Average Circuit Depth and Average Communication Complexity

Bruno Codenotti*
Istituto di Matematica Computazionale del CNR, Pisa, Italy

Peter Gemmell†
Sandia National Labs

Janos Simon‡
Department of Computer Science
The University of Chicago

June 7, 1995

Abstract

We use the techniques of Karchmer and Widgerson [KW90] to derive strong lower bounds on the expected parallel time to compute boolean functions by circuits. By average time, we mean the time needed on a self-timed circuit, a model introduced recently by Jakoby, Reischuk, and Schindelhauer, [JRS94] in which gates compute their output as soon as it is determined (possibly by a subset of the inputs to the gate).

More precisely, we show that the average time needed to compute a boolean function on a circuit is always greater than or equal to the average number of rounds required in Karchmer and Widgerson's communication game. We also prove a similar lower bound for the monotone case. We then use these techniques to show that, for a large subset of the inputs, the average time needed to compute $s-t$ connectivity by monotone boolean circuits is $\Omega(\log^2 n)$.

We show, that, unlike the situation for worst case bounds, where the number of rounds characterize circuit depth, in the average case the Karchmer-Widgerson game is only a lower bound. We construct a function g and a set of minterms and maxterms such that on this set the average time needed for any monotone circuit to compute g is polynomial, while the average number of rounds needed in Karchmer and Widgerson's monotone communication game for g is a constant. Related work by Raz and Widgerson [RW89] shows that the monotone probabilistic communication complexity (a model weaker than ours) of the s-t connectivity problem is $\Omega(\log^2 n)$.

Keywords: circuit complexity, parallel time, communication complexity, lower bounds

*Partially supported by ESPRIT Basic Research Action, Project 9072 'GEPPCOM'.
†Portions of this work were done while visiting IMC-CNR in Pisa, partially supported by GNIM-CNR
‡Portions of this work were done while visiting IMC-CNR in Pisa, sponsored by a grant from CNR

1 Introduction

A recent paper of Jakoby, Reischuk, and Schindelhauer, [JRS94] formalizes the important and useful notion of self-timed circuits. In a self-timed circuit a gate produces its output as soon as a large enough subset of the inputs to it becomes available. More precisely, if at time t a subset S of the inputs of gate g is defined, and the output of g is determined by the inputs in S, then at time $t + \Delta$ the output of g is determined (and becomes available to the gates that it is an input to.) Here Δ is the *gate delay*, which we will suppose to be 1. Thus, if a 0 appears at the input of an AND gate, by the next clock tick the gate will produce a 0 output, without waiting for the other input value to be defined. For some inputs, some circuits may produce an output much earlier than the worst-case bound given by the depth of the circuit.

Self-timed circuits are used in some fast computer architectures, [1] and [JRS94] makes a compelling argument for their theoretical study.

We will examine the *expected parallel time* to compute boolean functions by self-timed circuits. [JRS94] discuss the average time needed to compute some simple functions like addition and parity, showing that they can be done much faster on the average than in the worst case.

There are several possible definitions for expected or average behavior. A simple and natural choice is to compute the expected delay under the assumption of uniform distribution of the inputs. We will call this measure the *average* parallel time. Unfortunately, average time is not a very robust measure: it is possible to change it radically by simple padding (for example Wilf exhibits an NP-complete problem that can be solved in constant average time [W]). We refer to the more complete discussion of these problems in [JRS94], [RS93], [L86]. A more robust, and more complicated measure was introduced by Levin [L86]. We will call the distribution given by Levin's definition the *Levin measure*. Our results hold for both. In the interest of clarity and brevity, we postpone the definitions and proofs related to the Levin measure to the full paper.

A beautiful technique, due to Karchmer and Widgerson [KW90], relates circuit depth to the communication complexity of boolean relations. Given a boolean function f, consider the following *communication game*: There are two players. Player 0 has an input $x \in f^{-1}(0)$ and player 1 has an input $y \in f^{-1}(1)$.

The objective of the game is for player 1 to learn an index i such that $x_i \neq y_i$.

The game consists of messages exchanged by the two players according to some protocol, agreed upon in advance by the two players. The protocol is such that the messages sent by player 1 depend only on x and on the messages previously received; similarly the messages sent by player 2 depend only on y and on the previous messages. The communication complexity of f (more precisely, of the relation $f^{-1}(1) \times f^{-1}(0) \times i$ such that $x_i \neq y_i$) is the number of bits exchanged by the best protocol in the worst case. We refer to [KW90] for precise definitions.

Karchmer and Widgerson showed that the number of bits of communication necessary, in the worst case, in this game is exactly the minimum depth of a bounded fan-in boolean circuit that computes f. A similar characterization holds for monotone circuits: one of the players has a minterm of the circuit, the other a maxterm. They exchange messages until they can agree on an index that belongs to both the maxterm and the minterm. (To see how the monotone game relates to the

[1] In actual circuits it is also possible to take advantage of varying gate delays and varying delays in different subcircuits: we will ignore these, as we are interested in asymptotics.

general game, recall that a minterm is a minimal set of variables that set to 0 make the function have the value 0. Similarly, setting the variables of maxterm to 1 will force the function to have the value 1. So finding an index i that belongs to the minterm and to the maxterm means that there is an input x extending the maxterm – and thus $f(x) = 1$ – an input y extending the minterm – and thus $f(y) = 0$ – with $x_i = 1$ and $y_i = 0$).

Communication complexity of boolean relations is of intrinsic interest, and has been extended to probabilistic versions by Raz and Widgerson [RW89]. Average case communication complexity has also been previously studied [O91], [FKN91], but in a different context.

Lower bounds on the communication complexity for explicit functions can be used to derive lower bounds on worst case parallel time (circuit depth). While the notoriously hard problem of proving superlogarithmic parallel time bounds for explicit boolean functions remains open, there are some strong results for monotone circuits. Karchmer and Widgerson were able to prove that s-t connectivity (given a directed graph and two distiguished vertices s and t, is there a path from s to t) requires monotone circuits of depth $\Omega(\log^2 n)$ [KW90]. An even stronger, linear depth lower bound was obtained by Raz and Widgerson [RW92] for matching, a problem known to require nonpolynomial size monotone circuits [R85].

In this paper we study the average communication complexity of monotone boolean functions, in both the average and the Levin measure. We show that in both measures, the average number of rounds (bits) required in the Karchmer-Widgerson game is a lower bound on the average parallel time. We can then adapt the Karchmer-Widgerson lower bound proof to show an $\Omega(\log^2 n)$ lower bound on parallel average time for s-t connectivity on a certain natural set of inputs.

We also show, that unlike the deterministic case, the complexity of the game is not a characterization of average time – in fact the difference between the two bounds may be unbounded. More precisely, we construct a function g and a set of minterms and maxterms such that, on this set, the average time needed for any monotone circuit to compute g is a polynomial (n^α), while the average number of rounds needed in Karchmer and Widgerson's monotone communication game for g is $O(1)$.

Our results are somewhat related to those in [RW89]. Raz and Widgerson show that the monotone probabilistic communication complexity of the s-t connectivity problem is $\Omega(\log^2 n)$. Since probabilistic complexity is asymptotically not less than average complexity, our lower bounds imply theirs. They also show that in the general (nonmonotone) model, every relation has an $O(\log n)$ complexity protocol. This implies a similar bound in our model. It also shows that probabilistic communication complexity is not a characterization for probabilistic parallel time, and the difference can be from a polynomial to a logarithm. In our model, we can show an even bigger gap, from a polynomial to a constant.

2 Definitions

We introduce some general notation as well as the definitions that we will use for the computing time of functions on circuits and the communication complexity of functions.

First, some simple notation: For an integer n, let $[n]$ denote $\{1, 2 \ldots n\}$. $x \in_U S$, means that element x is chosen uniformly at random from set S.

We now consider definitions to do with the depth and the computing time of circuits.

Given a circuit C and input x, let $C(x)$ be the output of C on x.

Given a function f on domain D, let $depth_D(f)$ be the minimum depth of any fan-in 2 circuit that computes f.

Given a monotone function f on domain D, let $depth_D^m(f)$ be the minimum depth of any monotone fan-in 2 circuit that computes f.

In the following sense, the output of a circuit may be often determined in time less than the depth of the circuit:

Definition 1 *Let C be a circuit with NOT gates only on the first level. Let x be an input for C. We will say that a subcircuit, C_x, of C* ***determines*** *$C(x)$ if:*

C_x contains the output gate of C.

If $C(x) = 1$ then:

- All the gates or inputs that feed into the AND gates of C_x are also contained in C_x.

- At least one of the gates or inputs, with value equal to 1, that feed into every OR gate of C_x is contained in C_x.

If $C(x) = 0$ then:

- All the gates or inputs that feed into the OR gates of C_x are also contained in C_x.

- At least one of the gates or inputs, with value equal to 0, that feed into every AND gate of C_x is contained in C_x.

Definition 2 *$time_C(x)$, or the time required on circuit C to compute on x, is equal to the minimum depth of any subcircuit C_x that determines $C(x)$.*

We define the *average computing time* of a function f on domain D:

Definition 3 *Given a function f on domain D,*

$AT_D(f) = min_{C\,:\,C \text{ computes } f \text{ on } D} [\sum_{x \in D} time_C(x)/|D|]$

If f is monotone, then

$AT_D^m(f) = min_{C\,:\,C \text{ monotone, computes } f \text{ on } D} [\sum_{x \in D} time_C(x)/|D|]$

We now make definitions for communication games, where the goal is for two players to learn one index where their inputs differ.

Definition 4 *Let f be a boolean function. Given two players, P_0 who knows string $x \in f^{-1}(0)$ and P_1 who knows string $y \in f^{-1}(1)$, we define a communication game G for f on domain D to be a sequence of interactions where P_0 and P_1 exchange bits back and forth until both know the same value i such that $x_i \neq y_i$. We refer to each bit communicated as a* round *and to the number of rounds communicated by the players using a game strategy G as $Rounds_G(x, y)$.*

We now define **average communication complexity** for a function f on domain D.

Definition 5

$$AC_D(f) = min_{G:game \text{ for } f \text{ on } D} \left[\sum_{(x,y) \in (D \cap f^1(0) \times D \cap f^{-1}(1))} \frac{Rounds_G(x,y)}{|(D \cap f^{-1}(0)) \times (D \cap f^{-1}(1))|} \right]$$

Definition 6 *Let f be a monotone function.*

Let MAX_f be the set of maxterms *for f, ie MAX_f = all minimal subsets, q, of $[n]$ such that $(\forall i \in q, x_i = 0) \Rightarrow f(x) = 0$.*

Let MIN_f be the set of minterms *for f, ie MIN_f = all minimal subsets, p, of $[n]$ such that $(\forall i \in p, x_i = 1) \Rightarrow f(x) = 1$.*

Given sets of minterms B_1 and maxterms B_0, we define extensions of the minterms/maxterms to the input set $\{0,1\}^n$:

$$B_0^* = \{x | i \in q \Rightarrow x_i = 0, i \in \overline{q} \Rightarrow x_i = 1\}_{q \in B_0}$$

$$B_1^* = \{y | i \in p \Rightarrow y_i = 1, i \in \overline{p} \Rightarrow y_i = 0\}_{p \in B_1}$$

Given a boolean function, f, and two players, P_0 who knows a maxterm $q \in B_0$ and P_1 who knows a minterm $p \in B_1$, we define a monotone communication game G for f on $B_0 \cup B_1$ to be a sequence of interactions where P_0 and P_1 exchange bits back and forth until both know the same value i such that $i \in p \cap q$. We refer to each bit communicated as a round *and to the number of rounds communicated by the players using a game strategy G as $Rounds_G^m(x,y)$.*

Definition 7 *We now define* average monotone communication complexity*. Let D be a set of minterms and maxterms:*

$$AC_D^m(f) = min_{G:monotone\ game\ for\ f\ on\ D} \left[\frac{\sum_{(x,y) \in (D \cap MAX_f \times D \cap MIN_f)} Rounds_G^m(x,y)}{|(D \cap MAX_f) \times (D \cap MIN_f)|} \right]$$

3 Average Communication Complexity Lower Bounds Average Computing Time

Theorem 1 *For any boolean function f on domain D, we have:*

$$AC_D(f) \leq AT_D(f)$$

Proof:

The proof is similar to the corresponding worst-case proof in [KW90] except that the path that the two players take as they "walk up" the circuit is determined by the quickest way to determine the output of the gates.

Let C be a circuit such that $AT(f) = [\sum_{x \in D} time_C(x)/|D|]$

Let $(x,y) \in_u (f^{-1}(0) \cap D \times f^{-1}(1) \cap D)$.

¿From the fact that $x \in f^{-1}(0)$ and by the definition of $time$, we know there is a subcircuit, C_x, of C, with the same output gate as C, with inputs that are a subset of C's inputs, and with maximum depth $time(x)$. Furthermore, each of C_x's AND gates has one input and one output and each of C_x's OR gates has two inputs and one output.

Similarly, we know there is a subcircuit C_y of C with the same output gate as C, with inputs that are a subset of C's inputs, and with maximum depth $time(y)$. Furthermore, each of C_y's OR gates has one input and one output and each of C_y's AND gates has two inputs and one output.

The game that players P_0 and P_1 will play is to start at the output of C and move up their subcircuits as follows:

- If the gate is an AND gate, it is P_0's move, and (s)he sends an R or an L to P_1 according to whether the single branch that C_x takes at this point is the right or left input of this gate in C.
- If the gate is an OR gate, it is P_1's move, and (s)he sends an R or an L to P_0 according to whether the single branch that C_y takes at this point is the right or left input of this gate in C.
- If the players have reached an input, then the players have arrived at an input bit where they disagree.

We note that, in the course of the game, the two players take a walk in $C_x \cap C_y$ and so the total number of rounds is at most $min(time(x), time(y))$.

The expected communication time is:

$$E_{(x,y)\in_u((D\cap f^{-1}(0))\times(D\cap f^{-1}(1)))} min(time_C(x), time_C(y)) \leq E_{z\in_u D}(time_C(z))$$

□

We now discuss a corresponding theorem for average monotone time and communication complexity.

Theorem 2 *For any boolean function f and sets of maxterms and minterms, B_0 and B_1, we have:*

$$AC^m_{B_0\cup B_1}(f) \leq AT^m_{B_0^*\cup B_1^*}(f)$$

The proof is identical to the one above, except that we may have the two parties extend their inputs. P_0 extends his/her maxterm input with 1's. P_1 extends his/her minterm input with 0's. The index i that the communication protocol will find is one where $x_i = 0$ and $y_i = 1$. Therefore, i is a desired element of $p \cap q$.

4 An $\Omega(\log^2 n)$ Lower Bound on Average Time on Monotone Circuits for STCONN

We now show that, on the set of input graphs, D, described in [KW90], $AT^m_D(STCON) = \Omega(\log^2 n)$. The overall strategy of the proof is very similar, but the fact that we must use averages instead of individual graphs is responsible for some added difficulty.

First, we change the requirement of a lower bound on the number of bits exchanged into a requirement for a lower bound on the number of rounds. Our lemma is analogous to [KW90]'s Theorem 2.3:

Lemma 3 *For any function f and domain D, there exists a communication game G for f on D where at each round P_0 sends 2^a bits while P_1 responds with a bits and such that the* average *number of rounds k satisfies:*

$$k \leq \frac{AT_D(f)}{a}$$

.

Similarly, for any monotone function f and set of minterms and maxterms D, there exists a monotone communication game G for f on D where at each round P_0 sends 2^a bits while P_1 responds with a bits and such that the average *number of rounds k satisfies:*

$$k \leq \frac{AT_D^m(f)}{a}$$

Proof: Let C be the best average case circuit for f on domain D. At each round, the two players traverse (away from the output gate) a levels of the circuit C. There are 2^a inputs to the subcircuit that is rooted at the round's starting gate. The function computed by this subtree can be expressed in CNF using at most 2^{2^n} clauses of the 2^n input variables to the subcircuit. P_0 sends to P_1 the index of a clause for which all his/her variables are most quickly determined to be 0. P_1 then returns the index of the variable within the clause that s/he most quickly determines is equal to 1. $\Box$

We will restrict ourselves to the following domain: $D = B_0 \cup B_1$, where B_0 is the set of those graphs with exactly one $s-t$ cut and all other edges present, and B_1 is the set of those graphs with one path connecting s and t, with length at most $n^{1/10}$ and all other edges absent.

We now state the main result of the section:

Theorem 4

$$AT_D^m(STCONN) = \Omega(\log^2 n)$$

To prove the theorem, we first note that by lemma 3 it suffices to prove an $\Omega(\log n)$ lower bound on the number of rounds needed in the game to obtain an $\Omega(\log^2 n)$ lower bound on the number of bits exchanged. The theorem then follows from theorem 2.

We need some rather technical definitions, borrowed from [KW90].

Definition 8 *Let $S' \subset S$.*

$$\mu_S(S') = \frac{|S'|}{|S|}$$

Let $\epsilon = 1/10$. Let $l = n^\epsilon$.

Let $U_p = [n]^l$, the set of all paths of length l and let $U_c = \{0,1\}^l$, the set of all 2-colorings of l vertices.

Assume that there is a monotone communication game G that can be used by players P_0 and P_1, for inputs (x, y) from $(B_0 \times B_1)$, to find an index $i : i \in x \cap y$. Assume that G is of the form described in lemma 3 with $a = \epsilon \log(n)$ and that the expected number of rounds $k_{max} = \frac{\epsilon}{2} \log(n)$.

Define $t_{max} = \log(l) - 1, n_0 = n, l_0 = l$. For $j \in [t_{max} - 1]$, let $n_{t+1} = n_t - 4\sqrt{n}_t, l_{t+1} = l_t/2$.

Definition 9 *We define the property* $\mathbf{H}(t, k)$*:*

There exists a collection of vectors $P^t \subset [n_t]^{l_t}$ *and a collection of colorings* $Q^t \subset \{0,1\}^{n_t}$*, with* $\mu_{[n_t]^{l_t}}(P^t) \geq \frac{1}{8}n^{-\epsilon}$ *and* $\mu_{\{0,1\}^{n_t}}(Q^t) \geq 2^{-2tn^{\epsilon}}$ *such that there is a monotone communication game* G^t *for STCONN on* (P^t, Q^t) *with* $E_{(q,p)\in Q^t\times P^t}(Rounds^m_{G^t}(q, p)) \leq k$.

Note that $\overline{H(0, k_{max})}$ implies that the protocol needs $\Omega(\log n)$ rounds, and this suffices to prove our theorem.

We will prove the following two claims that imply (by induction) that $\overline{H(0, k_{max})}$, concluding the proof of Theorem 4.

Claim 5 *For* $t \leq t_{max}, \overline{H(t, 0)}$.

Proof:

Because we have $\mu_{[n_t]^{l_t}}(P^t) \geq \frac{1}{8}n^{-\epsilon}$, and because the fraction of all paths of length t, $[n_t]^{l_t}$, that contain any one node is $1 - (1 - \frac{1}{n_t})^{l_t} << n^{-\epsilon}$, we know that there is no one node that is contained in all of P_1's paths. Therefore, P_0 can not know a vertex adjacent to a bichromatic edge.

□

Claim 6 *For* $t \leq t_{max}, H(t, k) \Rightarrow H(t + 1, k - \frac{1}{2})$.

Proof: We assume $H(t, k)$ and construct P^{t+1}, Q^{t+1}, and G^{t+1}.

Divide P^t into equivalence classes so that for every member of each equivalence class, P_1 sends the same message to P_0 in the first round of G^t. We know that the combined weight of those equivalence classes such that G^t requires at most expected $k + 1/4$ rounds (when that equivalence class is paired with Q^t) is at least $\frac{1}{4k}$.

By the pigeon-hole principle, there exists a subset $P \subset P^t$ such that $\mu_{[n_t]^{l_t}}(P) \geq \frac{1}{8}\frac{1}{4k}n^{-2\epsilon}$,for every $p \in P$, P_1 sends the same message in the first round of G^t, and the average expected time that G^t takes on $P \times Q^t$ is at most $k + \frac{1}{4}$.

Now divide Q^t into equivalence classes so that for every member of each equivalence class, P_0 sends the same message to P_1 in the first round of G^t. We know that the combined weight of those equivalence classes such that G^t requires at most expected $k + 1/2$ rounds (when that equivalence class is paired with P) is at least $\frac{1}{4k}$. By the pigeon-hole principle, there exists a subset $Q \subset Q^t$ such that $\mu_{\{0,1\}^{n_t}}(Q) \geq \frac{1}{4k}2^{-(2t+1)n^{\epsilon}}$,for every $q \in Q$, P_0 sends the same message in the first round of G^t, and the average expected time that G^t takes on $P \times Q$ is at most $k + \frac{1}{2}$.

We now prune the sets P and Q down further so that they will meet the requirements of claim 6.

We must introduce several further pieces of notation, borrowed from [KW90].

Definition 10 *Given an interval* $I \subset [l_t]$ *of consecutive integers and a vector* $p \in [n_t]^{l_t}$*, let* p_I *be the projection of* p *into* I*. For* $P \subset [n_t]^{l_t}$*, let* $P_I = \{p_I : p \in P\}$.

Given a set of paths, P, a set of vertices, $I \subset [n_t]$, and a vector $p \in I$, let $\mathbf{E}xt_{P,I}(p) = \{\tilde{p} \in P : \tilde{p}_I = p\}$

Similarly, given a subset $T \subset [l_t]$ and a coloring $q \in \{0,1\}^{n_t}$, let q_T be the projection of q into T. For a set of colorings, Q, let $Q_T = \{q_T : q \in Q\}$.

Given a restriction function $\rho : [n_t] \to \{0,1,*\}$, let $Q^\rho = \{q \in Q : \forall i \in [n_t], \rho(i) \neq * \Rightarrow q_i = \rho(i)\}$.

Definition 11 *Let $L = [l_t/2]$, $R = [l_t] - L$.*

We say that P is L (or R) good if many left (right) projections of P each have many extensions to the right (left):

*In particular, P is **L good** if:*

$$\mu_{P_L}(\{p_L : \mu_P(Ext_{P,L}(p_L)) \geq n^{-2\epsilon}/32\}) \geq \frac{1}{4}n^{-\epsilon}$$

*P is **R good** if:*

$$\mu_{P_R}(\{p_R : \mu_P(Ext_{P,R}(p_R)) \geq n^{-2\epsilon}/32\}) \geq \frac{1}{4}n^{-\epsilon}$$

Lemma 7 *P is either L good or R good.*

Proof:

The proof is exactly as in [KW90] and follows from a lemma due to Hastad.

□

Without loss of generality, we will assume that P is L good.

Lemma 8 *There exists a restriction $\rho : [n_t] \to \{0,1,*\}$ with $|\rho^{-1}(*)| = n_{t+1}$ such that the following properties hold:*

G1: $\mu_{\{0,1\}^{n_{t+1}}}(Q^\rho_{\rho^{-1}(*)}) \geq 2^{-2(t+1)n^\epsilon}$.

G2: $\exists \tilde{P} \subset P$ *such that :*

- $\forall p \in \tilde{P}, p_L \in \rho^{-1}(*)$ *and* $p_R \in \rho^{-1}(1)$
- $\forall p, p' \in \tilde{P}, p_L \neq p'_L$
- $\mu_{[n_t]^{l_t}}(\tilde{P}_L) \geq \frac{1}{8}n^{-\epsilon}$.

Proof: This lemma is almost straight out of [KW90] □

Let $Q^{t+1} = Q^\rho_{\rho^{-1}(*)}$ and $P^{t+1} = \tilde{P}_L$ and rename the coordinates so that $[n_{t+1}] = \rho^{-1}(*)$.

There is a natural 1-1 correspondence between Q^{t+1} and Q^ρ and between P^{t+1} and $\tilde{P}$.

Also, for any $q \in Q$ and $p \in P$, any bichromatic edge lies in the interval L.

The game G^{t+1} simulates the remaining rounds of G^t on vector in P^{t+1} and coloring in Q^{t+1} by following G_t on the associated vector in P and coloring in Q.

□

5 Average Communication Complexity May be Much Lower than Average Circuit Time

We now construct an example that shows that, unlike the situation with the worst-case complexity of communication games and circuits, the reverse of theorem 1 does not hold.

Theorem 9 *For all constants $\alpha < 1$, there exists a function f and domain $D \subset \{0,1\}^n$ such that $AC_D(f) = O(1)$, whereas $AT_D(f) = \Omega(n^\alpha)$.*

Proof:

We let g be a random boolean function such that $|g^{-1}(1)| = 2^{n^\alpha}$.

Most such functions must be such that $AT_D(g) = \Omega(n^\alpha)$ and we let g be one such function.

We now create f by padding with one extra bit to include a larger set of values for which $f = 1$:

We define $f : \{0,1\}^n \times \{0,1\} \to \{0,1\}$:

$$f(x,y) = \begin{cases} g(x) & \text{if } y = 0 \\ 1 & \text{otherwise} \end{cases}$$

We have:

$$f^{-1}(0) = g^{-1}(0) \times \{0\}$$

$$f^{-1}(1) = (g^{-1}(1) \times \{0\}) \cup (\{0,1\}^n \times \{1\})$$

Note that $|f^{-1}(0)| = 2^n - 2^{n^\alpha}$, and $|f^{-1}(1)| = 2^n + 2^{n^\alpha}$.

The proof of theorem 1 gives us:

$$AC_D(f) \leq E_{(x,y)\in_u f^{-1}(0)\times f^{-1}(1)} min(time_C(x), time_C(y)) \leq E_{y\in f^{-1}(1)}(time_C(y)) ,$$

for any circuit C that computes f.

Because $2^n >> 2^{n^\alpha}$, and because the last bit can be determined in unit time, we have $AC_D(f) \leq E_{y\in f^{-1}(1)}(time_C(y)) = O(1)$ and then the thesis follows by noting that $AT_D(f) = AT_D(g) = \Omega(n^\alpha)$.
□

References

[FKN91] T. Feder, E. Kushilevitz, M. Naor, *Amortized Communication Complexity*, Proc. 32nd Symposium on the Foundations of Computer Science, October 1991, pp. 239 - 248.

[JRS94] A. Jakoby, R. Reischuk, C. Schindelhauer, *Circuit Complexity: from the Worst Case to the Average Case*, Proc. 26th ACM Symposium on the Theory of Computing, May 1994, pp.58 - 67.

[KW90] M. Karchmer and A. Wigderson, *Monotone Circuits for Connectivity Require Superlogarithmic Depth*, Siam Journal of Discrete Math, vol. 3, no 2, May 1990, pp.255 - 265.

[L86] L. Levin, *Average Case Complexity Problems*, SIAM J. Computing 15, 1986, pp. 285-286.

[O91] A. Orlitsky, *Interactive Communication: Balanced Distributions, Correlated Files, and Average-Case Complexity*, Proc. 32nd Symposium on the Foundations of Computer Science, October 1991, pp. 228 - 238.

[RW89] R. Raz and A. Wigderson, *Probabilistic Communication Complexity of Boolean Relations*, Proc. 30th Symposium on the Foundations of Computer Science, October 1989, pp. 562 - 567.

[RW92] R. Raz and A. Wigderson, *Monotone Circuits for Matching Require Linear Depth*, Journal of the ACM v.39 1992.

[R85] A. A. Razborov, *A lower bound on the monotone network complexity of the logical permanent* Mat. Zametki v.37 n.6 1985 pp. 887 - 900.

[RS93] R. Reischuk, C. Schindelhauer, *Precise Average Case Complexity*, Proc. 10th Symposium on Theoretical Aspects of Computer Science, Feb. 1993, pp.650 - 661.

[W] H. S. Wilf, *Backtrack: An $O(1)$ expected time algorithm for the graph coloring problem*, Information Processing Letters v.18 n.3 1984 pp. 119-121.