is no very exact knowledge of what a ΔP count should look like, even for a given end of a given link, since the count depends on the particular operator and the content of the message. The factor which a supposed ΔD count gives, in favour of the de-chi being correct, is discussed in 22Y. Here we discuss shortly the method of obtaining typical counts.

Suppose we have r samples, all of length 3200, of ΔD for a particular link end and value of d. It is so convenient to be able to work with the average of these counts that we normally do so unless there is too obviously more than one type of language represented. Suppose the numbers of occurrences of Θ in the samples are

$$n_\Theta^{(1)},\ n_\Theta^{(2)},\ \ldots,\ n_\Theta^{(r)}.$$

The obvious thing to do is to take the number of occurrences in a typical example as

$$n_\Theta \pm \sigma_\Theta,$$

where

$$r n_\Theta = \sum_{s=1}^{r} n_\Theta^{(s)}$$

$$r\sigma_\Theta^2 = \sum_{s=1}^{r} \left(n_\Theta^{(s)} - n_\Theta\right)^2 \qquad \text{(K1)}$$

In order to estimate σ_Θ it is easier to calculate $\sum_{s=1}^{r} \left| n_\Theta^{(s)} - n_\Theta \right|$, which can be done in a self-checking way, and to write

$$8\sigma_\Theta = \sum_{s=1}^{r} \left| n_\Theta^{(s)} - n_\Theta \right|, \qquad \text{(K2)}$$

since the expected value of the modulus of the deviation from the mean is $\sigma\sqrt{\frac{2}{\pi}} \approx .80\sigma$ in the case of a normal variate. Of course this is not accurate, but accuracy is not the point.

The expected sigma-age of a chi run (See 23C(d)) can be worked out sufficiently accurately from the average letter count, i.e. the 32 numbers n_θ. Some estimate of the S.D. of this sigma-age can be obtained from the numbers σ_θ. A very crude method of doing this is given in R2,56,60,61 and pp 17,21 of the note-book 'Alphabetical counts and runs statistics'.

22W. SOME FURTHER STREAMS

(a) The Sum of two P- Streams

The frequency of letters in $P_a + P_b$ is deducible from the frequency of letters in P_a by means of the Faltung Theorem (22E).

We can score a stream of letters suspected of being $P_a + P_b$. For each occurrence of θ in the stream we get a factor

$$\frac{P\,(P_a + P_b = \theta)}{1/32}$$

that is a decibanage of $10 \log_{10} \{32P(P_a + P_b) = \theta\}$ (W1)

The following table gives the <u>centiban</u> scores actually used in Room 41 for scoring suspected depths.

θ	score	θ	score	θ	score	θ	score
/	+31	R	-15	A	-2	D	-2
9	-1	C	-1	U	+11	F	+2
H	-12	V	+7	Q	-12	X	-2
T	-16	G	+2	W	-1	B	-14
O	+7	L	-24	5	+3	Z	-4
M	+1	P	-4	8	+2	Y	-3
N	-17	I	-1	K	-3	S	+17
3	+4	4	+10	J	+6	E	-12

FIG 22 (XIV)

(b) The sum of two extended psi-streams

Given two stretches of de-chi (a,b) which are known to have the same decode (as in an overlap) it is often possible to find the relative position of the P in the two stretches. For when set correctly

$$\Delta D_a + \Delta D_b = \Delta\Psi'_a + \Delta P_a + \Delta\Psi'_b + \Delta P_b$$

$$= \Delta\Psi'_a + \Delta\Psi'_b \qquad (\text{since } \Delta P_a = \Delta P_b)$$

If θ_n^m is a letter of n dots and m crosses

$$P(\Delta\Psi'_a + \Delta\Psi'_b = \theta_n^m \mid TM_a = \cdot\,,\ TM_b = \cdot\,) = X_n^m = \begin{cases}1, & m = 0\\ 0, & m \neq 0\end{cases} \qquad (W1)$$

$$P(\Delta\Psi'_a + \Delta\Psi'_b = \theta_n^m \mid TM_a = \cdot\ ;\ TM_b = x) = Y_n^m = \left(\frac{1+\beta}{2}\right)^m\left(\frac{1-\beta}{2}\right)^n \qquad (W2)$$

$$P(\Delta\Psi'_a + \Delta\Psi'_b = \theta_n^m \mid TM_a = x\,,\ TM_b = x) = Z_n^m = \left(\frac{1-\beta^2}{2}\right)^m\left(\frac{1+\beta^2}{2}\right)^n \qquad (W3)$$

$$\text{and } P(\Delta\Psi'_a + \Delta\Psi'_b = \theta_n^m) = (1-a)^2 X_n^m + 2a(1-a)Y_n^m + a^2 Z_n^m$$

$$= \frac{\beta^2 X_n^m + 2\beta Y_n^m + Z_n^m}{(1+\beta)^2} \qquad (W4)$$

Because limitation (L) is equivalent to $\Delta\Psi'_b + x$,

$$P(\Delta\Psi'_a + \Delta\Psi'_b = \theta_n^m \mid L_a + L_b = \cdot\,) = P(\Delta\Psi'_a + \Delta\Psi'_b = \theta_{n+1}^m \mid \Delta\Psi'_a + \Delta\Psi'_b = \theta_1^0)$$

$$= \frac{P(\Delta\Psi'_a + \Delta\Psi'_b = \theta_{n+1}^m)}{P(\Delta\Psi'_a + \Delta\Psi'_b = \theta_1^0)}$$

$$= 2P(\Delta\Psi'_a + \Delta\Psi'_b = \theta_{n+1}^m) \qquad (W5)$$

$$\text{Similarly } P(\Delta\Psi'_a + \Delta\Psi'_b = \theta_n^m \mid L_a + L_b = x) = 2P(\Delta\Psi'_a + \Delta\Psi'_b = \theta_n^{m+1}) \qquad (W6)$$

The following table (for m + n = 5) is constructed, with the aid of W1, 2, 3, 4, 5, 6, in the same way as the table in the last section and gives deciban scores per letter and is used for scoring possible positions for go-backs. Scores for intermediate dottages can be interpolated.

	$L_a + L_b$ = dot	$L_a + L_b$ = cross	Dottages 15	18	21	24	27
Number of dots (n)	5	-	+5½	+7	+8	+9	+10½
	4	5	-1	-1	-	-	+½
	3	4	-1	-1	-1	-2	-2
	2	3	-1	-1	-2	-2	-5
	1	2	0	0	-	-1	-2
	0	1	+½	+1	+2	+2½	+3
	-	0	+2	+3½	+5	+7	+8½

FIG (XV)

<u>(c) The sum of two key streams</u>

It has been suggested that in cases where there are two stretches of Z with the same P it might be possible to find the relative positions of the P, even if neither messages has been decoded for $\Delta Z_a + \Delta Z_b = \Delta K_a + \Delta K_b$

$$\therefore \underset{w_i w_j}{\Delta}\{\Delta Z_a^{ij} + \Delta Z_b^{ij}\} = \underset{w_i w_j}{\Delta}\{\Delta K_a^{ij} + \Delta K_b^{ij}\} \xrightarrow[\frac{1}{2}(1+\beta^2)]{} \text{dot} \qquad (W8)$$

22X THE ALGEBRA OF PROPORTIONAL BULGES.

(a) The Problem: Recovery of ΔP from ΔD

It has been pointed out in 22H that the expected letter count of ΔD can be obtained from that of ΔP by means of the equations

$$\text{P.B.}(\Delta D = \theta) = 1/32 \sum_{\xi} \text{P.B.}(\Delta P = \xi)\ \text{P.B.}(\Delta \Psi' = \theta + \xi) \qquad \text{(X1)}$$

The problem of solving these equations for P.B. (ΔP) given P.B. (ΔD) led to the 'algebra of proportional bulges'. Even theoretically the problem is not simple, since the determinant of the coefficients vanishes. The advantage of using P.B.'s rather than probabilities is not great, but it does help a little. The reasong why proportional bulges were first introduced are mentioned in 21(J) (R1,20).

(b) Application to Motor Runs

The problem we are considering here has an application to the question of the expected score on a motor run (R5 23,32). For we know that

$$\text{P.B.}(\Delta D \mid \text{B.M.} = \cdot) = \tfrac{1}{2}\,\text{P.B.}(\Delta P) + \tfrac{1}{2}\,\text{P.B.}(\Delta P + \Delta \Psi),$$

and the second term can be written as a 'Faltung', i.e. in a form similar to (1) above. When the limitation is $\bar{\chi}_2$ the count of ΔD against $\bar{\chi}_2 =$ dot provides a sample of ΔD against motor crosses and we can therefore obtain a good idea of the L.C. of ΔP and of the expected score in a motor run (R0 47-50). For limitations other than $\bar{\chi}_2$, the usual method was to assume 'flatness' of $\Delta P + \Delta \Psi$ in order to obtain a quick estimate (See chapter 23).

(c) Efforts at Solution

The problem of solving equations (X1) for P.B. (ΔP) was first attacked in R2,69 where an erroneous connection with 'Fourier Transforms' was suggested. The theoretical aspects of the problem were pursued in R2 p 87,104; R3 pp 24,28,32,34,37,38,48; R5 23 32; and a practical experiment in the solution of ΔP from ΔD is described in R3 pp 71-3. Finally a relatively simple exposition of the whole subject was given in R5 59. In this chapter we give a still simpler account which contains all the essential ideas, with the introduction of the minimum of new notation. It will be observed that 'Fourier Transforms' are after all the simplest way of treating the problem.

(d) Exposition of the algebra

Denote an arbitrary teleprinter letter by θ or ξ. Let $F(\theta)$ be an arbitrary numerical function of teleprinter letters. The Fourier Transform

(F.T.) of F is defined as the function F^* where

$$F^*(\Phi) = \frac{1}{\sqrt{32}} \sum_{\Theta} F(\Theta)(-1)^{\Theta.\Phi} \qquad (X2)$$

where $\Theta.\Phi$ is the scalar product of Θ and Φ when they are considered as vectors with 0 for dot and 1 for cross. For example (U.N.) = 1.0+1.0+1.1+0.1+0.0= 1 It can easily be shown that $F^{**} = F$, i.e. that F is the F.T. of F^*, so the relation between F and F^* is symmetrical.

The "Faltung", F, of two functions F_1 and F_2 is defined by the equation

$$F(\Theta) = \sum_{\Phi} F_1(\Phi) F_2(\Theta + \Phi) \qquad (X3)$$

which is clearly also equal to $\sum_{\Phi} F_2(\Phi) F_1(\Theta + \Phi)$.

It is easy to see that if F is the Faltung of F_1 and F_2 then $F^* = \sqrt{32}\, F_1^*.F_2^*$. In other words the F.T. of a Faltung is $\sqrt{32}$ times the product of the F.T.'s. Therefore, by equation (X1)

$$\sqrt{32}.\text{P.B.}^*(\Delta D) = \text{P.B.}^*(\Delta P)\ \text{P.B.}^*(\Delta \Psi') \qquad (X4)$$

(see foot-note).

where P.B.* means the Fourier Transform of the Proportional Bulge.

This gives P.B.* (ΔP) in terms of P.B.* (ΔD) and P.B.* ($\Delta\Psi'$) and hence P.B. (ΔP) in terms of P.B. (ΔD) and P.B. ($\Delta\Psi'$). The process is not as laborious as it sounds in virtue of the rather simple interpretation of an F.T. For example if Θ is the T.P. letter J or vector (1,1,0,1,0) and if F is a P.B. function, taken as P.B. (ΔD) for definiteness, we have

$$F^*(J) = \frac{1}{\sqrt{32}}\Big\{\sum_{\Xi_1+\Xi_2+\Xi_4 = \cdot} F(\Xi) - \sum_{\Xi_1+\Xi_2+\Xi_4 = \times} F(\Xi)\Big\}$$

$$= \frac{2}{\sqrt{32}} \sum_{\Xi_1+\Xi_2+\Xi_4 = \cdot} F(\Xi)$$

since F is assumed to be a P.B. function.

Thus P.B.* (J) = $\sqrt{32}$ P.B. ($\Delta D_{1+2+4} = \cdot$) (X5)

so we see that the F.T. of a P.B. is $\sqrt{32}$ times the P.B. of the so-called "32-combination count" (R3 p 49; R5 p 55), for which the lower half of the Colossus switchboard is well adapted. The equation (X4) is now seen to express the well known and elementary property of the multiplication of P.B.'s.

Observe that P.B. (ΔP) is not quite determinate since

$$\text{P.B.}^*\,P(\Xi) = \sqrt{32}\ \frac{\text{P.B.}^*\Delta D(\Xi)}{\text{P.B.}^*\Delta\Psi'(\Xi)}$$

and the expected values of both numerator and denominator of this are zero, if ab = $\frac{1}{2}$. The same applies to the arguments 4,9,3,T.

Note: P.B. (ΔP) is a function of Θ and should strictly be written as P.B.($\Delta P = \Theta$).

22Y THE AMOUNT OF EVIDENCE DERIVED FROM A LETTER COUNT

The fundamental problem in chi-setting from a theoretical point of view is of the following type: given a ΔD letter count in which θ occurs n_θ times, with $\sum_{\theta} n_\theta = N$, to estimate the decibannage in favour of the χ's being correct. The link and end being dealt with will be known always, the dottage (d) possibly. We will also have some prior knowledge of expected ΔD characteristics.

This knowledge can be expressed by saying that there is a probability P_i ($\sum P_i = 1$) for the theory, T_i, that the frequency of letter θ in ΔD is $p_\theta^{(i)}$; (θ = /, 9, H ....., i = 1, 2, 3 .....).

If theory T_i is true then the factor in favour of the χ's being correctly set rather than random is f_i, where

$$f_i = \prod_{\theta} \left(32\, p_\theta^{(i)}\right)^{n_\theta} \qquad \text{(Y1)}$$

This factor can be conveniently expressed in decibans of course.

Now, by the theorem of the weighted average of factors (see 21(i)), the factor in favour of the χ's being correct is $\sum P_i f_i$. (Y2)

So we have a complete theoretical solution of the problem. The method could be made practicable for letter counts which are of a more or less standard type, but even for these, a great deal of preliminary statistical work would have to be done (R2 pp 1,59). If the letter count is not of a standard type it is tempting to use the χ^2 test. This has the disadvantage that the χ^2 test takes no account of which are the high-scoring letters and which the low-scorings ones. An attempt to overcome this objection is made in R5 pp 1-4. This attempt is a theoretical formulation of what is really done in practice - namely the count is looked at to see if it is sufficiently 'bulgy' and then (slightly less important) to see if the bulges come at the right letters.

An alternative test which is quicker to apply, is the method of 'decibanning a letter count using the message as its own sample' (R4 pp 56,121). This method is obtained by writing, in (Y1), $p_\theta^{(i)} = n_\theta / N$.

The decibanage given by this is

$$\sum_{\theta} n_\theta \log n_\theta - N\{\log N - \log 32\}, \qquad \text{(Y3)}$$

when the logarithms are to base $\sqrt[10]{10}$ of course. It can be proved easily that this is equivalent to taking the maximum possible value of f_i and therefore, by (Y2), the method is optimistic. It was designed originally as a method of rejecting seedy wheel-breaking stories. It is shown in R4,121 that the decibanage will not be more the 80 d.b. too high.

23 MACHINE SETTING

23A Introduction

23B The choice of runs

23C Weighing the evidence

23D Annotated Exhibits

23E χ - setting with $\overline{\chi}_1$ limitation

23F Message slides

23G Wheel slides

23H Flogging runs

23J Flogging the evidence

23K Checks on setting

23L Statistical setting of the motor

23M ψ -setting

23N Coalescence

23P Example

23W Calculation of the odds of the best score in a χ -setting run.

23X Theory of coalescence

23Z History of machine setting.

23A INTRODUCTION

(a) The problem of chi-setting

The problem of chi-setting is: given the cipher Z and the chi-patterns, to find the settings of the chis relative to Z and so obtain

$$D \equiv Z + \chi$$

(b) The evidence available

The evidence available is that of the ΔD letter count, which has non-random bulges: the method is to find settings which make these bulges as large as is possible, discriminating in favour of settings whose bulges are on the right letters. Unless the bulges are so large as to be unlikely to have occurred at random, the chis cannot be regarded as set.

(c) The ideal method

The ideal method would be to examine the 32 letter count at all possible settings, but this means 41 x 31 x 29 x 26 x 23 = 23,561,898 letter counts.

(d) Practical chi-setting

Practical chi-setting must be completed in a reasonable time, so that it will be necessary at each stage to set a smaller number of chis and to examine not the whole letter count, but only its strongest feature. Runs are classified as one-wheel or short, 2-wheel or long, 3-wheel, and 4-wheel.

(e) The art of chi-setting

The art of chi-setting consists of:

(i) choosing runs so as to obtain significant scores as quickly as possible.

(ii) knowing how significant the scores obtained are; in particular, knowing when they are "good" or "certain".

23B THE CHOICE OF RUNS

(a) ΔD Statistics

The choice is based on the statistics of ΔD letter counts for messages already set (22 H). Some ΔD characteristics are permanent and common to all links, others are peculiar to a particular link, or to one end of a link, or to particular messages.

In almost all messages /,5,U,8 are common;
B is rare;
In Type A (stroky) messages / is very common;
In Type B (language) messages 3,J,F,G, are common.

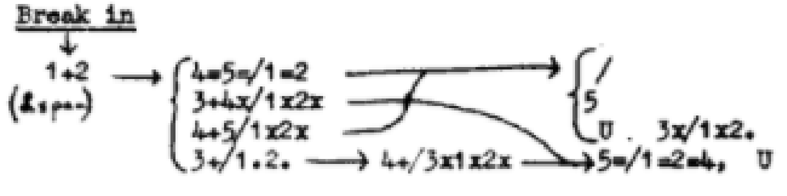
Originally the Berlin ends of Western links were type B, the outer ends of most Western links and both ends of Eastern links were type A. Later the situation became confused and so did the notation A,B,C.... [cf 22 G (c)]

(b) Practical Runs

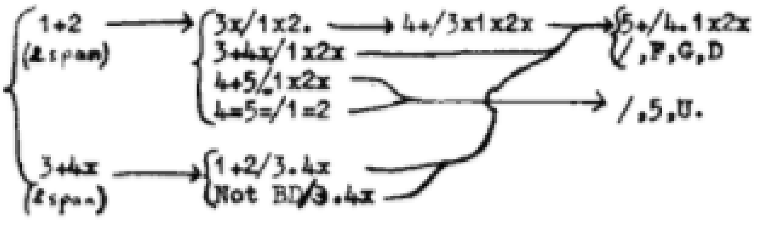
For rapid setting it is insufficient to remember the frequencies of the 32 individual letters: it is necessary to know explicitly what are the best runs for direct application; e.g. to know that 1 + 2 = . is the best run involving only two wheels. This is of course deducible from the 32 letter count, largely because 1+2/ is satisfied by all the letters /,5,U,8, 3,J, and not by B. Succint rules are given in "trees".

(c) A simple tree

TYPE A



TYPE B



(i) Runs bracketed are to be tried, in order, till one of them gives a "certain" or "good" setting. See 23O(a) The runs for the last wheel should be "certain". If all these fail, the message is abandoned, unless it is to be flogged (23 J)

(ii) ΔD is omitted and only the suffixes denoting the impulses are written: this is the invariable custom. (R0 p110).

(iii) Impulses to the right of the oblique stroke are supposed already set.

(iv) The Break In is the initial run used when setting a message (which has nothing to the right of the oblique stroke).

(v) "Span" is in the diagram, because, as soon as the first wheels are set, the message is invariably spanned for possible message slides (See 23 F.) (See also R3 p 134; R4 p 7; R1 p 99; R2 pp 42,44,48.)

(d) More powerful methods

Though the above tree will suffice to set a large proportion of messages, it is rather crude. Having already set several recent messages on the same link, one would probably introduce a few modifications.

For the best results messages on χ_2 limitation may require a quite different break-in. (23L)

Other runs are mentioned in 23 J: R1 is full of such references; recent notes include R3 p 131, R5 p 106.

23O WEIGHING THE EVIDENCE

(a) Sigma-age

The bulge of a score is its excess over random.

The sigma-age is the ratio of the bulge to the standard deviation for random scores: it is a measure of the improbability that the sum will occur at random in a single trial, i.e. at a particular setting. If many settings are tried, the improbability will be proportionally reduced. In a one-wheel run the number of settings tried lies between 23 and 41,, in a two-wheel run between 598 and 1271 and so on.

This improbability that a score will have occurred at random is clearly some indication of the degree of certainty that the corresponding setting is correct. Unless there are rival settings the following table is used.

	Number of wheels set by the run	1	2	3	4	5
Sigma-age	for a "certain" setting i.e. odds 50:1 on	3.8	4.5	5.2	5.8	6.4
	for a "good" setting i.e. odd 6:1 on	3.2	4.0	4.7	5.4	6.0

The formula for sigma is $\sigma = \sqrt{p(1-p)N}$, where p is the random proportional frequency [21(X)] . In χ- setting p is almost always $\frac{1}{2}$, $\frac{1}{4}$ or $\frac{1}{8}$, giving $\sigma = \frac{1}{2}\sqrt{N}, \frac{1}{4}\sqrt{3N}, \frac{1}{8}\sqrt{7N}$.

(b) Pick-ups

If two independent runs contain the same wheel, their evidence may be combined. A table has been compiled which is sufficient for elementary setting , [for the basis of the table see 23J(b) and 23X$_4$]

CERTAIN						GOOD					
Long	Long	Long	Short	Short	Short	Long	Long	Long	Short	Short	Short
4.5	-	4.5	-	3.8	-	4.0	-	4.0	-	3.2	-
4.4	2.7	4.4	1.0	3.7	1.0	3.9	2.7	3.9	1.0	3.1	1.0
4.3	2.8	4.3	1.2	3.6	1.1	3.8	2.9	3.8	1.3	3.0	1.2
4.2	3.0	4.2	1.6	3.5	1.3	3.7	3.0	3.7	1.5	2.9	1.5
4.1	3.1	4.1	1.8	3.4	1.6	3.6	3.1	3.6	1.7	2.8	1.7
4.0	3.2	4.0	2.0	3.3	1.8	3.5	3.2	3.5	1.9	2.7	1.8
3.9	3.4	3.9	2.3	3.2	2.0	3.4	3.3	3.4	2.1	2.6	2.0
3.8	3.5	3.8	2.5	3.1	2.1			3.3	2.3	2.5	2.1
3.7	3.7			3.0	2.3			3.2	2.5	2.4	2.2
				2.9	2.5						
				2.8	2.6						
				2.7	2.7						

As an example of the use of the table, suppose that with the same setting of χ_3 the sigma-age of 3x/1x2. is 2.4 σ
and of 3+4x/1x2x is 3.9 σ

According to the table, the settings of χ_3, χ_4 are both "certain", though neither run separately would give even a "good" setting.

(c) Rival Settings

In this section the effects of competing scores have been ignored. (See 23J, 23X)

(d) Expected Sigma-age

The expected sigma-age is $\frac{\text{expected bulge}}{\sigma} = \frac{\xi N}{\sqrt{Np(1-p)}} = \xi\sqrt{N\frac{p}{1-p}}$,
where ξ is the proportional bulge. For p = $\frac{1}{2}, \frac{1}{4}, \frac{1}{8}$ this is $\xi\sqrt{N}$, $\xi\sqrt{N/3}$, $\xi\sqrt{N/7}$.

23D ANNOTATED EXHIBITS

This is rather illogically included here to exhibit the practice of chi-setting as concretely as possible: its perusal is recommended. Inevitably it includes much which is explained only in the later sections of the chapter but this is always indicated by reference. The message shown is on $\bar{\chi}_2$ limitation, but no special method is used except that all runs are made against $\bar{\chi}_1$ crosses only. (The operator neglects the four letter count on ΔD_1 ΔD_2 : . it may be repeated that on the whole text there can be only a random bulge of xx over ..) .

```
BR 3407 0450/24/2 WD 23/2 COL 7

T 6020

1P2/L R 3106 A 1553 ø 27.8 ST 1624
K1 K2
02 08 E 1631
02 20 E 1625
11 09 A 1633
16 07 A 1629
18 08 D 1629
19 31 C 1625
37 21 E 1637
40 28 B 1655     B 102   3.7ø
40 28 C 1655

SET K1 K2  40 28

SPAN  IN 1000'S


0271
0245

0268
0249

0301
0214

0280
0237

0268
0247

0261
0257

SPAN 4000-END IN 500'S

0139
0119

0129
0128

0131
0128

0130
0129

SPAN 01-4500

1259
1064    2B 195 B 98    4.1ø

SPANNING 01-4500

SET K1 K2 40 28  GOOD
```

The items in the first line are message number, time and date sent, wheel day and Colossus number.

T 6020 is the text length, measured as a check, as soon as the tape is on Colossus.

1P2/L is typewriterese for 1+2/$\bar{\chi}_2$x; this run is chosen because the chit (not preserved) was so marked [23E].

R 3106 is the number of places looked at, i.e. the number of places where $\bar{\chi}_2$ = x .

At random the expected number (A) of these when 1+2 = . is $\frac{1}{2}$ x 3106 = 1553.

ø (typewriterese for σ) 27.8 is the standard deviation of 1+2 = . viz. $\frac{1}{2}\sqrt{R} = \frac{1}{2}\sqrt{3106}$. This is of course an application of the formula quoted in 21(b), that if random proportional frequency in a normal distribution is p, the standard deviation is $\sqrt{Rp(1-p)}$. A table of $\frac{1}{2}\sqrt{R}$ and $\frac{1}{4}\sqrt{3R}$ is provided at each Colossus.

ST 1624 is the set total, i.e. Colossus is set so as not to display or print any smaller score. Because this is a two-wheel run ST is taken as A + $2\frac{1}{2}\sigma$.

The best score is 3.7σ ,not even "good" [23C(a)] but worth spanning [23F(c)]. In each pair of span scores the upper is 1+2 = . , the lower 1+2 = x : this makes it easy to see where a slide occurs, evidently between 4000 and 5000, for 5000 - 6000 shows almost no bulge and 4000 - 5000 only a small bulge. 4000 - 5000 is therefore spanned in 500's and the bulge of 1+2 = . is seen to cease at about the 4500th letter: it is therefore believed that there is a message slide here and the subsequent runs are done spanning 1 - 4500: the sigma-age is now 4.1 instead of 3.7; the setting is therefore "good".

Here the operator makes the mistake of neglecting a 4-letter count for ΔD_1, ΔK_2 [23E(h)] this is easily reconstructed and would read

```
..  592
.x  498
xx  667
x.  567
```

Because xx is so strong, this would have suggested the run 3+4x/1x2x which would in fact yield a score of 7.9σ.

C3 R 1259 A 315 Ø 15.4 ST 353
K4 K5
05 06 B 0369
05 13 B 0356
05 22 B 0379 B 64 4.15Ø
17 06 E 0357
18 11 D 0363
26 11 A 0357
26 11 B 0358

Instead the operator uses C3, i.e. 4=5=/1=2. R 1259 is the number of places looked at, i.e. of places where 1=2. A, the expected random number of places where 4=5=/1=2 is a quarter of this, because two more conditions are imposed, and $\sigma = \frac{1}{2}\sqrt{3R} = \frac{1}{2}\sqrt{3 \times 1259} = 15.4$.

SET K4 K5 05 22 GOOD

ST as above.

/// 555 UUU
168 212 177

The best score is 4.15 σ. It should be noticed that three scores above the set total have χ_4 at 05; and that the χ_5 settings are 22, 22+7, 22+14, suggesting a wheel-slide (23G) of 7 on χ_5, but fortunately one too weak to make the setting really doubtful.

555 A 106 Ø 7.2 ST 115
K3
02 A 0125
08 A 0146 B 40 5.6Ø
10 A 0116
12 A 0116
14 A 0118
16 A 0125

The most likely letters to set χ_3 are /,5,U: to decide which the operator counts / & 9, 5 & 8, U & E; and because 5 & 8 are most numerous (212) chooses 5

K1 K2 K3 K4 K5
40 28 08 05 22 SPAN 01-4500

A and σ are as before, but ST is now only A + σ, because this is a one-wheel run.

The setting obtained is "certain". K1 K2 K3 K4 K5 40 28 08 05 22 is printed by means of P.M.H. so that errors in setting will be manifest.

AG X2 XX means against χ_2 = x.

	AG X2 XX ·	AG X2 ...
/	0086	0092
9	0082	0084
H	0063	0067
T	0052	0064
O	0084	0055
M	0086	0078
N	0044	0063
3	0095	0057
R	0058	0059
C	0053	0053
V	0042	0073
G	0075	0082
L	0053	0094
P	0088	0067
I	0072	0055
4	0057	0065
A	0066	0078
U	0111	0097
Q	0067	0066
W	0058	0047
5	0146	0074
8	0066	0060
K	0057	0060
J	0096	0058
D	0049	0064
F	0120	0074
X	0064	0082
B	0054	0067
Z	0055	0071
Y	0087	0068
S	0081	0066
E	0056	0067

Motor run
555
1 dot
R46 A82
E.S. 114

The settings for $\chi_1, \chi_2, \chi_4, \chi_5$ were not very strong, so that although the final χ_3 score makes them "certain", it is just as well to inspect the letter count.

This resolves all doubts as to the correctness of the settings, e.g. χ_3 is made very certain by the scores for U > Q, 5 > J, F > L. The count is in fact much better than average; the worst contradictions with the pairs in 23 H(e) are CM, DB, ZR.

The dossier is therefore marked all certain.

The letters have been inserted in the letter count for the purpose of this report: Colossus operators knew them too well to need this.

The pen entries at the right of the letter count are the DO's order for a motor run [which appears on the next page but one]

The part 4500 - end is not yet set: it is believed that there is a message slide so that the settings for all chi's in the part of the message will be increased, or decreased, equally.

ALL CERTAIN SPAN 01-4500

E.M.LEWIS.

33GGUU55FF

SPAN 4500-END

K1	K2	K3	K4	K5		
30	18	27	21	12	A	0108
31	19	28	22	13	A	0129
32	20	29	23	14	A	0138
34	22	02	25	16	A	0125
35	23	03	26	17	A	0129
36	24	04	01	18	A	0123
37	25	05	02	19	A	0121
39	27	07	04	21	A	0134
40	28	08	05	22	A	0123
41	29	09	06	23	A	0170
01	30	10	07	01	A	0139

SPAN 4500-END

K1	K2	K3	K4	K5
41	29	09	06	23

X2 XX	X2 ...
0028	0027
0031	0021
0019	0024
0018	0019
0024	0028
0034	0029
0021	0022
0030	0017
0019	0021
0013	0027
0024	0026
0026	0027
0015	0018
0026	0023
0023	0026
0026	0024
0040	0016
0037	0019
0017	0019
0020	0028
0050	0017
0029	0030
0015	0017
0024	0024
0022	0020
0027	0019
0027	0019
0010	0024
0017	0021
0030	0030
0019	0030
0022	0023

745

The chis are therefore set back equally and stepped together, counting 3GU5F (G evidently in mistake for J)

For this run R is $\frac{16}{31} \times 1520$ (There are 16 x's in χ_2).

$A = \frac{5}{32} \times \frac{31}{16} \times 1520$ (3GU5F are five letters out of 32).

$\sigma = \sqrt{\frac{16}{31} \times 1520 \times \frac{5}{32} \times \frac{27}{32}}$ (using $\sqrt{Rp(1-p)}$)

The sigma-age obtained is 4.3 σ which is ample for the slide is of one place only.
Note: In most cases, as here, the calculation of σ for a slide run is unnecessary.

A letter count is done on the newly set part. It looks much worse: this is due in part to the shorter text which makes random effects larger relative to systematic effects; it is possible that a small part should be set at 01,30,10,07,01. An excellent feature of this count is low B's. This part could have been set by itself.

The de-chi check [23L(f)] is made by switching Q = Z + χ and counting 1x,2x,3x,4x,5x, simultaneously on the five counters, spanning 01 - 08 The scores obtained are 1,1,1,0,0, showing thatthe second letter of Z + χ is U; similiarly GYN.....
[01-08 is a mistake for 02-09]

Four letters are found at intervals of 620 up to 3100, thereafter only the last five.

Message particulars are repeated here because the de-chi check is sent to the Tunny room for making the de-chi tape: it is left here only because a motor run was ordered instead.

BR 3407 0450/24/2 WD 23/2 COL 7

T 6020

DE CHI ON 1ST 4500

K1	K2	K3	K4	K5
40	28	08	05	22

01-08	UGYNPS5X
620	5ZA/
1240	CYS5
1860	DYCN
2480	L3KJ
3100	EEXY
4495	WA8WN

For completeness the remainder of the Colossus record, showing the setting of motors and psis is included here: for such further explanation as is needed see 33 L.M. It will be noted that several runs are done simultaneously on different counters, e.g. 1., 2., 3x, 4., 5.

```
BR 3407 0450/24/2 WD 23/3 COL 9 PG2

T 6P20
SPAN 1 . 4500
K1 K2 K3 K4 K5
40 28 08 05 22

MOTOR RUN 555 R 146 A 82 Ø 6.2
ST 100 ES 114
M1 M2
27 05 B 0091
50 15 B 0105
52 16 A 0102
53 16 A 0106
54 16 A 0117
55 15 B 0111
56 15 B 0104
59 16 A 0106
60 15 B 0101
33 21 A 0103
05 26 A 0100
43 26 A 0102
44 26 A 0101
47 26 A 0101
49 26 A 0102
55 25 B 0104
06 27 E 0101

SET M1 M2  54 16

1.2.3X4.5. R 4500 A 2250 Ø 33.5 ST
ST 2350
S1 S2 S3 S4 S5
   01              B 2352
   06              B 2481
         24        D 2449
         46        D 2352
   01              B 2352
   06              B 2481

SET S2  06

1P/2 3P/2X 4P/2 5P/2
S1 S3 S4 S5
         02       D 2458
         05       D 2424
         07       D 2392
12                A 2568
         12       D 2377
    13            C 2468
17                A 2359
         19       D 2401
         24       D 2627
         26       D 2357
         29       D 2400
         31       D 2350
         36       D 2408
         41       D 2400
         46       D 2369
         48       D 2383
         53       D 2355

SET S1 S4  12 24
```

```
3P4X  5P/4

S3 S5
11      C 2350
13      C 2935
15      C 2383
18      C 2404
21      C 2386
29      C 2373
34      C 2432
36      C 2392
41      C 2404
43      C 2391
08      C 2364
11      C 2350

SET S3  13

999 R 640 A 320 Ø 12.6 ST 340
S5
05 A 0373
07 A 0341
10 A 0405
16 A 0354
19 A 0365
21 A 0533
23 A 0346
26 A 0345
32 A 0399
37 A 0380
42 A 0363
43 A 0360
45 A 0364
48 A 0367
53 A 0350
56 A 0353
58 A 0342
59 A 0367

SET S5 21
//3344 -   48

SPAN 1   100  //3344 - 000

K1 K2 K3 K4 K5 S1 S2 S3 S4 S5 M1 M2
40 28 08 05 22 12 06 13 24 21 54 16

DECODE FROM 02

9BOESE9FEIND9ERST9DA5ZA889KR5A

ALL CERTAIN

D/1/GUEST.    all.
```

23E χ-SETTING WITH $\bar{\chi}_2$ LIMITATION

(a) <u>Runs against $\bar{\chi}_2 = x$</u>

Bulges are greater when $\bar{\chi}_2 = x$ than when $\bar{\chi}_2 = .$.

To run against $\bar{\chi}_2 = x$, instead of on the whole text, approximately halves the effective text, so that it will not increase the sigma-age unless the proportional bulge is greater in the ratio $\sqrt{2}$ to 1 at least; but this is usually so.

It is shown below that 1+2, $\bar{\chi}_2$ x will have a greater sigma-age than 1+2 if d, the number of dots in μ_{37} is less than 28, so that a break-in against $\bar{\chi}_2$ crosses is preferable unless the dottage is very high. It is fairly obvious that the effect will be greater in subsequent runs, which involve altogether three or more χ-wheels; in fact, whenever it appears that a message is on $\bar{\chi}_2$ limitation, all subsequent runs are done against $\bar{\chi}_2 = x$

(b) <u>Break-in runs for $\bar{\chi}_2$ limitation.</u>

There is often a better break-in than either 1+2 $\bar{\chi}_2$x, or 1+2. On the whole text, excluding random effects, 1 = . , 2 = . , are flat, and 1x2x has the same bulge as 1.2. . Against $\bar{\chi}_2 = x$ this is not so, the bulges having the same direction as in ΔP. Against $\bar{\chi}_2 = .$; ΔP tends to appear reversed.

This suggests, if U58 are very numerous, the one-wheel break-in 2 = $\bar{\chi}_2$. (since 2x $\bar{\chi}_2$x, 2. $\bar{\chi}_2$. are equally strong, there is no point in running them separately); if /'s are very numerous (this is now rare) 2 $\neq$ $\bar{\chi}_2$.

It suggests further, the runs 1x2x $\bar{\chi}_2$x, 1.2. $\bar{\chi}_2$. or the combined run 1=2= $\bar{\chi}_2$ [for pluggging and switching see 53J(k)]

Note: the more consistently good run "1x2x $\bar{\chi}_2$x OR 1.2. $\bar{\chi}_2$." cannot be done on existing Colossi: it could be done on Super Rob. See R5 p 100 R0 pp 42, 43.

The following table is a useful practical guide: its theoretical basis is indicated in 23E(d) below.

	$d \leq 19$	$20 \leq d \leq 27$	$d \geq 28$
First choice	1+2. $\bar{\chi}_2$x	1=2= $\bar{\chi}_2$	1=2= $\bar{\chi}_2$
Second choice	1=2= $\bar{\chi}_2$	1+2. $\bar{\chi}_2$x	1+2

(c) <u>Theoretical not on A, σ, θ, ϕ.</u>

With negligible error A and σ for the runs 2 = $\bar{\chi}_2$, 1=2= $\bar{\chi}_2$ may be taken as

$$2 = \bar{\chi}_2 : A = \frac{N}{4}, \sigma = \frac{1}{2}\sqrt{N(1-\theta^2)},$$

$$1=2= \bar{\chi}_2 : A = \frac{N}{4} ; \sigma = \frac{1}{4}\sqrt{3N(1-\frac{\theta^2}{3})}$$

Where θ is the proportional bulge of $\Delta\chi_2 + \overline{\chi}_2 = .$

In practice σ is calculated by supposing $\theta = 0$, though because θ may be as great as $\frac{1}{3}$, the error is not always negligible [R5 p.93].

The exact expressions for A and σ are

$$2=\overline{\chi}_2:\quad A = \tfrac{N}{2}(1+\theta\phi);\quad \sigma^2 = \frac{N^2}{4(N-1)}\left\{1-(\theta^2-2\theta\phi+\phi^2-\theta^2\phi^2)\right\}$$

$$1=2=\overline{\chi}_2:\quad A = \tfrac{N}{4}(1+\theta\phi);\quad \sigma^2 = \frac{3N^2}{16(N-1)}\left\{1-\tfrac{1}{3}(\theta^2-4\theta\phi+\phi^2-\theta^2\phi^2)\right\}$$

where ϕ is the proportional bulge of $\Delta Z_2 = .$, its expected value being $\theta\beta\pi_x$

<u>(d) Expected sigma-age of $\overline{\chi}_2$ limitation break-ins</u>

The above table (para. (b)) is constructed by finding the expected sigma-ages, viz ~~(for the last three it~~ is supposed that $\theta = 0$).

1 + 2.	:	$\frac{\beta\sqrt{N}}{2\sqrt{6}}\,\pi_{xx}\,.\,\sqrt{6}\left(1+\frac{\pi_{..}}{\pi_{xx}}\right)$
1 + 2. $\overline{\chi}_2 x$	:	$\frac{\beta\sqrt{N}}{2\sqrt{6}}\,\pi_{xx}\,.\,\sqrt{3}\,(2-\beta)\left(1+\frac{\pi_{..}}{\pi_{xx}}\right)$
1 = 2 = $\overline{\chi}_2$	:	$\frac{\beta\sqrt{N}}{2\sqrt{6}}\,\pi_{xx}\,.\,2\sqrt{2}$
2 = $\overline{\chi}_2$	:	$\frac{\beta\sqrt{N}}{2\sqrt{6}}\,\pi_{xx}\,.\,\sqrt{6}\left(1+\frac{\pi_{.x}}{\pi_{xx}}\right)$
1 = 2 = $\overline{\chi}_2 x$ or 1.2. $\overline{\chi}_2 x$ or 1.2. $\overline{\chi}_2 .$	:	$\frac{\beta\sqrt{N}}{2\sqrt{6}}\,\pi_{xx}\,.\,\sqrt{\tfrac{1}{4}}\left\{(5-\beta)+(3-\beta)\frac{\pi_{..}}{\pi_{xx}}\right\}$

Comparing these

1+2. is better than 1+2. $\overline{\chi}_2 x$ if $\sqrt{2} > 2-\beta$, i.e. to the nearest integer [illegible]28;

1=2=$\overline{\chi}_2$ is better than 1+2. if $\frac{\pi_{..}}{\pi_{xx}} < \frac{2}{\sqrt{3}} - 1$;

1=2=$\overline{\chi}_2$ is better than 1+2. $\overline{\chi}_2$ x if $\frac{\pi_{..}}{\pi_{xx}} < \sqrt{\frac{2}{3}}\,\frac{2}{2-\beta} - 1$

$\frac{\pi_{..}}{\pi_{xx}}$ is usually small and often negative. The table is devised by supposing it to be 0.1

When θ is large, the above formulae are unfair to the last three runs, especially to 2 = $\overline{\chi}_2$.

It may be shown, similarly, but with more algebra, that neither component of 1=2=$\overline{\chi}_2$, i.e. 1.2. $\overline{\chi}_2$. or 1x2x $\overline{\chi}_2$x, can ever be the best run to use. [R0.pp.40,44,107; R1 pp.5,9,27; R5 p.38; See R5 pp.13,25]

<u>(e) 2 = $\overline{\chi}_2$</u>

This is better than its sigma-age would indicate, for it is a one-wheel run. It is at its best for large values of θ (which may be as great as $\frac{1}{2}$), but will never be the strongest run unless $\frac{\pi_{.x}}{\pi_{xx}} > -\frac{1}{4}$

It takes very little time to run. [R1 pp.5,9; see R4 pp.70,92].

<u>(f) QEQ</u>

It is not always known beforehand whether $\overline{\chi}_2$ limitation is in use. A few links change the limitation frequently (this was common in the days of $\overline{P}_5$.) : Sixta is sometimes able to give log information about this (QTQ information).

(g) Tests for $\overline{\chi}_2$ limitation

If there is any doubt, the initial run is chosen according to whichever limitation is the more probable, and when the message is set on χ_1 and χ_2, 1+2 = . is counted against $\overline{\chi}_2$= x and against $\overline{\chi}_2$= . . There is an exact formula for the decibannage which this gives in favour of $\overline{\chi}_2$ limitation, in terms of motor dottage; but commonly a simpler inexact rule is used, namely: for $\overline{\chi}_2$ limitation, the bulge against $\overline{\chi}_2$x is at least twice the bulge against $\overline{\chi}_2$. .

The earlier rule, that for $\overline{\chi}_2$ limitation the sigma-age against $\overline{\chi}_2$= x should be greater than the sigma-age on the whole text , is grossly biased against $\overline{\chi}_2$ limitation . [See R4p 89. R4 pp7,50,55,72.]. If the motor dottage is high it may be impossible to decide whether the limitation is χ_2 until more wheels are set.

(h) 4-letter counts

When a $\overline{\chi}_2$ limitation message is set on 1+2, four counts are made against $\overline{\chi}_2$= x : 1.2., 1.2x, 1x2x, 1x2. . These confirm that $\overline{\chi}_2$ is in use and indicate which letter to run for, in particular whether to run for 5&U or for / [R5 pp.38,71,80].

(i) 03 = $\overline{\chi}_2$

In R5 p 94 the run 5=4/=1x2= $\overline{\chi}_2$ is suggested, but the evidence is not unbiassed.

(j) $\overline{\chi}_2$+ $\overline{P}_5$ limitation

Since P_5 → . , this shows the characteristics of $\overline{\chi}_2$ limitation weakly; the letter 5 is anomalous, being stronger against $\overline{\chi}_2$ dots [illegible] 74,87.]

(k) The effect of corruption on 2 = $\overline{\chi}_2$, 1=2= $\overline{\chi}_2$

If there are many corrupt letters replaced by 9's, the not 99 gadget should be used to ignore these; otherwise, except when Θ = 0, the score may be spuriously enhanced.

It is easy to show that, if a proportion λ of the message consists of corruption 9's, and the sigma-age of these runs on the incorrupt text is S, then the apparent sigma-age is approximately

$$\text{for } 2 = \overline{\chi}_2 \quad : \quad S\sqrt{1-\lambda} + \lambda\theta\sqrt{N};$$

$$\text{for } 1=2= \overline{\chi}_2 \quad : \quad S\sqrt{1-\lambda} + \lambda\theta\sqrt{\tfrac{N}{2}};$$

23 F MESSAGE SLIDES

(a) Definition of Message Slides

In statistical setting, a few wrong letters of cipher do not matter much, but a single omitted letter or inserted letter makes it impossible to find any setting for the χ's which is correct for the whole message. The effect of one (or more) omitted or inserted letters is called a Message Slide. It does not necessarily make it impossible to find settings , for, with the χ's set correctly for one part of the message, ΔD will have systematic bulges on this part, which will not be greatly changed by the addition of the merely random bulges on the rest of the message: the sigma-ages will of course be reduced, because the text length is that of the whole message, the score that of a part only.

(b) Rival Settings

A message slide can sometimes be detected by inspection of the 1+2 scores. If several (say 3) letters are omitted, the settings of all χ - wheels will be increased by three.

A pair of scores such as

26	17	1398	$5.9\,\sigma$
29	20	1253	$4.1\,\sigma$

suggests very strongly that there is a slide of 3 at a place dividing the tape roughly in the ratio 3:2 ; but see Antislides [23G (d)].

(c) Spanning

In any case, as soon as a message is set on any wheels, the relevant score is spanned, in thousands or in thirds whichever is the less. If some parts show no bulge there is probably a slide: this will increase the sigma-age on the remainder; it is worth while to span scores down to $3.7\,\sigma$ unless a certain setting has already been obtained. Subsequent runs are done on a slide-free portion.

(d) Slide Runs

When the parts of a message at slide settings are of considerable length, it is usual, after setting all wheels, or even before, to set the other parts by means of a Slide Run. The χ's are all set back a few places and are stepped together (upper switches on Colossus) counting those letters which are most numerous in the part already set, e.g. /U58, spanning a part not set. Because this is a short run (usually 50 positions at most) it is not necessary to have a very high sigma-age, especially if the slide between the two parts is found to be small.

(e) Doctoring of tapes

If it is difficult to set the other wheels, it may be worth while to do a slide run on 1+2. , for when the settings of the various parts have been found it is possible to "doctor" the tape, i.e. to put the parts in their correct relative positions by inserting or removing letters: this is in fact rarely done except during wheel-breaking [redacted]).

(f) Break-ins with spanning

If it is thought likely that a message contains a slide, especially when it is to be "flogged" [23J(b)], the break-in runs may be done whilst spanning a suitable part of the text. Suitable spans are first two-thirds and last two-thirds.

Alternatively, since slides are more probable when interception fails to identify letters, which are then represented by 9's, count 99's with spanning, and select a stretch with as few as possible.

Raw tapes are spanned over the first 2500 letters, and, if long enough (> 4000) over the last 2500.

(g) Message slides and wheel slides

It is important not to confuse message slides with wheel slides [23G] whose only common feature is that they give rise to rival settings.

(h) X Procedure

Occasionally two messages are sent without resetting wheels: switching the Tunny machine out and in, automatically inserts exactly two letters of key between them; the two messages are therefore punched on the same tape with [redacted] two letters inserted, and become a single message so far as χ-setting is concerned. [cf 11B(k), 11D(4)]

Note: The interruption disturbs the stepping of the ψ's so that when setting ψ's the two cannot always be treated as a single message.

23G WHEEL SLIDES

(a) Definition

Consider a wheel which has a large number of agreements with itself at a different setting; for example, the extreme case of a "perfect" wheel, such as

$\Delta\chi_6$	x	x	.	x	.	x	.	x	.	x	.	x	.	x	.	x	.	x	.	x	.	x	.	
$\Delta\chi_6$ 2 back	x	.	x	x	.	x	.	x	.	x	.	x	.	x	.	x	.	x	.	x	.	x	.	

where there are only two disagreements between the wheel and the same wheel two back. The two settings are said to be slides of one another.

(b) Rival settings

At characters where two settings of a wheel agree, each setting will gain the same contribution for its ΔD count: if one of them is the right setting then at these characters the wrong ("slide") setting will have a systematically good ΔD count, elsewhere a systematically bad count. If the agreements are sufficiently numerous, this slide setting will have a score almost as large as the right setting, and may by random chance have a higher score.

With perfect wheels it is in fact, often difficult to distinguish between the right setting and its slides.

(c) Length of slides

Owing to the absence of long stretches of dots or crosses in $\Delta\chi$ wheels, slides at interval 1 do not occur: a slide at interval 2 is by far the most common: it tends to produce consequent slides of 4,6,...

(d) Antislides

In a run such as 1+2, which is unaffected by interchanging dot and cross in both $\Delta\chi_1$ and $\Delta\chi_2$, a good score will be obtained at settings with an excess of disagreements with the correct settings. This circumstance is called an antislide on both wheels. An antislide is usually at interval 1, and may be mistaken for a message slide until spanning is done.

(e) Setting slidy wheels

When setting messages on wheels known to have strong slides, the most rapid method is to accept, provisionally, the highest score for a slidy wheel, even though there are others almost equally good, for on this basis it will generally be possible to set the other wheels. When all wheels are "set", at settings which are either correct or good slides, all the evidence of the 32 letter count will be available to discriminate between a correct setting and its slides. The evidence from, say, /,5,U, may be adequate to set χ_3 uniquely, when the evidence of 1+2. is not.

Even in cases where the slides are only moderately strong, it is often worth while, at the end of setting, to "run back to confirm" a setting which has possible competitors.

(f) Random setting of perfect wheels

When some wheels are perfect or nearly perfect it should be possible to set messages by taking each such wheel at two (odd and even) random settings, and using these to set the other wheels. Perhaps the simplest method is to allow the perfect wheels to step while the other wheels are run round a few times. In this way it is feasible to do what are in effect 3- or 4- wheel break-ins. (R1 pp.19,22-25,29; R2pp.19,21;R4 pp.24,28.)

23H FLOGGING RUNS

(a) Flogging

Flogging is trying all methods which may possibly help to set a message. This may be done

(i) because of intelligence or cryptographic priority.
(ii) because of lack of work.
(iii) for ostentatious display (towards D.O. or Wrens).

(b) Flogging Break-ins.

The usual runs are 1+2. and 3+4x . If these fail on a message which is to be flogged, 2+5, 4+5, 1+3, 2+4 are all reasonable; but see R4 p.15. Note: except with $\bar{\chi}_2$ limitation the only 2-wheel break-ins are $i+j$ = . or x .

If there is any doubt about $\bar{\chi}_2$ limitation, break-ins can be done on both assumptions.

Break-ins with spanning can be used on a generous scale. [cf 23F(f)].

(c) 3- and 4- wheel runs

A more powerful method is to do a break-in on more than two wheels. It might [illegible] be possible to do a complete 3-wheel run in ten hours or so, but ΔD characteristics happen to be such that no 3-wheel run is very advantageous. 4-wheel runs, in particular 1=2=4=5/ are [redacted], but run completely they are intolerably long [but see ¶]

A compromise is to do a 1+2 break-in followed by 4=5=/1=2 at all $\chi_1\chi_2$ settings which score more than 2 σ , naturally taking the higher scores first. This has sometimes succeeded, but it is long and laborious.

So little evidence is obtained from the 2^{e} score that the full sigma-, a four-wheel run is needed [23 C (a)] [R2 p.76; R5 pp.35,54,97].

(d) Subsequent Runs

The number of theoretically possible runs is large. If there are two possible runs for the same wheels there is clearly some advantage in combining them: it saves times; the text is longer and if the runs are of similar strength the expected sigma-age is higher; but if, contrary to expectation, one of them is weak, or goes the wrong way, a great deal of evidence is lost. When flogging very hard it is better to keep runs separate and to combine their evidence by the methods of 23J.

Note: if two runs whose texts and proportional bulges are $n_1, \delta_1; n_2, \delta_2$, are run together the sigma-age is greater than that of the run n_1, δ_1, if

$$\frac{\delta_2}{\delta_1} > \sqrt{\left(\frac{n_1}{n_2}\right)^2 + \frac{n_1}{n_2}} - \frac{n_1}{n_2}$$

if $n_2 \ll n_1$, this is $\frac{1}{2}$; if $n_2 = n_1$, this is $\sqrt{2}-1$. [R1,p.62.]

(e) Construction of useful runs

It is unnecessary to enumerate all runs: consider how such runs may be devised. Suppose that $\chi_1 \chi_2$ are set, and that it is desired to set $\chi_3 \chi_4$. Clearly two letters differing only in the fifth impulse will be indistinguishable. Moreover when counting, for example, /T i.e. 1.2.3.4. , it will be necessary to look at all places where 1 = . 2 = . it is convenient to set forth the 32 letter alphabet thus:

$\underbrace{\text{/T, 9H, O3, MN}}_{1.2.}$ $\underbrace{\text{RG, CV, L4, IP}}_{1.2x}$ $\underbrace{\text{AW, UQ, 5J, 8K}}_{1x2x}$ $\underbrace{\text{DB, FX, ZE, YS}}_{1x2.}$

Where 1.2.	a good run is	$\frac{\text{/T O3}}{\text{9H MN}}$	i.e. 3./1.2.
1.2x	a weak but useable run is	$\frac{\text{RG IP}}{\text{L4 CV}}$	i.e. 3+4x/1.2x
1x2x	a good run is	$\frac{\text{UQ 5J}}{\text{AW 8K}}$	i.e. 3+4x/1x2x
	or if 8' are numerous	$\frac{\text{UQ 5J 8K}}{\text{AW}}$	i.e. not 3.4./1x2x
1x2.	a good run is	$\frac{\text{FX YS}}{\text{DB ZE}}$	i.e. 3x/1x2.
	a sometimes useable run is	$\frac{\text{FX YS ZE}}{\text{DB}}$	i.e. not 3.4x/1x2.

3+4x/1.2x and 3+4x/1x2x could be combined into 3+4x/2x, but the run 3+4x/1.2x is so much weaker than the other that this would be unwise.

Not infrequently 3x/1x2. and 3./1.2. can profitably be combined as 3+/1.2.

To set $\chi_4\ \chi_5$, having set $\chi_1\ \chi_2$ the useful runs (not all independent) are

$$\frac{\text{/9}}{\text{HT CM N3}}\qquad \text{i.e. } 4.5./1.2.$$

$$\frac{\text{58}}{\text{AU QW KJ}}\qquad \text{i.e. } 4x5x/1x2x$$

$$\frac{\text{/9 58}}{\text{HT CM N3 AU QW KJ}}\qquad \text{i.e. } 4=5=/1=2$$

$$\frac{\text{58 AU}}{\text{QW KJ}}\qquad \text{i.e. } 4+5/1x2x$$

$$\frac{\text{/9 58 AU}}{\text{HT CM N3 QW KJ}}\qquad \text{i.e. } \begin{cases} 4+5/1x2x \\ \text{or } 4.5./1.2. \end{cases}$$

All these can easily be run using multiple testing.

To set $\chi_3\ \chi_4$ having set $\chi_1\ \chi_2$ the only new useful run is 3.5./1.2.

The reader may be interested to work out all possible runs supposing that $\chi_3\ \chi_4$ are set first [R3 pp.95,124; R5 p.106]

(f) Runs for the last wheel

These may be expressed compactly

For χ_3 $\dfrac{\text{U / 5 J 3 F X O G P Q Y S H I R}}{\text{A 9 8 K N D B M V L W Z E T 4 C}}$

For χ_5 $\dfrac{\text{/ U 5 8 D F G Z 9 P 3 A Y M}}{\text{T Q J K B X R E H I O W S N}}$

The letters above are good letters in order of merit, the letter below is that which differs from it on the impulse to be set.

For hard flogging the letters may be run separately but simultaneously on the five counters of Colossus.

Otherwise the letters may be run in batches e.g. for χ_3 U/5 ; J3FXOG ; PQYSH. [RA pp.42,82.]

(g) ΔD Bigram Runs

Because Colossus looks only at one place and remembers one other, the use of these is limited. The multiple test memory circuits are unsuitable because they remember only a single wheel.

The ΔD bigram U5 since Colossus Δ's backwards, is equivalent to $\Delta D = 5\ \ \Delta^2 D = M$. If a ΔZ tape and $\Delta\chi$ wheels are used the Colossus plugging and switching required is

$$Z_1 + \chi_1 = x\ ,\ Z_2 + \chi_2 = x\ , Z_3 + \chi_3 = \cdot\ ,\ Z_4 + \chi_4 = x\ .\ Z_5 + \chi_5 = x\ .$$
$$\Delta Z_1 + \Delta\chi_1 = \cdot\ , \Delta Z_2 + \Delta\chi_2 = \cdot\ , \Delta Z_3 + \Delta\chi_3 = x\ , \Delta Z_4 + \Delta\chi_4 = x\ , \Delta Z_5 + \Delta\chi_5 = x\ .$$

(h) Use of evidence other than ΔD

If a message can be set on some but not all χ's it may yet be possible to

(i) set the motors [23 L]
(ii) send a de-chi on fewer than 5 wheels to the Testery, where language methods can be applied.

23J FLOGGING THE EVIDENCE

(a) Impracticability of an exact formula.

No simple formula for weighing the evidence of a run can be exact. Evidence is derivable not only from the sheer magnitude of the bulges but also from having bulges on the right letters, or on a consistent group of letters (e.g. on all language letters); in other words it is unjust to take the message as a fair sample of itself, and necessary to include other messages.

This section gives only a brief crude account with a minimum of mathematics. For a more refined treatment see 23X.

(b) A primitive formula

If it is assumed that the message is a fair sample of itself, the factor in favour of a setting due to a sigma-age is proportional to $e^{\frac{s^2}{2}}$ [cf 24X.]

It follows that the odds in favour of a setting with sigma-age s_1 is about

$$\frac{e^{\frac{s_1^2}{2}}}{2\omega + \sum e^{\frac{s^2}{2}}}$$

where $\sum$ refers to rival settings and 2ω allows for random settings.

The decibanage is 10 $\log_{10}$ of this [21 (g)]. This is, essentially, the formula used to construct the table for decibanning wheel-setting runs.

(c) Combining the evidence of several runs

If several runs are used to set the same wheel or wheels.

$$\text{odds} = \frac{e^{\sum_{\text{runs}} s_i^2/2}}{\omega' + \sum_{\text{competitors}} e^{\sum_{\text{runs}} s_i^2/2}}$$

If there is no competition the decibanage is

$$\sum_{\text{runs}} 2.17\, s_i^2 - 10 \log_{10} \omega' - 3.$$

from which the "Certain,Good" tables [23C(b)] may be derived.

If there is competition, $\sum 2.17\, s_i^2$ can be found for each competitor and the results compared. [R3 p.134; R4 p.1,70; R5 p.1,3,7,113.]

23K CHECKS ON SETTING

(a) General

This does not deal with the complete system of checks [35 D+E], but only with checks applied during setting on Colossus.

Setting yields D = χ + Z.

Both χ and Z are checked beforehand; D is checked afterwards. Each score used is checked as it occurs [see 23D].

(b) χ Tests

The χ to be tested is the pattern set up on the triggers: this is not checked for each message, but only when patterns are set up afresh or are subject to suspicion.

(c) χ Test Tapes

The obvious method of checking χ triggers is to make a tape Z = χ at some definite settings, and count /'s in Z + χ = χ + χ = /. The correct score is of course the text length, or span length. It is better to count /'s in ΔZ + $\Delta\chi$ which checks Colossus Δ'ing simultaneously : this of course reduces the score by 1.

Such a tape not only checks the trigger; but, by being spanned, enables a fault to be located either on the trigger or on the tape itself.

χ test tapes are made to a standard length of 2002 and spanned 0001 - 2001.

(d) χ Test Runs

To avoid the need for putting on the special χ test tape, counts are made depending only on the χ trigger and the span, so that any sufficiently long tape which happens to be on Colossus can be used. The χ test tape is required once only, as early as possible: if it checks, χ test runs are done at once and the scores recorded. Thereafter the trigger can be checked by repeating these runs and seeing that the same scores are obtained.

The actual form of the test is to count $\Delta\chi_1 + \Delta\chi_2 + \Delta\chi_3 + \Delta\chi_4 + \Delta\chi_5 = \cdot$

spanning 0001-2002, starting with settings 01, 01, 01, 01, 01 and stepping χ_1, χ_2 together through ten places.

(e) Z Check

The preliminary checks are described in 35 . The text length is measured by hand counter: as soon as the tape is put on Colossus the text length is counted: the score should be one less because of Δ'ing.

(f) D Checks (i.e. check of the D tape made by Tunny).

Two different methods are used

(i) Comparison of $\begin{cases} \Delta D \text{ 32 letter count using Z-tape and } \chi \text{ wheels.} \\ \Delta D \text{ 32 letter count using D-tape.} \end{cases}$

(ii) On Colossus, using a slide-free portion of text, find the 2nd,3rd,....9th letters (by spanning 01-02, 02-03 etc.) and similarly 4 letters at the beginning of each stretch of 620 letters, and the last 4 letters.

Compare this with a print-out, on Junior, of D in widths of 31 (620 = 20 x 31) [For an early form of the test R4 p 65].

(g) Theory of χ Test Runs

Suppose there is one erroneous character in $\Delta\chi_i$ (in fact, if there is one there must be two, because χ_i is Δ'd by Colossus). As usual let the text length be N, the wheel length ω.

This one error will cause the score of $\Delta\chi_i + U$ = . to be changed by the excess of dots over crosses in U at the $\frac{N}{\omega}$ places against the erroneous character of $\Delta\chi_i$.

This excess has expected value 0 and standard deviation $\sqrt{\frac{N}{\omega}}$.

The change will be numerically less than 4 if

$$|\text{sigma-age}| \times \sqrt{\frac{N}{\omega}} < 4$$

If $\omega = 41$, N = 2000, then $|\text{sigma-age}| < .57$
whose probability is 0.43

To exclude the possibility of having all changes less than 4 (smaller changes being liable to confusion with unsteady counting by Colossus) a considerable number of readings is required. Ten readings reduce the probability to $(0.43)^{10} = \frac{1}{5,000}$.

It is clearly wasteful not to include every $\Delta\chi_i$ in every reading taken.

In an archaic version $\Delta\chi_1 + \Delta\chi_2$ was counted in four positions only: the chance of nearly correct scores with a wrong wheel in the trigger was considerable and is believed to have occurred. [R3 p 60,127,128,129]

23L STATISTICAL SETTING OF THE MOTOR

(a) Rough Method

When the motor is set by hand it is done after the Ψ's have been set on the de-chi. In statistical setting the motor is set before the Ψ's. The usual method of doing this is by consideration of the number of occurrences of various ΔD letters occurring opposite BM dots, though it is occasionally convenient to make use of the BM crosses also. For example if / is a very good letter in ΔD this will mean that it is even better, relatively, in ΔD opposite BM = . If the limitation is $\bar{\chi}_2$ one would naturally 'look' at places on the tape where $\bar{\chi}_2$ = x, in order not to water down the run. In this case the run for the BM may be regarded as a run for the TM and therefore the ΔD frequencies opposite motor dots will be ΔP frquencies.

(b) Expected sigma-ages

Suppose that the limitation is $\bar{\chi}_2$ and that there are $r_x, r_.$ /'s opposite $\bar{\chi}_2$ = x,• in ΔD. Let the text length be N of which $N_x, N_.$, letters occur opposite $\bar{\chi}_2$ = x,• . Let the number of dots in μ_{37} be 37D. Let the proportion of /'s in ΔP be p, and let the proportion of /'s in ΔD at motor crosses be q. The expected proportion of /'s in ΔD at TM dots is p and the expected value of q is $r_./N_.$. (This idea of using the count of ΔD at $\bar{\chi}_2$ = . as a means of sampling what happens at motor crosses was first suggested in RO.49) The expected number of /'s in ΔD at $\bar{\chi}_2$ = x is

$$N_x \left\{ D p + (1-D) q \right\}$$

and the expected no. of /'s opposite TM dots is $N_x D p$

Thus $$r_x = N_x \left\{ D p + (1-D) \frac{r_.}{N_.} \right\}$$

and $$E.S. = N_x D p = r_x - (1-D) r_. \frac{N_x}{N_.}$$

where E.S. means expected score. If the motor is incorrectly set the expected score or average, a, is given by $a = D r_x$

and $$\sigma = \sqrt{r_x D (1-D)\left(1 - \frac{r_x}{N_x}\right)} \qquad \text{[see 21(n)]}$$

$$\doteqdot \sqrt{r_x D (1-D)} \qquad \text{in most cases}$$

Therefore expected bulge is $(1-D)\left(r_x - r_. \frac{N_x}{N_.}\right)$

and this is fairly close to $(1-D)(r_x - r_.)$

The expected sigma-age is $(r_x - r_.)\sqrt{\frac{1-D}{D r_x}}$

For example if $D = \frac{1}{2}$, $r_x = 169$, $r_. = 100$

the expected sigma-age would be 5.3 . This would be more than sufficient to distinguish between the 2257 (= 37 x 61) different possible hypotheses about the possible motor settings. With D = 3/4 and the same values of r_χ and $r_\cdot$ the expected sigma-age would be only 3.7 .

The argument and formula for the expected sigma-age would be equally valid for any other letter or group of letters, instead of /'s. In particular it can be used for groups of weak letters instead of strong ones. The expected sigma-age is then negative and one has to look for low scores instead of high ones. The formula is not so reliable in this case, since the sampling numbers r_χ and $r_\cdot$ are smaller.

(c) Expected sigma-age with limitation not $\bar{\chi}_2$.

When the limitation is not $\bar{\chi}_2$, a similar formula can be obtained equally easily if ΔD is assumed to be 'flat' against motor crosses.

If r is the number of occurrences of the letters in ΔD and if p, q, N, D have the same meanings as before, then, by equating the expected value of r to the observed value we have

$$r = N\frac{D}{2}p + N\left(1 - \frac{D}{2}\right)q$$

and $$E.S. = N\frac{D}{2}p + N\frac{D}{2}q$$

$$= r - (1 - D)Nq$$

Expected bulge $$= (1 - D)(r - Nq)$$

$$= (1 - D)(r - N\nu)$$

where ν is the number of letters of the alphabet being looked for. Expected sigma-age is

$$\left(r - \frac{N\nu}{32}\right)\sqrt{\frac{1 - D}{Dr\left(1 - \frac{r}{N}\right)}}$$

$$\approx \left(r - \frac{N\nu}{32}\right)\sqrt{\frac{1 - D}{Dr}}$$

Sometimes the assumption of 'flatness' opposite motor crosses is quite wrong. For example, if / is a common P letter then 8 is a good motor cross (ΔD) letter and a motor run for 8's may be far less powerful than the preceding formula suggests.

(See operational log 01, pp. 3237, and R5 p.32 etc.).

This difficulty does not arise when the limitation is $\bar{\chi}_2$.

(d) Complementary nature of machine and hand methods.

It is interesting to observe that, for given ΔD count, the expected sigma-age on any motor run is larger for smaller μ_{37} dottages d. This is what has been described as a 'swings and roundabouts' effect. When d is lower it is harder to set the χ's, but if they can be set then it is easier to set the motor. Fortunately machine and hand methods are complementary in this respect. When d is high, the psis are easy to set by hand and then the setting of the motor is a routine job.

(e) Pick-ups

The formula of the expected sigma-age can be used for deciding between alternative motor runs, but of course, it is possible to do more than one independent motor run and look for pick-ups between the runs. (This is a reason for using a set total of not more than $2\frac{1}{2}$ sigma in motor runs.)

(f) Switching of a motor run on Colossus

The motor run is usually of the form

$$\delta M = \cdot | \Delta D \in \tau$$

or

$$\delta M = \cdot | \Delta D \in \tau \; ; \; \bar{\chi}_2 = x$$

where τ is a class of teleprinter letters. When the conditions to the right of the vertical line are switched by themselves the score obtained, which is called r , provides a check of the χ settings and patterns and of the correctness of the tape etc. The routine of counting r before doing the run is the same as in the case of χ setting. The run is done quintuple testing on μ_{37} and takes under 10 minutes for a tape of length 5000. For further details as to switching see 53L (h)(1) . The best score on the motor run is always checked even if it is not good enough to use.

(g) Good slides of the motor

Quite often a top score of as much as $5\,\sigma$ on a motor run may not be certain due to strong competition arising from good slides of the basic motor against itself. These good slide settings do not all agree with one or other of the settings corresponding to the top score. See for example R0,58 and R3,9. In this way good slides of the motor are rather different from those of the χ's and ψ's. In particular it is not a good policy to stop motor runs in the middle when a good score comes up and then cross run for μ_{37} and μ_{61} as short runs.

(h) Motor runs with not all the χ's set.

Suppose $\chi_{1,2,3,4}$ are set but χ_5 has given difficulty. Then we may sometimes be able to set the motor and to use the new information for setting χ_5 . The expected score for a motor run with not all the χ's set can be obtained in the same way as in the case when all five χ's are set, but it so happens that we are more likely to run into trouble due to the use of good motor cross letters. For example, the expected score for the motor run on C3 (not χ_1 limitation) has been found by a semi-empirical method to be about $\left(1 - \frac{d}{10}\right)$ times the value obtained by the crude method of assuming flatness against motor crosses (See R5 pp.26,32).

We should perhaps emphasise here that with χ_2 limitation there is always the sample of $\bar{\chi}_2 = .$ and complicated formulae can be avoided.

(i) Motor run with only χ_1 and χ_2 set

The last remark applies even in the extreme case in which the only wheels set are χ_1 and χ_2, when the 4 letter counts against $\bar{\chi}_2 = x$ and $.$ may both be done and the best run or combination of runs may be deduced. There is a single exception to this, namely in the run BM = . /1+2. In this case the behaviour of ΔD_{12} at motor crosses can be calculated easily from the score of /1+2 at $\bar{\chi}_2 = x$ and the result obtained in this way is subject to a much smaller S.D. than the result obtained from the sample opposite $\bar{\chi}_2 = .$. In theory a similar remark applies however many χ's are set, but the calculations are usually too complicated.

It was first realised that motor runs of the type BM = . /1+2 may be frequently practicable when the formula for σ of the type $\sqrt{Np(1-p)q(1-q)}$ was found to apply to motor runs (see 21(n) and R4 pp.4,44,88). The earlier assumption was that σ was $\sqrt{2}$ times as large as it really is. It is found (R4 p.44) that the expected sigma-age of the run BM = ./1+2 divided by the sigma-age of /1+2 is

$$\sqrt{\frac{1-D}{D} \cdot \frac{1-D}{1-\frac{3}{2}D}}$$

The corresponding formula in the case of χ_2 limitation is (R4,p.91).

$$\frac{8(1-D)}{4-3D}\sqrt{\frac{1-D}{6D}}$$

These expressions are sensitive functions of d. (See R4 p.88).

A peculiar feature of the run BM = . /1+2 is that the top score is not necessarily the most probable, if the additional evidence of the number of BM dots in the whole text is taken into account (R4,47). (This type of difficulty occurs also in runs against partial wheels - see 25D(e)) A method of getting round the difficulty is to run BM+/1+2 (See R4,pp.50,55,56,58,105). In theory the same difficulty arises in all motor runs, but the effect is usually negligible.

(j) Spanning

It is sometimes possible to do a more powerful motor run by using only part of the message tape, even if there is no slide, because the message may contain patches which are rich in particular properties. Such spanning can be done in conjunction with an examination of the Red Form, by correlating the spanning with pauses, but in practice it is found too much trouble to get the Red Form as a rule.

(k) Proving the motor settings.

When the limitation does not involve P_5, that is when there is no autoclave it is easy to set the Ψ's. However, for this purpose it is nearly always necessary for the motor to be correctly set (not merely a good slide). In this sense the setting of the Ψ's is the most conclusive way of testing the motor settings. If, however, there are many different settings to choose between, it may be quicker to do a corroborative motor run and look for pick-ups; or simply to count a group of good (or bad) ΔD letters against motor dots at the rival settings of the motor.

Suppose, however, that there is still some uncertainty about the χ's. Then a motor setting which is knew to be at least a good slide of the correct motor may be used for setting or resetting the χ's, by means of runs against motor dots, just as if the motor were correctly set (R3 p.66). If in this way a new χ setting is found it may be used to reset the motor. This is an example of a method of successive approximation. (R3 p.56). A motor setting can be identified as probably a good slide of the right setting by its sigma-age and by comparison of the relations between the settings that have turned up in the run. Observe that if a particular day's motor has a lot of good slides against itself, then there are effectively a lot less than 2257 independent settings possible and therefore a lower sigma-age may be significant. Thus the effect of the motor having good slides is double-edged.

(l) Proving mu 61.

Sometimes a motor run is done with a provisional μ_{61} and the result used to clear up ambiguities in μ_{61}.

23M Ψ-SETTING

(a) Setting Ψ_1 as a motor run

Suppose that the limitation is $\bar{\chi}_2 + \bar{\Psi}_1'$. Then the correct TM depends on the setting of Ψ_1. Therefore it is possible to do a run for Ψ_1 as a motor run, provided the BM and χ_2 are set correctly. Observe that the Ψ_1 wheel is driven by a motor on which it itself has an influence, and in this respect the run differs from a BM run. A similar method can be used for Ψ_5 when the limitation is $\bar{\chi}_2 + \bar{P}_5$ (R2,32) but in this case the dangers of corruption are greater and the usual practice is to use stretches of 800 letters of the message for all Ψ-runs with an autoclave limitation.

In these runs for Ψ_1 or Ψ_5 as motor runs there is a tendency for the settings to bunch together. This is due to an effect from a coalescence which is described below. As a consequence a given sigma-age is more significant than it would otherwise be.

(b) Statistical Ψ-setting with χ_2 limitation.

Once the TM is known, the most powerful Ψ runs are usually those which depend on undifferenced plain language properties. Easily the best letter in undifferenced plain language is 9, so it is not very surprising that one of the five short runs P_1 = ., P_2 = ., P_3 = x, P_4 = ., P_5 = . is usually successful. These runs are done simultaneously on the five counters with S.T. of 3 or 4 sigma. If one of the psis sets there are good runs like 4+5, 1+3^x, 1+2, 2+5, and if more than one psi sets there are even more powerful runs. For example 3^x/1245 should give a nearly 100% score. However for convenience one may use runs of the form $P_{ij\ldots k}$= . or x throughout, since the switching is simple and no change in ST is required. For statistics of these runs see R5, p86. If all five of the short runs fail, the best long runs to try are 1+3x/, 4+5/ and 1+2/. The time taken for a long psi run can be cut down by a method called the 'dottery'. This method depends on the fact that the psis usually have good slides on themselves and also the expected sigma-age in the right place is so large (see RO,41). However if the short runs all fail one should seriously consider the possibility of some of the previous settings being wrong.

A possible effect of a wrong chi setting which is only a good slide for the differenced chi and an antislide for the undifferenced chi is that the corresponding psi may set as an antislide.

When all the wheels have been set the acid test of their correctness is a count of /34 in undifferenced plain language. There should be a patch of about 200 letters with no /34. This test can be used as a method of detecting slides, in order to make the decoding easier. It can also be used for resetting any wheels that have been incorrectly set. Another test of the correctness of the settings is to do some Colossus decoding - the first 9 letters is usual. This helps with the decoding on Tunny later on. The method is to span (n-1) to n (n = 2,3.....) and count P_1 = x, P_2 = x etc. on the five counters. If the scores are say 00100 then the nth letter is 9. The possibility of decoding in this way on Colossus was not foreseen and is a good example of the flexibility of the machine.

Sometimes the '/34 test' fails because all the psis are antislides. When this happens it is easy to put it right. It can also fail due to a 'smooth motor' effect. (This happens about 5 times.) This means that the motor settings are wrong, but happen to give long patches in which the Ψ's are correctly set. It is not easy to put this right on Colossus and the best thing to do is to give the hand cryptographer a de-chi and 'pseudo-psi' stream. This will enable him to get a 'break' and thus to set the psis correctly and reset the motor. Finally the /34 test could fail due to the machine being out of order. The easiest way of deciding the cause of failure is, as ever, to do a letter count, in this case on undifferenced plain language.

(c) <u>Setting Ψ's when not all the χ's are set.</u>

If not all the χ's are set but the motor is set, then this motor can be used for more powerful χ runs, as already pointed out. However a more powerful method is to set the χ's and Ψ's simultaneously.

For example if $\chi_1, \chi_2, \mu_{61}, \mu_{37}$ are set the most powerful procedure is to set Ψ_1 and Ψ_2 and then say χ_3 and Ψ_3 together (R4 p 46).

(d) <u>Testing the machine.</u>

When Ψ runs are done the machine is fully extended and test runs become particularly important. The test runs done are similar to those in the case of χ's and motorised Ψ tapes are made available for each day's keys.

23N COALESCENCE

Suppose that the limitation is $\bar{\chi}_2 + \bar{\Psi}_1'$. Then the Ψ_1 character at any letter of the message may have an influence on the setting of Ψ_1 at the next letter. This gives rise to a remarkable phenomenon known as coalescence. For example two different hypotheses about the initial setting of Ψ_1 with χ_2 and basic motor settings fixed, may give rise to the same Ψ_1 setting at the nth letter and all succeeding letters. The two initial settings are then said to have coalesced by the nth letter. Two theories coalesce by the nth letter if and only if they give rise to the same setting at both the nth letter and the (n+1)th letter. It is shown in (23X) that the chance of the right setting not being coalesced with a good proportion of the 42 other hypotheses after n basic motor dots is about $1{\cdot}3\, e^{-n/160}$.

There are several ways of taking advantage of the phenomenon of coalescence. If a message is sufficiently long, there is no need to run for Ψ_1 if χ_2 and the basic motor are set. We can simply assume a conventional setting (say 01) for Ψ_1 and span from about 2000 to the end, and the wheel will probably be correctly set for the part of the message used. Long runs can be replaced by short runs and 3-wheel runs by ordinary long runs. For example the run $P_3 + P_1 = x$ can be done as a short run (with multiple testing). Or a total motor run can be done instead of a basic motor run (but this cannot be done without multiple testing).

If χ_1 and χ_2 are set a total motor run can be done with a set total of 2σ and then all the results tested out by running $P_2 + /P_1$ multiple testing at each motor setting. If ψ_2 has very good slides against itself it is not even necessary to finish the short runs and 20 or 30 different motor settings can be tried out in a few minutes. Another method of doing the total motor run is to do the basic motor run with a set total of 2σ and then run for ψ_1 quintuple testing, but using only counter 1 (the ψ's corresponding to the other counters are not correctly motorised).

The phenomenon of coalescence occurs with $\overline{\chi}_2\overline{P}_2$ limitation, this time ψ_2 Corruption is liable to interfere in this case. For further suggestion related to coalescence, see R4 pp 74, 75, 87, 91, 97. R5 pp 36, 57, 112.

23P EXAMPLE

For a dossier showing a simple example of motor and psi run see 23D. For an example showing coalescence see Fig 23(I) at the end of this chapter (23).

23W CALCULATION OF THE ODDS OF THE BEST SCORE IN A χ-SETTING RUN

Suppose we have a message of length N and the score of $\Delta D_1 + \Delta D_2 = \cdot$ is $\frac{1}{2}(N + x)$ for particular settings of χ_1 and χ_2. Then, as in 24X(e), the factor in favour of these settings is roughly

$$\frac{25}{\sqrt{N}}\, e^{x^2/2N}$$

provided that nothing is known about the scores at other settings. In practice however we do possess additional information. In fact the knowledge which we are usually willing to use in practice is as follows. The bulge of the top score is β_1, the bulge of the second best score is β_2 and the bulges at all the other settings are (of course) less than β_2. Let T_1, T_2 be the theories that the top score is right or that the second best score is right, respectively, and let T_3 be the theory that one of the others is right. The prior probabilities of these theories are respectively, $\frac{1}{1271}, \frac{1}{1271}, \frac{1269}{1271}$. The factors in favour of the first two, not allowing for competition are

$$25/\sqrt{N}\; e^{2\beta_1^2/N}, \quad 25/\sqrt{N}\; e^{2\beta_2^2/N}$$

In order to obtain the corresponding factor in favour of T_3 it is necessary to introduce a new symbol. Let q be the probability that the correct setting will have a bulge less than β_2. The probability that 1269 wrong settings will all have bulges less than β_2 is obviously a number fairly close to 1 (e.g. at least $\frac{4}{5}$), unless θ_2 is unusually small. Therefore, in most cases, the factor in favour of T_3 not allowing for competition is approximately q. It follows now by the general form of Bayes' Theorem (21(f)) that the odds of theory T_1 allowing for all the evidence mentioned is usually approximated by

$$\frac{\frac{1}{1271}\cdot\frac{25}{\sqrt{N}}\,e^{2\theta_1^2/N}}{\frac{1}{1271}\cdot\frac{25}{\sqrt{N}}\,e^{2\theta_1^2/N}+\frac{1269}{1271}\cdot q}$$

$$\simeq \frac{e^{\frac{1}{2}s_1^2}}{e^{\frac{1}{2}s_2^2}+\frac{1269\sqrt{N}}{25}\cdot q}$$

where S_1 S_2 are the best and second best sigma-ages. The estimate of q must be based on statistics. It depends on the link and end and on N, d, quality of interception and θ_2. However it is a reasonable approximation to assume $q\sqrt{N}$ to be independent of N and this enables the decibannage of the odds to be calculated easily, with the help of tables of

$$10\log_{10} e^{\frac{1}{2}s^2} = 2\cdot 17\,s^2 \quad\text{and}\quad 10\log_{10}\left\{e^{\frac{1}{2}s^2}+\frac{1269\sqrt{N}}{25}\,q\right\}$$

This is how the 'χ-setting scoring charts' were constructed. The tables required for all types of runs are of the form

$$10\log_{10}\left\{e^{\frac{1}{2}s^2} + \text{constant}\right\}$$

Discussion of the subject may be found in R2 pp.7,27,30 and R5 pp.66,73,74, 83,89.

23X THEORY OF COALESCENCE (R4 pp.83-85)

Suppose that we know the settings of χ_2, μ_{61}, μ_{37} for a particular message on $\bar{\chi}_2+\bar{\Psi}_1'$ limitation. Consider two different hypotheses about the Ψ_1 setting at a particular letter of the message. If these two Ψ_1 settings differ by s (s = 2,3,...) it is a reasonable approximation to suppose that at the next BM dot there is a chance $\frac{1}{2}$ that they will remain s apart, a chance $\frac{1}{4}$ that they will become (s +1) apart and a chance $\frac{1}{4}$ that they will become (s -1) apart. The probabilities in the case of s =0 and 1 (when the streams can even cross over) are more complicated. It is worth making the assumption that for s = 1 the probabilities are the same as for $s > 1$ and that coalescence is complete if s=0. These assumptions simplify the problem and are unlikely to produce any serious error.

We now ask "What is the probability that a setting S which is s positions behind a setting T, of Ψ_1, will have coalesced with it after m BM dots?" The question can be tied up with a problem which was stated by Lagrange. (See Uspensky "Mathematical Theory of Probability", ch8 pp. 154,158).

"Players A and B agree to play not more than n games, the probabilities of winning being p and q respectively. Assuming that the fortunes of A and B amount to a and b single stakes, find the probability for A to be ruined in the course of n games.

"The chance of A being ruined is

$$\frac{q^a(p^b-q^b)}{p^{a+b}-q^{a+b}}$$

$$-\frac{(2\sqrt{pq})^{n+1}(qp^{-1})^{\frac{1}{2}a}}{a+b}\cdot\sum_{r=1}^{a+b-1}\frac{\sin\frac{\pi r}{a+b}}{1-2\sqrt{pq}\cos\frac{\pi r}{a+b}}\sin\frac{\pi ar}{a+b}\left(\cos\frac{\pi r}{a+b}\right)^n$$

The first term should be replaced by $\frac{b}{a+b}$ if $p=q=\frac{1}{2}$."

If we imagine two games played corresponding to every motor dot and equate a difference of 1 in the Ψ_1 setting to two units of the stake we can apply Lagranges result with $n=2m$, $p=q=\frac{1}{2}$ and $a=2s$, $a+b=2\times 43=86$. We see then that the chance that a particular Ψ_1 setting will have caught up with the setting s places ahead on the Ψ_1 wheel, after m BM dots is (if $t=s/43$),

$$1-t-\frac{1}{86}\sum_{r=1}^{85}\cot\frac{\pi r}{172}\sin\pi tr\left(\cos\frac{\pi r}{86}\right)^{2m}$$

$$\doteq 1-t-\frac{2}{\pi}e^{-\frac{m}{750}}\sin\pi t$$

If $m>500$ the error involved here is very small. Thus the probability that the correct setting will have coalesced with a proportion t of the Ψ_1 settings following it, or else a proportion $1-t$ behind it is

$$1-\frac{2}{\pi}e^{-\frac{m}{750}}\left(\sin\pi t+\sin\pi\,\overline{1-t}\right),$$

so the chance of not doing this is

$$\frac{4}{\pi}e^{-\frac{m}{750}}\sin\pi t$$

If m is at all large this probability is surprisingly insensitive to the size of t. Our result can be stated in the crude form:

<u>The chance that the right setting will not have collected a high proportion of the Ψ_1 wheel, after m BM dots is roughly $1{\cdot}3\,e^{-m/750}$.</u>

For a more elementary and less rigorous approach to the problem of coalescence see R4,102. There is an interesting exposition in terms of Quantum Theory methods in R5,71

23Z HISTORY OF MACHINE SETTING

The original machine methods of setting were naturally the same as the hand statistical method (see ch44). That is to say the χ runs were of the form $i+j/$.

The motor runs were all of the form motor = . given $\Delta D = /$. The Ψ runs were of the form $P_i + P_j = \cdot$, using a contracted de-chi (see part 4).

The statistics for all this were at first very scanty. Consider for example the surprise expressed in RO.25 at the failure of a 1+3/ run.(See also RO,72).

When the χ_2 limitation was introduced it was seen that this was no serious matter and the B.I.'s involving χ_2 were done making use of the limitation by having $\bar{\chi}_3$ put in the third impulse of the $\chi_{1,2}$ tape.

After this it was realised that /'s in ΔD were a good thing to look for, so that χ_4 and χ_5, for example, could be set by the long run 45/123, instead of 4+5, 5+2 etc. This was done by a de-chi of the first three impulses only (RO,1). Anti-repeats in D were suggested too, as being due to /'s in ΔP at motor crosses. It was only later realised that anti-repeats in P were quite likely to be good (RO,44,45).

The idea of making simultaneous use of repeats and anti-repeats occurred first in connection with motor setting (RO,77).

The run repeats or anti-repeats was an example of the value of being able to use the same electrical impulse more than once. This facility was advocated first in RO,41. At the same time the 'and/or' machine was advocated. The fact that 'not' can be used as a method of saying 'or' was implied in RO,23. All this can be regarded as the germ of the idea of the Colossus switchboard. Other suggestions for machine improvements that were suggested in those days but which were adopted only in the sense ~~that they had~~ some slight influence on future methods were

(i) Possible use of Δ^2 properties for χ-setting (August,1943).

(ii) Decibanning machine (RO,43)

(iii) Square-summing method for using heterogeneity (RO,29).

The tendency to think in terms of repeats instead of in terms of the 32 letter count of ΔD is the origin of the use of the symbol r to denote the 'number of places looked at'. r at first was always a number of repeats. This attitude was changed overnight by a single ΔP letter count that was

done in connection with a motor rectangle (RO,45,48). Effects of this were
(i) General method of setting motor (instead of by using strokes) and calculation of expected score in case of χ_2 limitation (RO,47-49).
(ii) Tendency to use ΔP statistics for finding the best runs (e.g. RO,103,105). But when we had set enough messages we felt that ΔD letter counts of messages set by us would not be misleading for run statistics (Dec.1943).

Other lessons learnt at the time of Heath Robinson setting were
(i) The importance of checks at every stage, including two makes, hand checks and exact numerical checks.
(ii) Ability of Wrens to compute and use simple formulae for set totals etc.
(iii) Possibility of good slides on $\Delta\chi$'s.
(iv) Value of having sprocket guide near lamp on a Robinson to minimise the effect of the sprockets of two tapes not matching exactly.
(v) Importance of careful labelling of all work and of pigeon holes for tapes. (Tapes were originally hung up on hot water pipes.)
(vi) Value of using Bayes' theorem rather than orthodox statistical outlook.
(vii) 'Dottery' method for setting Ψ's.
(viii) Use of Δ wheel tape to save plugging.

When the first 'Robinson' arrived we had not yet adopted the method of checking the result of every run before accepting it. This was done by using various standard lengths of tape. For example the 1+2 run was usually done with tape length of 3814, even if this meant putting in a thousand blanks. The object was first to make the Robinson 'readings' equal to the settings, and second so that the tape could have one letter removed and then be used for checking the result of the run. This idea of using a message tape of length a multiple of a wheel length was first devised for Heath Robinson and enabled Robinson de-chis to be done. The method really came into its own with the double Robinsons which could take four tapes. It then became possible to set all five χ's without ever making a de-chi tape. For example, when setting χ_3 given the setting of χ's 1,2,4,5, a message tape of length 3813 was used with a $\Delta\chi_{12}$ tape and a special $\Delta\chi_{45}$ tape of length 3813 (and therefore non-periodic). It was necessary to have four distinct types of $\Delta\chi_{45}$ tape(R1,58).

In the Robinson period a large variety of new setting runs were discovered and routines were improved to a point at which not many mistakes were made. However when Colossus 1 arrived it was found that it could cope with more material than all the three Robinsons then operating. This applied to wheel-breaking as well as setting.

For the history of setting in the Colossus period the reader is referred to the references in the earlier part of the chapter and to the index of the Research logs.

In conclusion we give a list of some difficulties that occurred in the early days, particularly in the Heath Robinson period:-

(1) Sprockets tearing and stretching.

(2) Tapes breaking and coming unstuck.

(3) Failure of experiments with oiled tape.

(4) Incorrect setting up of wheel settings and wheel patterns on Tunny.

(5) Blurred figures on Robinson printer and running out of printing ink.

(6) Putting tape on Robinson back to front.

(7) Inaccurate punching of start and stop signals - high standards required by Heath Robinson.

(8) Incorrect setting of repeat dials.

(9) Difficulty in calculation of wheel settings from readings, especially motor settings.

(10) Incorrect setting of χ_1 when contracting a tape on Tunny.

(11) Mysteriously long time taken for production of de-χ tapes and contractions.

(12) Prevalence of transient faults on machines which were therefore difficult to diagnose.

(13) Badly written figures and figures incorrectly written down.

(14) Runs not checking with de-χ tape and other mysteries.

(15) Insufficient handing over from one shift to the next.

(16) Print-outs with letters erroneously inserted or omitted by the machine.

(17) Habit of guessing the average from readings in the run, instead of calculating it in advance.

(18) Using even length of tape for runs unvolving χ_4.

(19) Inaccurate counting by Heath Robinson.

(20) Damaging tapes by maltreatment.

(21) Numerous slides in tapes provided at that time by Knockholt.

(22) Presumed certainty of 4σ on a long run.

(23) Running out of benzene, squared paper, and method of obtaining benzene, paint brushes and rubbers from local sources.

(24) Difficulty of getting supplied with the small machines like hand counters and stickers.

(25) Setting tape in wrong place (on any machine). Forgetting χ_2 lim for Tunny contraction. Forgetting to reset a tape when restarting a job.

(26) Sickness due to intolerable working conditions.

(27) Knockholt perforating the wrong tapes (e.g. R.O. 95).

(28) Mechanical relays developing 'pips'.

(29) Over emphasis on (necessarily meagre) operational results at the expense of research work.

Suffice it to say that most of these difficulties and troubles were eventually almost entirely eliminated.

GHB 9904 WD 29/3 COL 3 Page 2

FIG 23 (I)

EXAMPLE OF MOTOR AND PSI RUNS SHOWING COALESCENCE.

SETTINGS on 29 th wheels
k1 k2 k3 k4 k5
2o o1 12 12 18

Motor run
///
r 183 a 199 eb 26 ea165 & 3.8 at 156
k1rk
?m1 m2
2o o3 b o156
32 o3 b o156
37 o4 e o156
38 o4 e o156
39 o4 e o156
43 o4 o o160
44 o4 o o163
45 o4 o o162
46 o4 o o156
31 o9 e o160
32 o9 e o161
33 o8 d o15
36 o8 d o157
37 o8 d o157
38 o8 d o157
39 o8 d o157
41 o8 d o15
42 o8 d o163
43 o8 d o16
44 o8 d o170
45 o8 d o167
46 o8 d o160
48 o8 d o156
49 o8 d o156
53 o9 e o158
54 o9 e o160
55 o9 e o161
56 o8 d o157
o2 13 d o156
o3 13 d o157
31 13 d o161
42 16 a o162
42 12 e o162
43 16 a o171
43 12 e o16
44 16 a o172
~~44 12 e o16~~
45 16 a o168
45 12 e o165
53 13 d o160
54 13 d o161
55 13 d o160
43 2o b o162
44 2o b o163
53 17 e o160
54 17 e o162
43 28 d o162

The χ's have already been set.

The motor run is BM = . / ΔD = /

The S1 (typewriterese for Ψ_1) run is the Ψ_1 motor run TM = . / ΔD = /

It will be seen that the basic motor run was insufficiently powerful to produce the best score at the correct setting; but that the scores on the Ψ_1 motor run make it obvious that the second highest BM score is at the correct setting.

One effect of coalescence is that settings 26,31,36 for Ψ_1 all score alike.

set m1 44 m2 16
m 3 \

s1 run

s1
o1 a oo97
o6 a oo88
11 a oo86
16 a oo86
21 a o1o1
26 a oo93
31 a oo93
36 a oo93
41 a oo93
o1 a oo93

set m1 43 m2 16

s1
s1
o1 a o1o1
o6 a o1o2
11 a o1o3
16 a o1o1
21 a o123
26 a o137
31 a o137
36 a o137
41 a oo99

FIG 23(I) (continued)

```
set s1 26      1▇    2    3x    4  5
r2281      s   11 40      & 24     st 1215
s2 s3 s4 s5
      o1        d 1226
o2              b 1230
      o3        d 1232
12              b 1244
14              b 1279
   14           c 1265
   16           c 1268
19              b 1268
         19     c 1346        s5
21              b 1257
      26        d 1251
28              b 1249
      28        d 122
   29           c 1313
   31           c 1456      s3
33              b 1306
   33           c 1293
      41        d 1383      s4
   44           c 1236
45              b 1292
   46           c 1308
47              b 1518     s2
```

```
k1 k2 k3 k4 k5 s1 s2 s3 s4 s5 m1 m2
20 o1 12 12 18 26 47 31 41 19 43 16
```

///333444 1o

psis 1o back
step ///333444

```
s1 s2 s3 s4 s5
30 o4 35 45 23   s 0008
31 o5 36 46 24   s 0004
35 o9 4o 5o 28   s 0002
36 1o 41 51 29   s 0004
37 11 42 52 30   s 0002
```

on 1st 2oo

```
s1 s2 s3 s4 s5
31 o5 36 46 24   s 0002
35 o9 4o 5o 28   s 0000
36 1o 41 51 29   s 0002
37 11 42 52 30   s 0000
```

```
k1 k2 k3 k4 k5 s1 s2 s3 s4 s5 m1 m2
20 o1 12 12 18 35 o9 4o 5o 28 43 16
```

Ψ_1 is set provisionally at 26,(later found to be incorrect) but coalescence enables the other Ψ settings to be found easily using 2.3 x 4.5., the weakest setting having an 8.6 bulge.

The 'Ψ's are set back and stepped together looking for the least number of /'s,3's and 4's. Settings 35,37 both yielf only 2 (the provisional setting yields 10) and neither yields any /,3,or 4 in the first 200 letters of text.

A decode at each of these settings shows that 37 is correct, and that setting 35 coalesces with it at the tenth letter.

SETTINGS

```
k1 k2 k3 k4 k5 s1 s2 s3 s4 s5 m1 m2
20 o1 12 12 18 35 o9 4o 5o 28 43 16
```

///333444   0000 on 1st 2oo

DECODE from o1

gnoqakqste9kmaben9

```
k1 k2 k3 k4 k5 s1 s2 s3 s4 s5 m1 m2
20 o1 12 12 18 37 11 42 52 30 43 16
```

///333444 0000 on 1st 2oo

DECODE from o1

9fuehrerote9kmaben99vv9899ar9b

[illegible]

24 - RECTANGLING

24A Introdu...

24B Making and entering rectangles

24C Crude convergence

24D Starts for converging rectangles

24E Rectangle significance tests

24F Conditional rectangle

24G Some generalised rectangles

24W Theory of convergence

24X Theory of significance tests

24Y Other theory of rectangles

24A INTRODUCTORY

(a) General remarks on Chi-breaking

The ultimate criterion in chi-breaking, as in chi-setting, is the ΔD count.

As in setting, and for like reasons, runs are limited to:

1-wheel runs, known as short wheel-breaking runs;

2-wheel runs known as rectangles.

Even these are impracticable to run by actually trying all possible wheels, involving millions of trials [25X]

Instead methods are used which, in effect, count ΔD against each character supposing it to be a dot: a good count is evidence that it is a dot; a bad count that it is a cross.

This applies equally to short wheel-breaking runs [25A] and to rectangles: a rectangle could be treated as a short wheel-breaking run whose wheel is composite, e.g. in a 1+2 rectangle the "wheel" is $\Delta\chi_1 + \Delta\chi_2$ which is 41 x 31 = 1271 long.

(b) <u>The 1 + 2 rectangle.</u>

It will be convenient to describe a rectangle for two particular wheels. In fact in chi-breaking from cipher the 1 + 2 rectangle was used almost exclusively. (For other rectangles see 24F, 24G).

$\Delta Z_1 + \Delta Z_2 + \Delta\chi_1 + \Delta\chi_2 = \Delta D_1 + \Delta D_2$ which $\rightarrow$.

Thus any place of Z would contribute favourably to the ΔD count if $\Delta\chi_1 + \Delta\chi_2$ had the same sign as $\Delta Z_1 + \Delta Z_2$, which is evidence that it has the same sign as $\Delta Z_1 + \Delta Z_2$ has: the magnitude of this evidence is called a pip.

Consider all the places of the cipher which are opposite the i^{th} character of $\Delta\chi_1$ and the j^{th} character of $\Delta\chi_2$: if there are u of these where $\Delta Z_1 + \Delta Z_2 = \cdot$, and v where $\Delta Z_1 + \Delta Z_2 =$ x the net evidence that $\Delta\chi_1^i + \Delta\chi_2^j$ is a dot is u − v pips.

This score is entered in the i^{th} column and j^{th} row of a 41 x 31 rectangle (+ x as ⊗, − x as x).

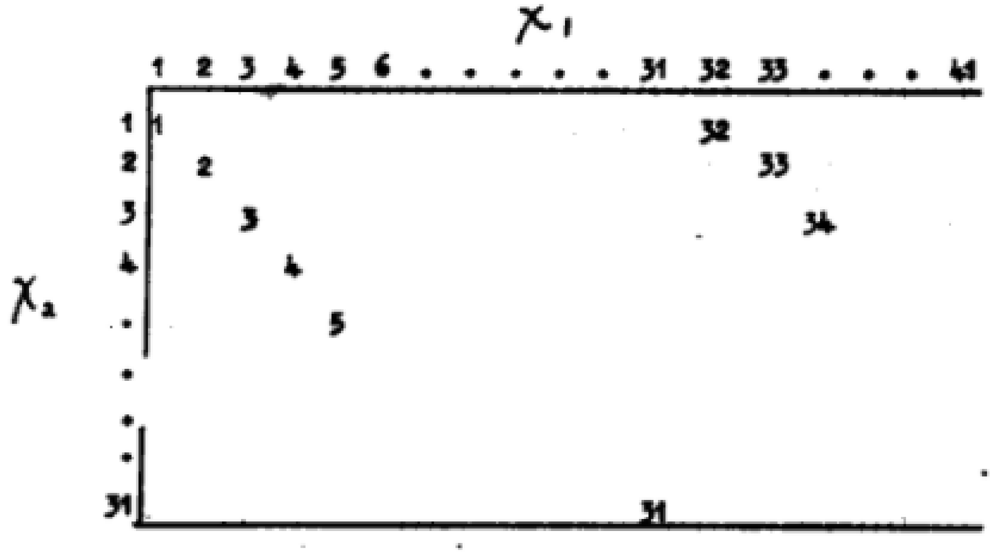
The substance of the foregoing is that the 41 columns of the rectangle correspond to the characters of $\Delta\chi_1$, the 31 rows to the characters of $\Delta\chi_2$. The entry in any cell (i, j) in the excess of contributory places where $\Delta Z_1 + \Delta Z_2 = \cdot$ over places where $\Delta Z_1 + \Delta Z_2 =$ x, and measures the evidence that $\Delta\chi_1 + \Delta\chi_2$ is a dot.

The rectangle so constructed is afterward converged, i.e. wheels $\Delta\chi_1$, $\Delta\chi_2$ are found, to agree as well as possible with the evidence for $\Delta\chi_1 + \Delta\chi_2$.

<u>24B MAKING AND ENTERING RECTANGLES</u>

(a) The entry in each cell of the rectangle is found by determining which places of Z correspond to it, and then taking the excess of such places where $\Delta Z_1 + \Delta Z_2 = \cdot$ over those where $\Delta Z_1 + \Delta Z_2 =$ x.

To find which places correspond to any cell remember that Z and the chis move together. If all the places of Z are numbered successively 1, 2, 3 ..., these will appear in order on the diagonal



The 32nd place will clearly be in the cell (32,1); similarly whenever a side of the rectangle is reached.

The first 1271 places will just fill the rectangle.

Evidently the first cell will contain not only the first place but also the (1271 + 1)th, (2 x 1271 + 1)th, etc. places, and similarly for every cell.

(b) Two methods for entering have been used:

(i) Find the score for all places spaced at interval 1271 beginning with the 1st place of [redacted], then for all places spaced at interval 1271 beginning with the 2nd place of the cipher, and so on; afterwards enter diagonally.

(ii) Look for the scores in the various cells of the rectangle arranged by rows and columns, entering directly in the correct position.

Method (i) was normally used for Garbo, Thurlow and Robinson rectangles.

Method (ii) was used normally for Colossus rectangles.

The mechanical difficulty in method (ii) is the irregular stepping at the end of a row: this was found to make it not worth while except on Colossus, which can step irregularly (5B C (4)) : even Colossus requires a gadget to do this properly (Colossus rectangling gadgets do much more besides); with the gadgets this method is preferred.

Note: prior to the introduction of the gadget, Colossus rectangling used method (i). Method (ii) was attempted on Super-Robinson, but [redacted] (R5 p 81).

(c) <u>Garbo rectangles.</u>

By means of the special switches (54E), Garbo is made to print $\Delta Z_1 + \Delta Z_2$, as . or x, in widths of 41, with plenty of spacing.

After 31 rows, i.e. after 1271 places, a dot or cross will have been printed for each cell of the rectangle. The 1272nd entry is printed immediately below the 1st, the 1273rd below the 2nd, and so on. Finally the scores for a particular cell of the rectangle will be a short column of dots and crosses: the excess of dot over cross for each cell is entered by hand on the Garbage, and afterwards transferred diagonally to a rectangle.

Because Garbo deltas backwards it is necessary to start at the second place of the cipher tape and correct the first entry by hand.

The method is very convenient for short texts, such as key. Its disadvantage is that if the depth, i.e. the number of places per cell, is large, adding the scores for each individual cell is laborious.

In diagonal entering each row of Garbage must obviously end in the last column of the rectangle: to aid and check entering, it is labelled with the row of the rectangle in which it should start, viz., in order, 1, 11, 21, 31, 10, 20, 30, 9, 19, 29, 8, 18, 28, 7, 17, 27, 6, 16, 26, 5, 15, 25, 4, 14, 24, 3, 13, 23, 2, 12, 22. A better plan would be to write (or have printed) Garbage row numbers against the rectangle: this has been done spasmodically for key rectangles.

For the complete system of checks see 36 G.

(d) <u>Thurlow rectangles.</u>

A modification of Garbo rectangles, devised for long texts to reduce the labour in finding the scores for individual cells: the idea is to represent 5 dots and crosses by a single figure.

The first step is to produce a tape on Miles, on which is punched nothing but $Z_1 + Z_2$, as dot or cross, arranged thus

1st	1271	places	2nd	1271	places	3rd	1271	places
4th	.	.	5th	.	.	6th	.	.
7th	.	.	8th	.	.	9th	.	.
10th	.	.	11th	.	.	12th	.	.
13th	.	.	----			----		

Thurlow tapes of the first kind.

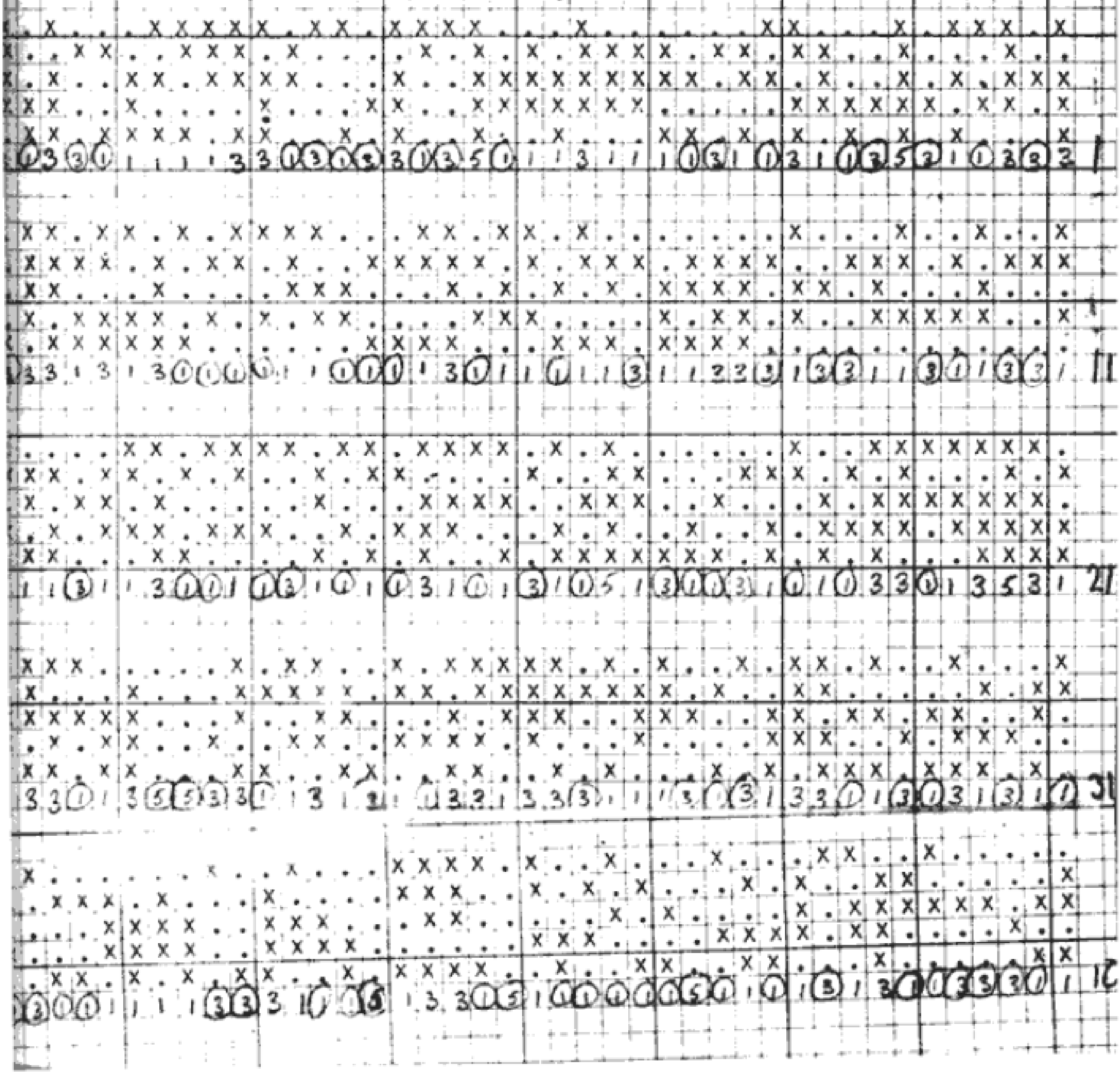
FIG 24 (I) Significant

first nine rows in Gorbo Rectangle

WVB 1514

TEXT: 5314 (1)

Gorbo 1 + 2



1st 1271 places	6th 1271 places	11th 1271 places
2nd " "	7th " "	12th " "
3rd " "	8th " "	13th " "
4th " "	9th " "	----
5th " "	10th " "	----

Thurlow tapes of the second kind.

Such tapes are easily made on Miles: the first character of each batch of 1271 places on the cipher tape is marked. For a Thurlow tape of the second kind 1st, 2nd, 3rd, 4th, 5th marks are placed in the eyes of the 1st, 2nd, 3rd, 4th, 5th transmitters of Miles.

Z_1 and Z_2 from the n^{th} transmitter are added into the n^{th} impulse of the distributor.

When 1271 characters have been punched the machine is stopped, the 2nd mark on the cipher tape will be in the 1st eye, the 3rd in the 2nd eye and so on (if not, something is wrong - a useful check). The 6th, 7th, 8th, 9th, 10th marks are now placed in the 1st, 2nd, 3rd, 4th, 5th eyes, the machine restarted and so on.

The second step is to difference the Thurlow tape just made on Garbo (with normal deltaing, not the special rectangle device) and print out, steckering

/ to 0

all 1 cross letters to 1

" 2 " " " 2

" 3 " " " 3

" 4 " " " 4

" 5 " " " 5

As in an ordinary Garbo rectangle the 32nd row is printed immediately below the 1st and so on.

The entry for a cell is now the depth minus twice the sum of the scores printed. Otherwise the entering is the same as for a Garbo rectangle.

Note: Alternatively, if Miles A is available, a deltaed Thurlow tape can be made: this is printed out without deltaing on Garbo or Junior.

(For Thurlow tapes R4 p.71, Wheel Man's log book II, 103.)

(e) Robinson rectangles.

Two tapes are used, viz.

(i) cipher tape, on bedstead A, tape length one less than a multiple of 1271, with start and stop.

(ii) control tape, on bedstead B, tape length 1271, with a start (for counting position only) and a single "X" in the first place of the tape.

Switch B = "X": this selects those places on A opposite the "X" on B, which are of course spaced at intervals 1271 (the length of B). Moreover in each successive revolution of the cipher tape A, all the places opposite "X" will move one forward (because the length of A is one less than a multiple of 1271), so that the 1271 cells are selected in "diagonal" order.

The score counter is split; one half counts $\Delta Z_1 + \Delta Z_2 = \bullet$ the other $\Delta Z_1 + \Delta Z_2 = x$.

The difference between them is the score for the corresponding cell.

Their sum is the depth, which serves as a check, for there can be only one change of depth.

The position counter is split to repeat after 41, 31. Since the start on A is used, it necessarily records how much A is ahead of B and so runs backwards, 0000, 4030, 3929,...... These figures are written along the sides of the rectangle to check the entering.

As a check on Robinson scores the machine is allowed to run round a few times after the rectangle is finished; it immediately begins to repeat the rectangle.

In fact, the B tape contains also 41 "4"s at intervals 31, which are used analogously for $\hat{\chi}_1$ runs. The first "4" is one place back from the "X": this is merely a trick to make the position counter readings tally with those of a $\hat{\chi}_2$ run on Colossus.

For the details of plugging and switching see Synopsis of Robinson plugging (54 J). It will be noticed that some unnecessary cords are used: this is to minimise changes between 1 + 2 rectangles, $\hat{\chi}_1$, and counting "9"s.

(For early versions see R1, p 32.)

(f) Colossus Rectangling.

Colossus rectangling is the most highly developed method in use.

The necessary rectangle gadgets have been fitted to Colossi 2, 4, 6, 7, 9. Colossus 6 has a bedstead for tapes 26,000 long, and is used almost continuously for rectangling.

The basis of Colossus rectangling is as follows: put one cross in chi 1, one cross in chi 2 and switch the condition $\chi_1 = x$, $\chi_2 = x$: This will select a set of places on the cipher spaced at intervals 1271, i.e. the places in a cell of the rectangle. If these wheels step through all settings, they will select all cells of the rectangle in turn. Chi wheels move backwards when their settings increase, and therefore the rectangle is made backwards. If the wheels were to step uniformly the rectangle would be made backwards diagonally.

On Colossus, however, it is possible to produce the rectangle row by row. Step chi 1 fast, chi 2 slow (i.e. chi 2 steps only when chi 1 reaches the setting plug in χ_1): chi 1 steps and a row of the rectangle is produced; when chi 1 reaches its setting plug, chi 2 steps and another row is produced and so on.

It is impossible to make Colossus rectangling fully intelligible without a detailed account of the operations performed by the machine. For this reason the instructions are given here baldly, the explanation being postponed to 53M.

It may be remarked at once that the "rectangling gadget" modifies the operation of Colossus in many ways. Optionally, if the depth is constant, it can be made to perform the subtraction pippage = 2 × (score of $\Delta Z_{12} =$.) — depth: rectangling which uses this facility is known as "Normal" as opposed to "Print Scores". This reduction of the length to a multiple of 1271 may cause a serious loss of evidence on a short text.

The instructions for a 1 + 2 rectangle are:

Spanning. Span 04 to (04 + 1271 x depth)

Count text.

Chi-patterns. (triggers) Crosses in 02, 02 of χ_1, χ_2: on rectangling Colossi one trigger has this permanently set up.

Selection switches. Q = χ

Q Panel. $\chi_1 = x$ in all counters.

Multiple test impulses R_1, R_2, R_3, R_4, R_5 = x in counters 5, 4, 3, 2, 1

Control Panel Multiple test switch to χ_1

Check depth, i.e. $\chi_1 = x$, $\chi_2 = x$

Rectangle switch to "Normal".

Rectangling gadget Carriage return on χ_1

Switch in appropriate depth.

Plug Panel $\Delta Z_1 + \Delta Z_2 = .$ in all counters.

Settings $\chi_1 = 06$, $\chi_2 = 02$

After setting wheels return plugs to 01,01, without resetting.

Step χ_1 (lower switch down) fast to control χ_2 slow (lower switch up).

Printer Paper of sufficient width, start at extreme left.

Final Checks. Repeat first and last rows.

Unfortunately, although the rectangle is produced in its final form, it was in practice found necessary to transfer it by hand to squared paper in order to converge it, so that the advantages of this method are less than would be supposed.

24C CRUDE CONVERGENCE

(a) The general idea of convergence of a 1+2 rectangle is to find wheels $\Delta\chi_1, \Delta\chi_2$ which agree as well as possible with the entries in the cells of the rectangles.

The interpretation of 'agreeing as well as possible' is not obvious nor is Crude Convergence the only convergence which has been contemplated.

In a sense the evidence would be better represented, not by ordinary wheels of dots and crosses, or say ± 1, but by generalised wheels in which the magnitude of a character is proportional to the evidence in its favour. It would be possible to work in terms of generalized wheels and finally convert into ordinary wheels by taking each character as dot or cross according to its sign. There is some evidence that the particular method known as 'accurate convergence' is more reliable than crude convergence. For references to other proposed methods see 24W.

(b) Crude Convergence The only form of convergence used operationally is crude convergence which uses only ordinary wheels of dots, crosses, and doubts to make the bulge of $\Delta D_{12} = .$ a maximum.

It is not easy to find which $\Delta\chi_1$ and $\Delta\chi_2$ make this bulge a maximum.

It is however, very easy, if one is given, to find the other, viz. by 'taking the known wheel through the rectangle' (details below).

Accordingly the method used is to find somehow a crude approximation (a start) to one wheel, say $\Delta\chi_2$, take it through the rectangle to get $\Delta\chi_1$, take this through to get a new $\Delta\chi_2$ and so on till $\Delta D_{12} = \cdot$ is a maximum. The rectangle is then said to be crudely converged.

Unfortunately this maximum may be only a relative maximum (false convergence) in the sense that though the score cannot be increased by changing either wheel separately, it can be increased by changing both wheels at once [24W(c)] For this reason the most important item in convergence is finding a correct start.

(c) <u>To take a wheel through the rectangle</u> place the given wheel (say $\Delta\chi_1$) against the first row of the rectangle and add all the entries therein, changing their signs wherever $\Delta\chi_1$ is a cross (and counting 0 where $\Delta\chi_1$ is 'doubted'). According to whether this sum is positive or negative, the first character of $\Delta\chi_2$ is taken to be a dot or cross. Likewise for all rows.

It is easy to see why. The rectangle entries are bulges of $\Delta Z_{12} = \cdot$ and if their signs are changed where $\Delta\chi_1 = x$ they become bulges of $\Delta Z_{12} + \Delta\chi_1 = \cdot$, i.e. of $\Delta D_{12} + \Delta\chi_2 = \cdot$ The sum of these for a particular row is the total $\Delta D_{12} + \Delta\chi_2$ bulge against the corresponding character of $\Delta\chi_2$ (the 'score for this character'). By giving each character of $\Delta\chi_2$ the same sign as this bulge, each is made to contribute positively to the bulge of $\Delta D_{12} = \cdot$ With the given $\Delta\chi_1$ and this $\Delta\chi_2$ the ΔD_{12} bulge for the whole rectangle is the sum of the moduli of the scores for $\Delta\chi_2$ characters.

When the rectangle is converged, the bulge is, by definition, a maximum (possibly only relative). If a wheel is taken through again, the score (which will certainly not diminish) must remain constant. In other words the sum of the moduli is the same for $\Delta\chi_1$ and $\Delta\chi_2$. It is easy to see that, conversely, when two consecutive scores are equal, the rectangle is converged. This is a useful check.

It is found better not to take all characters of a wheel when converging, but only those which score reasonably well, say more than 10 pips. The others are 'doubted', i.e. ignored. The start is usually made from very few characters, more being added at each stage: towards the end, the standard of 10 pips may need to be lowered, and finally all characters are taken. While doubting is in use, the score does not necessarily increase at each stage.

Note 1: To take a wheel through write out $\Delta\chi_1$ (say) on a strip of paper which can be placed against each row in turn. It will suffice to include only new or changed characters, the earlier score for $\Delta\chi_2$ being added in.
Note 2: Taking a wheel through is in fact a short wheel-breaking run (25A : R1 pp92, 94) and can be done on Colossus (25A) but computer time is often cheaper than Colossus time.
Note 3: For a suggested automatic converging machine R1 p 91.
Note 4: For the standard in taking characters during convergence R2 pp 9, 11, 15,

24D STARTS FOR CONVERGING RECTANGLES

(a) In the following paragraphs several methods will be described. All have been used operationally: the 9 x 9 flag and "R2" are probably the most popular with computers, who are normally allowed considerable freedom of choice. The skeleton was rather neglected, probably because it is unsuitable for depth 8, at one time the maximum for a Colossus rectangle. (R2 pp 4, 14, 17, 19. R3 p 21. R4 p 23.)

(b) Flagging.

In 24W(a) an "accurate" system of scoring the evidence that two wheels are alike (or opposite) is given. This may be applied to two rows of a rectangle to find whether the corresponding characters of $\Delta\chi_a$ are alike or unlike. The calculation is too long for starting rectangles quickly, but there are two simple approximations

(i) the sum of products of corresponding entries (Scalar product)

(ii) the sum of the smaller of every two corresponding entries, with a positive or negative sign according to whether the two entries are alike or unlike (Jacob flagging).

(i), (ii) are exact in the limiting cases $\delta = 0$, $\delta = 1$ respectively.

Using either method the scores for each pair of rows can be entered in a square, which however is symmetrical, so that half of it suffices. This is the flag.

The score in the cell (i,j) measures the evidence that $\Delta \chi_1^{(i)} + \Delta \chi_1^{(j)}$ is a dot: thus the flag square behaves like a rectangle. In particular it may be converged: a correct convergence should give the same wheel along both sides.

A flag may be tested for significance (R2 p 92. R3 pp 8, 79, 81, 82).

To flag all the 31 scores of the rectangle by hand would take too much time. A special machine is feasible; for the attempted flagging on Miles and Robinson see Appendix 95.

Three abbreviated methods of flagging are described in the ensuing paragraphs (b), (c), (d).

(c) <u>9 x 9 flag</u>.

For each row find the sum of the entries ignoring their signs (sum of moduli).

Take the 9 best rows and flag them (by Scalar products).

There may be an obvious start: if not, converge the flag. To save time divide by 10 and ignore fractions.

Note: If chi 2 lim is expected, flagging is applied, not to 9 rows, but to 11 columns.

(d) <u>Skeleton</u>. (See R2 p 4.)

Make a skeleton of the rectangle; if, for example, the depth is 7 this means: take sums of ± 7 as ± 2, ± 5 and ± 3 as ± 1, ± 1 as 0. This reduces the arithmetic substantially: it is practicable to flag many more rows.

Note: These are written in the rectangle as dots and crosses with 2 entries in a cell for ± 7.

A skeleton is unsatisfactory if the depth is even, e.g. if it is 6 the possible sums are ± 6, ± 4, ± 2, 0, which cannot effectively be simplified without taking ± 2 as 0, and this throws away too much evidence.

(e) <u>E 2</u>. (R2 p 82, R3 p 74, R4 pp 4, 20.)

Select the five best rows, as for 9 x 9 flag: A, B, C, D, E.

In A take all scores above the standard (see below) to form a rudimentary $\Delta\chi_1$ wheel.

Take this through the rectangle, getting $\Delta\chi_2 A$, similarly $\Delta\chi_2 B$, $\Delta\chi_2 C$, $\Delta\chi_2 D$, $\Delta\chi_2 E$, each a column of scores, not merely dots and crosses.

Make a flag of these five $\Delta\chi_2$'s by Jacob's method.

Choose 2, 3, 4 or 5 of these, and, with the appropriate ± signs add them. The high scoring characters can be used as a start.

Depth	4–6	6–8	8–10	10–12	12–14	14–16
Standard	4	5	6	7	8	9

(f) <u>Restarts.</u>

At the end of a convergence the characters used in the start are liable to score unduly well; but even if the start is a poor one, some of the characters for which the rectangle really does provide strong evidence should also score well (R3 p 16.). If high scoring characters which appeared late in the convergence are taken as a new start, a better convergence may be obtained. (R2 p 101, R3 p 98.)

(g) <u>E 1</u>.

An elaborate variation on restarts is E 1 for which the instructions are:-

Make a start by eye

Purge

Take 5 characters as a new start

Purge again

Each purge involves the following:-

Suppose the eye-start is $\Delta\chi_2\alpha$ of 3 to 5 characters. Take $\Delta\chi_2\alpha$ through the rectangle getting $\Delta\chi_1 A$ of 6–10 characters. Take $\Delta\chi_1 A$ through the rectangle getting $\Delta\chi_2\beta$ of 8 – 12 characters, in choosing which, reduce the score of any character which was in $\Delta\chi_2\alpha$ by one-third. Take $\Delta\chi_2\beta$ through the rectangle getting $\Delta\chi_1 B$ of 5 – 10 characters, excluding all characters which were in $\Delta\chi_1 A$. (R4 p 3; for random starts R1 p 93.)

24E RECTANGLE SIGNIFICANCE TESTS

(a) In view of the account given in 24X this deals only with tests in practical use.

It is perhaps desirable to stress the distinction between tests for rectangles not converged, i.e. treating the rectangle simply as a run for a wheel 1271 long; and tests for converged rectangles, i.e. using the additional knowledge that the 1271 cells of the rectangle are derived from two wheels 41 and 31 long. The latter are naturally more powerful.

Essentially only one test of each type used operationally; this excludes tests which involve the use of additional evidence.

For rectangles not converged: the square-summing test, or its equivalent the Δ1271 test.

For converged rectangles: Significance Test IV and several simple approximations to it.

(b) Test for rectangle not converged.

If θ_{ij} is the entry in a cell of a 1 + 2 rectangle of length N and depth k (so that N = 1271k) the random value of $\sum_{1}^{1271}\theta_{ij}^2$ is N and its variance is

$$2N(k-1) \qquad (24X(4))$$

$\sum \theta_{ij}^2$ is evaluated when making a rectangle on Colossus, by means of a series of cyclometers which record the number, $n(\theta)$, of occurrences of each possible score. Then $\sum \theta_{ij}^2 = \sum \theta^2 n(\theta)$: the calculation is made foolproof by means of a printed form.

The analogous hand process is possible for a non-Colossus rectangle.

The test is not ordinarily a very powerful one (24), but the following statistics are of some interest

Depth		3	4	5	6	7	8	9	10	11	12	13	14	15	16
Significant Rectangles	Number	8	30	9	12	9	4	1	3	1	2	3	1	-	-
	Average sigma-ages.	2·13	1·54	1·63	1·93	2·3	1·55	1·8	1·85	3·5	2·62	3·3	3·4	-	-
Abandoned Rectangles	Average sigma-ages.	·14	·58	·51	·55	·19	1·13	·15	1·23	1·06	·45	·58	·07	·89	·83
	Number	41	295	88	112	18	28	11	8	9	2	7	5	8	1

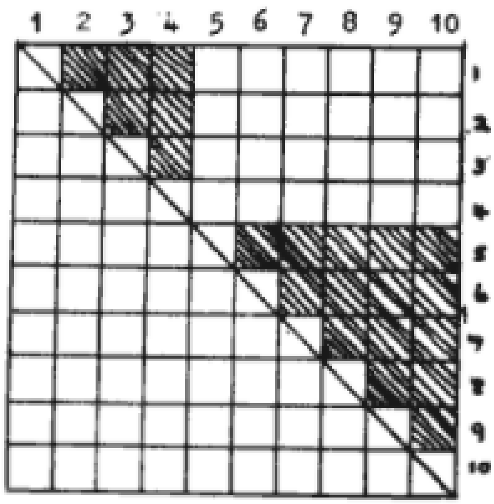
(R1 pp 32, 34, 38. R3 pp 37, 77.)

(c) Δ1271 Test

Since $\Delta_{1271}\,\Delta Z_{12} = \Delta_{1271}\,(\Delta D_{12} + \Delta\chi_{12}) = \Delta_{1271}\Delta D_{12}\,\overrightarrow{\frac{1+\xi^2}{2}}$.
a count of $\Delta_{1271}\,\Delta Z_{12} =$. is a possible test. It is strengthened if differencing at every multiple of 1271 is included, when it becomes equivalent to the $\sum \theta_{ij}^2$ test (24X(b) of R2 p 102), for which reason it was discontinued when the cyclometers came into use.

It is however more easily adaptable to the detection of slides. A (half) square is made in which the entry in the cell (m,n) is the number of agreements between the mth and nth stretches of 1271 in ΔZ_{12}. Two stretches in the correct relative positions will show a bulge: two between which there is a slide will show no bulge.

In the example depicted there is a slide between the fourth and fifth stretches of 1271 letters. Only the entries in the shaded positions show a bulge. If the slide is near the middle of the fifth stretch, the entries in the fifth row will also show no bulge.



In fact the expected bulge in a single cell is only about $\frac{1}{2}\sigma$, so that long texts are required: the method is not in current use.

The counts can easily be made on Robinson using a cipher tape or any kind of Thurlow Tape. Two copies are required; if their lengths are consecutive multiples of 1271, the whole test can be made very quickly without stopping the machine.

If a slide is suspected, it may be investigated by similar runs with an artificial slide between stretches from different parts.
(See R3 pp 77,82,92. R4 pp 71,82,122.)

(d) Significance test for converged rectangles.

The standard test for a 1+2 rectangle is

$$2\cdot 17\frac{x^2}{N} + \sum \rho^2\left(\frac{2y_i(x_i-k)}{N}\right) - 2\cdot 19 > 0 \;;$$

the left hand side being the decibanage in favour of significance, where x_i is the modulus of the score of a character and Σ is extended over both wheels, $f(u) \equiv 10 \log_{10}(1 + e^{-u})$ and is tabulated, k is controversial (see 24X (e))

For other rectangles 219 should be replaced by $3.01(w_1 + w_2 - 1) + 5$, where w_1, w_2 are the two wheel lengths.

The formula is believed to provide a normally reliable condition for the essential correctness of the rectangle wheels. Ordinarily, though not always on all links, this implies that wheel-breaking can be completed, though it cannot be guaranteed, for it depends on supporting messages and on ΔP characteristics in impulses not used for the rectangle.

The formula has been criticised because Σf is tedious to calculate and varies but little. Approximations have been suggested

$\sum f = \frac{2.4 \times 10^{11}}{x^3} \pm 3.6$ (for messages 10168 long: R3 p5).

$\sum f = 23$ i.e. $\frac{x_i}{\sqrt{N}} > 9.5$ (based on a perverseattitude to decibans:R4 pp111,115)

$\sum f = 2 + \frac{217,000}{N} - \frac{54,350,000}{N^2}$ i.e. $\frac{x_i}{\sqrt{N}} > 10(1 - \frac{5000}{N})$

(Too optimistic for small N: used by the computers).

An empirical formula for Σf as a function of N in a marginally significant rectangle would have been preferable.

In practice everyone assumes that Σf is about 20-30, being greater for short messages and that if $2.17 \frac{x^2}{N}$, the LEADING TERM, is more than 200 or much less than 180 it is unnecessary to calculate the f terms. (see R2 p.15, R4 pp 40,111,117).

24F CONDITIONAL RECTANGLE

This means a rectangle in which scores are counted only at places of Z where some fixed condition is satisfied.

e.g. in a cell of the 3+4x/1x2x rectangles the entry is

(the number of places where $\Delta Z_3 + \Delta Z_4 = x, \Delta D_1 = x, \Delta D_2 = x$) minus

(the number of places where $\Delta Z_3 + \Delta Z_4 = \cdot, \Delta D_1 = x, \Delta D_2 = x$).

The convergence is identical with that of an ordinary rectangle.

Almost the only conditional rectangles used are 3+4x/1x2x, 4+5/1+2, 4+5/1x2x (see next section 24G)

Because the number of places where ΔD_1 = x, ΔD_2 = x varies from call to call (and in addition $\Delta\chi_1$, $\Delta\chi_2$ may be 'doubted') the depth cannot be made constant, so that even if Colossus is used 3 + 4 x / 1 x 2 x and 3 & 4 • / 1 x 2 x must be printed separately, preferably in alternate lines and distinctive colours, and the differences found by hand. Although the other methods can be applied Colossus preferred because it avoids auxiliary tapes.

<u>Colossus switching</u>. (c.f. 1+2 rectangle)

Count text, and check 1+2 = .

<u>Chi-patterns</u> (triggers) Cross in 02, 02 of χ_3, χ_4 .

$\Delta\chi_1$, $\Delta\chi_2$ in χ_1 , χ_2 triggers

Doubts in special patterns χ_1 , χ_2 triggers.

Plugging (everything plugged goes to all counters)

Special pattern χ_1 = . } It is improbable that there will
Special pattern χ_2 = . } be no doubting.

Check effective text

$\Delta Z_1 + \chi_1$ = x

$\Delta Z_2 + \chi_2$ = x

Check "R"

$\Delta Z_3 + \Delta Z_4$ = x.

<u>Selection switches</u> Q = χ

Q Panel χ_3 = x in all counters

Multiple test impulses R_1 R_2 R_3 R_4 R_5 into counters 5, 4, 3, 2, 1, respectively

<u>Control panel</u> Multiple test switch to χ_4

Rectangle switch to "Print Scores"

<u>Rectangling gadget</u> Carriage return on χ_4

Do <u>not</u> switch a depth

<u>Settings</u> χ_1 = 41, χ_2 = 31, χ_3 = 02, χ_4 = 02

After setting wheels replace χ_3, χ_4 plugs in 01, 01, <u>without resetting</u>

<u>Step</u> χ_4 fast (lower switch down) to control χ_3 (lower switch up)

<u>Printer</u> Triple line feed

<u>Final checks</u> Repeat first and last rows

<u>Re-run</u> with ΔZ_3 + ΔZ_4 = . instead of x

(For an attempt to avoid the separate printing of x and . see R3 p 11.)

24G SOME GENERALISED RECTANGLES

In order that the entry in each cell of a rectangle shall be a single number only a single condition can be imposed on the two impulses involved. The condition must therefore be of the form i + j /(known ΔD) = $\frac{x}{\cdot}$, with or without fixed conditions.

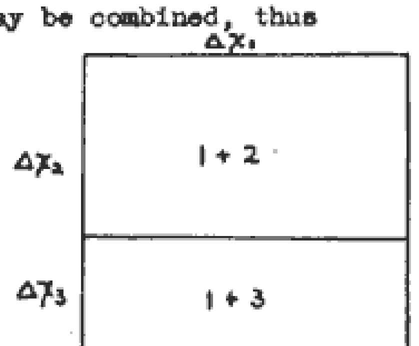
Among the plain i + j rectangles 4+5, 2+5, 1+3, 3+4x, 2+4 have all been tried: indeed at one time it was erroneously supposed that 4+5 would be better than 1+2 (see 24Y (a)).

A peculiar class of i + j rectangle is that of i + 6 rectangles in which each entry is the score for $\Delta Z_i + \Delta Z_6 = \cdot$ i.e. $\Delta Z_i = \cdot$, entered in a 31 x w_i rectangle. In particular if i = 2 all entries lie on the principal diagonal and the rectangle degenerates into ρ_2 .

A rectangle which makes full use of the run 4 = 5/1 = 2 requires 4 entries (3 independent) in each cell (cf. 25C(e) R1 p 62)

Several members of the section have contemplated "Rectangular parallelepipeds": probably the most favourable is i + j + 6/, ΔZ_6 being always dot.

Rectangles may be combined, thus



but in practice this is done only for key (24C) because in cipher, pips in different rectangles are of unequal value.

(For Motor Rectangles see Appendix 92)

24W THEORY OF CONVERGENCE

(a) Elementary properties of the convergence of a rectangle.

Let the length of message be N.

Let the entry in the cell which is the i^{th} row and j^{th} column be θ_{ij} .

If some value of δ is assumed then the odds that $\Delta\chi_{12}$ = dot in all (i,j) are $\zeta^{\theta_{ij}}$ where $\zeta = \frac{1+\delta}{1-\delta}$.
This is a trivial consequence of Bayes' theorem, if the message is assumed to contain no slide (see R3, p 130). Another way of stating the result is that the hypothesis $\Delta\chi_{12}$ = dot is θ_{ij} pips up, where a pip is $10\log_{10}\zeta$ decibans. This enables one to regard the rectangle as an array of 1271 pieces of probability information, arranged in a convenient form for attempting to find the $\Delta\chi_1$ and $\Delta\chi_2$ patterns. We now give a description of methods used for doing this.

A partial wheel pattern can be regarded as a sequence of numbers, ϵ_1 , ϵ_2 ,... each equal to ± 1 or 0, where + 1 stands for a dot and -1 for a cross and 0 for a doubt. The process of taking the pattern through the rectangle consists in forming scalar products

$$y_i = \sum_i \theta_{ij}\epsilon_i$$

The numbers y_i are then called the scores in pips of the characters of the other wheel.

In the original form of convergence one would take $\epsilon_{j'} = \operatorname{sgn} y_j$,
i.e. $\epsilon_{j'} = +1$ if $y_j > 0$
$\epsilon_{j'} = -1$ if $y_j < 0$
$\epsilon_{j'} = 0$ if $y_j = 0$
and take this wheel pattern back through the rectangles giving pippages

$$x_i = \sum \theta_{ij}\epsilon_{j'}$$

The resulting pattern is then taken back in a similar way, giving new values for y_i and so on until the pattern on one side of the rectangle is the same twice running. The rectangle is then said to be converged (crudely). The result of the convergence may depend on the particular pattern with which the convergence is started. The sum of the moduli of the scores of one wheel is called I, $I = \sum|x_i|$. This score is independent of which of the two wheels is used, when the convergence is completed, for

$$I = \sum_I \epsilon_i x_i = \sum_{ij} \epsilon_i \theta_{ij} \epsilon_{j'}$$

and this is symmetrical with respect to the two wheels. If the message were de-chied with the wheels consisting of the final patterns then X = the double bulge of the 1p2 score (provided that places where the differenced wheels are doubted are not included in the count).

The formula $X = \sum_{ij} \epsilon_i \theta_{ij} \epsilon_j'$

is true at all stages of the convergence and the effect on the wheel patterns of the progress of convergence is the same as first choosing the numbers $\epsilon_1', \epsilon_2' \cdots$ so as to maximise $\sum \epsilon_i \theta_{ij} \epsilon_j'$ (leaving $\epsilon_1, \epsilon_2, \cdots$ unchanged) and then changing $\epsilon_1, \epsilon_2, \cdots$ so as to maximise X (leaving ϵ_1', ϵ_2' unchanged) and so on. Clearly X must keep on becoming larger and larger until it reaches a maximum value, when the rectangle is converged.

If the phrase ' crude convergence ' is interpreted in a more up to date sense, in which characters may be doubted if their scores in pips are low (or on grounds of unfavourable wheel characteristics), then it is no longer essential that X should continually grow (see R2 pp 9,11). However it was always the practice to complete the convergence (i.e. to get complete patterns) in order to get a check on the sum of the moduli of the pippages of the two wheels.

The mathematical description given above applies to the hand process of crude convergence and to the Colossus process of convergence of a rectangle. The two processes are of course equivalent.

The reason for the adjective 'crude' is that there is another method called 'accurate convergence', in which

$$y^i = \sum_i f(\theta_{ij}, x_i)$$
$$x_i = \sum_j f(\theta_{ij}, y^i)$$

where $f(k,l)$ is a symmetrical function of k and l. It will be seen that the exact magnitude of the pippages of the wheel taken through are used, instead of their sign. The function $f(k,l)$ is defined as

$$f(k,l) = \log_{\zeta}\left(\frac{\zeta^{k+l}+1}{\zeta^k+\zeta^l}\right)$$

where $\zeta = \frac{1+\xi}{1-\xi}$

and (see R1 pp 37, 43, 45, 49) a conventional value of ξ is assumed. A table of $f(k,l)$ can be conveniently constructed by means of a specially made cardboard slide-rule, in view of the identity $\phi(k)+\phi(l) = \phi[f(k,l)]$ where $\phi(k) = \log\frac{\zeta^k+1}{\zeta^k-1}$.

It is found that the entries in the table are not sensitive to the exact value of ζ assumed. (R1 p 49, R2 p 1)

The sense in which this type of convergence is accurate is that if the x_i's are a correct measure of the odds of the characters of one wheel (measured in 'pips' of $10\log_{10}\zeta$ decibans each), then the formula gives the odds of the characters of the other wheel accurately, if the numbers θ_{ij} are regarded as evidence which is independent of the x_i's. Clearly the last assumption is not really accurate, but this does not prevent accurate convergence from being theoretically more satisfactory than crude convergence. In fact crude convergence is the limiting case of accurate scoring when $\zeta \to \infty$, if the pippages of the characters of the wheel taken through exceed those in the cells of the rectangle.

The precise interpretation of the pippages of the characters of a wheel, as the result of a crude convergence is that they are proportioned to the decibanages assuming the pattern of the other wheel to be certain. In practice the relationship between the pippages and the true decibanage (assuming the patterns to be substantially correct) is not linear (see R3 p 132).

When a message contains a lot of 9's (representing letters missed) there is a modification that can be made to crude convergence. The modification was given in R4 p 39, but it was seldom used.

(b) Proof of accurate scoring formula.

The formula for accurate scoring is of exactly the same form as that for 'scoring one column of the rectangle against another'. Given two columns of the rectangle we may be interested in the question of whether the two corresponding characters of the wheel are the same or different. Let us suppose that the pippages of the two columns are respectively

$$\theta_1, \theta_2 \ldots$$

$$\theta_1', \theta_2' \ldots$$

Then the factor in favour of the two columns being the same (i.e. the two corresponding characters of the wheel being the same) is

$$\prod_i f_o(\theta_i, \theta_i')$$

where $f_o(\theta_i, \theta_i')$ is the factor accruing from one pair of corresponding cells. Let us then consider the following problem: Given two characters where odds of being dots are $\zeta^{\theta}, \zeta^{\theta'}$, what are the odds ζ^{π} that the two characters are the same? The proportional bulge corresponding to odds ζ^{θ} is $\frac{\zeta^{\theta}-1}{\zeta^{\theta}+1}$

Therefore, by the theorem of the chain of witnesses,

$$\frac{\zeta^{\pi}-1}{\zeta^{\pi}+1} = \frac{\zeta^{\theta}-1}{\zeta^{\theta}+1} \cdot \frac{\zeta^{\theta'}-1}{\zeta^{\theta'}+1}$$

and this gives the relation between π, θ, θ' in the slide-rule form.

(c) <u>Wrong convergences of a rectangle and methods of starting</u>.

A rigorous solution of the problem of the number of different crude convergences of a (1+2) rectangle seems to be very hard to find. However, two quite distinct attempts to solve the problem have been made. The first one (R1 pp 56, 57) tends to show that there are not more than 31 possible convergences.* The second one (R2 p 10, etc.) shows that for a rectangle of length 1271 probably at least 20 convergences are to be expected.

A very striking example of a wrong convergence occurred in about February, 1944. A message was converged twice on Colossus from two different random starts (R1 p 93, R2 p 14) and the same result was obtained each time. The rectangle was then converged by hand, using intellingence in the selection of a start and a very much better convergence was obtained (which was then checked on Colossus when the other wheels were broken). As an experiment, accurate convergence was applied to the original convergence and after a few steps it began to improve and became the same as the better convergence (R2 pp 21 etc.). Since that time more care was used in starting the convergence, but the accurate method was used only at first, and when there was not a flood of work.

One method of starting convergence is by the use of a skeleton (see e.g. R2 p 82, R4 p 20). This has the advantage that most of the arithmetic is avoided and a flag 16 by 16 can be made in the same time as a much smaller flag of the ordinary type. This method is not suitable for rectangles of length 2n x 1271 (n=2,3,4) and since so many of the rectangles were of length 8 x 1271 the method was not generally adopted (R3 p 74). The method is a special case of throwing away a lot of the smaller pieces of evidence in order to be able to work more quickly with the larger pieces (see R2 p 94).

* In fact there are exactly 31 convergences for 'scalar product' convergence.

Here is a list of references to methods of starting the convergence of a rectangle:

Techniques for starting convergence on Colossus R1 p 93.

Necessity of a good start. Suggestion of starting from eleven selected rows, trying all possible signs R2 p 4 (see also R2 pp18,22, R3 p 21).

Eye starts R3 p 108.

Random starts, with purging R4 p 3.

Methods of starting and suggestion that the choice amongst certain standard methods should be optional R4 p 23.

Statistics for various methods of starting R4 p 68.

Here are some references to methods of analysis of a rectangle, not connected with methods of starting.

Solving rectangle by linear equations. Crude convergence. Solving a rectangle by minimising a quadratic form R1 pp 40, 56.

Maximum likelihood solution of a rectangle R2 pp 16, 29, 32, 34, 35, 37, 39, 40.

There are other consequences of the knowledge that more than one convergence is possible, besides the importance of a good start. One is that the convergence must be done with care. The standard of acceptance of a character should be lowered gradually and arithmetical mistakes should be avoided. There were several examples of a wrong convergence being reached due to mistakes of various kinds. Another consequence is that a better convergence than the first one can often be obtained by a 'restart' in which the highest scoring characters of the first convergence are taken for the restart of another convergence (see R3, p 98). The validity of this method (apart from the successes attained) (see e.g. R2 p 101) depends on the empirical observation that the high-scoring characters tend to have the right sign even if the rectangle has not reached 'significance' (R3 pp 16, 17, 36). (For the meaning of the term significance see below - significance test IV.)

(d) __Flags.__

It has been found that crude convergence of a rectangle from a random start is liable to lead to a convergence which is not the best one.

Therefore various methods of starting the convergence have been suggested. One of these is the method of 'flags'. This consists in comparing every pair of a certain number of rows of the rectangle and scoring these pairs by some scoring system. The resulting scores are entered into a triangle like an American Tournament table and the result examined in order to get a starting pattern for $\Delta\chi_1$. This method using scalar products was started by Vergine who had used the method in connection with the Hagelin machine. Later we began entering the flag double entry, making it square and then crudely converging the flag, (R2 p 79). The number of rows used varied from 6 to 16 depending to some extent on the type of scoring system used.

The correct scoring system for an assumed value of δ is given by the function $f(\theta,\theta')$ above. This is troublesome to use in practice and an approximate formula must be used. The usual formula was $\theta\theta'$, so the entries in the flag were simply the scalar products of the pairs of rows. This method is a good approximation if δ is small. (It is the sort of method that a statistician would think of naturally.) When this method is used it is often convenient to divide all entries in the flag by 10 before converging it (giving the results to the nearest whole number).

It might be thought that the scalar product method could be used as a substitute for accurate convergence. However the degree of approximation would be very bad in this case since the pippages involved are much larger. In fact the accurate score of x pips compared with y pips is easily seen to be

$$\left(\log\cosh \tfrac{1}{2}(x+y)p - \log\cosh \tfrac{1}{2}(x-y)p\right) \text{ natural bans where}$$

$p = \log \frac{1+\delta}{1-\delta}$ (i.e. approximately 2δ).

and this is sufficiently close to

$$\log\cosh (x+y)\delta - \log\cosh (x-y)\delta$$
$$= \frac{\delta^2}{2}\left\{(x+y)^2-(x-y)^2\right\} - \frac{\delta^4}{12}\left\{(x+y)^4-(x-y)^4\right\} + \frac{\delta^6}{45}\left\{(x+y)^6-(x-y)^6\right\} \cdots\cdots\cdots$$
$$= 2\delta^2 xy - \frac{2}{3}xy(x^2+y^2)\delta^4 + \cdots\cdots\cdots$$

The first two terms can be written

$$2xy\delta^2\left\{1 - \frac{(x^2+y^2)\delta^2}{3}\right\}$$

As a rather extreme case, if $x = 8$, $y = 6$ and $\delta = \frac{1}{10}$, the term $2xy\delta^2$ would be 50% too large. So for flag making xy is quite a good approximation (R3 pp 4, 5, 29) if the unit (or 'pippette') is taken as $2\delta^2$ natural bans, i.e. 1 pippette $\doteq \delta$ pips. On the other hand, in accurate convergence one of the numbers x,y is generally far too large for the approximation to be valid. In this case the formula

$$\log \cosh (x+y) \delta - \log \cosh (x-y) \delta$$

can naturally be used to justify crude convergence.

There is another type of flag, called the Jacobs flag (see R2 p 101) in which the function xy is replaced by

$$\mathrm{sign}\ (xy)\ \min\ (|x|, |y|).$$

This type of flag was used for one of the methods of starting the convergence of a rectangle, because it is quicker than multiplication, though much less accurate. It would be a good approximation for large values of δ. If all the entries in the rectangle are ± 1 or 0 then Jacobs flag and the ordinary (scalar product) flag are the same thing. This remark applies in the case of most key rectangles.

For mechanical flag-making for cipher tapes see R3 pp63, 78, 82, 106, R2 p 101. and ch.91.

24X SIGNIFICANCE TESTS

(a) Introductory remarks.

We are about to discuss a number of significance tests for rectangles. The first one, 'significance test 0' is designed for rectangles not converged. Tests I to IV are for converged rectangles. The standard one is significance test IV, and is the most difficult to understand.

(b) Tests for unconverged rectangles (historical).

No rectangle was made with mechanical aid of any sort until after the autoclave had been generally introduced (January 1944). It was then suggested (R1 p 32) that if the rectangles were made on a Robinson, with a set total, the number of readings that came up would be an indication of how good the rectangle was likely to be. Such a test was particularly important at a time when it was troublesome to make rectangles. It was thought at first that such a test would be quite powerful and that it might even be possible to stop Robinson in the middle of the run. However some figures were then produced (R1 pp 34, 38) depending on a single message that had been rectangled by hand a long time before, and these figures tended to show that the method would not be very powerful. Soon after this the square-summing test was suggested, emerging from some calculations which appear in the black file. These calculations contain an error (corrected below) but the order of the answer was right and agreed with the indications of the message just mentioned. It was not until September 1944 that the slide and significance test was invented (R3 pp 77, 83). It was not realised absolutely at once that this test is equivalent to the square-summing test. The original object of the slide and significance test was for putting rectangles in a priority order and even for rejecting them. Unfortunately the tapes took some time to make and the earlier Robinsons were rather hard on long tapes, so the rectangle was often converged before the sigma-age of the test had been worked out. It was suggested further that a slight modification of the test could be used for attempting to detect slides of ± 1 (R3 p 92). This was tried only a few times and would probably have had an occasional success. The slide and significance test was made more practicable by the introduction of 'Thurlow tapes of the second kind' as the standard non-Colossus method of producing a rectangle (R4 pp 71, 82). However, the Robinson routine was dropped when the Colossus gadget, which counts the frequencies of occurrence of the different values of θ_ψ was brought in.

For another test for unconverged rectangles see R1 p 36. This test in effect is equivalent to a crude form of flagging a skeleton. Significance tests for flags are suggested in R2 p 92, and R3 p 8, and these can be regarded as tests for a rectangle on which no convergence has been done. But these tests would not be expected to do very well unless the rectangle is an exceptionally good one. On p 92, R2 there is also a suggestion which is a test rather of the start of a convergence.

An entirely different way of possibly obtaining evidence about the wheels without rectangling is by doing a $\Delta^2 Z$ alphabetical count (R3 p 64). This can be of value only if at least one of the χ's has good Δ^2 properties, i.e. $\Delta^2\chi_i$ nearly all crosses. (See also 25(a) for $\hat{\chi}_2$ runs and chapter 25F for one wheel break-ins if $ab \neq \frac{1}{2}$.)

(c) <u>Tests for converged rectangles (historical)</u>.

The first rectangle ever done for wheel-breaking purposes is mentioned in Part 4'. The first 10,000 letters of a message were used and the result of the convergence enabled the rest of the message to be set convincingly at a slide. This enabled the worker to feel that things were going well, and can be regarded as a form of significance test. It is a special case of setting another message against the (partial) wheels obtained from a rectangle. In the early days of mechanical wheel-breaking there was a tendency to rely rather too much on this method. At first the allied method of wheel-sliding was used, as it was believed to be more accurate in some ways, and it avoided the use of machine time.

Another test for significance, easy to apply with our improved machines, is to spin the message using partial wheels from the rectangle and see if there is an obvious slide. Yet another test is to see if the wheels obtained from the rectangle have outstandingly good Δ^2 properties (R3 p 63). This method was most successful when the Δ^2 properties were so good that perfect wheels were assumed for both χ_1 and χ_2 and the wheels were broken although the rectangle was considerably below significance.

Useful as all these methods have been, none of them has ever been successful for rectangles falling short of significance by more than 15 decibans, on significance test IV. This test was introduced about the 1st March, 1944. Up to about a fortnight before that time it was thought likely that the result of an accurately converged rectangle really did give the correct pippages of the characters of $\Delta\chi_1$ and $\Delta\chi_2$. The only important theoretical problem seemed to be to find an estimate of δ.

It was the failure of the wheel-sliding attempts on Jellyfish which made us suspect that a significance test was necessary. The tests I, II, III, IV were all put forward within about two weeks.

A crude form of significance test IV was designed in July, 1944 for the benefit of the computers (R3 p 23). The idea of this test was that the wheel man should be informed as soon as possible when a rectangle was likely to be quite good. It was observed empirically that the $\mathfrak{F}$ terms hardly ever added up to more than 30 decibans for the usual length of text, namely 10168. (See below for the definition of the $\mathfrak{F}$ terms.) Further it was assumed somewhat arbitrarily that $\Sigma\mathfrak{F}$ was inversely proportional* to N. The significance test can be written

* Perhaps inversely proportional to $\sqrt{N}$ would have been a better assumption.

$$\frac{2\cdot 17\, x^2}{N} > 219 - \frac{100000}{N}$$

This gives, to a sufficient approximation,

$$X > 10\sqrt{N - 1500}$$

and the function $10\sqrt{N - 1500}$ was therefore tabulated.

Some time later (R4 pp 111, 117) another alternative was suggested, also based on an empirical consideration of ϑ terms. Unfortunately it was not based on a careful study of the statistics about ϑ terms available by that time. The sum of the ϑ terms for N = 8 x 1271 were examined empirically, since the sample for this text length was considerable (R3 p 95). It was found that this sum could be approximated by the expression

$$\frac{24,000,000,000}{X^3} \pm 3\cdot 6 \text{ decibans.}$$

This enabled one to say (with only a small probable error) how many decibans up or down any rectangle of this length would be, given X. By 1945 there were probably sufficient statistics to obtain an empirical simplification for all values of N, but this was never done.

(d) Significance test for a rectangle not worked on - the square summing test.

By a 'significance test for a rectangle not worked on' we mean a test which depends only on the numbers in the 1271 cells of the rectangle and not on any convergence of the rectangle for comparison of the rows. Such a test is the one referred to as significance test 0, which amounts roughly to summing the squares of all the 1271 entries in the rectangle. (This test appeared in the 'Black File' at an early date.) Naturally such a test cannot be as powerful as tests which can be applied after the rectangle is converged but occasionally a result is obtained enabling one to forecast that the rectangle will be significant when converged.

Let the entry in the cell (i,j) of the rectangle be θ_{ij}. Then the function required is $s_2 = \Sigma_{ij}\theta_{ij}^2$. There is a gadget on Colossus which counts the number of occurrences of each value of $|\theta_{ij}|$ when producing a rectangle, so that s_2 can be calculated without difficulty.

A test that can be applied even before the rectangle is made is the so-called 'slide and significance test'. Leaving aside the part of this test that deals with the detecting of slides it can be shown that this test is equivalent to square summing. The test consists in counting

$\Delta_{1271\nu}(\Delta Z_{ij})$ = . for $\nu = 1, 2, \ldots, k-1$, using a message of length $N = 1271k$ stuck with the end running straight on to the beginning. This method of sticking enables the text length used for each of the $(k-1)$ counts to be equal to N. The result is that if the scores for $\nu = 1, 2, \ldots (k-1)$ are added together and the result is called X then every pair of letters in ΔD at a distance which is a multiple of 1271 will have an opportunity of contributing either 2 or 0 to X. The total number of such distinct pairs of letters is $1271 \times \frac{k(k-1)}{2}$ so that $\frac{1}{2}X - \frac{1}{2}(1271 \times \frac{k(k-1)}{2})$ is defined as the bulge B of the test. It is resonable to suppose that the value of B (if $\delta = 0$) is 0 and that its S.D. is $\frac{1}{2}\sqrt{\left\{1271\ \frac{k(k-1)}{2}\right\}}$. Both of these assertions are true, though the proofs are not entirely trivial. Further it is clear that

$$X = \Sigma\left\{r(r-1) + s(s-1)\right\}$$

summed over all cells of the rectangle, where r is the number of dots and s is the number of crosses in a typical cell. If we now remember that $r + s = k$, $r - s = \theta_{ij}$,

$S_2 = \Sigma\,\theta_{ij}^{\,2}$, $B = \frac{1}{2}X - \frac{1}{2}(1271\ \frac{k(k-1)}{2})$

it follows that

$$B = \tfrac{1}{4}(s_2 - N).$$

This is the connection between the square-summing test and the 'Slide and significance test'. It is implicit in all this that the expected value of s_2 is N and that its S.D. is $\sqrt{2N(k-1)}$.

The distribution of s_2 or B is really of χ^2 type but it is near enough to a normal distribution for most practical purposes.

In order to see how strong the test is we may argue as follows: The number of comparisons is $N_0 = 1271\ \frac{k(k-1)}{2}$ and the P.B. for a given value of δ, in each comparison is δ^2. Thus the expected sigma-age is $\delta^2\sqrt{1271\ \frac{k(k-1)}{2}}$. For example if k = 8 the expected sigma-age is $187\ \delta^2$. If $\delta = \cdot 1$, which is sufficient for the significance of the converged rectangle, the expected sigma-age would be 1·9. If $\delta = \cdot 15$ the expected sigma-age is 4·2, so highly significant rectangles are liable to be picked out quite well. One might be tempted to reject all rectangles whose sigma-age on the test was negative, but although this should not often happen if the rectangle is a good one, it also does not often happen anyway and the factor against the rectangle being significant is not at all large.

In order to estimate this factor, the simplest method is as follows:

Let sigma-age observed be s.

Let sigma-age expected for a given value of δ be s_1.

Then $s_1 = \delta^2\sqrt{1271\,\frac{k(k-1)}{2}}$

and the factor in favour of a particular value of δ rather than $\delta = 0$ is, if we assume σ independent of δ,

$$e^{-\frac{1}{2}(s_1-s)^2}\Big/e^{-\frac{1}{2}s^2}$$

$$= e^{ss_1-\frac{1}{2}s^2}$$

or, in natural bans, $ss_1 - \frac{1}{2}s^2$

$$s = \frac{B}{\frac{1}{2}\sqrt{\frac{k(k-1)1271}{2}}}$$

Therefore natural banage is $2B\delta^2 - \frac{N(k-1)}{4}\delta^4$

$= \frac{1}{2}(s_2 - N)\delta^2 - \frac{(k-1)N}{4}\delta^4$

$= \lambda\delta^2 - \mu\delta^4$ say.

The factor in favour of $\delta > \delta_0$, rather than $\delta < \delta_0$, assuming a uniform prior distribution for δ for positive δ (and no chance of $\delta < 0$), is

$$\int_{\delta_0}^{\infty} e^{\lambda\delta^2-\mu\delta^4}\,d\delta\Big/\int_{-\infty}^{\delta_0} e^{\lambda\delta^2-\mu\delta^4}\,d\delta$$

If $s_2 = N$, $k = 3$, $\delta = \cdot 08$ this reduces to

$$\int_{\cdot 08}^{\infty} e^{-17{,}800\,\delta^4}\,d\delta\Big/\int_{0}^{\cdot 08} e^{-17{,}800\,\delta^4}\,d\delta$$

$= \cdot 15.$

Thus with N = 10168 a zero score on the significance test implies a factor of about 6 against the rectangle being significant.

The original discussion of 'significance test θ', given in the black file, makes no assumptions about distributions and is a direct application of Bayes' theorem. We proceed now to give an account of this with simplification and correction of the original argument. It is not assumed that the length N of the message is necessarily a multiple of 1271.

Let us assume some definite value of δ and suppose that the depth of the rectangle in a particular cell is k. Then the probability that there will be an entry of θ in the cell (where θ and k are integers of like parity) is

$$\binom{k}{\frac{k}{2}+\frac{\theta}{2}} \times \frac{1}{2^k}\left\{(1+\delta)^{\frac{k}{2}+\frac{\theta}{2}}(1-\delta)^{\frac{k}{2}-\frac{\theta}{2}} + (1+\delta)^{\frac{k}{2}-\frac{\theta}{2}}(1-\delta)^{\frac{k}{2}+\frac{\theta}{2}}\right\}$$

and therefore the factor in favour of this value of δ rather than $\delta = 0$ is

$$(1-\delta^2)^{\frac{k}{2}} \times \frac{1}{2}\left\{\left(\frac{1+\delta}{1-\delta}\right)^{\frac{\theta}{2}} + \left(\frac{1+\delta}{1-\delta}\right)^{-\frac{\theta}{2}}\right\}$$

$= \operatorname{sech}^k \delta'.\cosh(\theta\delta')$,

where $\delta' = \frac{1}{2}\log\frac{1+\delta}{1-\delta} = \delta + \frac{1}{3}\delta^3 + \ldots,$

and is very close to δ in all practical cases. The natural banage from all the cells together is thus

$\sum_{ij} \log\cosh(\delta'\theta_{ij}) - N\log\cosh\delta'$

$= \frac{\delta'^2}{2}(s_2 - N) - \frac{\delta'^4}{12}(s_4 - N) + \frac{\delta'^6}{45}(s_6 - N) \ldots.$

where $a_n = \sum \theta_{ij}^{\,n}$

Now $E(a_2) = N$, $E(a_4) = 3kn$, $E(a_6) = 15k^2n$, ... if $\delta = 0$ and $N = 1271k$

so, if $\delta^2 N < 200$, a sufficiently good approximation is

$$\frac{\delta^2}{2}(s_2 - N) - \frac{\delta^4(s_4 - N)}{12}$$

Observe that we cannot neglect the term in δ^4 since $E(a_2 - N) = Nk\,\delta^2$, so the expected value of the second term is about half of that of the first term if δ is small. If we write $a_4 = 3kN$ there is still a small discrepancy between the natural banage obtained here and that obtained before. This discrepancy is due to the assumption (see R4 p 122) that σ is independent of δ. A more interesting remark is that the present method shows that the evidence of the value of a_4 should be taken into account. The 'maximum likelihood' value of δ is

$$\sqrt{\frac{3(a_2 - N)}{a_4 - N}}$$

though this is itself liable to a large S.D. which can be estimated. Larger values of a_4 given smaller values of δ so the previous formula lays too much stress on the higher entries in the rectangle.

(e) <u>Significance tests for rectangles which have been crudely converged.</u>

Let the double bulge on /1+2 on a message of length N, against the correct wheels be $\varkappa^a$. (We assume no slide - otherwise the phrase 'correct wheels' becomes ambiguous.) If a crude convergence is done, starting with one of the correct wheels (say $\Delta\chi_1$), then a result will be obtained in which the double bulge x is greater than or equal to x^*. The true value of δ is approximately x^*/N (see R5 pp 68, 87). The difference $x - x^*$ is something like $\sqrt{N}$ (R3 pp 117, etc.). This estimate depends on the assumption that the final convergence gives wheels that are substantially correct and this is the question we are going to consider here. We begin with three significance tests which have a certain weakness in common and then describe a fourth test which is <u>relatively</u> free from this weakness.

I. We may try to use the value of a pip to estimate the factor in favour of the wheel patterns being substantially right. If we say that the rectangle is x half pips up we get a decibanage of roughly $2{\cdot}17 \times x^*/N$.

This expression is very sensitive to the exact estimate of x^*.

II. Suppose we imagine $\delta = 0$ and assume the distribution of x is normal. Then the probability that x will reach a specified value is roughly

$$\frac{1}{x}\sqrt{\frac{N}{2\pi}}\ e^{-x^2/2N}$$

We should like this to be less than 2^{-71}, since 2^{-71} represents the prior probability of the wheel patterns assumed ($71 = 41+31-1$). (One is subtracted because two theories for which the wheels are relatively inside out are equivalent).

III. There is a method called the square summing of columns, described in R1 p 95, which is more rigorously provable than II but is more trouble to apply. (Also it sacrifices some of the evidence, unless the rectangle is exactly 1271 long) (See R2 p 15.)

In the three methods described above it is implicit that there is a prior probability of 2^{-71} to be offset, or a decibanage of 214. But really it is not as bad as this, because we are interested only in the wheels being substantially right, and the number of wheel patterns which can be regarded as substantially the same as the converged rectangle wheels may be quite large. In this sense the tests II and III are too harsh, but in another sense they are too lenient, namely in the sort of way that the glib use of the error function is too lenient when setting chi's. (See chapter 21(c) 'Statisticians' Fallacy'.) On the whole it seems best to make a direct appeal to Bayes' theorem.

IV. Consider first the two theories

(i) Two definite wheel patterns and a definite value of δ

(ii) $\delta = 0$ (i.e. rectangle is random).

The probability of an excess θ of dots over crosses in a cell of the rectangle containing k entries (where θ and k have the same parity) is

$$\frac{1}{2^k}\binom{k}{\frac{k}{2}+\frac{\theta}{2}}(1+\delta)^{\frac{k}{2}+\frac{\theta}{2}}(1-\delta)^{\frac{k}{2}-\frac{\theta}{2}}$$

if $\Delta\chi_{12}$ is assumed to be a dot in the cell. Therefore the factor for theory (i) rather than (ii) is

$$\left(\frac{1+\delta}{1+\delta}\right)^{\frac{\theta}{2}}(1-\delta^2)^{\frac{k}{2}}$$

Therefore, using all the cells of the rectangle, the total factor in favour of theory (i) rather than (ii) is

$$\left(\frac{1+\delta}{1-\delta}\right)^{\frac{x}{2}}(1-\delta^2)^{\frac{N}{2}},$$

where x is the double bulge of /1+2 using the wheel patterns of theory (i). Denote by $\varphi(\delta)$ the prior probability distribution of δ. Then the factor in favour of the particular wheel patterns, not allowing for competition is a number f where

$$f = \int_{-1}^{1}\varphi(\delta)\left(\frac{1+\delta}{1-\delta}\right)^{\frac{x}{2}}(1-\delta^2)^{\frac{N}{2}}d\delta$$

$$= \int_{-1-\frac{x}{N}}^{+1-\frac{x}{N}}\varphi\left(\frac{x}{N}+\epsilon\right)\exp.\left\{\lambda - \frac{N}{1-\left(\frac{x}{N}\right)^2}\cdot\frac{\epsilon^2}{2}+\cdots\right\}d\epsilon$$

where $\lambda = \log\left\{\left(\frac{1+\delta}{1-\delta}\right)^{\frac{x}{2}}(1-\delta^2)^{\frac{1}{2}N}\right\}\Bigg|_{\delta=\frac{x}{N}}$

$$= \frac{x^2}{2N} + \frac{x^4}{12N^3} + \cdots$$

Therefore $f \simeq e^{\frac{x^2}{2N}+\frac{x^4}{12N^3}+\cdots}\cdot\sqrt{\frac{2\pi}{N}}\,\varphi\left(\frac{x}{N}\right)$

If+ $x^2 < 120N$, the term $x^4/(12N^3)$ is less than $10(x/N)^2$ (natural bans) which is nearly always negligible. If we assume δ has a uniform distribution in an interval* of length $\cdot 1$, and has no chance of

---

\+ See below

* This estimate was originally a guess, but it was borne out quite well by statistics of set messages. In any case the result is not sensitive to variations in the assumption of the precise distribution of δ.

lying outside this interval, then $\varphi(x/N) = 10$ and the natural banage is

$$\frac{x^2}{2N} - \log \frac{\sqrt{N}}{25}$$

or roughly $\left(\frac{2.17x^2}{N} - 5\right)$ decibans with an error of less than two decibans for the usual values of N.

The prior probability of any particular (differenced) wheel patterns (for a 1+2 rectangle) is 2^{-71} if the patterns obtained by reversing dots and crosses are regarded as equivalent to the original patterns. (This neglects wheel characteristics.) So particular wheel patterns are evens not allowing for competition, if

$$\frac{2.17x^2}{N} - 219 = 0.$$

(Compare the argument this far with R3 p 40.)

If $x^2/N = 120$ the wheel patterns are 41 decibans up, not allowing for competition. This is the justification for assuming $x^2 < N.120$ in the argument above. If $x^2 \geq 120N$ it is certain that the wheels are substantially right and inaccuracy in the odds does not matter.

We now go on to the problem of finding the odds that the wheels are substantially right. Clearly the result must depend on what is meant by wheel patterns being substantially correct, but it may not be very sensitive to variations in the definition, provided that the definition is a reasonable one.

Let x' be the double bulge on a typical pair of wheel patterns. Then whatever the definition of substantially correct, the factor in favour of the wheel patterns, obtained from the rectangle, being substantially correct is

$$\frac{1}{3} \sum_{x'} \exp. \frac{x'^2}{2N}$$

summed over all wheel patterns which are regarded as substantially equivalent to those of the rectangle. (The factor 1/3 corresponds to the -5 d.b. referred to above.)

If, for a typical pair of wheel patterns, y is the sum of the moduli of the scores of the characters that are changed in the rectangle patterns in order to get the new ones, then a good approximation is $x' = x - 2y$ if the new patterns are not too different from the old ones. Therefore the factor above is approximately equal to

$$\frac{1}{3} \sum_{y} \exp. \frac{(x-2y)^2}{2N}$$

$$= \frac{1}{3} e^{\frac{x^2}{2N}} \sum_{y} \exp. \left\{-\frac{2y}{N}(x-y)\right\}$$

where the summation is over all wheel patterns defined as substantially the same as those of the rectangle. This formula is equal to

$$\frac{1}{3}\, e^{\frac{x^2}{2N}} \sum_{y} \exp.\left\{-\frac{2y}{N}(x-K)\right\}$$

where K is some sort of mean value of y for substantially equivalent patterns. We assume further that y is the sum of any number of terms y_1, y_2, ... which are the moduli of the x's. It might be objected that this includes values of y that are too large to be permitted for substantially equivalent patterns, but then the terms with large values of y are negligible anyway.

This makes the factor

$$\frac{1}{3}\, e^{\frac{x^2}{2N}} \sum_{i,j,\dots} \exp.\left\{-\frac{2(y_i+y_j+\dots)}{N}(x-K)\right\}$$

$$= \frac{1}{3}\, e^{\frac{x^2}{2N}} \prod_{i} \left\{1 + e^{-\frac{2(x-K)y_i}{N}}\right\}$$

Expressed in decibans, this gives, allowing for the prior odds

$$\frac{2\cdot 17\, x^2}{N} + \sum \mathfrak{f}\left(\frac{2(x-K)y_i}{N}\right) - 219$$

where

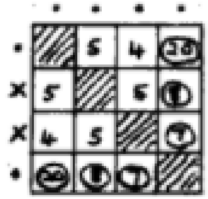
$$\mathfrak{f}(a) = 10\log_{10}(1 + e^{-a}).$$

The formula is now suitable for numerical calculation provided some value of K can be decided upon. It is just this part of the problem which is the least important though it is the most difficult. Let the pippages of the $\Delta\chi_1$ on the rectangle be $a_1, a_2, \dots, a_{41}$ and let any other pattern be put into correspondence with pippages which are the same as the a_i's at places where the wheels are the same and are $-a_i$ at places where they are different. We can then say that the wheel patterns are substantially equivalent if these two sets of pippages score positively against each other when scored on the wheel-sliding table. It can be shown (see Black File) that if the message is not too short this definition leads to a maximum value of y of about 432. This is the origin of the usual value of K, namely 216. A rival value for K is $\sqrt{N}$ (see R3 pp 117, 118, R4 p 38) and in any case K must be taken as a function of N in order to cope with key rectangles. As a rough judgement based on experience, $K = 1\cdot 5\sqrt{N}$ seems fairly good. Observe that every zero scoring character contributes a factor of 2. This is exactly right because the character can be taken as a dot or a cross without affecting the double bulge, so the prior probability of the wheel patterns permitting the double bulge of x is 2×2^{-72} instead of 2^{-72}.

When a rectangle has a positive decibanage on significance test IV it is usually said to be 'significant'.

(f) Significance tests for flags.

When a flag is entered double (in the form of a square) and is crudely converged, the convergence differs from ordinary crude convergence in that it is one-sided instead of two-sided. That is to say the 'pattern' which is taken through the flag gives rise to another pattern which is written down on the same side of the flag. It is not necessarily possible to reach a complete convergence - it may be necessary to doubt some characters in order to avoid an oscillation of the pattern. For example consider



the flag shown in the diagram. The pattern inevitably oscillates between [illegible] and [illegible] or else between [illegible] and [illegible]. Observe that a pattern is equivalent to itself inside out just as in the case of an ordinary rectangle. If the effect of oscillation is ignored we may say that there are 2^{n-1} different possible patterns to choose between, so the prior probability of any particular pattern is 2^{-n+1}. The sum of the moduli of the pippages is still denoted by X, and the sigma-age of a convergence is $X/(2\sigma)$ where σ^2 = sum of square of entries in triangular flag. The presence of the factor 2 in the denominator is due to all the evidence being counted twice in virtue of the double-entering of the flag. The flag can be regarded as significant if the function $\Psi(\frac{X}{3\sigma})$ is greater than $3(n-1)$ decibans (where Ψ is the function defined in chapter 21). (See R2 p 92, R3 p 8.) This test is the analogue of significance test II for rectangles. It can be improved by making a mental allowance for λ^3 terms (as in significance test IV). Thus every very small pippage of a character is worth 3 decibans.

This test assumes a flag to be a random collection of numbers and this assumption is not strictly true even if the rectangle from which it is derived is random.

It is rare that a 9 by 9 flag has a significant convergence except for a very significant rectangle (R3 p 82). The main application of the test was to key flags (see Chapter 26). For another form of significance test, based on Bayes' theorem, see R3 pp 77, 79. This latter test was applied to 'flag rectangles' (R3 pp 84, 85).

For a theory which connects the score and significance of a complete flag with those of its rectangle, see R4 p 112, R5 pp 17, 21, 90.

24Y OTHER THEORY OF RECTANGLES

(a) Length required to break wheels and rectangles other than 1+2.

The message length required to break all the wheels is about the same as that required for a significant rectangle. Roughly, the score (or double bulge) x of the rectangle (assumed to be 1+2) must satisify the inequality

$$\frac{2\cdot 17x^2}{N} + 30 > 219$$

assuming the $\sqrt{}$ terms do not amount to more than 30 decibans,

$$\text{i.e.}\quad x > 9\cdot 4\sqrt{N}$$

i.e. since the score on correct wheels is approximately $x - \sqrt{N}$

$$\delta N + \sqrt{N} > 9\cdot 4\sqrt{N}$$

$$\text{or } N > {}^{71}/_{\delta^2} \quad \text{or } N > \frac{71}{\beta^4 \pi_{12}^2}$$

Observe how sensitive the minimum value of N is to the value of δ. The conclusion that the minimum text length required was proportional to $(\beta^4\pi^4)^{-1}$ was reached by an entirely different method in R1 pp 51, 53. With $\delta = 21$ and $\pi = \cdot 2$ the minimum N is about 11,000; with $\delta = 28$, $\pi = \cdot 2$ the minimum is about 3000.

For a 4+5 rectangle the condition would be roughly

$$\frac{2\cdot 17x^2}{N} + 20 > 149$$

$$\therefore\quad \delta N + \tfrac{1}{2}\sqrt{N} > 7\cdot 8N \qquad (x \doteq \delta N + \tfrac{1}{2}\sqrt{N}\text{: see R3 p 117})$$

$$\text{i.e. } N > {}^{53}/_{\beta^4\pi_{45}^2}$$

Incidentally this shows that a 4+5 rectangle would probably be just significant on a shorter text than a 1+2 rectangle if

$$\left(\frac{\pi_{45}}{\pi_{12}}\right)^2 > \frac{53}{71} \qquad \text{i.e. } \pi_{45} > \cdot 86\,\pi_{12}$$

This condition was seldom likely to be satisified and 4+5 rectangles were seldom made. The condition for a 4+5 rectangle to be more decibans up than a 1+2 rectangle is not the same (see R5 p 99)

It was thought at first that the 4+5 rectangle would be better, especially allowing for the greater time taken to make a 1+2 rectangle (R1 pp 35, 36). A 2+5 and a 4+5 rectangle could both be made, so as to obtain independent evidence for χ_5 (R1, p.48). In this case one would naturally have a 1+2 rectangle also, but it was decided that the extra trouble was not compensated for by the slightly increased power. For references to 3+4x rectangles see R3 p 7.

For a 'pseudo 2+5 rectangle' see R3 pp 81, 86. The method may be suitable for the case of $\bar{\chi}_2$ and $\bar{\bar{P}}_5$ limitations, but limited statistics tended to show than an ordinary 2+5 rectangle would be better. Another idea that was put forward was a Δ^2 rectangle or a 2-impulse bigram rectangle. This also was not encouraged by the statistics. (R3 pp 44, 52, 58.)

(b) <u>Rectangles with χ_2 limitation.</u>

As early as R1 p 59 it was thought that the χ_2 limitation might have a characteristic effect on rectangles. On p.62, R1 there was a reference to a suggestion for a 'repeats' rectangle in which .., .x, x. and xx would be treated separately. This makes sense for χ_2 limitation but not for other limitations (see R2, p.96).

The difference $X-X^*$ between the score of a converged rectangle and the score on the correct wheels tends to be greater when the limitation is χ_2.

Methods for diagnosing χ_2 limitation from a converged rectangle were suggested and discussed in R3 pp 59, 101, 119, 122, 123, 126, 128, R4 pp 31, 35, 38. More to the point is a note in R4 p 71 (see also R4 p 80, R5 p 38). It is pointed out here that a 4 l.c. provides evidence about the limitation and that this is so even if a complete χ_2 is assumed, because it will tend to be wrong at $\bar{\chi}_2$ dots rather than crosses.

(c) <u>Wheel-sliding.</u>

In the very early unsuccessful attempts on Jellyfish the following method was used. Several rectangles of messages on the same month were accurately converged. Then the relative positions of say χ_2 were looked for by sliding the pippages from one rectangle against those of another. The crudest method of wheel-sliding is to express the wheels in dots, crosses and doubts and to insist on an excess of say 6 or more agreements than disagreements, or vice versa. (Remember that it would not usually be known whether the Δ wheels were relatively inside out.) The rival good positions can then be scored by a more accurate [redacted] Before we had time to work out the correct wheel-sliding table a cruder method was used. This cruder method is to evaluate

$$\sum_i \tfrac{1}{2}\left\{1 \pm \operatorname{sign} a_i \operatorname{sign} a_i'\right\} \min\left(|a_i|, |a_i'|\right)$$

where the lower sign is taken if the patterns $a_1, a_2, \ldots$ and $a_1', a_2', \ldots$ are assumed to be relatively the right way round. This method is easy to apply in practice and is a reasonable approximation (in a sense) to the accurate method which we now prove.

Denote the decibanage of a typical character of one wheel by x, so that its odds of being a dot are $\varpi = 10^{x/10}$ and probability $p = \varpi/(1+\varpi)$. Let $p = \frac{1}{2}(1 + \pi)$. Let the probability of having an x in a cell of the first wheel be ρ_x if the character is a cross. Then the probability of having an x if the character is a dot is $\varpi\rho_x$. Denote by x', ϖ', ρ_x' the corresponding functions for the second wheel. Then the probability of seeing an x opposite an x' if the relative position of the two wheels is correct ~~and they are not relatively inside out, is~~

$$\tfrac{1}{2}\left(\rho_x \rho_{x'}' + \varpi \rho_x \varpi' \rho_{x'}'\right)$$

and if it is wrong

$$\tfrac{1}{2}\rho_x(1+\varpi) \cdot \tfrac{1}{2}\rho_{x'}'(1+\varpi')$$

Therefore the factor obtained from one pair of entries in favour of the slide being correct is

$$2 \cdot \frac{1+\varpi\varpi'}{(1+\varpi)(1+\varpi')} = \tfrac{1}{2}(1+\pi\pi')$$

The factor obtained from the complete comparison is

$$\prod \left\{\tfrac{1}{2}(1+\pi\pi')\right\}$$

In order that this formula should not be misleading, it is necessary to allow for competition, because the correct wheel may have very good slides against itself. A table exists for accurate wheel-sliding with pip value 2/3 deciban (See R1,97).

(d) <u>Setting two messages in depth on Chi1 and Chi 2</u>

Closely related to significance test 0 is the problem of attempting to set two messages in depth on chi 1 and chi 2 before either rectangle is converged: (R1,75;R3,28,35). In order to show how close the relationship is, the problem can be attacked in the following way. Let each of the 1271 different relative settings of chi 1 and chi 2 be tried out. For each of these let significance test 0 be applied. Let θ , θ' denote typical entries in the separate rectangles, then the expression considered is $\Sigma(\theta+\theta')^2$. This is equal to $\Sigma\ \theta^2+\Sigma\ \theta'^2+2\Sigma\ \theta\theta'$. The first two terms are independent of the particular selection amongst the 1271 theories. Thus the method is equivalent to scalar multiplication. If the lengths of the messages are 1271k and 1271k' with P.B. of ΔD_{12} = dot of δ and δ', then the propertionate bulge of ΔZ_{12} and $\Delta Z_{12}'$, in a particular cell, is $\delta\delta'$ if the rectangles are correctly set relatively. The number of comparison is 1271kk' so the expected sigma-age is $\delta\delta'\sqrt{1271\,kk'}$. In order that this should exceed 3 it is necessary that either $\delta\sqrt{1271k}$ or $\delta'\sqrt{1271k'}$ should exceed 10. Thus it is impossible for two rectangles to be set by Significance Test <u>0</u> (i.e. when unconverged), unless at least one of them would be significant according to Significance Test <u>IV</u> (i.e. when converged). The sum may nevertheless, of course, be significant according to Significance Test IV, but 1271 separate convergences are impracticable. This scalar product method is an approximation to the theoretically correct method of comparing the two rectangles by means of the wheel-sliding table treating them as wheels 1271 long. (R3,35).

25 CHI-BREAKING FROM CIPHER

25A The short wheel-breaking run

25B Weighing the evidence

25C General plan of wheel-breaking

25D Particular methods
- (a) Doubts
- (b) Setting other messages
- (c) Spanning of message slides
- (d) Spanning for changes in ΔP
- (e) Wheel characteristics
- (f) Inside out
- (g) Flogging

25E Special methods for $\bar{\chi}_2$ limitation.

25F Special method for ab $\neq \frac{1}{2}$

25G Exhibits

25W Derivation of formulae for the weighing of evidence.

25X The number of legal wheels

25Y Proportional bulges relating to $\hat{\chi}_2$

This chapter describes all aspects of chi-breaking from cipher except the details of rectangles and flags (24). The special case of chi-breaking from key is treated separately (26).

25A THE SHORT WHEEL-BREAKING RUN

(a) General description

The basic method is the short (i.e. one-wheel) wheel-breaking run which consists essentially of choosing each character of a wheel to make the ΔD letter count, against that character, as good as possible.

Suppose for example that χ_1, χ_2, χ_3, χ_4, are known: then ΔD_1 ($= \Delta Z_1 + \Delta\chi_1$). ΔD_2, ΔD_3, ΔD_4 can be found.

ΔD_1, ΔD_2, ΔD_3, ΔD_4, ΔZ_5 (a partial de-chi) represented at each place by a single letter, may be written out in widths of 23 so that all entries in a column are against the same character of $\Delta\chi_5$.

It is expected that in ΔD /'s will be more numerous T's. Suppose that in the first column of the partial de-chi there are 6 /'s and 10 T's: then if the first character of $\Delta\chi_5$ is a dot the contribution to ΔD is 6 /'s and 10 T's; but if the first character of $\Delta\chi_5$ is a cross the contribution to ΔD is 10 /'s and 6 T's wherefore the character is more likely to be a cross than a dot.

Each character of $\Delta\chi_5$ can thus be estimated, though some may be doubtful because the numbers of /'s and T's in a column are too nearly equal. Similarly evidence is obtainable from other pairs of ΔD letters differing only in ΔD_5, e.g. it is expected that there will be more 5's than J's, more U's than Q's.

The method does not, of course, require that four χ's shall be known e.g. if only χ_1, χ_2 are known, $\Delta\chi_4$ may be found using the ΔD characteristic: $4 = 1 = 2$ is commoner than $4 \neq 1 = 2$.

Nor does it require of a $\Delta\chi_i$, regarded as known, and used to find ΔD_i, that all its characters shall be known; places on Z against unknown ('doubted') $\Delta\chi$ characters are simply ignored.

The evidence for a particular character is derived only from places against that character; and, very crudely, the evidence for a dot may be described as 'excess of good letters over bad letters' measured in the first place as so many 'pips'.

Clearly refinements are needed. Even at random ΔD letters will not all be exactly equally numerous, so that it will be necessary to have a criterion to determine whether the bulges are significantly large; and, when they are, to have a method for evaluating the evidence with some precision. (25B). Further the evidence of a wheel-breaking run may conflict with known $\Delta\chi$ characteristics, and require adjustment.

A special instance of this is that wheels must have approximately equal numbers of dots and crosses: it might seem reasonable to take as dots and crosses not those characters where 'pippages' are positive and negative, but those whose 'pippages', having regard to sign, are above and below average. The two methods should however agree, just because wheels do contain approximately equal numbers of dots and crosses. Discrepancies are due to

(1) $\bar{\chi}_1$ limitation phenomena

(2) Corruption represented by 9's

(3) Random variations.

These are the origins of the "R minus twice norm" controversy. [R4. pp 44, 54, 73, 86.]

Before considering these necessary refinements, the adaptation of 'excess of good over bad' to Colossus counting will be described. The outlines of this are desirable for understanding the sequel.

(b) <u>Adaptation to Colossus counting.</u>

To save Colossus time the excess (to revert to the earlier example) of /'s over T's is found from a single run, not by counting /'s and T's separately.

μ_i = pippage of evidence that $\Delta\chi_5^i$, the i^{th} character of $\Delta\chi_5$ is a dot

$$\left.\begin{array}{l} = /\text{'s against } \Delta\chi_5^i - \text{T's against } \Delta\chi_5^i \\ = /\text{'s against } \Delta\chi_5^i + \text{T's against other characters} \\ \qquad - \text{T's against other characters} \\ \qquad - \text{T's against } \Delta\chi_5^i \end{array}\right\} \begin{array}{l}\Delta\chi_5 \\ \text{supposed} \\ \text{all dots}\end{array}$$

= (/'s against all characters, if $\Delta\chi_5^i$ is a dot, all other characters crosses)

- (/'s against all characters, if all are crosses) (A

= (T's against all characters, if $\Delta\chi_5^i$ is a cross, all other characters dots)

- (T's against all characters, if all are dots) (A

In either A1 or A2 the first term can be found on Colossus in one run, stepping chi 5; the second term (known as the NORM) can be found on Colossus as a single count without stepping.

The two descriptions A1, A2 are equivalent. Because it seems more natural to run for good letters, the theory, including the naming of runs, is in terms of the former.

Because it is better and easier to have strings of dots on Colossus than to have strings of crosses, the actual Colossus runs are those of the latter description.

Thus it is said "Wheelbreaking runs are always run inside out on the impulse being run for".

A simple check can be applied

$$\left.\begin{aligned} \sum_i x_i &= \sum_i /\text{'s against } \Delta\chi_5^i - \sum_i \text{T's against } \Delta\chi_5^i \\ &= \text{all /'s} - \text{all T's} \\ &= (\text{all /'s} + \text{all T's}) - 2(\text{all T's}) \\ &= \text{R} - 2 \text{ norm} \end{aligned}\right\} \begin{array}{l} \Delta\chi_5 \\ \text{supposed} \\ \text{all dots} \end{array}$$

R is easily measured, being independent of $\Delta\chi_5$. The check tests not only the Colossus readings, but, also the subtractions of the norm to find the x_i.

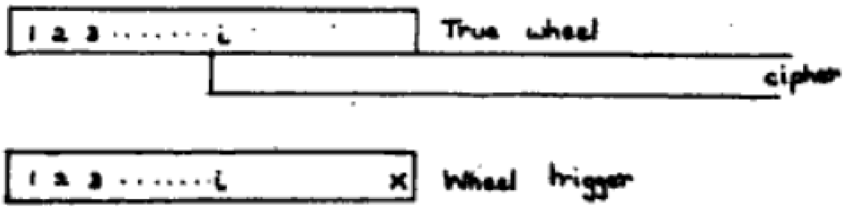
Counting T's in ΔD with each character of $\Delta\chi_5$ taken in turn to be a cross, all the others being dots, could be done, and in fact originally was done, by actually placing a cross in each position of the trigger in turn; but it is much easier to insert a cross in a fixed position (in practice the last) and allow the wheel to step.

• The characters of the wheel are produced in reverse order: (c) shows in detail why this happens.

(c) <u>Why the wheel is obtained backwards.</u>

In such a use of the Colossus wheel trigger it is necessary not to confuse the true wheel, which is of course fixed relative to the cipher, with the wheel trigger, which is deliberately stepped relative to the cipher.

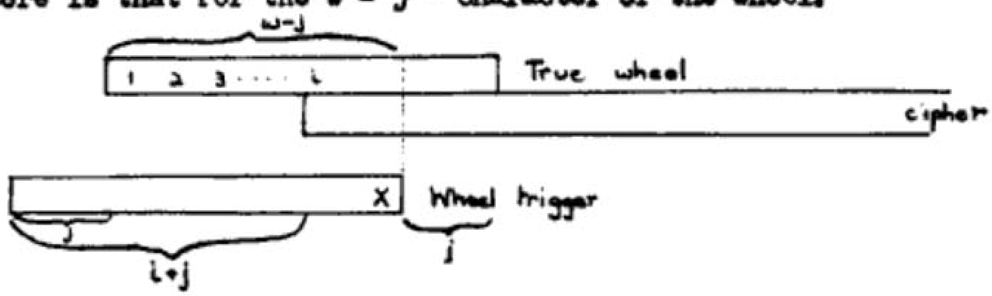
Suppose that the setting of the true wheel relative to the cipher is i.+ Consider firstly that particular position of the trigger in which its setting is also i (so that display and printer read i): true wheel and trigger now begin in the same place, thus:



The score measured in any position is for that character of the true wheel which is against the cross in the wheel trigger; in this position the last character of the true wheel.

+ i is not necessarily 01, for several messages may be used in a wheel-breaking job. The setting for the first message is naturally taken to be 01, though custom sanctions a curious inconsistency, viz. that for χ_1, χ_2 this refers to true settings; for χ_3, χ_4, χ_5, to Δ'd wheels set up on Colossus, whence the (Δ'd wheels) settings 41, 31, 01, 01, 01.

When the reading is i + j, the cipher, and therefore the true wheel also, has moved forward j places relative to the trigger, i.e. the trigger with its cross has moved backwards j places relative to the true wheel, and the score is that for the w - jth character of the wheel.



This argument depends only on relative settings and is not invalidated by the fact that deltaed wheels are set up on Colossus. Because Colossus deltas the cipher backwards, the settings recorded must be increased by one to obtain true settings, [53E]. To avoid confusion, settings appropriate to deltaed wheels are used throughout wheel-breaking, and converted only when sending messages to Ops.

(d) <u>Practical Procedure on Colossus.</u>

Count R the number of places looked at : i.e. /'s and T's

Count Norm: i.e. /'s assuming that $\Delta\chi_5$ is all crosses, measured on Colossus as T's with $\Delta\chi_5$ all dots.

Both R and norm are unaffected by stepping χ_5 , and as a check are each measured at least twice, whilst χ_5 steps.

Reset to the correct message setting: insert a cross in the last position of the χ_5 trigger, step χ_5 and start.

The frequent changes in the trigger were originally effected by pushing pins into the back of Colossus, but finally all machines used seriously for wheel-breaking were equipped with a wheel-breaking panel, on which each has a three-way switch, the three switch positions being

(i) single cross in last position

(ii) all dots

(iii) patterns as set up on panel.

(Early wheel-breaking on Robinson see R1, pp 51, 56, 86; On Colossus R1 p 96. Some suggestions not adopted R2 p 84, R4 p 26.)

25B WEIGHING THE EVIDENCE

(a) <u>Significance test.</u>

After a wheel-breaking run has been completed it is necessary to know:

whether it has any significance, and if so, to evaluate its evidence.

When no evidence other than that provided by the run itself is adduced, a condition for significance is

$$\frac{x}{\sqrt{R}} > 0.8\sqrt{\omega} + 1.2$$

where R is the number of places looked at

ω is the wheel length

x is the sum of the moduli of the scores x_i, i.e. the sum of the scores x_i ignoring their signs.

x is said to be the "score of the run on its own wheel", for if the run is so completely believed that each positive score is taken as a dot, and each negative score as a cross, the ΔD ~~double~~ bulge is the sum of the moduli.

The test is invariably used when making the initial runs for a new chi wheel.

The run is not necessarily a single run on Colossus, e.g. in attempting to obtain a $\Delta\chi_3$ knowing $\Delta\chi_1$, $\Delta\chi_2$ only, one can do all the runs,

3./1.2. , 3x/1x2. , 3x/1x2. , 3./1.2x .

and find that all fail to satisfy the test, but that if the scores, for each character, of 3./1.2. and 3x/1x2. are added, the resulting run 3+/1.2. is significant. It might otherwise be necessary to combine the three runs

3x/1.2., 3x/1x2., 3x/1x2x. Obviously the sum of the two runs will not be more significant unless there is some measure of agreement between them; and in fact it would be bad policy not to do the runs separately.

Note. It is not of course possible to add the x's of two runs to get the x of the combined run.

(b) __Fundamental decibanning formula.__

The formula for calculating the evidence of a significant short wheel-breaking run is

$$\text{decibans per pip} = 10 \log_{10} \frac{R + x^*}{R - x^*}$$

where x^* is the ΔD score on the __correct__ wheels. [25W(b) and (d)] When the scores of two or more __independent__ runs are expressed in decibans, they can be added directly.

(c) __Decibanning a run on its own wheel.__

The score of a run on its own wheel, is generally greater than on the correct wheel, cf para (b) for wherever the score against an individual character has the wrong sign, and should diminish the total score, ΔX has its sign incorrectly adjusted, so that it actually increases the score. Accordingly a table is used for the ratio

$$q = \frac{\text{expected score on the correct wheel}}{\text{score on the run's own wheel}}$$

so that decibans per pip = $10 \log_{10} \frac{R + qx}{R - qx}$

The table, whose construction is explained in 25X (e), is

$x/\sqrt{R_w}$	·798	·9	1·0	1·1	1·2	1·3	1·4	1·5	1·6	1·7	1·8	1·9	2·0	2·1
q	0	·57	·72	·82	·87	·91	·93	·95	·96	·97	·98	·98	·99	1·00

Crude decibanning is the result of taking q = 1.

A different rule is required for wheels obtained from a rectangle. [24X(e)]

(d) Decibanning a run on the wheel from another run.

Suppose, now, that a wheel has been obtained from a single run, say $\Delta\chi_3$ from /'s and that additional evidence is desired, say from 5's. The crude decibanning formula can be used, x being the score on the wheel obtained from /'s, for although this wheel is not necessarily the correct wheel, its wrong signs are unrelated to the scores for 5's, and there is no reason to suppose that the wrong signs will enhance the score.

The same remark applies to runs on another message set on these wheels, even runs for the letters used, on the first message, to make the wheel.

Moreover it is unnecessary to apply a significance test, the significance of the original run being sufficient.

The statements in this paragraph are not strictly exact [25W(f)] .

(e) Decibanning from a letter count.

When a previous approximation to a wheel is available, the usual method of decibanning for the next runs is to make a letter count (4, 8, 16 or 32) on the previous approximation. This is compact and helps one to see beforehand which runs are likely to be worth while (allowance being made for general fish characteristics): moreover runs having approximately the same decibanage per pip can be run together.

These runs, which may be numerous, will have contributed in varying degrees to the previous wheel. A table generalising that in para (c) , would b unwieldy: moreover it would necessarily use only the evidence of such messages as were set on these wheels. In fact general fish evidence cannot be ignored; for example very strong evidence would be required to justify running B's for any $\Delta\chi$. This remark about B's assumes that B's really are B's and would be invalid if it were not known which way round the wheels were [25D(f)]; or if (e.g.) $\Delta\chi_2$ were very uncertain, B's (against D's) for $\Delta\chi_5$ would not be unreasonable, because many apparent B's would in fact be 5's.

It is accordingly necessary to use judgement in choosing and decibanning runs, ignoring improbable runs, 'knocking off something' from the crude decibanage of runs already used in making the wheel, and generally exercising discretion.

'Knocking off' is needed till the wheels are almost complete and correct, when the effect becomes negligible.

Note: in decibanning U's for χ_5, for example $\frac{R+x}{R-x}$ is simply $\frac{\text{number of U's}}{\text{number of A's}}$

25C GENERAL PLAN OF WHEEL-BREAKING

(a) Typical description.

A complete wheel is comparatively rarely obtained from a single wheel-breaking run. The sort of thing to expect is more like the following. A rectangle provides incomplete $\Delta\chi_1$, $\Delta\chi_2$ wheels. Runs for $\Delta\chi_3$, $\Delta\chi_4$, $\Delta\chi_5$ are made, in an order depending on the particular fish link, until a significant one is found, say 5 = /1 = 2: this gives an incomplete $\Delta\chi_5$, using which 4 = /1 = 2 = 5 is significant for $\Delta\chi_4$. A 16 letter count indicates the most suitable runs for improving $\Delta\chi_1$, $\Delta\chi_2$, $\Delta\chi_5$, $\Delta\chi_4$ all of which are used, a fresh letter count being made whenever a wheel changes considerably. It is now possible to obtain a significant run for $\Delta\chi_3$. A 32 letter count indicates suitable runs for strengthening $\Delta\chi_3$, and another count indicates runs for improving $\Delta\chi_1$, $\Delta\chi_2$, $\Delta\chi_5$, $\Delta\chi_4$,

$\Delta\chi_3$ in turn (unless there are contradictions, it is preferable to treat wheels cyclically), and finally, perhaps after going round all wheels several times, and with the aid of methods yet to be described, all wheels are made certain.

(b) Wheel sheets.

The whole process is unmanageable unless the results at each stage are recorded systematically. This is done on five appropriately headed wheel-sheets, each containing the runs for one chi wheel.

For each run the following particulars are entered (horizontally: see exhibits).

Number of run (corresponding to that on the Colossus run sheet).

Number of messages used.

Wheels used (the various incomplete wheels are named systematically, $\Delta\chi_1 A$, $\Delta\chi_1 B$, $\Delta\chi_1 C$ e.g. on the chi 4 sheet. BB--A means that $\Delta\chi_1 B$, $\Delta\chi_2 B$, $\Delta\chi_5 A$ were used, $\Delta\chi_3$ being as yet unknown).

Spanning, limitation,.doubting, etc. (if needed).

The run used.

Decibans per pip, and/or a statement (simply PIPS) that results are entered in pips.

The score for each character (in pips or decibans).

$$\left.\begin{array}{l} R \\ x \\ \frac{x}{\sqrt{x}} \\ q \end{array}\right\}$$ generally omitted when the wheels are complete enough to use letter counts for decibanning.

Other particulars are recorded in a log book. (cf. R4 p 19.)

(c) <u>Choosing wheel-breaking runs.</u>

In setting, the break-in is usually followed by another two-wheel run. In breaking, the rectangle is NOT usually followed by another two-wheel run, i.e. a conditional rectangle, because of the time required: the neglect of conditional rectangles has perhaps been excessive. (See 24F.)

It is very easy to see that the conditions for the success of a given short run in setting and breaking are similar but not identical, for the criterion in setting is sigma-age.

The sigma-age of a wheel-breaking run on its own wheel is $\frac{x}{\sqrt{R}}$.

Significance depends on $\frac{x/\sqrt{R}}{0{\cdot}8\sqrt{w}+1{\cdot}2}$

Decibanage per pip depends on $\frac{x/\sqrt{R}}{\sqrt{w}}$

The average number of pips per character is $\frac{x}{w}$

Evidently, when there is a choice of the wheel to be run for, a weaker run for a shorter wheel may be preferable.

Because of different decibanages per pip, and the possibility that one of the component runs may be very weak there is rather more advantage than when setting in keeping run separate e.g. 5.1.2. and 5x1x2x rather than 5=1=2. If the two runs can profitably be added this is evident to the eye. (R2 p 14, but see R2 p 62.)

Once a wheel is obtained, runs to improve it are chosen with the aid of the letter count.

At all stages, resourcefulness and experience are needed to deal with abnormal cases.

(d) Some particular runs.

Wheel-breaking almost always starts from $\Delta\chi_1, \Delta\chi_2$: even if it starts from $\hat{\chi}_2$, the second wheel obtained is usually $\Delta\chi_1$.

The short runs then available are

3./1.2. 3x/1x2. 3x/1x2x 3./1.2x

4./1.2. 4x/1x2x

5./1.2. 5x/1x2x

The remaining four theoretically possible runs are generally useless.

On a particular link at a particular period some of these are better than others, but strong preferences, applied universally, seem difficult to justify, especially when, as ordinarily, the wheels may be inside out.

It is not unusual to do these runs more or less blindly till one of them is found to be significant.

The best run is generally the result of containing two of the above runs, thus obtaining 5=/1=2, 4=/1=2, 3+/1.2. (or 3+/1.2x if the wheels are inside out); indeed if the rectangle is highly significant it may save time to run them thus combined.

If χ_4 or χ_5 is obtained first, the next run is 4=5=1=2 or 4+5.1x2x.

If χ_3 is obtained first, the next run is 4+/3x1x2x.

For the fifth wheel the best letters are as in setting: to attain significance it may be necessary to combine runs. (See R3 p 131, R5 p 106.)

(e) Two-wheel convergence.

If all short wheel-breaking runs fail a conditional rectangle, which is a 2-wheel wheel-breaking run, may be used.

Alternatively it is possible to use a two-wheel convergence i.e. an alternating sequence of short wheel-breaking runs involving two unknown wheels.

Suppose that a $\Delta\chi_1$, and $\Delta\chi_2$ have been obtained, and that although there is no significant run for $\Delta\chi_3$, a few characters can be guessed. With this rudimentary $\Delta\chi_3$ a short wheel-breaking run e.g. 5JUQ may produce a $\Delta\chi_4$ wherewi a run, say 5JUQO3 produces a new $\Delta\chi_3$, whence a new $\Delta\chi_4$ and so on.

Because the characters of both $\Delta\chi_3$ and $\Delta\chi_4$ are arbitrary the significance value of $\frac{3}{\chi}$ is not 5·3 or 5·5 but approximately 8·4, as for a 3+4x/ rectangle (24X, 24Y).

This is easily overlooked, because the individual runs are short.

In particular if the runs are 4+/3x1x2x and 3+/4x1x2x, the two wheel convergence is identical with the convergence of a 3+4x/1x2x conditional rectangle. Indeed every rectangle convergence is a two-wheel convergence, as is easily seen, "taking a wheel through a rectangle" is really a short wheel-breaking run. The only advantage of an actual rectangle, apart from fact that computer time may be cheaper than Colossus time, is that it provides powerful methods, e.g. flagging, for starting the convergence. In a two wheel convergence a good start is often available from the high scorin characters of a not quite significant short run.

A popular run for two wheel convergence is 4=5=/1=2. The rectangle which fully corresponds to this is not an ordinary rectangle, but has four entries in each cell viz.

$(.\ .) - (x\ .),\ \ (.\ x) - (x\ x),\ \ (.\ .) - (.\ x),\ \ (x\ .) - (x\ x)$

where, e.g. $(.\ x)$ means $\left.\begin{matrix}\Delta Z_4 = \\ \Delta Z_5 \neq\end{matrix}\right\} \Delta D_1 = \Delta D_2$.

(R5 pp 35, 95, 96 (but the method is of course much older.))

25D PARTICULAR METHODS

(a) Doubts.

The use of incomplete wheels is unavoidable; indeed it is rarely wise to use any character, the evidence for which is less than 10 decibans. A character not assumed to be either dot or cross is said to be 'doubted': the evidence of letters of cipher against such characters is ignored ('runnin on doubted wheels'). This is effected on Colossus by means of the special pattern trigger of the wheel-breaking panel (formerly by means of trigger e the doubted characters are made crosses in the special pattern, and the condition imposed: special pattern = dot (or vice versa if the doubts are very numerous).

Evidence using letters against doubted characters is obtainable from runs not involving the chi-wheel to which the doubts belong ('running against doubts'); and may be worth while; e.g. if chi 5 is heavily doubted 4=/5=1=2 against the known characters of $\Delta\chi_5$, and 4=/1=2 against the doubted characters of $\Delta\chi_5$ are independent, and the latter is likely to be useful.

N.B. It should NOT be decibanned from the letter count against known characters.

In difficult wheel-breaking this device is used extensively.(R3 pp 13,

Doubting reduces the effective text: for example if one third of each of the four wheels is doubted, the remaining text is $(\frac{2}{3})^4$, i.e. less than one fifth of the whole.

When deciding how many characters to doubt, it is necessary to judge between the conflicting considerations of not losing too much text, and of not including too many wrong characters. 10 decibans is usually reasonable evidence for inclusion.

(b) Setting other messages (on Colossus)

That the evidence from a single message should suffice to make all wheels complete and certain is exceptional, but it will commonly make them sufficiently complete to set other messages, the addition of whose evidence, which is independent, will suffice. The addition of so much independent evidence is most effective; but rather prosaic, and apt to be unjustly neglected in favour of 'squeezing' a single message.

When there are more than a very few doubts, setting is complicated by 'variable R' e.g. if χ_3 is being set by means of 3x/1x2., χ_1 , χ_2 are fixed in the cipher, whilst χ_3 is tried in all possible 29 positions. Of the places where 1x2., the only ones looked at are those where $\Delta\chi_3$ is known and this may vary considerably when χ_3 steps. Thus a large 3x1x2. may be due to a large 1x2., which is not relevant to setting χ_3.

This is commonly circumvented by printing R, i.e. (1x2.) and the score, (3x1x2.), for all positions of χ_3, afterwards finding the sigmaa-age $\frac{x - R/2}{\frac{1}{2}\sqrt{R}}$ for promising scores.

A preferred modification which reduces useless printing is to run simultaneously, on two counters: 3x/1x2. with a high set total; 3./1x2. with a low set total, (with SIP if available). If the bulge of 3x/1x2. over 3./1x2. is significant, one score or the other must be printed. To consider only scores too large to be explained by random variations in R^{+} throws away evidence, for in fact R can be found at each setting; but in long subsequent runs such as 4=5=/1=2 it may be necessary to consider only scores which are reasonably good on this basis. In a break-in run, as a little consideration will show, the variation of R is usually negligible.

When two messages have each produced a wheel (generally from a rectangle, or especially, $\hat{\chi}_2$) these can be set by a direct comparison of the (incomplete) wheels. See 24Y(c) R1 pp 53, 76, 79, 83, 97; R2 p 29.
For application of corrected excess to wrongly set messages (never used) R3 p 91

(c) <u>Spanning for message slides.</u>

This is particularly important in wheel-breaking: as soon as the rectangle message is on Colossus the 1+2/ score is checked and spanned. If a message slide is found, the remainder of the message is set by slide runs (23F(d)) after which the tape may be doctored so that its parts are in the correct relative position.

Every supporting message set should at once be spanned and possibly doctored.

Doctoring requires only the removal or insertion of sprocket holes. A hole is quickly removed by covering it with opaque paper. Inserting a hole is done by copying and takes time; meanwhile wheel-breaking should proceed on a slide - free portion: if this portion is most of the message, doctoring may be not worth while.

Note. To decide whether to remove or insert a hole imagine that each place on the tape is marked with the corresponding position of (say) chi 1

04	05	06	07	08	09	10	setting before slide 04
06	07	08	09	10	11	12	setting after slide 06

slide here

07, 08 are missing, wherefore two holes must be <u>inserted</u>.

(d) <u>Spanning for changes in ΔP characteristics.</u>

The character of P and hence of ΔP may change considerably during the same 'message' (meaning transmission or QEP), for it may contain several messages, possibly from different originators; hand passages, tables of figures, list of names, etc. will have abnormal characteristics.

+ The standard deviation for this is $\sqrt{Np(1-p)q(1-q)}$, for the meaning of which (21(n); R4 p4,11,12,17.)

It may well happen for example, that in one part of a message 8's are more numerous than 5's, whilst in the rest 5's are more numerous than 8's. Evidently more evidence is obtained by spanning the parts separately. This however take twice the time and is not done unless there is difficulty in completing the wheels, or in making them certain. (R5 p 11.)

(e) <u>Wheel characteristics.</u>

Restrictions on permissible chi wheels have been mentioned (11C). Wheels which conform are said to be legal. Any deltaed wheels must have an even number of crosses, and for legality both Δ'd and un- Δ'd wheels must have, as nearly as possible, equal numbers of dots and crosses. For the five wheels the number of crosses is:

Δ	20	16	14	12 or 14	12
un-Δ	20 or 21	15 or 16	14 or 15	13	11 or 12

The final form of legality forbade more than four consecutive like characters in the un- Δ wheel, i.e. more than three consecutive dots in the Δ'd wheel.

If most characters are certain on the evidence from wheel-breaking runs the requirement of legality may suffice to complete the wheels: various tri have been devised for doing this easily.

$\Delta\chi_5$ · x · x · x · · x · · · x · x x x x · · · x x x ·

is legal because (i) it has 12 crosses

(ii) if the 12 crosses are paired as indicated there are 6 dots inside the pairs, as nearly as possible half the 11 dots.

Integrating,

$\Delta\chi_5$ · x · x · x · · x · · · x · x x x x · · · x x x ·

χ_5 · · x x · · x x x · · · x x · x · x x x · x · 12 crosses

The underlining of three characters indicates, conventionally, that they are doubtful; the first and second of these cannot be interchanged, for if they were the characters of chi 5 between them would be changed in sign, increasing the number of crosses to 13. Similarly the first and third of these can be interchanged.

At an early stage in wheel-breaking it may be justifiable to accept rather weak scoring characters which interrupt what would otherwise be long strings of dots. Of course until it is known which way round (25D(F)) the if there were many weak characters.

The following paragraphs enumerate methods which can be used in difficult cases to make wheels complete and certain.

1. Set all messages, with flogging.
2. Make sure that all wheel-breaking runs for each chi not yet certain have been done using the latest wheels for the other four chis, and that the decibanning is on the basis of these wheels: if the wheels are nearly correct, crude decibanning is permissible.
3. Do a 32-letter count against each doubtful character, and deciban it on the 32-letter count for the whole wheel. This is equivalent to doing every possible short wheel-breaking run separately, but saves time by considering only uncertain characters. It is done easily on Colossus by putting a single pin in the special pattern trigger, and plugging special pattern = cross.
4. Span all messages, looking for slides [25D(c)] and changes in Δ P characteristics [25D(d)]
5. Make a temperate use of wheel characteristics.
6. Make a provisional de-chi on uncertain wheels for Room 41 where it can be treated by non-statistical methods. In an extreme case de-chi on

four wheels only.

7. Span /'s on ΔD on a hundred letters immedately before each autopause with faint hope that ΔZ is really Δ key, the P tape of the German Tunny machine having broken. (R5 pp 70, 80)

8. In one instance wheel-breaking was completed because there was a crib into a message already set on four chis: the ordinary crib run failed because of a slide, but running $\Delta P_{1,2,4,5}$ against $\Delta D_{1,2,4,5}$, and looking for /'s in $\Delta\Psi'_{1,2,4,5}$ succeeded.

25E SPECIAL METHODS FOR $\bar{\chi}_2$ LIMITATION

(a) Running against $\bar{\chi}_2$ crosses.

Because the bulges of runs against $\bar{\chi}_2$ = x are so much greater than against $\bar{\chi}_2$ = ., these are made separately (as in setting), and indeed it is rarely worth while to do runs against $\bar{\chi}_2$ = ., and then only for good motor cross letters (R3 p 101).

<u>(b) Runs for $\Delta\chi_2$ and $\bar{\chi}_2$</u>

In a run for $\Delta\chi_2$ however, the scores for all characters of $\Delta\chi_2$ will appear, those where $\bar{\chi}_2$ = x scoring strongly, those where $\bar{\chi}_2$ = . weakly, so that the run provides two types of evidence:

(i) high and low scores indicate $\bar{\chi}_2$ = x and . ,

(ii) positive and negative scores indicate $\Delta\chi_2$ = . and x ,

moreover the $\bar{\chi}_2$, and $\Delta\chi_2$ obtained by differencing, must be consistent.

Scores against $\bar{\chi}_2$ = x and $\bar{\chi}_2$ = . must be decibanned separately, the result of which is usually that scores against $\bar{\chi}_2$ = . are found to be negligible. Until a complete χ_2 can be found the best plan is to ignore all but strong characters.

<u>(c) "Working out the limitation".</u>

It is often possible to find a complete or nearly complete χ_2 at an early stage, even straight from the rectangle. It is justifiable to assume $\bar{\chi}_2$ limitation if there are many high scores and many low scores for $\Delta\chi_2$ characters, but few moderate ones.

An easy example of this is:

Scores for part of $\Delta\chi_2$ 9 27 12 5 15 30 1 41 36 - 2

It is reasonable to suppose that 27, 30, 41, 36, 51 are $\bar{\chi}_2$ crosses and here $\Delta\chi_2$ is reliable. It is reasonable to suppose that 9, 5, 1, -2, are $\bar{\chi}_2$ dots, and here $\Delta\chi_2$ is uncertain.

$\Delta\chi_2$			·				·		·	X	
χ_2	·	X		·		X		X	X	·	·

It will be seen that the differencing is always wrong so that $\Delta\chi_2$ must be inside out. For clarity the scores will be written with the signs changed.

		9	27	12	5	15	30	1	41	36	-	2
$\Delta\chi_2$			X				X		X	·		
χ_2	·	X		·		X	·	X	X	·	·	

Here differencing enables additional characters to be inserted.

$\Delta\chi_2$	X	·	X			X	X	·	X	·	
χ_2	·	X	X	·		X	·	X	X	·	·

Because the 5 is a $\bar{\chi}_2$ cross, it probably gives the right sign for $\Delta\chi_2$ whe

$\Delta\chi_2$	X	·	X	·	X	X	X	·	X	·	
χ_2	·	X	X	·	·	X	·	X	X	·	·

the scores opposite the 5 being obtained by differencing.

If such methods leave only a few doubts, wheel characteristics may solve them.

In marginal cases the difficulty is that the highest $\bar{\chi}_2$ dot scores and the lowest $\bar{\chi}_2$ cross scores may be confused, so that the evidence appears to be conflicting.

The same methods can be used when making chi 2 certain but moderately scor characters can be tricky because the decibannage for a character depends on whether it is taken as a $\bar{\chi}_2$ cross or a $\bar{\chi}_2$ dot. A more precise formulation is given in R4 p 57 sqq. Whilst the wheel-breaker is cerebrating, all available runs should be done, for if each supposed $\bar{\chi}_2$ cross scores 40 decibans more than any supposed $\bar{\chi}_2$ dot, even when the latter is decibanned as though it were a $\bar{\chi}_2$ cross, the wheel is certain. For decibanning R3 p 42, R 4 pp 57, 104, R 5 p 65.

(d) <u>The four-letter count.</u>

As in setting, [23E(h)] a 4-letter count for ΔD_1, ΔD_2 against $\bar{\chi}_2$ crosses, provides some evidence for the sort of ΔP to be expected. On the whole text there is no bulge of x x over . ., or vice versa [22H(f)], the bulge against $\bar{\chi}_2$ dots being equal and opposite to that against $\bar{\chi}_2$ crosses;

but at an early stage in wheel-breaking, so many of the $\Delta\chi_2$ characters against $\bar{\chi}_2$ dots may be wrong that even on the whole text a significant bulge will appear. This will not occur with other limitations and provides additional evidence that the limitation is $\bar{\chi}_2$.

(e) $\underline{\hat{\chi}_2}$.

From a $\bar{\chi}_2$ limitation message, it is sometimes possible to break wheels without a rectangle. This depends on $\Delta\chi_2 + \bar{\chi}_2$, usually written $\hat{\chi}_2$. (22A(b), 22D(g)), which has of course a definite value at each position of the chi 2 wheel.

Proportional bulge of ($\Delta Z_2 + \hat{\chi}_2 = .$) = $p\pi_x$

where π_x is the P.B. of $\Delta P_2 = x$ [22H9]

So that if π_x is great enough $\hat{\chi}_2$ may be found from the short wheel-breaking run $\hat{\chi}_2 + \Delta Z_2 = x$, the condition for significance being as usual

$\frac{x}{\sqrt{k}} > 5{\cdot}7$. (R1 p 11, R4 pp 70, 92, R5 p 9.)

This run is made systematically on A-tapes [33A(c)] of links likely to use $\bar{\chi}_2$ limitation, both on the whole text; and also, in order to detect slides, on thirds. Corruption 9's spuriously enhance the score, so that NOT 99 must be used.

(f) Runs to follow $\hat{\chi}_2$

Unfortunately it commonly happens that although the $\hat{\chi}_2$ run is genuinely significant it is impossible to proceed further.

The strongest run to follow $\hat{\chi}_2$ is usually (R5 pp 8,11,17,28; 25Y4)

$\Delta\chi_1 + /\Delta Z_1 + \Delta Z_2 + \hat{\chi}_2 = \cdot$ whose proportional bulge is

$$p(1-p)\frac{\pi_{\cdot\cdot} + \pi_{xx}}{2}$$

The ratio of this to the proportional bulge of $\hat{\chi}_2$ is

$$(1-p)\frac{\pi_{\cdot\cdot} + \pi_{xx}}{2\pi_x}$$

which is often considerably less than unity (R5 p 108).

Statistics (R5 pp 98,105,106) show that wheel-breaking from a $\hat{\chi}_2$ start rarely succeeds unless $\frac{x}{\sqrt{N}} > 7$.

Having a significant $\hat{\chi}_2$ the best policy seems to be to set all available messages on $\hat{\chi}_2$ (a one-wheel run), not forgetting to span for message slides, strengthening $\hat{\chi}_2$, and then trying the wheel-breaking run $\Delta\chi_1 + /\Delta Z_1 + \Delta Z_2 + \hat{\chi}_2 = \cdot$ on each message set. When a $\Delta\chi_1$ is obtained the next run 2+/1 is $\Delta\chi_2 + \Delta Z_2 + \Delta\chi_1 + \Delta\chi_2 = \cdot$ after which ordinary runs are possible.

It is sometimes possible to integrate $\hat{\chi}_2$ i.e. to find χ_2 directly from $\hat{\chi}_2$, either as a whole, if $\hat{\chi}_2$ is nearly complete, otherwise in stretches: in the latter case the ambiguities are apt to make the method of doubtful value (See also 26)

It is believed that Jellyfish 4/3/45, broken on $\hat{\chi}_2$, could not have been broken otherwise, (R5 p 52) but ordinarily the advantage of $\hat{\chi}_2$ over a rectangle is speed. $\hat{\chi}_2$ is perhaps, most useful as an ancillary method, detecti slides in rectangles, setting rectangles on χ_2 , providing a start for convergence, strengthening marginally significant rectangles, acting as a check on dubious characters in χ_2 , ($\bar{\chi}_2, \Delta\chi_2$ must satisfy $\bar{\chi}_2 + \Delta\chi_2 = \hat{\chi}_2$).

<u>(g) Excess of dot or cross in $\hat{\chi}_2$</u>

The number of dots and crosses in $\hat{\chi}_2$ may be very far from equal: if the proportional bulge of dots is θ , then $\Delta Z_2 = \cdot$, which can be counted in one operation, has a proportional bulge $\theta\beta\pi_\chi$(25Y1): this has been suggested as a significance test; but it is really more profitable to do $\hat{\chi}_2$ properly, for it takes very little time.

<u>(h) $\bar{\chi}_2 + \bar{\bar{P}}_5$ limitation.</u>

Because P_5 tends to be dot, this exhibits weakly the characteristics of $\bar{\chi}_2$ limitation; but insufficiently to do more than justify separate decibanning against $\bar{\chi}_2$ cross and $\bar{\chi}_2$ dot, both being used. The ΔD letter 5 is peculiar in scoring better against $\bar{\chi}_2$ dot than against $\bar{\chi}_2$ cross. [22H(d)] (R3 pp 10, 59.)

25F SPECIAL METHOD FOR ab$\neq \frac{1}{2}$

$$\text{PB}\ (\Delta D_i = \ .) = \text{PB}\ (\Delta\Psi'_i + \Delta P_i = \ .\ )$$
$$= \beta'_i \ \pi_i$$

where β'_i is the proportional bulge of $\Delta\Psi' = .$, so that if ab $\neq \frac{1}{2}$, single wheel initial χ - breaking runs are possible.

The resultant wheel is of course a true $\Delta\chi$ wheel and not a horrid hybrid like $\hat{\chi}_2$.

The rule ab = $\frac{1}{2}$ was introduced in March 1942. In one later instance the limitation on a machine used by the Stickleback link became inoperative; this in effect doubled the motor dottage, making ab $\neq$ $\frac{1}{2}$ and $\beta'_i = \beta$.

25G WHEEL-BREAKING EXHIBITS

MB 2005 Run 1
WHaa---
41 31 - - -

1p2. 2177
1p2x 1472   et 3649
dh 705 £ 60.6 11.6£
span in 2oo's

0096	
0057	
	0093
	0060
0076	
0077	
	0106
	0050
0090	
0064	
	0082
	0069
0090	
0063	
	0093
	0061
0091	
0063	
	0090
	0062
0086	
0069	
	0058
	0045
0097	
0057	
0082	
0069	
0087	
0067	
[illegible]	

These consist of the wheel-sheets and most of the Colossus sheets of Mullet 25/4; and some miscellaneous exhibits. Mullet 25/4 is rather easier and more straightforward than the average wheel-breaking job. The margins of Colossus sheets have been drastically reduced.

(a) <u>The rectangle</u> (ch 24)

This was evidently a Garbo rectangle (24B(c)), but the Garbage is not preserved. At bottom right is the 9 x 9 flag and its convergence, used as a start for converging the rectangle (24D(c). When converged the rectangle is easily significant; the 1 + 2 double bulge is 758 (or 759), 615 being sufficient according to the crude computery test; the leading term of significance test IV (24E(d)) is 258, so that it is unnecessary to calculate the $\mathfrak{J}$ terms. Raw means made from a raw tape. (33B).

(b) <u>Checks on Colossus</u>

The rectangle wheels, $\Delta\chi_1$, $\Delta\chi_2$ with low-scoring characters doubted (25D(a)), are set up on Colossus (wheels AA---, Figs II, III) and the scor is checked: doubting reduces the double bulge to 705. The message is spanned (run 1) in 200's for possible message slides: none is found. The two readings in each pair are 1 + 2 = . , 1 + 2 = x .

(c) <u>Initial runs for $\Delta\chi_5$, $\Delta\chi_4$</u>

The first short run is C2, 5 = /1 = 2. It is just significant (25B(a)): x/σ = 5·1. Note the check Σx_i = r - 2xnorm with a discrepancy of 2. The pencilled figures are the pippages (25A for the various characters, i.e. score minus norm. The wheel $\Delta\chi_5 A$, heavily doubted, is set up (Fig VI). A bold run, 4 = /5 = 1 = 2, for χ_4 is comfortably

0097
0054

0100
0052

0092
0066

0093
0060

0097
0058

0103
0048

0090
0063

0084
0068

0093
0062

A bold run, 4 = /5 = 1 = 2, ~~form~~ χ_4 is comfortably significant producing wheel $\Delta\chi_4 R$. (Fig V).

2 o2 r 2177 a 1082
2164
13

k5
o1 a 1088 6
o2 a 1069 13
o3 a 1074 9
o4 a 1085 3
o5 a 1105 23
o6 a 1080 2
o7 a 1088 6
o8 a 1077 5
o a 1056 26
1o a 1069 13
11 a 1093 11
12 a 1073 9
13 a 1092 10
14 a 1097 15
15 a 1095 13
16 a 1072 10
17 a 1099 17
18 a 1079 3
1 a 1090 8
2o a 1092 10
21 a 1076 6
22 a 1084 2
23 a 1064 18

This is the calculation of r-2nam

This is the calculation of Σx

+124
−113
+11

X = 237

NTR = 5·1

3 o3 r 715 a 356
k4 712 3
o1 a 0362 14
o2 a 0361 5
o3 a 0361 5
o4 a 0349 7
o5 a 0357 1
o6 a 0342 14
o7 a 0363 7
o8 a 0349 7
o9 a 0350 6
1o a 0367 11
11 a 0354 2
12 a 0361 5
13 a 0365 9
14 a 0347 9
15 a 0359 3
16 a 0351 5
17 a 0346 10
18 a 0352 4
19 a 0361 5
2o a 0347 9
21 a 0354 2
22 a 0359 3
23 a 0359 3
24 a 0352 4
25 a 0370 14
26 a 0363 7

+84
−79
+5

X = 161

NTR = 6.

4 mb 2005
41,31,-,ol,ol
AA_AA

X5

0096 2 6
0052
0063
0056

0040
0038
0043
0051

0043
0056

120

5588
5 r 29
k5
ol a o
o2 a
o3 a o
o4 a o
o5 a o
o6 a o
o7 a o
o8 a o
o a oI
o a ol
11 a o
12 a
13 a
14 a

0056 13
0120 19 $3 \cdot 2.$ $\left(18.\ 10 \log_{10} \frac{120}{58}\right)$
0058 M1

0033 LP
0048 1H
0046 RC
0038 VG

14 a
15 a o
16 a o
17 a
18 a
1 a o
20 a o
21 a o
22 a o
23 a

(d) Sixteen-letter counts

A 16-letter count is made on wheel
and deciban runs to improve $\Delta\chi_5$ (25B(d)
The pencilled letters at the right indi
wheels are inside out (25D(f)); but it

Runs (5) (6) are entered in pips or
wheel sheet (Fig VI).

$\Delta\chi_5 B$ is a great improvement. A f
runs for $\Delta\chi_4$. The suspicion that the

8 55588 r 525 n 256
k4
~~o1 a o256~~ +13
k4
7 mb 2oo5
AA_AB

χ_4

o14o	2·8	o1 a o257 (1)
oo66		o2 a o262 (6)
AU o1o5	2·0	o3 a o259 (3)
oo73		o4 a o249 7
		o5 a o253 3
		o6 a o245 11
oo48		o7 a o263 (9)
oo57		o8 a o247 9
oo66		o9 a o25o 6
oo61		1o a o265 (9)

+79
-66
+13

0061

0083
0073
56 0170) 3 7
0075

0066
0063
0067
0070

10 a 0265 9 +15
11 a 0259 3
12 a 0256 -
13 a 0265 9
14 a 0256 -
15 a 0260 4
16 a 0250 6
17 a 0249 7
18 a 0257 1
19 a 0258 2
20 a 0250 6
21 a 0255 1
22 a 0253 3
23 a 0258 2
24 a 0249 7
25 a 0273 17
26 a 0271 15

MB 2005

16 l.c.

WH -AA-BB et 2675

41 31 - el el

/(90255 χ_5 2·1

ht o155

om o225 1·95

n3 o144

re o120

vg o157

lp o130

14 o140

au o188

qv o163

58 o300 3·0

kj o150

L3 df o128

? 14 xb o140

AC zy o152

√a se o148

12 55888 r 548 263

k5

o1 a o256 7

o2 a o270 7

o3 a o258

o4 a o267 4

o5 a o277 14

o6 a o256 7

o7 a o273 10

o8 a o257 6

o a o255 10

1o a o255 10

11 a o266 3

12 a o256 7

13 a o278 15

14 a o272 9

15 a o276 13

16 a o256 7

17 a o273 10

18 a o266 3

1 a o270 7

2o a o259 4

21 a o263 –

22 a o264 1

23 a o249 14

+19 -17 +19

13 //990oomm r 940 n 462

k5

o1 a o458 4

o2 a o475 13

o3 a o457 5

o4 a o471 9

o5 a o468 6

o6 a o464 2

o7 a o468 6

o8 a o453 9

o a o450 12

1o a o452 10

11 a o467 5

12 a o448 14

13 a o474 13

14 a o470 8

15 a o471 9

16 a o456 6

17 a o457 5

18 a o470 8

1 a o478 16

2o a o449 13

21 a o449 13

22 a o485 23

23 a o457 11

+117 +8

(e) $\Delta\chi_5$ made certain

Run (11) is yet another 16-letter count, followed by runs (12) (13) for $\Delta\chi_5$ yielding a nameless wheel having 12 dots (instead of 11), the weakest character being 19 decibans up, so that in view of other evidence, reversal seems inevitable, and on this assumption $\Delta\chi_5 C$ is 47 decibans up and therefore "certain". (25D(g)). Characters 13, 18 cannot be interchanged (cf 25D(e)).

(f) Unsuccessful attempt to get a $\Delta\chi_3$. Run (14) evidently made on reversed wheels

(g) Wheels reversed

After reversing the wheels a letter count is made to select runs for improving $\Delta\chi_2$ and $\Delta\chi_1$, viz (16) - (21).

KD4

to select runs for improving Δx_2 and Δx_1, viz (16) - (21).

14 ///

r ~~xxx~~ 365 n 178

k3

o1 a o175 3
o2 a o180 (2)
o3 a o177 1
o4 a o176 2
o5 a o177 1
o6 a o174 4
o7 a o181 (3)
o8 a o179 (1)
o9 a o174 4
1o a o178 1
11 a o181 (3)
12 a o179 (1)
13 a o172 6
14 a o179 (1)
15 a o179 (1)
16 a o187 (9)
17 a o175 3
18 a o188 (9)
19 a o177 1
2o a o179 (1)
21 a o183 (5)
22 a o176 2
23 a o181 (3)
24 a o180 (2)
25 a o183 (5)
26 a o177 1
27 a o173 5
28 a o172 6
29 a o179 (1)

MB 2005 (15)

41, 31, -, 01, 01

16 L C.

WH ~~xxx~~ bb-oo
et 3228

	X_2	X_1
o365	3.5	3.5
o188	1.0	
o235	1.5	1.8
o196		
RC o180		
VG o167		
LD o147		
14 o161		
o276	2.0	2.3
o173		
o310	3.0	2.6
o188		
o166		
o154		
o160		
o162		

1102

16 o3 r ~~1091~~ n 551

k2

~~31 a o543~~ 12 ~~15~~
d1 a o567 (16)
o2 a o537 14
o3 a o566 (15)
o4 a o540 11
~~o5 a o564~~ (15)
o6 a o566 (15)
o7 a o537 14
o8 a o558 (7)
o9 a o569 (18)
~~1o a o527~~ 24
11 a o547 4
12 a o536 15
13 a o539 12
14 a o569 (18)
~~15 a o534~~ 17
16 a o564 (13)
17 a o565 (14)
18 a o534 17
19 a o560 (9)
~~2o a o532~~ (1)
21 a o567 (16)
22 a o539 12
23 a o568 (17)
24 a o550 1
~~25 a o536~~ 15
26 a o570 (19)
27 a o536 15
28 a o541 10
29 a o546 5
30 a o544 7

203
191
-12

504

17 uuu r 482 n

12

k2

~~31 a o248~~ 4
o1 a o254 (2)
o2 a o249 3
o3 a o257 (5)
o4 a o247 5
~~o5 a o253~~ (1)
o6 a o250 2
o7 a o248 4
o8 a o256 (4)
o9 a o266 (14)
~~1o a o258~~ (6)
11 a o243 ~~(2)~~ 9
12 a o244 (2)
13 a o250 2
14 a o257 (5)
~~15 a o250~~ 2
16 a o257 (5)
17 a o253 (1)
18 a o242 10
19 a o260 (8)
2o a o260 (8)
~~21 a o253~~ (1)
22 a o246 6
23 a o253 (1)
24 a o253 (1)
25 a o246 6
~~26 a o255~~ (3)
27 a o244 8
28 a o242 10
29 a o247 5
30 a o248 4

20

1?? ooo mmmm r 444 n 22'

4 4.5

k2
31 a 0220 3
01 a 022? 5
02 a 0220 3
03 a 0219 4
04 a 0221 2
05 a 0224 1
06 a 0227 4
07 a 0220 3
08 a 0231 8
09 a 0222 1
10 a 0215 8
11 a 0221 2
12 a 0223 1
13 a 0214 9
14 a 021? 5

1195 n ~~5?? kl~~ 5

kl
41 a 0589
01 a 0603
02 a 0595
03 a 0606
04 a 058?
05 a 061? 10 19
06 a 0608 20 9
07 a 0594 6 5
08 a 0611 23 17
09 a 0610 22 11
10 a 0595 4
11 a 0592 7
12 a 0602 14 3
13 a 0612 24 13
14 a 059? 19 1
15 a 0597 9 2
16 a 0608 9

14 a 021[illegible]	5
15 a 0220	3
16 a 0226	3
17 a 0227	4
18 a 0223	–
19 a 0226	3
20 a 0218	5
21 a 0224	1
22 a 0225	2
23 a 0225	2
24 a 0230	7
25 a 0228	5
26 a 0231	8
27 a 0223	–
28 a 0218	5
29 a 0224	1
30 a 0220	3

57
5

16 a 0606	[illegible]	[illegible]
17 a 0603	15	4
18 a 0608	20	9
19 a 0594	6	5
20 a 0592	[illegible]	7
21 a 0589	[illegible]	10
22 a 0591	3	8
23 a 0606		7
24 a 0589		10
25 a 0613		14
26 a 0603		4
27 a 0595		4
28 a 0600		1
29 a 0587		12
30 a 0611		12
31 a 0590	9	
32 a 0607	8	
33 a 0587	12	
34 a 0596	3	
35 a 0596	3	
36 a 0607	8	
37 a 0594	5	
38 a 0588	11	
39 a 0598	1	
40 a 0585	14	

15
+15

22 mb 2005 41,31,[illegible],01,01

C	χ_4
0441	245
0219	
0271	0.9.
0226	
0228	
0207	
0184	
0202	
0335	2.3
0215	
0365	2.3
0197	
0215	
0182	
0210	
0183	

(h) $\Delta\chi_4$ made certain

Run 22 is used runs for $\Delta\chi_4$ viz 23, which suffice to make

22 24 aauu5588 r 1243 n 611

k4
01 a 0598 13
02 a 0593 14
03 a 0599 12
04 a 0628 (17)
05 a 0623 (12)
06 a 0620 (9)
07 a 0593 18
08 a 0618 (2)
09 a 0612 (1)
10 a 0600 11
11 a 0618 (3) (5)
12 a 0626 (15)
13 a 0608 3
14 a 0618 (7)
15 a 0589 7
16 a 0616 (5)
17 a 0626 (6)
18 a 0622 (11)
19 a 0600 11
20 a 0636 (25)
21 a 0628 (7)
22 a 0610 1
23 a 0601 10
24 a 0626 (15)
25 a 0595 16
26 a 0602 9

1222
+19

144
163
+19

25 ooo mmm r 555 n 262

k4
01 a 0263 (1)
02 a 0264 (9)
03 a 0262 -
04 a 0265 (3)
05 a 0269 (7)
06 a 0271 (9)
07 a 0261 1
08 a 0260 2
09 a 0265 (3)
10 a 0266 (8)
11 a 0257 5
12 a 0264 (2)
13 a 0261 1
14 a 0266 (4)
15 a 0260 2
16 a 0272 (10)
17 a 0261 1
18 a 0259 3
19 a 026 2
20 a 0265 (3)
21 a 0267 (5)
22 a 0255 1
23 a 0259 3
24 a 0268 (6)
25 a 0255 2
26 a 0268 (6)

524
31

+65

496
478
18

447
480

x=102

34
31

$\frac{x}{\sqrt{R}}=4.6$

21 a 241
22 a 237

26

/////

k3
01 a 0233 6
2 a 0240 (1)
03 a 0242
04 a 0241
05 a 0242
06 a 0236 3
07 a 0246
08 a 0244 (5)
09 a 0239
10 a 0236
11 a 0244 (5)
12 a 0241
13 a 0235
14 a 0242
15 a 0245
16 a 0244
17 a 0239
18 a 0246 (7)
19 a 0239
20 a 0237 2
22 a 0234 (2)
23 a 0241 2
24 a 0239
25 a 0245
26 a 0239
27 a 0233
28 a 0232 7
29 a 0240

(x) A partial $\Delta\chi_3$ obtained

Runs (26), (27), (28), (29) are made for $\Delta\chi_3$, only (28) has $x/\sqrt{R} > 5\cdot5$, the condition for significance. From the table in 25B(c), this is found to be worth 2·5 decibans per pip; and from it wheel $\Delta\chi_3{}^A$ is constructed.

27
5555 R 399 NM186

k3
o1 a o189 3
o2 a o19o 4
o3 a o187 1
o4 a o18o 5
o5 a o181 5
o6 a o184 2
o7 a o188 2
o8 a o188 4
o9 a o181 5
1o a o185 1
11 a o187 1
12 a o19o 4
13 a o188 3
a 1192 6
15 a o189 3
16 a o189 3
17 a o184 2
18 a o189 3
19 a o189 3
2o a o189 3
21 a o185 1
22 a o19o 4
23 a o186 -
24 a o187 1
25 a o187 1
26 a o191 5
27 a o182 4
28 a o186 -
29 a o188 2

53
26
27

X = 79

$\frac{X}{\sqrt{R}} = 3.8$

UUU
R 368 NM 191 28

k3
o1 a o185 6
o2 a o194 3
o3 a o188 3
o4 a o193 2
o5 a o195 4
o6 a o185 6
o7 a o193 2
o8 a o193 2
o9 a o189 2
1o a o183 8
11 a o186 5
12 a o2oo 9
13 a o185 6
14 a o197 1
15 a o194 3
16 a o189 2
17 a o181 10
18 a o195 4
19 a o195 4
2o a o187 4
21 a o185 6
22 a o193 2
23 a o192 1
24 a o191 -
25 a o192 1
26 a o192 1
27 a o185 6
28 a o19o 1
29 k3o195 4

392
368
114

65
48+
17

X = 113

$\frac{X}{\sqrt{R}} = 5.9$

fff
R 247 NM 1o8

k3
29 a o11o 2
o1 a o111 3
o2 a o1o9 1
o3 a o1o9 1
o4 a o11o 2
o5 a o1o7 1
o6 a o1o7 1
o7 a o111 3
o8 a o1o4 4
o9 a o11o 2
1o a o111 3
11 a o118 10
12 a o1o6 2
13 a o11o 2
14 a o1o2 6
15 a o1o8 -
16 a o11o 2
17 a o111 3
18 a o111 3
19 a o1o5 3
2o a o1o4 4
21 a o1o8 -
22 a o1o8 -
23 a o113 5
24 a o11o 2
25 a o111 3
26 a o1o8 -
27 a o1o9 1
28 a o112 4

5
2
3

ccadc

no.31

0110		JJSSYY00
90066		
0049		
0041		P 980 NM 475
0061	1.1	k3
0051		01 a 0467 2
0048		02 a 0479 4
0052		03 a 0473 2
		04 a 0474
0047		05 a 0482 7
0050		06 a 0476 1
0049		07 a 0484 G
0055		08 a 0475 -
		09 a 0470 5
0048		10 a 0473 2
0034		11 a 0476 1

0034		11 a 0476 1
0047		12 a 0476 1
0043	JSYO	13 a 0466 9
		14 a 0480 5
0040		15 a 0470 5
0111		16 a 0478 3
0040		17 a 0474 1
0054		18 a 0481 6
		19 a 0489 14
0078		20 a 0486 11
0065		21 a 0466 9
0036		22 a 0487 12
0050	1·3	23 a 0477 2
		24 a 0472 3
0056		25 a 0471 4
0039		26 a 0482 7
0042		27 a 0466 9
0039		28 a 0477 2
		29 a 0479 4
0036	1·3	
0052		
0039	1·2	
0029		

91

50

41

(j) Runs to improve $\Delta\chi_3$: redecibanning

A 32-letter count is used to choose runs to improve $\Delta\chi_3$, and, more especially, to deciban the runs (26), (27), (29) already made, so that they appear twice on the wheel-sheet, entered firstly in pips, and then in decibans. Actually JSYO is the only new run, but $\Delta\chi_3 B$ is a great improvement on $\Delta\chi_3 A$, and a further letter count, numbered (32), suggests additional runs as well as redecibanning (27) a second time.

36

///UUU

R 851 NM 433

k1
20 a 0440
21 a 0439
22 a 0426
23 a 0437
24 a 0427
25 a 0438
26 a 0434
27 a 0421
28 a 0440
29 a 0434
30 a 0436
31 a 0420
32 a 0435
33 a 0441
34 a 0439
35 a 0430
36 a 0443
37 a 0442
38 a 0432
39 a 0426
40 a 0429
41 a 0428
01 a 0423
02 a 0441
03 a 0431
04 a 0435
05 a 0431
06 a 0425
07 a 0435
08 a 0424
09 a 0436
10 a 0437

+151
-11

37

AAA555

R 833 NM 412.
814
9

k1
20 a 0412
21 a 0421
22 a 0414
23 a 0416
24 a 0405
25 a 0418
26 a 0415
27 a 0402
28 a 0415
29 a 0418
30 a 0415
31 a 0408
32 a 0417
33 a 0413
34 a 0413
35 a 0402
36 a 0408
37 a 0415
38 a 0418
39 a 0424
40 a 0401
41 a 0414
01 a 0411
02 a 0405
03 a 0410
04 a 0411
05 a 0416
06 a 0407
07 a 0409
08 a 0412
09 a 0412

38

000QQQ888

R 1119 NM 538

k1
20 a 0542
21 a 0540
22 a 0527
23 a 0537
24 a 0542
25 a 0546
26 a 0539
27 a 0535
28 a 0544
29 a 0542
30 a 0547
31 a 0529
32 a 0539
33 a 0536
34 a 0547
35 a 0538
36 a 0557
37 a 0542
38 a 0542
39 a 0537
40 a 0535
41 a 0535
01 a 0533
02 a 0538
03 a 0536
04 a 0542
05 a 0541
06 a 0534
07 a 0533
08 a 0525
09 a 0557

39

////MMM333UUU

R 936 NM 4

k1
16 a 0454
17 a 0460
18 a 0449
19 a 0465
20 a 0456
21 a 0463
22 a 0459
23 a 0444
24 a 0452
25 a 0454
26 a 0452
27 a 0447
28 a 0451
29 a 0470
30 a 0451
31 a 0452
32 a 0458
33 a 0463
34 a 0453
35 a 0450
36 a 0453
37 a 0442
38 a 0448
39a 0447
40 a 0446
41 a 0453
01 a 0451
02 a 0448
03 a 0464
04 a 0447

40

0000555J

443
R 746 N

k1
16 a 055
17 a 056
18 a 056
19 a 057
20 a 055
21 a 057
22 a 056
23 a 056
24 a 057
25 a 056
26 a 056
27 a 056
28 a 056
29 a 056
30 a 056
31 a 056
32 a 056
33 a 056
34 a 0567
35 a 055
36 a 055
37 a 0361
38 a 0372
39 a 0362
40 a 0362
41 a 0375
01 a 0365
02 a 0366
03 a 0367
04 a 0361
05 a 0368
06 a 0371

10 a 0437 14 13
11 a 0446
12 a 0425 8
13 a 0433 3
14 a 0430
15 a 0432 1
16 a 0432 1
17 a 0428 5
18 a 0428 5 6
19 a 0427

09 a 0412
10 a 0414 2
11 a 0412
12 a 0406 6
13 a 0416 4
14 a 0413
15 a 0418
16 a 0418
17 a 0412
18 a 0412
19 a 0403 9

09 a 0557 14
10 a 0540 2
11 a 0540 2
12 a 0557 1
13 a 0534
14 a 0538 13
15 a 0551
16 a 0534 4
17 a 0524 14
18 a 0555 3 8
19 a 0530

04 a 0447 6
05 a 0467 14
06 a 0463 16
07 a 0462 9
08 a 0442 11
09 a 0459 6
10 a 0446 7
11 a 0468 1
12 a 0446 7
13 a 0443
14 a 0454 1
15 a 0451 2

06 a 0371
07 a 0373
08 a 0365
09 a 0365
10 a 0364
11 a 0368
12 a 0367
13 a 0365
14 a 0362
15 a 0363

(k) <u>Setting other messages</u>

MB2004, MB2003 are now set on the wheels already obtained,but the setting runs were sent to Ops and not preserved. The letter counts also are lost. These were used to choose and deciban runs 36 to 40, yielding $\Delta X_1 D$ complete and nearly, but not quite,certain; the 7th and 10th characters can be interchanged with a loss of only 38 decibans.

41

MB 2005

40a

MB 2005

32 L.C

Count of 1st char.

42 MB 2005

Count of 15th X-D of numbers (total)

32L.C

Y1		X		
0285	4.4	Using FX		
0211	3	1 0006 (13)	0010 (26)	
0143		0005 (9)	0003	9
0111		0002	0001	
		0002	0003	
0177	3	1		
0124		0001 3	0001	
0128		0002	0001	
0130		0008	0003	
		0004	0001	
0130				
0125		0001	0003	
0114		0003	0002	
0123		0001	0002	
		0006	0006	
0113				
0099		0002	0004	
0113		0004	0002	
0116		0002	0003	
		0007	0003	
0131				
0257	3	3 0004	0001	
0141	1.5	0003 (3)	0008	(9)
0109		0006 (3)	0003	(4.5)
	2.6	0003	0004	
0225		4	2.6	
0176	1.9	1.7 0007 (2.1)	0003	(8)
0109		0006	0006	
0117		0003	0003	
		0004	0003	
0136				
0111		0006	0007	
0117		0002	0004	
		0003	0003	

43

MB 2004 RAW

doodo

k1 k2 k3 k4 k5

20 12 18 22 13

Y3

$	0269	1.1
9	0205	
h	0192	
t	0191	
e	0213	1
m	0172	
n	0170	
3	0180	
r	0191	
c	0167	
v	0157	
g	0218	1.4
l	0149	
p	0138	
f	0161	
4	0156	
a	0198	
u	0267	1.3
q	0262	1.7
w	0138	
		.4
5	0261	
8	0256	
k	0163	
j	0176	
d	0190	

44 MB 2004

//OOGGUUQQ

2020 R NM 1033

k3

18 a 1046 7
19 a 1057 (4)
20 a 1038 15
21 a 1056 (3) (5)
22 a 1058
23 a 1023 30 3
24 a 1030
25 a 1032 1
26 a 1034 19
27 a 1040 13
28 a 1034 19
29 a 1071 (18)
01 a 1035 18
02 a 1071 (18) (13)
03 a 1066
04 a 1063 (10) 14
05 a 1059 (9)
06 a 1062 (9) (14)
07 a 1067
08 a 1041 12
09 a 1046 7
10 a 1049 4
11 a 1063 (13)
12 a 1046 7 (17)
13 a 1070
14 a 1049 4
15 a 1042 11
16 a 1029 24
17 a 1048 5

259 Page M

k3

///3333

R 0758 NM

k2

31 a 0368
01 a 0397
02 a 0364
03 a 0389
04 a 0374
05 a 0390
06 a 0393
07 a 0363
08 a 0388
09 a 0392
10 a 0357
11 a 0377
12 a 0364
13 a 0368
14 a 0393
15 a 0363
16 a 0377
17 a 0389
18 a 0368
19 a 0378
20 a 0377
21 a 0389
22 a 0364
23 a 0389
24 a 0378
25 a 0364
26 a 0394
27 a 0363
28 a 0367
29 a 0376

e109				
e117	0003	0005	5	e261
	0004	0003	8	e256
			k	e163
e136	0006	0007	j	e176
e111	0002	0004		
e117	0003	0003	d	e190
e087	0002	0001	f	e195
			x	e186
e105	0002	0002	b	e158
e139	0004	0002		
e106	0002	0006	z	e165
e103	0003	0004	y	e183
	36	Total 36	s	e165
	for X		e	e159

12 a 1046 / (17)
13 a 1070
14 a 1049 4
15 a 1042 11
16 a 1029 24
17 a 1048 5

24 a 0378
25 a 0364
26 a 0394
27 a 0365
28 a 0367
29 a 0376
30 a 0374

(l) Letter counts against doubtful characters

To make $\Delta\chi_1$ certain a new ordinary 32-letter count (40a) is made on the rectangle message MB2005, and also a 32-letter count against the doubtful 7th character, supposing it to be a cross. The letter count against the 7th character is decibanned from the complete letter count, for example for /'s the decibannage is $(6-3)\times 10\log_{10}\frac{286}{105} = 3\times 4{\cdot}4 = 13.$

In effect 7 runs are used; these make $\Delta\chi_1$ certain. (cf 25D(g)3)

(m) Making $\Delta\chi_2$ certain

The letter count (43) on MB2004 suggests a slightly odd run (44) for $\Delta\chi_3$, and also run (48) for $\Delta\chi_2$. The previous letter count (40a) is used to deciban runs (45), (46), (47) for $\Delta\chi_2$; $\Delta\chi_2$ becomes certain.

999000 (46)

R 727 NM 586

k2

31 a 0376 10
01 a 0391 5
02 a 0379 7
03 a 0392 1
04 a 0374 12
05 a 0384 2
06 a 0395 9
07 a 0385 3
08 a 0388 2
09 a 0405 7
10 a 0384 4
11 a 0375 11
12 a 0374 12
13 a 0388 3
14 a 0394 8
15 a 0374 12
16 a 0393 7
17 a 0387 1
18 a 0378 9
19 a 0399 18
20 a 0389 3
21 a 0388 2
22 a 0378 8
23 a 0393 7
24 a 0390 4
25 a 0376 10
26 a 0396 10
27 a 0376 10
28 a 0373 13
29 a 0375 11
30 a 0374 12.

letter in MB 2003 missing

50.

UUU54

47

0088 R 649 NM 532

k2

31 a 0321 11
01 a 0331 1
02 a 0335 3
03 a 0337 5
04 a 0326 6
05 a 0335 3
06 a 0336 4
07 a 0326 6 84
08 a 0340 8 70
09 a 0333 1 14
10 a 0327 5
11 a 0332 –
12 a 0334 2
13 a 0324 8
14 a 0336 4
15 a 0329 3
16 a 0341 9
17 a 0329 3
18 a 0330 2
19 a 0338 6
20 a 0334 2
21 a 0337 5
22 a 0325 7
23 a 0335 3
24 a 0328 4
25 a 0337 5
26 a 0342 10
27 a 0329 3
28 a 0319 13
29 a 0325 7
30 a 0327 5

51.

55HHOG 77 209

750

48. Decibanned from 43

111555

R844 NM 417

k2

12 a 0403 14
13 a 0425 8
14 a 0404 13
15 a 0432 15
16 a 0413 4
17 a 0415 2
18 a 0423 6
19 a 0410 7
20 a 0420 3
21 a 0427 10
22 a 0410 7
23 a 0414 3
24 a 0408 9
25 a 0417 –
26 a 0432 15
27 a 0419 2
28 a 0424 7
29 a 0424 7
30 a 0419 2
31 a 0422 5
01 a 0418 1
02 a 0421 4
03 a 0412 5
04 a 0421 4
05 a 0427 10
06 a 0414 3
07 a 0437 20
08 a 0407 10
09 a 0401 16
10 a 0412 5
11 a 0403 14

−110
+119

250 Page

(m) Making $\Delta\chi_5$ certain

A (lost) letter cou on MB2003 is used to decib runs 50, 51, 52 for $\Delta\chi_5$. Most characters score wel but the 1st character has score with the wrong sign, and the wheel is not cert

Individual letter co against the three weakest characters on the three

52 (loss) 53

MB 2005.

MB 2004

dodds

count
changes
score in fav

41 31 01 01 01

0010 3
0007
0010
0006

/ 0299 1.3
9 0224 .9
H 0149 .9
T 0122

0006 3
0009
0003
0011

0185 1.3
0134
0135
0134

0007

UUU 54
R 245 NM 127
9

k5
03 a 0120 7
04 a 0128 1
05 a 0125 2
06 a 0131 4
07 a 0127 —
08 a 0123 4
09 a 0128 1
10 a 0130 3
11 a 0125 2
12 a 0122 5
13 a 0124 3
14 a 0133 6
15 a 0125 2
16 a 0131 4
17 a 0132 5
18 a 0131 4
19 a 0129 2
20 a 0131 4
21 a 0125 2
22 a 0122 5
23 a 0127 —
24 a 0129 2
25 a 0128 1
26 a 0126 1
27 a 0129 2
28 a 0126 1
29 a 0124 3
01 a 0121 6
02 a 0122 5

-48
+39

55HHOO 10/7 ✓

750
743 NM 375
7

k5
03 a 0374 1
04 a 0376 1
05 a 0371 4
06 a 0381 6
07 a 0376 1
08 a 0368
09 a 0377
10 a 0380
11 a 0371
12 a 0375
13 a 0367 8
14 a 0367 8
15 a 0365 10
16 a 0378 3
17 a 0386
18 a 0382
19 a 0373
20 a 0382 7
21 a 0380 5
22 a 0359 16
23 a 0371 4
24 a 0378
25 a 0383 8
26 a 0369 6
27 a 0376 1
28 a 0385 10
29 a 0370 5
01 a 0373 2
02 a 0375 —
03 a 0374

-110
+119

52
333QQQJJJFFFSSS

RI[illegible] 1090 NM554

k5
03 a 0543 11
04 a 0566 12
05 a 0543 11
06 a 0561 7
07 a 0556
08 a 0552 2 92
09 a 0552 2 73
10 a 0557 3 19 ✓
11 a 0547 7
12 a 0549 5
13 a 0544 10
14 a 0561 7
15 a 0543 11
16 a 0562
17 a 0559
18 a 0558
19 a 0554
20 a 0550 4
21 a 0555
22 a 0545 9
23 a 0549 6
24 a 0555 1
25 a 0553 1
26 a 0548 6
27 a 0565 11
28 a 0562 8
29 a 0554 —
01 a 0547 7
02 a 0558 4

0133
0134

0146
0137
0127
0140 -4

0122
0106
0126
0132

0143
0297 2.5
0144 .5
0127

0230 .5
0202
0114
0132 .6

0149
0116
0127 1.2
0097

0111 1.3
0150
0109
0111

0011

0007
0008
0008
0010 1

0009
0006
0004
0002

0004
0006 2
0003
0004

0006
0005
0005
0004

0002
0011
0009
0005

0007
0005
0008
0006
7

53
mb 2004
count ag
8th character of χ_3

0007 (1)
0006
0006
0008

0008 (3)
0005
0008
0007

0001
0006
0007
0005 2.8

0002
0001
0002
0004

0007
0005 2.6
0005 7
0009

0013 1.6
0009
0006
0010

0008
0008
0011 1.4
0009

53
mb 2004
count ag 26th
character of χ_3

0009 3.3
0006
0004
0004

0006
0006
0004
0009

0005
0009
0009
0004 - 7

0005
0007
0003
0007

0009
0008 1.3
0008 7
0004

0011 2
0006
0005
0004

0008
0010
0009 3.5
0004

54 mb 2005
count ag. 1st. character of χ_3
[illegible] for x

0009 1.3
0010
0005 1.8
0003

0003 2.6
0001
0009
0005

0002
0010
0006
0007

0003
0003
0003
0003

0010
0007 7.5
0003 .5
0004

0007 1
0009
0004
0007 1.8

0004
0003
0001
0005 4.8

54
MB 2005
doubting 8th character of χ_3

0010 2.6
0012
0006 2.7
0003

0008 6.5
0003
0005
0003

0003
0007
0003
0005 .8

0004
0005
0006
0004

0005 5
0007
0002
0002

0013 3
0007
0004
0006 1.2

0003
0003
0005 3.6
0002

54
MB 2005
doubting 26th character of χ_3

0012 2.6
0010
0002 5.4
0008

0002 9
0009
0002
0004

0007
0002
0000
0004 1.6

0006
0006
0003
0007

0003 15
0009
0003 1
005

0003 3.5
0010
0005
0007 ~~1.4~~

0001
0005
0000 ~~1.2~~

55
mb 2003
1st [illegible] of [illegible] x

0003
0004
0002 1.2
0003

0004
0005
0004
0005 1.2

0004
0006
0003
0004 1.7

0004
0006
0004
0001

0001
0006 0.5
0002 2
0004

0006
0006
0004
0006 2

0004
0003 1
0001

55
MB 2003
8th chr. of χ_3

0006
0007
0005
0005

0006
0001
0004
0004

0007
0003
0001
0009 13.4

0004
0005
0000
0005

0004
0006 8.2
0005 1
0002

0002 9
0007
0004 1
0005

0004

55
MB 20[illegible]
26 o[illegible] of χ_3

0004
0005
0003
0004

0004
0002
0002
0007

0004
0007
0002
0002

0003
0005
0004
0001

0002 8
0006
0003
0000

0009
0002
0005
0005

0004

ooo8	oolo		ooo5	ooo1	ooo4	ooo5	ooo5
oo11 (1.4)	ooo9 (3.5)	ooo3	ooo3	ooo5	ooo3		ooo5
ooo9	ooo4	ooo1	ooo5 (3.6)	oooo	ooo1	ooo4	ooo4
		ooo5 4.8	ooo2	ooo1	ooo3	ooo4	ooo4
ooo8	ooo5					oooo	ooo1
ooo8	ooo8	ooo8	ooo2	ooo5	ooo6	ooo2	ooo6
ooo2	ooo5	ooo5 3.9	ooo9 (9)	ooo7 (26)	ooo5		
ooo5	ooo5	oooo	ooo6	ooo1	ooo1 4.4	ooo5	ooo1 (5
		ooo5	ooo1	ooo3	ooo5	ooo5	ooo7
						ooo3 (1)	ooo5
							ooo6
−5	+14 −10 +4	+6.2 −19 −13	29	3.6	+3	13.6	+33 −24 39

60 mb 2oo9

1st chr k3

9	oolo ooo7	at 1 db	so 3
u	ooo6		
a	ooo3	at 2 db	so 6
5	oo11		
8	ooo6	at 1.7db	so 8

score 17 db

makes k3 certain.

messages already used, still fail to make the wheel certain, because the 1st character retains its wrong sign; but a count against the 1st character on a newly set message, MB2009, (decibanned of course from the complete count on that message) is conclusive.