BRICS

Basic Research in Computer Science

BRICS RS-96-1 Brodal & Husfeldt: Symmetric Functions have Logarithmic Depth

A Communication Complexity Proof that Symmetric Functions have Logarithmic Depth

Gerth Stølting Brodal
Thore Husfeldt

BRICS Report Series **RS-96-1**

ISSN 0909-0878 **January 1996**

See back inner page for a list of recent publications in the BRICS Report Series. Copies may be obtained by contacting:

BRICS
Department of Computer Science
University of Aarhus
Ny Munkegade, building 540
DK - 8000 Aarhus C
Denmark

Telephone: +45 8942 3360
Telefax: +45 8942 3255
Internet: BRICS@brics.dk

BRICS publications are in general accessible through WWW and anonymous FTP:

http://www.brics.dk/
ftp ftp.brics.dk (cd pub/BRICS)

A COMMUNICATION COMPLEXITY PROOF THAT SYMMETRIC FUNCTIONS HAVE LOGARITHMIC DEPTH

GERTH STØLTING BRODAL AND THORE HUSFELDT

BRICS*
Department of Computer Science, University of Aarhus,
Ny Munkegade, DK–8000 Århus C, Denmark

Abstract. We present a direct protocol with logarithmic communication that finds an element in the symmetric difference of two sets of different size. This yields a simple proof that symmetric functions have logarithmic circuit depth.

1. Introduction

Alice and Bob, two co-operating but distant players, each hold a set $A, B \subseteq \{1, \ldots, n\}$ such that $|A| \neq |B|$. They want to find an element that is in one set but not in the other, using as little communication as possible.

We present a simple and asymptotically optimal protocol for this problem. This provides us with a completely new proof of an old and important result in Boolean circuit complexity, which we state as Theorem 1 below.

We consider circuits of fan-in two over the basis $\vee$, $\wedge$, and $\neg$. For a function f we let $d(f)$ denote the depth of the shallowest circuit that computes it. A function is *symmetric* if its value depends only on the number of ones in the argument. Parity and the threshold functions are popular examples.

Theorem 1. *If* $f\colon \{0,1\}^n \to \{0,1\}$ *is symmetric then* $d(f) \in \mathrm{O}(\log n)$.

Wegener [2] presents the standard proof of this result and provides a general treatment of Boolean circuit complexity.

1.1. **Notation.** To alleviate notation we assume that n is a power of two. We write log for the logarithm with base two. For a set A and integers l and s (for 'left' and 'size') we let $A^{l,s}$ denote the set $A \cap \{l, \ldots, l+s-1\}$.

2. How To Find Elements in the Symmetric Difference

We start with two solutions that are obvious but weaker. Let us first see how Alice and Bob can find an element in $(A - B) \cup (B - A)$ using $\mathrm{O}(\log^2 n)$ bits of communication.

Key words. Boolean circuit complexity, communication complexity, symmetric functions.

*Basic Research in Computer Science, Centre of the Danish National Research Foundation.

Part of this work was done while the first author was at the Hebrew University, Jerusalem, supported by a grant of the Danish Research Academy. The second author is supported by grant no. 9400044 of the Danish Natural Science Research Council.

The protocol for this is a binary search in $\log n$ rounds. Alice and Bob will maintain two integers l and s such that

$$|A^{l,s}| \neq |B^{l,s}| \ .$$

This means that a valid answer is known to exist in the current interval $\{l, \ldots, l+s-1\}$. Initially, $l = 1$ and $s = n$. The interval is halved each round: Bob sends $|B^{l,s/2}|$ to Alice, who decides in which half to continue the search and tells Bob.

Under the stronger assumption that the parities of $|A|$ and $|B|$ differ, Alice and Bob need to send only $2 \log n$ bits. They will ensure that

$$|A^{l,s}| \neq |B^{l,s}| \pmod 2$$

during the protocol. Each round, Bob sends the parity of $|B^{l,s/2}|$, from which Alice can infer (and tell Bob) in which half to continue.

The next result shows how to achieve the asymptotic bound of the latter protocol under the conditions of the former.

Proposition 2. *If $|A| \neq |B|$ then Alice and Bob can find an element in $(A - B) \cup (B - A)$ using $\mathrm{O}(\log n)$ bits of communication.*

Proof. In addtion to l and s as above, Alice and Bob maintain a *marker* $j = 0, 1, \ldots, \log n - 1$, defined as follows. Let the bitstrings $a, b \in \{0,1\}^{\log n}$ denote the binary representation of the two cardinalities, i.e. $\sum a_i 2^i = |A^{l,s}|$ and $\sum b_i 2^i = |B^{l,s}|$. Then j marks a position where these two strings differ, so we have

$$|A^{l,s}| \neq |B^{l,s}| \pmod{2^{j+1}} \ . \tag{1}$$

Initially, such a marker can be found using $\mathrm{O}(\log n)$ bits of communication.

We introduce bitstrings a' and a'' for the two halves of Alice's current interval. More precisely, a' and a'' are the binary representations of $|A^{l,s/2}|$ and $|A^{l+s/2,s/2}|$, respectively. Similarly, b' and b'' represent Bob's intervals.

Bob starts each round by sending b'_j and b''_j. There are two cases.

1. If $a'_j \neq b'_j$ or $a''_j \neq b''_j$ then Alice and Bob can leave the marker unchanged and continue the search in the corresponding interval.
2. Otherwise, Alice and Bob have to look for a new marker. To this end, Bob sends b'_i and b''_i for decreasing values of $i = j-1, j-2, \ldots$. Alice tells him to stop when $a'_i \neq b'_i$ or $a''_i \neq b''_i$. The invariant (1) makes sure that such an $i < j$ exists. This yields a new interval and a new marker.

The two players use a constant number of bits in each of the $\log n$ rounds to decide which case they are in and each time i is decreased by one. The latter happens at most $\log n$ times in the entire protocol. $\square$

3. Symmetric Functions Have Logarithmic Circuit Depth

To prove Theorem 1 we use the well-known equivalence result of Karchmer and Wigderson [1], which we state for completeness. Let f be a Boolean function. Let R_f denote the game in which Alice gets $A \in f^{-1}(0)$, Bob gets $B \in f^{-1}(1)$, and they want to find an index where their input strings differ. The communication complexity of R_f is the minimal number of bits they have to exchange.

Lemma 3 (Karchmer–Wigderson)**.** *The communication complexity of R_f is $d(f)$ bits.*

The theorem follows from this lemma and the result of the last section, since if f is symmetric and $A \in f^{-1}(0), B \in f^{-1}(1)$ then we have of course $|A| \neq |B|$.

References

[1] Mauricio Karchmer and Avi Wigderson. Monotone circuits for connectivity require super-logarithmic depth. *SIAM Journal of Computing*, 3(2):255–265, May 1990.

[2] Ingo Wegener. *The Complexity of Boolean Functions*. Teubner, Stuttgart/Wiley & Sons, Chichester, 1987.

Recent Publications in the BRICS Report Series

RS-96-1 **Gerth Stølting Brodal and Thore Husfeldt.** *A Communication Complexity Proof that Symmetric Functions have Logarithmic Depth*. **January 1996. 3 pp.**

RS-95-59 **Luca Aceto and Anna Ingólfsdóttir.** *On the Finitary Bisimulation*. **November 1995. 29 pp.**

RS-95-58 **Nils Klarlund, Madhavan Mukund, and Milind Sohoni.** *Determinizing Asynchronous Automata on Infinite Inputs*. **November 1995. 32 pp.**

RS-95-57 **Jaap van Oosten.** *Topological Aspects of Traces*. **November 1995. 16 pp.**

RS-95-56 **Luca Aceto, Wan J. Fokkink, Rob J. van Glabbeek, and Anna Ingólfsdóttir.** *Axiomatizing Prefix Iteration with Silent Steps*. **November 1995. 25 pp.**

RS-95-55 **Mogens Nielsen and Kim Sunesen.** *Trace Equivalence - Partially Decidable!* **November 1995.**

RS-95-54 **Nils Klarlund, Mogens Nielsen, and Kim Sunesen.** *Using Monadic Second-Order Logic with Finite Domains for Specification and Verification*. **November 1995.**

RS-95-53 **Nils Klarlund, Mogens Nielsen, and Kim Sunesen.** *Automated Logical Verification based on Trace Abstractions*. **November 1995.**

RS-95-52 **Anton´n Kucera.** *Deciding Regularity in Process Algebras*. **October 1995. 42 pp.**

RS-95-51 **Rowan Davies.** *A Temporal-Logic Approach to Binding-Time Analysis*. **October 1995. 11 pp.**

RS-95-50 **Dany Breslauer.** *On Competitive On-Line Paging with Lookahead*. **September 1995. 12 pp.**

RS-95-49 **Mayer Goldberg.** *Solving Equations in the λ-Calculus using Syntactic Encapsulation*. **September 1995. 13 pp.**

RS-95-48 **Devdatt P. Dubhashi.** *Simple Proofs of Occupancy Tail Bounds*. **September 1995. 7 pp. To appear in** *Random Structures and Algorithms*.