FORSVARETS CHIFFERRAD
THE CIPHER BOARD.

~~TOP SECRET~~
~~STRENGT HEMMELIG~~

Avgradert av NSM
10.11.2020 SR

Oslo, May 7th, 1952.

From: The Cipher Board, Norwegian Forces.

To: Communications Security Panel, Shape
Communications Electronics Board.

Attention: Major Grigg.

Subject: Analysis of the Hagelin machine CX.

According to your oral request to lt.cmdr. Tor Paus on March 6th, 1952, the Cipher Board has effectuated an analysis of the new Hagelin machine CX with a view to its practical utility and its aptitude to resist a breaking. The analysis is hereby included and is divided into following items:

I. Introduction.

A. On the difference between the new machines of type CX and the older of type C.
B. Definitions.

II. Fitness for use.

A. On the working stability.
B. Correction of wrong ciphered letters.
C. Correction of the wrong setting of the machine.

III. Decrypting.

A. General principles for the process of ciphering.
B. On the frequencies of ciphered letters. System-analysis.
C. First remarks on the feeding.
D. The feeding function.
E. The structure of the inner key. Cycles.
F. Statistical expressions for the length of the cycle etc.

G. Individual sub-cycles.

H. Corresponding cipher and clear text.

IV. Conclusion.

According to this analysis, the Cipher Board can state:

1. With its actual construction the machine cannot be considered as fit for practical use.

2. In order to guarantee that the machine can resist a breaking, all the outer-keys to be used must be controlled so they cannot lead to any repetition in the key-text. This control of the singular outer-key takes a very long time. Such a control is not possible practically to undertake with the actual known methods. The machine can therefore not be guaranteed as safe for breaking.

I will lastly mention that the time to our disposal was very short (about 1 1/2 month). The analysis was to be finished in due time for Paus to take it to the meeting.

Yours,

Nils Stordahl

Nils Stordahl
chairman

I. Introduction.

A. On the difference between the new machines of type CX and the older of type C.

I. There is variable feeding of the pin wheels. The feeding is determined by the number of outpicked and not outpicked slide-bars in the present machine-cycle.

There are different types of bars working in different ways as to the feeding of the wheels. Each bar is characterized by seven indications, each of which being A,B,C or O.

Ex: (A_T, O_I, O_{II}, O_{III}, B_{IV}, A_V, O_{VI})

The meaning of the first indication, the indication with respect to the type wheel, is illustrated by the following diagram:

	Not outpicked	Outpicked
A_T	No feeding	Feeding
B_T	Feeding	No Fedding
C_T	Feeding	Feeding
O_T	No feeding	No feeding

The indications with respect to the pin wheels are defined analogously.

The actual machine will be provided with bars that are all of type A with respect to the type wheel. Thus there will be no difference between the new and the older machine in this respect. Further, the actual machine will be provided with bars having only one of the six other indications different from O.

Ex: (A_I, O_I, O_{II}, O_{III}, B_{IV}, O_V, O_{VI})

Such a bar is completely characterized by the one indication different from O. The bar mentioned in the preceding example is thus completely characterized by the indication B_{IV}.

II. The slide bars can be removed and replaced by others. This will influence the feeding. Change of bars will be one part of the change of inner key.

The actual machine will be equiped with the following slide bars when delivered:

4 pieces A_i 1 piece B_i (i = I,II, -----, VI)

This machine has got 3o bars. There will be space for another two.

III. The bar lugs cannot be moved sideways from one lug-row to another, instead they can be pulled right up. Those "active" lugs will be picked out by the guide arms as before.

The actual machine will be provided with bars having one lug in each row except where there are also knots for the feeding of the pin wheels. Thus there will be 5 bars having no lugs in first row, 5 others having none in second row etc. - We notice that each bar can have 1,2,3,4 or 5 active lugs.

IV. The pin wheels can be removed and replaced by others of another length i.e. another number of pins. Change of pin wheels will be one part of the change of inner key.

The actual machine will be equiped with the following wheels.

Standard: 34(2.17), 38(2.19), 42(2.21), 46(2.23)

Extra: 29, 31, 37, 41, 43, and 47.

Pin wheels of any desired length between 25 and 5o can be fabricated.

V. The relative displacement between the primary and secondary type wheel will variate during the c~~h~~iphering of a message. This variation will be performed by a special arrangement that prevents the primary wheel from moving with the secondary wheel during the machine-cycles.

VI. The machine will not get an incoherent typewheel.

VII. The machine can be used for correspondance with the older one.

VIII. The machine will be equiped with an electrical key-board and an electrical motor.

B. Definitions.

When working with the new machine we shall need some new concepts having no relevance to the old ones.

1. The different types of slide-bars defined in the preceding chapter.
2. The "feeding key" determined by the amount of different bars. In the supplement p.1.. is shown how a feeding key can be indicated.
3. The "lug-key" determined by the amount of active lugs. In the supplement p.2. is shown how a lug-key can be indicated.
4. The total "bar-key" is determined by both the feeding key and the lug key. The concept of feeding key will evidently have no relevance to the old machine and thus respecting this machine the two latter concepts will turn out to be synonymous.
5. The pins are indicated by the numbers between 0 and l_i, l_i being the length of the pin wheel in question.
6. The numbers of steps that the secondary type wheel moves during one machine cycle is called the "saltus" performed by this cycle.
7. By the "exact saltus frequency" belonging to a certain inner key is meant the frequency function for those saltus that would occur if every one of the 64 combinations of active and inactive pins occurred once and only once.

   Provided the bars are all of type A_T, the exact saltus frequency depends on the lug key only.

   If there are also bars of type B_T for instance, this frequency will also depend on the feeding key with respect to the type wheel. The exact saltus frequency belonging to the inner key shown in the supplement can be found on p 3....
8. By the "adjusted saltus frequency" belonging to a certain inner key, is meant the frequency function for those saltus that would occur if every combination of active and inactive pins did not occur only

once, but a number of times determined by the probability of getting just this combination. As a measure of this probability is taken the product $p_1p_2 \dots p_6$ where p_i is the quotient between the number of pins having the desired polarity and the total number of pins of the wheel in question.

The adjusted saltus frequency depends also on the pin-key i.e. the amount of active and inactive pins. (A pin-key is shown in the supplement p.4.).

If there are approximately as many active as inactive pins on every wheel, the two frequencies will be nearly equal.

9. The frequency function for those saltus that occur in the cipher of some message is called the "actual saltus frequency" for this message.

The actual saltus frequency is determined by both the inner and outer key.

Later we will give an example of a special regularity in the feeding which will have as a result that some combinations of pins will be more or less frequent than would be the case if the feeding was chosen at random. This, however, is a very rare case.

If no such regularity exists, the actual saltus frequency will converge in probability to the adjusted saltus frequency.

Experience shows that in general there will be a rather rapid convergence.

10. The "exact feeding frequency" for the i-th pin wheel is defined analogously to the exact saltus frequency. The exact feeding frequencies belonging to the inner key shawn in the supplement can be found on p.6.

11. The "adjusted feeding frequency" is defined analogously to the adjusted saltus frequency.

12. The "actual feeding frequency" is defined analogously to the actua saltus frequencies.

What is mentioned on saltus frequencies also applies to th feeding frequencies as well.

13. The position W of the pin wheels at a certain time is characterized by six numbers. These numbers indicate the pins contacting just then the guide arms.

Ex.: W = (23,11,19,2,16,25)

The position of the wheels can of course also be indicated by the letters appearing on the index line. These two indications will evidently be connected by a relation of the following type:

$$x \equiv y + \text{const.} \pmod{t}$$

The total number of different wheel positions is the product of the length of the wheels. A machine equiped with standard wheels will have following number of wheel-positions:

$$N = 1\ 622\ 493\ 600 = 1,6 \cdot 10^9$$

14. With a given inner key there will to every position "W" of wheels correspond an immediate successor F(W) being the position after one machine cycle.

F(W) is called "feeding function" belonging to this inner key.

F(W) is a unique but generally not biunique transformation of the set of wheel positions into itself.

The successor of W after n cycles is called $F^n(W)$

If there exists an immediate predecessor W' of W, so that $F(W') = W$, then W' will be denoted $F^{-1}(W)$.

Analogously an eventual predecessor W' of W so that F^n (W') = W, will be denoted F^{-n} (W)

By a given inner key and a given W, F(W) can be found easily by use of the schemes

a) "Pin-key", supplement p. 4.

b) "Pins→feeding", supplement p. 5

Later we will return to the problem of finding F^{-1}(W).

II. FITNESS FOR USE.

A. On the working stability.

The new machine with its additional cog-wheels for feeding the pin wheels and its arrangement for clamping the primary type wheel while the secondary moves, has to be a more complicated machine from a mechanical point of view than the old one. As a general rule we may therefore expect that the chance of getting trouble with the mechanism will increase. We do not mean to say, however, that the construction of the new type is too complicated for the machine to wotk satisfactorily. Nevertheless, the cog wheel feeding the 4. pin on our trial machine worked in such an unstable way that we were unable to obtain more than 3 - 4 correct successive letters by the ciphering. The trial machine was therefore of very little value to us in our investigations. The given analysis had to be based on the working principles only, and the examples to be computed from the bar- and pin keys by means of the scheemes pins → saltus and pins- feeding.

Another detail that made the trial machine unfit for use was the performance of the lugs. A lug which is identical with a U-shaped spring, is active when elevated on the bar. During a cycle of the machine the guide arm is pressed against the active lug pushing it back to its lower position, and in a few cycles the lug is made in-active. This detail is of course of no great objection to the machine, as a better and safer construction of the lugs easily may be obtained.

The trial machine placed to our disposal had a fixed primary-secondary type wheel, and no informations can therefore be given as to the other performance of the type wheel.

The new machine will be equiped with an electric keyboard, the new principle for the coupling key → typed letter being an improvement as far as we can see. It will be more handy and take less space.

B. Correction of wrong ciphered letters.

The performance of the new machine makes it extremely difficult to reconstruct a previous position of the pin wheels during the ciphered process. Owing to the irregulas feeding of the pin wheels this cannot be done by a simple resetting of the pin wheels, as you do not know the number of steps the different wheels have moved during the foregoing cycle of the machine. Accordingly the correction of an erroneous letter is no easy task. The cipher-operator may avoid the difficulty by giving a signal for an erroneous letter and continue the message, but for the decipher-/operator the situation is different. If one or a few letters have come out incorrect, the meaning of the message need not be spoiled. The most frequent error, however, is perhaps to leave out a group of 5 letters, and there you are. The decipher-/operator then can choose between 3 different ways to obtain the meaning of the message:

1. Start once more from the beginning. Of course he does not need to repeat the original message. To save time he may choose a completely arbibrary text, but in any case he must make the necessary number of machine-cycles to reconstruct the previous positions of the pin wheels.
2. During the deciphering process record the position of the pin wheels at suitable intervals and when committing a mistake, repeat the deciphering from the nearest known position of the pin wheels.
3. Compute the foregoing positions of the pin wheels step by step.

The straight forward methods mentioned under point 1 and 2 take a lot of time and are therefore most unpractical. The procedure under point 3 is the following:

a. Compute the schemes Saltus → Pins and Pins → Feeding.
b. Find the saltus of the foregoing cycle and get the different possible pin combinations from the scheme Saltus → Pins. (In our example the number of alternatives is from 1 to 5).
c. Look up in the scheme Pins → Feeding the number of steps each pin wheel has to be set back. In case of ambiguity each possibility has to be tried, the right setting giving sense to the subsequent letters.
d. Instead of the trial and error method in c., the possibility is open to use the pin key, mark out the actual position of th pin wheels and see what foregoing position or positions are in conformance with the 1 to 5 possible pin-feedings found from a. and b.

It is worth noticing that this process a-b-c or a-b-d has to be repeated for each backward movement. The procedure is so complicated and takes so much time that the method hardly can be said to be any method at all, for solving the problem of correcting wrong ciphered letters.

Almost every ~~decipher~~ operator, even the experienced ones, happens to make erroneous touch during a long message. In our opinion a cipher machine is not very fit for use unless there is an easy way to reconstruct a previous position of the pin wheels during a deciphering process. Our conclusion is, that there is no such simple method for the present machine. This is therefore one of the greatest objections to the machines of type CX.

C. Correction of the wrong setting of the machine.

As every expert will know it is easy to find the error, and thus get the meaning out of a message on the old machine, if the error is due to an incorrect relative displacement, wrong set pins, wrong placed lugs or false starting position of the pin wheels, presupposed that not too many mistakes have been made simultanesously.

On the new machine the correction for a false relative displacement can be done in the same way as before, simply by trying the other 25 possibilities.

A single wrong set pin will alter the succeding text totally from the point where the pin functioned for the first time. If it is possible to determine the false letter, the right polarity of the pin can be found by trial and error. Changing the polarity of the 6 working pins, one at a time, the correct setting will give the desired text.

Errors in the bar setting, whatsoever they are, will distort the message from the beginning, and we have found no means of handling this case.

A wrong starting position of the pin wheels will obviously alter the text completely, and the only way in which to get the message out is to try the different combinations, hoping that a nearby position of the pin wheels is the right one.

From the above discussion it should be clear that even a single wrong setting may give a text with no resemblance to the correct one, and with no method to reconstruct the right setting apart from a completely arbitrary guessing. To all probability this would lead to a series of repetitions, delaying the traffic, and in case the repeated message is somewhat different from the original one, leading to parallel messages if sent with the same key, and thus be a danger to the security.

III. Dec~~k~~rypting.

A. General principles for the process of ciphering.

In the following chapters considerations of purely mathematical nature will be marked with a star (+) so that those readers who are less interested in these theoretical aspects may turn directly to the conclusions. These theoretical deductions, however, are likely to be those of the greatest interest to the expert.

In the following $\equiv$ (mod 26) is denoted only by $\equiv$.

We know the fundamental congruence for the old machine:

$$\boxed{C_n + K_n \equiv R + S_n}$$

C_n being n-th letter of ciphered text

K_n " " " " clear text

R " the fixed relative displacement between the two typewheels.

S_n being the n-th saltus.

The new patent of variable relative displacement will induce changement in this congrunce. The fundemental congrunce for the new machine will be:

$$\boxed{C_n + K_n \equiv \sum_{i=0}^{n} S_i}$$

S_o being the relative displacement at start.

(+) B. On the frequencies of ciphered letters. System-Analysis.

We know that the expected frequency of the ciphered letters was expressed by following formulas:

$$\underline{q_i = \sum_{i=0}^{25} s_{i-j}\, k_{r-j}} \qquad (i = 0,1,2 \dots 25)$$

k_i being the frequency of the letters of clear text.

s_i " the adjusted saltus frequency, which is supposed to be nearly equal to the actual frequency.

q_i being the frequency of the ciphered letters.

r " the relative displacement.

By using matrix notation we can write:

$$\underline{Q = S\ K}$$

Q being the column matrix with elements $a_i = q_i$

S " skew-cyclic square matrix with elements $a_{ij} = s_{i-j}$

K " the column matrix with elements $a_i = k_{r-j}$

For the new machine we will get the same formula for the expectation of the first ciphered letter.

For the next ciphered letter we obtain

$$\underline{q_i = \sum_{j,k=0}^{25} s_{i-j}\, s_{j-k}\, k_{r-k}}$$

r being the relative displacement at start.

By using matrix notation we can write

$$\underline{Q = S^2 K}$$

Analogously we obtain for the n-th letter

$$\underline{Q = S^n K}$$

Provided the greatest common divisor of those $s_i \neq 0$, is not itself a proper divisor of 26, <u>then the matrix S^n will converge to the matrix having all it's elements equal to 1/26</u>. Generally this condition is fulfilled. In fact the keys ought to be made so as to fulfill this condition. With those values of s_i that will be actual, the matrix will even converge very rapidly. Thus already for small values of n we can write:

$$\underline{q_i = 1/26} \qquad (+)$$

<u>Conclusion</u>:

<u>It will be theoretically impossible by means of the frequencies of the ciphered letters to separate chryptograms from series of random letters</u>.

<u>It will also be impossible by means of the frequencies of the ciphered letters to decide whether a chryptogram is ciphered by a certain inner key or not</u>.

This advantage obtained by variable relative displacement, is, however, accompanied by the following inconvenience: If we know the corresponding cipher and clear text, we get

$$\underline{(C_n + K_n) - (C_{n-1} + K_{n-1}) \equiv S_n}$$

<u>Thus we get the series of saltus directly</u>.

With an old machine the analogous expression would contain an unknown additiv constant, the fixed relative displacement. Determination of this constant will be a matter of routine, when working with a machine with regular feeding. When working with a machine with variable feeding this unknown constant will entail the first great difficulty. To have the remaining work increased 26 times is not unimportant at this early stage of the dechrypting.

We shall later return to the ~~dechrypting~~ decrypting of corresponding cipher and clear text.

C. First remarks on the feeding.

We know that the frequency of those letters ciphered with the same pin on a certain wheel, will have certain peculiarities.

But it is easily seen that these peculiarities will be of no use in the breaking of the new machine. In fact, we do not know these peculiarities, as we do not know where the mentioned letters appear in the text.

6+) Let us consider one wheel starting at 0. After first cycle the probability-density for the position of this wheel is expressed by:

$$\underline{p_i^{(1)} = f_i}$$

f_i being the adjusted feeding frequency which is supposed to be nearly equal to the actual feeding frequency.

The corresponding expression for the next position will be:

$$\underline{p_i(2) = \sum_{j=0}^{l} f_{i-j}\, f_j}$$

l being the length of the wheel in question.

Or, by using matrix notation, we get:

$$\underline{P = G\,F}$$

P being the column matrix with elements $a_i = p_i$

G " the skew-cyclic, square matrix with elements $a_{ij} = f_{i-j}$

F " the column matrix with elements $a_i = f_i$

For the next position we get

$$\underline{p_i^{(3)} = \sum_{j,k=0}^{l} f_{i-j}\, f_{j-k}\, f_k}$$

Or, in matrix notation:

$$\underline{P = G^2\,F}$$

In general the probability density for the n-th position will be expressed by:

$$\underline{P = G^{n-1}F}$$

Provided the greatest common divisor of those f_i, being $\neq 0$ is not itself a proper divisor of l (the wheel length), then the matrix G^n will converge to the matrix whose elements are all equal to 1/l. If $f_i=0$, for $i>5$ for instance, i.e. the possible number of steps are only 0, 1, 2, .. 5, then G^n will not converge as rapidly as the corresponding matrix of the saltus frequency. In general it is necessary that n ranges between 10 and 20 in order to get a suitable approximation.

Then we can write:

$$\underline{p_i^{(n)} = 1/26}$$

Provided conversely that the greatest common divisor (d) of those $f_i \neq 0$ is in fact a proper divisor of l, then the matrix G^n will converge to a matrix whose elements are:

$$a_{ij} = \begin{cases} 0 & \text{if } i-j \not\equiv 0 \pmod{d} \\ d/l & \text{if } i-j \equiv 0 \pmod{d} \end{cases}$$

Thus for bigger n, ($n>20$) we can write:

$$p_i^{(n)} = \begin{cases} 0 & \text{if } i \not\equiv 0 \pmod{d} \\ d/l & \text{if } i \equiv 0 \pmod{d} \end{cases} \qquad (+)$$

<u>Conclusion:</u>

<u>If the greatest common divisor of the possible feeding steps of a certain wheel is not itself a proper divisor of the wheel length, then, after about 10 or 20 machine-cycles, any position will be almost equally probable.</u>

<u>If the greatest common divisor (d), however, really is a proper divisor of the wheel length, then only every d-th position can be possible, but after about 10 or 20 machine-cycles each of these positions will be equally probable.</u>

This latter case will be rare. And in fact the keys ought to be made so as to prevent this. Occurrence of this phenomenon implies that only one d-th of the pins of the wheel in question is really used.

This phenomenon can imply that the real probability of getting a certain combination of pins can not be expressed in the way we did in the introduction.

Thus we have seen an example of a regularity in the feeding, that makes some combinations of pins more or less frequent than they would be if the feeding was chosen at random. We have given the example mentioned on page 5 in the introduction. In this case the actual frequencies will not converge in probability to the adjusted ones. This implies that we cannot use the adjusted frequencies as approximations to the actual ones, in the way we have done in the preceeding deductions. But by replacing the adjusted frequencies by the actual ones, we will get matrices of the same kind, and all what is said on their convergence will remain true.

D. The Feeding function.

We have seen how we can find the successor of a certain wheel position by means of the schemes Pin key page 4, Pins → Feeding page 5 in the supplement. It is also possible to find an eventual predecessor. We have then to read through the scheme Pins → Feeding in search of a combination of pins and feeding that are in accordance with the pin key.

This procedure may give one, two, three etc. solutions or perhaps none at all.

(+) We make the following idealisations. We imagine that any wheel position be equally probable as successor of W.

Then the expected number of wheel positions having exactly i immediate predecessors is expressed by:

$$E_{i,N} = \binom{N}{i}\left(\frac{1}{N}\right)^{i}\left(1 - \frac{1}{N}\right)^{N-i}$$

As N is very big in comparison to i, we can write

$$E_{i,N} = \lim_{N \to \infty} E_{i,N} = \frac{1}{i!e}$$

We have performed the following experiment: 60 wheel positions were chosen at random. The number of these having 0, 1, 2, 3, ... predecessors is given in the following table together with the expected numbers.

Number of predecessors	Counted	Expected
0	21	22
1	23	22
2	15	11
3	1	4
4	0	1
Rest.	0	0
Sum	60	60

We stress that these statistics of course are too restricted to prove anything at all. But it shows the tendency.

When beginning the ciphering one can chose any wheel position, but only those positions having an immediate predecessor can serve as second position, and only those implying the existence of $F^{-n}(w)$, can serve as n-th position. Let N_n denote the number of positions implying the excistence of $F^{-n}(w)$. Then the sequence:

$$N, N_1, N_2, N_3, \ldots .$$

will be never increasing.

Specially we get:

$$\underline{(1 - 1/e)N \approx N_1}$$

It is, however, not easy to obtain further relations of the same kind. We do not get:

$$\underline{(1 - 1/e)N_n \approx N_{n+1}}$$

because of the fact that the set of wheel positions implying the existence of $F^{-n}(w)$ is not a random sample of the whole set.

A question of some interest is: What will happen to N_n when n tends to infinity. This problem will be solved later. (+)

E. The structure of inner keys. Cycles.

We are now going to consider problems of the greatest interest. What about periodicity ? What about chains having common terms ? To answer these questions we have to make a slightly deeper analysis of what we may call the structure of an inner key.

(+) We know that F(w) is a unique, but not biunique transformation of the set, W, of all wheel positions into itself.

Definition:

A proper subset M of W is said to reduce W if both M and M' (the complement to M) are closed under F(w).

Obviously $F^n(w)$ is closed too, so that if w belongs to M, then the whole chain $F^n(w)$ will also belong to M.

Theorem:

If M and N are both reducing subsets, so are their join, meet and difference, provided these are in fact proper subsets.

The proofs are all evident.

Definition:

If M is a reducing set, containing itself no reducing set, then M is called a resolvent.

The partition theorem:

If W contains a reducing set, then W can be uniquely partitioned into a disjoint class of subsets each of which being a resolvent.

Proof:

1. The possibility of a sub-dividing into resolvents, is easily proved by complete induction from the preceeding results.
2. Two different resolvents are always disjoint, otherwise their meet would be a reducing set (cfr. the theorem above).
3. If R_1 and R_2 be two resolvents belonging to two different subdivitions, then they are either equal or disjoint. This proves the uniqueness.

By a successive performance of the terms of the chain $F^n(w)$, we must sooner or later get a repetition. This implies entrance into a cycle from which we can never escape. The fact that $F^{-1}(w)$ is not unique, implies that many chains may enter the same cycle.

Theorem:

Each resolvent will contain one and only one cycle.

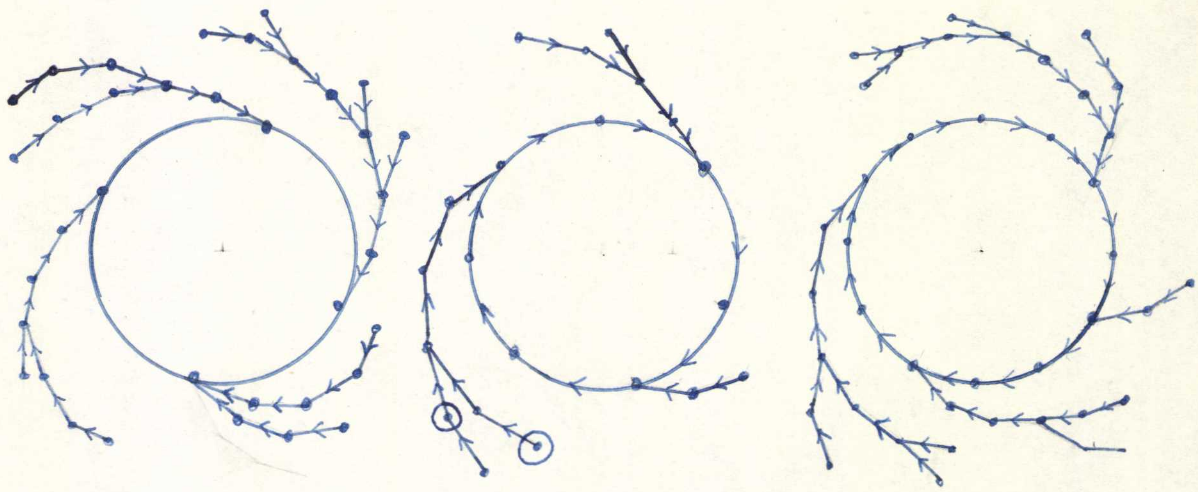
Proof:

1. The considerations above shows that it will contain at least one cycle.
2. The set of elements w, whose chains $F^n(w)$ lead to the same cycle, will obviously be a reducing set. Ex~~c~~istence of more than one cycle therefore implies the ex~~c~~istence of reducing sets in the resolvent. This contradiction establishes the theorem. (+)

Conclusion:

We consider a certain inner key with a certain feeding function.

Then the whole set of wheel positions can be mapped as follows:



Here, each wheel position is denoted by a dot, and the arrows lead from each position to it's immediate successor.

This structure implies two very dangerous possibilities:

1. The cycles may be shorter than the length of an actual message.
2. Two outer keys may lead to chains having some terms in common, like the two wheel positions marked at the figure.

We see that outer keys from the central parts of the resolvents are particularly dangerous.

In both of these cases the messages can be decrypted.

By an increasing amount of messages, the chance of getting chains with common terms, will increase very rapidly. This will represent a real danger.

That it is also possible to get short cycles, is shown in the example on page 9, 10 and 11 in the supplement.

We succeeded in constructing a pin key, which together with the same bar key being used in the other examples, gave as a result an inner key possessing two short cycles. Each of these cycles contained only 9 elements.

A mapping of these two small resolvents is shown on page 10 and 11 in the supplement.

Without any difficulty we have succeeded in constructing short cycles with different types of bar keys.

If a machine of type CX shall be employed it will be necessary to control before hand, all the outer keys to be used. If not, there is a risk to get parallel or partly parallel messages, or worse, messages sent with a periodic series of saltus.

In a machine with regular feeding it is very easy to ascertain that there is no parallelity, and with respect to this machine the question of obtaining periodicity within one single message will not be actual.

With the new machine the situation is entirely quite different. As a matter of fact, the only known method to control the outer keys, is to cipher with every one of them the letter A as many times as there are letters in a part, then control all the obtained parts as for parallelity in every relative position and as for periodicity. To be stressed, that for a machine whose feeding is determined by the inner key this operation can not be done once for all, but has to be done over again for every change of the inner key.

Such a control of the outer keys will be extremely troublesome. This will be one of the greatest objections to the new machine, as long as no better method for control is found.

F. Statistical expressions for the lengths of the cycle etc.

In order to find statistical expressions for the lengths of the cycles etc., it is necessary to simplify the problem in the same way as done before, supposing that any wheel position is an equally probable value for $F(w)$. It can only be found out by experiments to which extent results obtained in this way, really give an adequate description of the machine.

Such an experiment can be performed as follows: Remove the lock-pawl that prevents the drum from moving more than one cycle at the time. The machine will then work automatically by the electric motor. Having no machine working satisfactorily it has not been possible to perform this operation.

(+) A set containing n wheel positions will be a cycle if and only if it's elements can be ordered in a sequence, so that:

$$w_{i+1} = F(w_i) \qquad i = 0, 1, 2, \ldots, n-1$$

$$w_o = F(w_n)$$

The number of subsets containing n elements is expressed by:

$$\binom{N}{n}$$

The total number of all transformations of a subset of n elements is N^n.

The number of transformations organizing the set to a cycle is $(n - 1)!$

Proof: A cycle is uniquely characterized as a class of orderings that can be transferred into each other by cyclic permutations. Each such class corresponds uniquely to a certain transformation. The number of classes): of desired transformations, are obviously $(n - 1)!$ q.e.d.

The probability that a subset containing n elements is a cycle, are then:

$$\frac{(n-1)!}{N^n}$$

For the expected number of cycles of length n, the expression will be:

$$\binom{N}{n} \frac{(n-1)!}{N^n}$$

The distribution function for the length of cycles is then given by:

$$C(n) = \sum_{i=1}^{n} \binom{N}{i} \frac{(i-1)!}{N^i}$$

Further mathematical computation gives for small n the following approximation:

$C(n) \approx \ln n +$ Euler's constant

The following inequality is always valid:

$C(n) < \ln n +$ Euler's constant

This proves that the probability density of the length of cycles is greatest for small n and will decrease as n increases.

For very small n, i.e. $n < 20$ for instant, the results obtained by the previously done simplification can not be expected to be valid, as every wheel must have rotated at least once before there can be any repetition.

The mean length of cycles is expressed by

$$M = \frac{1}{C(N)} \cdot \sum_{i=1}^{N} \binom{N}{n} \frac{n!}{N^n}$$

Further mathematical deductions give as result:

$$M = \Theta\sqrt{\frac{\pi}{2}}\,\frac{\sqrt{N}}{\ln N} \qquad 1 < \Theta < 2$$

In numbers:

$$2500 < M < 5000$$

The mean length of cycles will range somewhere between 2500 and 5000.

The total number of resolvents is expressed by:

$$C(N) = \sum_{i=1}^{N} \binom{N}{n} \frac{(n-1)!}{N^n}$$

Further mathematical deductions show that:

$$C\,(N) = \Theta^{-1} \ln N \qquad 1 < \Theta < 2$$

In numbers

$$10 < C(N) < 20$$

The expected number of resolvents will range somewhere between 10 and 20.

We are now able to give the answer to another question, asked on page 16. What about $\lim_{n \to \infty} N_n$?

$$\lim_{n \to \infty} N_n = N_N = \sum_{i=1}^{N} \binom{N}{n} \frac{n!}{N^n}$$

From the preceeding results the following deduction can be made:

$$N_N = \Theta_1 \sqrt{\frac{\pi}{2}}\,\frac{\sqrt{N}}{\ln N} \cdot \Theta_2^{-1} \ln N$$

Hence:

$$N_N = \Theta_3 \sqrt{\frac{\pi}{2}}\sqrt{N} \qquad 1/2 < \Theta_3 < 2$$

In numbers:

$$20000 < N_N < 80000 \qquad (+)$$

To be stressed again, that these results are obtained by means of the above mentioned simplifications. We do not, believe, however, that the order of magnitude of the obtained results would be essentially changed by taking in consideration the rather complicated way in which the feeding function is really defined. But we repeat, that only experiments can prove this.

G. Individual sub-cycles.

One may ask if there will appear any periodicity in the movement of one single wheel or a set of wheels, in a similar way to the old machine. A tempting solution is the following.

Provided the first wheel is commended by the second and the third, there will be a repetition of the position of the second and the third wheel, before $l_1 \cdot l_2$ machine-cycles have been made.

In this point we could believe there is a beginning periodicity. But this is erroneous. The second and third wheel will in their turn be commended by other wheels e.g. the fifth and the sixth. The latter wheels will very likely be in new positions when the repetition appears.

The necessary and sufficient condition for getting individual sub-cycles for one wheel or a set of wheels, is that there exists a closed subset of the wheels. The meaning of the word closed in this connection is that the wheels in the mentioned subset mutually commend their feeding.

The length of such a subcycle will be a divisor of the length of a cycle for the whole machine. In general all the statistical expression previously deduced will apply to these subcycles if N is replaced by the product of those wheels constituting this closed subset. The existence of such subcycles will however be rare, and what is important: The keys can be easily made so that the subcycles can not appear. The individual subcycles will therefore not endanger the security of the machines of type CX.

H. Corresponding cipher and clear text.

The preceeding chapters shows that in some cases messages ciphered with a machine of type CX can be decrypted. The next step in the breaking of the machine, will be to reconstruct the pin- and lug-setting.

We may at once notice that the variation of the relative displacements between the primary and secondary type wheel during the ciphering process, causing the summation mark in the equation for the new machine:

$$C_n + K_n = \sum_{i=0}^{n} S_i$$

make it easy to determine the saltus. We have:

$$S_n = (C_n - C_{n-1}) + (K_n - K_{n-1})$$

The equation for the old machine contained a constant which had to be determined.

The method used for the old machine is based on the fixed periods of the 6 pin wheels. If for instance the length of one wheel is 25, letters in intervals of 25 will be ciphered with the same pin in action with respect to the wheel in question. Obviously the same thing does not happen with the new machine. Due to the irregular feeding of the pin wheels the period of a wheel is not determined only by length of the wheel, but also by the periods of the wheels that control the feeding. The periods of the pin wheels will therefore depend on the whole setting of the machine in a complicated way, and nothing can be said about the length of these periods in advance except that they probably are equal to the period of the whole machine. The method mentioned above for breaking the machine when the cipher and corresponding clear text are known, can therefore not be used for the CX type.

Any method for breaking the machine must therefore be based on other and real regularities in the machine. Though we have not succeeded in finding a complete method, the deductions below may be of interest.

First some words about the actual saltus frequency. In a long message we may expect each pin combination to occur in accordance with the probability for that combination, and the longer the message, the better the concordance. That means that the actual saltus frequency converges in probability to the adjusted saltus frequency. This reasoning can be applied to the new machine as well as the old one. Perhaps we may get a faster convergence in case of the new machine, due to the irregular feeding of the pin wheels.

We did the following experiment. The letter A was ciphered 3840 times, and in supplements 13 to 18 the actual saltus frequencies are given after 640, 1280, 1920, 2560, 3200 and 3840 cycles respectively. In the same figures the values of the adjusted saltus frequency are also indicated. The result is interesting. After 640 cycles the number of discrepancies are 12 but already in the next figure this amount is reduced to 3. After 3200 cycles 1 differ from its expected value, and after 3840 cycles the conformity is complete. The chance of getting the adjusted saltus frequency from the actual saltus frequency is therefore great if the message is not too short. If then the number of active and inactive pins is about the same, the adjusted and exact saltus frequencies will be identical. As a matter of fact this was the case in our setting.

From the exact saltus frequency it will be possible to reconstruct the lug key. Theoretically this can be done if the different lug keys with corresponding exact saltus frequencies are given in a tabular form. If conveniently arranged, the lug key could at once be found from such a table, which however would be inconvenient to handle because of its immensity. But even a "reduced" catalogue would be of great help. The lug setting and the corresponding saltus frequencies could for instance be computed once for all for the 3 first rows. Such a table would reduce the amount of labour in finding the lug key in an actual case.

The considerations above show that it is possible to determine the lug key from the exact saltus frequency and <u>such determinations have been done</u>. Experience shows that the solutions almost always are unique, and if the exact saltus frequency are not correctly determined, we usually get no solutions at all. The existence of a solution may therefore serve as a control of the determination of the exact saltus frequency.

The next step would be to find the feeding key. This problem we have not been able to solve so far, nor have we been able to find the pin settings if the total bar key is known.

A way of tackling the last problem may however be as indicated in the example below. The letter A is ciphered 14 times, the starting position of the pin wheels being (2,2,2,2,2,2).

Saltus	23	24	24	6	19	10	1	2	20	18	23	19	1	14
Number of feedings	3	4	4	1	3	2	2	2	3	2	3	3	2	3

In the first line the saltus are given and in the next the number of possible feedings of the pin wheels corresponding to the saltus in the line above (supplements 7 and 5). If the relations saltus → feeding had been unique, the polarity of the different pins on a wheel could be found directly. But as the number of saltus and pin combinations are 26 and 64 respectively, each saltus will give 64/26 feedings on an average. Even though such an ambiguity exists, there will still be some unique relations saltus → pins as shown in supplement 8. The setting of the pins could be determined if the right "chain of feedings" could be found, and the problem is again one of trial and error. One possible chain of feedings would give as many pin determinations as there are steps in the chain, and after one turn of a wheel the positions begin to overlap. This will be a control for the chosen chain, and by utilizing the 6 pin wheels, the wrong chains will probably be excluded a few cycles after the overlapping has started.

In our setting of the machine the weightened means of the feeding frequencies of the 6 pin wheels can be found from the feeding frequencies on page 6 in the supplement. They are 2,5, 3,3, 3,0, 2,5, 2,5 and 3,0 respectively. That means that the first wheel has made one turn after 11,6 cycles on an average, the second after 9,5 cycles, the third after 11,0, the fifth after 13,6 and the sixth after 12,3 cycles. After about 13 cycles we may expect the 6 pin wheels to have moved more than the length of the wheel and the overlapping to have started. But even 13 cycles will give $(64/26)^{13}$ = 121 800 possible chains of feedings on an average which have to be tried, causing a great amount of work. By help of the modern computing machines the labour involved in such an investigation is not insurmountable, though we have not carried out any complete reconstruction of the pins. Evidently the labour will increase with the length of the wheels.

IV. CONCLUSION.

The conclusion of the preceeding examination will be as follows:

1. The machine can hardly be used in the field. In our opinion the construction is too complicated. Second, there is no simple method to correct erroneous letters if the operator has committed a mistake during the ciphering process. Any wrong set lug or couple of wrong set pins will further completely change the message and will make it almost impossible to find the mistake. This will no doubt lead to repetitions which will delay the traffic and endanger the security.

2. In principle it is impossible by means of the frequencies of the ciphered letters to separate cryptograms from series of random letters. It is also impossible by means of the frequencies of the ciphered letters to decide whether a cryptogram is ciphered by a certain inner key or not. These two properties are caused by the new patent of the variable relative displacement.

3. It is known that the frequency of the letters ciphered with the same pin on a certain wheel, will have certain peculiarities. But it is obvious that these peculiarities are of no use in the breaking of the new machine. In fact these peculiarities are unknown, as it is not known where the mentioned letters appear in the text.

   If the greatest common divisor of the possible feeding-steps of a certain wheel is not itself a proper divisor of the wheel length, any position is almost equally probable after about 10 or 20 machine cycles.

   If the greatest common divisor (d), however, really is a proper divisor of the wheel length, then only every d-th position can be possible.

   The keys should be made so as to prevent this latter case.

4. The structure of an inner key is illustrated by the drawing on page 18 . This structure implies two very dangerous possibilities:

   1. The outer keys may lead to chains having common terms.

2. The cycles may be shorter than the length of an actual message.

By an increasing amount of messages, the chance of getting chains with common terms will increase very rapidly. This represents a real danger.

It is also possible to get short cycles. This is illustrated by the examples of short cycles shown on page 10 and 11 in the supplement. Both of these cycles are of length 9.

If the cases 1 or 2 do occur, the messages can be decrypted.

In order to prevent this, all the outer keys to be used should be controlled beforehand. With a machine having regular feeding, this control is easy to perform. With a machine having irregular feeding the situation is entirely different. As a matter of fact the only known method to control outer keys is to cipher with every one of them the letter A as many times as there are letters in a part, and then control all the obtained parts as for parallelity in every relative position, and as for periodicity.

It is to be stressed, that this control has to be done over again for every change of the inner key.

Such a control of the outer keys will be extremely troublesome.

There are thus two possibilities:

1. Control all the outer keys by means of this method.
2. Do not effectuate the control, hoping that these cases will not occur.

None of these two solutions are recommendable.

The statistical expressions on page 21 may give an indication of how much the security is endangered if the control is not effectuated.

5. We have not been able to give any complete method for breaking the machine if the cipher and corresponding clear text are known, but in our opinion it is not impossible that such a method can be found. In any case the lug key can be determined if the message is not too short, and it is also possible, at least theoretically, to reconstruct the pin key if the total bar key is given. It should, however, be

emphasized that even if two parallel messages should lead to reconstruction of bar and pin keys, messages sent on the same inner keys, but with another starting position of the pin wheels, can not be decrypted. The decrypting of single messages ciphered with the new machine will not imply continously reading of the whole correspondance. This is the greatest improvement obtained by the new construction.

- - - - - - - - - -

As far as security is concerned, the construction of the new machine eliminates certain weaknesses with the old machine, but presents some other vulnerable aspects.

- - - - - - - - - -

~~STRENGT HEMMELIG~~

~~TOP SECRET~~

Feeding Key.

I	II	III	IV	V	VI	
					B	30
					A	29
					A	28
					A	27
					A	26
				B		25
				A		24
				A		23
				A		22
				A		21
			B			20
			A			19
			A			18
			A			17
			A			16
		B				15
		A				14
		A				13
		A				12
		A				11
	B					10
	A					9
	A					8
	A					7
	A					6
B						5
A						4
A						3
A						2
A						1

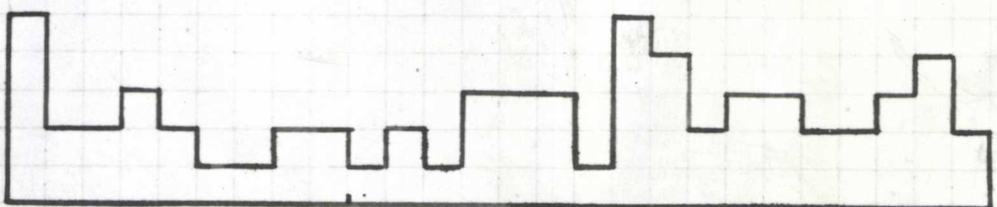
Lug key.

I	II	III	IV	V	VI	
						30
	X					29
	X					28
	X					27
	X					26
X						25
X						24
X						23
	X				X	22
	X				X	21
	X			X		20
		X		X		19
X	X					18
X	X					17
X	X					16
X						15
X						14
X						13
X						12
X						11
				X		10
				X		9
			X			8
X						7
X						6
			X		X	5
		X	X			4
					X	3
					X	2
					X	1

Bar key.

I	II	III	IV	V	VI	
					B	30
	X				A	29
	X				A	28
	X				A	27
	X				A	26
X				B		25
X				A		24
X				A		23
	X			A	X	22
	X			A	X	21
	X		B	X		20
		X	A	X		19
X	X		A			18
X	X		A			17
X	X		A			16
X		B				15
X		A				14
X		A				13
X		A				12
X		A				11
	B			X		10
	A			X		9
	A		X			8
X	A					7
X	A					6
B			X		X	5
A		X	X			4
A					X	3
A					X	2
A					X	1

Exact saltus frequency.



5	2	2	3	2	1	1	2	2	1	2	1	3	3	3	1	5	4	2	3	3	2	2	3	4	2
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

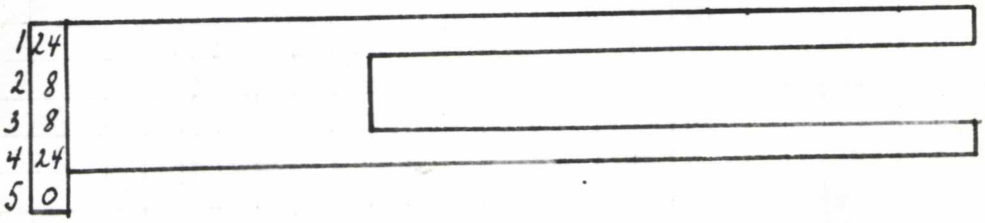
Pin key.

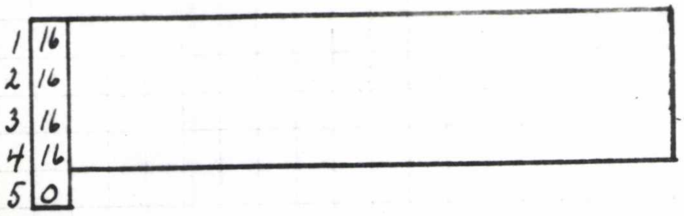
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
I			+	+	+		+	+			+			+	+			+	+		+	+				+	+		+								
II	+		+				+	+	+	+			+	+		+		+			+		+	+			+		+		+						
III		+				+	+		+	+	+		+				+	+		+		+	+	+					+	+		+	+				
IV	+				+	+		+	+			+	+			+	+	+			+	+	+	+				+		+		+					
V	+		+	+		+	+	+			+	+	+					+	+				+			+	+	+		+	+						
VI	+	+					+	+		+		+		+	+		+				+			+	+		+		+	+		+	+	+		+	

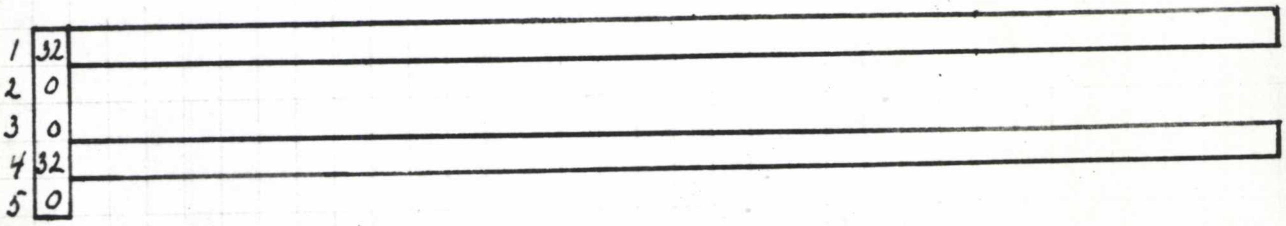
Pins → Feeding.

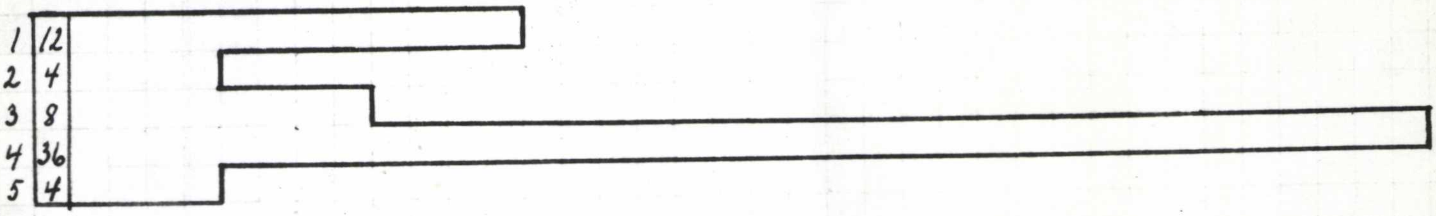
0	0	-	-	-	-	-	-
		1	1	1	1	1	1
1	6	-	-	-	-	-	+
		3	1	1	1	3	1
2	4	-	-	-	-	+	-
		1	1	1	1	1	1
3	10	-	-	-	-	+	+
		3	1	1	1	3	1
4	3	-	-	-	+	-	-
		1	2	1	1	1	1
5	8	-	-	-	+	-	+
		4	2	1	1	3	1
6	7	-	-	-	+	+	-
		1	2	1	1	1	1
7	12	-	-	-	+	+	+
		4	2	1	1	3	1
8	2	-	-	+	-	-	-
		2	1	1	2	1	1
9	8	-	-	+	-	-	+
		4	1	1	2	3	1
10	5	-	-	+	-	+	-
		2	1	1	1	1	1
11	11	-	-	+	-	+	+
		4	1	1	1	3	1
12	4	-	-	+	+	-	-
		1	2	1	2	1	1
13	9	-	-	+	+	-	+
		4	2	1	2	3	1
14	7	-	-	+	+	+	-
		1	2	1	1	1	1
15	12	-	-	+	+	+	+
		4	2	1	1	3	1
16	10	-	+	-	-	-	-
		1	1	1	3	3	5
17	14	-	+	-	-	-	+
		3	1	1	3	3	5
18	13	-	+	-	-	+	-
		1	1	1	4	3	5
19	17	-	+	-	-	+	+
		3	1	1	4	3	5
20	13	-	+	-	+	-	-
		1	2	1	3	3	5
21	16	-	+	-	+	-	+
		4	2	1	3	3	5
22	16	-	+	-	+	+	-
		1	2	1	4	3	5
23	19	-	+	-	+	+	+
		4	2	1	4	3	5
24	12	-	+	+	-	-	-
		2	1	1	4	3	5
25	16	-	+	+	-	-	+
		4	1	1	4	3	5
26	14	-	+	+	-	+	-
		2	1	1	4	3	5
27	18	-	+	+	-	+	+
		4	1	1	4	3	5
28	14	-	+	+	+	-	-
		1	2	1	4	3	5
29	17	-	+	+	+	-	+
		4	2	1	4	3	5
30	16	-	+	+	+	+	-
		1	2	1	4	3	5
31	19	-	+	+	+	+	+
		4	2	1	4	3	5
32	13	+	-	-	-	-	-
		1	3	4	4	2	1
33	19	+	-	-	-	-	+
		3	3	4	4	4	1
34	17	+	-	-	-	+	-
		1	3	4	4	2	1
35	23	+	-	-	-	+	+
		3	3	4	4	4	1
36	16	+	-	-	+	-	-
		1	4	4	4	2	1
37	21	+	-	-	+	-	+
		4	4	4	4	4	1
38	20	+	-	-	+	+	-
		1	4	4	4	2	1
39	25	+	-	-	+	+	+
		4	4	4	4	4	1
40	15	+	-	+	-	-	-
		2	3	4	5	2	1
41	21	+	-	+	-	-	+
		4	3	4	5	4	1
42	18	+	-	+	-	+	-
		2	3	4	4	2	1
43	24	+	-	+	-	+	+
		4	3	4	4	4	1
44	17	+	-	+	+	-	-
		1	4	4	5	2	1
45	22	+	-	+	+	-	+
		4	4	4	5	4	1
46	20	+	-	+	+	+	-
		1	4	4	4	2	1
47	25	+	-	+	+	+	+
		4	4	4	4	4	1
48	20	+	+	-	-	-	-
		1	3	4	3	4	5
49	24	+	+	-	-	-	+
		3	3	4	3	4	5
50	23	+	+	-	-	+	-
		1	3	4	4	4	5
51	1	+	+	-	-	+	+
		3	3	4	4	4	5
52	23	+	+	-	+	-	-
		1	4	4	3	4	5
53	0	+	+	-	+	-	+
		4	4	4	3	4	5
54	0	+	+	-	+	+	-
		1	4	4	4	4	5
55	3	+	+	-	+	+	+
		4	4	4	4	4	5
56	22	+	+	+	-	-	-
		2	3	4	4	4	5
57	0	+	+	+	-	-	+
		4	3	4	4	4	5
58	24	+	+	+	-	+	-
		2	3	4	4	4	5
59	2	+	+	+	-	+	+
		4	3	4	4	4	5
60	24	+	+	+	+	-	-
		1	4	4	4	4	5
61	1	+	+	+	+	-	+
		4	4	4	4	4	5
62	0	+	+	+	+	+	-
		1	4	4	4	4	5
63	3	+	+	+	+	+	+
		4	4	4	4	4	5

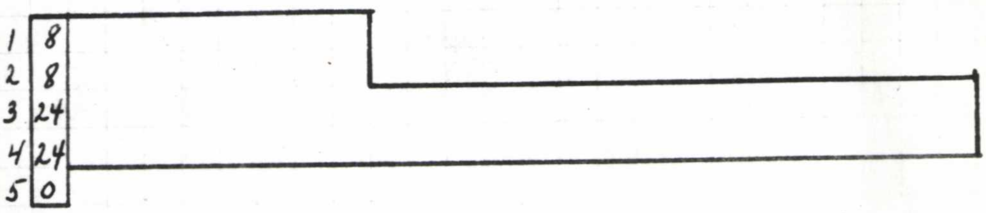
Exact feeding frequencies

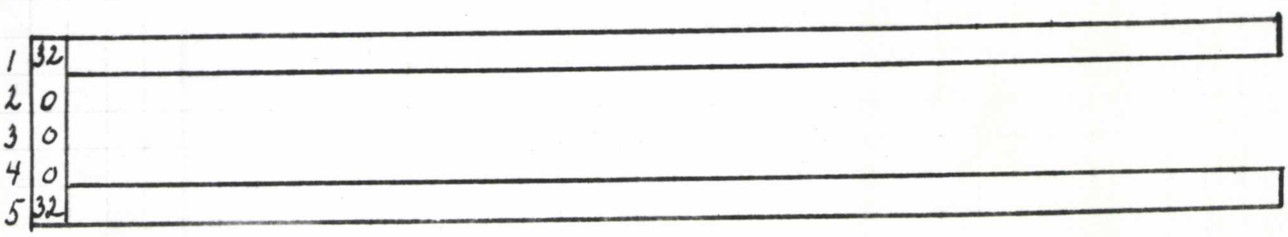












Saltus → Pins.

	Alt. 1		Alt. 2		Alt. 3		Alt. 4		Alt. 5	
0	0	- - - - - -	54	+ + - + + -	62	+ + + + + -	53	+ + - + - +	57	+ + + - - +
1	51	+ + - - + +	61	+ + + + - +						
2	8	- - + - - -	59	+ + + - + +						
3	4	- - - + - -	55	+ + - + + +	63	+ + + + + +				
4	2	- - - - + -	12	- - + + - -						
5	10	- - + - + -								
6	1	- - - - - +								
7	6	- - - + + -	14	- - + + + -						
8	5	- - - + - +	9	- - + - - +						
9	13	- - + + - +								
10	16	- + - - - -	3	- - - - + +						
11	11	- - + - + +								
12	24	- + + - - -	7	- - - + + +	15	- - + + + +				
13	32	+ - - - - -	20	- + - + - -	18	- + - - + -				
14	28	- + + + - -	26	- + + - + -	17	- + - - - +				
15	40	+ - + - - -								
16	36	+ - - + - -	22	- + - + + -	30	- + + + + -	21	- + - + - +	25	- + + - - +
17	34	+ - - - + -	44	+ - + + - -	19	- + - - + +	29	- + + + - +		
18	42	+ - + - + -	27	- + + - + +						
19	33	+ - - - - +	23	- + - + + +	31	- + + + + +				
20	38	+ - - + + -	46	+ - + + + -	48	+ + - - - -				
21	37	+ - - + - +	41	+ - + - - +						
22	56	+ + + - - -	45	+ - + + - +						
23	52	+ + - + - -	50	+ + - - + -	35	+ - - - + +				
24	60	+ + + + - -	58	+ + + - + -	43	+ - + - + +	49	+ + - - - +		
25	39	+ - - + + +	47	+ - + + + +						

Detemined Pins.

	I	II	III	IV	V	VI
0						
1	+	+				+
2			+	−		
3				+		
4	−	−				−
5	−	−	+	−	+	−
6	−	−	−	−	−	+
7	−	−		+	+	−
8	−	−			−	+
9	−	−	+	+	−	+
10	−		−	−		
11	−	−	+	−	+	−
12	−					
13			−			−
14	−	+				
15	+	−	+	−	−	−
16						
17						
18			+	−	+	
19						+
20	+					−
21	+	−			−	+
22	+		+		−	
23	+		−			
24	+					
25	+	−		+	+	+

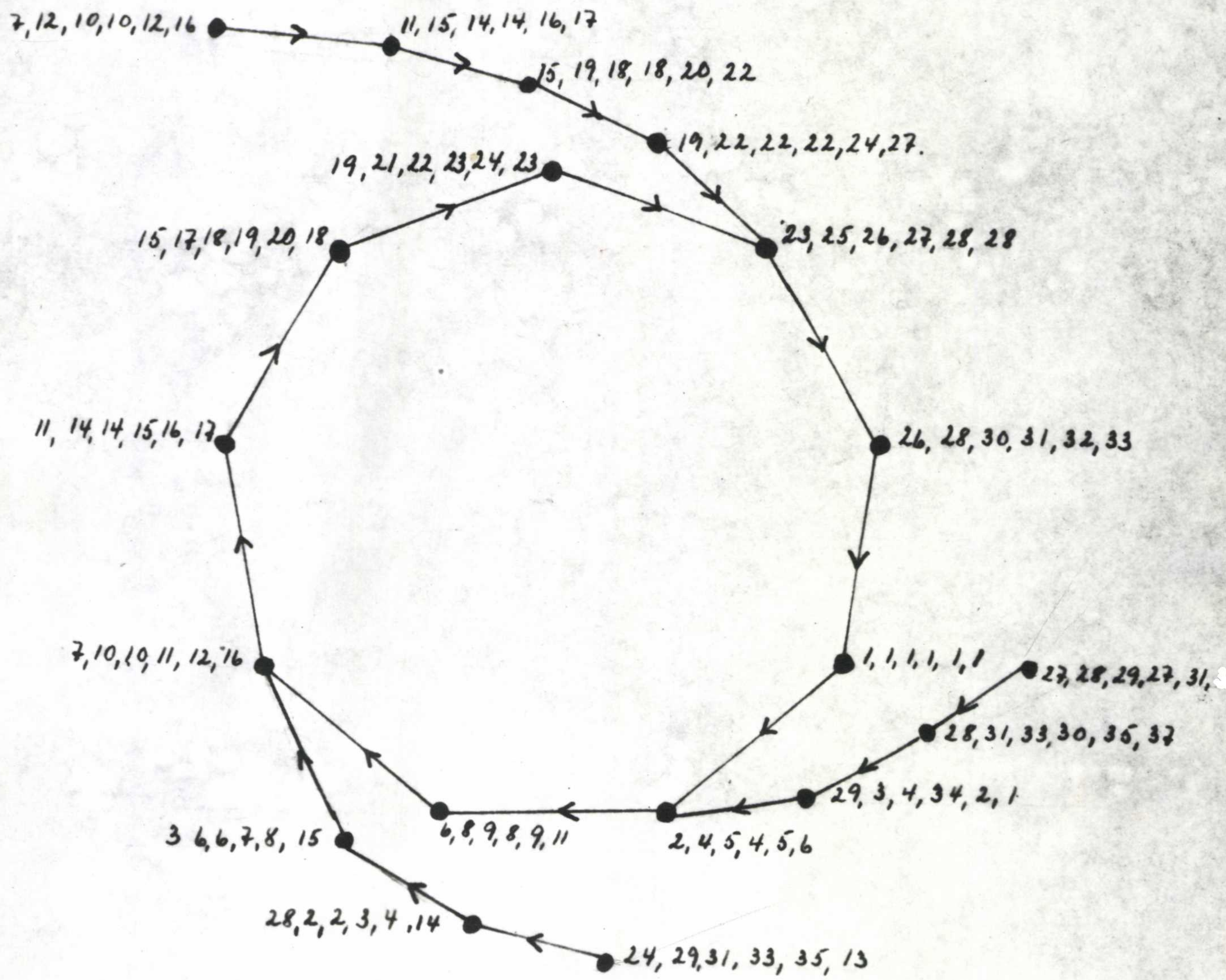
Example of small resolvents I.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
I	+	+	+	+	−	−	+	−	−	−	+	+	−	+	+	+	−	−	+
II	+	−	+	+	+	−	+	+	+	−	−	−	+	−	+	−	+	−	+
III	−	+	+	+	−	−	−	+	−	+	+	+	−	+	−	−	+	+	−
IV	−	+	+	+	−	+	+	+	−	−	+	−	+	+	−	+	+	−	+
V	−	+	−	+	+	−	−	+	−	−	−	+	+	−	+	+	+	+	−
VI	−	+	−	+	−	+	+	+	−	+	−	−	+	+	+	+	+	+	−

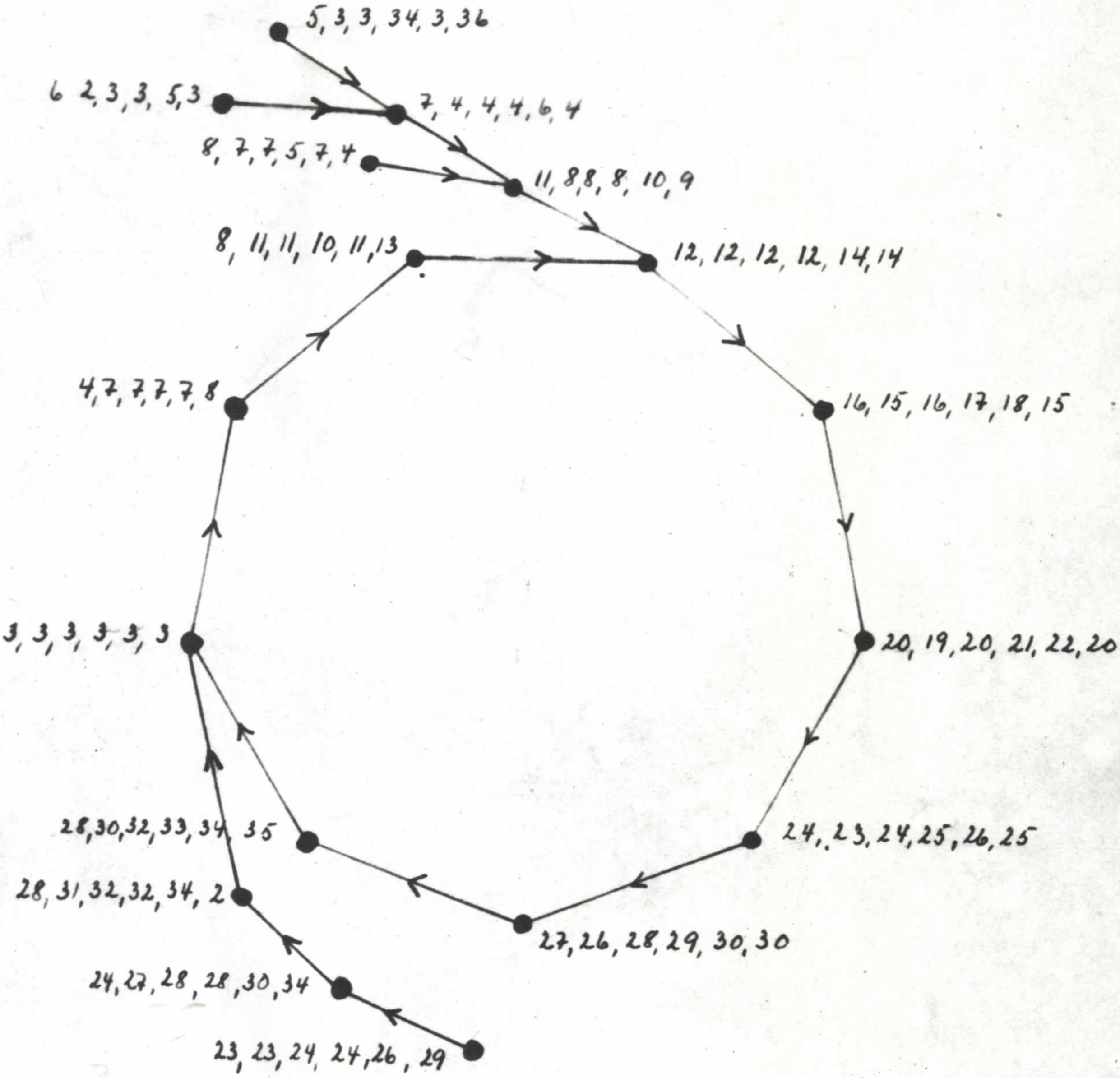
	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
I	+	−	+	+	+	−	+	+	+	−								
II	+	+	−	+	−	+	+	+	+	−	+	−						
III	+	−	+	+	−	+	−	−	+	−	−	+	+	−				
IV	−	+	−	+	+	−	−	−	+	+	−	+	−	+	−			
V	+	+	+	−	−	−	+	−	+	+	−	−	+	+	−	+		
VI	+	−	+	+	−	+	−	+	+	−	−	+	−	+	+	+	−	−

9.

Example of small resolvents II.

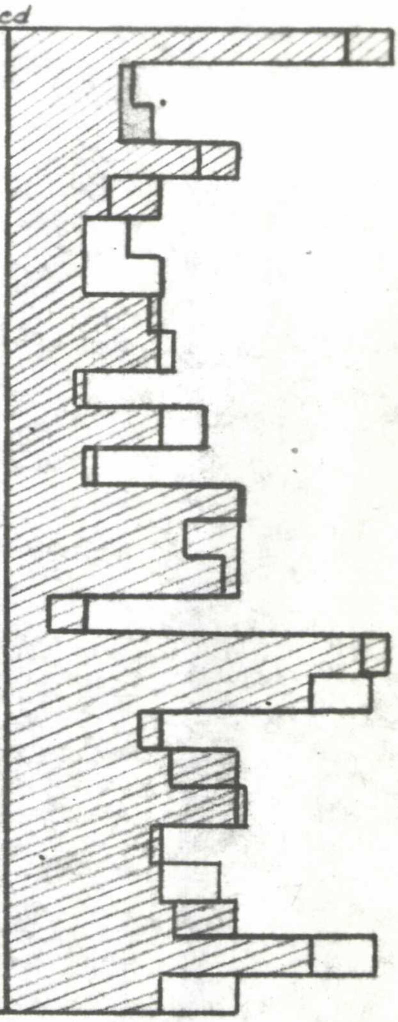


Example of small resolvents. III.



Convergence of actual saltus frequency I.

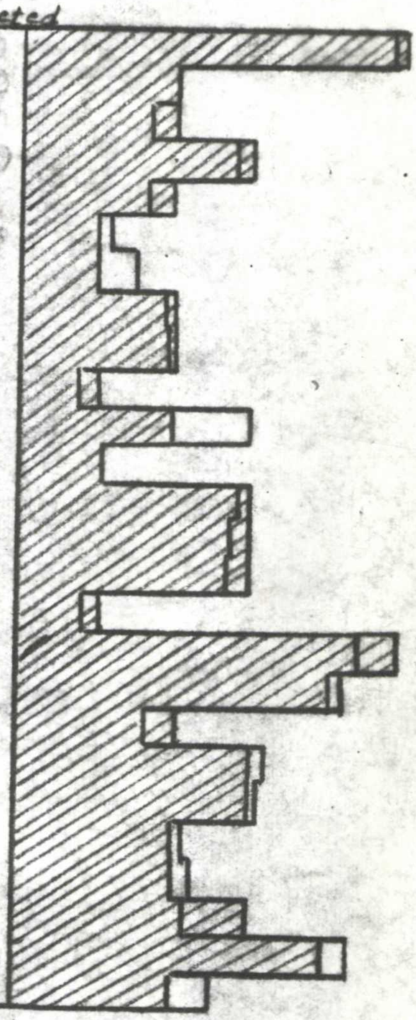
	Counted	Expected
0	4,4	5
1	1,6	2
2	1,9	2
3	2,5	3
4	1,3	2
5	1,6	1
6	2,0	1
7	1,9	2
8	2,2	2
9	0,8	1
10	2,6	2
11	1,2	1
12	3,1	3
13	2,3	3
14	2,8	3
15	0,5	1
16	4,7	5
17	4,8	4
18	1,7	2
19	2,2	3
20	3,1	3
21	1,9	2
22	2,8	2
23	2,2	3
24	4,9	4
25	3,1	2
	64	64



640 Letters. 12 discrepancies

Convergence of actual saltus frequency II.

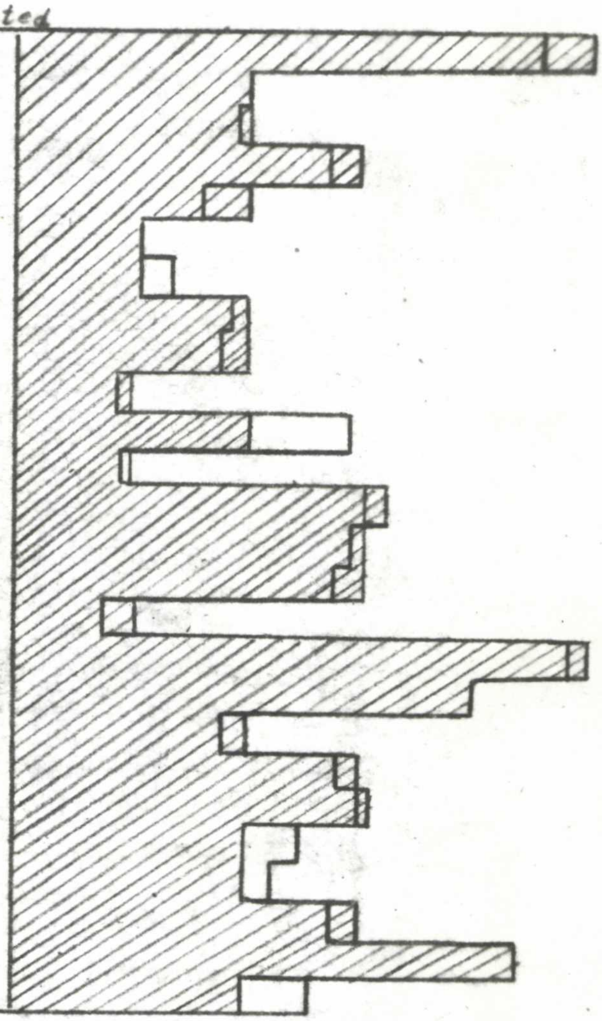
	Counted	Expected
0	4,95	5
1	2,05	2
2	1,70	2
3	2,80	3
4	1,55	2
5	1,15	1
6	1,50	1
7	1,90	2
8	1,95	2
9	0,70	1
10	3,05	2
11	1,05	1
12	2,90	3
13	2,85	3
14	2,80	3
15	0,80	1
16	4,50	5
17	4,25	4
18	1,60	2
19	3,25	3
20	3,15	3
21	2,20	2
22	2,25	2
23	2,15	3
24	4,40	4
25	2,50	2
	64	64



1280 letters. 13 discrepancies

Convergence of actual saltus frequency III

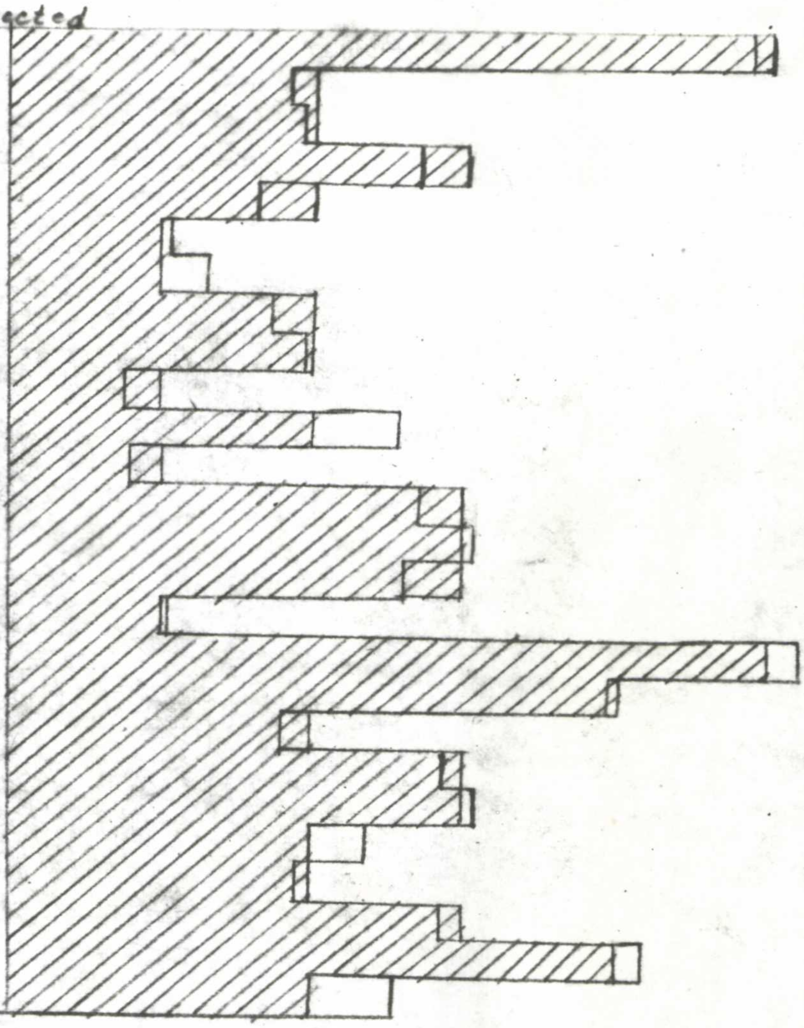
	Counted	Expected
0	4,60	5
1	2,00	2
2	1,90	2
3	2,76	3
4	1,55	2
5	1,03	1
6	1,27	1
7	1,87	2
8	1,83	2
9	0,80	1
10	2,93	2
11	0,90	1
12	3,20	3
13	2,90	3
14	2,76	3
15	0,70	1
16	4,83	5
17	4,00	4
18	1,76	2
19	2,80	3
20	3,03	3
21	2,50	2
22	2,26	2
23	2,76	3
24	4,43	4
25	2,63	2
	64	64



1920 letters 2 discrepancies.

Convergence of actual saltus frequency IV

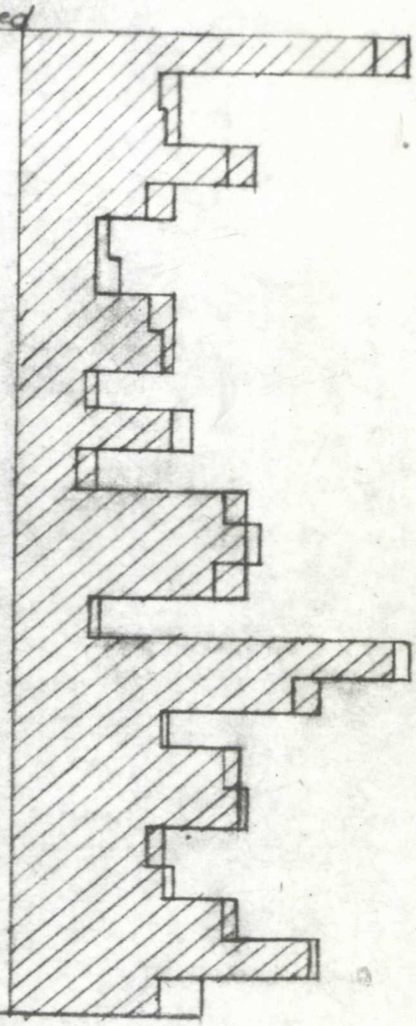
	Counted	Expected
0	4.81	5
1	1.82	2
2	1.92	2
3	2.74	3
4	1.64	2
5	1.09	1
6	1.34	1
7	1.74	2
8	1.97	2
9	0.77	1
10	2.55	2
11	0.77	1
12	2.72	3
13	3.07	3
14	2.89	3
15	1.02	1
16	5.23	5
17	3.97	4
18	1.84	2
19	2.89	3
20	3.04	3
21	2.3[illegible]	2
22	2.18	2
23	2.89	3
24	4.19	4
25	2.57	2
	64	64



2560 Letters   2 discrepancies

Convergence of actual saltus frequency V

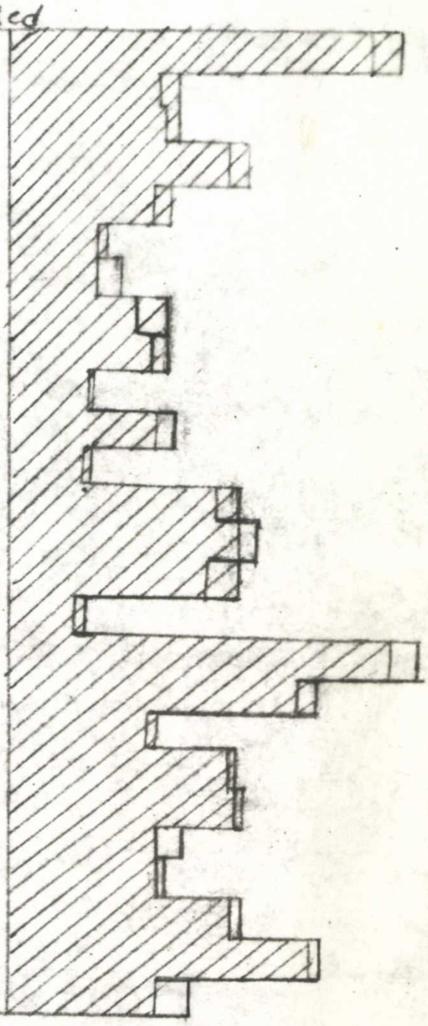
	Counted	Expected
0	4.55	5
1	1.82	2
2	1.88	2
3	2.73	3
4	1.68	2
5	1.24	1
6	1.34	1
7	1.74	2
8	1.92	2
9	0.96	1
10	2.40	2
11	0.78	1
12	2.72	3
13	3.24	3
14	2.62	3
15	1.12	2
16	5.38	5
17	3.74	4
18	2.06	2
19	2.89	3
20	3.06	3
21	2.39	2
22	2.04	2
23	2.90	3
24	4.24	4
25	2.56	2
	64	64



3200 Letters. 1 discrepancy.

Convergence of actual saltus frequency VI

	Counted	Expected
0	4.65	5
1	1.87	2
2	1.88	2
3	2.78	3
4	1.79	2
5	1.08	1
6	1.39	1
7	1.71	2
8	1.89	2
9	0.94	1
10	2.28	2
11	0.89	1
12	2.79	3
13	3.19	3
14	2.68	3
15	0.96	1
16	5.45	5
17	3.77	4
18	1.88	2
19	2.99	3
20	3.08	3
21	2.34	2
22	2.04	2
23	3.03	3
24	4.15	4
25	2.50	2
	64	64



3840 Letters No discrepancy.