Dispersers and Circuit Lower Bounds

Alexander Golovnev
New York University

ITCS 2016

Dispersers

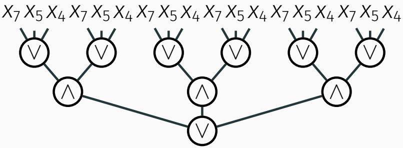
$f\colon \{0,1\}^n \to \{0,1\}$ is a disperser if $f|_S \not\equiv \text{const}$,
$\forall S = \{x \in \{0,1\}^n \colon p_1(x) = \ldots = p_k(x) = 0\}$.

DEPTH-3 CIRCUITS

Dispersers

$f\colon \{0,1\}^n \to \{0,1\}$ is a disperser if $f|_S \not\equiv$ const,
$\forall S = \{x \in \{0,1\}^n\colon p_1(x) = \ldots = p_k(x) = 0\}$.

- Bit-fixing Disperser
  - $p_i(x) = x_j \oplus c_j$
  - parity
  - $\Sigma_3(f) \geq 2^{\Omega(\sqrt{n})}$ [Hås89]



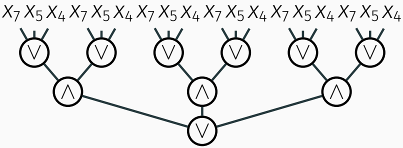
depth: 3, bottom fan-in: unbounded

DEPTH-3 CIRCUITS

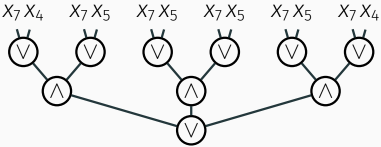
Dispersers

$f\colon \{0,1\}^n \to \{0,1\}$ is a disperser if $f|_S \not\equiv$ const,
$\forall S = \{x \in \{0,1\}^n \colon p_1(x) = \ldots = p_k(x) = 0\}$.

- Bit-fixing Disperser
    - $p_i(x) = x_j \oplus c_j$
    - parity
    - $\Sigma_3(f) \geq 2^{\Omega(\sqrt{n})}$ [Hås89]
- Projections Disperser
    - $p_i(x) = x_j \oplus x_k \oplus c_j$
    - BCH codes [PSZ97]
    - $\Sigma_3^2(f) \geq 2^{n-o(n)}$ [PSZ97]



depth: 3, bottom fan-in: unbounded

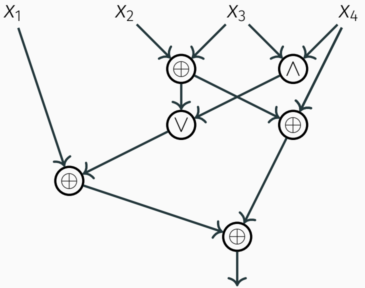


depth: 3, bottom fan-in: 2

Dispersers

$f\colon \{0,1\}^n \to \{0,1\}$ is a disperser if $f|_S \not\equiv$ const,
$\forall S = \{x \in \{0,1\}^n \colon p_1(x) = \ldots = p_k(x) = 0\}$.

- Affine Disperser
  - $p_i(x) = \bigoplus_{j \in J} x_j \oplus c_i$
  - constructions in P [BK09]
  - $C(f) \geq 3.01n$ [FGHK16]

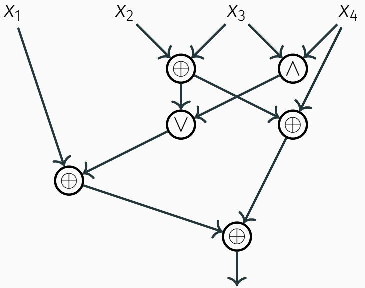


depth: unbounded, fan-in: 2

Dispersers

$f\colon \{0,1\}^n \to \{0,1\}$ is a disperser if $f|_S \not\equiv$ const,
$\forall S = \{x \in \{0,1\}^n \colon p_1(x) = \ldots = p_k(x) = 0\}$.

- Affine Disperser
    - $p_i(x) = \bigoplus_{j \in J} x_j \oplus c_i$
    - constructions in **P** [BK09]
    - $C(f) \geq 3.01n$ [FGHK16]
- Quadratic Disperser
    - $\deg(p_i) \leq 2$
    - over large fields [Dvi09]
    - $C(f) \geq 3.1n$ [GK16]

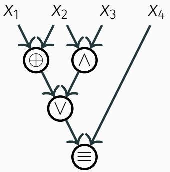


depth: unbounded, fan-in: 2

Dispersers

$f\colon \{0,1\}^n \to \{0,1\}$ is a disperser if $f|_S \not\equiv$ const,
$\forall S = \{x \in \{0,1\}^n \colon p_1(x) = \ldots = p_k(x) = 0\}$.

- Varieties of const deg
  - $\deg(p_i) \leq$ const
  - no known constructions
  - $\omega(n)$-bound for s.-p. NC_1



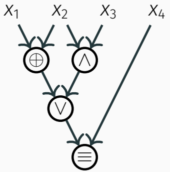
depth: $O(\log n)$, fan-in: 2
series-parallel circuit

LOG-DEPTH CIRCUITS

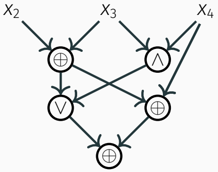
Dispersers

$f\colon \{0,1\}^n \to \{0,1\}$ is a disperser if $f|_S \not\equiv \text{const}$,
$\forall S = \{x \in \{0,1\}^n \colon p_1(x) = \ldots = p_k(x) = 0\}$.

- Varieties of const deg
    - $\deg(p_i) \leq \text{const}$
    - no known constructions
    - $\omega(n)$-bound for s.-p. $\mathbf{NC_1}$
- Varieties of poly deg
    - $\deg(p_i) \leq n^{\varepsilon}$
    - no known constructions
    - $\omega(n)$-bound for $\mathbf{NC_1}$



depth: $O(\log n)$, fan-in: 2
series-parallel circuit



depth: $O(\log n)$, fan-in: 2