

Some New Results for Reliable 2-of-3 Valued Systems

Hu, Mou

Shanghai Institute of Railway Technology
Shanghai, China

Smith, K.C.

University of Toronto
Toronto, Ontario, Canada

Abstract

TSC (totally self-checking) 2-of-3 valued systems were first proposed in the authors' previous papers [1], [2], [3]. In this paper, some new results on reliable 2-of-3 valued systems are presented. These include the design of a TSC checker for 2-of-3 valued systems, two-rail, 2-of-3 valued systems, and the design of a fail-safe checker for two-rail 2-of-3 valued systems.

I. Introduction

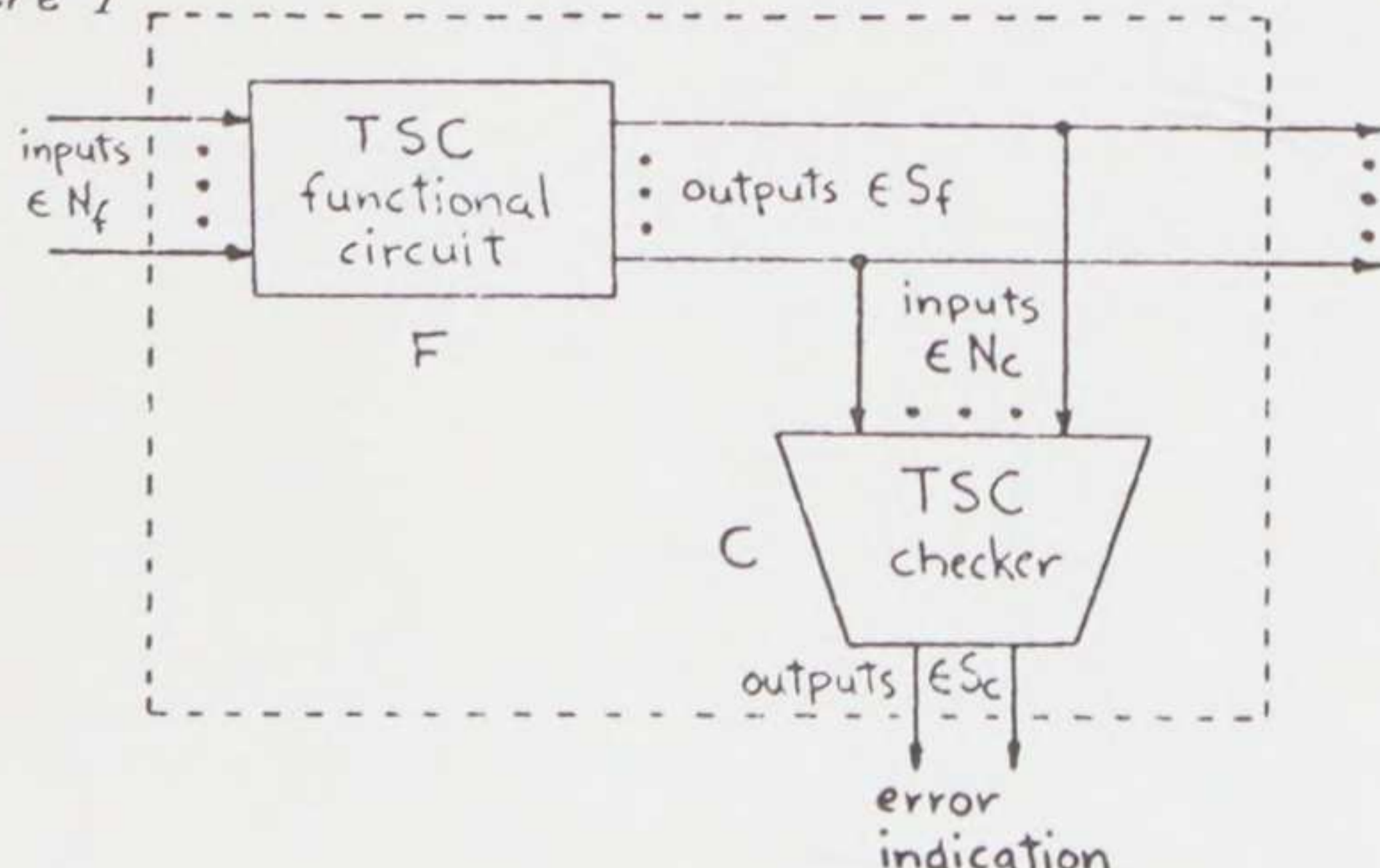
A TSC 2-of-3 valued system consists of special ternary logic circuits working in binary mode. The redundant third logic value, which is usually the middle value, can provide the system with TSC properties. In [1] and [2], TSC 2-of-3 valued combinational systems were proposed, whereas TSC 2-of-3 valued synchronous sequential systems were addressed in [3]. More work must be done in this field before these systems can be used practically.

In this paper some new results for reliable 2-of-3 valued systems are presented. These include the design of a TSC checker for 2-of-3 valued systems presented in Section II, two-rail 2-of-3 valued systems as presented in Section III, and the design of a fail-safe checker for two-rail 2-of-3 valued systems as presented in Section IV. Section V concludes the paper.

II. TSC Checker Design for 2-of-3 Valued Systems

In [4] and [5], a model of a TSC network was given as shown in Figure 1. It is also directly applicable to a TSC 2-of-3 valued network. The TSC network consists of a TSC functional circuit and a TSC checker.

Figure 1



To specify the input and output domains of the TSC functional circuit and TSC checker, let us denote the logic value set provided by the 2-of-3 valued circuit as Q , where $Q = \{0, 1/2, 1\}$. Q is further divided into two disjoint subsets N and E , where $N = \{0, 1\}$, and $E = \{1/2\}$. Assume that the functional circuit F has m input lines and n output lines. Then the total input space of F (denoted as R_f) is N^m , and the normal output space of F (denoted as S_f) is N^n . Accordingly the abnormal output space of F is $(Q^n - N^n)$.

In other words, for a fault-free functional circuit, the outputs will always be in N^n . If the outputs of F are in $(Q^n - N^n)$, there must be a fault in F . A TSC checker C monitors the outputs of F . So the normal input space of C (denoted as R_c) is equal to S_f , which is again equal to N^n . Similarly, the abnormal input space of C is $(Q^n - N^n)$. But both the normal output space (denoted as S_c) and the abnormal output space of C cannot be specified here, since they depend on the coding or value assignment scheme used for the checker outputs.

A TSC checker must meet two essential conditions: The first is that it be "space disjoint". The second is that it be totally self-checking. The concept here labelled "space disjoint" is extended from the Anderson's definition of "code disjoint" [5] as follows:

Definition 1

A circuit (or a logic function) is space disjoint for a normal input space S' and a normal output space S , if for any input X , $Z(X, \varphi) \in S \iff X \in S'$, where $Z(X, \varphi)$ denotes the output of the fault-free circuit (function) with input X (i.e. $Z(X, f)$ for $f = \varphi$).

A fault-free space-disjoint circuit will map the normal input space into the normal output space, and the abnormal input space into the abnormal output space. This condition is necessary for a checker to signal an error properly.

The second condition a TSC checker must meet is that it should be totally self-checking. This condition ensures that a fault in the checker itself will produce an error signal.

Now let us discuss the design of a TSC checker for a 2-of-3 valued system. The output value assignment of the checker can be made as follows:

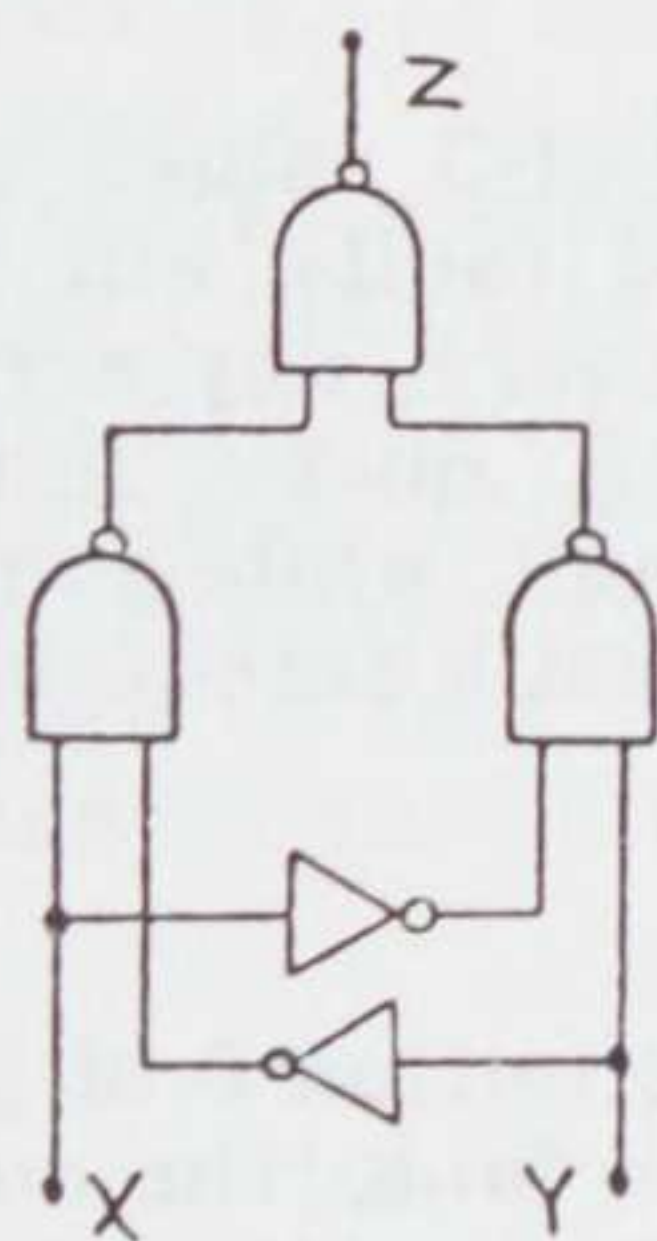
The normal output space is N, while the abnormal output space is E. Under this assignment, it is easy to prove that a 2-of-3 valued exclusive-OR circuit is space disjoint and that it can be used as a checker. Its logic expression is $Z = X \oplus Y = X\bar{Y} + \bar{X}Y$. Its truth table is shown in Table 1. It is observed in Table 1 that whenever one or both inputs are 1/2, the output will be 1/2. According to Definition 1, the Exclusive-OR is space disjoint.

Table 1

X	Y	Z = $X\bar{Y} + \bar{X}Y$
0	0	0
0	1/2	1/2
0	1	1
1/2	0	1/2
1/2	1/2	1/2
1/2	1	1/2
1	0	1
1	1/2	1/2
1	1	0

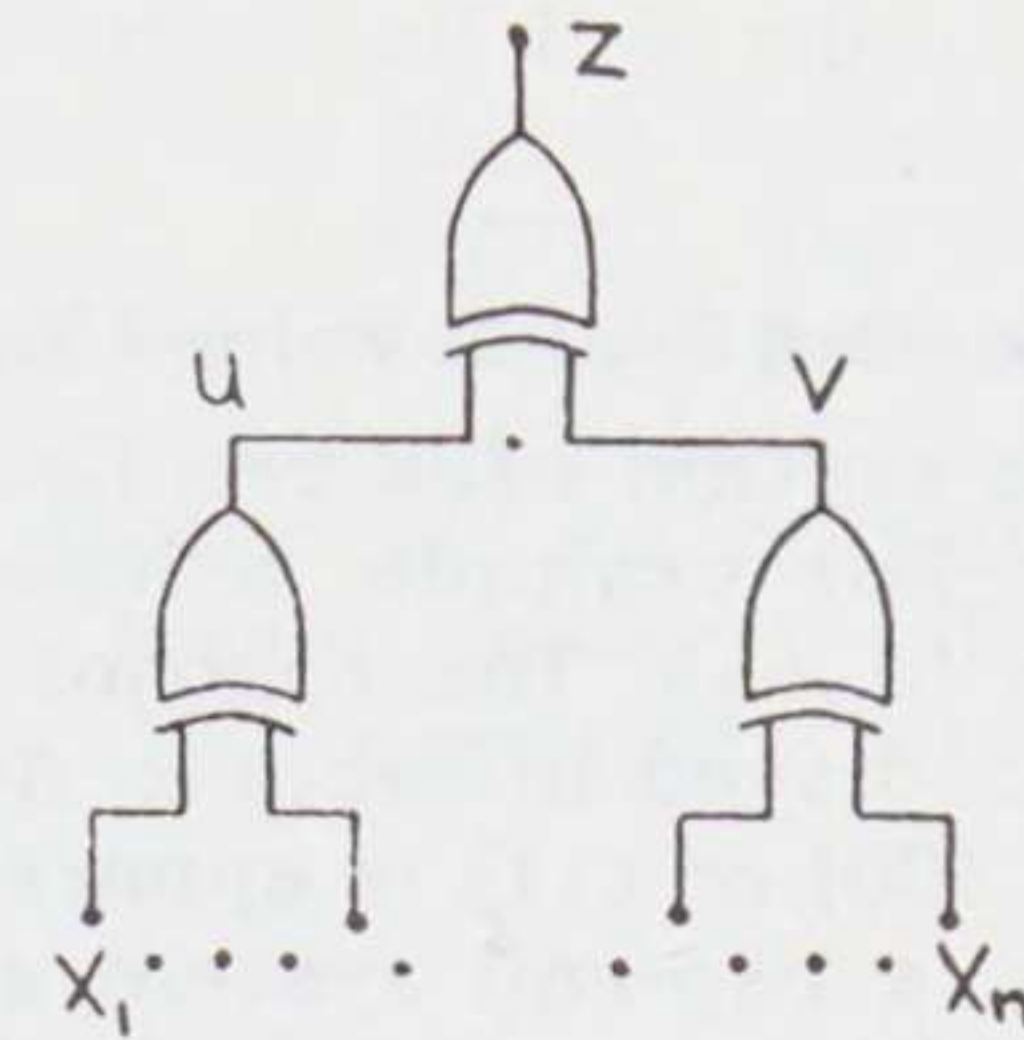
The Exclusive-OR function can be implemented by 2-of-3 valued Inverters and NAND gates as shown in Figure 2. Theorem 1 of [2] states that for any mid-seeking or quasi-mid-seeking fault, any irredundant combinational logic network which consists of 2-of-3 valued inverters and NAND gates is totally self-checking. Thus the circuit of Figure 2 is totally self-checking for any single mid-seeking or quasi-mid-seeking fault. But since this circuit is used as a checker, its whole input space (normal and abnormal) will be Q^2 instead of N^2 as it would be for a functional circuit. Thus this circuit is totally self-checking for mid-seeking faults only. The quasi-mid-seeking faults and mid-rejecting faults in this circuit must be detected by off-line test.

Figure 2



Note that this checker can monitor two lines only. To monitor additional lines, an Exclusive-OR tree can be formed as shown in Figure 3. To show that this tree is space disjoint, we will first prove a broader statement expressed as Theorem 1.

Figure 3



Theorem 1

If $U = u(X)$ and $Z = z(Y)$ are both space disjoint functions, where $Y = (U, V)$ then the composite function $Z = z(U, V) = z[u(X), V]$ is still a space disjoint function.

Proof:

For the composite function Z, the input vector is (X, V) . If (X, V) is in the normal input space, then both X and V are normal. Since $U = u(X)$ is a space disjoint function, U is normal. Thus (U, V) is normal. Since $Z = z(Y) = z(U, V)$ is a space disjoint function, Z is in the normal output space.

On the other hand, if (X, V) is in the abnormal input space, there will be three possible cases: In Case 1, only X is abnormal; In Case 2 only V is abnormal; In Case 3, both X and V are abnormal. For Cases 2 and 3, (U, V) is abnormal. For case 1, since $U = u(X)$ is a space disjoint function, U is abnormal. Thus (U, V) is also abnormal. Since $Z = z(Y) = z(U, V)$ is a space disjoint function, Z is in the abnormal output space.

Thus the composite function meets Definition 1. The Theorem is proved.

Q.E.D.

Theorem 2

The Exclusive-OR tree shown in Figure 3 is a TSC checker for a 2-of-3 valued system.

Proof:

From Definition 1, the Exclusive-OR gate is a space-disjoint circuit. From Theorem 1, the Exclusive-OR tree is also a space-disjoint circuit.

Furthermore, since the Exclusive-OR tree is an irredundant combinational network, consisting of 2-of-3 valued Inverters and NAND gates, it is totally self-checking for any mid-seeking fault. Thus it can serve as a TSC checker for a 2-of-3 valued system.

Q.E.D.

A second, more economical, implementation of the Exclusive-OR circuit will be discussed in detail in Section IV.

III. Two-Rail 2-of-3 Valued Systems

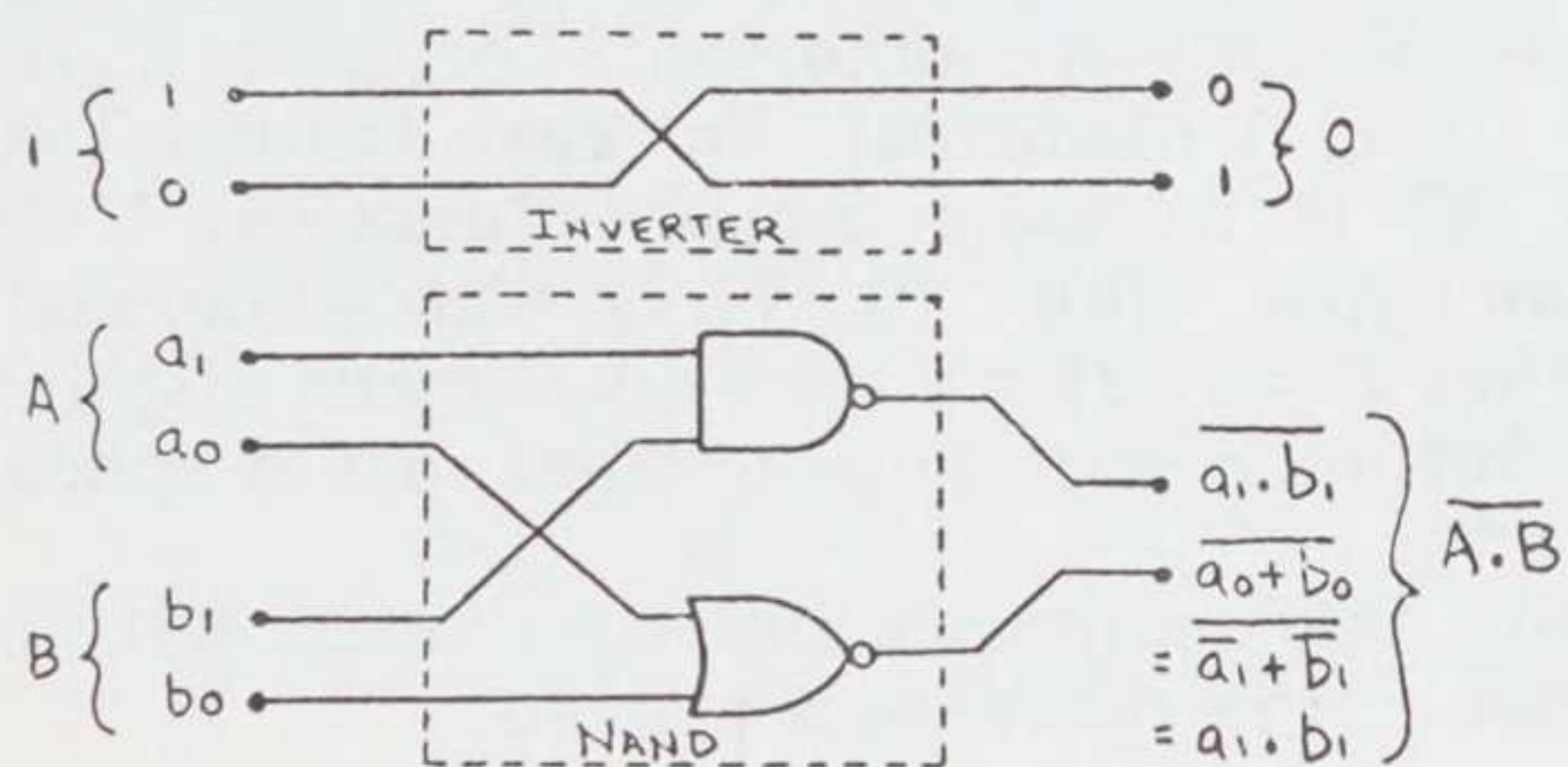
A two-rail logic system uses two lines to represent each variable. For example, a logic variable A is represented as $(a_1 a_0)$. The relationship between A and $(a_1 a_0)$ is displayed in Table 2. Any fault resulting in $(a_1 a_0) = (00)$ or (11) is apparent. It is known further that in a two-rail system any single fault will be detected [6], since such a fault cannot affect both the "true" and "complement" outputs simultaneously.

Table 2

A	$a_1 a_0$
0	0 1
1	1 0

If 2-of-3 valued circuits are used, a two-rail system becomes a two-rail 2-of-3 valued system. The basic gates of this system are shown in Figure 4. For a two-rail 2-of-3 valued system, several theorems result:

Figure 4



Theorem 3

In a two-rail 2-of-3 valued combinational system, an error caused by any mid-seeking or quasi-mid-seeking fault is a correctable error.

Proof:

Since a single fault in a two-rail system cannot change the "true" and "complement" outputs simultaneously, errors caused by a mid-seeking or quasi-mid-seeking fault will take only the forms shown in Table 3. It is obvious that these errors are correctable using information conveyed by the unchanged (normal) output.

Q.E.D.

Table 3

Outputs	$a_1 a_0$	$a_1 \bar{a}_0$
Correct Values	0 1	1 0
Errors	0 $\frac{1}{2}$ $\frac{1}{2}$ 1	1 $\frac{1}{2}$ $\frac{1}{2}$ 0

Theorem 4

In a two-rail 2-of-3 valued combinational system, an error caused by any mid-rejecting fault is a detectable error.

Proof:

Errors caused by a mid-rejecting fault are listed in Table 4. Of course they are detectable (but not correctable).

Q.E.D.

Table 4

Outputs	$a_1 \bar{a}_0$	$a_1 a_0$
Correct Values	0 1	1 0
Errors	0 0 1 1	1 1 0 0

Theorem 5

In a two-rail 2-of-3 valued combinational system, masked faults will not cause an error. Furthermore, any error caused by any mid-seeking, quasi-mid-seeking, or mid-rejecting fault, while a masked fault is present, is at least a detectable error.

Proof:

According to Definition 6 of [2], for a gate having a masked fault, the output remains correct. Thus the first part of the Theorem is obvious. For the second part of the Theorem, when a masked fault exists, an error through any fault other than a masked fault will result in one of the paired output lines turning to 1/2 or to the incorrect (opposite) value. These errors are at least detectable in a two-rail 2-of-3 valued system.

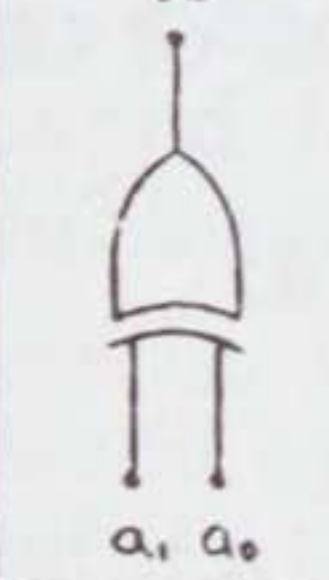
Q.E.D.

IV. Fail-Safe Checker Design for Two-Rail 2-of-3 Valued Systems

Since Two-Rail 2-of-3 Valued Systems can produce both correctable errors as well as detectable but uncorrectable errors, their checkers should distinguish three states. As we will see, the simplest available checker is not itself a two-rail circuit. For this checker, the coding or the value assignment schemes for the input space and the output space of the checkers are different. Moreover, with three output states, a fail-safe checker is easier to define than a TSC checker. Accordingly in this section, only fail-safe checker design is discussed.

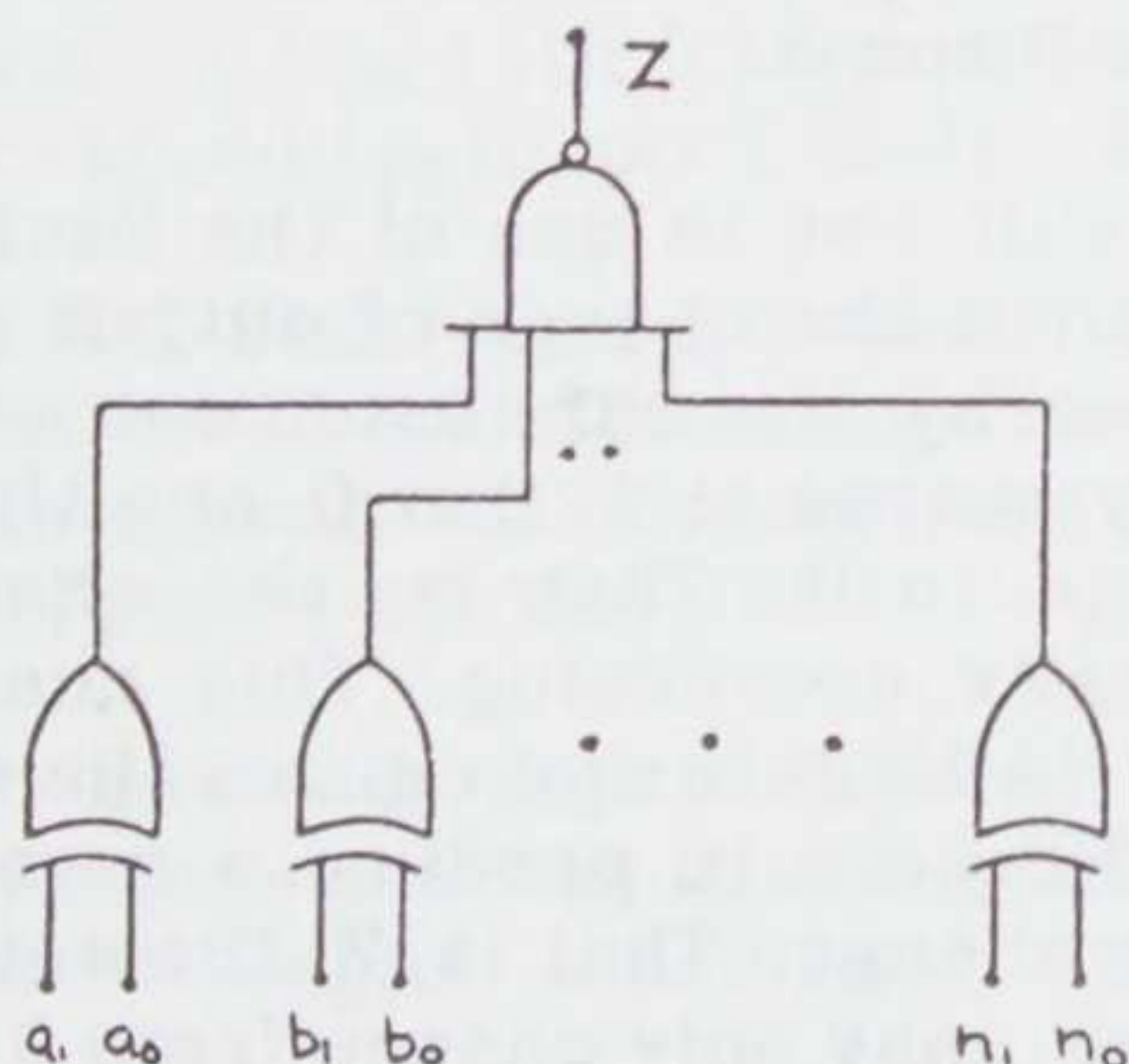
Let us first consider the situation of monitoring only one pair of outputs. An Exclusive-Or gate can be used as a checker in this case with the following output value assignment: 0 indicates an uncorrectable error, 1/2 indicates a correctable error, while 1 indicates that the outputs of the checked circuit are correct. This situation is summarized in Table 5.

Table 5

Checker	Output of Checked Circuit		Output of Checker	Meaning
	0	0	0	uncorrectable error
	1	1	0	
	0	1/2	1/2	correctable error
	1/2	0	1/2	
	1/2	1	1/2	
	1	1/2	1/2	fault-free
0	1	1		
1	0	1		

For n pairs of checked outputs, an Exclusive-OR-NAND network can be used as a checker as shown in Figure 5. By virtue of the inversion in the NAND gate, $Z = 0$ now indicates the checked circuit to be fault-free. $Z = 1/2$ indicates a correctable error of the checked circuit, while $Z = 1$ signals an uncorrectable error. Furthermore, if the output of one Exclusive-OR gate is 1/2 indicating a correctable error, while another Exclusive-OR gate is 0 indicating an uncorrectable error, then the output of the checker will be 1 indicating an uncorrectable error. This is clearly preferable to a scheme which propagates the 1/2 output. Thus it can be seen that some outputs of the checker may be more safe than others. As a measure of this variation, a "safety factor" can be defined for the output of a circuit:

Figure 5



Definition 2

A safety factor is a factor assigned to each logic value of a circuit indicating the degree of safety present. Larger factors represent safer output values. A change in the safety factor of an output from a smaller to a larger value is safe, while a change in the opposite direction is dangerous.

For example, in the checker shown in Figure 5, an output of 1 signals an uncorrectable error; output 1/2 indicates a correctable error; output 0 means the circuit is fault-free. Now if the checker fails, output 0 may change to 1/2 or 1, indicating a nonexisting error in a fault-free circuit, a result which is not dangerous. However if output 1 or 1/2 of a failed checker changes to 0, the checker will fail to signal an error in the circuit. This situation is dangerous. Thus in general we find that changes in output from 1 to 1/2 or 0 or from 1/2 to 0, are safe but changes in the reverse direction are dangerous. Thus safety factors for the output Z have the following relationship:

$$S(0) < S(1/2) < S(1),$$

where $S(X)$ denotes the safety factor for output X .

For the same reason, in Table 5

$$S(0) > S(1/2) > S(1).$$

Now let us consider the Exclusive-OR gate implementation. Since both the "true" and "complement" outputs are available in a two-rail system, it is easy to implement an Exclusive-OR gate more directly than by use of the circuit of Figure 2. Such a CMOS Exclusive-OR gate for a two-rail system is shown in Figure 6.

Figure 6

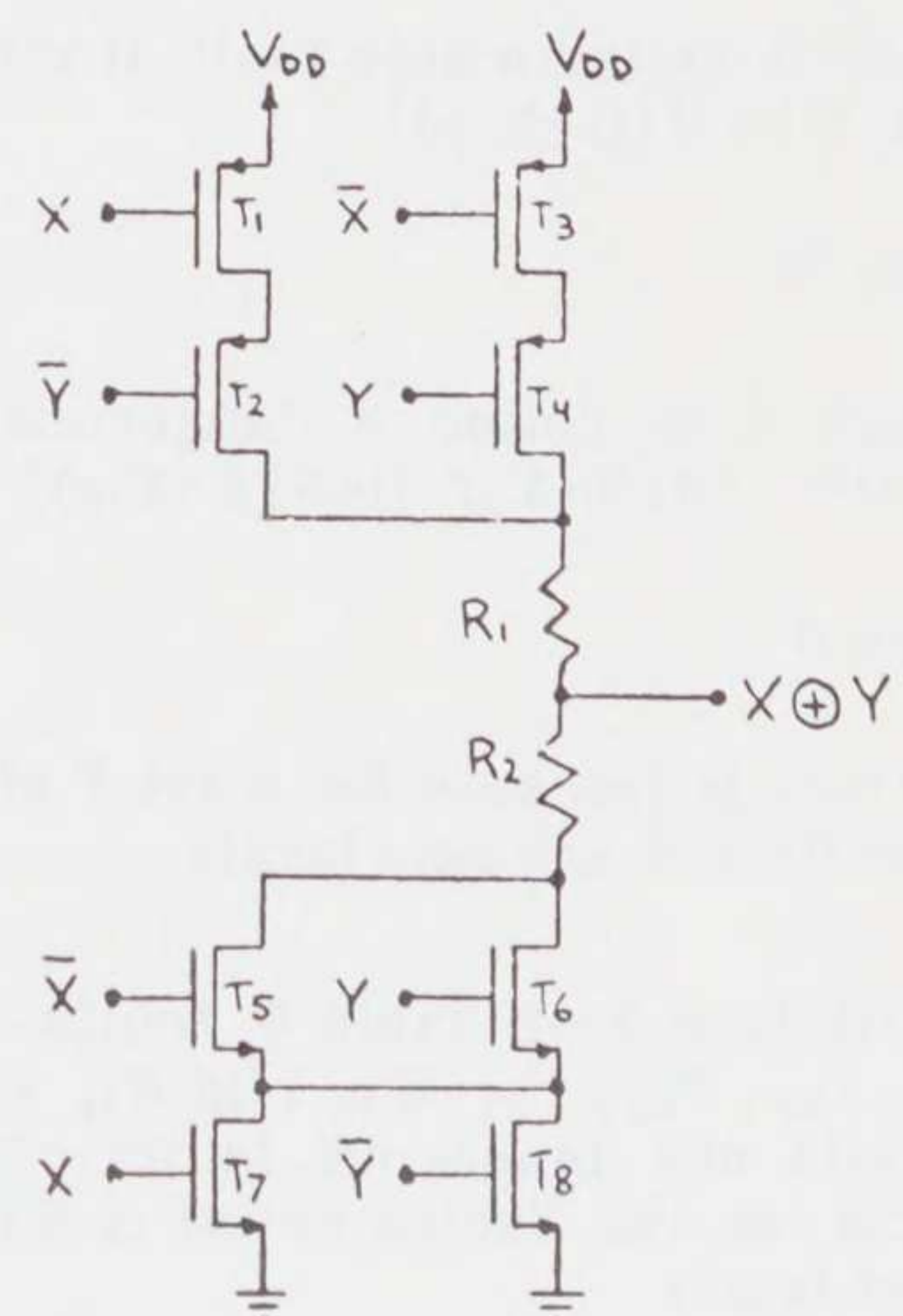


Table 6

Inputs		fault-free	Outputs																			
			Safe Faults											Dangerous Faults								
X	Y	X⊕Y	T _{5s}	T _{6s}	T _{7s}	T _{8s}	R _{2s}	T _{1o}	T _{2o}	T _{3o}	T _{4o}	R _{1o}	T _{1s}	T _{2s}	T _{3s}	T _{4s}	R _{1s}	T _{5o}	T _{6o}	T _{7o}	T _{8o}	R _{2o}
0	0	0	0	0	0	0	0	0	0	0	0	0	0	1/2	1/2	0	0	F	0	0	F	F
0	1/2	1/2	1/2	1/2	1/2	1/2	0	0	0	1/2	1/2	0	1/2	1/2	1/2	1/2	1	1/2	1/2	1/2	1	1
0	1	1	1	1	1/2	1/2	1	F	F	1	1	F	1	1	1	1	1	1	1	1	1	1
1/2	0	1/2	1/2	1/2	1/2	1/2	0	1/2	1/2	0	0	0	1/2	1/2	1/2	1/2	1	1	1/2	1/2	1/2	1
1/2	1/2	1/2	1/2	1/2	1/2	1/2	0	1/2	1/2	1/2	1/2	0	1/2	1/2	1/2	1/2	1	1/2	1/2	1/2	1/2	1
1/2	1	1/2	1/2	1/2	1/2	1/2	0	0	0	1/2	1/2	0	1/2	1/2	1/2	1/2	1	1/2	1/2	1	1/2	1
1	0	1	1/2	1/2	1	1	1	1	1	F	F	F	1	1	1	1	1	1	1	1	1	1
1	1/2	1/2	1/2	1/2	1/2	1/2	0	1/2	1/2	0	0	0	1/2	1/2	1/2	1/2	1	1/2	1	1/2	1/2	1
1	1	0	0	0	0	0	0	0	0	0	0	0	1/2	0	0	1/2	0	0	F	F	0	F

*F denotes that the output is floating. The real output value depends on the last value attained before this situation applies.

With the same fault model used in [1], that is, the single component open-short model, the fault table of the Exclusive-OR gate is shown in Table 6. In this table, the subscript "S" is used to denote a component short-circuit condition, while "O" is used to denote a component open-circuit condition. Circles and squares serve to highlight the conditions which lead to faulty outputs.

To facilitate the analysis, some new definitions for fault classification will be given:

Assume that the number of the inputs of a circuit G is m. With an input vector X, and a fault f, the output of the circuit G is denoted as G(X, f). Correspondingly the output of fault-free circuit G is denoted as G(X, φ).

Definition 3

A fault is called a safe fault, if $\forall X \in Q^m$ $S[G(X, f)] \geq S[G(X, \phi)]$.

Definition 4

A fault f is called a dangerous fault, if $\exists X \in Q^m$ $S[G(X, f)] < S[G(X, \phi)]$.

Definition 5

A circuit is fail-safe for a set F of faults, if all faults in F are safe faults.

From Definition 3, in Table 6, faults T_{5s}, T_{6s}, T_{7s}, T_{8s}, R_{2s}, T_{1o}, T_{2o}, T_{3o}, T_{4o} and R_{1o} are safe faults. Other faults are dangerous faults. The number of safe faults for the Exclusive-OR is 50% of the total number of faults.

For the NAND gate of Figure 5, the fault table is listed in Table 4 of [1]. Faults T_{1on}, T_{2on}, T_{3off}, T_{4off}, R_{1o}, R_{2o}, R_{po}, R_{n∞}, R_{1∞}, R_{2∞}, R_{3∞} and R_{4∞} are safe faults. The number of safe faults is 60% of the total number of faults.

For safe faults, the following theorem is valid:

Theorem 6

For any single safe fault in its component gates, the checker shown in Figure 5 is a fail-safe checker.

Proof:

In Figure 5, the safe factors of Z are related as follows:

$$S(0) < S(1/2) < S(1).$$

The safe factors of the outputs of the Exclusive-OR gates are related as follows:

$$S(0) > S(1/2) > S(1)$$

If a safe fault occurs in the NAND gate, this theorem is satisfied as a direct result of Definitions 3 and 5.

If a safe fault lies in one of the Exclusive-OR gates then the change of output of this gate caused by the safe fault can only be that 1 may change to 1/2 or 0, and that 1/2 may change to 0. That is, the change is monotonically decreasing. This change is fed to the NAND gate and causes the output of the NAND gate to produce a monotonic increasing change. That is, Z, the output of the checker, may only change from 0 to 1/2

or 1, and from 1/2 to 1. Thus the checker shown in Figure 5 is a fail-safe checker for any single safe fault in the component gates.

Q.E.D.

It is interesting to note that if only the error detecting properties (and not the error correcting ones) are required, then the set of safe faults will become much larger. This results from the fact that for this situation the 0 and 1/2 outputs have the same interpretation. In particular the relationship between the safe factors is

$$S(0) = S(1/2) > S(1).$$

Thus, in Table 6, T_{1s} , T_{2s} , T_{3s} and T_{4s} are safe faults instead of dangerous faults as in the former case. This results in an increase of safe faults from 50% to 70% for the circuit of Figure 5.

V. Summary

In this paper, some new results for reliable 2-of-3 valued systems have been presented.

First the "space disjoint" concept is defined. With this concept, a TSC checker design for 2-of-3 valued systems is given.

Secondly, a two-rail 2-of-3 valued system is discussed for which all errors are detected and for which some errors can be corrected.

Finally, fail-safe checker design for two-rail 2-of-3 valued systems is pursued. For this purpose, a new "safety factor" concept is defined; a new circuit for a 2-of-3 valued Exclusive-OR gate is given; and fault analysis for this circuit is presented.

VI. Acknowledgements

The authors are grateful for support from the Natural Sciences and Engineering Research Council of Canada and the Shanghai Institute of Railway Technology of the People's Republic of China.

VII. Glossary [2]

a) Mid-seeking fault: output is either correct or 1/2. b) Quasi-mid-seeking fault: output is correct or incorrect or 1/2. c) Mid-rejecting fault: output is correct or incorrect but never 1/2. d) Masked fault: output is always correct.

VIII. References

[1] Mou Hu and K.C. Smith, "On the Use of CMOS Ternary Gates to Realize a Self-Checking Binary Logic System", Proc. of the 11th International Symposium on Multiple-Valued Logic, pp. 212-217, May 1981.

[2] Mou Hu, K.C. Smith and H.T. Mouftah, "Low Power 2-of-3 Valued CMOS Self-Checking Circuits", Proc. of the 13th International Symposium on Multiple-Valued Logic, pp. 64-69, May 1983.

[3] Mou Hu and K.C. Smith, "A New Type of Self-Checking Synchronous Sequential Machine Based on 2-of-3 Valued Logic Circuits". Proc. of 12th

International Symposium on Multiple-Valued Logic, pp. 139-145, May 1982.

[4] D.A. Anderson, "Design of Self-Checking Digital Networks Using Coding Techniques", Tech. Rpt. R-527, Urbana, U of Illinois Coordinated Science Laboratory, 1971.

[5] J. Wakerly, "Error Detecting Codes, Self-Checking Circuits and Applications", Elsevier North-Holland, Inc., 1978.

[6] F.F. Sellers, Jr., Mu-Yue Hsiao, and L.W. Bearnson, "Error Detecting Logic for Digital Computers", McGraw-Hill Book Co., 1968.