Banbury bombe with applications to Wehrkries

Introduction

The only technique which seems at the moment* to offer any chance of a break into Wehrkries is a systematic attack by Banbury and tetragram methods. Unfortunately our present mechanised resources are rather ill-suited to taking advantage of anything that may be picked up in this line except in the rare case of finding two messages which appear to be on the same indicators. A convincing fit at a distance n apart cannot be made full use of even in the particularly fortunate case n = 0 (mod 26) owing to the very limited type of problem with which present bombes are designed to cope. For instance suppose two messages with indicators PQR LMN and ABC DEF appear to be encoded at positions n apart. Suppose the inside indicators of these messages are ((((((and (((respectively. Then if n is not too large we have a fair chance that (and ((are the same letter and we can use the following links in a bombe menu, viz.:-

X

but no further information can be used unless n (0 (26). On the other hand this is only a fraction (and an uncertain fraction) of the information supplied by the fit. We know also that ((=(+((where n=26r + n) and that ((= (+ r or (+r+1 (or possibly (+r+2 but in this case ((((as there must be a middle wheel turnover) and for any given w.o. and ringstellung we know which of the alternatives is true provided we have the values of (and ((. The crying need therefore is for a bombe, or other machine, which can make use of the known facts. The rudimentary clumsy (and complicated-in-practice though simple-in-theory) machine proposed here still fails to make the maximum use of the information available, but seems a slight advance on the ordinary bombe in that it makes some use of it. It should be emphasised at this stage that the machine proposed here has an extremely limited range of application and may never be used (even if it comes to life) more than three or four times in its existence; also that the idea of putting it forward in its present embryonic state is not that I believe it to be practical, but that I hope that it is just possible that it may suggest a more workable line of approach to those who have sensible (and not purely visionary) ideas of what is attainable.

The machine

Suppose then we have made up a menu from stray cillis (if any), fits at distances which are either small or multiples of 26, and that we have, for preference, a fair ringstellung cut-out. Our menu then has links of the following types:-

(¾¾¾((¾¾¾?¾¾¾(

We also add links of this type (which we shall call staggered links)

(¾¾((

(((((((((

(((¾¾¾(

derived from the R.H. wheel settings of indicators of messages fitting at known distances apart. The two links above are to be regarded as not connected. We then plug up the menu on a bombe (preferably a Mammoth but at least a Jumbo) which in addition to the usual diagonal board has also what I shall call a dummy board with a convenient even number of rows and 26 columns labelled A - Z. The ordinary letters on the menu are plugged into the diagonal board in the usual way and the pairs of letters (i(i(are represented in the same way by neighbouring rows of the dummy board. The dummy board has no diagonal wiring, but every row is fitted with switches so that it can be identified at will with any desired row of the diagonal board. The bombe is set running in the usual way and stops when there is a straight. During this time the dummy board has no effect whatever on the proceedings. When a stop occurs the input is changed to the significant letter and the points of the diagonal board and dummy board energised represent stecker implied by the stop. For instance if the point (i X of the dummy board is energised in means that (i is the stecker of X. The machine gun comes into operation (unless the bombe is a mammoth) and eliminates the straight if it gives a contradiction. If it does not, instead of printing stecker we introduce the following new processes. The corresponding pairs of columns of diagonal and dummy board are scanned to see if in any such pair there is a point activated on each board. Suppose for instance the E column gives a point activised on each board, say QE and (i E. This implies Q=(i and (i(=Q+(1. The (i row of the dummy board and the (i(row are then simultaneously switched in to the Q and Q+(I rows of the diagonal board respectively and the same is done for any other pairs of (j (j' brought out by the scanning process. 1 The stop is then re-tested when three possibilities arise: (a) the stop is still good and repetition of the above procedure would get us no further, (b) the stop is still good but we can still make progress by repeating the scanning or (c) we arrive at a contradiction. In case (b) we repeat the processes until we finally reach (a) or (c). In case (c) the stop is rejected and we unswitch the dummy board from the diagonal board and restart the machine. In case (a) the stop is recorded, the stecker printed and the machine restarted after the same unswitching as before. A stop such as (a) is conveniently described as an "irreducible stop".

It will be seen that this procedure may give a very powerful reduction in the number of stories as compared with a menu run on an ordinary bombe without the staggered links. It will take a long time to run, but on a purely research job this is not too serious, and in any case we should have to concentrate on a day with a reasonably sort of ringstellung range unless, of course, we had a particularly good day which provided a menu strong enough to be put through the full range. The obvious drawbacks are that our information is not fully used, it merely stands a chance of being called into play to give a contradiction, and that we have still made no use of the middle wheel positions of the indicators., though they can, of course, be used for testing. The first objection is a fundamental weakness of the machine which we appear to have little hope of rectifying. The second objection might possibly be overcome at a considerable cost in complication. Two methods readily suggest themselves: we shall consider them both (though, of course we give no practical details and doubt very much if any could be given.)

Method I Although we don't know (i - (i(there are (risking middle wheel turnover) only two possible alternatives. Suppose therefore that we put (i , (i (on the menu, but plug them into a part of the dummy board, or a second dummy board, which is not activised until an irreducible stop is reached. Let us then bring (i, (1 (into play at one of the two possible distances and see if this will lead (through the scanning process) to a contradiction. If it does try it at the other distance. If this gives a contradiction too, the stop can be thrown out. If this fails to reduce the stop we again, cut out (1 , (1 (and try (2, (2 i(and so on. The practicability of this method is open to some doubt.

Method II This is best illustrated by making our example a little more concrete. Suppose we are running a menu on 421 and that (1((1((1(=(1(1(1+32. It follows that (1(=(1+6, (1(=(1+1 or (1+2 (neglecting middle-wheel turnover, i.e. assuming that we have used the equality of (1(and (1 in our menu.) It follows that if the R.H. wheel turnover lies between (1 and (1(i.e. for (1=L,M,N,O,P, or Q (l(= (1+2, otherwise (1=(1 + 1. All we require then is that the links involving (1 and (1(be put on the menu and plugged into rows of the dummy board which come to life only if (1 ,(1(have gone over to the diagonal board, thus fixing by the value of (1 the relative distance (1(-(1. The same arrangements, with the obvious modifications could be used on all middle wheel settings, thus even further increasing our chances of throwing out a stop. The procedures outlined here can also be carried a stage further and used with end-wheel settings in cases where we are dealing with fits so far apart that we cannot afford to risk a middle wheel turnover.* However, in most cases we must take this risk as we need some foundation of ordinary bombe menu.

A comparison of the merits and defects (apart from the overriding difficulty of practicality) of these two methods is not without interest. Method II does not use all pairings (i(i (but only those for which (i(i(get on the diagonal board. Method I uses all pairs irrespective of the properties of their corresponding ('s but suffers from the two other theoretical drawbacks. The first is that throwing out a stop on a pair (((is purely fortuitous as it depends not only on getting a contradiction on a correct setting of the menu, but also getting a contradiction on a wrong one. (This is of course only an approximate description, but it conveys my meaning better than a more accurate one.) The second drawback is that all the data is used separately and therefore loses the immense potential power of a co-ordinated offensive. This suggests that the ideal is to use Method II as far as it will go and apply Method I to the rest.

* i.e. prior to the discovery of 371

1 There is nothing to stop two rows of the dummy board going to the same one on the diagonal board.

* This will involve further complications with the third possible relative positions of the middle wheel settings. Consideration of this difficulty is better postponed though there appears to be a solution of no greater order of difficulty than the ideas already discussed.

1