Semi-unbounded fan-in circuits: Boolean vs. arithmetic *

Anna Gál †
The University of Chicago
Department of Computer Science
1100 E. 58th Street
Chicago, IL 60637
panni@cs.uchicago.edu

Abstract

We prove that polynomial size semi-unbounded fan-in Boolean circuits of depth d can be simulated by polynomial size semi-unbounded fan-in arithmetic circuits of depth $O(d+\log n)$, where the arithmetic operations $+$, $-$, $\times$ are performed in an arbitrary finite field. It is impossible to achieve this via gate-by-gate simulation. Instead, the proof is based on a randomized reduction to "unique witnesses" in the spirit of Valiant, Vazirani [VV], Mulmuley, Vazirani and Vazirani [MVV] and Wigderson [W].

1 Introduction

This paper extends the results of [W] to circuits. The problem is to simulate certain classes of Boolean circuits by the corresponding classes of arithmetic circuits. We consider Boolean circuits with gates from the standard Boolean basis $\{\wedge, \vee, \neg\}$, and arithmetic circuits with gates from the basis $\{+, -, \times\}$ over a finite field F. *Semi-unbounded fan-in* circuits have constant fan-in $\wedge$ (resp. $\times$) gates and unbounded fan-in $\vee$ (resp. $+$) gates. For semi-unbounded fan-in Boolean circuits we allow negations only at the input level.

Complexity classes defined by semi-unbounded fan-in Boolean circuits have been characterized in terms of several other models, and they correspond to some well known language classes. SAC^k denotes the class of

*To appear at Structure in Complexity Theory '95

†Most of this work was done while the author was visiting the Hebrew University in Jerusalem, partially supported by the Computer Science Department of the Hebrew University.

languages accepted by polynomial size, $O((\log n)^k)$ depth semi-unbounded fan-in Boolean circuits. SAC^1 is equal to the class $LOGCFL$ of languages logspace reducible to context-free languages [S], [V1]. Properties and characterizations of $LOGCFL$ are studied in [C], [SV]. Semi-unbounded fan-in circuits of larger depths correspond to extensions of context-free languages. For $d = \Omega(\log n)$ the class of languages accepted by polynomial size, depth $O(d)$ semi-unbounded fan-in circuits is identical to the class of languages accepted by nondeterministic auxiliary pushdown automata of $O(\log n)$ space and $2^{O(d)}$ time [C], [V1]. There are other characterizations of these language classes in terms of alternating Turing machines and first order formulae [I], [Ru], [V1]. These equivalences hold for both the uniform and the nonuniform versions of the models. For a survey see [BCDRT].

An interesting property of classes defined by semi-unbounded fan-in circuits, proved by Borodin et al. [BCDRT], is that they are closed under complementation for all depths that are $\Omega(\log n)$.

We consider the arithmetic analogs of the above complexity classes, defined by semi-unbounded fan-in arithmetic circuits. These classes have been studied for example in [AJ].

$\oplus SAC^k$ denotes the class of polynomials over $GF(2)$ computed by polynomial size, depth $O((\log n)^k)$ semi-unbounded fan-in arithmetic circuits over $GF(2)$.

We denote by $\hat{d}(f)$ (resp. $\hat{d}_F(f)$) the smallest depth of polynomial size semi-unbounded fan-in Boolean (resp. arithmetic) circuits for computing f.

We prove the following results.

Theorem 1 *For every Boolean function f on n variables and every finite field F, $\hat{d}_F(f) = O(\hat{d}(f) + \log n)$*

Corollary 1 $LOGCFL/poly \subseteq \oplus SAC^1/poly$

Theorem 2 *Every Boolean function f on n variables can be approximated, i.e. computed on $\geq (1 - 2^{-k})$ fraction of the inputs, by semi-unbounded fan-in arithmetic circuits over any fixed finite field in polynomial size and depth $O(\hat{d}(f) + \log k)$, for arbitrary $k > 0$.*

Valiant and Vazirani [VV] give a randomized reduction from SAT to $USAT$ (unique satisfiability). Given any Boolean formula F, their probabilistic construction yields another formula F', such that if F is not satisfiable then F' is not satisfiable, while if F is satisfiable then with reasonable

($\geq n^{-c}$) probability F' has a unique satisfying assignment. From this reduction, it follows that $NP/poly \subseteq \oplus P/poly$.

Avi Wigderson [W] proves that $NL/poly \subseteq \oplus L/poly$. The proof is based on a randomized reduction from $s-t$ connectivity to unique $s-t$ connectivity for directed graphs.

A single $\vee$ of m inputs can be expressed as a polynomial of degree m over any field. Thus it is easy to simulate unbounded fan-in polynomial size, depth d Boolean circuits by unbounded fan-in polynomial size, depth $O(d)$ arithmetic circuits simply by replacing each $\wedge$ gate by $\times$ and simulating each $\vee$ gate by such a polynomial. Similarly, bounded fan-in Boolean circuits are easy to simulate by bounded fan-in depth $O(d)$ arithmetic circuits.

The problem becomes nontrivial for semi-unbounded fan-in circuits, allowing the $\vee$ and $+$ gates to have unbounded fan-in while requiring the fan-in of the $\wedge$ and $\times$ gates to remain bounded.

For semi-unbounded fan-in circuits, replacing each $\vee$ gate by the corresponding polynomial we obtain $\Omega(d \log n)$ depth arithmetic circuits. Razborov [Ra] showed that an m-input $\vee$ can be well approximated by degree $\log m$ polynomials over finite fields. Using these polynomials and amplifying the approximation it is possible to get $O(d \log\log n + \log n)$ depth and polynomial size exact arithmetic circuits for our problem. However we cannot hope for further improvement if we try to simulate each $\vee$ gate separately.

We achieve the depth $O(d + \log n)$ simulation by a randomized reduction to "unique witnesses" using a slight modification of the Isolation Lemma of Mulmuley, Vazirani and Vazirani [MVV]. We note that the proof of [W] is based on using the Isolation Lemma, and that [MVV] showed that the Isolation Lemma can be used to prove the Valiant-Vazirani [VV] result for the clique function.

A different approach for comparing Boolean and arithmetic circuits is considered in [GS].

2 Certificates

We define our "unique witnesses" and describe the randomized reduction.

Let us consider an arbitrary Boolean circuit with $\vee$, $\wedge$ gates, provided with the $2n$ input literals $x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n$. Fixing a 0-1 assignment to the variables $x_1, \ldots, x_n$ determines the values computed by each gate of the circuit. We refer to the wires of the circuit as edges. The edges are oriented from the inputs of a gate g to g. For a fixed input assignment we label each edge of the circuit with the value computed by the gate at the starting node of the edge. For each gate that outputs 1, there is a set of edges all labelled

1 that forces the given gate to output 1. We call the graphs formed by these edges *certificates*. A certificate depends on the gate it belongs to and on the particular assignment to the input variables. There may be several certificates for the same gate on the same input. Gates that output 0 on a given input do not have certificates on that input.

Let us now give a formal definition of certificates. We denote the set of gates that are inputs to a given gate g by $I(g)$.

Definition 1 *The circuit Z is called a partial circuit of C if it satisfies the following conditions:*

- *the set of gates of Z is a subset of the set of gates of C*
- *the output gate of Z is the output gate of C,*
- *for every $\wedge$ gate g of Z, $I_Z(g) = I(g)$,*
- *for every $\vee$ gate g of Z, $\emptyset \neq I_Z(g) \subseteq I(g)$,*

where $I_Z(g)$ stands for the set of input gates to g in the circuit Z.

Definition 2 *A partial circuit Z is minimal, if for every $\vee$ gate g of Z, $|I_Z(g)| = 1$.*

Let α be a fixed assignment to the input variables. Let $\epsilon \in \{0, 1\}$. We say that $g(\alpha) = \epsilon$ if the gate g outputs the value ϵ on the input assignment α. We say that $C(\alpha) = \epsilon$ if the circuit C outputs the value ϵ on the input assignment α.

Observation 1 *If Z is a partial circuit of C then given any input assignment α, $Z(\alpha) \leq C(\alpha)$.*

Definition 3 *A certificate for $C(\alpha) = 1$ is a partial circuit Z of C that satisfies the condition that all the gates of Z output 1 on the assignment α.*

We note that an equivalent definition is to require that all the literals participating in Z are set to 1 by the assignment α.

Definition 4 *For a given gate g of a circuit C the subcircuit C_g is defined as follows:*

- *the set of gates of C_g is a subset of the set of gates of C,*

- *the output gate of C_g is the gate g,*
- *for every gate h of C_g, $I_{C_g}(h) = I(h)$.*

Definition 5 *A certificate for $C_g(\alpha) = 1$ is called a certificate for $g(\alpha) = 1$.*

We note that a certificate for $g(\alpha) = 1$ exists if and only if $g(\alpha) = 1$.

Definition 6 *A certificate is minimal if the corresponding partial circuit is minimal.*

Observation 2 *If there is a unique certificate for $g(\alpha) = 1$, it has to be a minimal certificate.*

Our randomized reduction will transform a $d = O(\log n)$ depth polynomial size circuit C into a polynomial size circuit C' of depth $\leq 2d$ with the property that on any fixed input α

- if $C(\alpha) = 0$ then $C'(\alpha) = 0$
- if $C(\alpha) = 1$ then with reasonable probability there is a unique certificate for $C'(\alpha) = 1$.

3 The Isolation Lemma

We state the Isolation Lemma of Mulmuley, Vazirani and Vazirani [MVV]. Let us consider the set system $(V, \mathcal{F})$ where $V = \{v_1, \ldots, v_n\}$ is a finite set, and $\mathcal{F}$ is a family of distinct subsets of V, i.e. $\mathcal{F} = \{F_1, \ldots, F_k\}$, $F_j \subseteq V$ for $1 \leq j \leq k$. Given weights w_i to each element $v_i \in V$, we define the weight of the set F_j to be $\sum_{v_i \in F_j} w_i$.

Isolation Lemma [MVV] *If we choose integer weights uniformly and independently from $[1, 2n]$ then with probability $\geq 1/2$ there is a unique minimum weight set in $\mathcal{F}$.*

In this paper we need a version of the Isolation Lemma that holds for multisets as well, i.e. for sets possibly containing some elements with multiplicities. The *support* of a multiset F is the set of elements occuring in F.

For multisets the Isolation Lemma does not hold in its original form. However the proof of the Isolation Lemma in [MVV] yields the following.

Lemma 1 *[MVV] Let $(V, \mathcal{F})$ be a multiset-system, where $\mathcal{F}$ is a family of multisets of the elements of V. Let us assign integer weights to the elements of V uniformly and independently from $[1, 2|V|]$. Then with probability $\geq 1/2$, all minimum weight sets in $\mathcal{F}$ have the same support.*

We note that Nisan [N] proved that the Isolation Lemma holds for multisets as well if we allow larger weights depending on the maximum multiplicity.

Let G be a partial circuit of the circuit C, and suppose that the edges of C have been assigned weights. Let E be the set of edges of G. For a given partial circuit G with edges E we define a multiset $\tilde{E}(G)$ with support E as follows. We expand G into a tree $\tilde{G}$ by taking the output of G to be the root and by splitting the nodes of G that have outdegree ≥ 2 into several copies. We define $\tilde{E}(G)$ to be the multiset of edges of G, taking each edge with multiplicity according to $\tilde{G}$. We assign the weight of each edge of G to all of its copies in $\tilde{E}(G)$.

Definition 7 *We define the weight of a partial circuit G to be the weight of the multiset $\tilde{E}(G)$.*

We define the weight of a certificate to be the weight of the corresponding partial circuit.

Lemma 2 *Let us assign integer weights to the edges of the circuit C uniformly and independently from $[1, 2m]$, where m is the number of edges of C. Then for every fixed input assignment α such that $C(\alpha) = 1$, with probability $\geq 1/2$, there is a unique minimum weight certificate for $C(\alpha) = 1$.*

Proof The statement of the lemma follows from Lemma 1, since multisets with the same support belong to the same certificate.

4 The randomized construction

Lemma 3 *Let C be a polynomial size, depth $d = O(\log n)$ circuit with unbounded fan-in $\vee$ gates and bounded fan-in $\wedge$ gates. Let m be the number of edges of C, and let c be the maximum fan-in of the $\wedge$ gates. One can construct a polynomial size, depth $\leq 2d$ circuit C' with unbounded fan-in $\vee$ gates and bounded fan-in $\wedge$ gates, such that*

- *if $C(\alpha) = 0$ then $C'(\alpha) = 0$*
- *if $C(\alpha) = 1$ then with probability $\geq 1/c^d 4m$, there is a unique certificate for $C'(\alpha) = 1$.*

Proof For simplicity, we present the construction for circuits with $\wedge$ gates of fan-in 2. It can be generalized easily to any fan-in c. The size remains polynomial if c is constant.

We assume that both C and C' are provided with the values of the $2n$ input literals $x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n$.

Let C be a Boolean circuit with $\vee$ gates of unbounded fan-in and $\wedge$ gates of fan-in 2, that has polynomial size and depth $d = O(\log n)$. Let m be the number of edges in the circuit. We assign a weight to each edge of the circuit by chosing a random integer uniformly and independently from $[1, 2m]$.

Next we choose a random integer L uniformly from $[1, 2^d 2m]$. ($2^d 2m$ is the maximum possible weight of a minimal certificate.)

Let us denote by $\Gamma(C)$ the set of gates of the circuit C.

$\Gamma(C')$ will consist of two disjoint classes of gates: principal gates and auxiliary gates. We denote the set of principal gates by Φ and the set of auxiliary gates by Φ_{aux}. Thus $\Gamma(C') = \Phi \,\dot{\cup}\, \Phi_{aux}$. All principal gates (except the ones for the literals) will be $\vee$ gates and all auxiliary gates will be $\wedge$ gates.

Φ will be a subset of $\Gamma(C) \times \{1, \ldots, L\}$. For a fixed $g \in \Gamma(C)$ the set $H(g) \subseteq \{g\} \times \{1, \ldots, L\}$ will denote the set of all principal gates of the form (g, i), and $\Phi = \dot{\bigcup}_{g \in \Gamma(C)} H(g)$.

If g is an $\wedge$ gate of C then the gate $(g, i) \in H(g)$ will be associated with a set $A(g, i) \subseteq \Phi_{aux}$ of auxiliary gates where $0 \leq |A(g, i)| \leq L^2$.

We refer to the gates in the sets $H(g)$ and $A(g, i)$ as copies of g.

We construct the circuit C' inductively. We say that a gate $g \in \Gamma(C)$ has been *processed* if we have created all its copies in C'.

We start by processing the literals. For each literal x_i^ϵ we create a gate labelled $(x_i^\epsilon, 0)$. This gate will output the value of the corresponding literal x_i^ϵ. Each literal will have only one copy.

Let $g \in \Gamma(C)$ be an $\vee$ gate that has all its input gates processed. Let w_h denote the weight of the edge from $h \in I(g)$ to g. For each gate $h \in I(g)$ we consider the set $H(h)$. For each $(h, i) \in H(h)$ we create an $\vee$ gate $(g, i + w_h)$ if $i + w_h \leq L$ and if $(g, i + w_h)$ has not been created yet. The input gates to the $\vee$ gate (g, j) are the gates (h, i) with $h \in I(g)$ satisfying $i + w_h = j$.

Let $g \in \Gamma(C)$ be an $\wedge$ gate with input gates h_1, h_2 such that h_1 and h_2 have been processed. Let w_1 and w_2 denote the weights of the corresponding edges from h_1 and h_2, resp., to g. For each pair of gates $(h_1, i) \in H(h_1)$, $(h_2, j) \in H(h_2)$ such that $i + j + w_1 + w_2 \leq L$ we create an $\wedge$ gate in $A(g, i + j + w_1 + w_2)$ with input gates $(h_1, i), (h_2, j)$. For each $k \in \{1, \ldots, L\}$ such that $A(g, k) \neq \emptyset$ we create an $\vee$ gate (g, k) with input set $I((g, k)) = A(g, k)$.

Let g_{out} be the output gate of the circuit C. The output gate of the circuit C' will be the gate (g_{out}, L) if it exists. If we did not create such a gate, we make the output of C' to be constant 0.

The circuit C' we constructed has the following properties.

Observation 3 *Let g be any gate of C. Then $(g, w) \in \Gamma(C')$ if and only if the circuit C_g has a minimal partial circuit with weight w.*

Observation 4 *Let α be a fixed assignment to the input variables and $(g, w) \in \Gamma(C')$. Then $(g, w)(\alpha) = 1$ if and only if there is a minimal certificate for $g(\alpha) = 1$ with weight w.*

We note that these properties would not hold if we defined the weight of partial circuits and certificates as the weight of their set of edges instead of using Definition 7, and that these properties are crucial for proving Lemma 3.

Next we show that the circuit C' constructed this way satisfies the requirements of Lemma 3.

The depth of C' is $\leq 2d$ and the size of C' is $\leq 2L^3S = n^{O(1)}$, where S is the size of C.

For any gate g of C and all gates (g, i) of C' we have $(g, i)(\alpha) \leq g(\alpha)$ on any assignment α. Thus if $C(\alpha) = 0$ then $C'(\alpha) = 0$.

To prove that the last requirement of Lemma 3 is satisfied, we need the following lemma.

Let α be a fixed input assignment such that $C(\alpha) = 1$. Let $\mathcal{F}_\alpha \neq \emptyset$ be the family of all certificates for $C(\alpha) = 1$. Let W denote a fixed assignment of weights to the edges of C. Let $\rho(W, \alpha)$ denote the weight of the minimum weight certificate in $\mathcal{F}_\alpha$.

Lemma 4 *Suppose there is a unique minimum weight certificate in $\mathcal{F}_\alpha$ and suppose that $L = \rho(W, \alpha)$. Then there is a unique certificate for $C'(\alpha) = 1$.*

Proof From the conditions of the lemma it follows that there is a minimal certificate of weight L for $C(\alpha) = 1$. By Observations 3 and 4 this means that in the circuit C' there is a gate (g_{out}, L) (where g_{out} is the output gate of C), and that $C'(\alpha) = (g_{out}, L)(\alpha) = 1$.

Thus, there is a certificate for $C'(\alpha) = 1$. If it is not unique, then there is more than one minimal certificate for $C(\alpha) = 1$ with weight L, and we get a contradiction. This proves Lemma 4.

The probability that there is a unique minimum weight cerificate in $\mathcal{F}_\alpha$ and $L = \rho(W, \alpha)$ is at least $1/2 \cdot 1/(2^d 2m)$ (by Lemma 2 and by choosing

L uniformly from $[1, 2^d 2m]$). Thus, we proved that if $C(\alpha) = 1$ then with probability $\geq 1/2^d 4m$ there is a unique certificate for $C'(\alpha) = 1$. This concludes the proof of Lemma 3.

5 The simulation

Proof of Theorem 1 Let us first consider the case of depth $d = O(\log n)$ circuits. By a standard probabilistic argument it follows from Lemma 3 that there exist $T = c^d 8nm = n^{O(1)}$ circuits $C^1, \ldots, C^T$ such that the following is true for every input assignment α

- if $C(\alpha) = 0$ then $\forall i \in \{1, \ldots, T\}$, $C^i(\alpha) = 0$,
- if $C(\alpha) = 1$ then $\exists j \in \{1, \ldots, T\}$ such that there is a unique certificate for $C^j(\alpha) = 1$.

Now we are ready to construct the simulating arithmetic circuit. In each circuit C^i we replace each $\vee$ gate by a $+$ gate and each $\wedge$ gate by a $\times$ gate. We denote the new circuit by $\Diamond C^i$. We let the circuits $\Diamond C^1, \ldots, \Diamond C^T$ compute in parallel over a common input $x_1, \ldots, x_n, 1 - x_1, \ldots, 1 - x_n$. To their outputs we apply a transformation that turns any value that is different from 1 into 0, and keeps the values that are equal to 1 unchanged. Over a given finite field this takes a constant number of gates for each $\Diamond C^i$. To compute the $\vee$ of these values, recall that the $\vee$ of T variables can be represented by a polynomial of degree T over the given field. We compute this polynomial by a $\log T$ depth semi-unbounded fan-in circuit with $+$ and $\times$ gates. Let us denote the circuit obtained this way by $\Diamond C$.

The circuits $\Diamond C^1, \ldots, \Diamond C^T$ have the following property:

- if $C(\alpha) = 0$ then $\forall i \in \{1, \ldots, T\}$, $\Diamond C^i(\alpha) = 0$,
- if $C(\alpha) = 1$ then $\exists j \in \{1, \ldots, T\}$ such that $\Diamond C^j(\alpha) = 1$.

This follows from the corresponding properties of the circuits $C^1, \ldots, C^T$ and from the fact that if there is a unique certificate for $C^j(\alpha) = 1$ then $\Diamond C^j(\alpha) = 1$.

We conclude that on any input assignment α, $C(\alpha) = \Diamond C(\alpha)$. This proves the theorem if $d = O(\log n)$.

For larger d we divide the circuit C into $r = \log n$ depth parts and perform the above simulation on each part. The total depth of the simulating circuit will be $\leq (d/r) \cdot (2r + O(\log n)) = O(d + \log n)$, which concludes the proof of Theorem 1.

For proving Theorem 2 we construct the circuits $\Diamond C^1, \ldots, \Diamond C^T$ and transform their outputs to Boolean values as above. To achieve the $O(d + \log k)$ depth for approximate simulations over a fixed finite field we use polynomials of degree k that approximate the $\vee$ of these values. By [Ra] (cf. [Sm], Lemma 1) given any probability distribution on the 2^T inputs there exist polynomials of degree k that compute the $\vee$ of T variables with probability $\geq (1 - 2^{-k})$ over the input distribution. This proves Theorem 2.

Acknowledgements

I would like to thank Avi Wigderson for suggesting the problem and the approach of unique certificates, and for his help and support during this work. I would also like to thank László Babai, Amos Beimel and János Simon for their helpful comments. Venkateswaran independently suggested a similar construction [V2].

References

[AJ] E. Allender and J. Jiao: Depth reduction for noncommutative arithmetic circuits, In *Proc. of the 25th STOC*, (1993), pp. 515-522.

[BCDRT] A. Borodin, S. A. Cook, P. W. Dymond, W. L. Ruzzo, M. Tompa: Two applications of inductive counting for complementation problems, *SIAM J. Comput.*, Vol. 18, No. 3, (1989), pp. 559-578.

[C] S. A. Cook: A taxonomy of problems with fast parallel algorithms, *Inform. and Control*, 64 (1985), pp. 2-22.

[GS] J. von zur Gathen and G. Seroussi: Boolean circuits versus arithmetic circuits, *Inform. and Computation*, 91 (1991), pp. 142-154.

[I] N. Immerman: Upper and lower bounds on first order expressibility, *J. Comput. System Sci.*, 25 (1982), pp. 76-98.

[MVV] K. Mulmuley, U. Vazirani and V. Vazirani: Matching is as easy as matrix inversion, In *Proc. of the 19th STOC*, (1987), pp. 345-354.

[N] N. Nisan: Personal communication.

[Ra] A. A. Razborov: Lower bounds for the size of circuits of bounded depth with basis $\{\wedge, \oplus\}$, *Math. notes of the Academy of Sciences of the USSR*, 41(4), (1987), pp. 333-338.

[Ru] W. L. Ruzzo: Tree-size bounded alternation, *J. Comput. System Sci.*, 21, (1980), pp. 218-235.

[Sm] R. Smolensky: Algebraic methods in the theory of lower bounds for Boolean circuit complexity, In *Proc. of the 19th STOC*, (1987), pp. 77-82.

[SV] S. Skyum and L. G. Valiant: A complexity theory based on Boolean algebra, In *Proc. of the 22nd FOCS*, (1981), pp. 244-253.

[S] I. H. Sudborough: On the tape complexity of deterministic context-free languages, *J. Assoc. Comput. Mach.*, 25 (1978), pp. 405-414.

[V1] H. Venkateswaran: Properties that characterize LOGCFL, In *Proc. of the 19th STOC*, (1987), pp. 141-150.

[V2] H. Venkateswaran: Personal communication.

[VV] L. G. Valiant and V.V. Vazirani: NP is as easy as detecting unique solutions, *Theoretical Computer Science*, 47 (1986), pp. 85-93.

[W] A. Wigderson: $NL/poly \subseteq \oplus L/poly$, In *Proc. of 9th Conf. Structure in Complexity Theory*, (1994), pp. 59-62.