Information Theory and Noisy Computation

William S. Evans[1]
Dept. of Computer Science, Univ. British Columbia

Leonard J. Schulman[2]
Dept. of Applied Mathematics, Weizmann Inst. Science
College of Computing, Georgia Inst. Technology

We report on two types of results. The first is a study of the rate of decay of information carried by a signal which is being propagated over a noisy channel. The second is a series of lower bounds on the depth, size, and component reliability of noisy logic circuits which are required to compute some function reliably. The arguments used for the circuit results are information-theoretic, and in particular, the signal decay result is essential to the depth lower bound.

Our first result can be viewed as a quantified version of the data processing lemma, for the case of Boolean random variables.

Theorem 1 (Signal Decay) *If X, Y are Boolean random variables and Z is the output of the channel $\begin{bmatrix} 1-a & a \\ b & 1-b \end{bmatrix}$ on input Y then $\frac{I(X;Z)}{I(X;Y)} \leq \sin^2\theta$, where θ is the angle in the plane between the vectors $(\sqrt{1-a}, \sqrt{a})$ and $(\sqrt{b}, \sqrt{1-b})$.*

It is worth emphasizing that the bound holds regardless of the distribution on X and Y, and is a property of the channel alone. The bound is tight in that for any such channel, one can describe a joint distribution for X and Y so that $I(X;Z)/I(X;Y)$ is arbitrarily close to $\sin^2\theta$.

The previous theorem is a general result about mutual information. The remaining theorems concern the noisy circuit model of Von Neumann [7]. The signal decay theorem is useful in proving lower bounds on the structure of such circuits whose components (i.e. individual logic gates) fail with some probability. These results improve and simplify all previous lower bounds in this model.

Theorem 2 (Noisy Circuit Depth) *Let f be a Boolean function which depends on n inputs. Let C be a circuit of depth c using gates with at most k inputs, where each gate fails independently with probability $(1-\xi)/2$. Suppose C computes the function f correctly on all inputs with probability at least $1-\delta$ where $\delta < 1/2$. Let $\Delta = 1+\delta\log\delta+(1-\delta)\log(1-\delta)$.*

- *If $\xi^2 > 1/k$ then $c \geq \frac{\log(n\Delta)}{\log(k\xi^2)}$*
- *If $\xi^2 \leq 1/k$ then $n \leq 1/\Delta$*

To prove this theorem, we analyze the mutual information between the input to the noisy circuit and its output. This information must be large since the circuit reliably computes the function f; yet, according to the signal decay theorem, each noisy gate in the circuit, when viewed as a noisy channel, decreases information. Together, these observations imply the lower bound on circuit depth. This improves on the lower bounds of Pippenger [5] and Feder [1].

A similar technique, using a different measure of correlation than mutual information, provides a lower bound on noisy circuit size.

Theorem 3 (Noisy Circuit Size) *Let f be a Boolean function with sensitivity[1] s. Let C be a circuit using gates with at most k inputs, where each gate fails independently with probability $(1-\xi)/2$. Suppose C computes the function f correctly on all inputs with probability at least $1-\delta$ where $\delta < 1/2$, then the number of gates in C is at least $\frac{s\log s + 2s\log(2(1-2\delta))}{k\log t}$ where $t = \frac{\omega^3+(1-\omega)^3}{\omega(1-\omega)}$ and $\omega = \frac{1-\sqrt[k]{\xi}}{2}$.*

Previously, Gál [3], Reischuk and Schmeltz [6], and Gács and Gál [2] proved an $\Omega(s\log s)$ bound on reliable circuit size. Our improvement is in the bound's dependence on component reliability.

Finally, we establish a threshold for component reliability below which one cannot reliably compute all functions.

Theorem 4 (Component Reliability) *For k odd there exists $\delta < 1/2$ such that for all Boolean functions f there exists a formula[2] (using gates with at most k inputs, where each gate fails independently with probability ϵ) which computes f correctly on all inputs with probability at least $1-\delta$ if and only if*

$$\epsilon < \frac{1}{2} - \frac{2^{k-2}}{k\binom{k-1}{\frac{k-1}{2}}}.$$

This extends work done by Hajek and Weller [4], who showed the result for $k = 3$.

References

[1] T. Feder. Reliable computation by networks in the presence of noise. *IEEE Transactions on Information Theory*, 35(3):569–571, May 1989.

[2] P. Gács and A. Gál. Lower bounds for the complexity of reliable Boolean circuits with noisy gates. *IEEE Transactions on Information Theory*, 40(2):579–583, March 1994.

[3] A. Gál. Lower bounds for the complexity of reliable Boolean circuits with noisy gates. In *Proceedings of the 32nd Annual Symposium on Foundations of Computer Science*, pages 594–601, 1991.

[4] B. Hajek and T. Weller. On the maximum tolerable noise for reliable computation by formulas. *IEEE Transactions on Information Theory*, 37(2):388–391, March 1991.

[5] N. Pippenger. Reliable computation by formulas in the presence of noise. *IEEE Transactions on Information Theory*, 34(2):194–197, March 1988.

[6] R. Reischuk and B. Schmeltz. Reliable computation with noisy circuits and decision trees — a general $n\log n$ lower bound. In *Proceedings of the 32nd Annual Symposium on Foundations of Computer Science*, pages 602–611, 1991.

[7] J. von Neumann. Probabilistic logics and the synthesis of reliable organisms from unreliable components. In C. E. Shannon and J. McCarthy, editors, *Automata Studies*, pages 43–98. Princeton University Press, 1956.

[1]Supported by a Canadian International Fellowship and NSF grant CCR 92-01092. wevans@cs.ubc.ca

[2]Supported in part by an NSF Postdoctoral Fellowship. schulman@cc.gatech.edu

[1]The sensitivity of a function is the maximum (over all inputs) of the number of bits in the input which, when changed individually, change the function value.

[2]A formula is a circuit in which each gate has out-degree one.