A Note on Error Detection in Noisy Logical Computers

Murray Eden*

Center for Communication Sciences, Massachusetts Institute of Technology, Cambridge, Massachusetts

A method of error detection is proposed for noisy logical computer elements. The proposal extends the range of the propositional variables so that residue class check symbols may be used in error detection. The principal consequence is that individual logical elements may be designed to process binary inputs with arbitrary reliability and nonzero channel capacity.

Programs for the construction of finite state automata assembled out of components that are liable to some errors in their output have been considered in some detail by von Neumann (1956) and by Moore and Shannon (1956). Although these two theories are quite different in detail and, indeed, consider errors at different places in the automaton, both derive a comparable principal theorem, namely, that if components with a reliability less than 1 (and greater than \( \frac{5}{6} \) in the von Neumann model or different from \( \frac{1}{2} \) in the Moore and Shannon model) are composed in some suitable way into a redundant net of components, then the over-all reliability can be made arbitrarily close to 1 by a sufficient redundancy.

Elias (1958) has pointed out a weakness in these constructions, in that the coding theorem for noisy channels does not hold for such automata; that is, even though "the receiver has only a small amount of equivocation, and it would take only a small additional amount of information to correct the occasional errors which are present in the computer output, it is not possible to provide this extra information by coding the different blocks of \( k \) digits independently of one another before the computation begins."

* Permanent address: Laboratory of Technical Development, National Heart Institute, National Institutes of Health, Bethesda 14, Maryland.
ERROR DETECTION IN LOGICAL COMPUTERS

A typical Boolean algebra employed in discussions of automata consists of a set of two elements \( C = \{1, 0\} \), a binary operation \( \lor \) ("or") such that \( A \lor B \) is defined by the matrix given in Fig. 1a, and a singular operation \( \sim \) (complement or "not") defined by the (column) matrix, also shown in this figure. It is well known that such an algebra is an adequate model for propositional calculus and it is such a model that leads to the negative results found by Elias.

Since Elias' results represent a serious limitation on the structure of automata it seems worthwhile to consider whether an alternative formulation may not provide slightly more positive results.

We may consider a somewhat different algebra including the one described above. Thus we may let the set of symbols \( C = 0, 1, 2, \ldots, n \); the binary operation being defined as addition \( \text{mod } p \), \( p \geq 2n + 1 \), and complementation defined so that \( \sim 0 = 1 \) and \( \sim \alpha = 0 \) (for any \( \alpha \neq 0 \)).

The advantage of such a structure is revealed in the following example. Consider a single "\( \lor \)" organ with independent parallel inputs of "0's" and "1's". The matrix corresponding to Fig. 1a is shown in Fig. 1b.

If "2" is interpreted as "1" the tables are identical, but in this latter case a residue class check symbol may be associated with each input digit independent of the other input stream. In the case of mod 2 addition, Peterson (1958) has shown that a mod 3 check symbol will provide single error detection and in consequence for a suitable set of check digits the channel coding theorem can be shown to hold for this operation; that is, if the digits are introduced in larger and larger blocks, keeping the ratio of check digits to information digits a constant, the reliability of the output can be made as large as we please. It will be noted that even before introducing a \( \text{mod } 3 \) check digit we had cut the channel ca-
pacity to $1/1.58$ of its original value as a binary channel (since now the
device must discriminate between three symbols rather than two).

We may attempt to improve reliability for a cascade of “or” circuits.
For each organ added to the cascade, the maximum value of the matrix
entries increases by a factor of 2 so that for $k$ organs in a cascade the
check digit must be a member of a residue class $\mod p$, $p \geq 2^k + 1$.
If all symbols other than “0” are interpreted as “1”, the coding theorem
will hold for a $k$-fold cascade. The channel capacity $C_k$ before the addi-
tion of check digits will become $C/\ln_2 p$, $C$ being the channel capacity of
the cascade viewed as a binary channel, or $C_k < C/\ln_2 2^k = C/k$. Ob-
viously for any prime $p$ we can find a value $k$ such that $2^k + 1$ will ex-
ceed $p$. As a consequence the general negative result for arbitrarily large
machines with one errorless encoder and one errorless decoder must hold
for this model as well.

In any case the “or” operation taken by itself is insufficient for proposi-
tional calculus and we must introduce another logical operation, say
negation, and define negation on the set $C$ in a way that is consistent
with the interpretation of “or” as addition ($\mod p$).

It is well known that a single binary operation, the Sheffer stroke, is
sufficient to complete the propositional calculus. The Sheffer stroke $A \mid B$, can be defined in terms of the operations we have introduced above;
that is

$$A \mid B = \sim A \lor \sim B$$

We now propose for $\gamma \in C$, $\sim \gamma \equiv -\gamma + 1$. Thus $\sim 0 = 1$, $\sim 1 = 0$,
$\sim m = -m + 1$. Again this addition will be considered $\mod p$. For the
Sheffer stroke the matrix is given in Fig. 1c. Again, 2 is to be interpreted
as 1.

Consider a Sheffer stroke organ with two independent binary inputs
taken in blocks of $k$-digits $\alpha_1 \cdots \alpha_k$ and $\beta_1 \cdots \beta_k$. Let $\gamma_\alpha$ be a residue
class check digit for $\sum_k \alpha_j$ such that $\sum_k \alpha_j + \gamma_\alpha \equiv 0 \pmod 3$. In like
manner $\sum_k \beta_j + \gamma_\beta \equiv 0 \pmod 3$. The output

$$\sum_k \omega_j + \gamma_\omega = k + \sum_k (-\alpha_j) + k + \sum_k (-\beta_j) - \gamma_\alpha - \gamma_\beta + 2$$

$$= 2(k + 1) - \left[ \sum_k (\alpha_j + \beta_j) + \gamma_\alpha + \gamma_\beta \right]$$

but the term in the bracket $\equiv 0 \pmod 3$. Hence $\sum_k \omega_j + \gamma_\omega \equiv 2(k + 1)$
($\mod 3$). Thus a decoder operating on the output of the Sheffer stroke
organ can detect single errors on the basis of the residue class output check digit and the length of a block which certainly must be known.

However, if an attempt is made to cascade two such organs the proposed model will lead to inconsistencies. By our interpretation $0 \mid 2 = 0 \mid 1$. But $0 \mid 2 = 1 - 1 = 0$ and $0 \mid 1 = 1 + 0 = 1$. This would imply $0 = 1$, an obvious inconsistency.

Thus it is seen that while enlarging the range of the propositional variables permits a certain extension of the coding theorem to single components in probabilistic automata it has not yet been possible to construct a model sufficient for arbitrary aggregates of components or to show that such a model cannot be found.

Received: May 1, 1959.

References


