On the Maximum Tolerable Noise for Reliable Computation by Formulas

William Evans*
will@cs.arizona.edu

Department of Computer Science
The University of Arizona
Tucson, AZ 85721-0077, USA

Nicholas Pippenger**
nicholas@cs.ubc.ca

Department of Computer Science
The University of British Columbia
Vancouver, BC V6T 1Z4, Canada

Abstract: It is shown that if a formula is constructed from noisy 2-input NAND gates, with each gate failing independently with probability ε, then reliable computation can or cannot take place according as ε is less than or greater than $\varepsilon_0 = (3-\sqrt{7})/4 = 0.08856\ldots$.

* This research was supported by an NSERC Canada International Fellowship.
** This research was supported by an NSERC Research Grant.

1. Introduction

By a *Boolean function* we shall mean an element of the free Boolean algebra on countably many generators $X_1, X_2, \ldots$. We shall identify a Boolean function f that belongs to the free Boolean algebra on $X_1, \ldots, X_n$ with the function $f : \{0,1\}^n \to \{0,1\}$ in the customary way.

By a *formula* we shall mean an element of the free algebra with one dyadic operation $|$ and two constants 0 and 1, generated by countably many variables $X_1, X_2, \ldots$. A formula F may be regarded as computing a Boolean function F_0 by interpreting the dyadic operation $|$ as the Boolean function NAND. Specifically, we regard the variable X_i in formulas as computing the corresponding generator X_i for Boolean functions; we regard the constants 0 and 1 in formulas as computing the corresponding constant functions; and if the formulas F and G compute the functions F_0 and G_0, then we regard the formula $F \mid G$ as computing the function $F_0 \mid G_0 = \neg(F_0 \wedge G_0)$. It is well known that every Boolean function is computed in this way by some formula (even by a formula not containing constants).

Our interest in this paper is in what von Neumann has called “probabilistic logics”, where in the computation scheme described above, each occurrence of the operation $|$ is assumed to fail independently with some probability ε. In this case we want to keep track not just of the Boolean values 0 and 1 but of their probabilities. To this end, we shall regard each formula F as computing a polynomial in the indeterminates $X_1, X_2, \ldots$ with real coefficients. We shall set $I = [0,1]$, and identify such a polynomial f with the corresponding function $F_\varepsilon : I^n \to I$. Specifically, we shall regard the variable X_i in formulas as computing the indeterminate X_i for polynomials; we shall regard the constants 0 and 1 in formulas as computing the corresponding constant polynomials; and if the formulas F and G compute the polynomials F_ε and G_ε, then we regard the formula $F \mid G$ as computing the polynomial $(1-\varepsilon) - (1-2\varepsilon)F_\varepsilon G_\varepsilon$. We observe that $F_\varepsilon(p_1, \ldots, p_n)$ is the probability that the formula $F(X_1, \ldots, X_n)$ produces the value 1 when each occurrence of the variable X_i independently assumes the value 1 with probability p_i, and when each gate fails independently with probability ε. We shall always assume that $\varepsilon > 0$, but we observe that if we take $\varepsilon = 0$ in the polynomial F_ε, and restrict its indeterminates to Boolean values, it assumes only Boolean values and agrees with the Boolean function F_0.

Let $\delta_0 > 0$ and $\delta_1 > 0$ be such that $\delta_0 + \delta_1 < 1$ (or equivalently $\delta_0 < 1 - \delta_1$). Let $I_0 = [0, \delta_0]$ and $I_1 = [1-\delta_1, 1]$. We shall say that the formula F $(\varepsilon, \delta_0, \delta_1)$*-computes* the Boolean function f if, for every $x_1, \ldots, x_n \in \{0,1\}$, we have

$$F_\varepsilon(I_{x_1}, \ldots, I_{x_n}) \subseteq I_{f(x_1, \ldots, x_n)}. \tag{1.1}$$

A few words about this definition are in order. Firstly, we have adopted separate bounds δ_0 and δ_1 to the probabilities of error for 0 and 1. Most previous work has adopted a single bound $\delta = \delta_0 = \delta_1$ (so that the condition $\delta_0 + \delta_1 < 1$ becomes $\delta < 1/2$). But this previous work has dealt largely with "self-dual" situations, wherein 0 and 1 play symmetric roles. Our situation is not self-dual: the dual of a NAND gate is a NOR gate, and separate bounds δ_0 and δ_1 seem both natural and necessary to obtain the sharpest results. Secondly, we assume "soft inputs". By requiring (1.1) rather than merely

$$F_\varepsilon(x_1, \ldots, x_n) \subseteq I_{f(x_1,\ldots,x_n)}, \tag{1.2}$$

we are allowing the occurrences of variables in the formula to be independently erroneous observations of the corresponding arguments, with the same error bounds δ_0 and δ_1 that apply to the output of the formula. Most previous work has assumed "hard inputs" by requiring only (1.2). But our definition has an important advantage. The Boolean functions that are $(\varepsilon, \delta_0, \delta_1)$–computable form a *clone*; that is, they include the projection functions $f(X_1, \ldots, X_n) = X_i$ (this is true for any reasonable definition) and they are closed under composition (this is an immediate consequence of (1.1)). The clones of Boolean functions have been completely classified; see Post [P2].

The case in which computation is to be done by noisy NAND gates is one considered by von Neumann [N]. He was considering circuits rather than formulas, and he was employing different input-output conventions (using bundles of wires rather than single wires), so his quantitative results are not strictly comparable to ours. But a straightforward adaptation to NAND gates of an argument he gives for formulas using MAJORITY gates shows that reliable computation is possible if $\varepsilon < (3\sqrt{22} - 14)/6 = 0.01187\ldots$. We do not know of any larger lower bound to the threshold in the literature.

Pippenger [P1] showed that formulas in which all gates have at most k inputs cannot compute reliably unless $\varepsilon \le (1 - 1/k)/2$, and Evans and Schulman [ES1] improved this bound to $\varepsilon \le (1 - 1/\sqrt{k})/2$. For $k = 2$, these results give upper bounds to the threshold of $1/4 = 0.25$ and $(1 - 1/\sqrt{2})/2 = 0.1464\ldots$.

Hajek and Weller [HW] showed that for $k = 3$, the threshold is exactly $1/6$, and Evans and Schulman [ES2] (see also Evans [E], Chapter 5) generalized this result to $\left(1 - 2^{k-1}/k\binom{k-1}{\frac{k-1}{2}}\right)/2$ for all odd $k \ge 3$. (This generalized expression gives 0 for $k = 1$. This might be taken as correct in some sense, since it is is not possible to perform computation, even in the absence of noise, when all gates have at most one input.)

In this paper we shall prove the following two results. Let $\varepsilon_0 = (3 - \sqrt{7})/4 = 0.08856\ldots$.

Theorem 1.1: Suppose $\varepsilon < \varepsilon_0$, and define x_-, x_0 and x_+ by

$$x_0 = \frac{-1 + \sqrt{(1-\varepsilon)(1-2\varepsilon)+1}}{2(1-2\varepsilon)}$$

and

$$x_\pm = \frac{1 \pm \sqrt{4(1-\varepsilon)(1-2\varepsilon)-3}}{2(1-2\varepsilon)}.$$

Then if δ_0 and δ_1 satisfy

$$x_- < \delta_0 < x_0 < 1 - \delta_1 < x_+,$$

every Boolean function can be $(\varepsilon, \delta_0, \delta_1)$–computed by some formula.

This theorem will be proved in Section 2 by methods similar in spirit to, but much more elaborate than, those originally used by von Neumann [N].

We shall say that a Boolean function $f : \{0,1\}^n \to \{0,1\}$ *depends essentially* on its i-th argument (where $1 \le i \le n$) if there exist Boolean constants $c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n$ such that $f(c_1, \ldots, c_{i-1}, 0, c_{i+1}, \ldots, c_n) \ne f(c_1, \ldots, c_{i-1}, 1, c_{i+1}, \ldots, c_n)$. We note that a function that depends essentially on at most one argument must be a projection function, a complement function (that is, the complement of a projection function), or a constant function.

Theorem 1.2: If $\varepsilon > \varepsilon_0$ and $\delta_0 + \delta_1 < 1$, then any Boolean function that is $(\varepsilon, \delta_0, \delta_1)$–computed by a formula essentially depends on at most one argument.

This theorem will require the introduction of new methods in Section 3. These methods are related to those of Hajek and Weller [HW] and those of Evans and Schulman [ES2], but it does not appear that either the new methods or the old can reproduce the results of the other.

2. Lower Bound

We shall begin with a crude argument that shows that reliable computation is possible if $\varepsilon < (3\sqrt{22} - 14)/6 = 0.01187\ldots$. This result is due in essence to von Neumann [N], though he does not state it explicitly. In his discussion of computation with NAND gates, he states a slightly weaker result, but he is employing a different model at that point, and his results are strictly speaking incomparable to the ones presented here. But the bound of $(3\sqrt{22} - 14)/6$, which we shall present as Theorem 2.1, results from adapting to NAND gates precisely the arguments that von Neumann gives for 3-input MAJORITY gates.

Theorem 2.1: If $\varepsilon < (3\sqrt{22} - 14)/6$ and

$$\frac{1 - \sqrt{1 - 72\varepsilon}}{12} < \delta < \frac{1 + \sqrt{1 - 72\varepsilon}}{12},$$

then every Boolean function can be $(\varepsilon, \delta, \delta)$-computed by some formula.

Proof: Consider an arrangement of 3 NAND gates in a balanced binary tree of depth 2, with 4 inputs. Suppose that each of the inputs assumes some Boolean value X, except that the inputs may each independently be in error with probability at most ϑ. Suppose further that each of the 3 gates correctly computes the NAND, except that each gate may independently fail with probability at most ε. Then, except with probability at most 3ε, this arrangement computes the OR of the ANDs of its two pairs of inputs, and this will be the value X unless at least 2 of the 4 inputs are in error, which happens with probability at most $\binom{4}{2}\vartheta^2 = 6\vartheta^2$. Thus if $3\varepsilon + 6\vartheta^2 < \vartheta$, this arrangement may be used to reduce error levels from ϑ at its inputs to $3\varepsilon + 6\vartheta^2$ at its output. Since $3\varepsilon + 6\vartheta^2$ is convex in ϑ, its graph lies below that of ϑ in the interval (x_-, x_+) bounded by the two solutions of $3\varepsilon + 6\vartheta^2 < \vartheta$, which are given by $x_\pm = (1 \pm \sqrt{1 - 72\varepsilon})/12$.

Suppose now that $\delta \in (x_-, x_+)$. Since the set of $(\varepsilon, \delta, \delta)$-computable Boolean functions forms a clone, and since NAND function generates the clone of all Boolean functions, it will suffice to show that the NAND function is $(\varepsilon, \delta, \delta)$-computable. Consider now a single NAND gate. Suppose that its inputs assume the values X and Y, except that each input may independently be in error with probability at most α. Suppose further that the gate correctly computes the NAND function, except that it may fail with probability at most ε. The gate will produce the NAND of X and Y, except with probability at most $2\alpha + \varepsilon$.

Now if $\varepsilon < (3\sqrt{22} - 14)/6$, then we can choose $\alpha_0 > x_-$ such that $2\alpha_0 + \varepsilon < x_+$ (indeed, the threshold $(3\sqrt{22} - 14)/6$ was determined by finding the value of ε for which $2x_- + \varepsilon = x_+$). By repeated use of the error-reducing arrangement described above, we can reduce the errors at the inputs from δ to at most α_0; a NAND gate will increase the error to at most $2\alpha_0 + \varepsilon < x_+$; and further repeated use of the error-reducing arrangement will restore the error in the output to at most δ. △

Our main lower bound, Theorem 1.1, is obtained by stretching every last bit of slack from the argument given above. (That we have indeed gotten the last bit out is of course shown by the matching upper bound in the next section.) A key feature of the tightened argument is that it is no longer possible merely to argue with upper bounds to probabilities of failure and error. We shall be relying on effects whereby errors cancel each other out, so we shall also need exact values for probabilities of failure and lower bounds to probabilities of error. This type of argument first appears in the work of Hajek and Weller [HW] (Section IV, Proposition 3). A consequence of this style of argument is that the constructed formulas may suffer increased probability of error, for certain inputs, if their gates enjoy a decreased probability of failure.

Theorem 1.1: Suppose $\varepsilon < \varepsilon_0$, and define x_-, x_0 and x_+ by

$$x_0 = \frac{-1+\sqrt{4(1-\varepsilon)(1-2\varepsilon)+1}}{2(1-2\varepsilon)}$$

and

$$x_\pm = \frac{1 \pm \sqrt{4(1-\varepsilon)(1-2\varepsilon)-3}}{2(1-2\varepsilon)}.$$

Then if δ_0 and δ_1 satisfy

$$x_- < \delta_0 < x_0 < 1-\delta_1 < x_+,$$

every Boolean function can be $(\varepsilon, \delta_0, \delta_1)$–computed by some formula.

We begin by considering the formula $F(X) = X \mid X$, with polynomial $F_\varepsilon(X) = (1-\varepsilon) - (1-2\varepsilon)X^2$. We shall be interested in analyzing the composition of F with itself. This analysis is simplified by a renormalization: set $\zeta = (1-\varepsilon)(1-2\varepsilon)$ and $\Phi(X) = \zeta - X^2$. We then have $F_\varepsilon(X) = \Phi\big((1-2\varepsilon)X\big)/(1-2\varepsilon)$, so that the problem of composing F_ε with itself is transformed into that of composing Φ with itself. (This transformation may be thought of as scaling certain probabilities by a factor of $(1-2\varepsilon)$.) We observe that the condition $0 < \varepsilon < \varepsilon_0$ corresponds to the condition $3/4 < \zeta < 1$.

To study the iteration of Φ, we begin by finding its fixed points, which are the roots of the equation $\Phi(X) = X$. These are

$$\xi_0 = \frac{-1+\sqrt{1+4\zeta}}{2},$$
$$\xi_1 = \frac{-1-\sqrt{1+4\zeta}}{2}.$$

The fixed point ξ_1 is negative, and thus does not correspond to a scaled probability; it will not concern us further. The fixed point ξ_0 is the one we are interested in. The derivative of Φ there is negative: we have $\Phi'(\xi_0) = -\eta$, where $\eta = 2\xi_0 = -1+\sqrt{1+4\zeta}$. Conversely, $\zeta = \eta/2 + \eta^2/4$. We observe that the condition $0 < \varepsilon < \varepsilon_0$ corresponds to the condition $1 < \eta < \sqrt{5}-1$.

Next consider the formula $G(X) = (X \mid X) \mid (X \mid X)$. Since $G(X) = F\big(F(X)\big)$, the corresponding polynomial is $G_\varepsilon(X) = F_\varepsilon\big(F_\varepsilon(X)\big)$ or, after renormalization $\Psi(X) =$

$\Phi\big(\Phi(X)\big) = \zeta - (\zeta - X^2)^2$. We shall be interested in the fixed points of Ψ, which are the roots of the equation $\Psi(X) = X$. These are four in number (counted according to multiplicity). Two of them, ξ_0 and ξ_1, are inherited from Φ, and are thus the roots of the polynomial $X - \Phi(X) = X^2 + X - \zeta$. The remaining two are therefore the roots of the polynomial $\big(X - \Psi(X)\big)/(X^2 + X - \zeta) = X^2 - X + (1 - \zeta)$. The discriminant of this quadratic is $4\zeta - 3$. Thus if $0 < \varepsilon < \varepsilon_0$, so that $3/4 < \zeta < 1$, the two additional fixed points ξ_- and ξ_+ of Ψ are real and distinct:

$$\xi_\pm = \frac{1 \pm \sqrt{4\zeta - 3}}{2}.$$

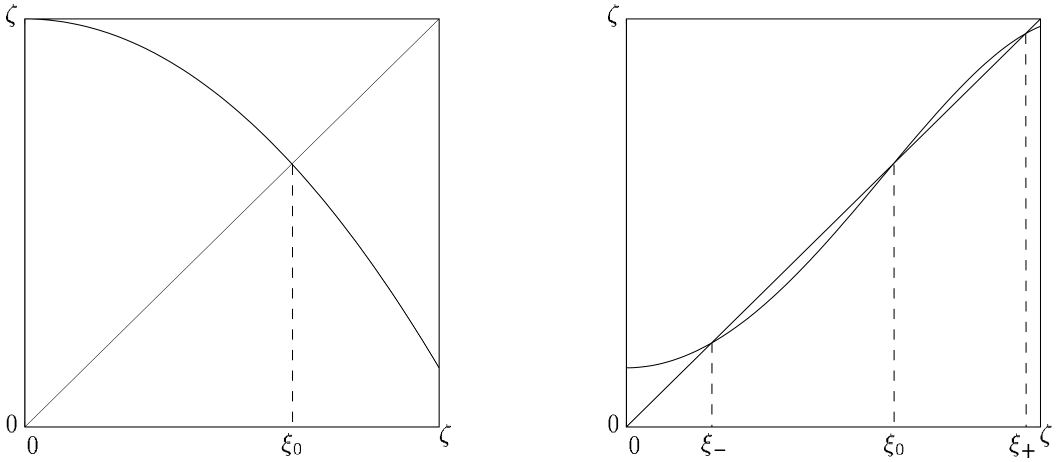

Figure 1: The functions Φ and Ψ and their fixed points ($\varepsilon = 0.05$).

Now the derivative of Ψ at ξ_0 is, by the chain rule, $\Psi'(\xi_0) = \Phi'\big(\Phi(\xi_0)\big)\,\Phi'(\xi_0) = (-\eta)^2 = \eta^2 > 1$. Thus the graph of Ψ crosses the diagonal from below to above at ξ_0. Since this graph begins above the diagonal at 0 (note that $\Psi(0) = \zeta - \zeta^2 > 0$, since $\zeta < 1$), and is again below the diagonal at ζ (note that $\Psi(\zeta) = \zeta - (\zeta - \zeta^2)^2 < \zeta$, since $\zeta - \zeta^2 > 0$), the graph must cross the diagonal from above to below at remaining fixed points ξ_- and ξ_+. In particular, we must have

$$0 < \xi_- < \xi_0 < \xi_+ < 1 - 2\varepsilon,$$

as well as $\Psi'(\xi_-) < 0$ and $\Psi'(\xi_+) < 0$.

At this point we have a qualitative picture of the behavior of Ψ under iteration. The polynomial Ψ has a repulsive fixed point at ξ_0 and attractive fixed points at ξ_- and ξ_+.

The interval $[0, \xi_0)$ is the basin of attraction of ξ_-; thus any point in this interval converges under iteration to ξ_-. Similarly, the interval $(\xi_0, 1-2\varepsilon]$ is the basin of attraction of ξ_+. The convergence in either case is uniform on compact sets, so we have the following proposition.

Proposition 2.2: If $I_- \subseteq [0, \xi_0)$ and $I_+ \subseteq (\xi_0, 1-2\varepsilon]$ are closed intervals, and J_- and J_+ are closed intervals such that $\xi_- \in J_-$ and $\xi_+ \in J_+$, then there exists a natural number L such that

$$\Psi^{(L)}(I_-) \subseteq J_-$$

and

$$\Psi^{(L)}(I_+) \subseteq J_+,$$

where $\Psi^{(L)}$ denotes the L-th iterate of Ψ.

Proposition 2.2 will be used to reduce errors. To accomplish computation we shall need to analyze the formula $H(X, Y) = X \mid Y$, corresponding to the polynomial $H_\varepsilon(X, Y) = (1-\varepsilon) - (1-2\varepsilon)XY$ or, after renormalization, $\Omega(X, Y) = \zeta - XY$.

Proposition 2.3: There exist closed intervals J_- and J_+ such that

$$\xi_- \in J_- \subseteq [0, \xi_0)$$

and

$$\xi_+ \in J_+ \subseteq (\xi_0, 1-2\varepsilon],$$

and I_+ such that

$$\xi_+ \in I_+ \subseteq (\xi_0, 1-2\varepsilon],$$

and such that

$$\Omega(J_-, J_+) \subseteq I_+.$$

Proof: Since ξ_- and ξ_+ are roots of the monic polynomial $X^2 - X + (1-\zeta)$, we have $\xi_- \, \xi_+ = 1 - \zeta = 1 - \eta/2 - \eta^2/4$. Since ξ_0 is a root of the polynomial $X^2 + X - \zeta$, we have $\xi_0^2 = \zeta - \xi_0 = (\eta/2 + \eta^2/4) - \eta/2 = \eta^2/4$. Thus we have $\xi_0^2 - \xi_- \, \xi_+ = \eta^2/2 + \eta/2 - 1 > 0$, since $\eta > 1$. This yields

$$\Omega(\xi_-, \xi_+) > \Phi(\xi_0) = \xi_0.$$

By continuity, Ω maps points (X, Y) with X sufficiently close to ξ_- and Y sufficiently close to ξ_+ into the basin of attraction of x_+. $\triangle$

We are now ready to prove Theorem 1.1. We first note that the quantities x_0, x_- and x_+ defined there are, after renormalization, the fixed points ξ_0, ξ_- and ξ_+.

As in the proof of Theorem 2.1, it will suffice to show that the NAND function is $(\varepsilon, \delta_0, \delta_1)$–computable.

By virtue of Proposition 2.3, we can find $\alpha > 0$ sufficiently small that, if we set $J_- = [\xi_- - \alpha, \xi_- + \alpha]$, $J_+ = [\xi_+ - \alpha, \xi_+ + \alpha]$, $I_- = [0, \xi_0 - \alpha]$ and $I_+ = [\xi_0 + \alpha, 1 - 2\varepsilon]$, then we have

$$\Omega(J_-, J_+) \subseteq I_+.$$

By the symmetry of Ω, we have

$$\Omega(J_+, J_-) \subseteq I_+.$$

We can also ensure, by decreasing α if necessary, that

$$\Omega(J_-, J_-) \subseteq I_+$$

and

$$\Omega(J_+, J_+) \subseteq I_-.$$

(This follows from the continuity of Ω and the identities $\Omega(\xi_-, \xi_-) = \Phi(\xi_-) = \xi_+$ and $\Omega(\xi_+, \xi_+) = \Phi(\xi_+) = \xi_-$.)

Let $\beta_0 = (1 - 2\varepsilon)\delta_0$ and $\beta_1 = (1 - 2\varepsilon)(1 - \delta_1)$ be the renormalized versions of δ_0 and $1 - \delta_1$. By virtue of Proposition 2.2, we can find L sufficiently large that, if we set $K_- = [0, \beta_0]$ and $K_+ = [\beta_1, 1 - 2\varepsilon]$, then we have

$$\Psi^{(L)}(K_-) \subseteq J_-$$

and

$$\Psi^{(L)}(K_+) \subseteq J_+.$$

We can also ensure, by increasing L if necessary, that

$$\Psi^{(L)}(I_-) \subseteq K_-$$

and

$$\Psi^{(L)}(I_+) \subseteq K_+.$$

These four inclusions, taken together with the four in the preceding paragraph, imply that the formula $G^{(L)}\big(H\big(G^{(L)}(X), G^{(L)}(Y)\big)\big)$ $(\varepsilon, \delta_0, \delta_1)$–computes the NAND function $X \mid Y$. $\triangle$

It is clear that as ε tends to ε_0, the parameter L in the proof of Theorem 1.1 tends to infinity. It is of some interest to consider the rate of growth of L in this situation, as it corresponds roughly to the factor by which the depth of reliable formulas with noise exceed the depth of formulas without noise. We shall not attempt to state or prove a precise result, but merely sketch an analysis of the situation.

Let us set $\sigma = \varepsilon_0 - \varepsilon$. Then the equation $\zeta = (1-\varepsilon)(1-2\varepsilon)$ yields $\zeta = 3/4 + \Theta(\sigma)$. The equation $\eta = -1 + \sqrt{1+4\zeta}$ yields $\eta = 1 + \Theta(\sigma)$. The critical case is that in which the two inputs of a NAND gate have opposite values. From the proof of Proposition 2.3 we have $\xi_0^2 - \xi_-\xi_+ = \eta/2 + \eta^2/2 - 1 = \Theta(\sigma)$. Since the partial derivatives of $\Omega(X,Y)$ at $X = \xi_-$ and $Y = \xi_+$ are $\Theta(1)$, we must take $\alpha = \Theta(\sigma)$ in order to have $\Omega(\xi_- + \alpha, \xi_+ - \alpha) \geq \xi_0 + \alpha$. Since the distance $\xi_+ - \xi_0 = \Theta(\sqrt{4\zeta - 3}) = \Theta(\sqrt{\sigma})$ is large compared with $\alpha = \Theta(\sigma)$, the value of L will be determined by the number of iterations of Ψ needed to increase the distance $X - \xi_0$ from a value of order $\Theta(\sigma)$ to one of order $\Theta(\sqrt{\sigma})$. Since each application of Ψ increases this distance by a factor of about $\Psi'(\xi_0) = \eta^2 = 1 + \Theta(\sigma)$, we must take

$$L = \Theta\left(\frac{1}{\sigma}\log\frac{1}{\sigma}\right) = \Theta\left(\frac{1}{\varepsilon_0 - \varepsilon}\log\frac{1}{\varepsilon_0 - \varepsilon}\right).$$

3. Upper Bound

In this section we shall show that the construction given in the proof of Theorem 1.1 is the best possible, in the sense that no construction can yield a larger threshold. We do this by proving Theorem 1.2, which we restate here.

Theorem 1.2: If $\varepsilon > \varepsilon_0$ and $\delta_0 + \delta_1 < 1$, then any Boolean function that is $(\varepsilon, \delta_0, \delta_1)$–computed by a formula essentially depends on at most one argument.

Since the set of $(\varepsilon, \delta_0, \delta_1)$–computable Boolean functions forms a clone, and since every Boolean function that depends essentially on more than one variable generates a clone that contains functions depending on arbitrarily many variables, Theorem 1.2 will follow from the following theorem.

Theorem 3.1: For every $\varepsilon > \varepsilon_0$ and $\delta_0 + \delta_1 < 1$, there exists a natural number n such that any Boolean function that is $(\varepsilon, \delta_0, \delta_1)$–computed by a formula essentially depends on fewer than n arguments.

For every formula F, we shall define the *rank* $\varrho(F)$ to be the length of the shortest path (that is, the minimum number of gates on a path) from an occurrence of a variable to the root in F (with the understanding that this is ∞ if there is no occurrence of a variable); thus, $\varrho(F)$ is defined by induction on the structure of F by (1) $\varrho(X_i) = 0$ for each variable X_i, (2) $\varrho(c) = \infty$ for each constant $c \in \{0,1\}$, and (3) $\varrho(F \mid G) = 1 + \min\{\varrho(F), \varrho(G)\}$.

We shall now use an argument first presented by Pippenger [P1] to reduce the problem of formulas reliably computing functions with many arguments to the problem of formulas with large rank reliably computing functions of a single argument.

Consider a formula F on the variables $X_1, \ldots, X_n$. Associate with each occurrence A of a variable X_i in F the length $\ell(A)$ from A to the root in F, and the *weight* $\lambda(A) = 2^{-\ell(A)}$. Clearly, the sum of the weights of all occurrences of variables in F is at most 1. Let Λ_i denote the sum of the weights of the occurrences of the variable X_i. Then $\sum_{1 \leq i \leq n} \Lambda_i \leq 1$, so there must exist some i in the range $1 \leq i \leq n$ such that $\Lambda_i \leq 1/n$. For any occurrence A of X_i in F, we have $\lambda(A) \leq \Lambda_i \leq 1/n$, and thus $\ell(A) \geq \log_2 n$.

Suppose now that F $(\varepsilon, \delta_0, \delta_1)$–computes a Boolean function f that essentially depends on the n arguments $X_1, \ldots, X_n$. In particular, f essentially depends on X_i. Then there exist Boolean constants $c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n$ such that $g(X) = f(c_1, \ldots, c_{i-1}, X, c_{i+1}, \ldots, c_n)$ essentially depends on X (and thus is either the projection function $g(X) = X$ or the complement function $g(X) = \neg X$). Since the constants 0 and 1 are formulas that $(\varepsilon, \delta_0, \delta_1)$–compute the Boolean constant functions, the formula $G(X) = F(c_1, \ldots, c_{i-1}, X, c_{i+1}, \ldots, c_n)$ $(\varepsilon, \delta_0, \delta_1)$–computes $g(X)$. And since all occurrences A of X_i in satisfy $\ell(A) \geq \log_2 n$, we have $\varrho(G) \geq \log_2 n$. Thus Theorem 3.1 will follow from the following theorem.

Theorem 3.2: For every $\varepsilon > \varepsilon_0$ and $\delta_0 + \delta_1 < 1$, there exists a natural number $k \geq 1$ such that any formula that $(\varepsilon, \delta_0, \delta_1)$–computes a projection function or a complement function has rank less than k.

To prove this theorem, we observe that if a formula G $(\varepsilon, \delta_0, \delta_1)$–computes a projection function or a complement function, then $G_\varepsilon(\delta_0)$ and $G_\varepsilon(1 - \delta_1)$ must differ by at least $1 - \delta_0 - \delta_1 > 0$. Thus it will suffice to establish a bound to $|G_\varepsilon(\delta_0) - G_\varepsilon(1 - \delta_1)|$ that tends to zero as $\varrho(G)$ tends to infinity.

To do this, we shall use the inequality

$$|G_\varepsilon(\delta_0) - G_\varepsilon(1 - \delta_1)| \leq \int_{\delta_0}^{1-\delta_1} |G'_\varepsilon(X)| \, dX,$$

where the prime denotes differentiation with respect to X. Since $\varrho(G) \geq 1$, G contains at least one gate, which implies that $\varepsilon \leq G_\varepsilon(X) \leq 1 - \varepsilon$ for all $0 \leq X \leq 1$. Since G $(\varepsilon, \delta_0, \delta_1)$–computes some function, we must have $\delta_0 \geq \varepsilon$ and $\delta_1 \geq \varepsilon$. Since $\delta_0 \geq 0$ and $1 - \delta_1 \leq 1 - \varepsilon$, we have

$$\int_{\delta_0}^{1-\delta_1} |G'_\varepsilon(X)| \, dX \leq \int_{0}^{1-\varepsilon} |G'_\varepsilon(X)| \, dX.$$

Letting Ψ denote the renormalized version of G_ε as in Section 2, we have

$$G_\varepsilon(X) = \Psi\big((1-2\varepsilon)X\big)/(1-2\varepsilon).$$

Using $\zeta = (1-\varepsilon)(1-2\varepsilon)$, we obtain

$$\int_0^{1-\varepsilon} |G_\varepsilon'(X)|\, dX = \frac{1}{1-2\varepsilon}\int_0^{\zeta} |\Psi_\varepsilon'(X)|\, dX$$

$$\leq \left(\frac{\zeta}{1-2\varepsilon}\right) \sup_{0\leq X\leq \zeta} |\Psi_\varepsilon'(X)|.$$

Thus it will suffice to establish a bound to $|\Psi_\varepsilon'(X)|$ that tends to zero uniformly for $0 \leq X \leq \zeta$ as $\varrho(G)$ tends to infinity.

To do this, we shall define a "Tent Function" $\phi : [0,\zeta] \to [1-\eta, 1]$ (where $\eta = -1+\sqrt{1+4\zeta}$, so that $\zeta = \eta/2 + \eta^2/4$, as in the proof of Theorem 1.1) by

$$\phi(x) = \begin{cases} (1-\eta) + 2x, & x \in [0, \eta/2]; \\ 1 - 2(2x-\eta)/\eta, & x \in [\eta/2, \zeta]. \end{cases}$$

This function rises linearly from a minimum of $1-\eta$ at 0 to a maximum of 1 at $\eta/2$, then falls linearly back to $1-\eta$ at ζ. We shall need the following "Tent Lemma".

Lemma 3.3: If $\eta < 1$, then

$$x\,\phi(y) + y\,\phi(x) \leq \eta\,\phi(\zeta - xy)$$

for all $x, y \in [0, \zeta]$.

The proof of this lemma is technical and will be deferred to an appendix (Section 6). Here we shall use it to complete the proof of Theorem 3.2.

Let G be any formula. We shall show that

$$|\Psi'(X)| \leq \phi\big(\Psi(X)\big)\, \eta^{\varrho(G)}/(1-\eta). \tag{3.1}$$

Since $\eta < 1$, this will complete the proof of Theorem 3.2.

We first observe that if $\varrho(G) = \infty$, then G contains no occurrences of the variable X, so $\Psi'(X) = 0$. On the right-hand side, we have $0 \leq \Psi(X) \leq \zeta$, so $\phi\big(\Psi(X)\big) \geq 1-\eta$, and we may agree that $\eta^\infty = 0$. For the rest, we shall show by induction on k that if $\varrho(G) \geq k$, then

$$|\Psi'(X)| \leq \phi\big(\Psi(X)\big)\, \eta^k/(1-\eta). \tag{3.2}$$

If $k = 0$, then G is an occurrence of the variable X, so $\Psi'(X) = 1$. On the right-hand side, we have $0 \leq \Psi(X) \leq \zeta$, so $\phi\big(\Psi(X)\big) \geq 1-\eta$, and we may agree that $\eta^0 = 1$. If $k \geq 1$, then G is of the form $C \mid D$ for some formulas C and D with $\varrho(C) \geq k-1$ and $\varrho(D) \geq k-1$. Letting Γ and Δ be denote the renormalized versions of C_ε and D_ε, we have

$$|\Gamma'(X)| \leq \phi\big(\Gamma(X)\big)\, \eta^{k-1}/(1-\eta) \tag{3.3}$$

and

$$|\Delta'(X)| \leq \phi\big(\Delta(X)\big)\, \eta^{k-1}/(1-\eta) \tag{3.4}$$

by inductive hypothesis. We have $\Psi(X) = \zeta - \Gamma(X)\,\Delta(X)$, so that $\Psi'(X) = -\big(\Gamma'(X)\,\Delta(X) + \Gamma(X)\,\Delta'(X)\big)$, and therefore

$$|\Psi'(X)| \leq |\Gamma'(X)|\,\Delta(X) + \Gamma(X)\,|\Delta'(X)|.$$

Applying the inductive hypotheses (3.3) and (3.4) and using Lemma 3.3 yields (3.2) and therefore (3.1). △

4. Conclusion

There are three obvious ways in which the upper bound we have established might be strengthened. Firstly, we have assumed that all gates are NAND gates. Of course, if one seeks to compute all Boolean functions with two-input gates of a single type, one must use either NAND gates or NOR gates (to which, by duality, our result also applies). But we do not know how to increase the threshold by using other two-input gates, and we conjecture that the same threshold applies to formulas in which gates may compute various two-argument functions in any combination. Secondly, we have assumed "soft inputs"; that is, we have assumed that the arguments of the function being computed by a formula are only available in noisy versions that may be as unreliable as the formula itself. Of course, this assumption has the attractive feature of making the class of reliably-computable functions closed under composition. But most previous upper bounds to reliable computation hold even with "hard inputs", and we conjecture that the same threshold applies to formulas for which the inputs are completely reliable. Thirdly, we have dealt with formulas rather than circuits. But most previous upper bounds to reliable computation were eventually shown to apply even for circuits, and we conjecture that the same threshold applies to circuits.

The reader may have noticed that our arguments do not address the question of whether reliable computation is possible when the failure probability is exactly equal to the threshold. We conjecture that it is not, but the argument given in Section 3 breaks down in this case, and we have not found a method to replace it.

Finally, for the range of failure probability where reliable computation is possible, it would be of interest to determine whether the factor by which the depth of formulas is increased has the order of growth discussed at the end of Section 2.

5. References

[E] W. S. Evans, *Information Theory and Noisy Computation*, Ph. D. Thesis, Computer Science, University of California, Berkeley, 1994.

[ES1] W. Evans and L. J. Schulman, "Signal Propagation, with Application to a Lower Bound on the Depth of Noisy Formulas", *Proc. IEEE Symp. on Foundations of Comp. Sci.*, 34 (1993) 594–599.

[ES2] W. Evans and L. J. Schulman, "Information Theory and Noisy Computation", *Proc. 1995 IEEE Internat. Symp. on Info. Theory*, 456.

[HW] B. Hajek and T. Weller, "On the Maximum Tolerable Noise for Reliable Computation by Formulas", *IEEE Trans. Info. Theory*, 37 (1991) 388–391.

[N] J. von Neumann, "Probabilistic Logics and the Synthesis of Reliable Organisms from Unreliable Components", in: C. E. Shannon and J. McCarthy (editors), *Automata Studies*, Princeton University Press, 1956, pp. 43–98.

[P1] N. Pippenger, "Reliable Computation by Formulas in the Presence of Noise", *IEEE Trans. Info. Theory*, 34 (1988) 194–197.

[P2] E. L. Post, *The Two-Valued Iterative Systems of Mathematical Logic*, Princeton University Press, Princeton, NJ, 1941.

6. Appendix: Proof of the Tent Lemma

Lemma 3.3: Suppose $0 < \eta < 1$, and set $\zeta = \eta/2 + \eta^2/4$. Define $\phi : [0, \zeta] \to [1-\eta, 1]$ by

$$\phi(x) = \begin{cases} (1-\eta) + 2x, & x \in [0, \eta/2]; \\ 1 - 2(2x - \eta)/\eta, & x \in [\eta/2, \zeta]. \end{cases}$$

Then

$$x\,\phi(y) + y\,\phi(x) \le \eta\,\phi(\zeta - xy)$$

for all $x, y \in [0, \zeta]$.

Proof: Setting $\psi(x, y) = \eta\,\phi(\zeta - xy) - x\,\phi(y) - y\,\phi(x)$, we see that our task is to prove

$$\psi(x, y) \ge 0 \tag{6.1}$$

over the square $0 \le x \le \zeta$, $0 \le y \le \zeta$. Since the definition of ϕ breaks into two cases, we can partition the square into regions according to the cases of ϕ that appear in the definition of ψ. These regions are delimited by the lines $x = \eta/2$ and $y = \eta/2$, which separate the cases of $\phi(x)$ and $\phi(y)$, and by the hyperbola $xy = \eta^2/4$, which separates the cases of $\phi(\zeta - xy)$. These three curves, together with the four lines bounding the square, partition the square into six regions, and it will suffice to prove (6.1) for each region.

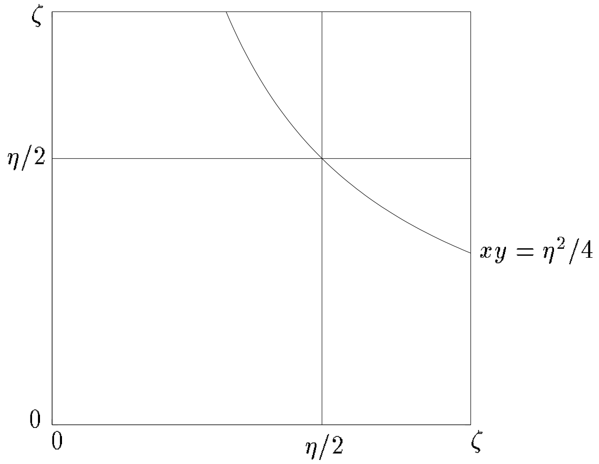

Figure 2: Partition of $[0, \zeta] \times [0, \zeta]$ according to the cases of ϕ that appear in the definition of ψ ($\varepsilon = 0.05$).

Within each region, $\psi(x, y)$ is bilinear, that is, of the form $a + bx + cy + dxy$. The graph of $\psi(x, y)$ thus forms a surface that has non-positive curvature at every point (since the Hessian determinant is $-d^2 \le 0$). Thus $\psi(x, y)$ cannot have a local extremum, and must assume its minimum over any bounded region on the boundary of the region. Thus it will suffice to prove (6.1) for each of the six lines $x = 0$, $x = \eta/2$, $x = \zeta$, $y = 0$, $y = \eta/2$, $y = \zeta$, and for the hyperbola $xy = \eta^2/4$ (where in each case only the segment of the curve included in the square $x, y \in [0, \zeta]$ is relevant).

Let us consider first the hyperbola $xy = \eta^2/4$. We must have either $x \le \eta/2$ or $y \le \eta/2$, and we may assume without loss of generality that $x \le \eta/2$ (the other case being symmetric). We shall compare $\psi(x, y)$ on the hyperbola with $\psi(\eta/2, y)$. In increasing x to $\eta/2$, the term $\eta\,\phi(\zeta - xy)$ can only decrease to $\eta\,\phi\big(\zeta - (\eta/2)y\big)$ (since $\psi(\zeta - xy)$ assumes its maximum value 1 on the hyperbola); the term $-x\,\phi(y)$ can only decrease to $-(\eta/2)\,\phi(y)$ (since $\phi(y)$ is non-negative); and the term $-y\,\phi(x)$ can only decrease to $-y\,\phi(\eta/2)$ (since $\phi(x)$ is increasing in the range $0 \le x \le \eta/2$). Thus the truth of (6.1) on the hyperbola follows from the truth of (6.1) on the lines $x = \eta/2$ and $y = \eta/2$, which we have already undertaken to prove.

It remains to prove (6.1) for the six line segments. Since the restriction of a bilinear form to a horizontal or vertical line segment is linear in the remaining variable (that is, of the form $a + bx$ or $a + by$), ψ must assume its minimum over such a line segment at one of the end points of the segment. Thus it will suffice to prove (6.1) at the nine points determined by $x \in \{0, \eta/2, \zeta\}$ and $y \in \{0, \eta/2, \zeta\}$.

For $x = y = \eta/2$, we have $\zeta - xy = \eta/2$. In this case, (6.1) is satisfied with equality. This leaves the eight points on the boundary of the square.

First let us consider the three points with $x = 0$ (the points with $y = 0$ being symmetric). In this case we have

$$\begin{aligned} y\,\phi(0) &= y(1-\eta) \\ &\le \zeta\,(1-\eta) \\ &\le \eta\,(1-\eta) \\ &= \eta\,\phi(\zeta), \end{aligned}$$

where we have used the inequalities $y \le \zeta$ and $\zeta \le \eta$.

Before proceeding further, let us note that for $0 \le y \le \eta/2$, we have

$$\phi(y) \ge 2y/\eta, \tag{6.2}$$

since $\phi(y) = (1-\eta) + \eta(2y/\eta)$ is a convex combination of $2y/\eta$ and 1, and $2y/\eta \le 1$.

Next let us consider the point $x = \eta/2$, $y = \zeta$ (the point $y = \eta/2$, $x = \zeta$ being symmetric). In this case we have

$$\begin{aligned} (\eta/2)\,\phi(\zeta) + \zeta\,\phi(\eta/2) &= (\eta/2)(1-\eta) + \zeta \\ &\le \zeta\,(1-\eta) + \zeta \\ &= \eta\,(2/\eta)\,(\zeta - \zeta\eta/2) \\ &\le \eta\,\phi\big(\zeta - \zeta(\eta/2)\big), \end{aligned}$$

where we have used the inequalities $\eta/2 \leq \zeta$ and (6.2) for $y = \zeta - \zeta(\eta/2)$.

Finally let us consider the point $x = y = \zeta$. In this case we have

$$\begin{aligned} 2\zeta\,\phi(\zeta) &= 2\zeta\,(1-\eta) \\ &\leq 2\zeta\,(1-\zeta) \\ &= \eta\big(2(\zeta-\zeta^2)/\eta\big) \\ &\leq \eta\,\phi(\zeta-\zeta^2), \end{aligned}$$

where we have used the inequalities $\zeta \leq \eta$ and (6.2) for $y = \zeta - \zeta^2$. $\triangle$