Uniform Direct Product Theorems: Simplified, Optimized, and Derandomized

[Extended Abstract]

Russell Impagliazzo *
UC San Diego
La Jolla, CA, USA
russell@cs.ucsd.edu

Ragesh Jaiswal †
UC San Diego
La Jolla, CA, USA
rjaiswal@cs.ucsd.edu

Valentine Kabanets
Simon Fraser University
Vancouver, BC, Canada
kabanets@cs.sfu.ca

Avi Wigderson
Institute of Advanced Studies
Princeton, NJ, USA
avi@ias.edu

ABSTRACT

The classical Direct-Product Theorem for circuits says that if a Boolean function $f : \{0,1\}^n \to \{0,1\}$ is somewhat hard to compute on average by small circuits, then the corresponding k-wise direct product function $f^k(x_1,\ldots,x_k) = (f(x_1),\ldots,f(x_k))$ (where each $x_i \in \{0,1\}^n$) is significantly harder to compute on average by slightly smaller circuits. We prove a *fully uniform* version of the Direct-Product Theorem with information-theoretically *optimal* parameters, up to constant factors. Namely, we show that for given k and ϵ, there is an efficient randomized algorithm A with the following property. Given a circuit C that computes f^k on at least ϵ fraction of inputs, the algorithm A outputs with probability at least 3/4 a list of $O(1/\epsilon)$ circuits such that at least one of the circuits on the list computes f on more than $1-\delta$ fraction of inputs, for $\delta = O((\log 1/\epsilon)/k)$. Moreover, each output circuit is an AC^0 circuit (of size $\mathrm{poly}(n, k, \log 1/\delta, 1/\epsilon)$), with oracle access to the circuit C.

Using the Goldreich-Levin decoding algorithm [5], we also get a *fully uniform* version of Yao's XOR Lemma [18] with *optimal* parameters, up to constant factors. Our results simplify and improve those in [10].

Our main result may be viewed as an efficient approximate, local, list-decoding algorithm for direct-product codes (encoding a function by its values on all k-tuples) with optimal parameters. We generalize it to a family of "derandomized" direct-product codes, which we call *intersection codes*, where the encoding provides values of the function only on a subfamily of k-tuples. The quality of the decoding algorithm is then determined by sampling properties of the sets in this family and their intersections. As a direct consequence of this generalization we obtain the first derandomized direct product result in the uniform setting, allowing hardness amplification with only constant (as opposed to a factor of k) increase in the input length. Finally, this general setting naturally allows the decoding of concatenated codes, which further yields nearly optimal derandomized amplification.

Categories and Subject Descriptors

F.2.0 [**Analysis of Algorithms and Problem Complexity**]: General; G.3 [**Probability and Statistics**]: probabilistic algorithms

General Terms

Theory

Keywords

Direct Product Theorem, Direct Product Code, XOR Code

1. INTRODUCTION

Applications such as cryptography and derandomization require reliably hard problems, ones that cannot be solved by any fast algorithm with even a non-trivial advantage over random guessing. Direct-product theorems are a primary tool in hardness amplification, allowing one to convert problems that are somewhat hard into problems that are more reliably hard. In a direct-product theorem, we start with a function f such that any feasible algorithm has a non-negligible chance of failing to compute $f(x)$ given a random x. We then show that no feasible algorithm can, given multiple instances of the problem $x_1,\ldots,x_k$, compute all of the values $f(x_i)$, with even a small probability of success. (Usually, the x_i's are chosen independently, but there are also derandomized direct-product theorems where the x_i's are chosen pseudo-randomly.) Many strong direct product theorems are known for non-uniform models, such as Boolean

*The author is also currently a member of the School of Mathematics at the Institute of Advanced Studies, Princeton, NJ, USA. Research partially supported by NSF Grants 0716790 and 0515332. Views expressed here are not endorsed by the NSF.

†Research partially supported by NSF Grant 0716790. Views expressed here are not endorsed by the NSF.

STOC'08, May 17–20, 2008, Victoria, British Columbia, Canada.