

Linear Circuits over $GF(2)$

Noga Alon
Mauricio Karchmer
Avi Wigderson

Abstract

For $n=2^k$, let S be an $n \times n$ matrix whose rows and columns are indexed by $GF(2)^k$ and, for $i, j \in GF(2)^k$, $S_{i,j} = \langle i, j \rangle$, the standard inner product. Size-depth trade-offs are investigated for computing Sx with circuits using only linear operations. In particular, linear size circuits with depth bounded by the inverse of an Ackerman function are constructed, and it is shown that depth two circuits require $\Omega(n \log n)$ size. The lower bound applies to any Hadamard matrix.