From Independence to Expansion and Back Again

Tobias Christiani, Rasmus Pagh
IT University of Copenhagen

Mikkel Thorup
University of Copenhagen
Introduction

Topic of this talk:
- Upper bounds on the space-time tradeoff of $k$-independent functions in the word RAM model
Introduction

Topic of this talk:
• Upper bounds on the space-time tradeoff of $k$-independent functions in the word RAM model

**Definition** A family of functions $\mathcal{F}$ from $[u]$ to $[r]$ is $k$-independent if for every set of $k$ distinct keys $x_1, x_2, \ldots, x_k \in [u]$ and $k$ values $y_1, y_2, \ldots, y_k \in [r]$ we have that

$$\Pr_{f \in \mathcal{F}}[f(x_1) = y_1, f(x_2) = y_2, \ldots, f(x_k) = y_k] = r^{-k}$$
Introduction

Topic of this talk:
- Upper bounds on the space-time tradeoff of $k$-independent functions in the word RAM model

**Definition** A family of functions $\mathcal{F}$ from $[u]$ to $[r]$ is $k$-independent if for every set of $k$ distinct keys $x_1, x_2, \ldots, x_k \in [u]$ and $k$ values $y_1, y_2, \ldots, y_k \in [r]$ we have that

$$\Pr_{f \in \mathcal{F}}[f(x_1) = y_1, f(x_2) = y_2, \ldots, f(x_k) = y_k] = r^{-k}$$

- Example of a $k$-independent function:

$$f(x) = \sum_{i=0}^{k-1} a_i x^i \mod p$$
Introduction

Topic of this talk:
- Upper bounds on the space-time tradeoff of $k$-independent functions in the word RAM model

**Definition** A family of functions $\mathcal{F}$ from $[u]$ to $[r]$ is $k$-independent if for every set of $k$ distinct keys $x_1, x_2, \ldots, x_k \in [u]$ and $k$ values $y_1, y_2, \ldots, y_k \in [r]$ we have that

$$\Pr_{f \in \mathcal{F}}[f(x_1) = y_1, f(x_2) = y_2, \ldots, f(x_k) = y_k] = r^{-k}$$

- Example of a $k$-independent function:

$$f(x) = \sum_{i=0}^{k-1} a_i x^i \mod p$$

- Tradeoff:
  - Space used to represent $f \in \mathcal{F}$
  - Time used to evaluate $f \in \mathcal{F}$
Theorem [Siegel’89] A data structure for representing a $k$-independent function $f : [u] \rightarrow [r]$ with evaluation time $t < k$ must use at least $ku^{1/t}$ words of space.
Lower bound

Theorem [Siegel’89] A data structure for representing a $k$-independent function $f : [u] \rightarrow [r]$ with evaluation time $t < k$ must use at least $ku^{1/t}$ words of space.

Main result (vanilla version)

Randomized data structure for representing a $k$-independent function $f : [u] \rightarrow [r]$ with a space usage of $O(ku^{1/t}t)$ and evaluation time $O(t \log t)$.
Space-time tradeoff: Lower and upper bounds

Lower bound

**Theorem [Siegel’89]** A data structure for representing a $k$-independent function $f : [u] \rightarrow [r]$ with evaluation time $t < k$ must use at least $ku^{1/t}$ words of space.

Main result (vanilla version)

Randomized data structure for representing a $k$-independent function $f : [u] \rightarrow [r]$ with a space usage of $O(ku^{1/t})$ and evaluation time $O(t \log t)$.

Previous results

<table>
<thead>
<tr>
<th>Reference</th>
<th>Space</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polynomials [Joffe’74]</td>
<td>$O(k)$</td>
<td>$O(k)$</td>
</tr>
<tr>
<td>Graph powering [Siegel’89]</td>
<td>$O(k^tu^{1/t})$</td>
<td>$O(t)^t$</td>
</tr>
<tr>
<td>Recursive tabulation [Thorup’13]</td>
<td>$O(\text{poly } k + u^{1/t})$</td>
<td>$O(t^{\log t})$</td>
</tr>
</tbody>
</table>
Constructions of $k$-independent families of functions based on bipartite expander graphs

Neighbor function $\Gamma : U \rightarrow V^d$
• Constructions of $k$-independent families of functions based on bipartite expander graphs

• Neighbor function $\Gamma : U \rightarrow V^d$

**Definition** A bipartite graph $\Gamma$ is $k$-unique if for every $S \subseteq U$ with $|S| \leq k$ there exists $v \in V$ with exactly one neighbor in $S$
• Constructions of $k$-independent families of functions based on bipartite expander graphs

• Neighbor function $\Gamma : U \rightarrow V^d$

**Definition** A bipartite graph $\Gamma$ is $k$-unique if for every $S \subseteq U$ with $|S| \leq k$ there exists $v \in V$ with exactly one neighbor in $S$
• Constructions of $k$-independent families of functions based on bipartite expander graphs

• Neighbor function $\Gamma : U \rightarrow V^d$

**Definition** A bipartite graph $\Gamma$ is $k$-unique if for every $S \subseteq U$ with $|S| \leq k$ there exists $v \in V$ with exactly one neighbor in $S$
From independence to expansion and back again

- Constructions of $k$-independent families of functions based on bipartite expander graphs
- Neighbor function $\Gamma : U \rightarrow V^d$

**Definition** A bipartite graph $\Gamma$ is $k$-unique if for every $S \subseteq U$ with $|S| \leq k$ there exists $v \in V$ with exactly one neighbor in $S$
From expansion to independence

- Constructions of $k$-independent families of functions based on bipartite expander graphs
- Neighbor function $\Gamma : U \rightarrow V^d$

**Definition** A bipartite graph $\Gamma$ is $k$-unique if for every $S \subseteq U$ with $|S| \leq k$ there exists $v \in V$ with exactly one neighbor in $S$

**Lemma** [Siegel’89] Let $\Gamma : U \rightarrow V^d$ be $k$-unique and $h : V \rightarrow [r]$ be a random function. Then $f(x) = \sum_i h(\Gamma(x)_i) \mod r$ defines a $k$-independent family of functions
From expansion to independence

- Constructions of $k$-independent families of functions based on bipartite expander graphs
- Neighbor function $\Gamma : U \rightarrow V^d$

**Definition** A bipartite graph $\Gamma$ is $k$-unique if for every $S \subseteq U$ with $|S| \leq k$ there exists $v \in V$ with exactly one neighbor in $S$

- Peeling argument example:

$$f(x_3) = h(v_2) + h(v_4) + h(v_5) \mod r$$

**Lemma [Siegel’89]** Let $\Gamma : U \rightarrow V^d$ be $k$-unique and $h : V \rightarrow [r]$ be a random function. Then $f(x) = \sum_i h(\Gamma(x)_i) \mod r$ defines a $k$-independent family of functions
From expansion to independence

- Constructions of \( k \)-independent families of functions based on bipartite expander graphs
- Neighbor function \( \Gamma : U \to V^d \)

**Definition** A bipartite graph \( \Gamma \) is \( k \)-unique if for every \( S \subseteq U \) with \( |S| \leq k \) there exists \( v \in V \) with exactly one neighbor in \( S \)

- Peeling argument example:
  \[
  f(x_3) = h(v_2) + h(v_4) + h(v_5) \mod r
  \]

**Lemma [Siegel’89]** Let \( \Gamma : U \to V^d \) be \( k \)-unique and \( h : V \to [r] \) be a random function. Then \( f(x) = \sum_i h(\Gamma(x)_i) \mod r \) defines a \( k \)-independent family of functions
• Constructions of $k$-independent families of functions based on bipartite expander graphs

• Neighbor function $\Gamma : U \rightarrow V^d$

**Definition** A bipartite graph $\Gamma$ is $k$-unique if for every $S \subseteq U$ with $|S| \leq k$ there exists $v \in V$ with exactly one neighbor in $S$

• Peeling argument example:

$$f(x_3) = h(v_2) + h(v_4) + h(v_5) \mod r$$

**Lemma [Siegel’89]** Let $\Gamma : U \rightarrow V^d$ be $k$-unique and $h : V \rightarrow [r]$ be a random function. Then $f(x) = \sum_i h(\Gamma(x)_i) \mod r$ defines a $k$-independent family of functions
From expansion to independence

- Constructions of $k$-independent families of functions based on bipartite expander graphs
- Neighbor function $\Gamma : U \rightarrow V^d$

**Definition** A bipartite graph $\Gamma$ is $k$-unique if for every $S \subseteq U$ with $|S| \leq k$ there exists $v \in V$ with exactly one neighbor in $S$

- Peeling argument example:

$$f(x_3) = h(v_2) + h(v_4) + h(v_5) \mod r$$

**Lemma [Siegel’89]** Let $\Gamma : U \rightarrow V^d$ be $k$-unique and $h : V \rightarrow \mathbb{Z}_r$ be a random function. Then $f(x) = \sum_i h(\Gamma(x)_i) \mod r$ defines a $k$-independent family of functions
From expansion to independence

- Constructions of $k$-independent families of functions based on bipartite expander graphs
- Neighbor function $\Gamma : U \rightarrow V^d$

**Definition** A bipartite graph $\Gamma$ is $k$-unique if for every $S \subseteq U$ with $|S| \leq k$ there exists $v \in V$ with exactly one neighbor in $S$

- Peeling argument example:

$$f(x_3) = h(v_2) + h(v_4) + h(v_5) \mod r$$

**Lemma [Siegel’89]** Let $\Gamma : U \rightarrow V^d$ be $k$-unique and $h : V \rightarrow [r]$ be a random function. Then $f(x) = \sum_i h(\Gamma(x)_i) \mod r$ defines a $k$-independent family of functions
From expansion to independence

• Constructions of $k$-independent families of functions based on bipartite expander graphs
• Neighbor function $\Gamma : U \rightarrow V^d$

**Definition** A bipartite graph $\Gamma$ is $k$-unique if for every $S \subseteq U$ with $|S| \leq k$ there exists $v \in V$ with exactly one neighbor in $S$

• Peeling argument example:

$$ f(x_3) = h(v_2) + h(v_4) + h(v_5) \mod r $$

**Lemma [Siegel’89]** Let $\Gamma : U \rightarrow V^d$ be $k$-unique and $h : V \rightarrow [r]$ be a random function. Then $f(x) = \sum_i h(\Gamma(x)_i) \mod r$ defines a $k$-independent family of functions
Existence of optimal $k$-unique graphs

$k$-unique $\Gamma : U \rightarrow V^d$
Existence of optimal $k$-unique graphs

$k$-unique $\Gamma : U \rightarrow V^d$

$k$-independent family $\mathcal{F}$

\[ f(x) = \sum_i h(\Gamma(x)_i) \mod r \]

$h : V \rightarrow [r]$ is random

Space $|V|$  

Time $d$
Existence of optimal $k$-unique graphs

$k$-unique $\Gamma : U \rightarrow V^d$

$k$-independent family $\mathcal{F}$

$$f(x) = \sum_i h(\Gamma(x)_i) \mod r$$

$h : V \rightarrow [r]$ is random

Space $|V|$

Time $d$

**Lemma [Siegel’89]** Most graphs $\Gamma$ give an optimal space-time tradeoff for $k$-independent hashing
Existence of optimal $k$-unique graphs

$k$-unique $\Gamma : U \to V^d$

$k$-independent family $F$

$f(x) = \sum_i h(\Gamma(x)_i) \mod r$

$h : V \to [r]$ is random

Space $|V|$

Time $d$

**Lemma [Siegel’89]** Most graphs $\Gamma$ give an optimal space-time tradeoff for $k$-independent hashing

- Explicit $k$-unique graphs with optimal parameters are not known
Existence of optimal $k$-unique graphs

$k$-unique $\Gamma : U \to V^d$

$k$-independent family $\mathcal{F}$

$$f(x) = \sum_i h(\Gamma(x)_i) \mod r$$

$h : V \to [r]$ is random

Space $|V|$

Time $d$

Lemma [Siegel’89] Most graphs $\Gamma$ give an optimal space-time tradeoff for $k$-independent hashing

- Explicit $k$-unique graphs with optimal parameters are not known
- Storing a random $\Gamma$ defeats the purpose of $k$-independent hashing
Existence of optimal $k$-unique graphs

$k$-unique $\Gamma : U \to V^d$

$k$-independent family $\mathcal{F}$

$$f(x) = \sum_i h(\Gamma(x)_i) \mod r$$

$h : V \to [r]$ is random

Space $|V|$

Time $d$

**Lemma [Siegel’89]** Most graphs $\Gamma$ give an optimal space-time tradeoff for $k$-independent hashing

- Explicit $k$-unique graphs with optimal parameters are not known
- Storing a random $\Gamma$ defeats the purpose of $k$-independent hashing
- Verifying that a given $\Gamma$ is $k$-unique is infeasible
Set of all functions $\Gamma : U \rightarrow V^d$
Set of all functions $\Gamma : U \rightarrow V^d$

Optimally $k$-unique
Set of all functions $\Gamma : U \rightarrow V^d$

- Optimally $k$-unique
- $k$-independent family
Set of all functions $\Gamma : U \rightarrow V^d$

Optimally $k$-unique

$k$-independent family
Set of all functions $\Gamma : U \rightarrow V^d$

**Optimally $k$-unique**

$k$-independent family

**Lemma** A $k$-independent function $\Gamma : U \rightarrow V^d$ with $|U| = u$, $|V| = O(ku^{1/t}t)$ and $d = O(t)$ is $k$-unique with high probability.
Set of all functions $\Gamma : U \rightarrow V^d$

**Lemma** A $k$-independent function $\Gamma : U \rightarrow V^d$ with $|U| = u$, $|V| = O(ku^{1/t}t)$ and $d = O(t)$ is $k$-unique with high probability.

$k$-unique $\quad$ $k$-independent family $\quad$ $k$-unique whp.

$\Gamma \quad \rightarrow \quad \mathcal{F} \quad \rightarrow \quad \Gamma \in \mathcal{F}$
Overview of technique

$k$-unique
Overview of technique

Increase domain

$k$-unique
Overview of technique

$k$-unique

Increase domain

$k$-unique

Define family

$F$

$k$-independent
Overview of technique

$k$-unique

Increase domain

$\vdots$

Define family

$\vdots$

Sample $\Gamma \in \mathcal{F}$

$k$-independent

$k$-unique

$k$-unique

$k$-unique whp.
A randomized recursive construction of a $k$-unique function

- View $x \in [u]$ as a string of characters from an alphabet $\Sigma$

$$
\Gamma(ax) = \bigoplus_i h(a, \Gamma(x)_i), \quad a \in \Sigma, \ ax \in \Sigma^*
$$

$h : \Sigma \times V \rightarrow V^d$ is random
A randomized recursive construction of a $k$-unique function

- View $x \in [u]$ as a string of characters from an alphabet $\Sigma$

$$\Gamma(ax) = \bigoplus_i h(a, \Gamma(x)_i), \quad a \in \Sigma, \ ax \in \Sigma^*$$

$h : \Sigma \times V \rightarrow V^d$ is random
A randomized recursive construction of a $k$-unique function

- View $x \in [u]$ as a string of characters from an alphabet $\Sigma$

  $$\Gamma(ax) = \bigoplus_i h(a, \Gamma(x)_i), \quad a \in \Sigma, \ ax \in \Sigma^*$$

  $$h : \Sigma \times V \rightarrow V^d \text{ is random}$$
A randomized recursive construction of a $k$-unique function

- View $x \in [u]$ as a string of characters from an alphabet $\Sigma$

$$\Gamma(ax) = \bigoplus_i h(a, \Gamma(x)_i), \quad a \in \Sigma, \ ax \in \Sigma^*$$

$h : \Sigma \times V \to V^d$ is random
A randomized recursive construction of a $k$-unique function

- View $x \in [u]$ as a string of characters from an alphabet $\Sigma$

$$\Gamma(ax) = \bigoplus_i h(a, \Gamma(x)_i), \quad a \in \Sigma, \ ax \in \Sigma^*$$

$h : \Sigma \times V \rightarrow V^d$ is random

From Independence to Expansion and Back Again
A randomized recursive construction of a $k$-unique function

- View $x \in [u]$ as a string of characters from an alphabet $\Sigma$

$$\Gamma(ax) = \bigoplus_i h(a, \Gamma(x)_i), \quad a \in \Sigma, \ ax \in \Sigma^*$$

$h : \Sigma \times V \rightarrow V^d$ is random

Lemma $\Gamma$ is $k$-unique over $\Sigma^j$

$\Rightarrow \Gamma$ is $k$-independent over $\Sigma^{j+1}$

$\Rightarrow \Gamma$ is $k$-unique over $\Sigma^{j+1}$ whp.
A randomized recursive construction of a $k$-unique function

- View $x \in [u]$ as a string of characters from an alphabet $\Sigma$

$$\Gamma(ax) = \bigoplus_i h(a, \Gamma(x)_i), \quad a \in \Sigma, \ ax \in \Sigma^*$$

$h : \Sigma \times V \rightarrow V^d$ is random

**Lemma** $\Gamma$ is $k$-unique over $\Sigma^j$

$\implies \Gamma$ is $k$-independent over $\Sigma^{j+1}$

$\implies \Gamma$ is $k$-unique over $\Sigma^{j+1}$ whp.

- Parameterizing for $k$-independence with domain size $u$ and tradeoff parameter $t$

$$|\Sigma| = u^{1/2t}$$
$$|V| = O(ku^{1/2t}t)$$
$$d = O(t)$$

- Space $O(ku^{1/t}t^2)$. Time $O(t^2)$.
**Definition** A bipartite graph $\Gamma$ is $k$-majority-unique if for every $S \subseteq U$ with $|S| \leq k$ there exists $x \in S$ such that the majority of vertices in $\Gamma(\{x\})$ have exactly one neighbor in $S$. 

\[ U \quad \xrightarrow{d} \quad V \]
**Definition** A bipartite graph $\Gamma$ is $k$-majority-unique if for every $S \subseteq U$ with $|S| \leq k$ there exists $x \in S$ such that the majority of vertices in $\Gamma(\{x\})$ have exactly one neighbor in $S$. 
A stronger expansion property

**Definition** A bipartite graph $\Gamma$ is $k$-majority-unique if for every $S \subseteq U$ with $|S| \leq k$ there exists $x \in S$ such that the majority of vertices in $\Gamma(\{x\})$ have exactly one neighbor in $S$. 

![Diagram of a bipartite graph](image-url)
**Definition** A bipartite graph $\Gamma$ is $k$-majority-unique if for every $S \subseteq U$ with $|S| \leq k$ there exists $x \in S$ such that the majority of vertices in $\Gamma(\{x\})$ have exactly one neighbor in $S$.
Lemma Let $\Gamma$ be $k$-majority-unique over an alphabet $\Sigma$. Then the function defined by $\Gamma(x_1x_2)_i = \Gamma(x_1)_i\Gamma(x_2)_i$ is $k$-unique over $\Sigma^2$. 
**Lemma** Let $\Gamma$ be $k$-majority-unique over an alphabet $\Sigma$. Then the function defined by $\Gamma(x_1 x_2)_i = \Gamma(x_1)_i \Gamma(x_2)_i$ is $k$-unique over $\Sigma^2$.

**Proof:**
- Goal: Find a key $x'_1 x'_2 \in S \subseteq \Sigma^2$ that has a unique neighbor
Lemma Let $\Gamma$ be $k$-majority-unique over an alphabet $\Sigma$. Then the function defined by $\Gamma(x_1x_2)_i = \Gamma(x_1)_i\Gamma(x_2)_i$ is $k$-unique over $\Sigma^2$.

Proof:
• Goal: Find a key $x'_1x'_2 \in S \subseteq \Sigma^2$ that has a unique neighbor
• There exists $x'_1 \in \{x_1 \mid x_1x_2 \in S\}$ with $> d/2$ unique neighbors
Lemma Let $\Gamma$ be $k$-majority-unique over an alphabet $\Sigma$. Then the function defined by $\Gamma(x_1x_2)_i = \Gamma(x_1)_i \Gamma(x_2)_i$ is $k$-unique over $\Sigma^2$.

Proof:
- Goal: Find a key $x'_1 x'_2 \in S \subseteq \Sigma^2$ that has a unique neighbor
- There exists $x'_1 \in \{x_1 \mid x_1 x_2 \in S\}$ with $> d/2$ unique neighbors
Lemma Let $\Gamma$ be $k$-majority-unique over an alphabet $\Sigma$. Then the function defined by $\Gamma(x_1x_2)_i = \Gamma(x_1)_i\Gamma(x_2)_i$ is $k$-unique over $\Sigma^2$.

Proof:
- Goal: Find a key $x'_1x'_2 \in S \subseteq \Sigma^2$ that has a unique neighbor
- There exists $x'_1 \in \{x_1 \mid x_1x_2 \in S\}$ with $>d/2$ unique neighbors
- There exists $x'_2 \in \{x_2 \mid x'_1x_2 \in S\}$ with $>d/2$ unique neighbors
A graph product based on component-wise concatenation

**Lemma** Let $\Gamma$ be $k$-majority-unique over an alphabet $\Sigma$. Then the function defined by $\Gamma(x_1x_2)_i = \Gamma(x_1)_i \Gamma(x_2)_i$ is $k$-unique over $\Sigma^2$.

**Proof:**
- Goal: Find a key $x'_1 x'_2 \in S \subseteq \Sigma^2$ that has a unique neighbor
- There exists $x'_1 \in \{x_1 \mid x_1 x_2 \in S\}$ with $> d/2$ unique neighbors
- There exists $x'_2 \in \{x_2 \mid x'_1 x_2 \in S\}$ with $> d/2$ unique neighbors
**Lemma** Let $\Gamma$ be $k$-majority-unique over an alphabet $\Sigma$. Then the function defined by $\Gamma(x_1x_2)_i = \Gamma(x_1)_i\Gamma(x_2)_i$ is $k$-unique over $\Sigma^2$.

**Proof:**
- Goal: Find a key $x'_1 x'_2 \in S \subseteq \Sigma^2$ that has a unique neighbor
- There exists $x'_1 \in \{x_1 \mid x_1x_2 \in S\}$ with $> d/2$ unique neighbors
- There exists $x'_2 \in \{x_2 \mid x'_1x_2 \in S\}$ with $> d/2$ unique neighbors
Lemma Let $\Gamma$ be $k$-majority-unique over an alphabet $\Sigma$. Then the function defined by $\Gamma(x_1 x_2)_i = \Gamma(x_1)_i \Gamma(x_2)_i$ is $k$-unique over $\Sigma^2$.

Proof:
- Goal: Find a key $x'_1 x'_2 \in S \subseteq \Sigma^2$ that has a unique neighbor
- There exists $x'_1 \in \{x_1 \mid x_1 x_2 \in S\}$ with $> d/2$ unique neighbors
- There exists $x'_2 \in \{x_2 \mid x'_1 x_2 \in S\}$ with $> d/2$ unique neighbors
Lemma Let $\Gamma$ be $k$-majority-unique over an alphabet $\Sigma$. Then the function defined by $\Gamma(x_1 x_2)_i = \Gamma(x_1)_i \Gamma(x_2)_i$ is $k$-unique over $\Sigma^2$.

Proof:
- Goal: Find a key $x'_1 x'_2 \in S \subseteq \Sigma^2$ that has a unique neighbor
- There exists $x'_1 \in \{x_1 \mid x_1 x_2 \in S\}$ with $> d/2$ unique neighbors
- There exists $x'_2 \in \{x_2 \mid x'_1 x_2 \in S\}$ with $> d/2$ unique neighbors
Lemma Let $\Gamma$ be $k$-majority-unique over an alphabet $\Sigma$. Then the function defined by $\Gamma(x_1x_2)_i = \Gamma(x_1)_i\Gamma(x_2)_i$ is $k$-unique over $\Sigma^2$.

Proof:
- Goal: Find a key $x'_1x'_2 \in S \subseteq \Sigma^2$ that has a unique neighbor
- There exists $x'_1 \in \{x_1 \mid x_1x_2 \in S\}$ with $> d/2$ unique neighbors
- There exists $x'_2 \in \{x_2 \mid x'_1x_2 \in S\}$ with $> d/2$ unique neighbors
**Lemma** Let $\Gamma$ be $k$-majority-unique over an alphabet $\Sigma$. Then the function defined by $\Gamma(x_1x_2)_i = \Gamma(x_1)_i\Gamma(x_2)_i$ is $k$-unique over $\Sigma^2$.

**Proof:**
- Goal: Find a key $x'_1x'_2 \in S \subseteq \Sigma^2$ that has a unique neighbor
- There exists $x'_1 \in \{x_1 \mid x_1x_2 \in S\}$ with $> d/2$ unique neighbors
- There exists $x'_2 \in \{x_2 \mid x'_1x_2 \in S\}$ with $> d/2$ unique neighbors
A divide-and-conquer recursion

- View $x \in [u]$ as a string of two characters and recurse on each

$$\Gamma(x_1 x_2) = \bigoplus_i h(\Gamma(x_1)_i, \Gamma(x_2)_i)$$
A divide-and-conquer recursion

- View $x \in [u]$ as a string of two characters and recurse on each

$$
\Gamma(x_1 x_2) = \bigoplus_i h(\Gamma(x_1)_i, \Gamma(x_2)_i)
$$

<table>
<thead>
<tr>
<th>Universe</th>
<th>Degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u$</td>
<td>$d$</td>
</tr>
</tbody>
</table>
A divide-and-conquer recursion

- View $x \in [u]$ as a string of two characters and recurse on each

$$\Gamma(x_1 x_2) = \bigoplus_i h(\Gamma(x_1)_i, \Gamma(x_2)_i)$$

Universes: $u$  Degree: $d$

Degree: $d/2$
A divide-and-conquer recursion

- View $x \in [u]$ as a string of two characters and recurse on each

$$\Gamma(x_1 x_2) = \bigoplus_i h(\Gamma(x_1)_i, \Gamma(x_2)_i)$$

```
\begin{array}{c|cc|cc|cc|cc}
\Gamma(x) & \Gamma(x_1) & \Gamma(x_2) & \Gamma(x_{1,1}) & \Gamma(x_{1,2}) & \Gamma(x_{2,1}) & \Gamma(x_{2,2}) \\
\hline
\text{Universe} & u & u^{1/2} & u^{1/4} & \text{Degree} & d & d/2 & d/4
\end{array}
```
A divide-and-conquer recursion

- View $x \in [u]$ as a string of two characters and recurse on each

$$\Gamma(x_1 x_2) = \bigoplus_i h(\Gamma(x_1)_i, \Gamma(x_2)_i)$$

```
\begin{array}{c}
\Gamma(x) \\
| \rho | \\
\Gamma(x_1) \quad \Gamma(x_2) \\
| \rho | \\
\Gamma(x_{1,1}) \quad \Gamma(x_{1,2}) \quad \Gamma(x_{2,1}) \quad \Gamma(x_{2,2}) \\
| \rho | \quad | \rho | \quad | \rho | \\
\vdots \\
| \rho | \\
\end{array}
```

<table>
<thead>
<tr>
<th>Universe</th>
<th>Degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u$</td>
<td>$d$</td>
</tr>
<tr>
<td>$u^{1/2}$</td>
<td>$d/2$</td>
</tr>
<tr>
<td>$u^{1/4}$</td>
<td>$d/4$</td>
</tr>
</tbody>
</table>
A divide-and-conquer recursion

- View $x \in [u]$ as a string of two characters and recurse on each

$$\Gamma(x_1x_2) = \bigoplus_i h(\Gamma(x_1)_i, \Gamma(x_2)_i)$$

![Diagram of a divide-and-conquer recursion]

Problems:

- By the lower bound $h$ must have a domain of size at least $k^2$
  - Use the first recursion to implement $h$
A divide-and-conquer recursion

- View $x \in [u]$ as a string of two characters and recurse on each

$$\Gamma(x_1 x_2) = \bigoplus_i h(\Gamma(x_1)_i, \Gamma(x_2)_i)$$

Problems:

- By the lower bound $h$ must have a domain of size at least $k^2$
  - Use the first recursion to implement $h$

- Low space usage, high degree: representing $\Gamma(x)$ in few words
  - Graph products that take the structure of $S$ into account
Summary

Result:
• Near-optimal space-time tradeoff for $k$-independent functions
Summary

Result:
- Near-optimal space-time tradeoff for $k$-independent functions

Technique:
- Graph products and alternating between expansion and independence
Summary

Result:
- Near-optimal space-time tradeoff for $k$-independent functions

Technique:
- Graph products and alternating between expansion and independence

Open questions:
- Optimal expanders without $k$-independence
Summary

Result:
- Near-optimal space-time tradeoff for $k$-independent functions

Technique:
- Graph products and alternating between expansion and independence

Open questions:
- Optimal expanders without $k$-independence

Thanks for listening!