

On the Shannon function for partially defined Boolean functions

Peter Bro Miltersen*

January 30, 2012

Abstract

Andreev, Clementi and Rolim considered the *Shannon function* for partially defined Boolean functions and derived an expression for the value of this function. They proved the expression correct for a special setting of the parameters. We give an easy proof that this expression is correct in general.

1 Introduction

As a tool for a derandomization technique, Andreev, Clementi and Rolim [2] considered the *Shannon function* for partially defined Boolean functions. More precisely, let $\mathcal{F}(n, N, m)$ be the set of all $\{0, 1\}$ -valued functions defined on some subdomain of $\{0, 1\}^n$ of size N , and assuming 1 on exactly $m \leq N$ inputs. A circuit for f should agree with f on its domain of definition but can take arbitrary values outside this domain. Let $M_{n, N, m}^{\text{partial}}$ be the complexity function in $\mathcal{F}(n, N, m)$ with maximum possible circuit complexity.

In the conference version of the paper of Andreev, Clementi and Rolim [2], the following theorem is stated.

Theorem 1 (Andreev, Clementi, Rolim)

$$M_{n, N, m}^{\text{partial}} = (1 + o(1)) \log \binom{N}{m} / \log \log \binom{N}{m} + O(n)$$

However, they only prove the theorem for the following settings of the parameters: $n^{1+\epsilon} \leq m \leq n^{O(1)}$ and $N = 2^{\Omega(n)}$ (which is the case relevant for their derandomization application) and the general case is postponed to the

*BRICS, Basic Research in Computer Science, Centre of the Danish National Research Foundation, Department of Computer Science, University of Aarhus. Email: bromille@brics.dk. Supported by the ESPRIT Long Term Research Programme of the EU under project number 20244 (ALCOM-IT).

final version. However in the final version of the paper (available as [3]), the theorem itself has been restricted to the case $n^{1+\epsilon} \leq m \leq n^{O(1)}$ and $N = 2^{\Omega(n)}$. According to Rolim (personal communication), their proof of the general case is very complicated and its publication has therefore been postponed indefinitely.

In our opinion, the Shannon function for the general case is interesting in its own right. Also, knowing its value within a low order term may have other applications. We give a simple (and presumably simpler, judging from the above mentioned personal communication) proof for the general case, based on our technique of replacing universal hashing with error correcting codes and bit sampling which we first used in [6].

2 The proof

For the proof, we need three facts. The first, appearing in [4] states that there are good error correcting codes with linear sized circuits.

Fact 2 (Gelfand, Dobrushin and Pinsker) *There are certain constants $c_1 \geq 1$, $\delta > 0$ and $c_2 \geq 1$, so that there for all n is a circuit E_n of size $c_2 n$, mapping n bits to $c_1 n$ bits, so that for all $x, y \in \{0, 1\}^n$ with $x \neq y$, $E_n(x)$ and $E_n(y)$ differ on at least a δ -fraction of their bits.*

A more recent reference for such codes is Spielman [8]. Unlike the above codes, Spielman's codes can be decoded efficiently. But we shall only care about the encoding circuits.

The following fact, appearing, e.g., in [1] can be proved using straightforward induction.

Fact 3 *Let X_1, X_2, \dots, X_l be independent 0-1 variables each taking the value 1 with probability p . Then $\Pr[\bigoplus_{i=1}^l X_i = 0] = \frac{1}{2}(1 + (1 - 2p)^l)$.*

The final fact we need is the Lupanov-Shannon bound [5, 7, 9] for total functions from $\{0, 1\}^n$ to $\{0, 1\}$ taking the value 1 on exactly m inputs:

Fact 4 (Lupanov and Shannon) *The maximum circuit complexity of a (total) Boolean function from $\{0, 1\}^n$ to $\{0, 1\}$ taking the value 1 on exactly m inputs is $(1 + o(1)) \log \binom{2^n}{m} / \log \log \binom{2^n}{m}$.*

Now we first show, by a proof very similar to the proof of Theorem 7.1 of [6], the following lemma:

Lemma 5 *There is a constant $c \geq 1$, so that for all $n, N_0, N_1 \leq 2^n$ and $k \geq 2$, the following holds: Let S_0 with $|S_0| = N_0$ and S_1 with $|S_1| = N_1$ be disjoint subsets of $\{0, 1\}^n$. There is a Boolean circuit C of size $c(n + N_0 N_1 \log(N_0 N_1) 2^{-k+k/2^l} + kl)$ mapping n bits to k bits so that for all $x \in S_0, y \in S_1$, $C(x) \neq C(y)$.*

Proof The circuit C works as follows. First we apply the circuit E_n of Fact 2 to the input, expanding the n bits to $c_1 n$ bits. Let c_2 and δ be the same values as in Fact 2. Let $z_1, z_2, \dots, z_{c_1 n}$ be the output bits of E_n . We will select a subset $z_{i_1}, z_{i_2}, \dots, z_{i_r}$ of the outputs with $r = \lceil \log(N_1 N_2) / \log \frac{1}{1-\delta} + 1 \rceil$, and disregard the rest. Call the resulting circuit E' , mapping $\{0, 1\}^n \rightarrow \{0, 1\}^r$. We shall make sure that E' is 1-1 on $S := S_0 \cup S_1$. Let E_j be the circuit mapping the input to $z_{i_1}, z_{i_2}, \dots, z_{i_j}$. Let $P_j = \{(x, y) \in S_0 \times S_1 \mid E_j(x) = E_j(y)\}$. Suppose $z_{i_1}, z_{i_2}, \dots, z_{i_j}$ have been selected. If we pick $z_{i_{j+1}}$ at random, for any particular pair in P_j , the probability that the pair is in P_{j+1} is at most $1 - \delta$. Thus, by an averaging argument, we can pick $z_{i_{j+1}}$, so that $|P_{j+1}| \leq (1 - \delta)|P_j|$. Since $|P_0| = N_0 N_1$, we can ensure that $|P_r| \leq (1 - \delta)^r N_0 N_1 < 1$, and since it is an integer, it is 0, so $E' = E_r$ is 1-1 on S . So far, we have constructed a circuit of size $O(n)$ mapping S 1-1 to $r = O(\log(N_0 N_1))$ bits.

We now construct another circuit with r inputs and k outputs which we will compose with E' to get the final circuit.

Again we use the circuit of Fact 2, defining an error correcting code with relative minimum distance at least δ , this time with number of inputs r , number of outputs $r' = O(r)$, and size $O(r) = O(\log N)$. Let the outputs be $q_1, \dots, q_{r'}$. We define gates o_1, o_2, \dots, o_{k-1} as XOR-gates of odd fan-in $l' \geq \lceil (l+1) / \log(\frac{1}{1-2\delta}) \rceil$, each adding size l' to the circuit, each taking a subset of the q_i 's as inputs. We will fix the inputs of the o_i 's iteratively. Suppose o_1, \dots, o_i have been fixed and let C_i be the circuit mapping the input to o_1, o_2, \dots, o_i . Let $P_i = \{(x, y) \in E'(S_0) \times E'(S_1) \mid C_i(x) = C_i(y)\}$. Now suppose we pick the l' inputs of o_{i+1} randomly from the q_j 's. By Lemma 3, for each $(x, y) \in P_i$, the probability that (x, y) is in P_{i+1} is at most $\frac{1}{2}(1 + (1 - 2\delta)^{l'}) \leq \frac{1}{2}(1 + 2^{-(l+1)})$. Thus, we can pick a setting of the inputs so that $|P_{i+1}| \leq \frac{1}{2}(1 + 2^{-(l+1)})|P_i|$, and thus ensure that $|P_k| \leq N_0 N_1 (\frac{1}{2}(1 + 2^{-(l+1)}))^{k-1} \leq N_0 N_1 2^{-k+1+k/2^l}$. Call this last quantity u . Let C_1 be the circuit, resulting from disregarding all outputs but the o_i 's. We can remove a subset T of size u from $E'(S)$ so that C_1 is 1-1 on $E'(S) - T$. Let C_2 be the obvious circuit of size $O(ur)$, taking r inputs and one output, and mapping $S_0 \cap T$ to 0 and $S_1 \cap T$ to 1. There is also an obvious circuit of size $O(ur)$ deciding membership of T . Now let $C_3(x) = 0^{k-1} \circ C_2(x)$ if $x \in T$ and $C_3(x) = 1 \circ C_1(x)$ otherwise.

The desired circuit is E' composed with C_3 . The size of this circuit is $O(n + \log(N_0 N_1) + kl + \log(N_0 N_1)u) = O(n + \log(N_0 N_1)N_0 N_1 2^{-k+k/2^l} + kl)$, as desired. \square

Proof (of theorem 1): The standard counting argument immediately gives $M_{n, N, m}^{\text{partial}} \geq \log \binom{N}{m} / \log \log \binom{N}{m}$. Thus, we need only show that for any fixed ϵ , sufficiently large N , and all n, m : $M_{n, N, m}^{\text{partial}} \leq (1 + \epsilon) \log \binom{N}{m} / \log \log \binom{N}{m} + O(n)$.

Let $\epsilon > 0$ be arbitrary. Let f be any function in $\mathcal{F}(n, N, m)$. Let S_0 be the instances for which f is 0 and let S_1 be the instances for which f is 1. Let $N = |S_0 \cup S_1|$ and let $m = |S_1|$. Assume without loss of generality that

$m \leq N/2$. Let us first make a circuit C mapping n bits to $\lfloor(1 + \epsilon) \log N\rfloor$ bits so that $C(x) \neq C(y)$ for $x \in S_0$ and $y \in S_1$. We make this circuit by applying Lemma 5 with $k = \lfloor(1 + \epsilon) \log N\rfloor$ and $l = \log(10/\epsilon)$. Thus, the circuit has size $O(n + m/N^{\epsilon/2})$. We can make a circuit for f by first applying the circuit C and then computing some function on the resulting $\lfloor(1 + \epsilon) \log N\rfloor$ variables (as the configuration of those variables determines the value of f). But by Lemma 4, this function has complexity at most

$$(1 + o(1)) \log \binom{2^{(1+\epsilon) \log N}}{m} / \log \log \binom{2^{(1+\epsilon) \log N}}{m}$$

Thus, the total complexity of the circuit is at most

$$O(n + m/N^{\epsilon/2}) + (1 + o(1)) \log \binom{2^{(1+\epsilon) \log N}}{m} / \log \log \binom{2^{(1+\epsilon) \log N}}{m}$$

which is smaller than

$$(1 + 2\epsilon) \log \binom{N}{m} / \log \log \binom{N}{m} + O(n)$$

for sufficiently large values of N and independently of the value of m . As $\epsilon > 0$ is arbitrary, this proves Theorem 1. \square

References

- [1] A. Andersson, P.B. Miltersen, S. Riis, and M. Thorup. Static dictionaries on AC^0 RAMs: Query time $\theta(\sqrt{\log n / \log \log n})$ is necessary and sufficient. In *FOCS: IEEE Symposium on Foundations of Computer Science (FOCS)*, 1996.
- [2] Alexander E. Andreev, Andrea E. F. Clementi, and José D. P. Rolim. Worst-case hardness suffices for derandomization: A new method for hardness-randomness trade-offs. In Pierpaolo Degano, Robert Gorrieri, and Alberto Marchetti-Spaccamela, editors, *Automata, Languages and Programming, 24th International Colloquium*, volume 1256 of *Lecture Notes in Computer Science*, pages 177–187, Bologna, Italy, 7–11 July 1997. Springer-Verlag.
- [3] Alexander E. Andreev, Andrea E. F. Clementi, and José D. P. Rolim. Worst-case hardness suffices for derandomization: A new method for hardness-randomness trade-offs. Technical Report TR96-055, Revision 01, Electronic Colloquium on Computational Complexity, 1997.
- [4] S.I. Gelfand, R.L Dobrushin, and M.S. Pinsker. On the complexity of coding. In *Second International Symposium on Information Theory*, pages 177–184. Akademiai Kiado, Budapest, 1973.

- [5] O.B. Lupanov. A method of synthesis of control system - the principle of local coding. *Problemy Kibernet.*, 10:31–110, 1965.
- [6] Peter Bro Miltersen. Error correcting codes, perfect hashing circuits, and deterministic dynamic dictionaries. In *Proceedings of the Ninth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 556–563, San Francisco, California, 25–27 January 1998.
- [7] Claude E. Shannon. The synthesis of two-terminal switching circuits. *Bell. Syst. Tech. J.*, 28:59–98, 1949.
- [8] D.A. Spielman. Linear-time encodable and decodable error-correcting codes. In *Proceedings 27th Annual Symposium on Theory of Computing*, pages 388–397, Las Vegas, Nevada, May 1995.
- [9] Ingo Wegener. *The Complexity of Boolean Functions*. Wiley-Teubner, 1987.