On Span Programs

Mauricio Karchmer
Avi Wigderson

Abstract

We introduce a linear algebraic model of computation, the Span Program, and prove several upper and lower bounds on it. These results yield the following applications in complexity and cryptography:

- $SL \subset \oplus L$ (a weak Logspace analogue of $NP \subset \oplus P$).
- The first super-linear size lower bounds on branching programs that count.
- A broader class of functions which posses information-theoretic secret sharing schemes.

The proof of the main connection, between span programs and counting branching programs, uses a variant of Razborov's general approximation method.