Bounding Signal Probabilities in Combinational Circuits

G. Markowsky

Reprinted from
IEEE TRANSACTIONS ON COMPUTERS
Vol. C-36, No. 10, October 1987
out that can be used to estimate signal probabilities in all lines of the
original circuit.

Index Terms—Error detection, fault detection, random testing, signal
probability.

I. INTRODUCTION

The signal probability of a line is the proportion of all possible
inputs that produce a 1 on that line. It is easy to compute the signal
probability of all lines in a circuit that do not have reconvergent fan-
out using the standard dependence relations of probability theory such
as the ones given in Feller's book [1] or the ones given in Savir,
Ditlow, and Bardell's paper [2]. In particular, the signal probability
of the output line of an AND gate is the product of the signal
probabilities of the input lines. The signal probability of the output
line of an inverter (NOT gate) is the complement of the signal
probability of the input line, i.e., Prob(Out) = 1 − Prob(In). The
signal probability of the output of an OR gate is the complement of the
product of the complements of the signal probabilities of the input
lines. In other words,

\[ \text{Prob}(\text{Out}) = 1 - (1 - \text{Prob}(I_{n1}))(1 - \text{Prob}(I_{n2})) \cdots (1 - \text{Prob}(I_{nk})) \]

where \( I_{n1}, I_{n2}, \ldots, I_{nk} \) are the input lines. Throughout this paper,
NAND gates will be considered to be AND gates followed by a NOT
gate, and OR gates will be considered to be OR gates followed by a
NOT gate.

If the circuit has reconvergent fan-out, the problem is more
complicated, because the signal probabilities are not longer independ-
ent. As a consequence of this fact, Savir, Ditlow, and Bardell estimate
the signal probability of lines rather than calculate them
exactly. Such an approach suffices for their purposes since they only
need to bound the signal probabilities away from 0 and 1.

II. AN OUTLINE OF THE ALGORITHM

The following are the key steps in the Savir, Ditlow, and Bardell
algorithm.

1) Assign a lower and upper bound of 1/2 to each primary input of
the circuit. Each line in the circuit will be eventually have a lower and
upper bound so that its signal probability will lie between its two
bounds.

2) Use the rules for reconvergent fan-out-free circuits to propagate
lower and upper bounds as far as possible through the circuit. Thus,
when passing through an AND gate, the lower and upper bounds of the
output line are the products of the lower and upper bounds,
respectively, of the input lines. When passing through an inverter, the
lower and upper bounds of the output line are the complements of the
upper and lower bounds, respectively, of the input line. Finally,
when passing through an OR gate, the lower and upper bounds of the
output line are the complements of the products of the complements
of the lower and upper bounds, respectively, of the input lines.

3) Choose a minimal reconverging fan-out line. Minimal means
that no line feeding the line in question is a reconverging fan-out line.
If there is no minimal reconverging fan-out line, stop the algorithm
because every line now has correct lower and upper bounds. If there
is a minimal reconverging fan-out line, cut one of the reconverging
branches of the line and assign new lower and upper bounds
according to the rules in Section IV.

4) Goto Step 2.

The remainder of this paper fleshes out the sketch given above and
proves that the method works correctly.

III. CLASSES OF GATES

Definition 1: a) Let \( C \) be a circuit. A path from one point in the
circuit to another has odd parity if it goes through an odd number of
inverters or inverting gates. Otherwise, it has even parity.
b) Let \( p, q \) be two points on lines attached to the same fan-out
point, and let \( G \) be any gate which has two disjoint paths, \( P \) and \( Q \),
such that \( P \) starts at \( p \) and \( Q \) starts at \( q \), and they both meet for the first time as inputs to \( G \). Then, \( G \) is of Class 1 or Class 2 depending on the table in Fig. 1.

The simple circuit in Fig. 2 illustrates how Definition 1 is to be used. Note that gate \( G_2 \) in Fig. 2 becomes a Class 2 gate if \( p \) and \( q \) are switched. Also, a gate may belong to more than one class, such as gate \( G_4 \) in Fig. 2.

IV. CUTTING LINES

As long as a circuit has reconfigurable fan-out, Savir, Ditlow, and Bardell choose a minimal reconvergent fan-out line and cut one of the branches. We assume that all fan-out points have degree 2 since fan-out points of higher degree can be replaced by a series of points of degree 2. The cut branch is labeled with the point \( p \) and the uncut branch is labeled with the point \( q \). Assume that the lower and upper bounds at the fan-out point before the line was cut were \( L \) and \( U \), respectively, then the bounds assigned at point \( p \) are chosen as follows.

1) The bounds \([L, 1]\) are assigned if there are no Class 2 gates (relative to \( p \) and \( q \)) in the circuit.
2) The bounds \([0, U]\) are assigned if there are no Class 1 gates (relative to \( p \) and \( q \)) in the circuit.
3) The bounds \([0, 1]\) are assigned if there are both Class 1 and Class 2 gates in the circuit.

The rules given above are a simplification of the rules in [2], and are based on an observation of Journeau. Once the bounds are assigned to \( p \) they are used as independent values to create new bounds in all the tree-like parts of the circuit that result from cutting \( p \) away from \( q \).

V. BASIC PROOF TECHNIQUES

To prove that the Savir, Ditlow, and Bardell algorithm is correct requires that functions, rather than probabilities be assigned to lines. Our goal is to show that the algorithm preserves ordering relations among functions. The relations between bounds and signal probabilities follow directly.

To begin with, assume that each primary input line receives as a lower and upper bound the function represented by a single variable. Functions are assigned to all the lines throughout the entire circuit in the obvious way. For noninverting gates, lower bound functions for output lines are derived from the lower bound functions of input lines and upper bound functions of output lines are derived from upper bound functions of input lines in the obvious way using the appropriate logical operators. Of course, for inverting gates, the lower bounds of the output lines use the upper bounds of the input lines, and vice versa.

Boolean functions are partially ordered by the relation \( \leq \), where \( f \leq g \) if and only if \( f(w) = 1 \) implies that \( g(w) = 1 \) for all inputs \( w \) to the circuit. It is very easy to see that replacing a lower bound function by a function less than or equal to it, or replacing an upper bound function by a function that is greater than or equal to it, decreases lower bounds and increases upper bounds of all lines that are successors of that line.

We will first consider the substitution \([L, 1]\), which is allowed if there are no Class 2 gates. Fig. 3 motivates the subsequent work. Fig. 3(a) shows the circuit \( C \) before the minimal fan-out line is cut. Both points \( p \) and \( q \) have the functions \( Y \) as a lower bound and \( Z \) as an upper bound. Nothing is known about \( Y \) and \( Z \) except that \( Y \leq Z \), and \( \text{Prob}(Y) = L \) and \( \text{Prob}(Z) = U \), where \( \text{Prob}(F) \) is defined as the ratio of the number of inputs that make \( F \) to the total number of possible inputs for \( F \).

Fig. 3(b) shows the minimal fan-out line being cut, but the same bounds remain on the line emanating from \( p \). We call this circuit \( C^* \) to distinguish it from the circuit \( C \). Note that all the bounding functions are the same in \( C \) and \( C^* \).

In Fig. 3(c), the function \( Z \) at point \( p \) is replaced by the function 1, which is identically 1 for all inputs. Since \( Z \leq 1 \), it is clear that the new bounding functions can only enlarge the range on lines in the circuit.

Fig. 3(d) shows the final step which consists of replacing the function \( Y \) by a function \( X \) such that \( X \) is rewritten with completely new variables which appear nowhere else in the circuit and \( \text{Prob}(X) = \text{Prob}(Y) \).

Our plan is to show that the bounds in this stage are wider than the original, i.e., if \( e \) is a line in the circuit \( C \) and \( G_e \) and \( H_e \) are the lower and upper bound functions in Fig. 3(c) so that \( G_e \leq H_e \) and \( G^*_e \) and \( H^*_e \) are the corresponding bounding functions in Fig. 3(d), then we will show that

\[
\text{Prob}(G_e^*) \leq \text{Prob}(G_e) \leq \text{Prob}(H_e) \leq \text{Prob}(H_e^*).
\]

In Fig. 3(d), bounding functions are computed using \( X \), \( Y \), and \( Z \), and other variables, instead of using only \( Y \), \( Z \), and other variables as in Fig. 3(a)–(c).

To make Fig. 3(d) look like a conventional circuit one may imagine that the circuit feeding the point \( q \) has been duplicated for \( p \) so that totally new primary inputs are added. In particular, we assume that the function \( X \) is totally independent of the functions \( Y \) and \( Z \). It is important to note that the lower and upper bounds at point \( p \) are no longer derived from the lower and upper bounds of the input lines, but that throughout the rest of the circuit \( C^* \) lower bounds are derived from lower bounds and upper bounds are derived from upper bounds.

Fig. 3 applies only to circuits without Class 2 gates. A similar figure could be drawn for circuits without Class 1 gates. In such circuits, the lower bound \( Y \) at \( p \) would be replaced by 0 and the upper bound \( Z \) at \( p \) would be replaced by \( X \).

VI. THE XYZ REPRESENTATION

To study the effects of these replacements some simple results about Boolean functions involving \( X \), \( Y \), and \( Z \) are needed. To begin with, every Boolean function that has \( X \), \( Y \), and \( Z \) as inputs along with Boolean variables that are totally unrelated to these variables can be written uniquely in the form

\[
AXY + BXY'Z + CXZ' + DX'Y + EX'Y'Z + FX'Z'.
\]

We will call this form the XYZ representation of a function. Since \( Y \leq Z \), \( YZ = Y \), \( YZ' = Z' \), and \( Y' = 0 \), there are only six terms in the expression instead of eight as one might expect. Of course, \( A, B, C, D, E, \) and \( F \) are Boolean functions involving variables that do not occur in \( X \), \( Y \), and \( Z \).

In particular, in the notation just used, \( G_e(H_e) \) can be derived from \([G^*_e, H^*_e]\) by substituting \( Y \) for \( X \) in the expansion just described. To prove our main result requires that conditions be established under which substituting \( Y \) for \( X \) increases or decreases the probability of the resulting function. These conditions are given in Lemma 1.
Fig. 2. A simple illustration of definition 1.

Fig. 3. Stages in replacing bounds when there are no class 2 gates.

**Lemma 1:** Let $H(X, Y, Z) = AXY + BXY'Z + CXZ' + DX'Y + EX'Y'Z + FX'Z'$ where $A, B, C, D, E,$ and $F$ are the functions of Boolean variables that do not appear in $X, Y,$ or $Z$. Furthermore, assume that the Boolean variables that appear in $X$ do not appear in $Y$ or $Z$, and that $Y \leq Z$. Then the following are true.

1) If $\text{Prob}(X) = \text{Prob}(Y)$ and $A \geq D$

   $A + E \geq D + B$ (means OR)

   $AE \geq DB$ (Concatenation means AND)

   $A + F \geq D + C$

   $AF \geq DC$

   then $\text{Prob}(Y, Y, Z) \geq \text{Prob}(H(X, Y, Z))$.

2) If $\text{Prob}(X) = \text{Prob}(Y)$ and $A \leq D$

   $A + E \leq D + B$

   $AE \leq DB$

   $A + F \leq D + C$

   $AF \leq DC$

   then $\text{Prob}(Y, Y, Z) \leq \text{Prob}(H(X, Y, Z))$.

3) If $\text{Prob}(X) = \text{Prob}(Z)$ and $F \geq C$

   $F + A \geq C + D$

   $FA \geq CD$

   $F + B \geq C + E$

   $FB \geq CE$

   then $\text{Prob}(H(Z, Y, Z)) \geq \text{Prob}(H(X, Y, Z))$.

4) If $\text{Prob}(X) = \text{Prob}(Z)$ and

   $F \leq C$

   $F + A \leq C + D$

   $FA \leq CD$

   $F + B \leq C + E$

   $FB \leq CE$

   then $\text{Prob}(H(Z, Y, Z)) \leq \text{Prob}(H(X, Y, Z))$.

**Proof:**

1) Let $w = \text{Prob}(X) = \text{Prob}(Y)$. Then

   $\text{Prob}(H(Y, Y, Z)) = \text{Prob}(H(X, Y, Z))$

   $= w(1 - w) \text{Prob}(A) - \text{Prob}(D) + w \text{Prob}(Y'Z) \text{Prob}(E)$

   $- \text{Prob}(B) + w \text{Prob}(Z) \text{Prob}(F) - \text{Prob}(C)$

   $= w[\text{Prob}(Y'Z) \text{Prob}(A) + \text{Prob}(E) - (\text{Prob}(D) + \text{Prob}(B))]

   + \text{Prob}(Z) [\text{Prob}(A) + \text{Prob}(F) - (\text{Prob}(D) + \text{Prob}(C))]$

   The last equation follows because $1 - w = \text{Prob}(Y'Z) + \text{Prob}(Z')$. If (2)-(5) hold [(1) is not really needed for this], $\text{Prob}(A) + \text{Prob}(E) \geq \text{Prob}(D + B) + \text{Prob}(DB) = \text{Prob}(D) + \text{Prob}(B)$. Similarly, $\text{Prob}(A) + \text{Prob}(F) = \text{Prob}(A + F) + \text{Prob}(AF) \geq \text{Prob}(D + C) + \text{Prob}(DC) = \text{Prob}(D) + \text{Prob}(C)$. Since $w, \text{Prob}(Y'Z)$ and $\text{Prob}(Z')$ are all $\geq 0$, it follows that

   $\text{Prob}(H(Y, Y, Z)) \geq \text{Prob}(H(X, Y, Z))$

2) This proof can be derived from the proof of 1) just by reversing all the inequality signs.

3) Let $w = \text{Prob}(X) = \text{Prob}(Z)$, so that $1 - w = \text{Prob}(Z')$. 

Arguing as before we derive the equation

\[
\text{Prob}(H(Z, Y, Z)) - \text{Prob}(H(X, Y, Z)) = \left(1 - w\right)\left[\text{Prob}(Y) \left[\text{Prob}(A) + \text{Prob}(F) - \left(\text{Prob}(C) + \text{Prob}(D)\right)\right] + \text{Prob}(Y' \ Z) \left[\text{Prob}(B) + \text{Prob}(F) - \left(\text{Prob}(E) + \text{Prob}(C)\right)\right]\right]
\]

As in 1), it follows that \(\text{Prob}(F) + \text{Prob}(A) \geq \text{Prob}(C) + \text{Prob}(D)\) and that \(\text{Prob}(F) + \text{Prob}(B) \geq \text{Prob}(C) + \text{Prob}(E)\).

4) This is like 3) but with the direction of all inequality signs reversed.

VII. THE MAIN RESULT

Theorem 1: Let C be a circuit that has reconvergent fan-out. Pick a minimal reconverging fan-out point and label one reconverging line \(p\) and the other fan-out line \(q\). Assume that \(C\) does not contain any Class 2 gates. Cut the line containing \(p\) in \(C\) to get the circuit \(C^*\) as shown in Fig. 3, and compute all lower and upper bound functions in terms of \(X, Y,\) and \(Z\). Then substituting \(Y\) for \(X\) in every lower bound function cannot reduce the signal probability of the function and substituting \(Y\) for \(X\) in every upper bound function cannot increase the signal probability of the function. Thus, the bounds derived in \(C^*\) using an independent variable \(X\) are correct for the lines in \(C\).

Proof: More specifically, we will prove that the XYZ representations of all lower bound functions in \(C^*\) satisfy (1)–(5) of Lemma 1, while the XYZ representations of all upper bound functions satisfy (6)–(10) of Lemma 1.

The proof is by induction on the length of the longest path in \(C^*\) from either point \(p\) or point \(q\) to the line in question. Lines not descended from either \(p\) or \(q\) are considered to have distance 0.

Clearly, since the functions on all lines at distance 0 are independent of \(X, Y,\) and \(Z,\) the XYZ representations of both lower and upper bound functions have \(A = B = D = E = F\), so both (1)–(5) and (6)–(10) hold. The only lines at distance 1 are the lines starting at \(p\), which has bounds \([X, 1]\), and the line starting at \(q\), which has bounds \([Y, Z]\). Since the XYZ representations of \(X, Y,\) and \(Z\) are \((A = B = C = 1; D = E = F = 0), (A = D = 1; B = C = E = F = 0),\) and \((A = B = D = E = 1; C = F = 0),\) respectively, it is easy to check that the appropriate equations hold.

Now assume that for some line in \(C^*\) either the XYZ representation of the lower bound violates (1)–(5) or the XYZ representation of the upper bound violates (6)–(10). Let \(e\) be such a line that is at the shortest distance from \(p\) or \(q\). This means that for every line feeding into \(e,\) the XYZ representation of the bounds behave as required by the induction hypothesis. Since \(e\) is at the shortest distance, it is the output line of a gate and not the output of a fan-out point. Note that \(e\) is not the output of an inverter, since if the input line of an inverter has the desired properties, it is trivial to verify that the output line does too.

To simplify matters assume that \(e\) is the output line of an AND gate \(G\) with input lines \(i_1, i_2, \ldots, i_k.\) We shall shortly discuss how to handle OR gates and deal with other assumptions that we make for this case. Let \(L_1, L_2, \ldots, L_k\) be the lower bounds and \(U_1, U_2, \ldots, U_k\) be the upper bounds on the input lines \(i_1, i_2, \ldots, i_k.\) If \(L\) and \(U\) are the lower and upper bounds of \(e,\) then \(L = L_1 \cdot L_2 \cdot \ldots \cdot L_k\) and \(U = U_1 \cdot U_2 \cdot \ldots \cdot U_k.\) Assume further that \(U\) does not satisfy (6)–(10), but that each \(U_i\) does. Let \(A_i, B_i, C_i, D_i, E_i, F\) be the coefficients of the XYZ representation of \(U_i,\) and \(A, B, C, D, E, F\) be the coefficients of the XYZ representation of \(U.\) Clearly, we have that \(A = A_1 \cdot \ldots \cdot A_k,\) \(B = B_1 \cdot \ldots \cdot B_k,\) etc. Now if for all \(i, A_i \leq D_i,\) then \(A = D.\)

Similarly, if for all \(i, A_i \leq D_i,\) and \(A_i \leq D_i,\) then \(AE \subseteq DB\) and \(AF \subseteq DC.\) Thus, either (7) or (9) are the only ones that can be violated. Assume that (7) is violated. The proof for (9) is very similar and will be discussed shortly.

Thus, we have that for all \(i, A_i + E_i \subseteq D_i + B_i,\) but \(A + E \subseteq D + B.\) The last inequality implies that there is an assignment of values
because no line can have both types of properties. Thus, we have two disjoint paths. Note also that no primary input not feeding either \( p \) or \( q \) has either property since all coefficients in the \( XYZ \) representations of the bounding functions on these lines are equal. Thus, the two disjoint paths end at points \( p \) and \( q \). It is easy to check that point \( p \) has only the \( L = [AD\,DE] \) property while point \( q \) has only the \( L = [AB\,BE] \) property. Since line \( r \) has the \( U = [AB\,BE] \) property, the path from \( r \) to \( q \) has odd parity. By Definition 1, \( G \) is a Class 2 gate, contradicting the assumption that there were no Class 2 gates in \( C^* \).

We conclude this proof by describing the modifications needed for the cases not discussed above. First, if (7) holds, but (9) fails, you use \([AD\,CF]\) and \([AB\,BE]\) properties. Of course, in this case (9), (10), (4), and (5) are used instead of (7), (8), (2), and (3). Again, if \( U \) satisfied (6)–(10) but \( L \) does not satisfy (1)–(5), essentially the same proof goes through with (1)–(5) switched around and inequalities reversed. Finally, if \( G \) is an OR gate, (2), (4), (7), and (9) are switched with (3), (5), (8), and (10).

The result for Class 1 gates follows in the same manner as the result for Class 2 gates. This is stated as Theorem 2.

**Theorem 2:** Let \( C \) be a circuit that has reconvergent fan-out. Pick a minimal reconverging fan-out point and label one reconverging line \( p \) and the other fan-out line \( q \). Assume that \( C \) does not contain any Class 1 gates. Cut \( C \) to get the circuit \( C^* \) similar to the manner illustrated in Fig. 3, and compute all lower and upper bound functions in terms of \( X \), \( Y \), and \( Z \). Then substituting \( Z \) for \( X \) in every lower bound function cannot reduce the signal probability of the function and substituting \( Z \) for \( X \) in every upper bound function cannot increase the signal probability of the function. Thus, the bounds derived in \( C^* \) using an independent variable \( X \) are correct for the lines in \( C \).

**Proof:** This is the same as the proof of Theorem 1, but with (11)–(20) replacing (1)–(10).

Theorems 1 and 2 show that the Savir, Ditlow, and Bardell algorithm is correct.

**ACKNOWLEDGMENT**

I would like to thank J. Savir for drawing my attention to the problem of bounding signal probabilities. I would also like to thank the referees for numerous suggestions that went to improve the exposition of this paper.

**REFERENCES**
