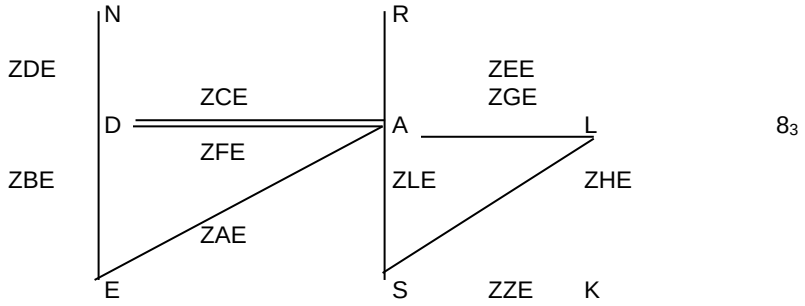
O.H.L.

BREAKING ON THE TWO-WHEEL BOMBE

1. Running on the column

Let us suppose we have a fairly lengthy crib and write it out in the usual way in banks of 26. If we then cast our eye down each of the 26 columns and see how they would make up into menus of the usual type, we may get if we are lucky something like this:-

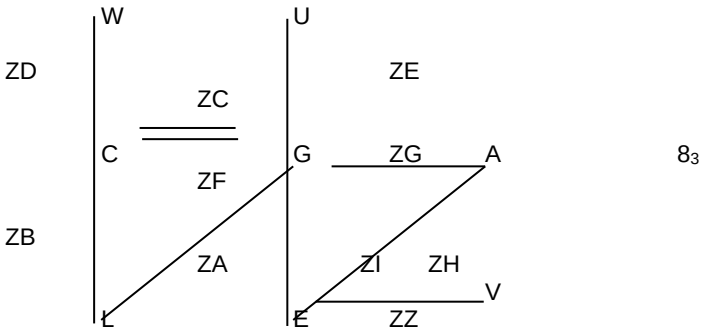
Fig. I.



This special example arose in a Quince message 247 long.

Now it follows as the last wheel is always in the same position that if we know the correct rod pairings a menu of precisely the same shape could be made up on these pairings. In the case under consideration the corresponding menu is actually:-

Fig. II.

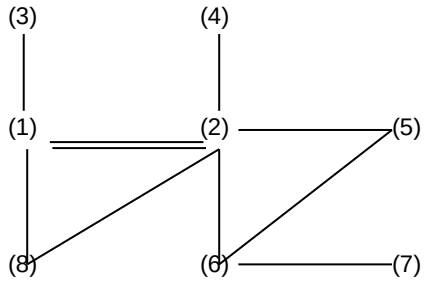


If this second menu could be run on a two-wheeled bombe the day would be broken just as certainly and far more quickly than if we ran the original menu

of Fig. I. But it is impossible to run Fig II as we do not know what the letters are and it is easy to see that using the corresponding letters of Fig. I would eliminate the correct stop as it would give rise to illegal contradictions.

It would be necessary to run the job as a dummy letter menu, probably using numbers for convenience: #

e.g. Fig. III



Then the correct stop would come out with the “stecker” 1/C 2/G 3/W, etc.

The above method of breaking is suitably termed “running on the column”.

II Advantages and disadvantages of the method.

I should say that I propose to eliminate any objections based on the argument that the opportunity of using the method will arise comparatively seldom. All methods of breaking assume the necessary material is to hand and it is no good argument against the value of any method when the material is there to claim that the material will rarely be available. If this method is technically possible I think we should use it when it will be quicker than other methods even though these other methods are good enough.

I have asked Oliver Lawn to write a note on the technical aspects of the problem, i.e. adapting a bombe to run two-wheeled menus.≠ Assuming that this can be done what are the advantages and disadvantages?

1) The principal advantage would be the tremendous saving in bombe time. It is true that there are moments when this is so plentiful that there seems little virtue in economy and methods for saving bombe time would be most unpopular with the Research Section; but such periods will not last for ever, and may vanish permanently when the Second Front is opened. In any case there can be no real gain in unnecessary waste of machine time.

The immensity of the saving in bombe time by this method is best realized

The numbers (1) to (8) all represent different letters; hence machine-gunning on the chain is desirable if this can be arranged.

≠ This note is appended to the present screed.

by contrasting 20 "short" w.o.s (i.e. $^1/_{26}$ of the normal run) with 60 w.o. on 2 menus – i.e. 120 on one which would be the normal alternative.[×] Only actual experiment could enable us to assess precisely the saving in machine time if this method were adopted whenever practicable, but it would certainly be worth while.

2) Regarding turnover the increased risk of m.w.t.o. may be regarded as counterbalanced by the elimination of ordinary t.o. risk. It is true that if a day failed one might feel inclined to rerun in the ordinary way in case there was a m.w.t.o. in the message; but even so the saving in bombe time on jobs that came out would outweigh any loss due to reruns, especially as in practice jobs that could be made up in this way would be based on very strong stories. (It is theoretically possible, of course, to allow for m.w.t.o. by running the column with a kind of delayed hoppity, but this I should consider too slow).

3) The increased difficulty in testing stops is undeniably a serious drawback. When a good stop comes up we have to test it a) on the three end wheels, b) in each rod position. Only the correct end wheel and correct rod position will give a consistent stecker.

While it is quite simple to lay down standard routine for this testing it would take up some time and so we must stipulate for rather strong menus. If the type of menu is strong enough (run in the ordinary way) to give one story per w.o. then run on the column it will give rather less than one stop altogether. This is what is required – a menu that will give one stop, presumably the right one.

Menus of this strength will not be often found in one column; if running on two columns (see sect. III) were introduced, sufficiently strong menus could be made up more often.

4) The most important advantage of the method is that it gives us a quick, certain and even easy method of breaking a new wheel if it is in the right-hand position. This is the strongest argument in favour of the method and is developed in the next section.

III Further developments of the method.

a) Running on Two Columns.

If it is impossible owing to the number of bombes available to make a satisfactory menu on one column, an alternative would be to make up a menu on two columns, of course keeping the two parts distinct. To allow for t.o. it would be necessary to run the menu twice as a double input job – once with settings ZZ and ZZ, the second time with setting ZZ and ZA

Running on two columns would make it possible to use shorter cribs and would thus enhance the utility of the method. The saving in bombe time would still be immense; 2 menus on 20 "short" w.o. instead of 2 menus on 60 w.o.

[×] On the other hand there would in general be less of a saving on reduced w.o. jobs.

Theoretically there is nothing against running on three or even more columns but this would be from the practical standpoint a considerable nuisance from the number of menus necessary with slightly altered menus.

b) Breaking a New Wheel.

Suppose the Germans introduce a new wheel and use it in the machine with the wheels at present known; how are we to break this new wheel?

It is generally accepted that all known methods demand a very long crib – the figure is never put lower than 1000 letters – and even so success would not be certain.

Running on the two wheel bombe provides a sure method of breaking when the new wheel is in the right hand position, and demands a crib or R.E. of only moderate length. It could doubtless be done on 4 banks (100 letters) if we are prepared (as we would be in the circumstances) to run on several columns.

When the correct stop was found we would know the first two wheels and their absolute positions and some of the rod pairings involved, together with the corresponding constatations. It would be easy to find more rod pairings by making use of females and closures 26 apart. The turnover could also be fixed in this way.

We would have still to discover a) the stecker and b) the wiring of the unknown wheel. This could be done by striving to reconstruct the inverse rod square. Considerable parts would be known of the inverse rods but we would not know (because of the unknown stecker) the order in which to lay these rods. The correct order, however, would eventually be reached by working out a kind of jigsaw puzzle and would give automatically the wiring of the unknown wheel and the stecker.

We would still not know the t.o. on the new wheel. This could be found if necessary by trying each of the 26 possibilities in turn and seeing which gave a r/s.

I regard this use of the method as its most important development, and consider that this alone should make it well worth our while to arrive, if possible, at a solution of the technical problems of the bombe adaptations involved.

J.M.A.

Technical Aspect

The following are some of the adaptations on the bombe which would be necessary if Dr. Aitken's methods were adopted.

Single Column

A menu made up from a single column would be run straightforwardly as a dummy-letter menu. No alteration would be necessary in this case. Stops could be thrown out on closures or on legal contradictions, but not on illegal

contradictions since the generalised stecker (through stecker and right hand wheel) is not reciprocal.

In order to make the bombe itself reject legal contradictions we should need to have a completely unwired "diagonal board". The letters of the 2-wheel menu would be plugged up on the separate rows of this board, and the board would have to be "machine-gunned" by columns instead of by rows. The board would have no diagonal wiring and so only legal contradictions would cause a stop to be rejected.

More than one column

A menu made up from, say, three separate columns would have to be run three times to allow for ordinary turnover. The relation between the generalised stecker in the three positions would be unknown, and so the menus from the three columns would have to be plugged up quite independently. The three inputs only would be connected together in series, and a stop would be noted when one relay of each input was up. The bombe modification necessary for this method of running is simply the wiring up of all four inputs in series – not a very serious matter, I believe.

General Remarks

1. With a crib or about 250 letters, running on a column entails a risk of 40% m.w.t.o. This risk could not possibly be taken for ordinary running of jobs, and so the menu would have to be run as a delayed hoppity; but the 10-12 short runs through 26^2 positions should take no longer than 1 complete run through 26^3 positions.

2. The case of a crib or R/E sufficiently long for this method does not arise sufficiently often to make any alteration of the bombe worthwhile. So I think the method would be quite impracticable for ordinary running.

3. However, it offers a very good chance of breaking a new wheel, and is partially complementary to the hand method of stecker knock-out. This latter method suppose a known right hand wheel, and possibly an unknown left hand wheel, middle wheel, and umkehrwalz. The "column menu" method supposes a known left hand wheel, middle wheel and umkehrwalz, and an unknown right hand wheel.

The menus made up on one column of a crib would normally be short, though they might have several closures. Machine-gunning on such menus, as contemplated above, would not therefore be very powerful and would probably not be worth the trouble. Further, if the crib is only about 150 letters long running on one column only would generally be impossible, and several columns would have to be used. The menus on the separate columns could, of course, only be machine-gunned independently, and they would be so short that the process would have a negligible effect.

Thus the best way to break a new wheel would be the multi-input method. "Illegal contradictions" would not be valid contradictions, and legal contradictions would not be noticed (supposing there to be no machine-gunning) and so only

closures should be put on the menu; no other links should be included. Testing of stops would be laborious and so the menu should be made strong enough to give only one or two stops on the whole job.

I suggest, therefore, that several bombes have their inputs modified so that all four can if necessary be connected in series, and that straights be provided for the slow positions of these bombes.

6th January 1944 O.H.L.

Distribution

Mr. Milner-Barry
Major Babbage
Mr. Fletcher
Major Manisty
Mr. Lawn
Mr. Welchman
Mr. Alexander
Dr. Aitken
Watch (2)
Research
M.R.
F/Lt. Jones