

The original of this document is held in the United Kingdom
at the National Archives, Kew, Richmond, Surrey, TW9 4DU
Reference HW 25/4 and HW 25/5

General Report on Tunny

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 p332 in section 53)

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	QKP Research
95	Mechanical Flags

General Report on Tunny

Page 2

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

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**

[< previous](#)

[next >](#)

[Back to General Report on Tunny. Contents.](#)

[Back to The Enigma and the Bombe main page](#)

[**Home**](#)

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.

General Report on Tunny

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	IN LETTER SHIFT	MEANING	IN FIGURE SHIFT
/		(no meaning)	
occasionally				
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 .	O	colon	
V	. x x x x	V	equals	
G	. x . x x	G	o	
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	shift	move to FIG	(none)
8 or -	x x x x x		(none)	move to LET.
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		percent
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 of 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
2nd Impulse	o o o o o
Sprocket holes (used to drive tape)
3rd Impulse	o o o o o o o o
4th Impulse	o o o o o o o
5th Impulse	o o o o o
<hr/>	
(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 and 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 SCHLUESSELZUSATZGERAET) 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 $\frac{1}{2}$ 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 93)

11B THE TUNNY CIPHER MACHINE.

(a) Addition.

Fig. 11 (I) THE ADDITION SQUARE

/ 9 H T	0 M N 3	R C V G	L P I 4	A U Q W	5 8 K J	D F X B	Z Y S E
				A U Q W			
/ / 9 H T	0 M N 3	R C V G	L P I 4	U A W	5 8 K J	D F X B	Z Y S E
9 9 / T H	M 0 3 N	C R G V	P L 4 I	Q	8 5 J K	F D B X	Y Z E S
H H T / 9	N 3 0 M	V G R C	I 4 L P	Q W A	K J 5 8	X B D F	S E Z Y
T T H 9 /	3 N M 0	G V C R	4 I P L	U	J K 8 5	B X F D	E S Y Z
				W Q U			
				A			

O	0	M	N	3	/	9	H	T	L	P	I	4	R	C	V	G	5	8	K	J	U	A	W	Z	Y	S	E	D	F	X	B
M	M	0	3	N	9	/	T	H	P	L	4	I	R	C	R	G	8	5	J	K	Q	Y	Z	E	S	F	D	B	X		
N	N	3	0	M	H	T	/	9	I	4	L	P	V	G	R	C	K	J	5	8	Q	W	A	S	E	Z	Y	X	B	D	
3	3	N	M	0	T	H	9	/	4	I	P	L	G	V	C	R	J	K	8	5	U	W	Q	U	E	S	Y	Z	B	X	F

R	R	C	V	G	L	P	I	4	/	9	H	T	0	M	N	3	D	F	X	B	Z	Y	S	E	U	A	W	5	8	K	J		
C	C	R	G	V	P	L	4	I	9	/	T	H	M	0	3	N	F	D	B	X	Y	Z	E	S	Q	W	A	8	5	J	K		
V	V	G	R	C	I	4	L	P	H	T	/	9	N	3	0	M	X	B	D	F	S	E	Z	Y	Q	W	A	K	J	5	8		
G	G	V	C	R	4	I	P	L	T	H	9	/	3	N	M	0	B	X	F	D	E	S	Y	Z	U	W	Q	U	A	J	K	8	5

L	L	P	PL	4I	R	CV	G	0	M	N	3	/	9	H	T	Z	Y	S	E	D	F	X	B	5	8	K	J	U	A	W	5	8	K	J	
P	P	I	I4	L	C	R	G	M	0	3	N	9	/	T	H	Y	Z	E	S	F	D	B	X	Y	8	5	J	K	Q	W	A	8	5	J	K
I	I	4	IPL	V	G	R	C	N	3	0	M	H	T	/	9	S	E	Z	Y	X	B	D	F	K	J	5	8	Q	W	A	K	J	5	8	
4	4	IPL	GV	CR	3	N	M	0	T	H	9	/	E	S	Y	Z	B	X	F	D	E	S	Y	Z	U	W	Q	U	A	J	K	8	5		

A	U	Q	W	A	U	A	W	5	8	K	J	D	F	X	B	Z	Y	S	E	/	9	H	T	0	M	N	3	R	C	V	G	L	P	I	4	IPL	
U	Q	8	5	J	K	F	D	B	X	Y	Z	E	S	Y	Z	U	W	Q	W	A	9	/	T	H	M	0	3	N	C	R	G	V	P	L	4	I	PL
Q	Q	W	A	K	J	5	8	X	B	D	F	S	E	Z	Y	W	Q	U	W	Q	U	A	HT	/	9	N	3	0	M	V	G	R	C	I	4	L	P
W	W	U	JK	8	5	B	X	F	D	E	S	Y	Z	U	W	Q	U	W	Q	U	A	TH	9	/	3	N	M	0	GV	C	R	V	4	I	P	L	

5	5	8	K	J	U	A	W	Z	Y	S	E	D	F	X	B	0	M	N	3	/	9	H	T	L	P	I	4	IPL	R	C	V	G		
8	8	8	5	J	K	Q	W	Y	Z	E	S	F	D	B	X	M	0	3	N	9	/	T	H	PL	4I	C	R	G	V	P	L	4	I	PL
K	K	K	J	5	8	Q	W	S	E	Z	Y	X	B	D	F	N	3	0	M	HT	/	9	I	4	L	P	V	G	R	C	I	4	L	P
J	J	J	JK	8	5	U	W	E	S	Y	Z	B	X	F	D	3	N	M	0	TH	9	/	4	I	P	L	GV	C	R	V	4	I	P	

A U Q
W
D D F X B Z Y S E U A W 5 8 K J R C V G L P I 4 / 9 H T 0 M N 3
F F D B X Y Z E S Q 8 5 J K C R G V P L 4 I 9 / T H M 0 3 N
X X B D F S E Z Y Q W A K J 5 8 V G R C I 4 L P H T / 9 N 3 0 M
B B X F D E S Y Z U J K 8 5 G V C R 4 I P L T H 9 / 3 N M 0
W Q U
A

A U Q
W
Z Z Y S E D F X B 5 8 K J U A W L P I 4 R C V G 0 M N 3 / 9 H T
Y Y Z E S F D B X 8 5 J K Q P L 4 I C R G V M 0 3 N 9 / T H
S S E Z Y X B D F K J 5 8 Q W A I 4 L P V G R C N 3 0 M H T / 9
E E S Y Z B X F D J K 8 5 U 4 I P L G V C R 3 N M 0 T H 9 /
W Q U
A

/ 9 H T 0 M N 3 R C V G L P I 4 A U Q 5 8 K J D F X B Z Y S E
W

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	•
×	plus	×	equals	•
•	plus	×	equals	×
×	plus	•	equals	×

$$\text{Therefore } 9 + Y = \left(\begin{array}{ccc} \bullet & \times & \times \\ \bullet & \bullet & \bullet \\ \times & \text{plus} & \times \text{ equals} \\ \bullet & \bullet & \bullet \\ \bullet & \times & \times \end{array} \right) = Z$$

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. (A1)

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.

<u>Example</u>	P-stream	9 D I E 9 S C H O E N E 9 J U N G F R A U 9
	K-stream	Y / R A V 8 B U J L / 3 K S H V 9 A I C D N
	Z-stream	Z D N 4 G G Q W W W N D J C W L V C N P C 3

(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 (X) Wheels	X_1 length	41 characters
	X_2	31
	X_3	29
	X_4	26
	X_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 the chi-key (X) formed by the five characters in the active positions of X_1, X_2, X_3, X_4, X_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) Chi-key.

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) Psi-key.

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.

Example

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, Ψ')-stream	D 5 H 3 S 9 K A O C A Y X D S C

(f) Motors.

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 in 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'.

Example of finding Basic Motor:

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 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 in (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 and 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 a limitation dot) there is a Total Motor cross and every psi moves on once.

Example:

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{X}_2 limitation (known for short as X_2 lim. or chi 2 lim).

The active character of the limitation at any position is given by the character of X_2 which was active in the previous position. This is called chi 2 ONE BACK and written \bar{X}_2 .

(NB $\bar{\bar{X}}_2$ means X_2 two back, \underline{X}_2 means X_2 one forward etc.)

(ii) $\bar{X}_2 + \bar{\Psi}'_1$ limitation (known for short as Ψ_1 lim or Psi 1 lim).

The active character of the limitation is given by the sum of the characters of X_2 and Ψ'_1 which were active in the previous position.

(iii) $\bar{X}_2 + \bar{\bar{P}}_5$ limitation (known for short as P_5 lim.)

The active character of the limitation is given by the sum of the character of X_2 which was active in the previous position and the character of P_5 which was active two positions previously.

(iv) $\bar{X}_2 + \bar{\Psi}'_1 + \bar{\bar{P}}_5$ (known for short as Ψ_1, P_5 lim.)

The active character of the limitation is given by the sum of the characters of X_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 $\bar{X}_2 + \bar{\Psi}'_1$ ' limitation.

- (i) P: 9 I M 9 K A M P F 9 G E G E N 9 (given)
- (ii) X: U O 8 X X R J Y W O 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) X_2 : x . x . . x x . x . x . . x x . (from ii)
- (vi) $X_2 + \Psi'_1$: x . x x x . . x x x . . x x x . (from v and x)
- (vii) $\bar{X}_2 + \bar{\Psi}'_1$: . x . x x x . . x x x . . x x x (from vi)
- (viii) TM: x . x x . . x x x x . x x . x x x . . x (from iv and vii)

- (ix) Ψ' : N L L D E E E Q / K K H B 4 4 4 (from iii and viii)
- (x) Ψ'_1 : . . . x x x x x . x x . x . . . (from ix)

- (xi) K = X + Ψ' : J R F H M J R 4 W Q S H C Y T R (from ii and ix)
- (xiii) 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

$$\begin{aligned} Z &= P + K \\ K &= X + \Psi' \end{aligned} \quad \text{(A2)}$$

TUNNY MACHINE

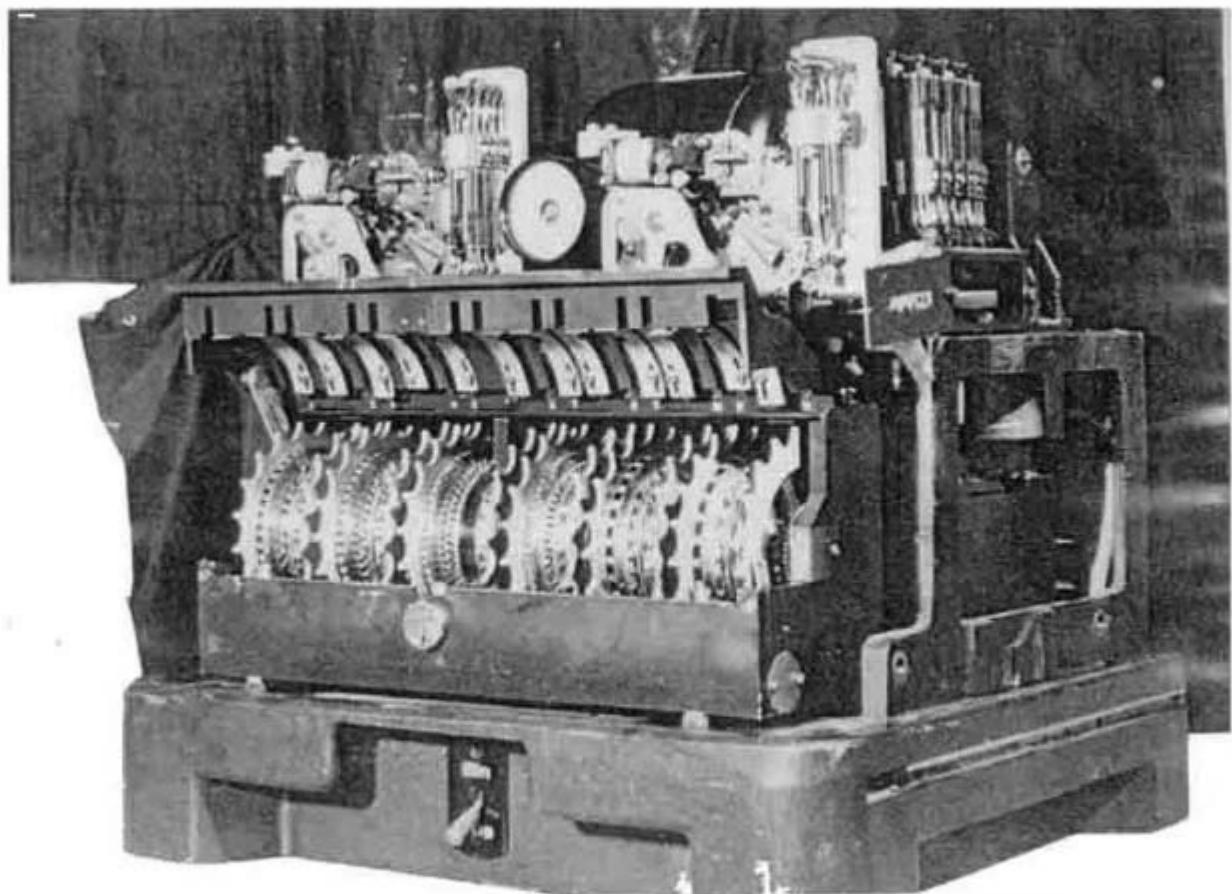


Fig. 11 (II)

It follows at once from (A1) that

$$\begin{aligned} K &= P + Z \\ P &= Z + K \end{aligned} \quad (\text{A3})$$

$$\text{and } Z + P + X + .\Psi' = / \quad (\text{A4})$$

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 X_2 or X_2P_5 lim.

SZ 42B (1942) with $X_2\Psi_1$ or $X_2\Psi_1P_5$ 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 15½ 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}	X_1	X_2	X_3	X_4	X_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).



In the photograph, the cams are most easily seen on X_2 (Wheel 9) and X_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 this 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 the third letters the psis move normally but μ_{37} always moves. After that, the machine moves in the normal way.

When the machine is switched off, no further letters are enciphered and the wheels stop two places ahead of the last ciphering position.

11C WHEEL PATTERNS.(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.

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

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

$$\Delta \Psi_3' = \Psi_3' + \underline{\Psi}_3'$$

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:

X_4 pattern : ... x x . x . x x x . . x . . x x . . x . x x x

ΔX_4 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) Construction 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 X and ΔX 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 $a = \text{proportion of crosses in TM} = \frac{74-d}{74}$

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

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 STRAUSSBERG exchange (near BERLIN), with HEERESGRUPPE D and 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 QKP book and transmits QKP 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 QKP and partly in the next, and resetting may also take place during a message if something goes wrong.

(e) 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 QKP 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 known as an OVERLAP.

(d) Depths.

Each QKP number, and each QKP list, should only be used once. However sometimes the same QKP number and settings are used for two (usually consecutive) transmissions. As long as a limitation involving P₅ 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 $ab = \frac{1}{2}$, and there was a regular excess of dots over crosses in the $\Delta\Psi'$ stream.

(ii) The QKP 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 $ab = \frac{1}{2}$ 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 QKP 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 P₅ 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.

(a) 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 P₅ limitation switched in (i.e. on Ψ_1 P₅ lim) but later it was decided that the P₅ 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.

D * A + P * E * I

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. $X_4 \Psi_4$) 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, X, 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 , X , 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.

$$Z = P + K$$

$$K = X + \Psi'$$

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

$$Z = P + K = D + X$$

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

$$D = Z + X = P + \Psi'$$

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 the 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 fall 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. X₄ Ψ₄) 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, X, 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. X and Ψ'). This may be described as the solution of an equation; in the example quoted the equation is $K = X + \Psi'$.

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 $ab \neq \frac{1}{2}$

$$K = X + \Psi'$$

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

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 ΔX from a long enough stretch of that impulse of ΔK .

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 deducible.

12B MODERN STRATEGY.

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

(a) 1st Method.

Stage I. Solution of $Z = X + D$. Various X-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 4000 and for chi setting about 1000 letters

(b) 2nd Method.

Stage I. Mechanical solution of $Z = X + D$ 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 patters 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) 3rd Method.

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 position of Z and the correct position distinguished by the statistical properties of ΔK .

Stage II. Solution of $K = X + \Psi'$. Various X -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.

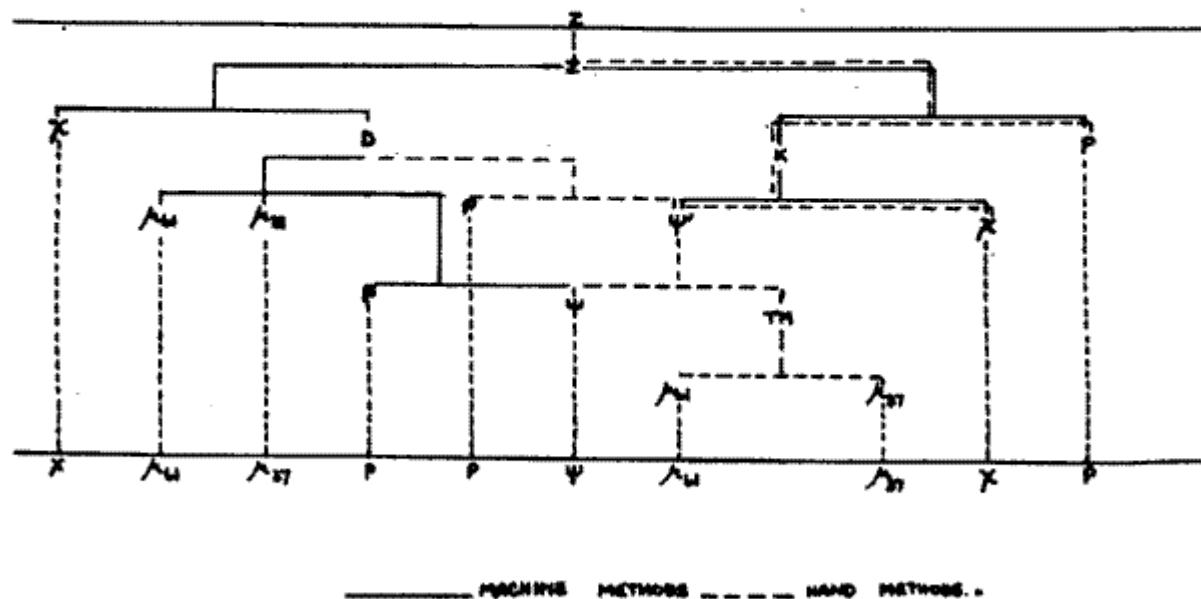


Fig. 12 (I)

12C CHI BREAKING AND SETTING Solution of $Z = X + D$.(a) Frequency of letters in $\Delta\Psi'$.

The precautions taken by the Germans in the construction of wheel patterns produce X , ΔX , 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 55M889 or 5M89 (full stop) E1, EN N9, SCH and so on naturally implies the frequent repetition in ΔP of their differenced equivalents /UA/5, UA5, U, F, 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 F 9 G E G E N 9

ΔP : 4 G O J N 8 R 5 D V 5 5 5 F 3

$\Delta \Psi'$: 8 / 5 3 / / P Q K / 5 / / V /

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 $\Delta D = \Delta P + \Delta \Psi'$ but also $\Delta Z + \Delta X$. 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 ΔX sequences corresponding to the X 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 $41 \times 31 \times 29 \times 26 \times 23$, 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 ΔD_1 is a dot, ΔD_2 a dot, ΔD_4 a cross, and ΔD_5 a cross. Therefore using the combined counts of O and M and of others 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 $\Delta D_1 + \Delta D_2 =$ 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 $\Delta D_1 + \Delta D_2 = x$. 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 $41 \times 31 = 1271$ 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 lengths required are very roughly as shown in the following table (d is the dottage of μ_{37}).

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 ΔX 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 $(41+31+29+26+23) = 1 \text{ in } 2^{150} = 1 \text{ in } 10^{45}$. (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 ΔX_1 and ΔX_2 which maximise the number of letters of ΔD in which $\Delta D_1 + \Delta D_2 = \text{dot}$. 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 wheel-breaking 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 ΔX_1 and ΔX_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'	$\Delta \Psi'$	ΔD	X	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
P	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	305	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 , Ψ' , ΔD have been explained. Ψ' , X, 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, ΔX , 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 $D = P + \Psi'$.(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 TTTT). Experienced men know at sight that

$$\text{JNKH} = 5\text{M}89 + \text{TTTT}$$

$$\text{NJ3W} = 5\text{M}89 + \text{QQQQ}$$

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 the 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 settings 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 $\Delta\Psi'$.

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 $\Delta D = \Delta P$, 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{X}_2 limitation, the extended psi pattern corresponding to each possible setting 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 long as $ab = \frac{1}{2}$, 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.

12E METHODS INVOLVING KEY Solution of $Z = K + P$, and $K = X + \Psi'$.

(a) Obtaining of key from depths.

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

$$\begin{aligned} Z_a + P_a &= K = Z_b + P_b \\ \therefore Z_a + Z_b &= P_a + P_b \end{aligned}$$

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.

Example:

$Z_a = A O 9 V Y P B 8 S L K N 9 I I / P R 8 Y Q A H V 8$

$Z_b = N N R Z Y A P Q U F C L I N C 3 A 4 L P 8 / K 9 Z$

$Z_a + Z_b = K H C K / Y K 3 4 8 Y V 4 R 3 3 Y 3 F A 3 A 5 G C$

$P_a = 5 Q M 8 9 E N G L 5 M 8 9 I N F 5 M 8 9 D I V 5 M$

$P_b = H A L T 9 H A L T 9 D E I N 9 S C H L U E S S E L$

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

(b) Obtaining of key from cribs.

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) Wheel-breaking from key.

Chi-breaking from key is analogous to chi-breaking from Z , the method being to select the patterns of ΔX 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 this are rarely broken from under 4000 letters of $Z = X + D$, they can sometimes be broken from 100 letters of $K = X + \Psi'$. 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 X_2 limitation normally starts with a \hat{X}_2 count or run. Wheel-breaking from other kinds of key normally starts with KEY RECTANGLES and a COMBINED (ΔX_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 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.

As 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 $\Delta X + \Delta Z$ in all possible relative positions, and counting for each position the number of places in which a condition such as $\Delta X_1 + \Delta X_2 + \Delta Z_1 + \Delta Z_2 = \text{dot}$ 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 either be 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 $\Delta D = \Delta Z + \Delta X$ and $P = Z + X + \Psi$. 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, not B, not C)".

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

The effective speed is increased five fold 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 vis. 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, Robinson has been used mostly for cribs and for experimental work, occasionally for rectangling.

(c) Specialised 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.

13C 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.

<u>INPUT</u>	<u>OUTPUT</u>	<u>NAME OF MACHINE</u>	<u>REMARKS</u>
Keyboard	→ tape	Hand perforator	
Tape	→ tape	Angel	
		Insert machine (or L.B.M.):	Special facilities for making correction 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 Δ:	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 Readers (or transmitters, or auto-transmitters).
2. Reperforators (or punches).
3. Electromatic Typewriters.

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 o): 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 the Cryptographic work on Tunny, and the sections at Station X concerned with this occupied an intermediate position between

GCWS KNOCKHOLT and ancillary 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 QKP 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 P₅ 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 P₅ 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 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 room 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 K-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 RF and chi-settings is sent by Room 12 to Room 41 for psi setting, passed on to Room 40 for motor settings, and on to the Decoding Room. The decode is passed to the Cribs 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.

RF 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 Garbo 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 RF 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 in abstracto 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 occurrence 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 P₅ 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 P₅ 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 P₅ 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 deliberately 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 ' \bar{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

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

In particular, if E_1 and E_2 are independent

$$P(E_1 E_2 | H) = P(E_1 | H) P(E_2 | H)$$

(f) Some theorems.

(i) $P(E_1 E_2 \dots E_n | H)$

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

$$\begin{aligned} \text{(ii)} \quad & P(E_1 \vee E_2 \vee \dots \vee E_n | H) \\ &= \sum_r P(E_r | H) - \sum_{r,s} P(E_r E_s | H) + \sum_{r,s,t} P(E_r E_s E_t | H) - \dots \text{etc.,} \end{aligned}$$

and in particular if E_1, E_2, \dots, E_n are all mutually exclusive, the right hand side can be replaced by $\sum_r P(E_r | H)$. If $E_1 \vee \dots \vee E_r$ is exhaustive the left hand side is 1.

Therefore $P(\bar{E}) = 1 - P(E)$.

(iii) Bayes' theorem.

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

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

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

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

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

$P(E | H)/P(E | \tilde{H})$ is called the factor in favour of H given E , 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 unbiased, (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

$$P(E | H) = 1$$

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

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, $10 \log_{10}$.)

(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 $1/(\text{million})$ 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, \dots and the factors in favour of an hypothesis H be f_1, f_2, \dots respectively. Then the resulting factor is $\sum p_i f_i$.

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' $\frac{1}{2}(1 + \zeta_i)$ ($i = 1, 2, 3, \dots$). (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 $\frac{1}{2}(1 + \prod_i \zeta_i)$.

This theorem is the real reason why 'proportional bulges' were introduced. The 'Proportional bulge' or P.B., ζ , of a proposition is defined by saying that its probability is $p(1 + \zeta)$ 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 'variante' 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

$$P(x_i < x < x_i + dx_i) = f(x_i)dx_i,$$

then

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

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

(I) 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 decimal form. A table of $\Psi(x)$ is given in R1, 109 where

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

The binomial distribution is closely approximated by the normal one for quite small values of n , if we take $x = pn$ 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 a^n , so that

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

The average and variance of the distribution are both equal to a .

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 a is small compared with a .

There is one other distribution used in the research logs, namely the 'X² distribution'. Given n independent variables each with a normal distribution of mean 0 and S.D. 1, let X² be the sum of the squares of these variables.

writing $\varphi(n) = P(X^2 > t)$, we have

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

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

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) Some simple formulae of a non-analytic type concerning proportional bulges.

If P and Q are independent propositions

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

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

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

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

$$P.B.(P_1 \vee P_2 \vee P_3 \vee \dots) = \text{Average}_i \{P.B.(P_i)\}$$

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

$$P.B.(P + Q = \Phi) = \text{Average}_{\Theta} \{P.B.(P = \Theta) P.B.(Q = \Phi + \Theta)\}$$

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

(n) The general formula for sigma in Tunny work.

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 ($i = 1, 2, \dots r$). Let the overlap of the two tapes be N.. Let the number of times A_i comes opposite B_i be v_i . Let $v = \sum_{i=1}^r v_i$. Then the average of v 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) The statistician's fallacy.

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 is 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 existence 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.)

(p) The principle of maximum likelihood.

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 $(x_0 - \varepsilon, x_0 + \varepsilon)$ 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 exhibited.

(a) Notation.

The letters Z, P, K, X, 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:

$$\begin{aligned}Z &= P + K \\K &= X + \Psi' \\D &= Z + X = P + \Psi'\end{aligned}$$

The suffixes 1, 2, 3, 4, 5 are used when a particular impulse is specified so that (using a generalised form) U_i 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) Some further definitions.

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

$$\begin{aligned}\overline{U} &= \text{letter preceding } U \\ \overline{U}_i &= \text{character preceding } U_i \\ \overline{\overline{U}} &= \text{letter preceding } \overline{U} \\ \underline{U} &= \text{letter following } U \\ \underline{\underline{U}} &= \text{letter following } \underline{U} \end{aligned} \quad \text{and so on.}$$

$$\begin{aligned}\Delta U &= U + \underline{U} \\ \Delta^2 U &= \Delta(\Delta U) \\ \Delta^n U &= \Delta(\Delta^{n-1} U) \\ \Delta_2 U &= U + \underline{\underline{U}} \\ \Delta_2 U &= U + \underline{\underline{\underline{U}}} \end{aligned} \quad \text{and so on.}$$

$$\begin{aligned}\hat{U} &= \overline{U} + U + \underline{U} = \overline{U} + \Delta U \\ U_{ij} &= U_i + U_j \\ \tilde{U}_i &= U_i + \text{a cross} \end{aligned}$$

$$\begin{aligned}U_i \longrightarrow x : P(U_i = x) &> \frac{1}{2} \\ U_i \longrightarrow . : P(U_i = .) &> \frac{1}{2} \\ U_i \xrightarrow{p} x : P(U_i = x) &= p \text{ where } p > \frac{1}{2} \\ U_i \xrightarrow{p} . : P(U_i = .) &= p \text{ where } p > \frac{1}{2} \end{aligned}$$

(c) Two general theorems.

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

$$\text{Theorem II: } \underline{\Delta^2 U} = \underline{\Delta_2 U} \tag{A2}$$

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

Theorem II is a special case of the general theorem:

$$\Delta^n U = \Delta_n U \text{ if and only if } n = 2^r. \text{ (See R5 p. 114)}$$

22B THE CHI-STREAM.

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 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:

$X: \dots x x \dots x x \dots$

$\Delta X: . x . x . x . x . x . x . x$

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

$X_5: \dots x x \dots x$

$\Delta X_5: . x . x . x . x . x . x . x . x . x . x . x . x x$

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

$$\Delta^2 X_i \xrightarrow{\text{as}} x$$

B1

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

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

Wheel	Length	No. of crosses in X	No. of crosses in ΔX	Av. no. of crosses in $\Delta^2 X$
1	41	20 or 21	20	26
2	31	15 or 16	16	19½
3	29	14 or 15	14	19
4	26	13	12 or 14	16½
5	23	11 or 12	12	14

Fig. 22(I)

The number of legal chis is discussed in 25X, and the frequency of various patterns of 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	$D = d/37$
Proportion of crosses in μ_{37} as	$a' = (1 - D)$
Proportion of crosses in TM as	a
Proportion of crosses in μ_{61} as	k

(b) The motor wheels.

μ_{61} is constructed so that $30 \leq k \leq 50$ and $k \neq 37$ without more than so far as is known 5 consecutive dots or 15 consecutive crosses.

μ_{37} is constructed so that $14 \leq d \leq 28$ 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

$$nk \equiv 0 \pmod{37}$$

Since $k \neq 37$, n must be multiple of 37, and the motor returns to its original 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{X}_2 or $\bar{X}_2\bar{P}_5$ limitation - we have:

$$\begin{aligned}\text{Proportion of dots in TM} &= \frac{1}{2} \times \text{proportion of dots in BM} \\ \text{i.e. } 1 - a &= \frac{1}{2}(1 - a')\end{aligned}$$

Proportion of crosses in TM is comprised of:

$$\left. \begin{array}{l} \text{Proportion of BM dot lim dot } \frac{1}{2}(1-a') \\ \text{BM cross lim dot } \frac{1}{2}a' \\ \text{BM cross lim cross } \frac{1}{2}a' \end{array} \right\} \quad (\text{C3})$$

Summary

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

(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 and 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.

$$\beta = 2b - 1 \quad (\text{D1})$$

$$a = \frac{1}{2b} = \frac{1}{1 + \beta} \quad (\text{D2})$$

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

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

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

(c) Corresponding value 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	32 or 34	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	34 or 36	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	36 or 38	40	42	46	27
28	.62	.81	.61	34	38	42	42	48	28

Fig. 22 (II)

(d) Frequency of letters in Ψ' .

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) Frequency of letters in $\Delta\Psi'$.

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.

T.M. 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 T.M. 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	$(1-b)^3$
MOGPUWJFBY	3 crosses	ab^3	$(1-b)^2$
VQ5KX	4 crosses	ab^4	$(1-b)$
8	5 crosses	ab^5	

(D6)
(f) $\Delta\Psi'_{ij}$.

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

When TM = cross

$$\begin{aligned} P(\Delta\Psi'_{ij} = \text{dot}) &= b^2 + (1-b)^2 \\ &= 2b^2 - 2b + 1 \end{aligned}$$

$\therefore \Delta\Psi'_{ij} \xrightarrow{\quad} \cdot$ with probability

$$\begin{aligned} & (1-a) + a(2b^2 - 2b + 1) \\ &= 1 - a + b - 1 + a = b \end{aligned}$$

$\therefore \Delta\Psi'_{ij} \xrightarrow{b} \cdot$

(D7)

(g) $\Delta\Psi'$ stream and limitation.

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 $\Delta\Psi'_i \xrightarrow{b} \text{cross}$
 $L \xrightarrow{b} \text{dot}$

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 $\Delta\Psi'_b$ - a stream of letters with a period of 31 for X_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

$$P(\Delta\Psi' = 9, L = .)$$

$$= P(\Delta\Psi' = N, L = x) = ab^2(1-b)^4$$

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 \bar{X}_2 lim and $\bar{X}_2\bar{\Psi}'_1$ lim, and in the case of \bar{X}_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

$$\Delta\Psi'_i + L \xrightarrow{b} x \quad (D8)$$

(h) Proportional bulges of letters in $\Delta\Psi'$ stream.

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 p. 27.

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

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

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

(i) Δ^2 characteristics.

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

$$\Delta^2 \Psi_i \rightarrow . \text{ with probability } b^2 + (1 - b)^2 = 2b^2 - 2b + 1$$

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

$$\Delta^2 \Psi'_{ij} \rightarrow . \text{ (see R3 p. 22).}$$

(j) The sum of Psi streams.

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 calculating 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,

$$\text{then } PB(U = \Theta) = \zeta_{\Theta}^U$$

$$\text{where } P(U = \Theta) = \frac{1}{r}(1 + \zeta_{\Theta}^U)$$

Summing over the r letters of the alphabet we get

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

$$\sum_{\Theta} \zeta_{\Theta}^U = 0$$

(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

$$\begin{aligned} P(U + V = \Theta) &= \sum_{\phi} \{P(U = \phi)P(V = \Theta + \phi)\} \\ \therefore \frac{1}{r}(1 + \zeta_{\Theta}^{U+V}) &= \frac{1}{r^2} \sum_{\phi} \{(1 + \zeta_{\phi}^U)(1 + \zeta_{\Theta+\phi}^V)\} \\ &= \frac{1}{r^2} \sum_{\phi} \{1 + \zeta_{\phi}^U \cdot \zeta_{\Theta+\phi}^V\} \\ &= \frac{1}{r^2} \left\{ r + \sum_{\phi} \zeta_{\phi}^U \cdot \zeta_{\Theta+\phi}^V \right\} \end{aligned} \tag{E1}$$

$$\therefore \zeta_{\Phi}^{U+v} = \frac{1}{r} \sum_{\Phi} (\zeta_{\Phi}^U \cdot \zeta_{\Phi+v}^v) \quad (E2)$$

$$\text{If every } \zeta_{\Phi}^U = 0, \text{ then } \zeta_{\Phi}^{U+v} = 0 \quad (E3)$$

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

$$\zeta_{\bullet}^{U+v} = \frac{1}{2} (\zeta_{\bullet}^U \zeta_{\bullet}^v + \zeta_x^U \zeta_x^v)$$

$$\text{But } \zeta_{\bullet} + \zeta_x = 0$$

$$\therefore \zeta_{\bullet}^{U+v} = \zeta_{\bullet}^U \zeta_{\bullet}^v$$

This multiplication property is first mentioned in R1 p. 20.

22F THE KEY STREAM

$$\begin{aligned} K &= X + \Psi' \\ \therefore \Delta K &= \Delta X + \Delta \Psi' \end{aligned}$$

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

(a) Recognising key on any limitation.

$$\begin{aligned} \Delta \Psi'_{ij} &\xrightarrow{\frac{1}{2}(1+\beta)} \text{dot} \\ \therefore \Delta X_{ij} + \Delta \Psi'_{ij} &\xrightarrow{\frac{1}{2}(1+\beta)} \Delta X_{ij} \\ \therefore \Delta K_{ij} &\xrightarrow{\frac{1}{2}(1+\beta)} \Delta X_{ij} \end{aligned} \quad (\text{F1})$$

Differencing at distance ω_i where ω_i is the length of X_i (R3 p. 62)

$$\Delta \omega_i(\Delta K_{ij}) \xrightarrow{\frac{1}{2}(1+\beta^2)} \Delta \omega_i(\Delta X_{ij})$$

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

$$\begin{aligned} \text{Now } \Delta \omega_i(\Delta X_i) &= \text{dot} \\ \therefore \Delta \omega_i(\Delta K_{ij}) &\xrightarrow{\frac{1}{2}(1+\beta^2)} \Delta \omega_i(\Delta X_j) \end{aligned} \quad (\text{F2})$$

Similarly, differencing at $\omega_i \omega_j$ (e.g. 26×23 for X_4 and X_5)

$$\Delta \omega_i \omega_j(\Delta K_{ij}) \xrightarrow{\frac{1}{2}(1+\beta^2)} \text{dot} \quad (\text{F3})$$

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{X}_2 limitation.

$$\begin{aligned}\Delta \Psi_i' + \lim_{\frac{1}{2}(1+\beta)} &\rightarrow x \\ \therefore \Delta K_i &\xrightarrow{\frac{1}{2}(1+\beta)} \Delta X_i + \lim x \\ \therefore \Delta K_2 &\xrightarrow{\frac{1}{2}(1+\beta)} \Delta X_2 + \bar{X}_2 + x \\ \therefore \Delta K_2 &\xrightarrow{\frac{1}{2}(1+\beta)} \bar{X}_2 + x\end{aligned}\tag{F4}$$

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

$$\Delta_{31}(\Delta K_2) \xrightarrow{\frac{1}{2}(1+\beta^2)} \text{dot}\tag{F5}$$

(c) $\Delta^2 K$.

In cases where $\Delta^2 X_i$ and $\Delta^2 X_j$ each $\rightarrow x$ with high probability $\Delta^2 X_{ij} \rightarrow \text{dot}$

Now $\Delta^2 \Psi_{ij}' \rightarrow \text{dot}$

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

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

$\Delta^2 \Psi' = \text{stroke at double dots in the TM}$

$\Delta^2 X \xrightarrow{.1} 8$ since $\Delta^2 X_i \xrightarrow{.63} x$

$\Delta^2 K \xrightarrow{.1} 8$ at double dots in the TM (R0 p. 53) (F 7)

(d) The sum of key streams.

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

22G THE PLAIN LANGUAGE STREAM

(a) P and ΔP .

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 ΔP 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 R0 pp. 21, 45 - 7 and to P counts on R2 pp. 83, 110 - 2)

(b) Heterogenous nature of P and ΔP .

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 occurrences of each ΔP letter occurs at the foot of each column.

Fig. 22 (IV) (Continued)

Fig. 22 (V)

Fig. 22 (VI).

THE D STREAM TYPE A (CdZ 3110 8.4.45).

Dottage

D₁	D₂	L₁	L₂	L₃	L₄	L₅	L₆	L₇	L₈	L₉	L₁₀	L₁₁	L₁₂	L₁₃	L₁₄	L₁₅	L₁₆	L₁₇	L₁₈	L₁₉	L₂₀	L₂₁	L₂₂	L₂₃	L₂₄	L₂₅	L₂₆	L₂₇	L₂₈	L₂₉	L₃₀	L₃₁	L₃₂	L₃₃	L₃₄	L₃₅	L₃₆	L₃₇	L₃₈	L₃₉	L₄₀	L₄₁	L₄₂	L₄₃	L₄₄	L₄₅	L₄₆	L₄₇	L₄₈	L₄₉	L₅₀	L₅₁	L₅₂	L₅₃	L₅₄	L₅₅	L₅₆	L₅₇	L₅₈	L₅₉	L₆₀	L₆₁	L₆₂	L₆₃	L₆₄	L₆₅	L₆₆	L₆₇	L₆₈	L₆₉	L₇₀	L₇₁	L₇₂	L₇₃	L₇₄	L₇₅	L₇₆	L₇₇	L₇₈	L₇₉	L₈₀	L₈₁	L₈₂	L₈₃	L₈₄	L₈₅	L₈₆	L₈₇	L₈₈	L₈₉	L₉₀	L₉₁	L₉₂	L₉₃	L₉₄	L₉₅	L₉₆	L₉₇	L₉₈	L₉₉	L₁₀₀	L₁₀₁	L₁₀₂	L₁₀₃	L₁₀₄	L₁₀₅	L₁₀₆	L₁₀₇	L₁₀₈	L₁₀₉	L₁₁₀	L₁₁₁	L₁₁₂	L₁₁₃	L₁₁₄	L₁₁₅	L₁₁₆	L₁₁₇	L₁₁₈	L₁₁₉	L₁₂₀	L₁₂₁	L₁₂₂	L₁₂₃	L₁₂₄	L₁₂₅	L₁₂₆	L₁₂₇	L₁₂₈	L₁₂₉	L₁₃₀	L₁₃₁	L₁₃₂	L₁₃₃	L₁₃₄	L₁₃₅	L₁₃₆	L₁₃₇	L₁₃₈	L₁₃₉	L₁₄₀	L₁₄₁	L₁₄₂	L₁₄₃	L₁₄₄	L₁₄₅	L₁₄₆	L₁₄₇	L₁₄₈	L₁₄₉	L₁₅₀	L₁₅₁	L₁₅₂	L₁₅₃	L₁₅₄	L₁₅₅	L₁₅₆	L₁₅₇	L₁₅₈	L₁₅₉	L₁₆₀	L₁₆₁	L₁₆₂	L₁₆₃	L₁₆₄	L₁₆₅	L₁₆₆	L₁₆₇	L₁₆₈	L₁₆₉	L₁₇₀	L₁₇₁	L₁₇₂	L₁₇₃	L₁₇₄	L₁₇₅	L₁₇₆	L₁₇₇	L₁₇₈	L₁₇₉	L₁₈₀	L₁₈₁	L₁₈₂	L₁₈₃	L₁₈₄	L₁₈₅	L₁₈₆	L₁₈₇	L₁₈₈	L₁₈₉	L₁₉₀	L₁₉₁	L₁₉₂	L₁₉₃	L₁₉₄	L₁₉₅	L₁₉₆	L₁₉₇	L₁₉₈	L₁₉₉	L₂₀₀	L₂₀₁	L₂₀₂	L₂₀₃	L₂₀₄	L₂₀₅	L₂₀₆	L₂₀₇	L₂₀₈	L₂₀₉	L₂₁₀	L₂₁₁	L₂₁₂	L₂₁₃	L₂₁₄	L₂₁₅	L₂₁₆	L₂₁₇	L₂₁₈	L₂₁₉	L₂₂₀	L₂₂₁	L₂₂₂	L₂₂₃	L₂₂₄	L₂₂₅	L₂₂₆	L₂₂₇	L₂₂₈	L₂₂₉	L₂₃₀	L₂₃₁	L₂₃₂	L₂₃₃	L₂₃₄	L₂₃₅	L₂₃₆	L₂₃₇	L₂₃₈	L₂₃₉	L₂₄₀	L₂₄₁	L₂₄₂	L₂₄₃	L₂₄₄	L₂₄₅	L₂₄₆	L₂₄₇	L₂₄₈	L₂₄₉	L₂₅₀	L₂₅₁	L₂₅₂	L₂₅₃	L₂₅₄	L₂₅₅	L₂₅₆	L₂₅₇	L₂₅₈	L₂₅₉	L₂₆₀	L₂₆₁	L₂₆₂	L₂₆₃	L₂₆₄	L₂₆₅	L₂₆₆	L₂₆₇	L₂₆₈	L₂₆₉	L₂₇₀	L₂₇₁	L₂₇₂	L₂₇₃	L₂₇₄	L₂₇₅	L₂₇₆	L₂₇₇	L₂₇₈	L₂₇₉	L₂₈₀	L₂₈₁	L₂₈₂	L₂₈₃	L₂₈₄	L₂₈₅	L₂₈₆	L₂₈₇	L₂₈₈	L₂₈₉	L₂₉₀	L₂₉₁	L₂₉₂	L₂₉₃	L₂₉₄	L₂₉₅	L₂₉₆	L₂₉₇	L₂₉₈	L₂₉₉	L₃₀₀	L₃₀₁	L₃₀₂	L₃₀₃	L₃₀₄	L₃₀₅	L₃₀₆	L₃₀₇	L₃₀₈	L₃₀₉	L₃₁₀	L₃₁₁	L₃₁₂	L₃₁₃	L₃₁₄	L₃₁₅	L₃₁₆	L₃₁₇	L₃₁₈	L₃₁₉	L₃₂₀	L₃₂₁	L₃₂₂	L₃₂₃	L₃₂₄	L₃₂₅	L₃₂₆	L₃₂₇	L₃₂₈	L₃₂₉	L₃₃₀	L₃₃₁	L₃₃₂	L₃₃₃	L₃₃₄	L₃₃₅	L₃₃₆	L₃₃₇	L₃₃₈	L₃₃₉	L₃₄₀	L₃₄₁	L₃₄₂	L₃₄₃	L₃₄₄	L₃₄₅	L₃₄₆	L₃₄₇	L₃₄₈	L₃₄₉	L₃₅₀	L₃₅₁	L₃₅₂	L₃₅₃	L₃₅₄	L₃₅₅	L₃₅₆	L₃₅₇	L₃₅₈	L₃₅₉	L₃₆₀	L₃₆₁	L₃₆₂	L₃₆₃	L₃₆₄	L₃₆₅	L₃₆₆	L₃₆₇	L₃₆₈	L₃₆₉	L₃₇₀	L₃₇₁	L₃₇₂	L₃₇₃	L₃₇₄	L₃₇₅	L₃₇₆	L₃₇₇	L₃₇₈	L₃₇₉	L₃₈₀	L₃₈₁	L₃₈₂	L₃₈₃	L₃₈₄	L₃₈₅	L₃₈₆	L₃₈₇	L₃₈₈	L₃₈₉	L₃₉₀	L₃₉₁	L₃₉₂	L₃₉₃	L₃₉₄	L₃₉₅	L₃₉₆	L₃₉₇	L₃₉₈	L₃₉₉	L₄₀₀	L₄₀₁	L₄₀₂	L₄₀₃	L₄₀₄	L₄₀₅	L₄₀₆	L₄₀₇	L₄₀₈	L₄₀₉	L₄₁₀	L₄₁₁	L₄₁₂	L₄₁₃	L₄₁₄	L₄₁₅	L₄₁₆	L₄₁₇	L₄₁₈	L₄₁₉	L₄₂₀	L₄₂₁	L₄₂₂	L₄₂₃	L₄₂₄	L₄₂₅	L₄₂₆	L₄₂₇	L₄₂₈	L₄₂₉	L₄₃₀	L₄₃₁	L₄₃₂	L₄₃₃	L₄₃₄	L₄₃₅	L₄₃₆	L₄₃₇	L₄₃₈	L₄₃₉	L₄₄₀	L₄₄₁	L₄₄₂	L₄₄₃	L₄₄₄	L₄₄₅	L₄₄₆	L₄₄₇	L₄₄₈	L₄₄₉	L₄₅₀	L₄₅₁	L₄₅₂	L₄₅₃	L₄₅₄	L₄₅₅	L₄₅₆	L₄₅₇	L₄₅₈	L₄₅₉	L₄₆₀	L₄₆₁	L₄₆₂	L₄₆₃	L₄₆₄	L₄₆₅	L₄₆₆	L₄₆₇	L₄₆₈	L₄₆₉	L₄₇₀	L₄₇₁	L₄₇₂	L₄₇₃	L₄₇₄	L₄₇₅	L₄₇₆	L₄₇₇	L₄₇₈	L₄₇₉	L₄₈₀	L₄₈₁	L₄₈₂	L₄₈₃	L₄₈₄	L₄₈₅	L₄₈₆	L₄₈₇	L₄₈₈	L₄₈₉	L₄₉₀	L₄₉₁	L₄₉₂	L₄₉₃	L₄₉₄	L₄₉₅	L₄₉₆	L₄₉₇	L₄₉₈	L₄₉₉	L₅₀₀	L₅₀₁	L₅₀₂	L₅₀₃	L₅₀₄	L₅₀₅	L₅₀₆	L₅₀₇	L₅₀₈	L₅₀₉	L₅₁₀	L₅₁₁	L₅₁₂	L₅₁₃	L₅₁₄	L₅₁₅	L₅₁₆	L₅₁₇	L₅₁₈	L₅₁₉	L₅₂₀	L₅₂₁	L₅₂₂	L₅₂₃	L₅₂₄	L₅₂₅	L₅₂₆	L₅₂₇	L₅₂₈	L₅₂₉	L₅₃₀	L₅₃₁	L₅₃₂	L₅₃₃	L₅₃₄	L₅₃₅	L₅₃₆	L₅₃₇	L₅₃₈	L₅₃₉	L₅₄₀	L₅₄₁	L₅₄₂	L₅₄₃	L₅₄₄	L₅₄₅	L₅₄₆	L₅₄₇	L₅₄₈	L₅₄₉	L₅₅₀	L₅₅₁	L₅₅₂	L₅₅₃	L₅₅₄	L₅₅₅	L₅₅₆	L₅₅₇	L₅₅₈	L₅₅₉	L₅₆₀	L₅₆₁	L₅₆₂	L₅₆₃	L₅₆₄	L₅₆₅	L₅₆₆	L₅₆₇	L₅₆₈	L₅₆₉	L₅₇₀	L₅₇₁	L₅₇₂	L₅₇₃	L₅₇₄	L₅₇₅	L₅₇₆	L₅₇₇	L₅₇₈	L₅₇₉	L₅₈₀	L₅₈₁	L₅₈₂	L₅₈₃	L₅₈₄	L₅₈₅	L₅₈₆	L₅₈₇	L₅₈₈	L₅₈₉	L₅₉₀	L₅₉₁	L₅₉₂	L₅₉₃	L₅₉₄	L₅₉₅	L₅₉₆	L₅₉₇	L₅₉₈	L₅₉₉	L₆₀₀	L₆₀₁	L₆₀₂	L₆₀₃	L₆₀₄	L₆₀₅	L₆₀₆	L₆₀₇	L₆₀₈	L₆₀₉	L₆₁₀	L₆₁₁	L₆₁₂	L₆₁₃	L₆₁₄	L₆₁₅	L₆₁₆	L₆₁₇	L₆₁₈	L₆₁₉	L₆₂₀	L₆₂₁	L₆₂₂	L₆₂₃	L₆₂₄	L₆₂₅	L₆₂₆	L₆₂₇	L₆₂₈	L₆₂₉	L₆₃₀	L₆₃₁	L₆₃₂	L₆₃₃	L₆₃₄	L₆₃₅	L₆₃₆	L₆₃₇	L₆₃₈	L₆₃₉	L₆₄₀	L₆₄₁	L₆₄₂	L₆₄₃	L₆₄₄	L₆₄₅	L₆₄₆	L₆₄₇	L₆₄₈	L₆₄₉	L₆₅₀	L₆₅₁	L₆₅₂	L₆₅₃	L₆₅₄	L₆₅₅	L₆₅₆	L₆₅₇	L₆₅₈	L₆₅₉	L₆₆₀	L₆₆₁	L₆₆₂	L₆₆₃	L₆₆₄	L₆₆₅	L₆₆₆	L₆₆₇	L₆₆₈	L₆₆₉	L₆₇₀	L₆₇₁	L₆₇₂	L₆₇₃	L₆₇₄	L₆₇₅	L₆₇₆	L₆₇₇	L₆₇₈	L₆₇₉	L₆₈₀	L₆₈₁	L₆₈₂	L₆₈₃	L₆₈₄	L₆₈₅	L₆₈₆	L₆₈₇	L₆₈₈	L₆₈₉	L₆₉₀	L₆₉₁	L₆₉₂	L₆₉₃	L₆₉₄	L₆₉₅	L₆₉₆	L₆₉₇	L₆₉₈	L₆₉₉	L₇₀₀	L₇₀₁	L₇₀₂	L₇₀₃	L₇₀₄	L₇₀₅	L₇₀₆	L₇₀₇	L₇₀₈	L₇₀₉	L₇₁₀	L₇₁₁	L₇₁₂	L₇₁₃	L₇₁₄	L₇₁₅	L₇₁₆	L₇₁₇	L₇₁₈	L₇₁₉	L₇₂₀	L₇₂₁	L₇₂₂	L₇₂₃	L₇₂₄	L₇₂₅	L₇₂₆	L₇₂₇	L₇₂₈	L₇₂₉	L₇₃₀	L₇₃₁	L₇₃₂	L₇₃₃	L₇₃₄	L₇₃₅	L₇₃₆	L₇₃₇	L₇₃₈	L₇₃₉	L₇₄₀	L₇₄₁	L₇₄₂	L₇₄₃	L₇₄₄	L₇₄₅	L₇₄₆	L₇₄₇	L₇₄₈	L₇₄₉	L₇₅₀	L₇₅₁	L₇₅₂	L₇₅₃	L₇₅₄	L₇₅₅	L₇₅₆	L₇₅₇	L₇₅₈	L₇₅₉	L₇₆₀	L₇₆₁	L₇₆₂	L₇₆₃	L₇₆₄	L₇₆₅	L₇₆₆	L₇₆₇	L₇₆₈	L₇₆₉	L₇₇₀	L₇₇₁	L₇₇₂	L₇₇₃	L₇₇₄	L₇₇₅	L₇₇₆	L₇₇₇	L₇₇₈	L₇₇₉	L₇₈₀	L₇₈₁	L₇₈₂	L₇₈₃	L₇₈₄	L₇₈₅	L₇₈₆	L₇₈₇	L₇₈₈	L₇₈₉	L₇₉₀	L₇₉₁	L₇₉₂	L₇₉₃	L₇₉₄	L₇₉₅	L₇₉₆	L₇₉₇	L₇₉₈	L₇₉₉	L₈₀₀	L₈₀₁	L₈₀₂	L₈₀₃	L₈₀₄	L₈₀₅	L₈₀₆	L₈₀₇	L₈₀₈	L₈₀₉	L₈₁₀	L₈₁₁	L₈₁₂	L₈₁₃	L₈₁₄	L₈₁₅	L₈₁₆	L₈₁₇	L₈₁₈	L₈₁₉	L₈₂₀	L₈₂₁	L₈₂₂	L₈₂₃	L₈₂₄	L₈₂₅	L₈₂₆	L₈₂₇	L₈₂₈	L₈₂₉	L₈₃₀	L₈₃₁	L₈₃₂	L₈₃₃	L₈₃₄	L₈₃₅	L₈₃₆	L₈₃₇	L₈₃₈	L₈₃₉	L₈₄₀	L₈₄₁	L₈₄₂	L₈₄₃	L₈₄₄	L₈₄₅	L₈₄₆	L₈₄₇	L₈₄₈	L₈₄₉	L₈₅₀	L₈₅₁	L₈₅₂	L₈₅₃	L₈₅₄	L₈₅₅	L₈₅₆	L₈₅₇	L₈₅₈	L₈₅₉	L₈₆₀	L₈₆₁	L₈₆₂	L₈₆₃	L₈₆₄	L₈₆₅	L₈₆₆	L₈₆₇	L₈₆₈	L₈₆₉	L₈₇₀	L₈₇₁	L₈₇₂	L₈₇₃	L₈₇₄	L₈₇₅	L₈₇₆	L₈₇₇	L₈₇₈	L₈₇₉	L₈₈₀	L₈₈₁	L₈₈₂	L₈₈₃	L₈₈₄	L₈₈₅	L₈₈₆	L₈₈₇	L₈₈₈	L₈₈₉	L₈₉₀	L₈₉₁	L₈₉₂	L₈₉₃	L₈₉₄	L₈₉₅	L₈₉₆	L₈₉₇	L₈₉₈	L₈₉₉	L₉₀₀	L₉₀₁	L₉₀₂	L₉₀₃	L₉₀₄	L₉₀₅	L₉₀₆	L₉₀₇	L₉₀₈	L₉₀₉	L₉₁₀	L₉₁₁	L₉₁₂	L₉₁₃</

Fig. 22 (VII)

THE D STREAM TYPE B (GEP 5717 9.4.46).

Fig. 22 (VIII).

THE D STREAM TYPE C (JB 8347 20.3.45).

P	AP	INDIA D (T2 T3m)						INDIA D (T2+ T1m)					
		T ₂	T ₃	T ₂	T ₃	T ₂	T ₃	T ₂	T ₃	T ₂	T ₃	T ₂	T ₃
/	0002	0100	/	0034	0003	0034	0035	0034	0035	0034	0035	0034	0035
9	0126	0073	9	0035	0067	0035	0068	0035	0069	0035	0069	0035	0069
11	0092	0088	11	0032	0053	0043	0058	0053	0060	0054	0060	0054	0060
12	0173	0073	12	0044	0061	0042	0061	0042	0063	0043	0064	0043	0064
13	0095	0093	13	0046	0043	0043	0060	0049	0052	0050	0050	0054	0050
14	0054	0060	14	0041	0052	0039	0045	0034	0045	0035	0045	0034	0045
15	0296	0080	15	0038	0049	0048	0049	0045	0045	0045	0045	0045	0045
16	0003	0218	16	0068	0070	0075	0079	0077	0075	0075	0075	0075	0075
17	0034	0059	17	0040	0043	0047	0046	0034	0046	0034	0046	0034	0046
18	0172	0091	18	0074	0072	0042	0045	0032	0037	0034	0041	0039	0042
19	0032	0053	19	0036	0052	0047	0046	0047	0046	0047	0046	0047	0046
20	0083	0147	20	0068	0051	0065	0059	0065	0059	0055	0059	0055	0059
21	0071	0066	21	0048	0060	0050	0059	0057	0056	0050	0059	0057	0056
22	0045	0107	22	0044	0060	0053	0057	0048	0056	0055	0054	0053	0054
23	0172	0076	23	0029	0031	0038	0034	0038	0034	0036	0034	0038	0034
24	0001	0075	24	0034	0062	0025	0060	0038	0036	0035	0035	0035	0035
25	0156	0072	25	0039	0060	0055	0058	0028	0043	0043	0044	0043	0044
26	0107	0198	26	0031	0045	0084	0062	0076	0045	0077	0050	0072	0052
27	0014	0095	27	0049	0069	0049	0073	0095	0097	0046	0060	0042	0063
28	0085	0074	28	0029	0042	0040	0053	0040	0052	0045	0044	0034	0040
29	0086	0149	29	0055	0058	0044	0034	0052	0047	0052	0048	0050	0050
30	0015	0075	30	0046	0064	0048	0051	0036	0059	0039	0057	0045	0055
31	0032	0075	31	0053	0049	0045	0047	0042	0058	0031	0041	0036	0050
32	0034	0167	32	0069	0053	0074	0046	0065	0052	0063	0049	0060	0056
33	0195	0066	33	0034	0040	0026	0036	0043	0068	0043	0055	0049	0049
34	0083	0220	34	0083	0042	0084	0046	0068	0037	0067	0039	0070	0040
35	0008	0078	35	0049	0016	0041	0019	0050	0048	0040	0052	0038	0037
36	0097	0026	36	0019	0050	0023	0046	0018	0045	0032	0052	0032	0049
37	0093	0112	37	0049	0049	0043	0047	0047	0046	0033	0045	0031	0048
38	0008	0118	38	0067	0056	0051	0048	0047	0062	0064	0066	0062	0054
39	0126	0119	39	0050	0036	0054	0057	0060	0055	0053	0046	0118	0119
40	0026	0104	40	0045	0047	0056	0048	0044	0043	0038	0033	0036	0040
41	0000	0200	41	0038	0162	1933	1632	1503	1632	1503	1632	1503	1632
42	1791	1821	42	1791	1821	1791	1821	1791	1821	1791	1821	1791	1821

These figures are not entered as $\Delta_{\text{D}^{\text{opt}}}$, $\Delta_{\text{D}^{\text{opt}}}$ and $\Delta_{\text{D}^{\text{opt}}}$ are normally counted before T2 is set and limitation positions determined (See 2).

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 28 dots JB	ΔD 26 dots CDB	ΔD 26 dots C2Z	ΔD 20 dots JP
/	149	175	213	117	188	164
9	46	95	166	148	189	111
H	142	119	102	94	123	102
T	40	83	79	69	86	87
O	71	116	88	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	168	102	118
Q	324	129	96	95	77	108
W	275	57	90	95	88	93
5	32	183	161	126	224	136
8	112	132	255	110	189	106
K	15	70	63	80	92	93
J	41	134	110	130	92	120
D	1	80	71	86	73	72
P	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 OF 100 $\sqrt{\frac{31}{N}}$	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 [illegible]P 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 impulses differ little in frequency. Hard to test on X_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. (R0 p. 67)

(c) Component types of language.

(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) Single Punctuation (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 Konigsberg exchange or on Rome Bream, but after the Konigsberg 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 QKP 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	N O C K E 5 N 8 9 N O C K E 5 N 8 9 K E I N E 5 N 8 9
ΔP	H P E C G Q W 5 3 H P E C G Q W 5 J C U R F G Q W 5

(d) P counts on i-2 impulses.

The best P_i bulge is on $P_3 = x$ for punctuation (single or double) and on $P_5 =$ dot for language. Normally $P_1, P_2, P_4, P_5 \rightarrow$ dot and $P_3 \rightarrow x$ 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. 86.

	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
$\Delta P_2 = .$	1565	1863	1572	
$\Delta P_{12} = .$	2135	1972	1670	
$\Delta P_{13} = .$	1874	1637	1821	
$\Delta P_{34} = x$	1461	1829	1791	
$\Delta P_{25} = .$	1881	1654	1766	
$\Delta P_{45} = .$	2025	1852	1478	

Fig. 22 (X)

(e) ΔP counts on 1 and 2 impulses.

Bulges on ΔP_1 are of interest only in the case of ΔP_2 on messages with \bar{X}_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 $\Delta P_2 = \text{dot}$.

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 $\Delta P_{12} \rightarrow$ dot is weak (though usually positive) and the best bulges are on $\Delta P_{34} \rightarrow$ x and $\Delta P_{13} \rightarrow$ dot. See Fig. 22(x)

PB ($\Delta P_i =$ dot) is defined as Π_i

PB ($\Delta P = \Theta$) is defined as Π_Θ

(f) $\Delta^2 P$.

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 S M 3 4 all occurring over 5% of the time. (R0 p. 50.)

(g) Bigrams in P and ΔP .

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

No statistics of ΔP bigrams were taken.

(h) The sum of two P streams.

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 in fact in depth or not. A Scoring table for alleged depths is given in 22 W(c).

22H THE DECHI STREAM

$$D = P + \Psi'$$

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

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

(a) Frequency of letters in ΔD .

Applying (E1) and (E2) we get

$$P(\Delta D = \Theta) = \sum_{\Phi} \{ P(\Delta \Psi' = \Phi) \cdot P(\Delta P = \Theta + \Phi) \} \quad (H1)$$

$$\delta_{\Theta} = PB(\Delta D = \Theta) = \frac{1}{32} \sum_{\Phi} \{ \beta_{\Phi} \cdot \Pi_{\Theta+\Phi} \} \quad (H2)$$

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 $P(\Delta \Psi' = /) = (1 - a) + a(1 - b)^5 = \text{approx. } (1 - a)$, 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 psis. 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 $(\Theta + 8)$ and of $(\Theta + V)$ etc. in ΔD . Letters whose frequency in ΔD gets a substantial contribution in this way are known as "Good T.M. x letters" (R0 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

$$P(\Delta D = \Theta) = (1 - a) \cdot P(\Delta P = \Theta) + aP(\Delta D = \Theta \mid TM\ x) \quad (H3)$$

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

$$P(\Delta D = \Theta) = [(1 - a) P(\Delta P = \Theta) + \frac{1}{2}a'P(\Delta D = \Theta \mid TM\ x)] + [\frac{1}{2}P(\Delta D = \Theta \mid TM\ x)]$$

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

$$\therefore P(\Delta D = \Theta \mid L = .) = P(\Delta D = \Theta \mid TM\ x) \quad (H4)$$

$$P(\Delta D = \Theta \mid L = x) = \{(1 - a') P(\Delta P = \Theta) + a'P(\Delta D = \Theta \mid TM\ x)\} \quad (H5)$$

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 T.M. x, and the proportion of ΔP in the reminder 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 $P(\Delta P = \Theta)$ put equal to zero, where Θ 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 \bar{X}_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 the $\Delta\Psi'$, ΔD counts are given separately for \bar{X}_2 lim. and $\bar{X}_2 \bar{\Psi}'_1$ lim., and in the case of \bar{X}_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 marked by random variations. The importance of good T.M. x 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 \bar{X}_2 limitation.

(d) ΔD counts with $\bar{X}_2 \bar{P}_5$ limitation.

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

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

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

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

	$\bar{X}_2 = x$	$\bar{X}_2 = .$
/	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.

(e) ΔD against B.M..

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

$$P(\Delta D = \Theta \mid BM = x) = P(\Delta D = \Theta \mid TMx) \quad (H6)$$

$$P(\Delta D = \Theta \mid BM = .) = \{\frac{1}{2}P(\Delta D = \Theta) + \frac{1}{2}P(\Delta D = \Theta \mid TMx)\} \quad (H7)$$

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

(f) ΔD counts on 1 and 2 impulses.

From (E4) we get $\delta_{ij} \equiv P\beta$ [illegible] ($\Delta D_{ij} = \text{dot}$) $= \beta'_{ij} \cdot \Pi_{ij}$

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

$$\delta_{ij} = \Pi_{ij} \cdot \beta \quad (\text{H8})$$

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

$$\therefore PB(\Delta D_i + \text{lim} = \text{cross}) = \Pi_i \cdot \beta$$

$$\therefore (\text{for } X_2 = \text{lim}) \quad PB(\Delta D_2 + \hat{X}_2 \rightarrow x) = \Pi_2 \cdot \beta \quad (\text{H9})$$

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

$$\therefore \Delta D_2 \rightarrow \text{dot}$$

$$\Delta D_2 + \text{Lim} \rightarrow \text{dot} \quad (\text{R1 p. 9}) \quad (\text{H10})$$

Figs. 22 (VI)(VII)(VIII) give scores [illegible] for the various ΔD counts shown.

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

$$\underline{\delta}_{..} \equiv PB(\Delta D_i = . \quad \Delta D_j = . \mid L = .)$$

$$\bar{\delta}_{..} \equiv PB(\Delta D_i = . \quad \Delta D_j = . \mid L = x)$$

$$\delta_{..} \equiv PB(\Delta D_i = . \quad \Delta D_j = .) \quad \text{and so on}$$

$\underline{\delta}_{..}$	$\frac{1}{2} \{ \beta(\Pi_{..} + \Pi_{xx}) - \beta(\Pi_{..} - \Pi_{xx}) \}$
$\underline{\delta}_{xx}$	$\frac{1}{2} \{ \beta(\Pi_{..} + \Pi_{xx}) + \beta(\Pi_{..} - \Pi_{xx}) \}$
$\underline{\delta}_{x.}$	$\frac{1}{2} \{ -\beta(\Pi_{..} + \Pi_{xx}) - \beta(\Pi_{x.} - \Pi_{.x}) \}$
$\underline{\delta}_{.x}$	$\frac{1}{2} \{ -\beta(\Pi_{..} + \Pi_{xx}) + \beta(\Pi_{x.} - \Pi_{.x}) \}$
$\bar{\delta}_{..}$	$\frac{1}{2} (1+\beta) \{ -\beta^2(\Pi_{..} + \Pi_{xx}) + 2\beta\Pi_{..} + (3\Pi_{..} + \Pi_{xx}) \}$
$\bar{\delta}_{xx}$	$\frac{1}{2} (1+\beta) \{ -\beta^2(\Pi_{..} + \Pi_{xx}) + 2\beta\Pi_{xx} + (3\Pi_{xx} + \Pi_{..}) \}$
$\bar{\delta}_{x.}$	$\frac{1}{2} (1+\beta) \{ +\beta^2(\Pi_{..} + \Pi_{xx}) + 2\beta\Pi_{x.} + (3\Pi_{x.} + \Pi_{.x}) \}$
$\bar{\delta}_{.x}$	$\frac{1}{2} (1+\beta) \{ +\beta^2(\Pi_{..} + \Pi_{xx}) + 2\beta\Pi_{.x} + (3\Pi_{.x} + \Pi_{x.}) \}$
$\delta_{..}$	$+ \frac{1}{2}\beta(\Pi_{..} + \Pi_{xx})$
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) $\delta_{..} = \delta_{xx}$ and $\delta_{x..} = \delta_x$. Whatever the relative values of $\Pi_{..}$ and Π_{xx} . This shows that the benefits of counting against X_2 limitation
-

increase as $|\Pi \dots - \Pi_{xx}|$ increases (R2 p. 96) (H11)

$$(ii) \quad \underline{\delta}_{ii} = \frac{1}{2} (\underline{\delta}_{\dots} + \underline{\delta}_{xx}) = \beta^2 (\Pi_{\dots} + \Pi_{xx}) = \beta^2 \Pi_{ii}$$

$$\text{But } \underline{\delta}_{ij} = \frac{1}{2} (\underline{\delta}_{ij} + \bar{\underline{\delta}}_{ij}) = \beta \Pi_{ij} \quad (\text{from H6}).$$

$$\therefore \bar{\underline{\delta}}_{ij} = \Pi_{ij} (2\beta - \beta^2) = \beta(2 - \beta) \Pi_{ij}$$

$$\therefore \frac{\bar{\underline{\delta}}_{ij}}{\underline{\delta}_{ij}} = \frac{2 - \beta}{\beta} \quad (\text{H12})$$

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

ΔD_1	ΔD_2	L	Type A	Type B	Type C
.	.	x	490	404	406
.	x	x	278	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 the result the count of $\Delta^2 D$ has no statistical (or other) advantages over that of ΔD . (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

$$Z = X + D$$

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

∴ Adapting (6a) and (6c) we get

$$\Delta Z_{ij} \xrightarrow{\frac{1}{2}(1+\theta_{ij})} \Delta X_{ij} \quad (J1)$$

$$\Delta_{\text{word}}(\Delta Z_{ij}) \xrightarrow{\frac{1}{2}(k+\theta_{ij}^2)} \text{dot}, \quad (J2)$$

and in particular

$$\Delta_{1271}(\Delta Z_{12}) \xrightarrow{\frac{1}{2}(k+\theta_{12}^2)} \text{dot}. \quad (J3)$$

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 context 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 the length 3200, of ΔD for a particular link and the 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

$$n^{(1)}_\Theta, n^{(2)}_\Theta, \dots, n^{(r)}_\Theta.$$

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

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

where

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

$$r\sigma_\Theta^2 = \sum_{s=1}^r (n_\Theta^{(s)} - n_\Theta)^2 \quad (K1)$$

In order to estimate σ_Θ it is easier to calculate $\sum_{s=1}^r |n_\Theta^{(s)} - n_\Theta|$, which can be done

in a self-checking way, and to write

$$\delta\sigma_0 = \sum_{k=1}^r n_0^{(k)} - n_0 | , \quad (K2)$$

since the expected value of the modulus of the deviation from the mean is $\sigma\sqrt{\frac{2}{\pi}} \approx \sigma$ in the case of 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 $10 \log_{10} \{32(P_a + P_b) = \Theta\}$ (W1)

The following table gives the centiban 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

$$\begin{aligned}\Delta D_a + \Delta D_b &= \Delta \Psi'_a + \Delta P_a + \Delta \Psi'_b + \Delta P_b \\ &= \Delta \Psi'_a + \Delta \Psi'_b \quad (\text{since } \Delta P_a = \Delta P_b)\end{aligned}$$

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

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

$$P(\Delta\Psi'_a + \Delta\Psi'_b = \Theta_n^m \mid TM_a = ., TM_b = x) = Y_n^m = \left(\frac{1+\beta}{2}\right)^m \left(\frac{1-\beta}{2}\right)^n \quad (W2)$$

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

$$\begin{aligned} P(\Delta\Psi'_a + \Delta\Psi'_b = \Theta_n^m) &= (1-a)^2 X_n^m + 2a(1-a)Y_n^m + a^2 Z_n^m \\ &= \frac{\beta^2 X_n^m + 2\beta Y_n^m + Z_n^m}{(1+\beta)^2} \end{aligned} \quad (W4)$$

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

$$\begin{aligned} P(\Delta\Psi'_a + \Delta\Psi'_b = \Theta_n^m \mid L_a + L_b = .) &= P(\Delta\Psi'_a + \Delta\Psi'_b = \Theta_{n+1}^m \mid P(\Delta\Psi'_a + \Delta\Psi'_b = \Theta_1^0)) \\ &= \frac{P(\Delta\Psi'_a + \Delta\Psi'_b = \Theta_{n+1}^m)}{P(\Delta\Psi'_a + \Delta\Psi'_b = \Theta_1^0)} \\ &= 2P(\Delta\Psi'_a + \Delta\Psi'_b = \Theta_{n+1}^m) \end{aligned} \quad (W5)$$

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

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)

(c) The sum of two key streams.

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 $\Delta Z_a + \Delta Z_b = \Delta K_a + \Delta K_b$

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

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

$$P.B.(\Delta D = \Theta) = \frac{1}{32} \sum_{\Phi} P.B.(\Delta P = \Phi) P.B.(\Delta \Psi' = \Theta + \Phi) \quad (X1)$$

The problem of solving these equations for $P.B.(\Delta P)$ given $P.B.(\Delta D)$ 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 reasons why proportional bulges were first introduced are mentioned in 21(J) (R1, 20).

(b) Application to Motor Runs.

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

$$P.B.(\Delta D | B.M. = .) = \frac{1}{2} P.B.(\Delta P) + \frac{1}{2} P.B.(\Delta P + \Delta \Psi'),$$

and the second term can be written as a 'Faltung', i.e. in a form similar to (1) above. When the limitation is \bar{X}_2 the count of ΔD against \bar{X}_2 = dot provides a sample of ΔD against motor crosses and we can therefore obtain a good idea of the $L.C. \propto \Delta P$ and of the expected score in a motor run (R0 47-50). For limitations other than \bar{X}_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 $P.B.(\Delta P)$ 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 Φ . 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

$$F^*(\Phi) = \frac{1}{\sqrt{32}} \sum_{\Theta} F(\Theta) (-1)^{\Theta \cdot \Phi} \quad (\text{X2})$$

where $\Theta \cdot \Phi$ is the scalar product of Θ and Φ when they are considered as vectors with 0 for dot and 1 for cross. For example $(U.N.) = 1.0 + 1.0 + 1.1 + 0.0 = 1$. 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

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

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

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)

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

(see foot-note).

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

This gives $P.B.^*(\Delta P)$ in terms of $P.B.^*(\Delta D)$ and $P.B.^*(\Delta \Psi')$ and hence $P.B.(\Delta P)$ in terms of $P.B.(\Delta D)$ 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 $P.B.(\Delta D)$ for definiteness, we have

$$\begin{aligned} F^*(J) &= \frac{1}{\sqrt{32}} \left\{ \sum_{\Phi_1+\Phi_2+\Phi_4=1} F(\Phi) - \sum_{\Phi_1+\Phi_2+\Phi_4=0} F(\Phi) \right\} \\ &= \frac{2}{\sqrt{32}} \sum_{\Phi_1+\Phi_2+\Phi_4=1} F(\Phi) \end{aligned}$$

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

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

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

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

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 $\sum n_\Theta = N$, to estimate the decibanage in favour of the X'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

$$P_\Theta^{(i)} ; (\Theta = /, 9, H \dots, i = 1, 2, 3 \dots).$$

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

$$f_i = \prod_\Theta (32P_\Theta^{(i)})^{n_\Theta} \quad (Y1)$$

This factor can be conveniently expressed in decibans of course.

Now, by the theorem of the weighted average of factors (see 21(1)), the factor in favour of the X'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 X^2 test. This has the disadvantage that the X^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

$$\sum_\Theta n_\Theta \log n_\Theta - N^2 (\log N - \log 32), \quad (Y3)$$

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 decibangage will not be more than 80 d.b. too high.

23 MACHINE SETTING

- 23A Introduction
 - 23B The choice of runs
 - 23C Weighing the evidence
 - 23D Annotated Exhibits
 - 23E X-setting with \bar{X}_2 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 X-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

$$D \equiv Z + X$$

(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 $41 \times 31 \times 29 \times 26 \times 23 = 23,561,898$ 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 (22H). 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.

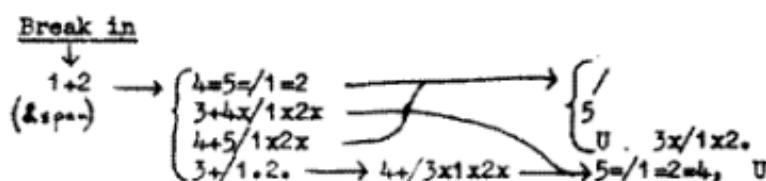
Originally the Berlin ends of Western links were type B, the outer ends of most Western links and both ends of Eastern links were type A. Later the situation became confused and so did the notation A, B, C... [of 22 G(c)]

(b) Practical Runs.

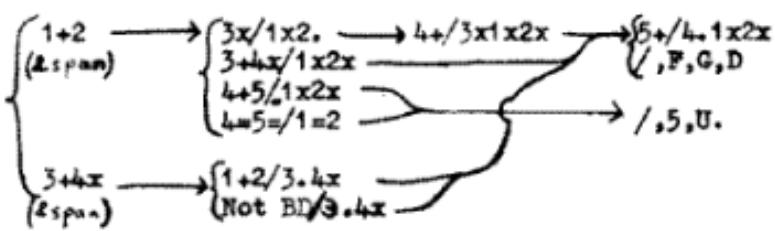
For rapid setting it is insufficient to remember the frequencies of the 32 individual letters: it is necessary to know explicitly what are the best runs for direct application; e.g. to know that $1 + 2 = .$ is the best run involving only two wheels. This is of course deducible from the 32 letter count, 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 23C(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 p. 110).

(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 \bar{X}_2 limitation may require a quite different break-in. (23 E)

Other runs are mentioned in 23 J: R1 is full of much references; recent notes include R3 p. 131, R5 p. 106.

23C 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 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 (K)]. In X-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.]

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 X_3 the sigma-age of $3x/1x2$, is 2.4σ

and of $3+4x/1x2x$ is 3.9σ

According to the table, the settings of X_3 , X_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 $\frac{\text{expected bulge}}{\sigma} = \frac{\xi N}{\sqrt{p(1-p)}} = \xi \sqrt{N \frac{p}{1-p}}$, where ξ is the proportional bulge. For $p = \frac{1}{2}, \frac{1}{4}, \frac{1}{6}$ 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{X}_2 limitation, but no special method is used except that all runs are made against \bar{X}_2 crosses only. (The operator neglects the four letter count on $\Delta D_1 \Delta D_2$ it may be repeated that on the whole text there can be only a random bulge of xx ever ..).

The items in the first line are message number, time and date sent, wheel day and Colossus number.

BR 3407 0450/24/2 WD 23/2 COL 7

T 6020

1P2/L R 3106 A 1553 Φ 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 3.7Φ
 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

T 6020 is the text length, measured as a check, as soon as the tape is on Colossus.

1P2/L is typewriterese for $1+2/\bar{X}_2$
 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 $\bar{X}_2 = x$.

At random the expected number (A) of these when $1+2 = .$ is
 $\frac{1}{2} \times 3106 = 1553$.

Φ (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 + $2\frac{1}{4}\sigma$.

The best score is 3.7σ, not even "good" [23C(a)] but worth spanning [23F(o)]. 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

0128
0131
0128
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".

0130
0129

SPAN 01-4500

1259
1064 2B 195 B 98 4.1Φ

SPANNING 01-4500

Here the operator makes the
mistake of neglecting a 4-letter count
for ΔD_1 , ΔD_2 [23E(h)] this is easily
reconstructed and would read

.	.	592
.	x	498
x	x	667
x	.	567

SET K1 K2 40 28 GOOD

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,
 $\sigma = \frac{1}{4} \sqrt{3R} = \frac{1}{4} \sqrt{3 \times 1259} = 15.4.$

ST as above.

SET K4 K5 05 22 GOOD

/// 555 UUU
 168 212 177

 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 best score is 4.15σ. It should be noticed that three scores above the set total have X₄ at 05; and that the X₄ settings are 22, 22+7, 22+14, suggesting a wheel-slide [23G] of 7 on X₄, but fortunately one too weak to make the setting really doubtful.

The most likely letters to set X's are /, 5, U: to decide which the operator counts / & 9, 5 & 8, U & K; and because 5 & 8 are numerous (212) chooses 5

K1 K2 K3 K4 K5
 40 28 08 05 22 SPAN 01-4500
 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

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 } is printed by means
 40 28 08 05 } of P.M.H. so that
 22 } errors in Colossus
 setting will be manifest.

AG X2 XX means against $\bar{X}_2=x$.

The settings for X₁ X₂ X₃ X₄ X₅ were not very strong, so that although the final X₃ score makes them "certain", it

L 0053	0094
P 0088	0067
i 0072	0055
4 0057	0065
A 0066	0078
U 0111	0067
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

ALL CERTAIN SPAN 01-4500
E.M. LEWIS.

is just as well to inspect the letter count.

This resolves all doubts as to the correctness of the settings, e.g. X₅ is made very certain by the scores for U>Q, 5>J, F>X. The count is in fact much better than average; the worst contradictions with the pairs in 23 H(e) are CM, DB, ZE.

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.

The chis are therefore set back equally and stepped together, counting 3GU5F (G evidently in mistake for J)

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

For this run R is $\frac{16}{21} \times 1520$ (There are 16 x's in X₂).

A = $\frac{5}{32} \times \frac{31}{16} \times 1520$ (3GU5F are five letters out of 32).

$$\sigma = \sqrt{\frac{16}{31} \times 1520 \times \frac{5}{32} \times \frac{27}{32}} \quad (\text{using } \sqrt{Rp(1-p)})$$

The sigma-age obtained is 4.3σ 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.

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
0028	0024

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 just have been set by itself.

The de-chi check [23E(f)] is made by switching Q = Z + X and counting 1x, 2x, 3x, 4x, 5x, simultaneously on the five counters, spanning 01-02. The scores obtained are 1, 1, 1, 0, 0, showing that the second letter of Z + X is U; similarly GYN... [01-08 is a mistake for 02-09]

0040	0016	Four letters are found at intervals of
0037	0019	620 up to 3100, thereafter only the last
0017	0026	five.
0020	0028	
0050	0017	Message particulars are repeated
0029	0030	here because the de-chi check is sent
0015	0017	to the Tunny room for making the de-
0024	0024	chi tape: it is left here only because a
		motor run was ordered instead.
0022	0020	BR 3407 0450/24/2 WD 23/2 COL 7
0027	0019	T 6020
0027	0019	DE CHI ON 1ST 4500
0010	0024	K1 K2 K3 K4 K5
		40 28 08 05 22
0017	0021	01-08 UGYNPNS5X
0030	0030	620 5ZA/
0019	0030	1240 CYS5
0022	0023	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 33L.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

3P/4X 5P/4

MOTOR RUN 555 R 146 A 82 Ø 6.2

S3 S5

ST 100 ES 114

11 C 2350

M1 M2

13 C 2935

27 05 B 0091

15 C 2383

50 15 B 0105

18 C 2404

52 16 A 0102

21 C 2386

53 16 A 0106

29 C 2373

54 16 A 0117

34 C 2432

55 15 B 0111

36 C 2392

56 15 B 0104

441 C 2404

59 16 A 0106

43 C 2391

60 15 B 0101

08 C 2364

33 21 A 0103

11 C 2350

05 26 A 0100

SET S3 13

43 26 A 0102

999 R 640 A 320 Ø 12.6 ST 340

44 26 A 0101

S5

47 26 A 0101

05 A 0373

44 26 A 0102

07 A 0341

55 25 B 0104

10 A 0405

06 27 E 0101

16 A 0354

SET M1 M2 54 16

19 A 0365

1.2. 3*4 .5. R 4500 A 2250 Ø 33.5 ST

21 A 0533

ST 2350

23 A 0346

S1 S2 S3 S4 S5

26 A 0345

01 B 2352

32 A 0399

06 B 2481

37 A 0380

24 D 2449

42 A 0363

46 D 2352

43 A 0360

B 2352

45 A 0364

06 B 2481

48 A 0367

SET S2 06

53 A 0350

56 A 0353

58 A 0342

59 A 0367

IP/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 S5 21
//3344 - 48
SPAN 1 100 //3344 - 000
K1 K2 K3 K4 K5 S1 S2 S3 S4 S5 M1 N
40 28 08 05 22 12 06 13 24 21 54 1

DECODE FROM 02
9BOESE9FE1ND9ERST9DA5ZA889KR5A
ALL CERTAIN
D/1/GUEST.
all

SET S1 S4 [illegible]

23E X-SETTING WITH \bar{X}_2 LIMITATION

(a) Runs against $\bar{X}_2 = x$.

Bulges are greater when $\bar{X}_2 = x$ than when $\bar{X}_2 = .$

To run against $\bar{X}_2 = x$, 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, $\bar{X}_2 = x$ 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{X}_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 X-wheels; in fact, whenever it appears that a message is on \bar{X}_2 limitation, all subsequent runs are done against $\bar{X}_2 = x$.

(b) Break-in runs for \bar{X}_2 limitation.

There is often a better break-in than either 1+2 \bar{X}_2x , or 1+2. On the whole text, excluding random effects, 1 = ., 2 = ., are flat and 1x2x has the same bulge as 1.2.. Against $\bar{X}_2 = x$ this is not so, the bulges having the same direction as in ΔP . Against $\bar{X}_2 = .$, ΔP tends to appear reversed.

This suggests, if U58 are very numerous, the one-wheel break-in 2 = \bar{X}_2 . (since 2x \bar{X}_2x , 2. $\bar{X}_2.$ are equally strong, there is no point in running them separately); if /'s are very numerous (this is now rare) 2 ≠ \bar{X}_2 .

It suggests further, the runs 1x2x \bar{X}_2x , 1.2. $\bar{X}_2.$ or the combined run 1=2x \bar{X}_2 [for plugging and switching see 53 J(k)]

Note: the more consistently good run "1x2x \bar{X}_2x OR 1.2. $\bar{X}_2.$ " 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	$1+2 \cdot \bar{X}_1 x$	$1=2x \bar{X}_2$	$1=2x \bar{X}_2$
Second choice	$1=2x \bar{X}_2$	$1+2 \cdot \bar{X}_1 x$	$1+2$

(c) Theoretical not on A, σ , Θ , Φ .

With negligible error A and σ for the runs $2=\bar{X}_2$, $1=2x \bar{X}_2$ may be taken as

$$2 = \bar{X}_2 : \quad A = \frac{N}{2}, \quad \sigma = \frac{1}{2} \sqrt{N(1-\Theta^2)},$$

$$1 = 2x \bar{X}_2 : \quad A = \frac{N}{4}; \quad \sigma = \frac{1}{4} \sqrt{3N\left(1 - \frac{\Theta^2}{3}\right)}$$

Where Θ is the proportional bulge of $\Delta X_2 + \bar{X}_2 = .$

In practice σ is calculated by supposing $\Theta = 0$, though because Θ may be as great as $\frac{1}{2}$, the error is not always negligible [R5 p. 93].

The exact expressions for A and σ are

$$2 = \bar{X}_2 : A = \frac{N}{2} (1 + \Theta\Phi); \sigma^2 = \frac{N^2}{4(N-1)} \left\{ 1 - (\Theta^2 - 2\Theta\Phi + \Phi^2 - \Theta^2\Phi^2) \right\}$$

$$1 = 2 = \bar{X}_2 : A = \frac{N}{4} (1 + \Theta\Phi); \sigma^2 = \frac{3N^2}{16(N-1)} \left\{ 1 - \frac{1}{3} (\Theta^2 - 4\Theta\Phi + \Phi^2 - \Theta^2\Phi^2) \right\}$$

where Φ is the proportional bulge of $\Delta Z_2 = .$, its expected value being $\Theta\beta\Pi_x$.

(d) Expected sigma-age of \bar{X}_2 limitation break-ins.

The above table para (b) is constructed by finding the expected sigma-ages, WZ (for the last three it is supposed that $\Theta = 0$).

$$1 + 2. : \frac{\beta\sqrt{N}}{2\sqrt{6}} \Pi_{\infty} \sqrt{6} \left(1 + \frac{\Pi_{\infty}}{\Pi_{\infty}} \right)$$

$$1 + 2 = \bar{X}_2 x : \frac{\beta\sqrt{N}}{2\sqrt{6}} \Pi_{\infty} \sqrt{3}(2 - \beta) \left(1 + \frac{\Pi_{\infty}}{\Pi_{\infty}} \right)$$

$$1 = 2 = \bar{X}_2 : \frac{\beta\sqrt{N}}{2\sqrt{6}} \Pi_{\infty} 2\sqrt{2}$$

$$2 = \bar{X}_2 : \frac{\beta\sqrt{N}}{2\sqrt{6}} \Pi_{\infty} \sqrt{6} \left(1 + \frac{\Pi_{\infty}}{\Pi_{\infty}} \right)$$

$$\begin{aligned} \bar{X}_2 x \\ \text{or } 1.2. \bar{X}_2 x \\ \text{or } 1.2. \bar{X}_2. \end{aligned} \left. \right\} : \frac{\beta\sqrt{N}}{2\sqrt{6}} \Pi_{\infty} \sqrt{\frac{3}{5}} \left\{ (5 - \beta) + (3 - \beta) \frac{\Pi_{\infty}}{\Pi_{\infty}} \right\}$$

Comparing these

1+2. is better than 1+2. $\bar{X}_2 x$ if $\sqrt{2} > 2 - \beta$, i.e. to the nearest integer [illegible] 28;

$1 = 2 = \bar{X}_2$ is better than $1+2$. if $\frac{\Pi_{..}}{\Pi_{\infty}} < \frac{2}{\sqrt{3}} - 1$;

$1 = 2 = \bar{X}_2$ is better than $1+2. \bar{X}_2x$ if $\frac{\Pi_{..}}{\Pi_{\infty}} < \sqrt{\frac{2}{3}} \frac{2}{2-\beta} - 1$

$\frac{\Pi_{..}}{\Pi_{\infty}}$ 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 $2 = \bar{X}_2$.

It may be shown, similarly, but with more algebra, that neither component of $1 = 2 = \bar{X}_2$, i.e. $1.2. \bar{X}_2.$ or $1x2x \bar{X}_2x$, 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, 29.]

(e) $2 = \bar{X}_2$.

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 great as $\frac{1}{2}$), but will never be the strongest run unless $\frac{\Pi_{..}}{\Pi_{\infty}} > -\frac{1}{6}$

It takes very little time to run. [R1 pp. 5, 9; see R4 pp. 70, 92].

(f) QTO.

It is not always known beforehand whether \bar{X}_2 limitation is in use. A few links change the limitation frequently (this was common in the

days of \bar{P}_5 .) : Sixta is sometimes able to give log information about this (QTQ information).

(g) Tests for \bar{X}_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 X_1 and X_2 , $1+2 = .$ is counted against $\bar{X}_2 = x$ and against $\bar{X}_2 = ..$ There is an exact formula for the decibannage which this gives in favour of \bar{X}_2 limitation, in terms of motor dottage; but commonly a simpler inexact rule is used namely: for \bar{X}_2 limitation, the bulge against \bar{X}_2x is at least twice the bulge against $\bar{X}_2..$

The earlier rule, that for \bar{X}_2 limitation the sigma-age against $\bar{X}_2 = x$ should be greater than the sigma-age on the whole text, is grossly biased against \bar{X}_2 limitation. [See R4 p. 89. R4 pp. 7, 50, 55, 72.] If the motor dottage is high it may be impossible to decide whether the limitation is \bar{X}_2 until more wheels are set.

(h) 4-letter counts.

When a \bar{X}_2 limitation message is set on $1+2$, four counts are made against $\bar{X}_2 = x$: $1.2., 1.2x, 1x2x, 1x2..$ These confirm that \bar{X}_2 is in use and indicate which letter to run for, in particular whether to run for 58U or for / [R5 pp. 38, 71, 80].

(i) $C_3 = \bar{X}_2$.

In R5 p. 94 the run $5-4/ = 1x2x \bar{X}_2$ is suggested, but the evidence is not unbiased.

(j) $\bar{X}_2 + \bar{\bar{P}}_5$ limitation.

Since $P_5 \rightarrow .$, this shows the characteristics of \bar{X}_2 limitation weekly; the letter 5 is anomalous, being stronger against \bar{X}_2 dots [illegible] 74, 87.]

(k) The effect of corruption on $2 = X_2, 1 = 2 = \bar{X}_2$.

If there are many corrupt letters replaced by 9's, the not 99 gadget should be used to ignore these; otherwise, except when $\Theta = 0$, 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

$$\text{for } 2 = \bar{X}_2 : S\sqrt{1 - \lambda} + \lambda\Theta\sqrt{N};$$

$$\text{for } 1 = 2 = \bar{X}_2 : S\sqrt{1 - \lambda} + \lambda\Theta\sqrt{\frac{N}{3}};$$

23F 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 X'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 X'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 sometime be detected by inspection of the 1+2 scores. If several (say 3) letters are omitted, the settings of all X-wheels will be increased by three.

A pair of scores such as	26 17	1398	5.9σ
	29 20	1253	4.1σ

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 [23 G(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 3.7σ unless a certain setting 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 the means of a Slide Run. The X'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 [illegible].

(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, count99'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) M 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 [illegible] two letters inserted, and become a single message so far as X-setting is concerned. [of 11B(k), 11D(d)]

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

ΔX_1	x x .	x .	x . x . x	. x	. x	. x	. x	. x	. x	.
ΔX_2 , 2 back	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 ΔX 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 ΔX_1 and ΔX_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 X_1 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; R2 pp. 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 intelligences 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{X}_2 limitation the only 2-wheel break-ins are $i + j = .$ or $x.$

If there is any doubt about \bar{X}_2 limitation, break-ins can be done on both assumptions.

Break-ins with spanning can be used on a generous scale. [of 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 be possible to do a complete 3- wheel run in 10 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 [illegible], but run completely they are intolerably long [but see: 918]

A compromise is to do a 1+2 break-in followed by $4=5=/1=2$ at all $X_1 X_2$ settings which score more than 2σ , naturally taking the higher scores first. This has sometimes succeeded, but it is long and laborious.

So little evidence is obtained from the 2σ score that the full sigma - a four-wheel run is needed [23C(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 time; 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 $n_1\delta_1$, 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 X_1X_2 are set, and that it is desired to set X_3X_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:

$\underbrace{/T,9H,O3,MN}_{1.2.}$ $\underbrace{RG,CV,L4,IP}_{1.2x}$ $\underbrace{AW,UQ,5J,8K}_{1x2x}$ $\underbrace{DB,FX,ZE,YS}_{1x2.}$

Where 1.2.	a good run is	$\begin{array}{c} /T \quad 03 \\ 9H \quad MN \end{array}$	i.e. 3./1.2.
1.2x	a weak but useable run is	$\begin{array}{c} RG \quad IP \\ L4 \quad CV \end{array}$	i.e. 3+4x/1.2x

1x2x	a good run is	$\begin{array}{r} \text{UQ} \quad \text{5J} \\ \hline \text{AW} \quad \text{8K} \end{array}$	i.e. 3+4x/1x2x
	or if 8' are numerous	$\begin{array}{r} \text{UQ} \quad \text{5J} \quad \text{8K} \\ \hline \text{AW} \end{array}$	not 3.4./1x2x
1x2.	a good run is	$\begin{array}{r} \text{FX} \quad \text{YS} \\ \hline \text{DB} \quad \text{ZE} \end{array}$	i.e. 3x/1x2.
	a sometime usable run is	$\begin{array}{r} \text{FX} \quad \text{YS} \quad \text{ZE} \\ \hline \text{DB} \end{array}$	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 X_4X_5 , having set X_1X_2 the useful runs (not all independent) are

$\begin{array}{c} /9 \\ \hline \text{HT} & \text{CM} & \text{N3} \end{array}$	i.e.	4.5./1.2.
$\begin{array}{c} 58 \\ \hline \text{AU} & \text{QW} & \text{KJ} \end{array}$	i.e.	4x5x/1x2x
$\begin{array}{c} /9 \ 58 \\ \hline \text{HT} & \text{CM} & \text{N3} & \text{AU} & \text{QW} & \text{KJ} \end{array}$	i.e.	4=5=/1=2
$\begin{array}{c} 58 \ \text{AU} \\ \hline \text{QW} & \text{KJ} \end{array}$	i.e.	4+5/1x2x
$\begin{array}{c} /9 \ 58 \ \text{AU} \\ \hline \text{HT} & \text{CM} & \text{N3} & \text{QW} & \text{KJ} \end{array}$	i.e.	$\left\{ \begin{array}{l} 4+5/1x2x \\ \text{or } \{ 4.5./1.2. \end{array} \right.$

All these can easily be run using multiple testing.

To set X_3X_5 having set X_1X_2 the only new useful run is 3.5./1.2.

The reader may be interested to work out all possible runs supposing that X_3X_4 are set first [R3 pp. 95, 124; R5 p. 106]

(f) Runs for the last wheel.

These may be expressed compactly

For X_3	$\begin{array}{c} \text{U} \ / \ 5 \ \text{J} \ 3 \ \text{F} \ \text{X} \ 0 \ \text{G} \ \text{P} \ \text{Q} \ \text{Y} \ \text{S} \ \text{H} \ \text{I} \ \text{R} \\ \hline \text{A} \ 9 \ 8 \ \text{K} \ \text{N} \ \text{D} \ \text{B} \ \text{M} \ \text{V} \ \text{L} \ \text{W} \ \text{Z} \ \text{E} \ \text{T} \ 4 \ \text{C} \end{array}$
For X_5	$\begin{array}{c} \text{/} \ \text{U} \ 5 \ 8 \ \text{D} \ \text{F} \ \text{G} \ \text{Z} \ 9 \ \text{P} \ 3 \ \text{A} \ \text{Y} \ \text{M} \\ \hline \text{T} \ \text{Q} \ \text{J} \ \text{K} \ \text{B} \ \text{X} \ \text{R} \ \text{E} \ \text{H} \ \text{Y} \ \text{O} \ \text{W} \ \text{S} \ \text{N} \end{array}$

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 X_3 U/5; J3FIOG; PQYSH. [R4 pp. 42, 82.]

(g) ΔD Bigram Runs.

Because Colossus looks only at 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 ΔX wheels are used the Colossus plugging and switching required is

$$Z_1 + X_1 = x, \quad Z_2 + X_2 = x, \quad Z_3 + X_3 = ., \quad Z_4 + X_4 = x, \quad Z_5 + X_5 = x.$$
$$\Delta Z_1 + \Delta X_1 = ., \quad \Delta Z_2 + \Delta X_2 = ., \quad \Delta Z_3 + \Delta X_3 = x, \quad \Delta Z_4 + \Delta X_4 = x, \quad \Delta Z_5 + \Delta X_5 = x.$$

(h) Use of evidence other than ΔD .

If a message can be set on some but not all X's it may yet be possible to

- (i) set the motors [23L]
 - (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 $e^{\delta^2/2}$ [of 24X.]

It follows that the odds in favour of a settings with a sigma-age S , is about

$$\frac{e^{\frac{\delta_1^2}{2}}}{2\omega + \sum e^{\frac{\delta_i^2}{2}}}$$

where Σ 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.

$$\text{odds} = \frac{e^{\sum_{\text{run}} \frac{s_i^2}{N}}}{\text{of} + e^{\sum_{\text{competitors}} \frac{s_i^2}{N}}}$$

If there is no competition the decibanage is

$$\sum_{\text{runs}} 2.17 s_i^2 - 10 \log_{10} \text{of} - 3.$$

from which the "Certain, Good" tables [23C(b)] may be derived.

If there is competition, $\sum 2.17s_i^2$ can be found for each competitor and the results compared. [R3 p. 134; R4 p. 1, 70; R5 p. 1, 3, 7, 113.]

23X CHECKS ON SETTINGS

(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 $D = X + Z$.

Both X and Z are checked beforehand; D is checked afterwards. Each score used is checked as it occurs [See 23D].

(b) X Tests.

The X 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) X Test Tapes.

The obvious method of checking X triggers is to make a tape $Z = X$ at some definite settings, and count $/$'s in $Z + X = X + X = /$. The correct score is of course the text length, or span length. It is better to count $/$'s in $\Delta Z + \Delta X$ 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.

X test tapes are made to a standard length of 2002 and spanned 0001-2001.

(d) X Test Runs.

To avoid the need for putting on the special X test tape, counts are made depending only on the X trigger and the span, so that any sufficiently long tape which happens to be on Colossus can be used. The X test tape is required once only, as early as possible: if it checks, X 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 $\Delta X_1 + \Delta X_2 + \Delta X_3 + \Delta X_4 + \Delta X_5$.

spanning 0001-2002, starting with settings 01, 01, 01, 01, 01 and stepping X_1 , X_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
 - ΔD 32 letter count using Z-tape and X wheels.
 - ΔD 32 letter count using D-tape.
- (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 ($620 = 20 \times 31$) [For an early form of the test R4 p. 65].

(g) Theory of X Test Runs.

Suppose there is one erroneous character in ΔX_i (in fact, if there is one there must be two, because X_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 $\Delta X_i + U = .$ to be changed by the excess of dots over crosses in U at the $\frac{N}{\omega}$ places against the erroneous character of ΔX_i .

This excess has expected value 0 and standard deviation $\sqrt{\frac{N}{\omega}}$.

The change will be numerically less than 4 if

$$|\text{sigma} - \text{age}| \times \sqrt{\frac{N}{\omega}} < 4$$

If $\omega = 41$, $N = 2000$, then $|\text{sigma}-\text{age}| < .57$

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 $(0.43)^{10} = \frac{1}{7,000}$.

It is clearly wasteful not to include every ΔX_i in every reading taken.

In an archaic version $\Delta X_1 + \Delta X_i$ 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{X}_2 one would naturally 'look' at places on the tape where $\bar{X}_2 = x$, 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 frequencies.

(b) Expected sigma-ages.

Suppose that the limitation is \bar{X}_2 and that there are r_x , r./'s opposite $\bar{X}_2 = x$, in ΔD . Let the text length be N of which N_x , N., letters occur opposite $\bar{X}_2 = x$,. 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 $\bar{X}_2 = .$ as a mean of sampling what happens at motor crosses was first suggested in R0, 49. The expected number of /'s in ΔD at $\bar{X}_2 = x$ is

$$N_x \{Dp + (1 - D)q\}$$

and the expected no. of /'s opposite TM dots is $N_x Dp$

$$\text{Thus } r_x = N_x \left\{ Dp + (1 - D) \frac{r}{N} \right\}$$

$$\text{and } E.S. = N_x Dp = r_x - (1 - D)r \cdot \frac{N_x}{N}$$

where E.S. means expected score. If the motor is incorrectly set the expected score or average, a , is given by $a = Dr_x$

$$\text{and } \sigma = \sqrt{r_x D(1 - D) \left(1 - \frac{r_x}{N_x} \right)}$$

[see 21(n)]

$$\approx \sqrt{r_x D(1 - D)}$$

in most cases

Therefore expected bulge is $(1 - D) \left(r_x - r \cdot \frac{N_x}{N} \right)$

and this is fairly close to $(1 - D)(r_x - r)$

The expected sigma-age is $(r_x - r) \sqrt{\frac{1 - D}{Dr_x}}$

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 (= 37x61) different possible hypotheses about the possible motor settings. With $D = 3/4$ and the same value of r_x and r , 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_x and r , are smaller.

(c) Expected sigma-age with limitation not \bar{X}_2 .

When the limitation is not \bar{X}_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

$$r = N \frac{D}{2} p + N \left(1 - \frac{D}{2}\right) q$$

$$\begin{aligned} \text{and E.S.} &= N \frac{D}{2} p + N \frac{D}{2} q \\ &= r - (1 - D)N_q \end{aligned}$$

$$\begin{aligned} \text{Expected bulge} &= (1-D)(r-N_q) \\ &= (1-D)(r-N_v) \end{aligned}$$

where v is the number of letters of the alphabet being looked for. Expected sigma-age is

$$\left(r - \frac{N_v}{32} \right) \sqrt{\frac{1-D}{D_r \left(1 - \frac{r}{N} \right)}}$$

$$\approx \left(r - \frac{N_v}{32} \right) \sqrt{\frac{1-D}{D_r}}$$

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. 32, 37, and R5 p. 32 etc.).

This difficulty does not arise when the limitation is \bar{X}_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 X'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

$$BM = . | \Delta D \in \zeta$$

or $BM = . | \Delta D \in \zeta; \quad \bar{X}_2 \neq x$

where ζ 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 X 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 X 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 5σ 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 X'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 X's net.

Suppose $X_{1,2,3,4}$ are set but X_5 has given difficulty. Then we may sometimes be able to set the motor and to use the new information for setting X_5 . The expected score for a motor run with not all the X's set can be obtained in the same way as in the case when all five X'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 X_2 limitation) has been found by a semi-empirical method to be about $\left(1 - \frac{d}{60}\right)$ 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 X_2 limitation there is always the sample of $\bar{X}_2 = .$ and complicated formulae can be avoided.

(i) Motor run with only X_1 and X_2 set.

The last remark applies even in the extreme case in which the only wheels set are X_1 and X_2 , when the 4 letter counts against $\bar{X}_2 = x$ 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 behavior of ΔD_{12} at motor crosses can be calculated easily from the score of $/ 1+2$ at $\bar{X}_2 = x$ and the result obtained in this way is subject to a much smaller S.D. than the result obtained from the sample opposite $\bar{X}_2 = ..$ In theory a similar remark applies however many X'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

$$\sqrt{\frac{1-D}{D} \cdot \frac{1-D}{1-\frac{1}{2}D}}$$

The corresponding formula in the case of X_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 25 D(b)) 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 setting.

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 X's. Then a motor setting which is known to be at least a good slide of the correct motor may be used for setting or resetting the X'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 X 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) Providing μ_{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 $\bar{X}_2 + \bar{\Psi}_1'$. 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 X_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 TM run. A similar method can be used for Ψ_5 when the limitation is $\bar{X}_2 + \bar{\bar{P}}_5$ (R8, 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 the Ψ runs with an autoclave limitation.

In these runs for Ψ_1 or Ψ_5 as motor runs there is a tendency for the setting 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 X_2 limitation.

Once the T.M. 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 signs. If one of the psi 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 $P_{ij...k} = .$ or x throughout, since the switching is simple and no change in S.T. is required. For statistics of these runs see R5, p. 86. 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 R0, 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 setting 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 ($n = 2, 3\dots$) 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 [illegible]ight 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) Setting Ψ 's when not all the X's are set.

If all the X's are set but the motor is set, then this motor can be used for more powerful X runs, as already pointed out. However a more powerful method is to set the X's and Ψ 's simultaneously.

For example if $X_1, X_2, \mu_{61}, \mu_{37}$ are set the most powerful procedure is to set Ψ_1 and Ψ_2 and then say X_3 and Ψ_3 together (R4 p. 46).

(d) Testing the machine.

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 X's and motorised Ψ tapes are made available for each day's keys.

23N COALESCENCE

Suppose that the limitation in $\bar{X}_2 + \bar{\Psi}_1$. 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 X_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 $1.3 e^{-n/760}$

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 X_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 X_1 and X_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 $\bar{X}_2 \bar{P}_5$ limitation, this time Ψ_5 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 a 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 X-SETTING RUN

Suppose we have a message of length N and the score of $\Delta D_1 + \Delta D_2 = .$ is $\frac{1}{2}(N + X)$ for particular settings of X_1 and X_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

B_1 , the bulge of the second best score is B_2 and the bulges at all the other settings are (of course) less than B_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

$$25 / \sqrt{N} e^{2B_1^2/N}, \quad 25 / \sqrt{N} e^{2B_2^2/N}$$

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 B_2 . The probability that 1269 wrong settings will all have bulges less than B_2 is obviously a number fairly close to 1

(e.g. at least $\frac{3}{4}$), unless B_1 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

$$\approx \frac{\frac{1}{1271} \cdot \frac{25}{\sqrt{N}} e^{\frac{2B_1^2}{N}}}{\frac{1}{1271} \cdot \frac{25}{\sqrt{N}} e^{\frac{2B_1^2}{N}} + \frac{1269}{1271} \cdot q} \\ \approx \frac{e^{\frac{1}{2}s_1^2}}{e^{\frac{1}{2}s_1^2} + \frac{1269\sqrt{N}}{25} \cdot q}$$

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 B_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

$$10 \log_{10} e^{\frac{1}{2}s^2} = 2.17s^2 \quad \text{and} \quad 10 \log_{10} \left(e^{\frac{1}{2}s^2} + \frac{1269\sqrt{N}}{25} q \right)$$

This is how the 'X-setting scoring charts' were constructed. The tables required for all types of runs are 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 setting of X_2 , μ_{61}, μ_{37} for a particular message on $\bar{X}_2 + \bar{\Psi}_1$ 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 ($s = 2, 3, \dots$) 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 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", ch 8 pp. 154, 158).

"Players A and B agreed to play not more than n games, the probabilities of winning being p and q respectively. Assuming that the fortunes of the 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

$$\frac{q^a(p^b - q^b)}{p^{a+b} - q^{a+b}} - \frac{(2\sqrt{pq})^{a+1}(qp^{-1})^{\frac{1}{2}a}}{a+b} \cdot \sum_{r=1}^{a+b-1} \frac{\sin \frac{\pi r}{a+b}}{1 - 2\sqrt{pq} \cos \frac{\pi r}{a+b}} \sin \frac{\pi ar}{a+b} (\cos \frac{\pi r}{a+b})^a$$

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 $t = s/43$),

$$1 - t - \frac{1}{86} \sum_{r=1}^{85} \cot \frac{\pi r}{172} \sin \Pi \operatorname{tr}(\cos \frac{\pi r}{86})^{2m}$$

$$\approx 1 - t - \frac{2}{\pi} e^{-\frac{m}{172}} \sin \Pi t$$

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 also a proportion $1-t$ behind it is

$$1 - \frac{2}{\pi} e^{-\frac{m}{172}} (\sin \Pi t + \sin \Pi \overline{1-t}),$$

so the chance of not doing this is

$$\frac{4}{\pi} e^{-\frac{m}{172}} \sin \Pi t$$

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:

The chance that the right setting will not have collected a high proportion of the Ψ_1 wheel, after m BM dots is roughly $1.3e^{-m/750}$.

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 Ch. 44). That is to say the X runs were of the form $i+j/$.

The motor runs were all of the form $\text{motor} = .$ given $\Delta D = /.$ The $\Psi.$ runs were of the form $P_i + P_j = .$, 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 R0, 25 at the failure of a $1+3/$ run. (See also R0, 72).

When the X_2 limitation was introduced it was seen that this was no serious matter and the B.I.'s involving X_2 were done making use of the limitation by having \bar{X}_2 put in the third impulse of the $X_{1,2}$ tape.

After this it was realised that $/$'s in ΔD were a good thing to look for, so that X_4 and X_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 (R0, 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 (R0, 44, 45).

The idea of making simultaneous use of repeats and anti-repeats occurred first in connection with motor setting (R0, 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 R0, 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 R0, 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 X-setting (August, 1943).
- (ii) Decibanning machine (R0, 43)
- (iii) Square-summing method for using heterogeneity (R0, 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 (R0, 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 X_2 limitation (R0, 47-49).
- (ii) Tendency to use ΔP statistics for finding the best runs (e.g. R0, 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 runs statistics (Dec. 1943).

Other lesson learnt at the time of the 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 ΔX '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 Robins which could take four tapes. It then became possible to set all five X's without ever making a de-chi tape. For example, when setting X_3 given the setting of X's 1, 2, 4, 5, a message tape of length 3813 was used with a $\Delta X_{1,2}$ tape and a special $\Delta X_{4,5}$ tape of length 3813 (and therefore non-periodic). It was necessary to have four distinct types of $\Delta X_{4,5}$ 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 Robins 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 standard 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 X_2 when contracting a tape on Tunny.
Mysteriously long time taken for production of de-chi tapes and contractions.
- (11) 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-chi 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 involving X_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 X_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.

CKB 9904 WD 29/3 COL3 Page 2

SETTINGS on 29th wheels

k1 k2 k3 k4 k5
20 01 12 12 18

Motor run

///
r 183 a 159 ob 26 es165 e 5.8 at 156
kixk
2ml m2
20 05 b 0156
32 05 b 0156
37 04 0 0156
38 04 0 0156
39 04 0 0156
43 04 0 0160
44 04 0 0163
45 04 0 0162
46 04 0 0156
31 09 0 0160
32 09 0 0161
33 08 d 015
36 08 d 0157
37 08 d 0157
38 08 d 0157
39 08 d 0157
41 08 d 015

Fig. 23(I)
EXAMPLE OF MOTOR AND
PSI RUNS SHOWING
COALESCENCE.

The X'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 the settings 26, 31, 36 for Ψ_1 all score alike.

42 08 d 0163
43 08 d 016
44 08 d 0170
45 08 d 0167
46 08 d 0160
48 08 d 0156
49 08 d 0156
53 09 0 0158
54 09 0 0160
55 09 0 0161
56 08 d 0157
02 13 d 0156
03 13 d 0157
31 13 d 0161
42 16 a 0162
42 12 a 0162
43 16 a 0171
43 12 a 016
44 16 a 0172
44 12 0 016
45 16 0 0168
45 12 0 0165
53 13 d 0160
54 13 d 0161
55 13 d 0160
43 20 b 0162
44 20 b 0163
53 17 0 0160
54 17 0 0162
43 28 d 0162

set m1 44 m2 16
e1, run
e1
01 a 0097
06 a 0088
11 a 0086
16 a 0086
21 a 0101
26 a 0093
31 a 0093
36 a 0093
41 a 0093
01 a 0093

set m1 43 m2 16
e1
e1
01 a 0101
06 a 0102
11 a 0103
16 a 0101
21 a 0125
26 a 0137
31 a 0137
36 a 0137
41 a 0099

Fig. 23(I) (continued)

```

set s1 26 1 2 3x 4 5
r2281      a 11 40 4 24 at 1215
02 03 04 05
    01      a 1226
02          b 1250
    03      d 1232
12          b 1244
14          b 1279
    14      0 1263
    16      0 1268
19          b 1268
    19      0 1346  05
21          b 1257
    26      d 1251
28          b 1249
    28      d 122
29          0 1313
31          0 1456  03
33          b 1306
    33      0 1295
    41      d 1385  04
    44      0 1236
45          b 1292
    46      0 1308
47          b 1518  02

```

k1 k2 k3 k4 k5 s1 s2 s3 s4 s5 m1 m2
 20 01 12 12 18 26 47 31 41 19 43 16

//333444 10

psi m 10 back
 step //333444

a1 a2 a3 a4 a5
 30 04 35 45 25 a 0008
 31 05 36 46 24 a 0004
 35 09 40 50 28 a 0002
 36 10 41 51 29 a 0004
 37 11 42 52 30 a 0002

Ψ_1 is set provisionally at 26, (later found to be incorrect) but coalescence enables the other Ψ setting to be found easily using 2.3 x 4.5.., the weakest setting having an 8.6σ bulge.

The ' Ψ 's are set back and stepped together looking for the least number of /'s, 3's, 4's. Settings 35, 37 both yield 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 a1 a2 a3 a4 a5 m1
m2
20 01 12 12 18 35 09 40 50 28 43
16
//333444 0000 on 1st 200

INCOME from 02

qnoqmkqste9kmobom9

k1 k2 k3 k4 k5 a1 a2 a3 a4 a5 m1
m2
20 01 12 12 18 37 11 42 52 30 43
16
//333444 0000 on 1st 200

INCOME from 02

on 1st 200

9fuaahurote9knobex95ww9899kr9b

s1 s2 s3 s4 s5

31	03	36	46	24	a	0002
33	09	40	50	28	a	0000
36	10	41	51	29	a	0002
37	11	42	52	30	a	0000

k1 k2 k3 k4 k5 a1 a2 a3 a4 a5 m1 m2

20	01	12	12	18	35	09	40	50	28	43	16
----	----	----	----	----	----	----	----	----	----	----	----

24 - RECTANGLING

- 24A Introduction
 - 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, in 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 [25 A] 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 $\Delta X_1 + \Delta X_2$ which is $41 \times 31 = 1271$ long.

(b) The 1 + 2 rectangle.

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).

$$\Delta Z_1 + \Delta Z_2 + \Delta X_1 + \Delta X_2 = \Delta D_1 + \Delta D_2 \text{ which } \rightarrow.$$

Thus any place of Z would contribute favourably to the ΔD count if $\Delta X_1 + \Delta X_2$ 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 ΔX_1 and the j^{th} character of ΔX_2 : if there are u of these where $\Delta Z_1 + \Delta Z_2 = .$, and v where $\Delta Z_1 + \Delta Z_2 = x$ the net evidence that $\Delta X_1^i + \Delta X_2^j$ 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 \otimes , -x as x).

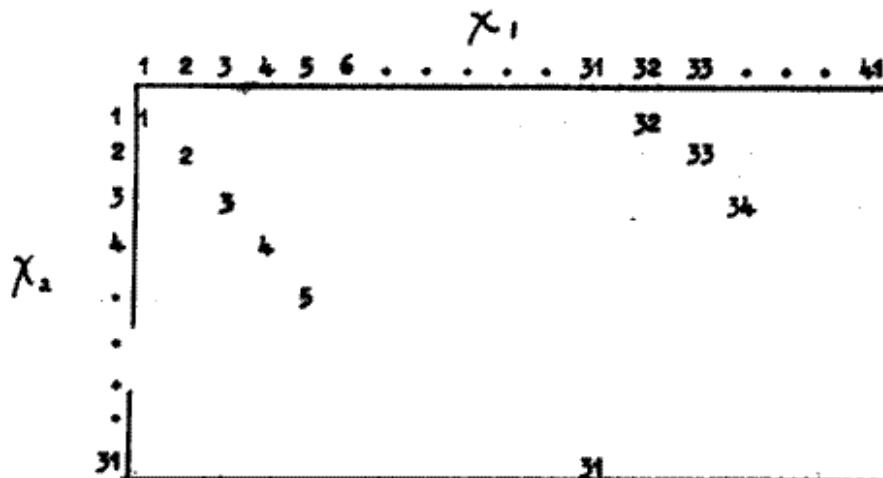
The substance of the foregoing is that the 41 columns of the rectangle correspond to the characters of ΔX_1 , the 31 rows to the characters of ΔX_2 . The entry in any cell (i,j) in the excess of contributory places where $\Delta Z_1 + \Delta Z_2 = .$ over places where $\Delta Z_1 + \Delta Z_2 = x$, and measures the evidence that $\Delta X_1 + \Delta X_2$ is a dot.

The rectangle so constructed is afterward converged, i.e. wheels ΔX_1 , ΔX_2 are found, to agree as well as possible with the evidence for $\Delta X_1 + \Delta X_2$.

24B MAKING AND ENTERING RECTANGLES

(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 $\Delta Z_1 + \Delta Z_2 = .$ 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 $(1271 + 1)^{\text{th}}$, $(2 \times 1271 + 1)^{\text{th}}$, etc. places, and similarly for every cell.

(b) The methods for entering have been used:

(i) Find the score for all places spaced at interval 1271 beginning with the 1st place of Z, 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 the row: this was found to make it not worth while except on Colossus, which can stop irregularly (38 C N): 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 abandoned (R5 p 81).

(c) Garbo rectangles.

By means of the special switches (56 E), Garbo is made to print $\Delta Z_1 + \Delta Z_2$, as, or x, in width 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 first, 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) Thurlow rectangles.

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)

Page 116a

FIG 24 (I)

Signdown

WVB

15-14

62/13/68/1

first nine rows

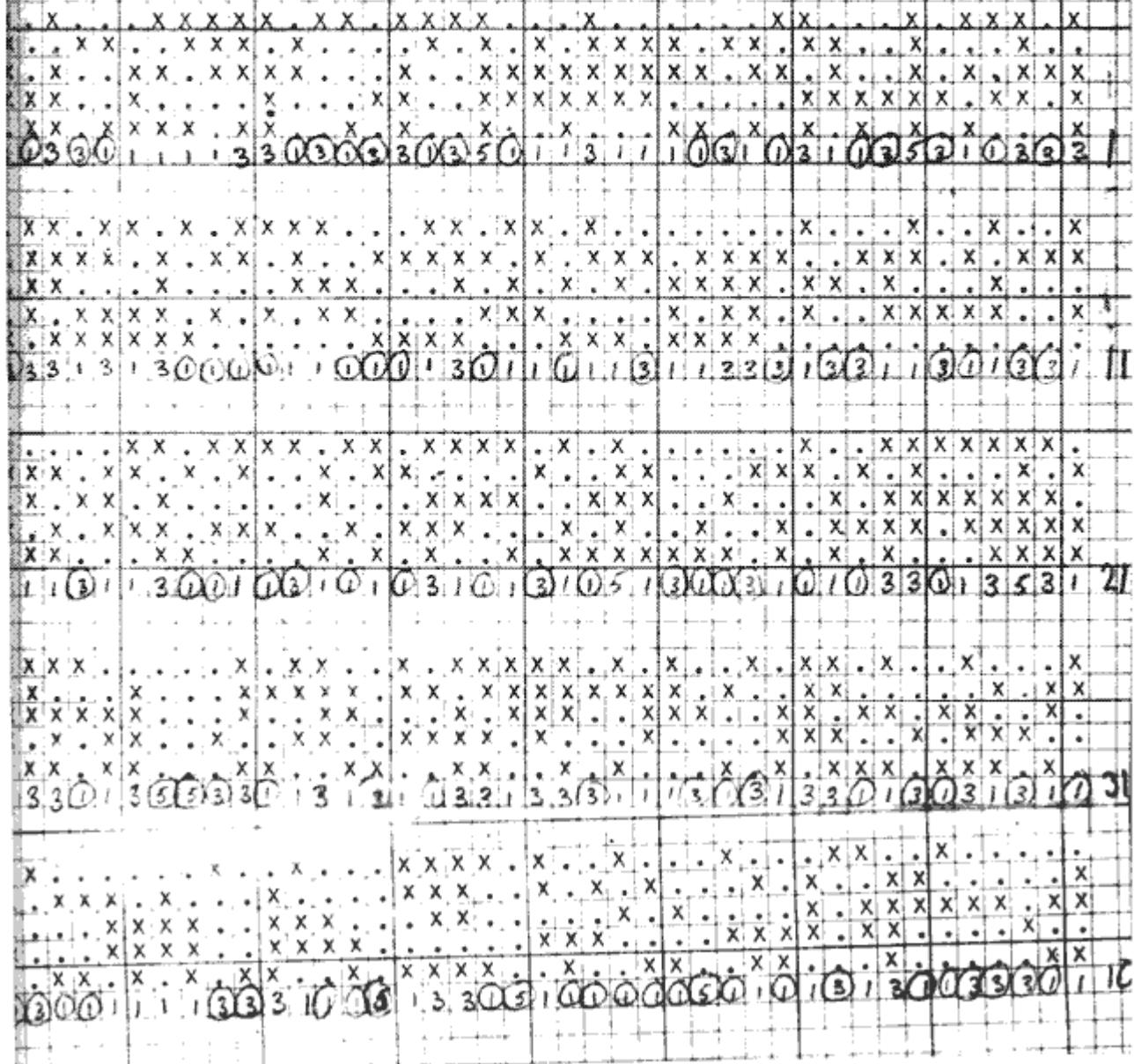
Gurbo Rectangle

TBX 12 S 314 (I)

Gurbo it's a □

Depth map from S

64 line by column



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	2	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 "E" in the first place of the tape.

Switch B = "E": this selects those places on A opposite the "E" 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 "E" 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 $\Delta Z_1 + \Delta Z_2 = .$ 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{X}_2 runs. The first "4" is one place back from the "E": this is merely a trick to make the position counter readings tally with those of a \hat{X}_2 run on Colossus.

For the details of plugging and switching see Synopsis of Robinson plugging (54J). It will be noticed that some unnecessary cords are used: this is to minimise changes between 1 + 2 rectangles, \hat{X}_2 , 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 $X_1 = x, X_2 = x$: 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 X_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 perform 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 = $2 \times (\text{score of } \Delta Z_{12} = .) - \text{depth}$: 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 instruction for a 1+2 rectangle are:

Spanning. Span 04 to $(04 + 1271 \times \text{depth})$
Count text.

Chi-patterns. (triggers) Crosses in 02, 02, of X_1, X_2 : on rectangling Colossi one trigger has this permanently set up.

Selection switches. $Q = X$

Q Panel. $X_2 = x$ 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 X_1

Check depth, i.e. $X_1 = x$, $X_2 = x$

Rectangle switch to "Normal".

Rectangling gadget Carriage return on X_1

Switch in appropriate depth.

Plug Panel $\Delta Z_1 + \Delta Z_2 = .$ in all counters.

Settings $X_1 = 06$, $X_2 = 02$

After setting wheels return plugs to 01, 01, without resetting.

Step X_1 (lower switch down) fast to control X_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 ΔX_1 , ΔX_2 which agree as well as possible with the entries in the cells of the rectangle.

The interpretation of 'agreeing as well as possible' is not obvious nor in 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 generalised 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 method 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 ΔX_1 and ΔX_2 do 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 ΔX_2 , take it through the rectangle to get ΔX_1 , take this through to get a new ΔX_2 and so on till $\Delta D_{12} = .$ 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) To take a wheel through the rectangle place the given wheel (say ΔX_1) against the first row of the rectangle and add all the entries therein, changing their signs wherever ΔX_1 is a cross (and counting 0 where ΔX_1 is 'doubted'). According to whether this sum is positive or negative, the first character of ΔX_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 $\Delta Z_{12} = .$ and if their signs are changed where $\Delta X_1 = x$ they become bulges of $\Delta Z_{12} + \Delta X_1 = ..$, i.e. of $\Delta D_{12} + \Delta X_2 = ..$ The sum of these for a particular row is the total $\Delta D_{12} + \Delta X_2$ bulge against the corresponding character of ΔX_2 (the 'score for this character'). By giving each character of ΔX_2 the same sign as this bulge, each is made to contribute positively to the bulge of $\Delta D_{12} = ..$ With the given ΔX_1 and this ΔX_2 the ΔD_{12} bulge for the whole rectangle is the sum of the moduli of the scores for ΔX_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 ΔX_1 and ΔX_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 ΔX_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 ΔX_2 being added in.

Note 2: Taking a wheel through is in fact a short wheel-breaking run (25A: R1 pp 92, 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 "E2" 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 ΔX_2 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 $\Delta X_2^{(i)} + \Delta X_2^{(j)}$ 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) 9 x 9 flag.

For each row find the sum of 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) Skeleton. (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 two 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 $\pm 6, \pm 4, \pm 2, 0$, which cannot effectively be simplified without taking ± 2 as 0, and this throws away too much evidence.

(e) E 2. (R2 p 82, R3 p 74, R4 pp 4, 20.)

Select the five best rows, as for 9 x 5 flag: A, B, C, D, E.

In A take all scores above the standard (see below) to form a rudimentary ΔX_1 wheel.

Take this through the rectangle, getting $\Delta X_2 A$, similarly $\Delta X_2 B$, $\Delta X_2 C$, $X_2 D$, $\Delta X_2 E$, each a column of scores, not merely dots and crosses.

Make a flag of these five ΔX_2 's by Jacob's method.

Choose 2, 3, 4 or 5 of these, and, with the appropriate \pm 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) Restarts.

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) E 1.

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 $\Delta X_2\alpha$ of 3 to 5 characters. Take $\Delta X_2\alpha$ through the rectangle getting $\Delta X_1\alpha$ of 6-10 characters. Take $\Delta X_1\alpha$ through the rectangle getting $\Delta X_2\beta$ of 8-12 characters, in choosing which, reduce the score of any character which was in $\Delta X_2\alpha$ by one-third. Take $\Delta X_2\beta$ through the rectangle getting $\Delta X_1\beta$ of 5-10 characters, excluding all characters which were in $\Delta X_1\beta$. (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 Δ_{1271} 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 the depth k (so that $N = 1271k$) the random value of $\sum_1^{1271} \theta_{ij}^2$ is N and its variance is

$$2N(k - 1) \quad (24X(d))$$

$\sum \theta_{ij}^2$ 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 $\sum \theta_{ij}^2 = \sum \theta^2 \cdot n(\theta)$: 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	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	.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

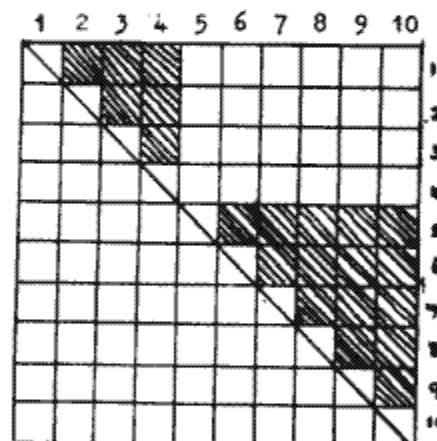
(R1 pp 32, 34, 38, R3 pp 37, 77.)

(c) $\Delta 1271$ Test.

Since $\Delta_{1271}\Delta Z_{12} = \Delta_{1271}(\Delta D_{12} + \Delta X_{12}) = \Delta_{1271}\Delta D_{12} \frac{1+\delta^2}{2}$ 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 $\sum \theta_i^2$ 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 m^{th} and n^{th} 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 σ , 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

$$2.17 \frac{x^2}{N} + \sum v \frac{(2y_i(x-k))}{N} - 219 > 0,$$

the left hand side being the decibanage in favour of significance, where y_i is the modulus of the score of a character and Σ is extended over both wheels, $\vartheta(u) = 10 \log_{10} (1 + e^{-u})$ 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 Σv is tedious to calculate and varies but little. Approximation have been suggested.

$$\sum \vartheta = \frac{2.4 \times 10^{10}}{x^4} \pm 3.6 \quad (\text{for messages 10168 long: R3 p 5}).$$

$$\sum \vartheta = 23 \text{ i.e. } \sum \vartheta = 23 \quad (\text{based on a perversattitude to decibans: R4 pp 111, 115})$$

$$\sum \vartheta = 2 + \frac{217,000}{N} - \frac{54,250,000}{N^2} \text{ i.e. } \frac{x}{\sqrt{N}} > w \left(1 - \frac{5000}{N} \right)$$

(Too optimistic for small N : used by the computers).

An empirical formula for Σv as a function of N in a marginally significant rectangle would have been preferable.

In practice everyone assumes that Σv is about 20-30, being greater for short messages and that if $2.17 x^2/N$, the LEADING TERM, is more than 200 or much less than 180 it is unnecessary to calculate the v 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 $\Delta Z_3 + \Delta Z_4 = .$, $\Delta D_1 = x$, $\Delta D_2 = x$).

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 $\Delta D_1 = x$, $\Delta D_2 = x$ varies from cell to cell (and in addition ΔX_1 , ΔX_2 may be 'doubted') the depth cannot be made constant, so that even if Colossus is used 3 + 4x / 1x2x and 3 + 4. / 1x2x 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.

Colossus switching. (c.f. 1+2 rectangle)

Count text, and check 1 + 2 = .

Chi-patterns (triggers) Cross in 02, 02 of X_3 , X_4 .

ΔX_1 , ΔX_2 in X_1 , X_2 triggers

Doubts in special patterns X_1 , X_2 triggers.

Plugging (everything plugged goes to all counters)

Special pattern $X_1 =$	}	It is improbable that there will be no doubting
•		
Special pattern $X_2 =$		

.

Check effective text

$\Delta Z_1 + X_1 = x$

$\Delta Z_2 + X_2 = x$

Check "R"

$\Delta Z_3 + \Delta Z_4 = x$.

Selection switches Q = X

Q Panel $X_3 = x$ in all counters

Multiple test impulses $R_1 R_2 R_3 R_4 R_5$ into counters 5, 4, 3, 2, 1, respectively

Control panel Multiple test switch to X_4

Rectangle switch to "Print Scores"

Rectangling gadget Carriage return on X_4

Do not switch a depth

Settings $X_1 = 41$, $X_2 = 31$, $X_3 = 02$, $X_4 = 02$

After setting wheels replace X_3 , X_4 plugs in 01, 01, without

resetting

Step X₄ fast (lower switch down) to control X₃ (lower switch up)

Printer Triple line feed

Final checks Repeat first and last rows

Re-run with $\Delta Z_3 + \Delta Z_4 = .$ 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 $i + j /(\text{known } \Delta D) = x$, with or without fixed conditions.

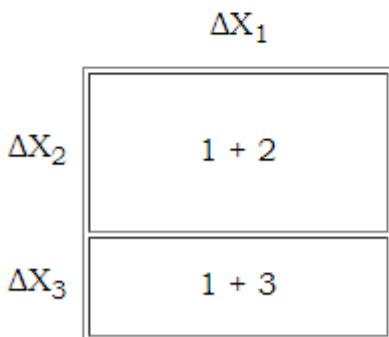
Among the plain $i + j$ rectangles $4+5$, $2+5$, $1+3$, $3+4x$, $2+4$ have all been tried: indeed at one time it was erroneously supposed that $4+5$ would be better than $1+2$ (see 24Y(a)).

A peculiar class of $i + j$ rectangle is that of $i + 6$ rectangles in which entry is the score for $\Delta Z_i + \Delta Z_6 = .$ i.e. $\Delta Z_i = .$, entered in a $31 \times w_i$ rectangle. In particular if $i = 2$ all entries lie on the principal diagonal and the rectangle degenerates into \hat{X}_2 .

A rectangle which makes full use of the run $4 = 5./1 = 2$ requires 4 entries (3 independent) in each cell (c.f. 25C(e) R1 p 62)

Several members of the section have contemplated "Rectangular parallelepipeds": probably the most favourable is $i + j + 6 / , \Delta Z_6$ being always dot.

Rectangles may be combined, thus



but in practice this is done only for key (26C), 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 $\Delta X_{12} = \text{dot}$ 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 $\Delta X_{12} = \text{dot}$ 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 ΔX_1 and ΔX_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, $\varepsilon_1, \varepsilon_2, \dots$ 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

$$y_i = \sum_i \theta_{ij} \varepsilon_i$$

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 $\varepsilon_j = \text{sign } y_j$,

- i.e. $\varepsilon_j = +1$ if $y_j > 0$
 $\varepsilon_j = -1$ if $y_j < 0$
 $\varepsilon_j = 0$ if $y_j = 0$

and take this wheel pattern back through the rectangles giving pippages

$$x_i = \sum_j \theta_{ij} \varepsilon_j$$

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 $X, X = \sum |x_i|$. This score is independent of which of the two wheels is used, when the convergence is completed, for

$$x = \sum_i \varepsilon_i x_i = \sum_{ij} \varepsilon_i \theta_{ij} \varepsilon_j$$

and this is symmetrical with respect to the two wheels. If the message were deciphered 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).

$$\text{The formula } X = \sum_{ij} \varepsilon_i \theta_{ij} \varepsilon_j$$

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 $\varepsilon_1, \varepsilon_2, \dots$ so as to maximise $\sum \varepsilon_i \theta_{ij} \varepsilon_j$ (leaving $\varepsilon_1, \varepsilon_2, \dots$ 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

$$y^i = \sum_i f(\theta_{ij}, x_i)$$

$$x_i = \sum_i f(\theta_{ij}, y^i)$$

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 $\zeta = \frac{1+\delta}{1-\delta}$

and (see R1 pp 37, 43, 45, 49) a conventional value of δ 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 $\zeta \rightarrow \infty$, 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

$$\Theta_1, \Theta_2.$$

$$\Theta'_1, \Theta'_2.$$

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 $f_0(\theta_i, \theta'_i)$ 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 ζ^Θ , $\zeta^{\Theta'}$, what are the odds ζ^Π that the two

characters are the same? The proportional bulge corresponding to odds

$$\zeta^0 \text{ is } \frac{\zeta^\theta - 1}{\zeta^\theta + 1}$$

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) Wrong convergences of a rectangle and methods of starting.

A rigorous solution of the problem of the number of different crude convergences of a (1+2) rectangles seem 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 intelligence 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 become 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 $2n \times 1271$ ($n = 2, 3, 4$) and since so many of the rectangles were of length 8×1271 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 pp 18, 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 are 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 ΔX_2 . 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

$(\log \cosh \frac{1}{2}(x+y)p - \log \cosh \frac{1}{2}(x-y)p)$ natural bans where $p = \log \frac{1+\delta}{1-\delta}$ (i.e. approximately 26).

and this is sufficiently close to

$$\begin{aligned} & \log \cosh (x+y)\delta - \log \cosh (x-y)\delta \\ &= \frac{\delta^2}{2} \left[(x+y)^2 - (x-y)^2 \right] - \frac{\delta^4}{12} \left[(x+y)^4 - (x-y)^4 \right] + \frac{\delta^6}{45} \left[(x+y)^6 - (x-y)^6 \right] \dots \\ &= 2\delta^2 xy - \frac{2}{3} xy(x^2 + y^2)\delta^4 + \dots \end{aligned}$$

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 $\delta = 1/10$, 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 'pipette') is taken as $2\delta^2$ natural bans, i.e. 1 pipette = 6 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

$$\text{sign}(xy) \min(|x|, |y|).$$

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 pp 63, 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 the 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_{ij} 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 X's has good Δ^2 properties, i.e. $\Delta^2 X_i$ nearly all crosses. (See also 25E(a) for \hat{X}_2 runs and chapter 25F for one wheel break-ins if $ab \neq \frac{1}{2}$.)

(c) Tests for converged rectangles (historical).

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 span 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 X_1 and X_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 ΔX_1 and ΔX_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 v 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 v terms.) Further it was assumed somewhat arbitrarily that Σv was inversely proportional* to N . The significance test can be written

* Perhaps inversely proportional to \sqrt{N} would have been a better assumption

$$\frac{2.17x^2}{N} > 219 - \frac{300,000}{N}$$

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 v terms. Unfortunately it was not based on a careful study of the statistics about v terms available by that time. The sum of the v terms for $N = 8 \times 1271$ 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

$$\frac{24,000,000,000}{x^3} \pm 3.6 \text{ decibans.}$$

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 text.

By a 'significant 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 θ_{ij} . Then the function required in $s_2 = \sum_j \theta_{ij}^2$. There is a gadget on Colossus which counts the number of occurrences of each values 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

$\Delta_{1271v}(\Delta Z_{12}) = .$ for $v = 1, 2, \dots, k-1$, 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 $v = 1, 2, \dots, (k-1)$ 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 N . The total number of such distinct pairs of letters is $1271 \times \frac{k(k-1)}{2}$ so that

$\frac{1}{2}x - \frac{1}{2}\left\{1271\frac{k(k-1)}{2}\right\}$ is defined as the bulge B of the test. It is reasonable 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

$$x = \sum (r(r-1) + s(s-1))$$

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 $r + s = k$, $r - s = \theta_{ij}$,

$$s_2 = \sum \theta_{ij}^2, \quad B = \frac{1}{2}x - \frac{1}{2}\left(1271\frac{k(k-1)}{2}\right)$$

it follows that

$$B = \frac{1}{4}(s_2 - N).$$

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 X^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 $N_c = 1271 \frac{k(k-1)}{2}$ 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 1878^2 . If $\delta = .1$, which is sufficient for the significance of the converged rectangle, the expected sigma-age would be 1.9. If δ

= .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 .

$$\text{Then } s_1 = \delta^2 \sqrt{1271 \frac{k(k-1)}{2}}$$

and the factor in favour of a particular value of δ rather than $\delta = 0$ is, if we assume σ independent of δ ,

$$e^{-\frac{1}{2}(s_1-s)^2} e^{-\frac{1}{2}\delta^2}$$

$$= e^{ss_1 - \frac{1}{2}s^2}$$

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 $2B\delta^2 - \frac{N(k-1)}{4}\delta^4$

$$= \frac{1}{2}(s_2 - N)\delta^2 - \frac{(k-1)N}{4}\delta^4$$

$$= \lambda\delta^2 - \mu\delta^4 \text{ say.}$$

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 if $\delta < 0$), is

$$\frac{\int_{\delta_0}^{\infty} e^{\lambda\delta^2 - \mu\delta^4} d\delta}{\int_{-\infty}^{\delta_0} e^{\lambda\delta^2 - \mu\delta^4} d\delta}$$

If $s_2 = N$, $k = 3$, $\delta = .08$ this reduces to

$$\frac{\int_{.08}^{\infty} e^{-17,800\delta^4} d\delta}{\int_0^{.08} e^{-17,800\delta^4} d\delta}$$

$$= .15.$$

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 0', 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

$$\left(\frac{k^k}{2} + \frac{\theta}{2}\right) \times \frac{1}{2^k} \left\{ (1+\delta)^{\frac{k+\theta}{2}} (1-\delta)^{\frac{k-\theta}{2}} + (1+\delta)^{\frac{k-\theta}{2}} (1-\delta)^{\frac{k+\theta}{2}} \right\}$$

and therefore the factor in favour of this value of δ rather than $\delta = \theta$ is

$$(1-\delta^2)^{\frac{\theta}{2}} \times \frac{1}{2} \left\{ \left(\frac{1+\delta}{1-\delta}\right)^{\frac{\theta}{2}} + \left(\frac{1+\delta}{1-\delta}\right)^{-\frac{\theta}{2}} \right\}$$

$$= \operatorname{sech}^{k\delta'} \cosh (\theta\delta'),$$

$$\text{where } \delta' = \frac{1}{2} \log \frac{1+\delta}{1-\delta} = \delta + \frac{1}{3}\delta^2 + \dots,$$

and is very close to δ in all practical cases. The natural banage from all the cells together is thus

$$\begin{aligned} & \sum_{ij} \log \cosh(\delta' \theta_{ij}) - N \log \cosh \delta' \\ &= \frac{\delta^{12}}{2} (s_2 - N) - \frac{\delta^{14}}{12} (s_4 - N) + \frac{\delta^{16}}{45} (s_6 - N) \dots \end{aligned}$$

$$\text{where } s_n = \sum \theta_{ij}^n,$$

Now $E(s_2) = N$, $E(s_4) = 3kn$, $E(s_6) = 15k^2n$, ... if $\delta = 0$ and $N = 1271k$ so, if $\delta^2 N < 200$, a sufficiently good approximation is

$$\frac{\delta^2}{2} (s_2 - N) - \frac{\delta^4 (s_2 - N)}{12}$$

Observe that we cannot neglect the term in δ^4 since $E(s_2 - N) = Nk\delta^2$, so the expected value of the second term is about half of that of the first term if δ is small. If we write $s_4 = 3kN$ 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 s_4 should be taken into account. The 'maximum likelihood' value of δ is

$$\sqrt{\frac{3(s_2 - N)}{s_4 - N}}$$

though this is itself liable to a large S.D. which can be estimated. Larger values of s_4 given smaller values of δ so the previous formula lays too much stress on the

higher entries in the rectangle.

(e) Significance tests for rectangles which have been crudely converged.

Let the double bulge on /1+2 on a message of length N, against the correct wheels be x^2 . (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 ΔX_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 R3 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 relatively 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 $2.17xx^*/N$.

II. This expression is very sensitive to the exact estimate of x^* . 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(o) '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

$$\therefore \frac{1}{2^k} \left(\frac{d^k}{2} + \frac{\theta}{2} \right) (1+\delta)^{\frac{k+\theta}{2}} (1-\delta)^{\frac{k-\theta}{2}}$$

if ΔX_{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

$$\begin{aligned} f &= \int_{-1}^1 \varphi(\delta) \left(\frac{1+\delta}{1-\delta} \right)^{\frac{x}{2}} (1-\delta^2)^{\frac{N}{2}} d\delta \\ &= \int_{-\frac{x}{N}}^{\frac{1-x}{N}} \varphi\left(\frac{x}{N} + \varepsilon\right) \exp\left[\lambda - \frac{N}{1-(\frac{x}{N})^2} \cdot \frac{\varepsilon^2}{2} + \dots\right] d\varepsilon \end{aligned}$$

$$\text{where } \lambda = \log \left[\left(\frac{1+\delta}{1-\delta} \right)^{\frac{x}{2}} (1-\delta^2)^{\frac{N}{2}} \right] \Big|_{\delta=\frac{x}{N}}$$

$$= \frac{x^2}{2N} + \frac{x^4}{12N^3} + \dots$$

$$\text{Therefore } f = e^{\frac{x^2}{2N} + \frac{x^4}{12N^3} + \dots} \cdot \sqrt{\frac{2\pi}{N}} \varphi\left(\frac{x}{N}\right)$$

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 .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 $\phi(x/N) = 10$ 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 too different from the old ones. Therefore the factor above is approximately equal to

$$\begin{aligned} & \frac{1}{3} \sum_y \exp \frac{(x-2y)^2}{2N} \\ &= \frac{1}{3} e^{\frac{x^2}{2N}} \sum_y \exp \left\{ -\frac{2y}{N} (x-y) \right\} \end{aligned}$$

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, \dots 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

$$\begin{aligned} & \frac{1}{3} e^{\frac{x^2}{2N}} \sum_{i,j,\dots} \exp\left\{-\frac{2(y_i + y_j + \dots)}{N}(x-K)\right\} \\ & \frac{1}{3} e^{\frac{x^2}{2N}} \prod_i \left\{1 + e^{-\frac{2(x-K)y_i}{N}}\right\} \end{aligned}$$

Expressed in decibans, this gives, allowing for the prior odds

$$\frac{2.17x^2}{N} + \sum v\left(\frac{2(x-K)y_i}{N}\right) - 219$$

where

$$\zeta(a) = 10 \log_{10}(1+e^{-a}).$$

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 ΔX_1 on the rectangle be a_1, a_2, \dots, a_4 , 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 experiences, $K = 1.3\sqrt{N}$ 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 z is 2×2^{-71} instead of 2^{-71} .

When a rectangle has a positive decibangage 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

*	*	*	*
*	5	4	30
x	5	x	1
x	4	5	7
*	0	0	0

the flag shown in the diagram. The pattern inevitably oscillates between and .xx. or else between xxxx and x..x. 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 till denoted by X, and the sigma-age of a convergence is $X/(2\sigma)$ where $\sigma^2 = \text{sum of square of entries in triangular flag}$. 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 $\Psi\left(\frac{x}{2\sigma}\right)$ 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 v 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 81, 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 satisfy the inequality

$$\frac{2.17x^2}{N} + 30 > 219$$

assuming the u terms do not amount to more than 30 decibans.

$$\text{i.e. } x > 9.4\sqrt{N}$$

i.e. since the score on correct wheels is approximately $x - \sqrt{N}$

$$\delta N + \sqrt{N} > 9.4\sqrt{N}$$

$$\text{or } \sqrt{N} > 7\frac{1}{12} \text{ or } N > \frac{71}{\beta^2 \Pi_{12}^2}$$

Observe how sensitive the minimum value of N is to the value of d . The conclusion that the minimum text length required was proportional to $(\beta^2 \pi^2)^{-1}$ was reached by an entirely different method in R1 pp 51, 53. Width $d = 21$ and $\pi = .2$ the minimum N is about 11,000; with $d = 28$, $\pi = .2$ the minimum is about 3000.

For a 4+5 rectangle the condition would be roughly

$$\frac{2.17x^2}{N} + 20 > 149$$

$$\therefore \delta N + \frac{1}{2}\sqrt{N} > 7.8N \quad (\text{x: } \delta N + \frac{1}{2}\sqrt{N} : \text{ see R3 p 117})$$

$$\text{i.e. } N > \frac{53}{\beta^2 \Pi_{45}^2}$$

Incidentally this shows that a 4+5 rectangle would probably be just significant on a shorter text than a 1+2 rectangle if

$$\left(\frac{\Pi_{45}}{\Pi_{12}}\right)^2 > \frac{53}{71} \quad \text{i.e. } \Pi_{45} > .86\Pi_{12}$$

This condition was seldom likely to be satisfied and 4+5 rectangles were seldom made. The condition for a 4+5 rectangle to be more decibans up than

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 X_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{X}_2 and \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) Rectangles with X_2 limitation.

As early as R1 p 59 it was thought that the X_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 X_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 X_2 .

Methods for diagnosing X_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 X_2 is assumed, because it will tend to be wrong at \bar{X}_2 dots rather than crosses.

(c) Wheel-sliding.

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 X_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 Δwheels were relatively inside out.) The rival good positions can then be scored by a more accurate method. Before we had time to work out the correct wheel-sliding table a cruder method was used. This cruder method is to evaluate

$$\sum_i \frac{1}{2} \{1 \pm \text{sign} a_i \text{sign} a'_i\} \min(|a_i|, |a'_i|)$$

where the lower sign is taken if the patterns a_1, a_2, \dots and a'_1, a'_2, \dots 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 $xy = 10^{x/10}$ and probability $p = \theta/(1+\theta)$. Let $p = \frac{1}{2}(1+\Pi)$.

Let the probability of having an x in a cell of the first wheel be p_x if the character is a cross. Then the probability of having an x if the character is a dot is θp_x . Denote by x' , θ' , $p'_{x'}$ 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

$$\frac{1}{2}(p_x p_{x'} + \theta p_x \theta' p'_{x'})$$

and if it is wrong

$$\frac{1}{2} p_x(1+\theta) \frac{1}{2} p'_{x'}(1+\theta')$$

Therefore the factor obtained from one pair of entries in favour of the slide being correct is

$$2 \cdot \frac{1+\theta\theta'}{(1+\theta)(1+\theta')} = \frac{1}{2}(1+\Pi\Pi')$$

The factor obtained from the complete comparison is

$$\Pi \frac{1}{2}(1+\Pi\Pi')$$

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) Setting two messages in depth on Chi 1 and Chi 2.

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 length of the messages are 1271k and 1271k' with P.B. of $\Delta D_{12} = \text{dot of } \delta \text{ and } \delta'$, then the proportionate 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 $66\sqrt{1271kk'}$. In order that this should exceed 3 it is necessary that either $6\sqrt{1271k}$ or $6\sqrt{1271k'}$ should exceed 10. Thus it is impossible for two rectangles to be set by Significance Test 0 (i.e. when unconvolved), unless at least one of them would be significant according to Significance Test IV (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{X}_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{X}_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 X_1, X_2, X_3, X_4 , are known: then $\Delta D_1 (= \Delta Z_1 + \Delta X_1), \Delta D_2, \Delta D_3, \Delta D_4$ can be found.

$\Delta D_1, \Delta D_2, \Delta D_3, \Delta D_4, \Delta Z_5$ (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 ΔX_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 ΔX_5 is a dot the contribution to ΔD is 6/'s and 10T's; but if the first character of ΔX_5 is a cross the contribution to ΔD is 10/'s and 6T's therefore the character is more likely to be cross than a dot.

Each character of ΔX_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 X's shall be known e.g. if only X_1 , X_2 are known, ΔX_4 may be found using the ΔD characteristic: $4 = 1 = 2$ is commoner than $4 \neq 1 = 2$.

Nor does it require of a ΔX_i , regarded as known, and used to find ΔD_i , that all its characters shall be known; places on Z against unknown ('doubted') ΔX 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 ΔX 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{X}_2 limitation phenomenon
- (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) Adaptation to Colossus counting.

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.

$$\begin{aligned}
 ij &= \text{pippage of evidence that } \Delta X_5^i, \text{ the } i^{\text{th}} \text{ character of } \Delta X_5 \text{ is a dot} \\
 &= /'s \text{ against } \Delta X_5^i - T's \text{ against } \Delta X_5^i \\
 &= /'s \text{ against } \Delta X_5^i + T's \text{ against other characters} \\
 &\quad - T's \text{ against other characters} \\
 &\quad - T's \text{ against } \Delta X_5^i \\
 &= (/'s \text{ against all characters, if } \Delta X_5^i \text{ is a dot, all other characters crosses}) \\
 &\quad - (/'s \text{ against all characters, if all are crosses}) \quad A1 \\
 &= (T's \text{ against all characters, if } \Delta X_5^i \text{ is a cross, all other characters dots}) \\
 &\quad - (T's \text{ against all characters, if all are dots}) \quad A2
 \end{aligned}$$

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.

This is said "Wheelbreaking runs are always run inside out on the impulse being run for".

A simple check can be applied

$$\begin{aligned} \sum_i x_i &= \sum_i /'s \text{ against } \Delta X_5^i - \sum_i T's \text{ against } \\ \Delta X_5^i & \\ &= \text{all } /'s - \text{all T's} \\ &= (\text{all } /'s + \text{all T's}) - 2(\text{all T's}) \\ &= R - 2 \text{ norm} \end{aligned} \quad \left. \right\} \begin{array}{l} \Delta X_5 \\ \text{supposed} \\ \text{all dots} \end{array}$$

R is easily measured, being independent of ΔX_5 . The check tests not only the Colossus readings, but, also the subtractions of the norm to find the x_i .

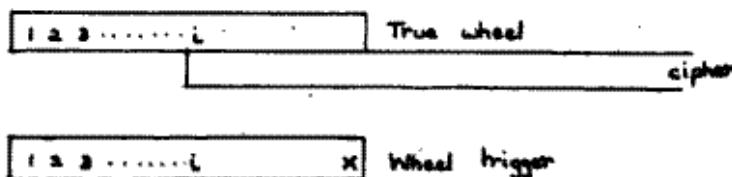
Counting T's in ΔD with each character of ΔX_5 taken in turn to be a cross, all the others being dots, could be done, and in fact originally was done, by actually placing a cross in each position of the trigger in turn; but it is much easier to insert a cross in a fixed position (in practice the last) and allow the wheel to step.

The characters of the wheel are produced in reverse order: (c) shows in detail why this happens.

(c) Why the wheel is obtained backwards.

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.

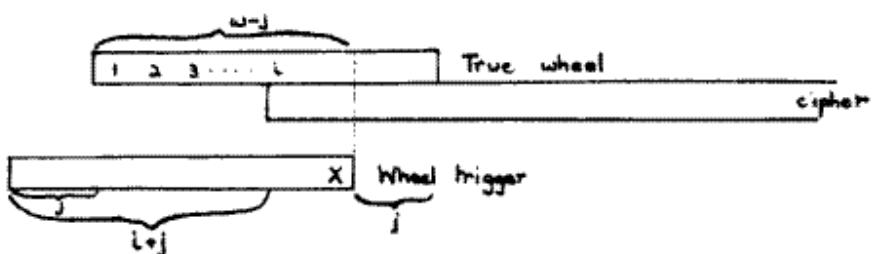
Suppose that the setting of the true wheel relative to the cipher is 1.⁺ Consider firstly that particular position of the trigger in which its setting is also 1 (so that display and printer read 1): true wheel and trigger now begin in the same place, thus:



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.

+ 1 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 X_1 , X_2 this refers to true settings; for X_3 , X_4 , X_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 $W - j^{\text{th}}$ 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) Practical Procedure on Colossus.

Count R the number of places looked at: i.e. /'s and T's

Count Norm: i.e. /'s assuming that ΔX_5 is all crosses, measured on Colossus, as T's with ΔX_5 all dots.

Both R and norm are unaffected by stepping X_5 , and as a check are each measured at least twice, whilst X_5 steps.

Reset to the correct message setting: insert a cross in the last position of the X_5 trigger, step X_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) Significance test.

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

$$\frac{x}{\sqrt{R}} > 0.8\sqrt{w} + 1.2$$

where R is the number of places looked at

w is the wheel length

x is 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 ΔX_2 knowing ΔX_1 , ΔX_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 3./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 combined run.

(b) Fundamental decibanning formula.

The formula for calculating the evidence of a significant short wheel-breaking 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 the 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 the run on its own wheel, is generally greater than on the correct wheel, of 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

$$q = \frac{\text{expected score on the correct wheel}}{\text{score on the run's own wheel}}$$

$$\text{so that decibans per pip} = \frac{R + qx}{R - qx}$$

The table, whose construction is explained in 25X (e), is

$\frac{x}{\sqrt{R}}$.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) IV)

(d) Decibanning a run on the wheel from another run.

Suppose, now, that a wheel has been obtained from a single run, say ΔX_3 from /'s and that additional evidence is desired, say from 5's. The crude decibanning formula can be used where x is 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 likely 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 be 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 ΔX . 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.) ΔX_2 were very uncertain, B's (against D's) for ΔX_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 X_2 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 ΔX_1 , ΔX_2 wheels. Runs for ΔX_3 , ΔX_4 , ΔX_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 ΔX_5 , using which $4 = /1 = 2 = 5$ is significant for ΔX_4 . A 16 letter count indicates the most suitable runs for improving ΔX_1 , ΔX_2 , ΔX_3 , ΔX_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 ΔX_3 . A 32 letter count indicates suitable runs for strengthening ΔX_3 , and another count indicates runs for improving ΔX_1 , ΔX_2 , ΔX_5 , ΔX_4 , ΔX_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, $\Delta X_1 A$, $\Delta X_1 B$, $\Delta X_1 C$ e.g. on the chi 4 sheet. BB--A means that $\Delta X_1 B$, $\Delta X_2 B$, $\Delta X_3 A$, were used, ΔX_2 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).

R x x/\sqrt{R} q	$\left. \right\}$ 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) Choosing wheel-breaking runs.

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 wheel is $\frac{x}{\sqrt{R}}$.

Significance depends on $\frac{x/\sqrt{R}}{0.8\sqrt{w+1.2}}$

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 decibannages 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 ΔX_1 , ΔX_2 : even if it starts from \hat{X}_2 , the second wheel obtained is usually ΔX_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 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 X_4 or X_5 is obtained first, the next run is $4=5=1=2$ or $4+5.1x2x$.

If X_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 ΔX_1 and ΔX_2 have been obtained and that although there is no significant run for ΔX_3 , a few characters can be guessed. With this rudimentary ΔX_3 a short wheel-breaking run e.g. 5JUQ may produce a ΔX_4 wherewith

a run, say 5JUQ03 produces a new ΔX_3 , whence a new ΔX_4 and so on.

Because the characters of both ΔX_3 , and ΔX_4 are arbitrary the significance value of $\frac{x}{\sqrt{R}}$ 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, for, 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 the 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 scoring 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.

$$(\cdot \cdot) - (x \cdot), (\cdot x), (\cdot \cdot) - (\cdot x), (x \cdot) - (x x)$$

where, e.g. $(\cdot x)$ means $\begin{cases} \Delta Z_4 = \\ \Delta Z_5 \neq \end{cases} \quad \left. \right\} \quad \Delta D_1 = \Delta D_2$.

(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 ('running on doubted wheels'). This is effected on Colossus by means of the special pattern trigger of the wheel-breaking in the special patterns 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 ΔX_5 , and 4=/1=2 against the doubted characters of ΔX_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, 25.)

Doubting reduces the effective text: for example if one third of each of the four wheels is doubted, the remaining text is $\left(\frac{2}{3}\right)^4$, 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 X_3 is being set by means of 3x/1x2., X_1 , X_2 are fixed in the cipher, whilst X_3 is tried in all possible 29 positions. Of the places where 1x2., the only ones looked at are those where ΔX_3 is known and this may vary considerably when X_3 steps. Thus a large 3x1x2. may be due to a large 1x2., which is not relevant to setting ΔX_3 .

This is commonly circumvented by printing R, i.e. (1x2.) and the score, (3x1x2.), for all positions of X_3 , afterwards finding the sigma-age $\frac{x - \bar{R}/2}{\frac{1}{2}\sqrt{R}}$ for promising scores.

A preferred modification which reduces unless 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 settings; 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{X}_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) Spanning for message slides.

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 not be 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

<u>04</u>	<u>05</u>	<u>06</u>	<u>07</u>	<u>08</u>	<u>09</u>	<u>10</u>	setting before slide 04
<u>06</u>	<u>07</u>	<u>08</u>	<u>09</u>	<u>10</u>	<u>11</u>	<u>12</u>	setting after slide 06
slide here							

07, 08 are missing, wherefore two holes must be inserted.

(d) Spanning for changes in ΔP characteristics.

The character of P and hence of ΔP may change considerably during the same 'message' (meaning transmission or QKP), 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) Wheel characteristics.

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 d	20 or 21	15 or 16	14 or 16	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 tricks have been devised for doing this easily.

$4x5 \cdot x \cdot x \cdot x \cdot \dots x \cdot \dots x \cdot x \cdot x x \cdot x x \cdot \dots x x x \cdot x \cdot$	<i>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 12 dots.</i>
$x \cdot \dots x x \cdot \dots x x x \cdot \dots x x \cdot x \cdot x x x \cdot x \cdot$	<i>12 crosses</i>

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 may 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 ΔP 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 immediately before each antopause 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{X}_2 LIMITATION

(a) Running against \bar{X}_2 crosses.

Because the bulges of runs against $\bar{X}_2 = X$ are so much greater than against $\bar{X}_2 = .$, these are made separately (as in setting), and indeed it is rarely worth while to do runs against $\bar{X}_2 = .$, and then only for good motor cross letters (R3 p 101).

(b) Runs for ΔX_2 and \bar{X}_2

In a run for ΔX_2 however, the scores for all characters of ΔX_2 will appear, those where $\bar{X}_2 = x$ scoring strongly, those where $\bar{X}_2 = .$ weakly, so that the run provides two types of evidence:

- (i) high and low scores indicate $\bar{X}_2 = x$ and $.$,
- (ii) positive and negative scores indicate $\Delta X_2 = .$ and x , moreover the \bar{X}_2 , and ΔX_2 obtained by differencing, must be consistent.

Scores against $\bar{X}_2 = x$ and $\bar{X}_2 = .$ must be decibanned separately, the result of which is usually that scores against $\bar{X}_2 = .$ are found to be negligible. Until a complete X_2 can be found the best plan is to ignore all but strong characters.

(c) 'Working out the limitation'.

It is often possible to find a complete or nearly complete X_2 at an early stage, even straight from the rectangle. It is justifiable to assume \bar{X}_2 limitation if there are many high scores and many low scores for ΔX_2 characters, but few moderate ones.

An easy example of this is:

Scores for part of Δx_1 : 9 2 12 8 10 2 0 9 36 - 2.

It is reasonable to suppose that 12, 20, 9, 36, - 2, are \bar{x}_1 crosses
and hence Δx_1 is reliable. It is reasonable to suppose that 9, 2, 0, - 2,
are \bar{x}_1 dots, and hence Δx_1 is uncertain.

Δx_1	X
x_1	- X	-	X	X X	-
	X				

It will be seen that the differencing is always wrong so that Δx_1
must be inside out. For clarity the scores will be written with the signs
changed.

	9	2	12	5	15	30	1	41	12	- 9
Δx_1	X			X	X		X			
x_1	- X	-	X	-	X X	-	X X	-		

Here differencing enables additional characters to be inserted.

Δx_1	X	- X		X X	- X	X	-		
x_1	- X	X	-	X	- X X	-	X X	-	

Because the 9 is a \bar{x}_1 cross, it probably gives the right sign for Δx_1 , whence

Δx_1	X	- X	-	X X	X	- X	-		
x_1	- X	X	-	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{X}_2 dot scores and the lowest \bar{X}_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 scoring characters can be tricky because the decibanage for a character depends on whether it is taken as a \bar{X}_2 cross or a \bar{X}_2 dot. A more precise formulation is given in R4 p57 eqn. Whilst the wheel-breaker is cerebrating, all available runs should be done, for if each supposed \bar{X}_2 cross scores 40 decibans more than any supposed \bar{X}_2 dot, even when the latter is decibanned as though it were a \bar{X}_2 cross, the wheel is certain. For decibanning R3 p 42, R4 pp 57, 104, R5 p 65.

(d) The four-letter count.

As in setting , (23E(h)) a 4-letter count for $\Delta D_1, \Delta D_2$ against \bar{X}_2 crosses, provides some evidence for the sort of ΔP to be expected. On the whole text is no bulge of $x x$ over .., or vice versa (22H(f)), the bulge against \bar{X}_2 dots being equal and opposite to that against \bar{X}_2 crosses; but at an early stage in wheel-breaking, so many of the ΔX_2 characters against \bar{X}_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{X}_2 .

(e) \hat{X}_2 .

From a \bar{X}_2 limitation message, it is sometimes possible to break wheels without a rectangle. This depends on $\Delta X_2 + \bar{X}_2$, usually written $\hat{X}_2 X_2$ (22A(b), 22D(g)), which has of course a definite value at each position of the chi 2 wheel.

Proportional bulge of $(\Delta Z_2 + \hat{X}_2 = .) = \beta \Pi_x$
where Π_x is the P.B. of $\Delta P_2 = x$ (22H9)

So that if Π_x is great enough \hat{X}_2 may be found from the short wheel-breaking run $\hat{X}_2 + \Delta Z_2 = x$, the condition for significance being as usual $\frac{x}{\sqrt{R}} >$

5.7 (R1 p11, R4 pp 70, 92, R5 p 9.)

This run is made systematically on A-tapes (33A(c)) of links likely to use \bar{X}_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{X}_2 .

Unfortunately it commonly happens that although the \hat{X}_2 run is genuinely significant it is impossible to proceed further.

The strongest run to follow \hat{X}_2 is usually (R5 pp 8, 11, 17, 28; 25Y4) $\Delta X_1 + \Delta Z_1 + \Delta Z_2 + \hat{X}_2 = .$ whose proportional bulge is

$$\beta(1 - \beta) \frac{\Pi_{..} + \Pi_{xx}}{2}$$

The ratio of this to the proportional bulge of \hat{X}_2 is

$$(1 - \beta) \frac{\Pi_{..} + \Pi_{xx}}{2\Pi_x}$$

which is often considerably less than unity (R5 p 108).

Statistics (R5 pp 98, 105, 106) show that wheel-breaking from a \hat{X}_2 start rarely succeeds unless $\frac{x}{\sqrt{R}} > 7.$

Having a significant \hat{X}_2 the best policy seems to be to set all available messages on \hat{X}_2 (a one-wheel run), not forgetting to span for message slides, strengthening \hat{X}_2 , and then trying the wheel-breaking run $\Delta X_1 \neq \Delta Z_1 + \Delta Z_2 + \hat{X}_2 = .$ on each message set. When a ΔX_1 is obtained the next run 2+/1 is $\Delta X_2 + \Delta Z_2 + \Delta X_1 + \Delta X_2 = .$ after which ordinary runs are possible.

It is sometimes possible to integrate \hat{X}_2 i.e. to find X_2 directly from \hat{X}_2 , either as a whole, if \hat{X}_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{X}_2 , could not have been broken otherwise, (R5 p 52) but ordinarily the advantage of \hat{X}_2 over a rectangle is speed. \hat{X}_2 is perhaps, most useful as an ancillary method, detecting slides in rectangles, setting rectangles on X_2 , providing a start for convergence, strengthening marginally significant rectangles, acting as a check on dubious characters in X_2 , ($\bar{X}_2, \Delta X_2$ must satisfy $\bar{X}_2 + \Delta X_2 = \hat{X}_2$).

(g) Excess of dot or cross in \hat{X}_2 .

The number of dots and crosses in \hat{X}_2 may be very far from equal: if the proportional bulge of dots is θ , then $\Delta Z_2 = ..$, which can be counted in one operation, has a proportional bulge $\theta\beta\pi_x$ (25Y1): this has been suggested as a significance test; but it is really more profitable to do \hat{X}_2 properly, for it takes very little time.

(h) $\bar{X}_2 + \bar{\bar{P}}_5$ limitation.

Because P_5 tends to be dot, this exhibits weakly the characteristics.

of \bar{X}_2 limitation; but insufficiently to do more than justify separate decibanning against \bar{X}_2 cross and \bar{X}_2 dot, both being used. The ΔD letter 5 is peculiar in scoring better against \bar{X}_2 dot than against \bar{X}_2 cross. (22H(d)) (R3 pp 10, 59.)

25F SPECIAL METHOD FOR $ab \neq \frac{1}{2}$

$$\begin{aligned} PB(\Delta D_i = .) &= PB(\Delta \Psi'_i + \Delta P_i = .) \\ &= \beta'_i \pi_i \end{aligned}$$

where β'_i is the proportional bulge of $\Delta \Psi' = .$, so that if $ab \neq \frac{1}{2}$, single wheel initial X - breaking runs are possible.

The resultant wheel is of course a true ΔX wheel and not a horrid hybrid like \hat{X}_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 $\beta'_i = \beta$.

25 WHEEL-BREAKING EXHIBITS

These consists 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 straight forward than the average wheel-breaking job. The margins of Colossus sheets have been drastically reduced.

(a) The rectangle (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 text; the leading term of significance test IV (24E(d)) is 258, so that it is unnecessary to calculate the ζ terms. Raw means made from a raw tape. (33B).

MB 2005 Run ①
Whan...
41 31 - - -
1p2. 2177
1p2x 1472 at 3649
 4h 705 60.6 11.6t
span in 200's

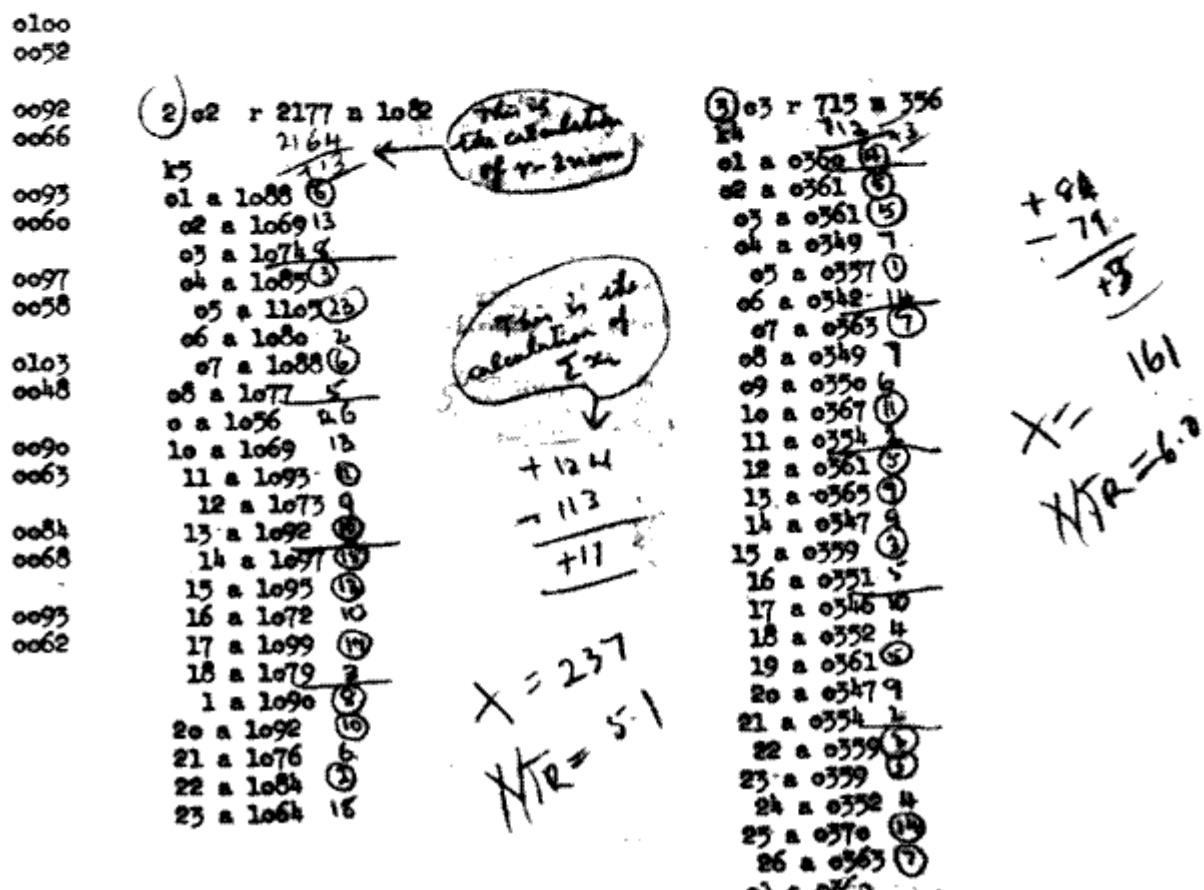
0096	
0057	0093
0076	0060
0077	0106
0090	0050
0064	0082
0090	0069
0063	0093
0091	0061
0063	0090
0086	0062
0069	0058
0097	0045
0057	
0082	
0069	
0087	
0067	
0097	
0054	

(b) Checks on Colossus.

The rectangle wheels, ΔX_1 , ΔX_2 with low-scoring characters doubted (25D(a)), are set up on Colossus (wheels AA --- Figs II, III) and the score 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) Initial runs for ΔX_5 , ΔX_4 .

The first short run is C2, $5=1=2$. It is just significant (25B(a)): $x = 5.1$. Note the check $\sum x_i = v - 2x$ norm with a discrepancy of 2. The pencilled figures are the pippages (25a) for the various characters, i.e. score minus norm. The wheel $\Delta X_5 A$, heavily doubted, is set up (Fig VI). A bold run, $4=5=1=2$, form X_4 is comfortably significant producing wheel $\Delta X_4 A$ (Fig V).



N m 2005
41,31,-,01,01
AA-AA

0096 11 6

0052 11

0062 11

0056 11

0048

0038

0043

0051

0043 11

0056 11

0120 11 3-2. (F. 10 6) 10 58

0058

0033 11

0045 11

0046 11

0038 11

5588 115
⑤ r 293 n 139

15
01 a 0133 6
02 a 0139 -

03 a 0141 14
04 a 0140 14

05 a 0148 14
06 a 0131 14

07 a 0143 14
08 a 0135 14

09 a 0137 14
10 a 0131 14

11 a 0133 14
12 a 0136 14

13 a 0144 14
14 a 0147 14

15 a 0148 14
16 a 0136 14

17 a 0147 14
18 a 0140 14

19 a 0136 14
20 a 0134 14

21 a 0135 14
22 a 0139 -

23 a 0132 14

14 14
14 14

10 2

6 238

119 119

15

01 a 0120

02 a 0119

03 a 0118

04 a 0120

05 a 0124

06 a 0123

07 a 0121

08 a 0113

09 a 0112

10 a 0118

11 a 0122

12 a 0112

13 a 0122

14 a 0123

15 a 0121

16 a 0117

17 a 0122

18 a 0122

19 a 0123

20 a 0119

21 a 0112

22 a 0126

23 a 0119

16

44

38

6

(d) Sixteen-letter counts.

A 16-letter count is made on wheels AA-AA, primarily in order to choose and deciban runs to improve ΔX_5 (25B (d), (e)). Only /9 and 58 seem to be worth while. The pencilled letters at the right indicate a justifiable suspicion that the wheels are inside out (25D (f)); but it is decided that reversal would be premature.

Runs ⑤ ⑥ are entered in pips on the run sheets, but in decibans on the wheel sheet (Fig. VI).

ΔX_5 B is a great improvement. A fourth 16-letter count is made before doing runs for ΔX_4 . The suspicion that the wheels are inside out grows.

7 mb 2005
 AA-AB
 X⁴
 0140 24
 0066
 A.U. 0105 20
 0013
 0048
 0051
 0066
 0061
 0053
 0073) 37
 0070
 0075
 0066
 0063
 0067
 0070

8 33583 r 525 n 256
 k4
01 a 0256 13
 k4
01 a 0257 ①
 02 a 0252 ⑥
 03 a 0259 ③
 04 a 0249 7
 05 a 0253 3
 06 a 0245 11
07 a 0253 ① +79
 08 a 0247 9 -66
 09 a 0250 6
 10 a 0265 ④ +13
11 a 0259 ③
12 a 0256 -
 13 a 0263 ④
 14 a 0256 -
15 a 0260 ④
16 a 0250 6
17 a 0249 7
 18 a 0257 ①
 19 a 0258 ⑤
 20 a 0250 6
 21 a 0255 1
 22 a 0253 3
 23 a 0258 ③
 24 a 0249 7
 25 a 0273 ⑦
 26 a 0271 ⑨

9 //99 r 459 n 238
 k4
 17
 k4
01 a 0256 ②
 02 a 0259 ①
 03 a 0246 ③
 04 a 0250 9
 05 a 0255 3
 06 a 0254 4
07 a 0246 ③
 08 a 0237 1
 09 a 0241 ③
 10 a 0244 ④
11 a 0233 5
12 a 0254 4 -81
13 a 0243 ⑤
 14 a 0226 12 +66
 15 a 0249 ⑦ -17
 16 a 0237 1
 17 a 0228 10
18 a 0233 5
 19 a 0245 ⑦
 20 a 0227 11
 21 a 0231 7
 22 a 0236 3
 23 a 0245 ③
 24 a 0232 6
 25 a 0242 ④
 26 a 0236 2

000000 r 417 n 206
 k4
01 a 0206 - 412
 02 a 0217 ④ +5
 03 a 0204 2
 04 a 0202 4
 05 a 0204 2
 06 a 0207 ①
 07 a 0211 ⑤
 08 a 0203 5
 09 a 0201 5
 10 a 0210 ④
 11 a 0208 ②
12 a 0206 - 41
13 a 0211 ⑤ 46
 14 a 0205 1
15 a 0206 - +5
 16 a 0206 -
 17 a 0203 3
 18 a 0204 2
 19 a 0210 ④
 20 a 0202 4
 21 a 0198 8
 22 a 0207 ①
 23 a 0208 ②
 24 a 0205 1
 25 a 0216 ⑥
 26 a 0207 ①

	12 55888 r 348 263	
MB 2005		
WH -AA-BB	16 l.c.	
41 31 - el el	et 2675	
/ 90255 15 2-1		
ht el55		
cm 0225 1-45		
n3 el44		
re ol2o		
vg el37		
lp el3e		
14 olko		
au ol88		
qv ol63		
58 0300 3-0		
kj el5o		
17 46 df el26		
14 xb el4e		
46 AC ty el72		
JK se el48		
	13 //9900mm r 940 n 462	
	13 a 0256 7 119	
	02 a 0270 7	
	03 a 0258 5 119	
	04 a 0257 6	
	05 a 0277 14	
	06 a 0256 7	
	07 a 0273 10 119	
	08 a 0257 6	
	9 a 0255 10	
	10 a 0253 10	
	11 a 0266 10	
	12 a 0256 7	
	13 a 0278 14	
	14 a 0272 9	
	15 a 0276 10	
	16 a 0256 7	
	17 a 0273 10	
	18 a 0266 10	
	1 a 0270 10	
	2 a 0259 4	
	21 a 0263 10	
	22 a 0264 10	
	23 a 0249 4	
	13 a 0458 4	
	14 a 0475 10	
	03 a 0457 5	
	04 a 0471 10	
	05 a 0468 10	
	06 a 0464 10	
	07 a 0469 10	
	08 a 0453 9	
	9 a 0450 10	
	10 a 0452 10	
	11 a 0467 10	
	12 a 0448 14	
	13 a 0471 10	
	14 a 0470 10	
	15 a 0471 10	
	16 a 0456 6	
	17 a 0457 5	
	18 a 0470 10	
	1 a 0478 10	
	2 a 0449 10	
	21 a 0449 10	
	22 a 0485 10	
	23 a 0484 10	

(e) ΔX_5 made certain.

Run (11) is yet another 16-letter count, followed by runs (12) (13) for ΔX_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 $\Delta X_5 C$ is 47 decibans up and therefore "certain". (23D(g)). Characters 13, 18 cannot be interchanged (of 25D(m)).

(e) Unsuccessful attempt to get ΔX_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 ΔX_2 and ΔX_1 , viz (16) - (21).

14 ///
r 365 n 178

k3
01 a 0175 3
02 a 0180 ①
03 a 0177 1
04 a 0176 2
05 a 0177 1
06 a 0174 4
07 a 0181 ③
08 a 0179 ①
09 a 0174 ④
10 a 0178 1
11 a 0181 ③
12 a 0179 ①
13 a 0172 6
14 a 0179 ③
15 a 0179 ①
16 a 0187 ③
17 a 0175 3
18 a 0188 ④
19 a 0177 1
20 a 0179 ①
21 a 0183 ③
22 a 0176 2
23 a 0181 ③
24 a 0180 ④
25 a 0183 ③
26 a 0177 1
27 a 0173 5
28 a 0172 6
29 a 0179 ①

M/B 2005 (15)

41, 31, - 01, 01

16 L C

WH ~~BB~~ bb-ee

et 3228

X 2 X
0365 3.5 3.5
0188 1.0
0255 1.5 1.5
0196)

L.C. 0180
✓ 0187
✓ 0147
14. 0161

0276 2.0 2.3
0173
0316 3.0 2.6
0188
0166
0154
0160
0162

(102)
16 o3 r 1091 n 351

k2

31 a 0543 16
04 a 0567 ⑥
02 a 0557 14
03 a 0566 ⑤
04 a 0540 11
05 a 0564 ⑦
06 a 0566 ⑨
07 a 0557 14
08 a 0558 ⑧
09 a 0569 ⑩
10 a 0557 14
11 a 0547 4
12 a 0536 15
13 a 0539 12
14 a 0569 ⑫
15 a 0534 12
16 a 0564 ⑬
17 a 0563 ⑭
18 a 0534 17
19 a 0560 ⑨
20 a 0552 ⑪
21 a 0567 ⑮
22 a 0539 12
23 a 0568 ⑯
24 a 0550 1
25 a 0536 15
26 a 0570 ⑯
27 a 0536 15
28 a 0541 10
29 a 0546 5
30 a 0544 7

17 umu r 482 n 252

504

T2

k2

31 a 0248 4
01 a 0254 ②
02 a 0249 3
03 a 0257 ⑤
04 a 0247 5
05 a 0253 ①
06 a 0250 2
07 a 0248 4
08 a 0256 ④
09 a 0266 ④
10 a 0258 ⑥
11 a 0245 ⑧ 9
12 a 0244 ⑦
13 a 0250 ⑤
14 a 0257 ⑤
15 a 0250 2
16 a 0257 ⑤
17 a 0253 ⑤
18 a 0242 15
19 a 0260 ④
20 a 0260 ⑧ ⑦
21 a 0255 ①
22 a 0246 16
23 a 0253 ①
24 a 0253 ①
25 a 0246 6
26 a 0255 ⑤
27 a 0244 8
28 a 0242 10
29 a 0247 5
30 a 0248 4

1195 n ~~599~~ 599 // 671 n ~~72~~

1 a 000 mm r 1111 n 22	k1	10	k1	36	21	00mm - 19 ^a n 26
	41 a 0593	11	11 a 0317	11	11 a 0261 1	
k2	21 a 0603	12	11 a 0334	12	21 a 0262 3	
31 a 0220	02 a 0595	13	02 a 0320	13	22 a 0261 4	
	03 a 0606	14	03 a 0327	14	03 a 0267 3	
02 a 0220	04 a 0596	15	04 a 0316	15	04 a 0261 1	
03 a 0219	05 a 0618	16	05 a 0334	16	05 a 0267 2	
04 a 0221	06 a 0608	17	06 a 0338	17	06 a 0266 3	
	07 a 0594	18	07 a 0328	18	07 a 0260 5	
05 a 0224	08 a 0611	19	08 a 0339	19	08 a 0265 3	
06 a 0227	09 a 0612	20	09 a 0377	20	09 a 0262 3	
07 a 0220	10 a 0595	21	10 a 0377	21	10 a 0262 3	
08 a 0231	11 a 0590	22	11 a 0325	22	11 a 0261 4	
09 a 0222	12 a 0602	23	12 a 0340	23	12 a 0262 3	
10 a 0215	13 a 0612	24	13 a 0332	24	13 a 0267 3	
11 a 0291	14 a 0597	25	14 a 0333	25	14 a 0265 3	
12 a 0293	15 a 0597	26	15 a 0321	26	15 a 0265 3	
13 a 0214	16 a 0603	27	16 a 0333	27	16 a 0265 3	
14 a 0211	17 a 0603	28	17 a 0328	28	17 a 0270 3	
15 a 0220	18 a 0607	29	18 a 0343	29	18 a 0265 3	
16 a 0226	19 a 0598	30	19 a 0314	30	19 a 0260 5	
17 a 0227	20 a 0592	31	20 a 0323	31	20 a 0265 3	
18 a 0223	21 a 0599	32	21 a 0322	32	21 a 0258 7	
19 a 0226	22 a 0591	33	22 a 0323	33	22 a 0258 7	
20 a 0213	23 a 0606	34	23 a 0338	34	23 a 0270 3	
21 a 0224	24 a 0599	35	24 a 0318	35	24 a 0259 6	
22 a 0225	25 a 0613	36	25 a 0333	36	25 a 0264 1	
23 a 0225	26 a 0603	37	26 a 0332	37	26 a 0262 3	
24 a 0230	27 a 0595	38	27 a 0323	38	27 a 0265 3	
25 a 0228	28 a 0600	39	28 a 0329	39	28 a 0264 1	
26 a 0231	29 a 0587	40	29 a 0329	40	29 a 0258 7	
27 a 0223	30 a 0611	41	30 a 0334	41	30 a 0267 3	
28 a 0218	31 a 0590	42	31 a 0333	42	31 a 0265 3	
29 a 0224	32 a 0607	43	32 a 0335	43	32 a 0270 3	
30 a 0220	33 a 0597	44	33 a 0321	44	33 a 0259 6	
	34 a 0596	45	34 a 0324	45	34 a 0267 3	
	35 a 0596	46	35 a 0317	46	35 a 0262 3	
	36 a 0607	47	36 a 0338	47	36 a 0264 1	
	37 a 0594	48	37 a 0323	48	37 a 0262 3	
	38 a 0598	49	38 a 0326	49	38 a 0261 4	
	39 a 0593	50	39 a 0325	50	39 a 0267 3	
	40 a 0595	51	40 a 0319	51	40 a 0266 1	

22 mb 2005 41,31,*,01,01

C

/4 0441 X4
1 0219 244
0 0271 04.
1 0226

4 0228
V 0207
1 0184
1 0202

W 0335 2.3
W 0215 2.3
W 0365 2.3
W 0197

1 0215
A 0102
7 0210
1 0183

(h) ΔX_4 made certain.

Run 22 is used to deciban runs for ΔX_4 viz. 23, 24, 25 which suffice to make ΔX_4 certain.

23 //99 r 754 n 380k4
 01 a 0375 5
 02 a 0370 6
 03 a 0374 6
 04 a 0389 9
 05 a 0357 2
 06 a 0395 17
 07 a 0369 11
 08 a 0393 13
 09 a 0390 18
 10 a 0363 12
 11 a 0366 14
 12 a 0356 6 +22
 13 a 0370 10 117
 14 a 0383 2 5
 15 a 0374 6 5
 16 a 0389 17
 17 a 0388 8
 18 a 0383 3
 19 a 0373 7
 20 a 0391 11
 21 a 0357 1
 22 a 0356 16
 23 a 0377 3
 24 a 0389 13
 25 a 0362 18
 26 a 0360 20

22 24 aaaaaaaa r 1243 n 611
 k4
 01 a 0598 13
 02 a 0593 14
 03 a 0599 12
 04 a 0628 1
 05 a 0623 11
 06 a 0620 9
 07 a 0593 16
 08 a 0618 3
 09 a 0612 1
 10 a 0600 11
 11 a 0618 7
 12 a 0626 1
 13 a 0608 3
 14 a 0618 3
 15 a 0589 7
 16 a 0616 3
 17 a 0626 1
 18 a 0622 1
 19 a 0600 11
 20 a 0636 1
 21 a 0628 1
 22 a 0610 1
 23 a 0601 10
 24 a 0626 1
 25 a 0595 16
 26 a 0602 9

1222
x 19

25 000 ---- r 555 n 262
 k4 524
 01 a 0263 1
 02 a 0264 2
 03 a 0262 3
 04 a 0265 5
 05 a 0269 7
 06 a 0271 9
 07 a 0261 1
 08 a 0260 2
 09 a 0265 3
 10 a 0266 4
 11 a 0257 5
 12 a 0264 7
 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 3
 23 a 0259 3
 24 a 0268 1
 25 a 0255 7
 26 a 0268 6

144
163
x 19

26
 524
 496
 478
 18
 +60
 X = 102
 Y = 4.6
 31
 21 a 0241
 22 a 0236 3
 11 a 0244 5
 12 a 0241 2
 13 a 0235 4
 14 a 0242 6
 15 a 0243 6
 16 a 0244 5
 17 a 0239 9
 18 a 0246 1
 19 a 0239 1
 20 a 0237 2
 21 a 0244 5
 22 a 0241 2
 23 a 0239 7
 24 a 0245 6
 25 a 0239 9
 26 a 0233 6
 27 a 0232 7
 28 a 0240 6

(i) A partial ΔX_3 obtained.

Runs (26), (27), (28), (29) are made for ΔX_3 only (28) has $\frac{X}{\sqrt{R}} > 5.5$,

the condition for significance. From the table in 25B(c), this is found to be worth 2.5 decibans per pips; and from it wheel ΔX_3 is considered.

27
5555 R 399 NM186

k3
01 a e189 ③
02 a e190 ③
03 a e187 5
04 a e188 5
05 a e181 5
06 a e184 2
07 a e188 ②
08 a e188 ③
09 a e181 5
10 a e185 1
11 a e187 ①
12 a e190 ④
13 a e188 ③
a e189 ③
15 a e189 ③
16 a e189 ③
17 a e184 2
18 a e189 ③
19 a e189 ③
20 a e189 ③
21 a e185 1
22 a e190 ④
23 a e186 -
24 a e187 ①
25 a e187 ③
26 a e191 ③
27 a e182 4
28 a e186 5
29 a e188 ③

(5)
26
27
 $X = 7.9$
 $\frac{X}{VR} = 3.8$

UUU
R 368 NM 191 (28) 3 4 2
3 6 5
3 1 4
k3
01 a e185 6
02 a e194 ③
03 a e188 3
04 a e193 ②
05 a e195 ③
06 a e185 5
07 a e193 ②
08 a e193 ③
09 a e189 1
10 a e183 6
11 a e186 5
12 a e200 ③
13 a e185 1
14 a e197 ④
15 a e194 2
16 a e189 10
17 a e181 6
18 a e195 5
19 a e195 4
20 a e187 6
21 a e185 6
22 a e193 ②
23 a e192 ③
24 a e191 1
25 a e198 ③
26 a e192 6
27 a e185 1
28 a e196 ③
29 k3 e195

$X = 11.3$

$\frac{X}{VR} = 5.9$

fff
R 247 NM 108
k3
29 a e110 ②
01 a e111 ③
02 a e109 ①
03 a e109 ①
04 a e110 ②
05 a e107 1
06 a e107 1
07 a e111 ③
08 a e104 4
09 a e110 ③
10 a e111 ③
11 a e118 ⑤
12 a e106 2
13 a e110 ②
14 a e102 6
15 a e103 -
16 a e110 ②
17 a e111 ③
18 a e111 ③
19 a e105 2
20 a e104 4
21 a e103 -
22 a e108 -
23 a e113 ③
24 a e110 ②
25 a e111 ③
26 a e108 -
27 a e109 ③
28 a e112 ③

32	33	34	35
code	code	code	code
0031	0031	0031	0031
0046	0046	0046	0046
0049	0049	0049	0049
0051	0051	0051	0051
0052	0052	0052	0052
0055	0055	0055	0055
0056	0056	0056	0056
0057	0057	0057	0057
0058	0058	0058	0058
0059	0059	0059	0059
0060	0060	0060	0060
0061	0061	0061	0061
0062	0062	0062	0062
0063	0063	0063	0063
0064	0064	0064	0064
0065	0065	0065	0065
0066	0066	0066	0066
0067	0067	0067	0067
0068	0068	0068	0068
0069	0069	0069	0069
0070	JSY0	JSY0	JSY0
0071	0071	0071	0071
0072	0072	0072	0072
0073	0073	0073	0073
0074	0074	0074	0074
0075	0075	0075	0075
0076	0076	0076	0076
0077	0077	0077	0077
0078	0078	0078	0078
0079	0079	0079	0079
0080	0080	0080	0080
0081	0081	0081	0081
0082	0082	0082	0082
0083	0083	0083	0083
0084	0084	0084	0084
0085	0085	0085	0085
0086	0086	0086	0086
0087	0087	0087	0087
0088	0088	0088	0088
0089	0089	0089	0089
0090	0090	0090	0090
0091	0091	0091	0091
0092	0092	0092	0092
0093	0093	0093	0093
0094	0094	0094	0094
0095	0095	0095	0095
0096	0096	0096	0096
0097	0097	0097	0097
0098	0098	0098	0098
0099	0099	0099	0099
0100	0100	0100	0100
0101	0101	0101	0101
0102	0102	0102	0102
0103	0103	0103	0103
0104	0104	0104	0104
0105	0105	0105	0105
0106	0106	0106	0106
0107	0107	0107	0107
0108	0108	0108	0108
0109	0109	0109	0109
0110	0110	0110	0110
0111	0111	0111	0111
0112	0112	0112	0112
0113	0113	0113	0113
0114	0114	0114	0114
0115	0115	0115	0115
0116	0116	0116	0116
0117	0117	0117	0117
0118	0118	0118	0118
0119	0119	0119	0119
0120	0120	0120	0120
0121	0121	0121	0121
0122	0122	0122	0122
0123	0123	0123	0123
0124	0124	0124	0124
0125	0125	0125	0125
0126	0126	0126	0126
0127	0127	0127	0127
0128	0128	0128	0128
0129	0129	0129	0129
0130	0130	0130	0130
0131	0131	0131	0131
0132	0132	0132	0132
0133	0133	0133	0133
0134	0134	0134	0134
0135	0135	0135	0135
0136	0136	0136	0136
0137	0137	0137	0137
0138	0138	0138	0138
0139	0139	0139	0139
0140	0140	0140	0140
0141	0141	0141	0141
0142	0142	0142	0142
0143	0143	0143	0143
0144	0144	0144	0144
0145	0145	0145	0145
0146	0146	0146	0146
0147	0147	0147	0147
0148	0148	0148	0148
0149	0149	0149	0149
0150	0150	0150	0150
0151	0151	0151	0151
0152	0152	0152	0152
0153	0153	0153	0153
0154	0154	0154	0154
0155	0155	0155	0155
0156	0156	0156	0156
0157	0157	0157	0157
0158	0158	0158	0158
0159	0159	0159	0159
0160	0160	0160	0160
0161	0161	0161	0161
0162	0162	0162	0162
0163	0163	0163	0163
0164	0164	0164	0164
0165	0165	0165	0165
0166	0166	0166	0166
0167	0167	0167	0167
0168	0168	0168	0168
0169	0169	0169	0169
0170	0170	0170	0170
0171	0171	0171	0171
0172	0172	0172	0172
0173	0173	0173	0173
0174	0174	0174	0174
0175	0175	0175	0175
0176	0176	0176	0176
0177	0177	0177	0177
0178	0178	0178	0178
0179	0179	0179	0179
0180	0180	0180	0180
0181	0181	0181	0181
0182	0182	0182	0182
0183	0183	0183	0183
0184	0184	0184	0184
0185	0185	0185	0185
0186	0186	0186	0186
0187	0187	0187	0187
0188	0188	0188	0188
0189	0189	0189	0189
0190	0190	0190	0190
0191	0191	0191	0191
0192	0192	0192	0192
0193	0193	0193	0193
0194	0194	0194	0194
0195	0195	0195	0195
0196	0196	0196	0196
0197	0197	0197	0197
0198	0198	0198	0198
0199	0199	0199	0199
0200	0200	0200	0200
0201	0201	0201	0201
0202	0202	0202	0202
0203	0203	0203	0203
0204	0204	0204	0204
0205	0205	0205	0205
0206	0206	0206	0206
0207	0207	0207	0207
0208	0208	0208	0208
0209	0209	0209	0209
0210	0210	0210	0210
0211	0211	0211	0211
0212	0212	0212	0212
0213	0213	0213	0213
0214	0214	0214	0214
0215	0215	0215	0215
0216	0216	0216	0216
0217	0217	0217	0217
0218	0218	0218	0218
0219	0219	0219	0219
0220	0220	0220	0220
0221	0221	0221	0221
0222	0222	0222	0222
0223	0223	0223	0223
0224	0224	0224	0224
0225	0225	0225	0225
0226	0226	0226	0226
0227	0227	0227	0227
0228	0228	0228	0228
0229	0229	0229	0229
0230	0230	0230	0230
0231	0231	0231	0231
0232	0232	0232	0232
0233	0233	0233	0233
0234	0234	0234	0234
0235	0235	0235	0235
0236	0236	0236	0236
0237	0237	0237	0237
0238	0238	0238	0238
0239	0239	0239	0239
0240	0240	0240	0240
0241	0241	0241	0241
0242	0242	0242	0242
0243	0243	0243	0243
0244	0244	0244	0244
0245	0245	0245	0245
0246	0246	0246	0246
0247	0247	0247	0247
0248	0248	0248	0248
0249	0249	0249	0249
0250	0250	0250	0250
0251	0251	0251	0251
0252	0252	0252	0252
0253	0253	0253	0253
0254	0254	0254	0254
0255	0255	0255	0255
0256	0256	0256	0256
0257	0257	0257	0257
0258	0258	0258	0258
0259	0259	0259	0259
0260	0260	0260	0260
0261	0261	0261	0261
0262	0262	0262	0262
0263	0263	0263	0263
0264	0264	0264	0264
0265	0265	0265	0265
0266	0266	0266	0266
0267	0267	0267	0267
0268	0268	0268	0268
0269	0269	0269	0269
0270	0270	0270	0270
0271	0271	0271	0271
0272	0272	0272	0272
0273	0273	0273	0273
0274	0274	0274	0274
0275	0275	0275	0275
0276	0276	0276	0276
0277	0277	0277	0277
0278	0278	0278	0278
0279	0279	0279	0279
0280	0280	0280	0280
0281	0281	0281	0281
0282	0282	0282	0282
0283	0283	0283	0283
0284	0284	0284	0284
0285	0285	0285	0285
0286	0286	0286	0286
0287	0287	0287	0287
0288	0288	0288	0288
0289	0289	0289	0289
0290	0290	0290	0290
0291	0291	0291	0291
0292	0292	0292	0292
0293	0293	0293	0293
0294	0294	0294	0294
0295	0295	0295	0295
0296	0296	0296	0296
0297	0297	0297	0297
0298	0298	0298	0298
0299	0299	0299	0299
0300	0300	0300	0300

(j) Runs to improve ΔX_3 : redecibanning.

A 32-letter count is used to choose runs to improve ΔX_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 JSY0 is the only new run, but ΔX_3B is great improvement on ΔX_3A , and a further letter count, numbered (32), suggests additional runs as well as redecibanning (27) a second time.

34	35
code	code
0031	0031
0046	0046
0049	0049
0051	0051
0052	0052
0055	0055
0056	0056
0057	0057
0058	0058
0059	0059
0060	0060
0061	0061
0062	0062
0063	0063
0064	0064
0065	0065
0066	0066
0067	0067
0068	0068
0069	0069
0070	0070
0071	0071
0072	0072
0073	0073
0074	0074
0075	0075
0076	0076
0077	0077
0078	0078
0079	0079
0080	0080
0081	0081
0082	0082
0083	0083
0084	0084
0085	0085
0086	0086
0087	0087
0088	0088
0089	0089
0090	0090
0091	0091
0092	0092
0093	0093
0094	0094
0095	0095
0096	0096
0097	0097
0098</td	

36

///UUU

R 851 NM 433

k1
 20 a 0440 (7) 6
 21 a 0439 (6)
 22 a 0426 7
 23 a 0437 (4) 6
 24 a 0427
 25 a 0438 (5) 1
 26 a 0434 (1)
 27 a 0421 12 (7)
 28 a 0440
 29 a 0434 (3) X K1
 30 a 0436
 31 a 0420 12 (3) 11
 32 a 0435 (3) 10
 33 a 0441 (6) 3
 34 a 0439 (6) 3
 35 a 0430
 36 a 0443 (6) 1
 37 a 0442
 38 a 0432 1
 39 a 0426 7
 40 a 0429 4
 41 a 0428 5
 01 a 0423 10
 02 a 0441 (1)
 03 a 0431 2
 04 a 0435 (1) 2
 05 a 0431
 06 a 0425 (2) 9
 07 a 0435 (2)
 08 a 0424 9
 09 a 0436 (3) 4
 10 a 0437 (4) 13
 11 a 0446 (13)
 12 a 0425 8
 13 a 0433 - 3
 14 a 0430
 15 a 0432 1
 16 a 0432
 17 a 0428 5
 18 a 0428 5 6
 19 a 0427

37

AAA555

0000000888

R 833 NM 412.

k1
 20 a 0412 -
 21 a 0421 (9)
 22 a 0414 (2)
 23 a 0416 (4)
 24 a 0405 7
 25 a 0418 (6) 10
 26 a 0415 (8) 10
 27 a 0402 (10) 4
 28 a 0415 (3)
 29 a 0418 (6)
 30 a 0415 (5) 8
 31 a 0408 4
 32 a 0417 (6)
 33 a 0413 (6)
 34 a 0413 (5)
 35 a 0402 11
 36 a 0408 (3)
 37 a 0415 (3)
 38 a 0418 (6)
 39 a 0424 (2)
 40 a 0401
 41 a 0414 (9)
 01 a 0411
 02 a 0405 7
 03 a 0410 2
 04 a 0411
 05 a 0416 (4)
 06 a 0407
 07 a 0409 3
 08 a 0412
 09 a 0412
 10 a 0414 (2)
 11 a 0412 -
 12 a 0406 (6)
 13 a 0416 (4)
 14 a 0413 (6)
 15 a 0418 (8)
 16 a 0418 (4)
 17 a 0412 -
 18 a 0412 (8)
 19 a 0403 9

38

39

40

///MM333UUU 0000999JJJ

R 1119 NM 538	R 936 NM 4 k1	R 746 NM. 36
20 a 0542 (2)	16 a 0454 (1)	16 a 0358 7
21 a 0540 (3)	17 a 0450 (1)	17 a 0364 1
22 a 0527 11	18 a 0450 (1)	18 a 0364 1
23 a 0537 (1)	18 a 0449 4	19 a 0371 (2)
24 a 0542 (5)	19 a 0463 (1)	20 a 0356 9
25 a 0546 (X)	20 a 0436 (3)	21 a 0366 (1)
26 a 0539 (1)	21 a 0463 (1)	23 a 0365 -
27 a 0535 3	22 a 0459 (6)	24 a 0372 (7)
28 a 0544 (6)	23 a 0444	25 a 0362 3
29 a 0542 (4)	24 a 0452	26 a 0369 (4)
30 a 0547 (1)	25 a 0434 (5)	27 a 0369 (4)
31 a 0529 (9)	26 a 0452 1	28 a 0360 5
32 a 0539 (1)	27 a 0437 6	29 a 0360 5
33 a 0536 2	28 a 0451 2	30 a 0369 (4)
34 a 0547 (5)	29 a 0470 (7)	31 a 0366 (1)
35 a 0538 - (1)	30 a 0451 1	32 a 0369 (4)
36 a 0557 (1)	31 a 0452 1	33 a 0360 5
37 a 0542 (4)	32 a 0458 (5)	34 a 0367 (2)
38 a 0542 (4)	33 a 0463 (10)	35 a 0359 6
39 a 0537 1	34 a 0453 -	36 a 0358 7
40 a 0535 2	35 a 0450 3	37 a 0361 4
41 a 0535 2	36 a 0453 -	38 a 0372 (7)
01 a 0533 4	37 a 0442 4	39 a 0362 3
02 a 0538 -	38 a 0448 5	40 a 0362 3
03 a 0536 2	39 a 0447 6	41 a 0375 (10)
04 a 0542 (4)	40 a 0446 7	01 a 0365 -
05 a 0541 (3)	41 a 0453 -	02 a 0366 (1)
06 a 0531 4	01 a 0451 2	03 a 0367 (2)
07 a 0533 (15)	02 a 0448 5	04 a 0361 4
08 a 0525 13	03 a 0464 (1)	05 a 0368 (3)
09 a 0557 (1)	04 a 0447 6	06 a 0371 (6)
10 a 0540 (2)	05 a 0467 (16)	07 a 0373 (3)
11 a 0540 (2)	06 a 0453 (16)	08 a 0365 -
12 a 0537 1	07 a 0462 (4)	09 a 0363 -
13 a 0534 T	08 a 0442 (1)	10 a 0364 1
14 a 0538 - (13)	09 a 0459 (6)	11 a 0368 (3)
15 a 0531 (13)	10 a 0446 1	12 a 0367 (2)
16 a 0534 4	11 a 0468 (1)	13 a 0363 -
17 a 0524 14	12 a 0446 (1)	14 a 0362 3
18 a 0535 3	13 a 0443 (1)	15 a 0363 2
19 a 0530 8	14 a 0454 (1)	
	15 a 0451 2	

(k) Setting other messages.

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 the 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 loss of only 38 decibans.

MS 2005
404
MS 2005 32 L.C.
2nd hand
400000
12-
32 L.C.

e285	4.4	1.00000	cool
e211	3	1.00000 (13)	cool 26
e143		0005 (4)	cool 9
e111		0002	cool
		0002	cool
e177	3		
e124		0001 3	cool
e126		0002	cool
e150		0008	cool
		0004	cool
e130			
e125		0001	cool
e114		0003	cool
e125		0001	cool
		0006	cool
e113			
ee99		0002	cool
e113		0004	cool
e116		0002	cool
		0007	cool
e131			
e277	7	3.00000	cool
e141	1.5	0005 (3)	cool
e109		0006 (3)	cool
		0005	cool
e223	1.6		
e176	1.9	1.00000 (6)	cool
e149		0006 (6)	cool
e117		0003 (6)	cool
		0004	cool
e136			
e111		0006	cool
e117		0002	cool
ee87		0005	cool
		0002	cool
e105			
e139		0002	cool
e106		0004	cool
e103		0002	cool

36 TEL 86

MS 2004 RAW

		/000000000	R 0753	BB577
g	0269	11	262e R NM 1053	12
g	0265		13	31 a 0368 9
h	0192		32 a 0397 13	
t	0191		33 a 0364 13	
e	0213	1	34 a 0389 13	
m	0172		35 a 0374 5	
n	0170		36 a 0390 3	
z	0180		37 a 0393 13	
r	0191		38 a 0363 13	
c	0187		39 a 0388 13	
v	0197		40 a 0392 13	
s	0218	1-4	41 a 0377 13	
l	0149		42 a 0377 13	
p	0158		43 a 0364 13	
i	0161		44 a 0368 9	
k	0156		45 a 0395 13	
a	0198	1-3	46 a 0363 13	
u	0267	1-3	47 a 0377 13	
q	0262	1-7	48 a 0389 13	
w	0138		49 a 0364 13	
j	0261	1-4	50 a 0399 13	
g	0256		51 a 0378 13	
k	0163		52 a 0364 13	
j	0176		53 a 0394 13	
d	0190		54 a 0363 13	
f	0193		55 a 0367 13	
x	0186		56 a 0376 1	
b	0158		57 a 0374 3	
z	0165			
y	0155			
z	0165			
z	0155			

(l) Letter counts against doubtful characters.

To make ΔX 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 $(6 - 3) \times 10 \log_{10} \frac{285}{103} = 3 \times 4.4 = 13$.

In effect 7 runs are used; this makes ΔX_1 certain. (cf 25D(g)3)

(m) Making ΔX_2 certain.

The letter count (43) on MB2004 suggests a slightly odd run (44) for ΔX_3 , and also run (48) for ΔX_3 . The previous letter count (40a) is used to deciban runs (45), (46), (47) for ΔX_2 ; ΔX_3 becomes certain.

(m) Making ΔX_3 certain.

A (lost) letter count on MB2003 is used to deciban runs (50), (51), (52) for ΔX_3 . Most characters score well, but the 1st character has a score with the wrong sign, and the wheel is not certain.

Individual letter counts against the three weakest characters on the three

52 (1a)		53
MB 2005.	MB 2004	
doddo	count ag 1st char w/ X_3 Score 4 x	
41 31 01 01 01	0007 3	
/ 0299 1 3	0007	
0 0224	0006	
H 0149 1 9	0006	
1 0122	0006 3	
	0009	
	0005	
	0011	
	0007	
	0008	
	0008	
	0006 1 8	
	0009	
	0006	
	0004	
	0002	
	0009	
	0006	
	0004	
	0006 2 6	
	0006 1 7	
	0004	
	0005 4	
	0006	
	0005	

999000	(46)			
R 727	MM 386	67	0088	R 649 MM 332
k2			k2	
31 a 0376	50		31 a 0321	11
01 a 0391	51		01 a 0331	1
02 a 0379	52		02 a 0333	3
03 a 0392	53		03 a 0337	3
04 a 0374	54		04 a 0326	6
05 a 0384	55		05 a 0335	3
06 a 0393	56		06 a 0336	3
07 a 0383	57		07 a 0326	24
08 a 0388	58		08 a 0340	23
09 a 0405	59		09 a 0333	14
10 a 0384	60		10 a 0327	5
11 a 0375	61		11 a 0338	
12 a 0374	62		12 a 0334	2
13 a 0388	63		13 a 0324	8
14 a 0394	64		14 a 0336	4
15 a 0374	65		15 a 0329	3
16 a 0393	66		16 a 0341	3
17 a 0387	67		17 a 0329	3
18 a 0378	68		18 a 0350	2
19 a 0399	69		19 a 0338	6
20 a 0389	70		20 a 0334	3
21 a 0388	71		21 a 0337	3
22 a 0378	72		22 a 0325	7
23 a 0393	73		23 a 0335	3
24 a 0390	74		24 a 0328	4
25 a 0376	75		25 a 0331	3
26 a 0396	76		26 a 0342	6
27 a 0376	77		27 a 0329	3
28 a 0373	78		28 a 0319	13
29 a 0373	79		29 a 0325	7
30 a 0374	80		30 a 0327	5
			51.	
			52.	
UUV 54	53HHOG	75		53 333000JJJJ777SSSS
R 245	MM 127	76		R 1090 MM 554
k3			k3	
03 a 0120	7		03 a 0574	1
04 a 0128	1		04 a 0576	1
05 a 0125	2		05 a 0571	4
06 a 0131	2		06 a 0581	6
07 a 0127	5		07 a 0576	6
08 a 0123	4		08 a 0568	8
09 a 0128	6		09 a 0577	1
10 a 0130	3		10 a 0580	1
11 a 0125	2		11 a 0571	1
12 a 0122	5		12 a 0575	6
13 a 0124	3		13 a 0567	6
14 a 0133	6		14 a 0567	6
15 a 0125	1		15 a 0563	10
16 a 0131	2		16 a 0578	5
17 a 0132	3		17 a 0586	8
18 a 0131	4		18 a 0582	9
19 a 0129	5		19 a 0573	7
20 a 0131	6		20 a 0582	7
21 a 0125	4		21 a 0580	7

13 a 0367	13 a 0367	0120
14 a 0133 ⑥	14 a 0367	0132
15 a 0125 1	15 a 0363	0004
16 a 0131 ④	16 a 0378	0006
17 a 0132 ⑤	17 a 0386	0003
18 a 0131 ④	18 a 0388	0004
19 a 0129 ④	19 a 0373	0006
20 a 0131 ④	20 a 0382	0005
21 a 0125 2	21 a 0386	0005
22 a 0122 5	22 a 0359	0001
23 a 0127 1	23 a 0371	0002
24 a 0129 ②	24 a 0378	0003
25 a 0128 1	25 a 0383	0003
26 a 0126 1	26 a 0369	0002
27 a 0129 ③	27 a 0376	0003
28 a 0126 1	28 a 0385	0003
29 a 0124 3	29 a 0370	0003
30 a 0121 6	30 a 0373	0007
31 a 0122 5	31 a 0375	0005
32 a 0122 5	32 a 0371	0008
	—	0006
		⑦

- 48
+ 37

55

mb 2004	53	mb 2005	54	mb 2005	54	mb 2005	54	mb 2005	55	mb 2003	55	mb 2003
count ag 8 th charact. /X ₃	count ag 26th	count ag. 1st.	doubting 8th	doubting 26th						1st charact. /X ₃	8 th char.	26 chr.
clearing 1/X ₃ character /X ₃	clearing 1/X ₃ character /X ₃	clearing 1/X ₃ character /X ₃	clearing 1/X ₃ character /X ₃	clearing 1/X ₃ character /X ₃					clearing 1/X ₃	1/X ₃	1/X ₃	
ooo7 (1) ooo9 1.3	ooo6 1.3	ooo9 1.3	ooo2 2.6	ooo2 2.6					ooo3	ooo6	ooo4	
ooo6 1.3	ooo6 1.3	ooo6 1.3	ooo2 2.6	ooo2 2.6					ooo3 1.2	ooo7	ooo5	
ooo6 1.3	ooo6 1.3	ooo6 1.3	ooo2 2.6	ooo2 2.6					ooo4	ooo5	ooo4	
ooo8 1.3	ooo4 1.3	ooo5 1.3	ooo3 5.4	ooo3 5.4					ooo5 1.1	ooo6	ooo4	
ooo8 1.3	ooo6 1.3	ooo3 2.6	ooo8 1.3	ooo8 1.3					ooo6	ooo5	ooo2	
ooo5 1.3	ooo6 1.3	ooo1 1.3	ooo2 1	ooo2 1					ooo7	ooo6	ooo2	
ooo8 1.3	ooo6 1.3	ooo9 1.3	ooo3 1	ooo3 1					ooo8	ooo7	ooo2	
ooo7 1.3	ooo9 1.3	ooo5 1.3	ooo4 1	ooo4 1					ooo9 1.1	ooo8	ooo2	
ooo1 1.3	ooo5 1.3	ooo2 1.3	ooo3 1	ooo3 1					ooo1 1.2	ooo3	ooo7	
ooo6 1.3	ooo9 1.3	ooo6 1.3	ooo7 1	ooo7 1					ooo2 1.2	ooo3	ooo2	
ooo7 1.3	ooo9 1.3	ooo6 1.3	ooo3 1	ooo3 1					ooo3 1	ooo5	ooo4	
ooo5 1.3	ooo4 1.3	ooo7 1	ooo4 1	ooo4 1					ooo4	ooo5	ooo4	
ooo2 1.3	ooo5 1.3	ooo3 1	ooo5 1	ooo5 1					ooo5	ooo6	ooo4	
ooo1 1.3	ooo7 1.3	ooo3 1	ooo6 1	ooo6 1					ooo6	ooo5	ooo4	
ooo2 1.3	ooo5 1.3	ooo3 1	ooo6 1	ooo6 1					ooo7	ooo6	ooo5	
ooo4 1.3	ooo7 1.3	ooo3 1	ooo6 1	ooo6 1					ooo8	ooo7	ooo6	
ooo7 1.3	ooo9 1.3	ooo4 1	ooo7 1	ooo7 1					ooo9 1.1	ooo8	ooo7	
ooo5 1.3	ooo8 1.3	ooo7 1	ooo5 1	ooo5 1					ooo1 1.2	ooo3	ooo2	
ooo7 1.3	ooo8 1.3	ooo4 1	ooo6 1	ooo6 1					ooo2 1.2	ooo3	ooo2	
ooo8 1.3	ooo8 1.3	ooo3 1	ooo5 1	ooo5 1					ooo3 1	ooo4	ooo3	
ooo6 1.3	ooo6 1.3	ooo3 1	ooo4 1	ooo4 1					ooo4	ooo5	ooo3	
ooo1 1.3	ooo9 1.3	ooo1 1	ooo3 1	ooo3 1					ooo5	ooo6	ooo4	
ooo3 1	ooo7 1	ooo3 1	ooo5 1	ooo5 1					ooo6	ooo5	ooo4	
ooo6 1	ooo7 1	ooo2 1	ooo4 1	ooo4 1					ooo7	ooo6	ooo5	
ooo6 1	ooo7 1	ooo3 1	ooo5 1	ooo5 1					ooo8	ooo7	ooo6	
ooo6 1	ooo7 1	ooo3 1	ooo6 1	ooo6 1					ooo9 1	ooo8	ooo7	
ooo6 1	ooo7 1	ooo3 1	ooo6 1	ooo6 1					ooo10	ooo9	ooo8	
-5	+1.4	+1.2	+1.2	+1.2								

(29)

(3.6)

5.1

+3
-24
60

(60)

mb 2009

1st chr k3

6	ccc6	at 1 db	≈ 3
7	ccc7		
8	ccc6	at 2 db	≈ 6
9	ccc7		

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.

25W DERIVATION OF FORMULAE FOR THE WEIGHING OF EVIDENCE(a) Significance test.

Let:

R be the number of places looked at

ω be the wheel length

σ be the standard deviation of the double bulge against a single character, viz \sqrt{R}/ω

z be the typical double bulge against a single character

x be the observed sum of the moduli of double bulges.

The expected modulus of the score against a single character is

$$\begin{aligned} & \int_{-\infty}^{\infty} \frac{e^{-\frac{z^2}{2\sigma^2}}}{\sqrt{2\pi}\sigma} |Z| dz \\ &= 2 \int_0^{\infty} \frac{e^{-\frac{z^2}{2\sigma^2}}}{\sqrt{2\pi}\sigma} \cdot Z dz \\ &= \sqrt{\frac{2}{\pi}} \sigma \quad \text{W1} \\ &= \sqrt{\frac{2}{\pi}} \sqrt{\frac{R}{\omega}} \quad \text{W2} \end{aligned}$$

Its variance is

$$\begin{aligned} & \int_{-\infty}^{\infty} \frac{e^{-\frac{z^2}{2\sigma^2}}}{\sqrt{2\pi}\sigma} \left(|Z| - \sqrt{\frac{2}{\pi}} \sigma \right)^2 dz \\ &= 2 \int_0^{\infty} \frac{e^{-\frac{z^2}{2\sigma^2}}}{\sqrt{2\pi}\sigma} \left(Z^2 - 2\sqrt{\frac{2}{\pi}} \sigma Z + \frac{2}{\pi} \sigma^2 \right) dz \\ &= \sigma^2 - \frac{4}{\pi} \sigma^2 + \frac{2}{\pi} \sigma^2 \end{aligned}$$

and hence its standard deviation is

$$\sqrt{1 - \frac{2}{\pi}} \sigma \quad \text{W3}$$

$$= \sqrt{1 - \frac{2}{\pi}} \sqrt{\frac{R}{\omega}} \quad \text{W4}$$

from W2, the expected sum of moduli for the whole wheel is

$$\omega \sqrt{\frac{2}{\pi}} \cdot \sqrt{\frac{R}{\omega}} \quad \text{or} \quad \sqrt{\frac{2}{\pi}} \sqrt{R\omega} \quad \text{W5}$$

from W4, its standard deviation is

$$\sqrt{\omega} \cdot \sqrt{1 - \frac{2}{\pi}} \sqrt{\frac{R}{\omega}} \quad \text{or} \quad \sqrt{1 - \frac{2}{\pi}} \sqrt{R} \quad \text{W6}$$

It is considered that for the significance of a single trial, a sufficient sigmaage is 2, i.e.

$$x > \sqrt{\frac{2}{\Pi}} \sqrt{R\omega} + 2 \cdot \sqrt{1 - \frac{2}{\Pi}} \sqrt{R} \quad W7$$

or approximately

$$\frac{x}{\sqrt{R}} > 0.8\sqrt{\omega} + 1.2 \quad W8$$

(For this test R3 pp 5, 6, 7. A slight generalization R4 p 100. Controversy R4 pp 93, 100. Tests based on a letter count X_2 test R4 p 54; R5 pp 3, 8, 11, 37, 113: $\Sigma n \log n$ R4 pp 56, 70, 121; R5 pp 1, 3, 7.)

(b) Fundamental decibanning formula.

Let δ be the true proportional bulge of the run.

Suppose that a particular place in the cipher is observed to favour a dot in ΔX .

If the corresponding character of ΔX is a dot, the probability of the observation is $\frac{1+\delta}{2}$

If the corresponding character of ΔX is a cross, the probability of the observation is $\frac{1-\delta}{2}$

Whence the factor in favour of a dot is $\frac{1+\delta}{1-\delta}$

Hence if the double bulge in favour of a dot, i.e. the excess of places favouring dot over places favouring cross, is x_i , the total factor is

$$\left(\frac{1+\delta}{1-\delta} \right)^{x_i}$$

whose decibanage is $x_i 10 \log_{10} \frac{1+\delta}{1-\delta}$

i.e. $10 \log_{10} \frac{1+\delta}{1-\delta}$ decibans per pip W9

N.B. This is the decibanage for dot rather than cross, not for dot rather than random.

The major problem is to find δ .

(c) Impracticability of exact formulae.

An exact formula is impracticable, for it must use not only the evidence of the run, but also general fish evidence. Even if it could be evaluated, its precision would be largely illusory. The formula is

$$\frac{\int_{-1}^1 p(x | R, \delta)p(\delta)\delta d\delta}{\int_{-1}^1 p(x | R, \delta)p(\delta)d\delta}$$

(d) Decibanning a run on its own message and correct wheels.

If δ is to be evaluated from the evidence of the message under consideration only, then $\delta = \frac{x^*}{R}$ where x^* is the double bulge on the correct wheels. This is a compact and convenient notion, though until the correct wheels are known, x^* is unknown and must be estimated.

(e) Decibanning a run from its own wheel.

To simplify the calculation it is assumed

- (i) that a sufficient approximation to the expected δ is that value of δ whose expected $\frac{x}{R}$ is the observed $\frac{x}{R}$.
- (ii) that the distribution of x is normal. This is satisfactory if $x \ll R$, a condition satisfied except in key.

It will be convenient, though using the same notation as before, to interpret it more generally by taking Z to be the deviation of a typical double bulge from its mean, $\frac{R\delta}{\omega}$, so that the variance of Z will be $\sigma^2 = \frac{R}{\omega}(1 - \delta^2)$. Previously we took $\delta = 0$.

Suppose that the wheel is constructed entirely from the run. Then the score, for a single character is

$$\left| z + \frac{R\delta}{\omega} \right| \quad \text{W10}$$

and the expected score, x , for the whole wheel is

$$\omega \int_{-\infty}^{\infty} \frac{e^{-z^2/2\sigma^2}}{\sqrt{2\pi}\sigma} \left| z + \frac{R\delta}{\omega} \right| dz \quad \text{W11}$$

$$\therefore \frac{1}{q} = \frac{x}{R\delta} = \frac{1}{R\delta} \left\{ - \int_{-\infty}^{\frac{R\delta}{\omega}} + \int_{\frac{R\delta}{\omega}}^0 + \int_0^{\frac{R\delta}{\omega}} \frac{e^{-z^2/2\sigma^2}}{\sqrt{2\pi}\sigma} \left(z + \frac{R\delta}{\omega} \right) dz \right\}$$

$$\text{which reduces to } \frac{1}{q} = \sqrt{\frac{2}{\Pi}} \frac{1}{\zeta e^{\frac{\zeta^2}{2}}} + 2 \int_0^\zeta \frac{1}{\sqrt{2\Pi}} e^{-\frac{t^2}{2}} \cdot dt \quad W12$$

$$\text{where } \zeta = \frac{R\delta}{\omega\sigma} \quad W13$$

$$\text{remembering } \sigma^2 = \frac{R}{\omega} (1 - \delta^2) \quad W14$$

$$q = \frac{R\delta}{\omega} \quad W15$$

and eliminating σ, δ from W13, W14, W15

$$\frac{\zeta}{q} = \frac{\omega}{\sqrt{R\omega}} \sqrt{1 + \frac{\zeta^2\omega}{R}} \quad W16$$

$$= \frac{\omega}{\sqrt{R\omega}} \quad W17$$

What is required is q as a function x, R, ω and this can theoretically be obtained by eliminating ζ from W12, W16.

It is more convenient to replace W16 by the pessimistic approximation W17. Then by taking a series of values of ζ , it is easy to construct a table of q as a function of $\frac{x}{\sqrt{R\omega}}$. This is given in 25B(c).

(f) Decibanning from a letter count.

On the correct wheel the expected score is the expected value of $|Z + R\delta|$, so that it can be calculated from W11 by putting $\omega = 1$, and the table of 25B(c) is applicable (R5 p 109). Inspection of the table shows that when $\omega = 1$, and the total decibannage, roughly $8.7 \left(\frac{x}{\sqrt{R}} \right)^2$, is sufficient to make the run worth while, $q = 1$ i.e. crude decibanning is adequate.

It follows that if the wheel is independent of the run, but not necessarily correct, crude decibanning will tend, in practice inappreciably, to be too pessimistic, except for very feeble runs. This remark applies to decibanning from a letter count, any run not used in making the letter count wheels, including all runs on a newly set message.

If the run is used, but not alone, in making the wheel, some value of ω between 1 and the actual wheel-length is required, but it has not been found necessary to investigate this more precisely.

(R3 pp 6,7. Premonitions R2 pp 57, 72. Non-linearity R3 p 132. Triviality R5 p 70. Further references under methods for \bar{X}_2 limitation.)

25X THE NUMBER OF LEGAL WHEELS.

In order that X_6 shall generate a ΔX_5 with 12 crosses, it must consist of 6 blocks of crosses and 6 blocks of dots. Each block must contain at least one character, and, for legality, not more than four. There must be in all 12 (or 11) crosses and 11 (or 12) dots.

The number of ways in which such blocks can be chosen is

$$\begin{aligned} & \{\text{coefft. of } x^2 \text{ in } (x + x^2 + x^3 + x^4)^6\} \cdot \{\text{coefft. of } x^4 \text{ in } (x + x^2 + x^3 + x^4)^6\} \\ = & \{\text{coefft. of } x^6 \text{ in } \frac{1}{(1-x)^6} - \frac{6x^2}{(1-x)^6}\} \cdot \{\text{coefft. of } x^5 \text{ in } \frac{1}{(1-x)^6} - \frac{6x^2}{(1-x)^6}\} \end{aligned}$$

To find the number of legal wheels this must be multiplied by 2, to allow for 11 crosses and 12 dots; divided by 6 because the first block of crosses may be any one of six; and if different settings of the same wheel

are to be distinguished, multiplied by 23.

In the following table the number of legal wheels is exact: other entries to four figures only.

Total no. of wheels.	Δ' d wheels with the correct no. of crosses.	Legal wheels.
X_1 2,193,000,000,000	271,900,000,000	23,314,226,716
X_2 21,43,000,000	304,000,000	73,241,034
X_3 535,800,000	78,320,000	14,524,128
X_4 66,990,000	19,544,000	2,869,568
X_5 8,434,000	1,364,000	556,416

From this table the factor in favour of a wheel because it is spontaneously legal can be calculated. It should be noticed that any supposed ΔX wheel corresponds to two X wheels or to none, so that e.g. a ΔX_5 , constrained to have the correct number of crosses gains a factor $\frac{2 \times 1,364,000}{556,416} = 4.4$ if it is spontaneously legal.

(R5 p 4; for factor given by integration R3 p 30.)

25Y PROPORTIONAL BULGES RELATING TO \hat{X}_2

These will all be derived using $\Delta X_6 \equiv \hat{X}_2$ (22D(g))

The following notation will be used for proportional bulges

$$\begin{aligned}
 (\dots x) &\equiv \beta & \dots x &\text{ denoted the P.B. of } 1 = ., 2 = ., 6 = x \text{ in } \Delta\Psi \\
 \{\dots x\} &\equiv \delta & \dots x &\text{ " " " " 1 = ., 2 = ., 6 = x in } \Delta D \\
 \Pi_x && &\text{ " " " " 2 = } \frac{x}{x}, & \Delta P \\
 \Pi_{..} && &\text{ " " " " 1 = ., 2 = ., } & \Delta P \\
 \Pi_{1+2} && &\text{ " " " " 1 + 2 = ., } & \Delta P \\
 \theta && &\text{ " " " " } \hat{X}_2 = .
 \end{aligned}$$

$$\begin{aligned}
 PB(\Delta Z_2 = .) &= PB(\Delta Z_2 + \Delta Z_6 = .) \\
 &= PB(\Delta\Psi'_2 + \Delta\Psi'_6 + \Delta X_2 + \Delta X_6 + \Delta P_2 + \Delta P_6 = .)
 \end{aligned}$$

$$= \text{PB}(\Delta\Psi'_{26} + \tilde{\hat{X}}_2 + \Delta P_2 = .)$$

$$= \beta\theta\Pi_x$$

$$\text{PB}(\Delta D_1 = ., \Delta D_{26} = .) = \frac{1}{2}[\{\dots\} + \{xx\}]$$

$$= \frac{1}{8} [\Pi_{..}(\dots + .xx) + \Pi_{xx}(xx. + x.x) + \Pi_{x.}(x.. + xxx) + \Pi_{.x}(.x. + ..x)]$$

$$\begin{aligned}
 &= \frac{1}{8} [\Pi_{..}(4\beta - \beta^2 - \beta^2) + \Pi_{xx}(-2\beta^2) + \Pi_{x.}(-2\beta + \beta^2 + 2\beta + \beta^2) + \Pi_{.x}(-4\beta + 2\beta^2)] \\
 &= \frac{\beta}{4} [(2 - \beta)(\Pi_{..} - \Pi_{xx}) - \beta(\Pi_{xx} - \Pi_{.x})]
 \end{aligned}$$

By changing the sign of ΔP_1

$$\begin{aligned}
 P\beta(\Delta D_1 = x, \Delta D_{26} = .) &= \frac{\beta}{4} [(2 - \beta)(\Pi_{x.} - \Pi_{xx}) - \beta(\Pi_{xx} - \Pi_{..})] \\
 \therefore P\beta(\Delta D_1 = . | \Delta D_{26} = .) &= \frac{\frac{1}{2}[P\beta(\Delta D_1 = ., \Delta D_{26} = .) - P\beta(\Delta D_1 = x, \Delta D_{26} = .)]}{P\beta(\Delta D_{26} = .)} \\
 &= \frac{\beta(1 - \beta)\Pi_{1+2}}{1 - \beta\Pi_x} \tag{Y2}
 \end{aligned}$$

Changing the sign of $\Delta P_1, \Delta P_2$

$$P\beta(\Delta D_1 = x | \Delta D_{26} = x) = \frac{\beta(1 - \beta)\Pi_{1+2}}{1 + \beta\Pi_x} \tag{Y3}$$

whence (or otherwise)

$$P\beta(\Delta D_1 + \Delta D_{26} = .) = \beta(1 - \beta)\Pi_{1+2} \tag{Y4}$$

Evidently, unless the Π_x is larger than is probable in cipher, as distinct from key, the P.Bs. of $1./2+6., 1x/2+6x$ do not differ sufficiently to justify running them separately.
