

Nisan's Guarantees

- Nisan shows that if $t, w \leq c \cdot \ell$ for a constant c , then the PRG fools a w space algorithm
- If $w = \Omega(\log d)$ and we need $\text{poly}(d)$ bits \Rightarrow seed length of $O(w \log d)$ bits
- Can compute any block in time required to apply t hash functions from $\{0,1\}^\ell \rightarrow \{0,1\}^\ell$
 - Fool larger space $\Rightarrow \ell$ needs to be large and the evaluation is slow

HashPRG