

*

On Yao's XOR-Lemma*

Oded Goldreich[†]

Noam Nisan[‡]

Avi Wigderson[§]

March 1995 (corrected December 1995, March and November 1998)

Abstract

A fundamental Lemma of Yao states that computational weak-unpredictability of functions gets amplified if the results of several independent instances are XOR together. We survey two known proofs of Yao's Lemma and present a third alternative proof. The third proof proceeds by first proving that a function constructed by *concatenating* the values of the function on several independent instances is much more unpredictable, with respect to specified complexity bounds, than the original function. This statement turns out to be easier to prove than the XOR-Lemma. Using a result of Goldreich and Levin and some elementary observation, we derive the XOR-Lemma.

* Work done in part while the authors were visiting BRICS, Basic Research in Computer Science, Center of the Danish National Research Foundation.

[†]Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot, Israel. Partially supported by grant No. 92-00226 from the United States – Israel Binational Science Foundation (BSF), Jerusalem, Israel.

[‡]Institute for Computer Science, Hebrew University, Jerusalem, Israel.

[§] Institute for Computer Science, Hebrew University, Jerusalem, Israel.