From Independence to Expansion and Back Again

Tobias Christiani, Rasmus Pagh
IT University of Copenhagen

Mikkel Thorup
University of Copenhagen

European Research Council
Established by the European Commission

Scalable Similarity Search

Topic of this talk:

- Upper bounds on the space-time tradeoff of k-independent functions in the word RAM model

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

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

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:

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

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

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

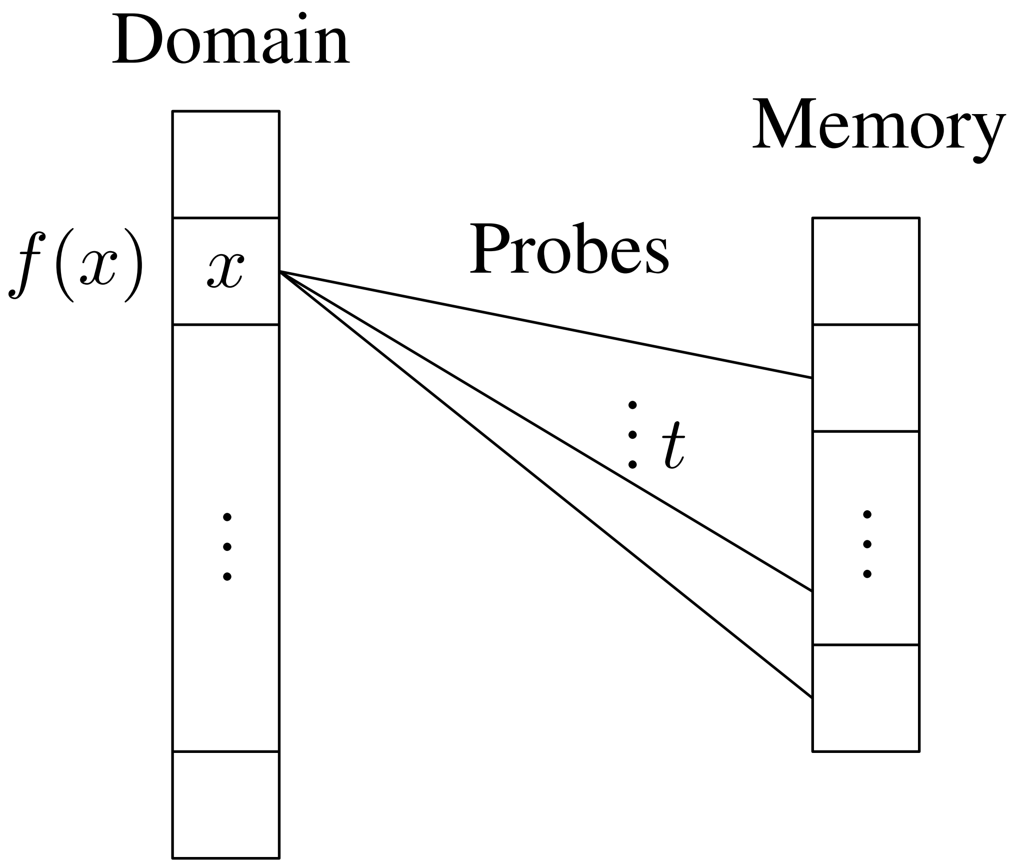
- Example of a k-independent function:

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

- Tradeoff:
  - Space used to represent $f \in \mathcal{F}$
  - Time used to evaluate $f \in \mathcal{F}$

Lower bound

Theorem [Siegel'89] A data structure for representing a k-independent function $f : [u] \to [r]$ 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 $f : [u] \to [r]$ 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 $f : [u] \to [r]$ with a space usage of $O(ku^{1/t}t)$ and evaluation time $O(t \log t)$

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

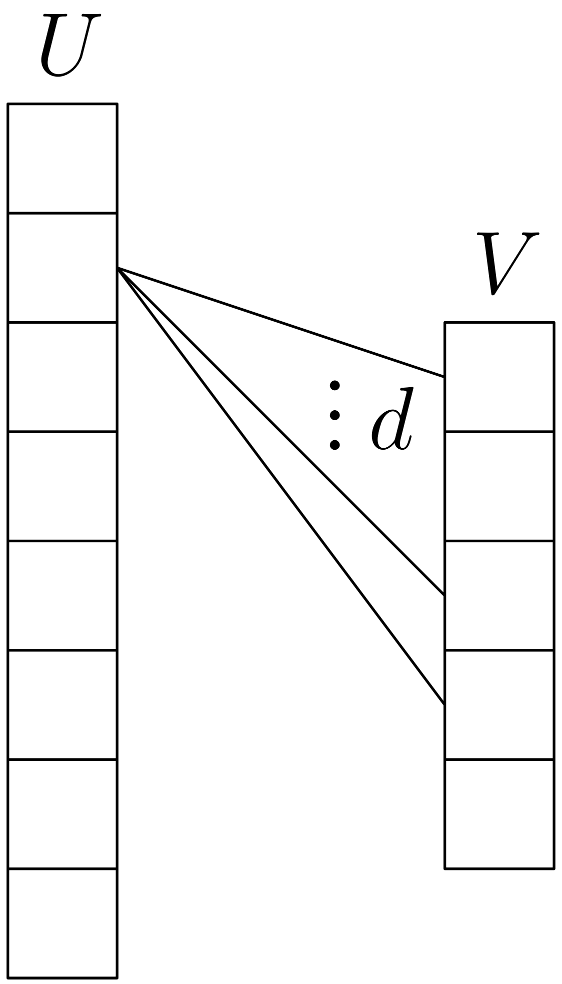
Main result (vanilla version)

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 $O(t \log t)$

Previous results

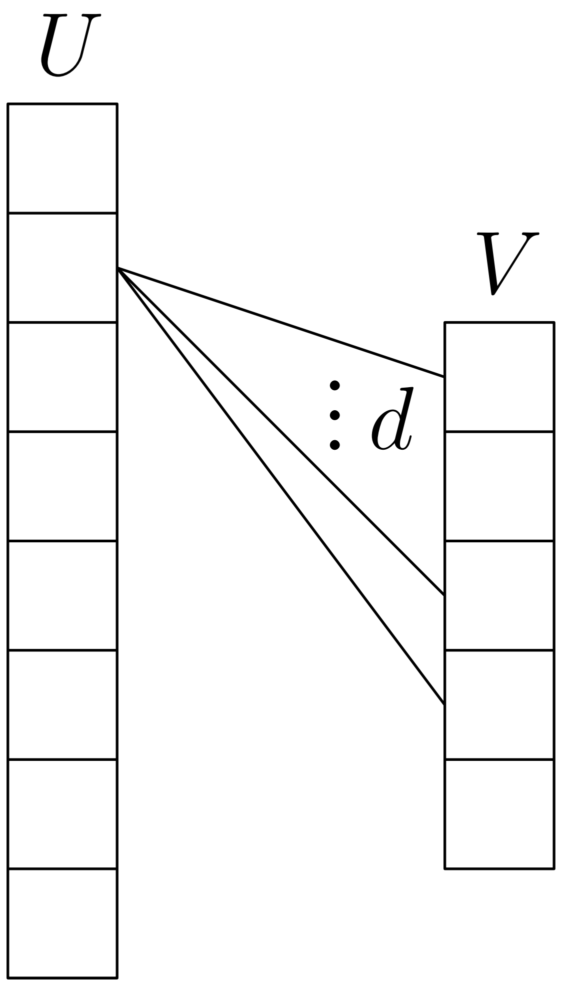
Reference	**Space**	**Time**
Polynomials [Joffe'74]	$O(k)$	$O(k)$
Graph powering [Siegel'89]	$O(k^t u^{1/t})$	$O(t)^t$
Recursive tabulation [Thorup'13]	$O(\text{poly}\, k + u^{1/t})$	$O(t^{\log t})$

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



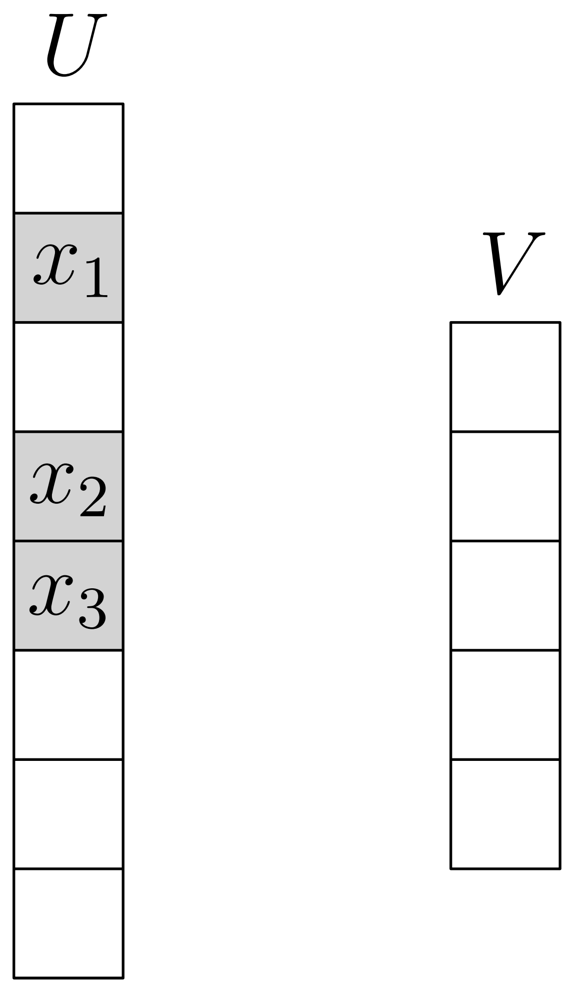
- Constructions of k-independent families of functions based on bipartite expander graphs
- Neighbor function $\Gamma : U \to V^d$

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



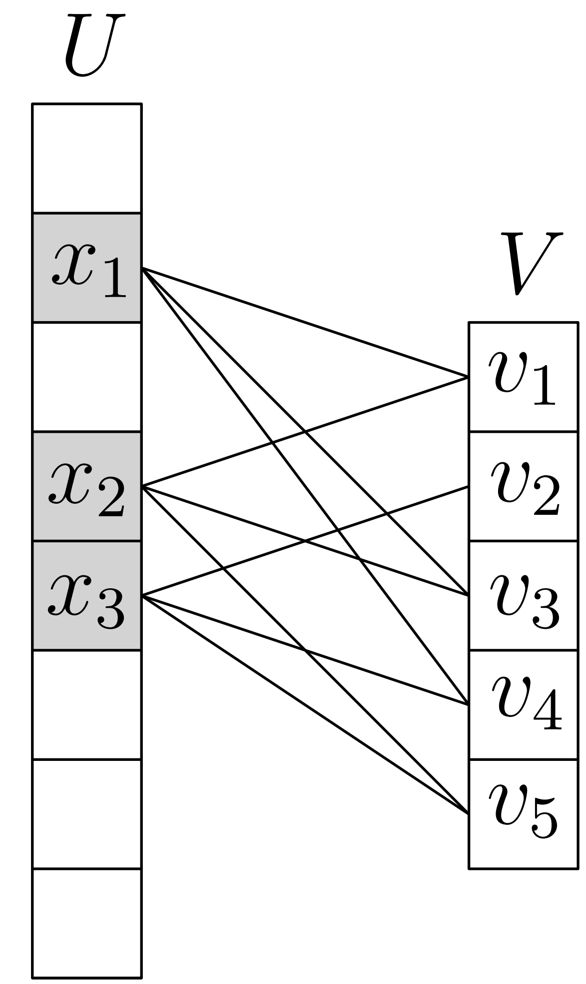
- Constructions of k-independent families of functions based on bipartite expander graphs
- Neighbor function $\Gamma : U \to V^d$

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



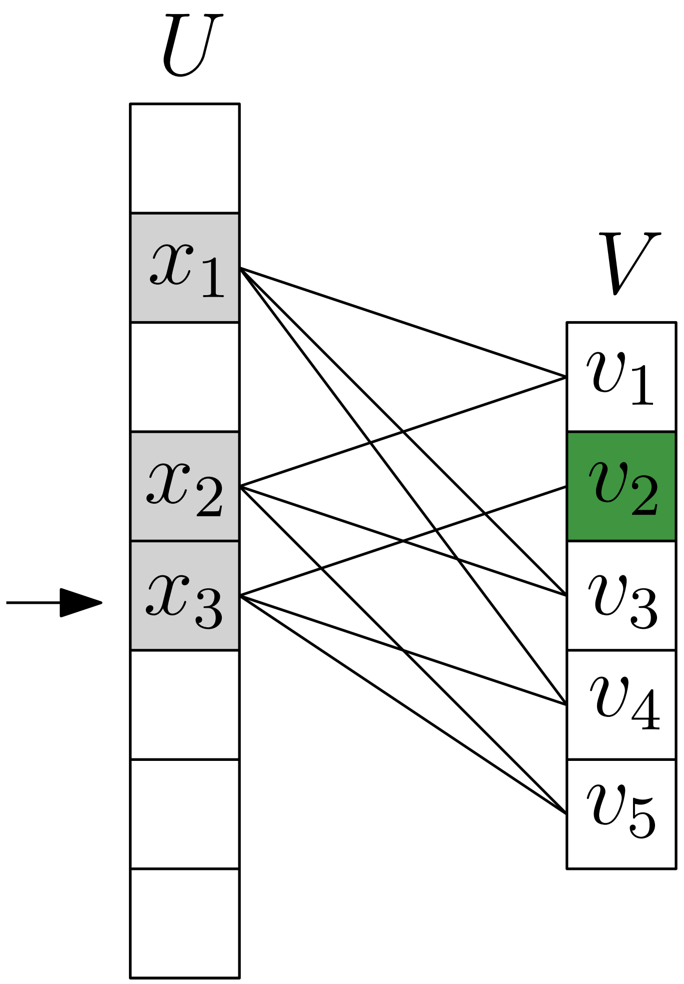
- Constructions of k-independent families of functions based on bipartite expander graphs
- Neighbor function $\Gamma : U \to V^d$

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



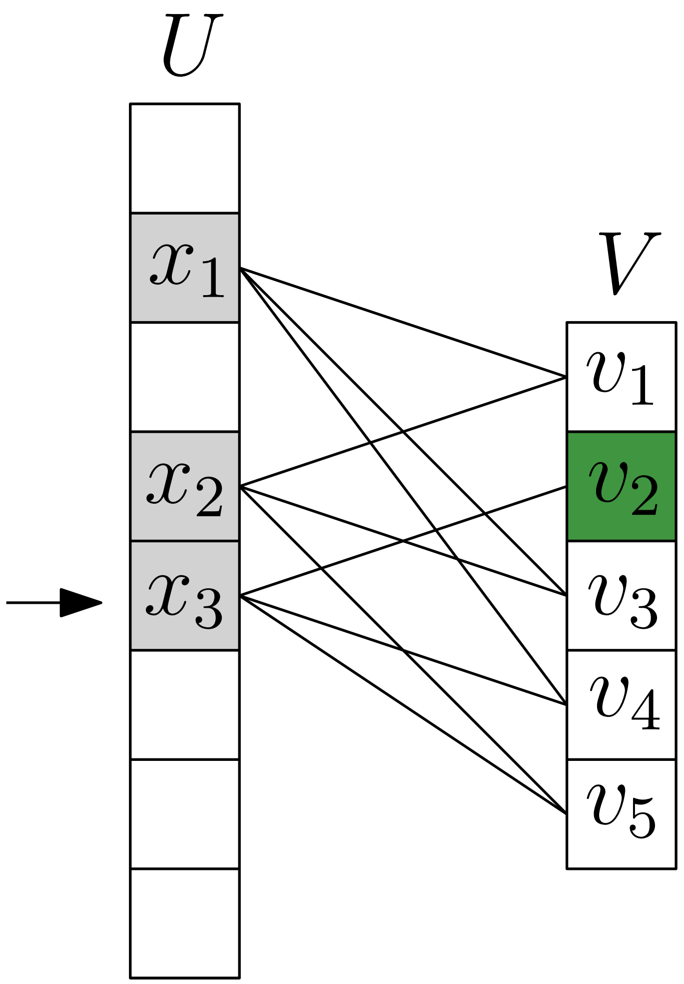
- Constructions of k-independent families of functions based on bipartite expander graphs
- Neighbor function $\Gamma : U \to V^d$

Definition A bipartite graph Γ 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 $\Gamma : U \to V^d$

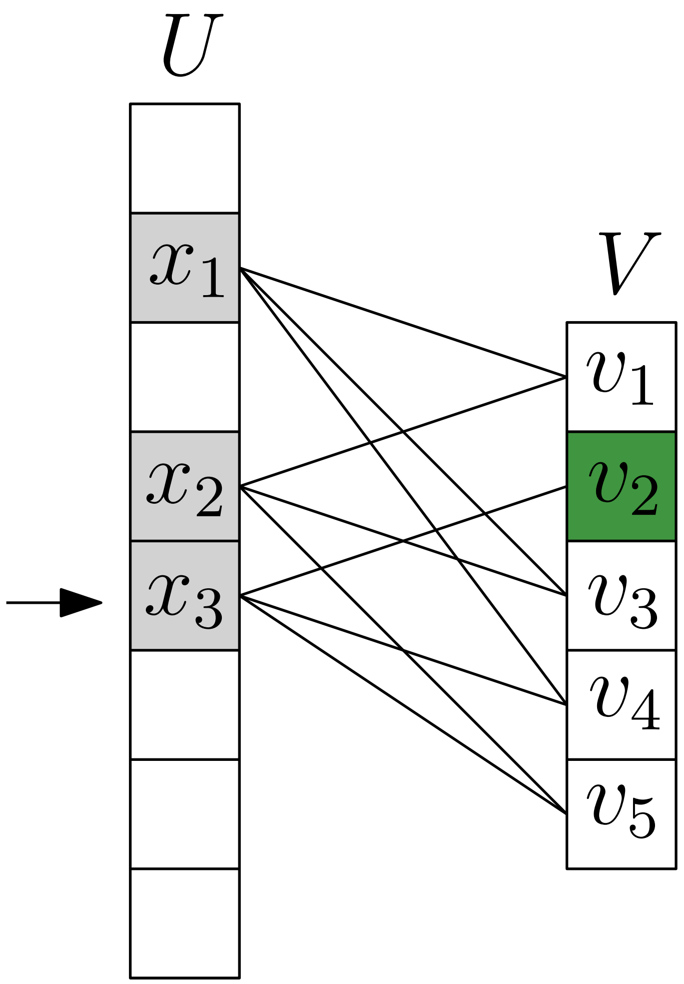
Definition A bipartite graph Γ is k-unique if for every $S \subseteq U$ with $|S| \leq k$ there exists $v \in V$ with exactly one neighbor in S



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

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

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

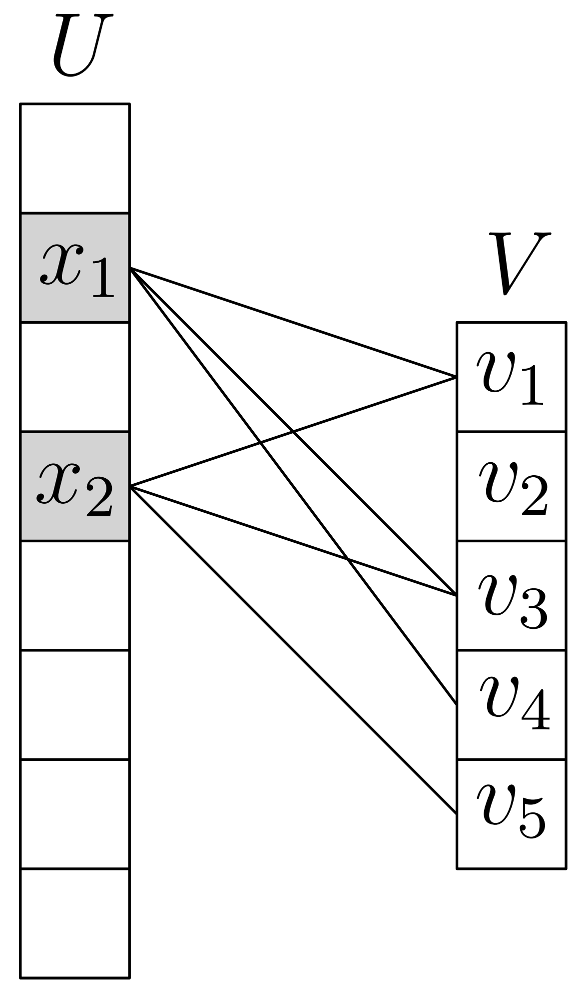


- Peeling argument example:

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

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

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



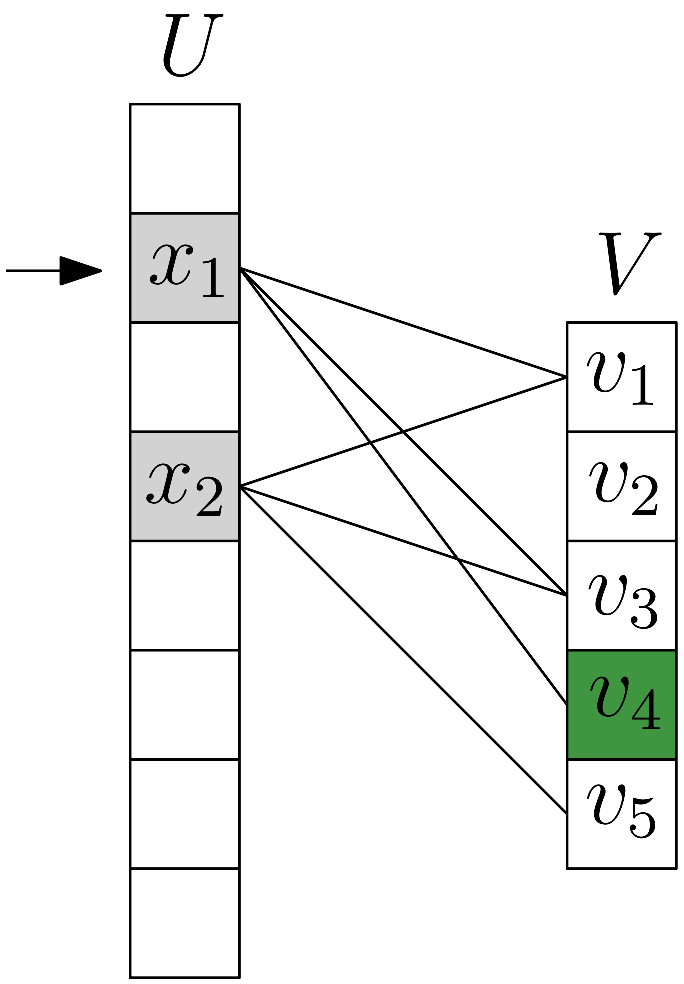
Definition A bipartite graph Γ is k-unique if for every $S \subseteq U$ with $|S| \leq k$ there exists $v \in V$ with exactly one neighbor in S

- Peeling argument example:

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

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

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



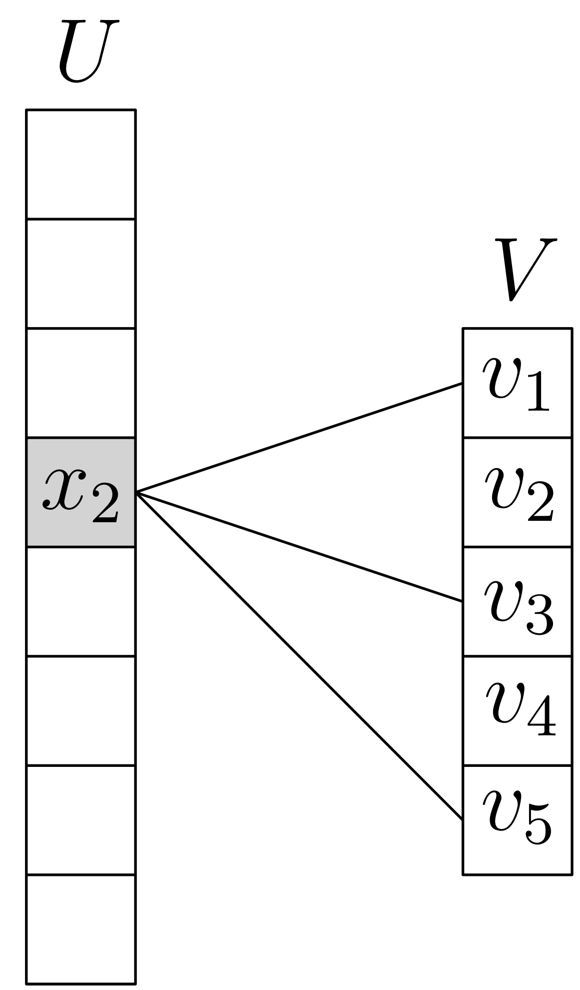
> **Definition** A bipartite graph Γ is k-unique if for every $S \subseteq U$ with $|S| \leq k$ there exists $v \in V$ with exactly one neighbor in S

- Peeling argument example:

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

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

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



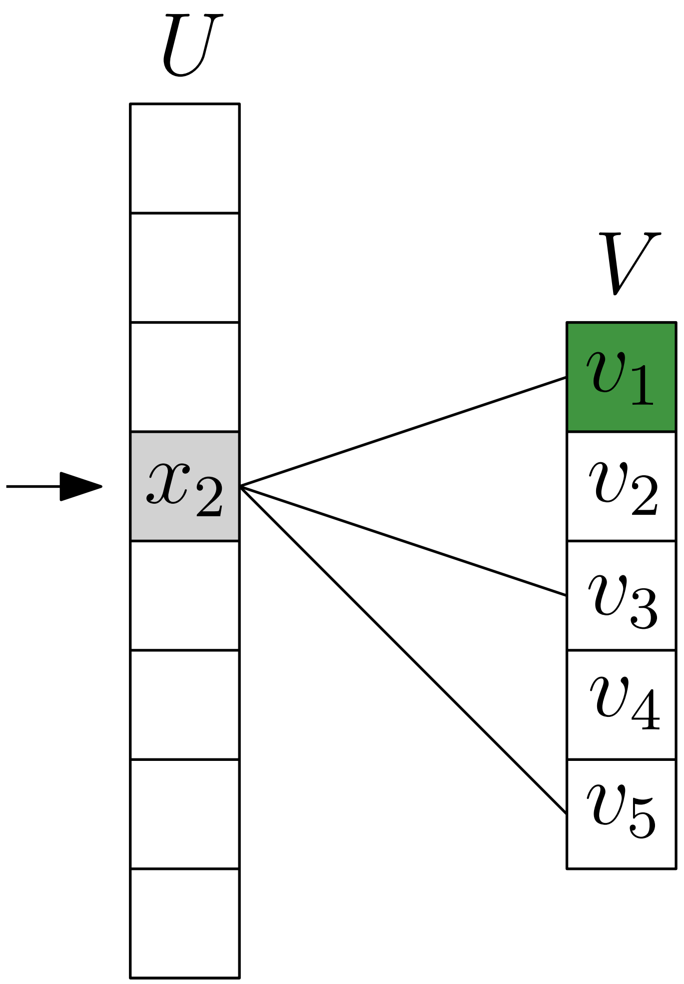
Definition A bipartite graph Γ is k-unique if for every $S \subseteq U$ with $|S| \leq k$ there exists $v \in V$ with exactly one neighbor in S

- Peeling argument example:

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

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

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



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

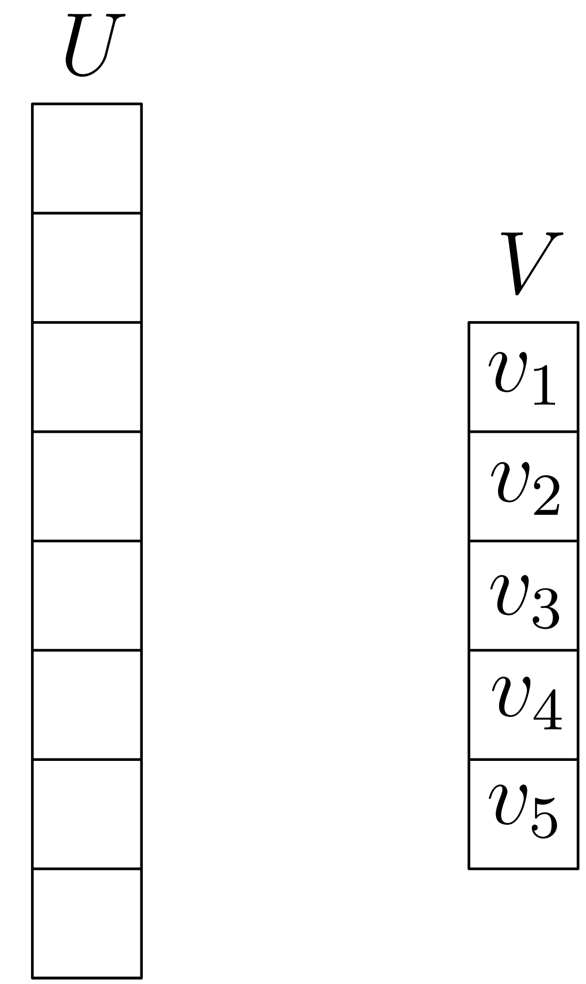
- Peeling argument example:

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

Lemma [Siegel'89] Let $\Gamma : U \to V^d$ be k-unique and $h : V \to [r]$ be a random function. Then $f(x) = \sum_i h(\Gamma(x)_i) \bmod r$ 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 $\Gamma : U \to V^d$



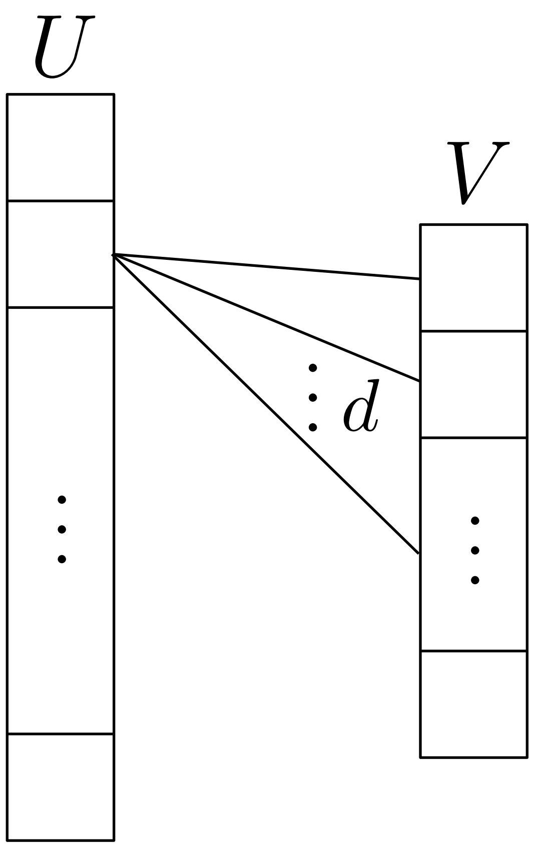
Definition A bipartite graph Γ is k-unique if for every $S \subseteq U$ with $|S| \leq k$ there exists $v \in V$ with exactly one neighbor in S

- Peeling argument example:

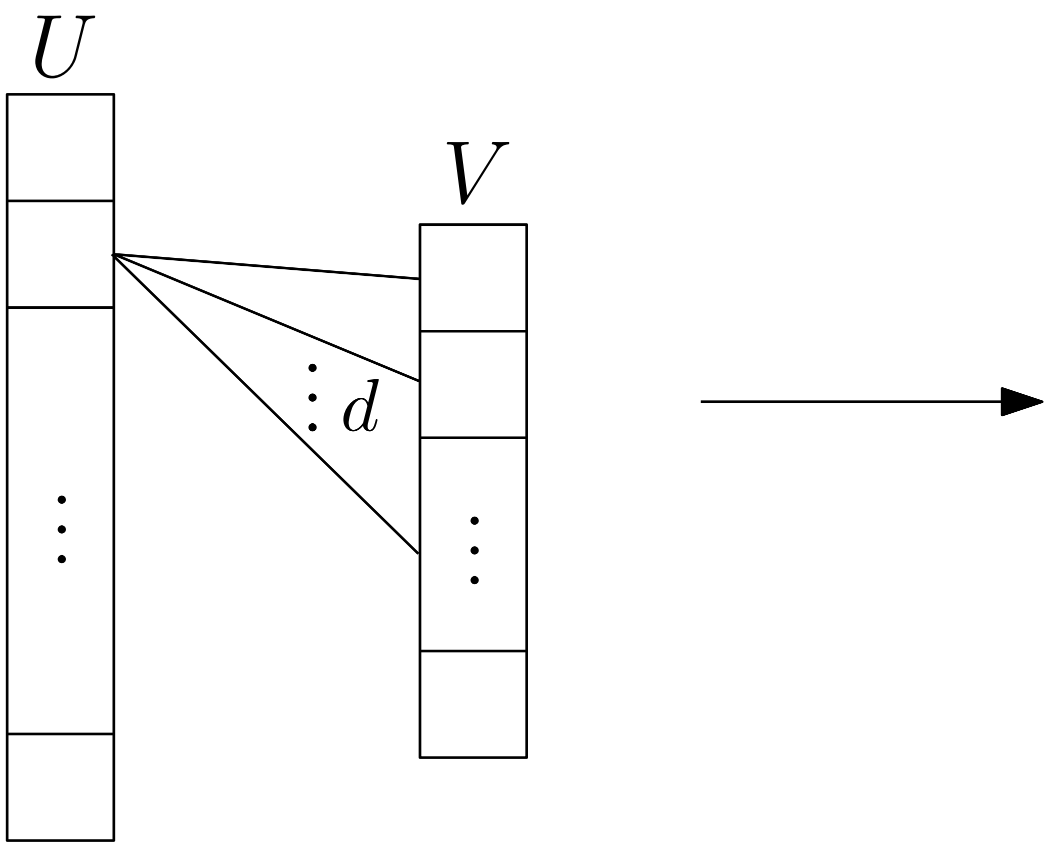
$$f(x_3) = h(v_2) + h(v_4) + h(v_5) \bmod r$$

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

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



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

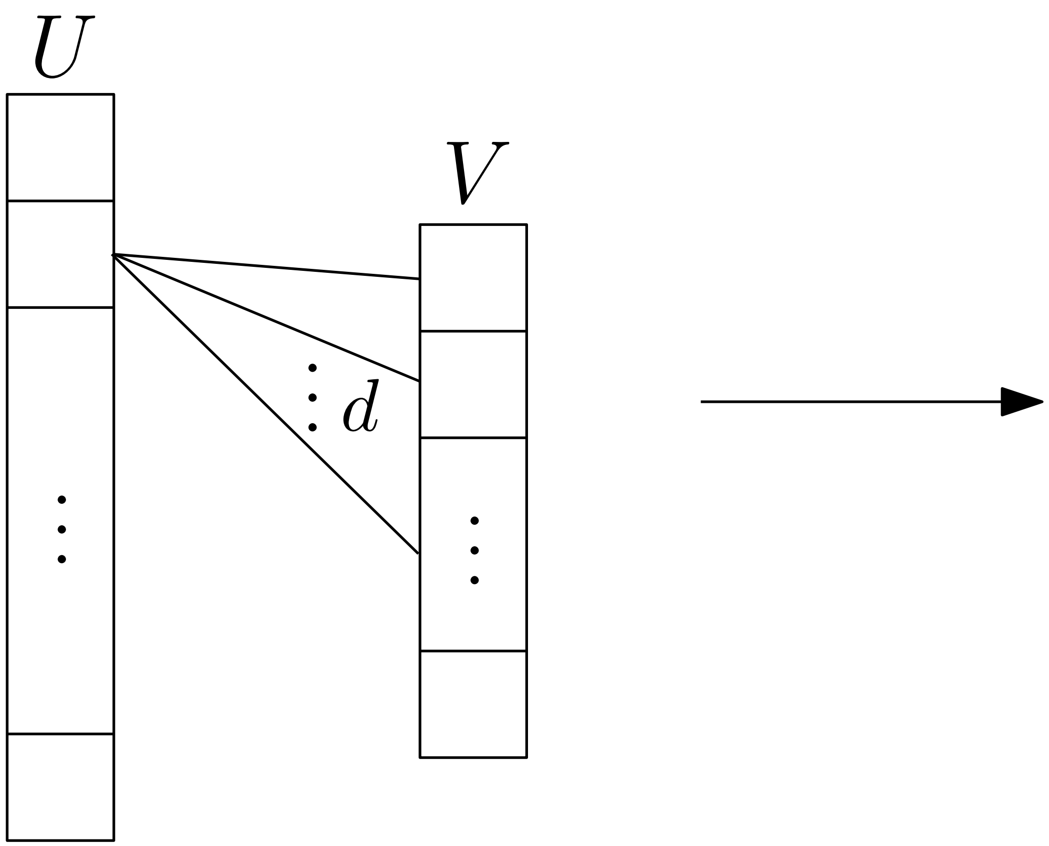


k-independent family $\mathcal{F}$

$f(x) = \sum_i h(\Gamma(x)_i) \bmod r$
$h : V \to [r]$ is random

Space $|V|$
Time d

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



k-independent family $\mathcal{F}$

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

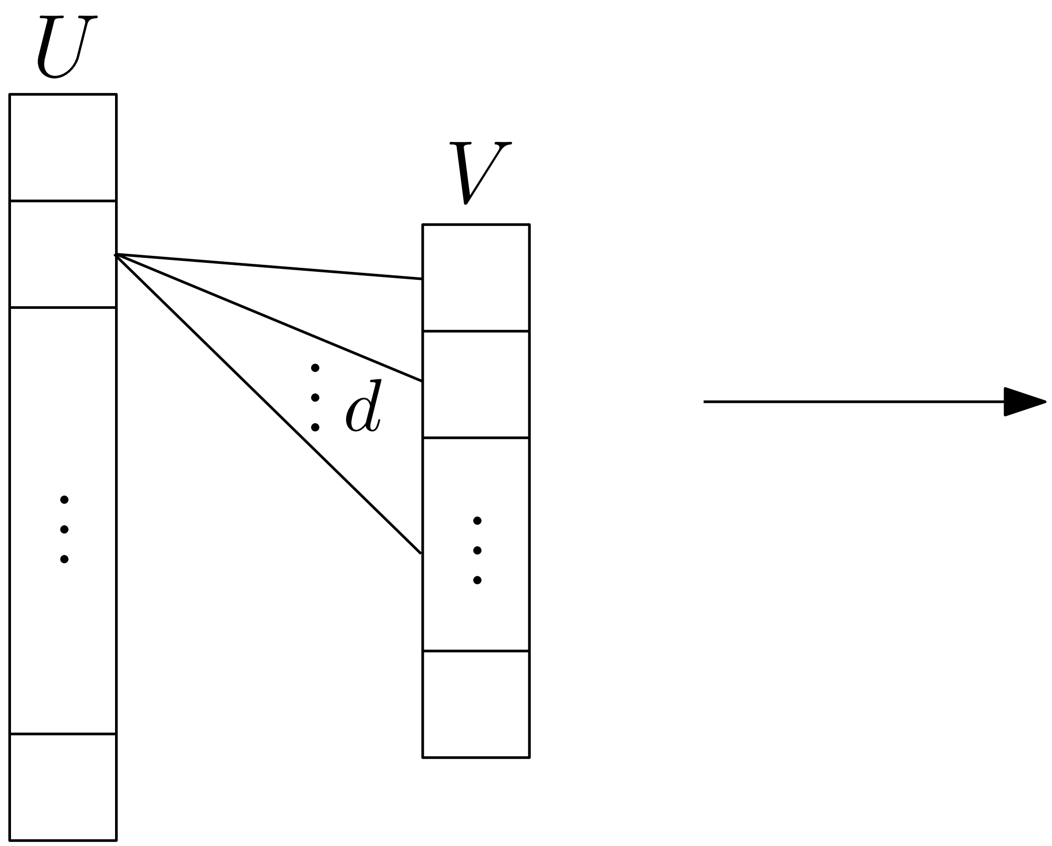
$h : V \to [r]$ is random

Space $|V|$

Time d

Lemma [Siegel'89] Most graphs Γ give an optimal space-time tradeoff for k-independent hashing

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



k-independent family $\mathcal{F}$

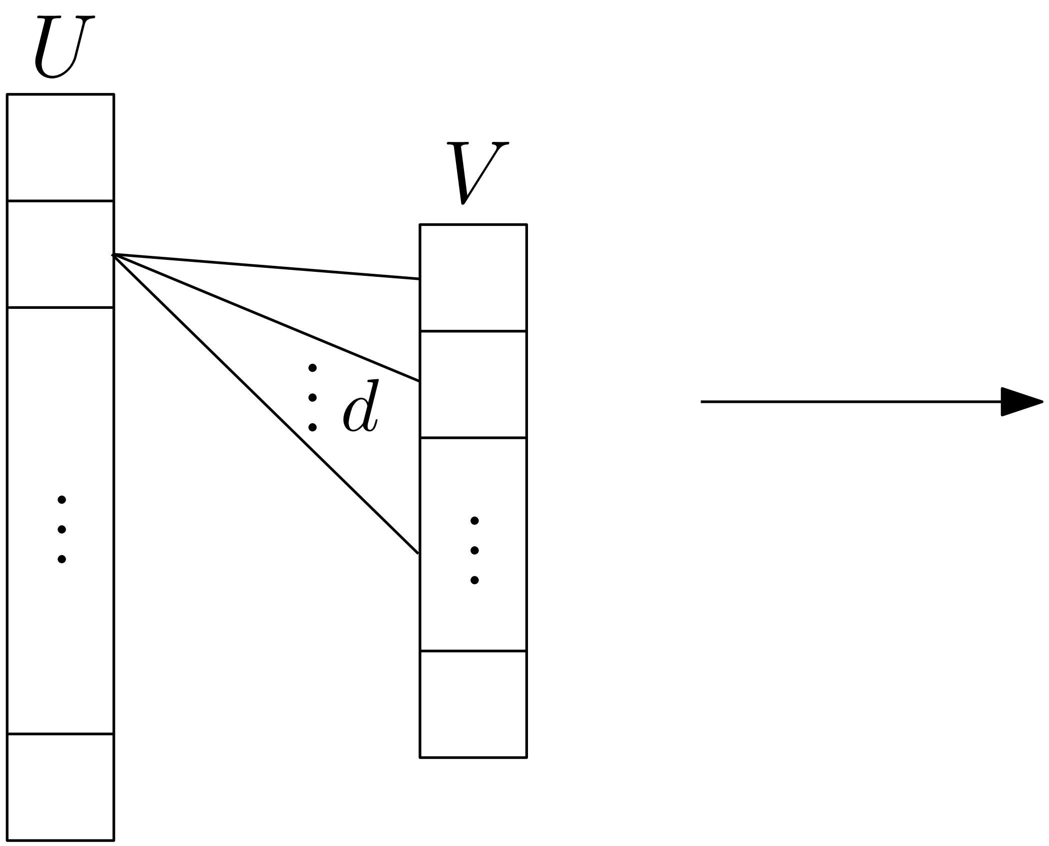
$f(x) = \sum_i h(\Gamma(x)_i) \bmod r$
$h : V \to [r]$ is random

Space $|V|$
Time d

Lemma [Siegel'89] Most graphs Γ give an optimal space-time tradeoff for k-independent hashing

- Explicit k-unique graphs with optimal parameters are not known

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



k-independent family $\mathcal{F}$

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

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

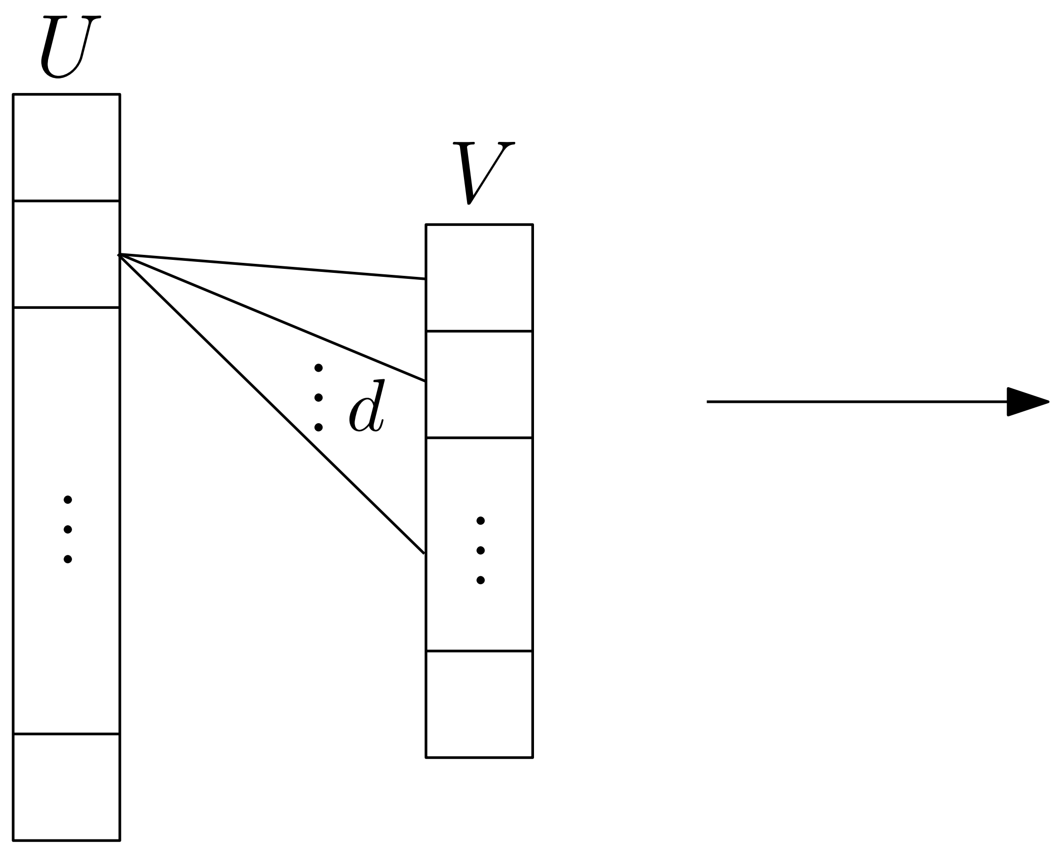
Space $|V|$

Time d

Lemma [Siegel'89] Most graphs Γ give an optimal space-time tradeoff for k-independent hashing

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

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



k-independent family $\mathcal{F}$

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

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

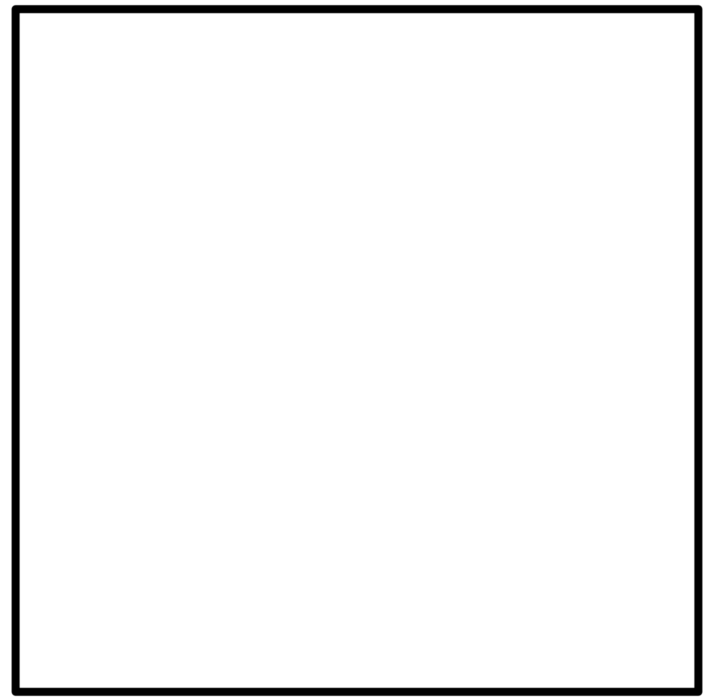
Space $|V|$

Time d

Lemma [Siegel'89] Most graphs Γ give an optimal space-time tradeoff for k-independent hashing

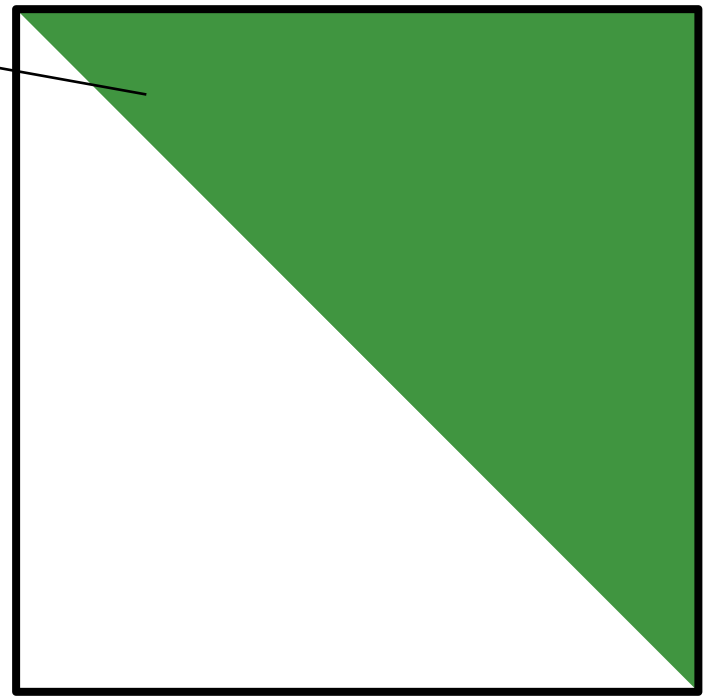
- Explicit k-unique graphs with optimal parameters are not known
- Storing a random Γ defeats the purpose of k-independent hashing
- Verifying that a given Γ is k-unique is infeasible

Set of all functions $\Gamma : U \to V^d$

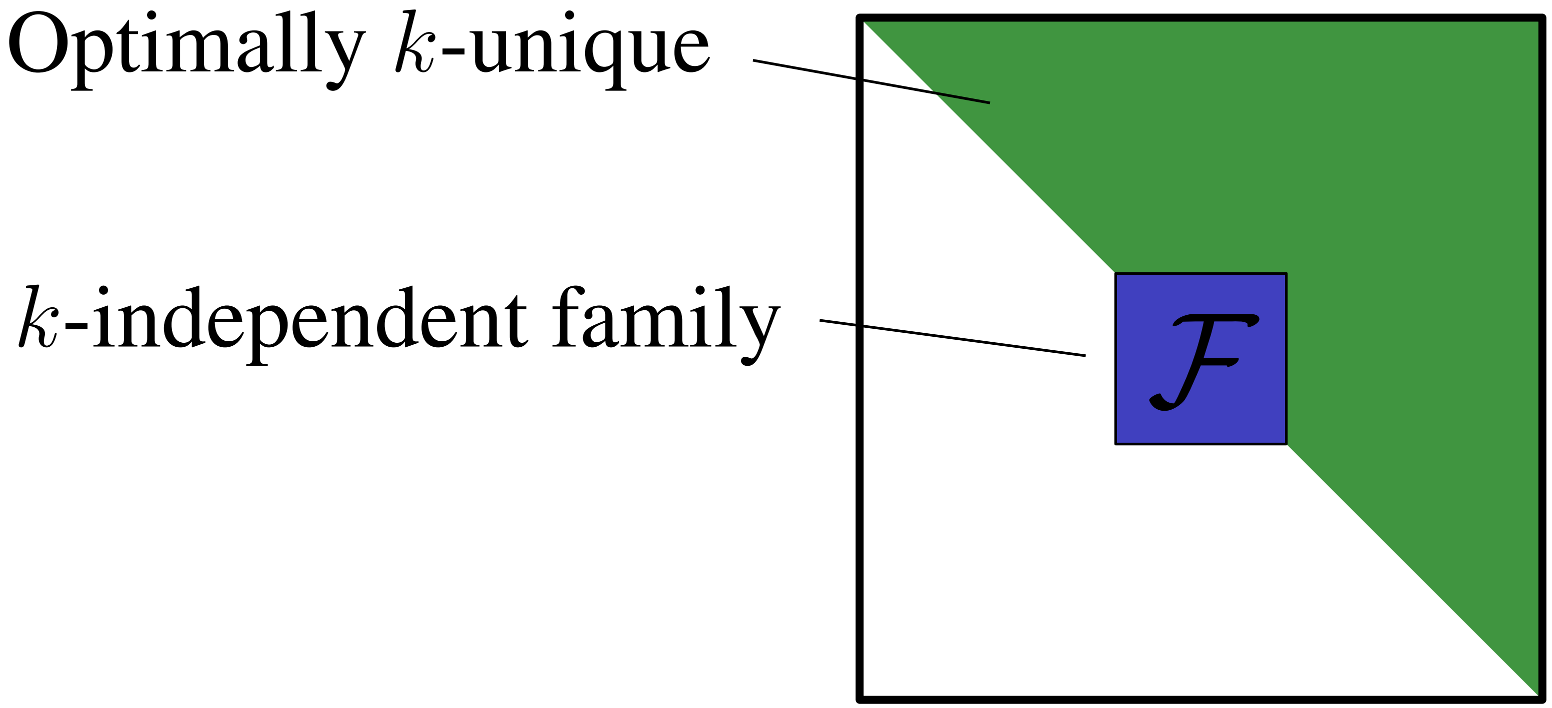


Set of all functions $\Gamma : U \to V^d$

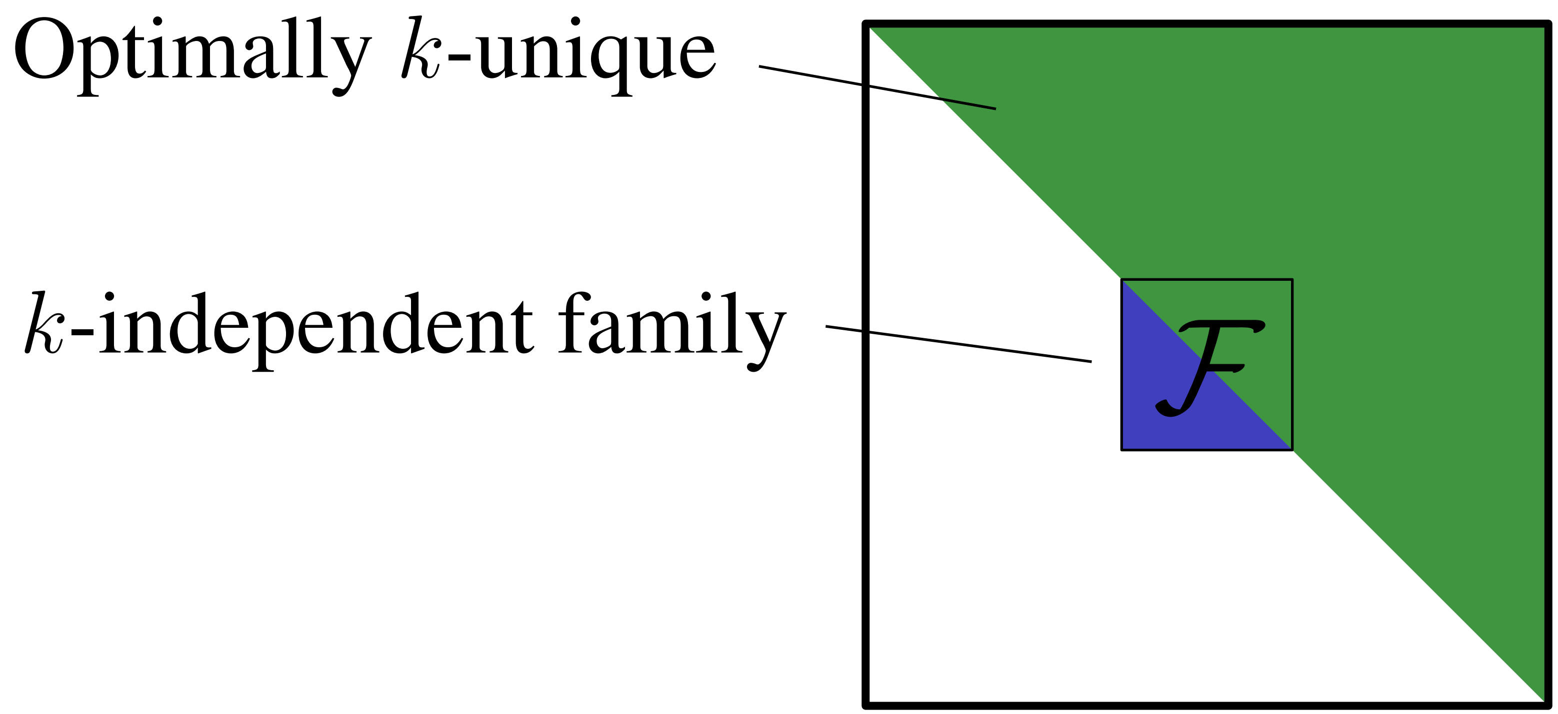
Optimally k-unique



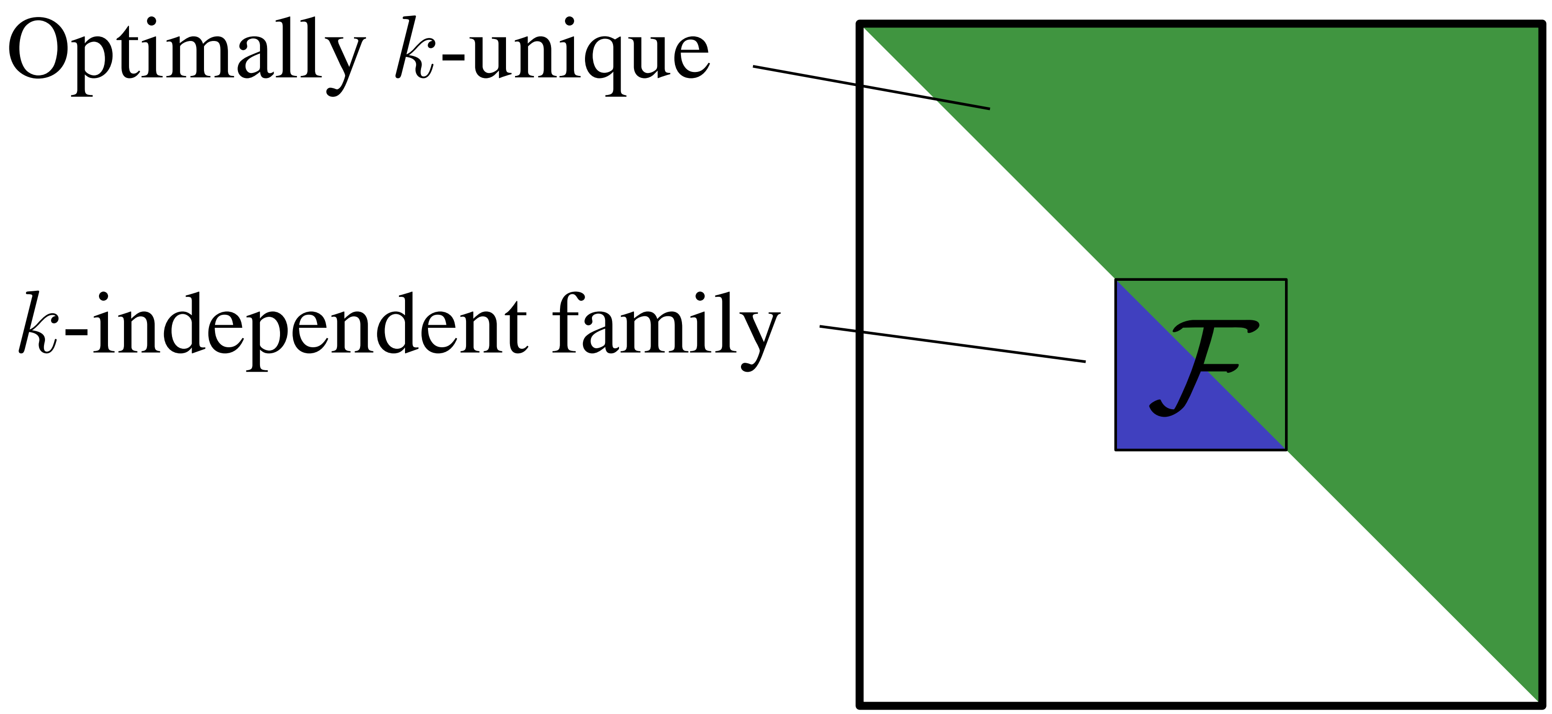
Set of all functions $\Gamma : U \to V^d$



Set of all functions $\Gamma : U \to V^d$

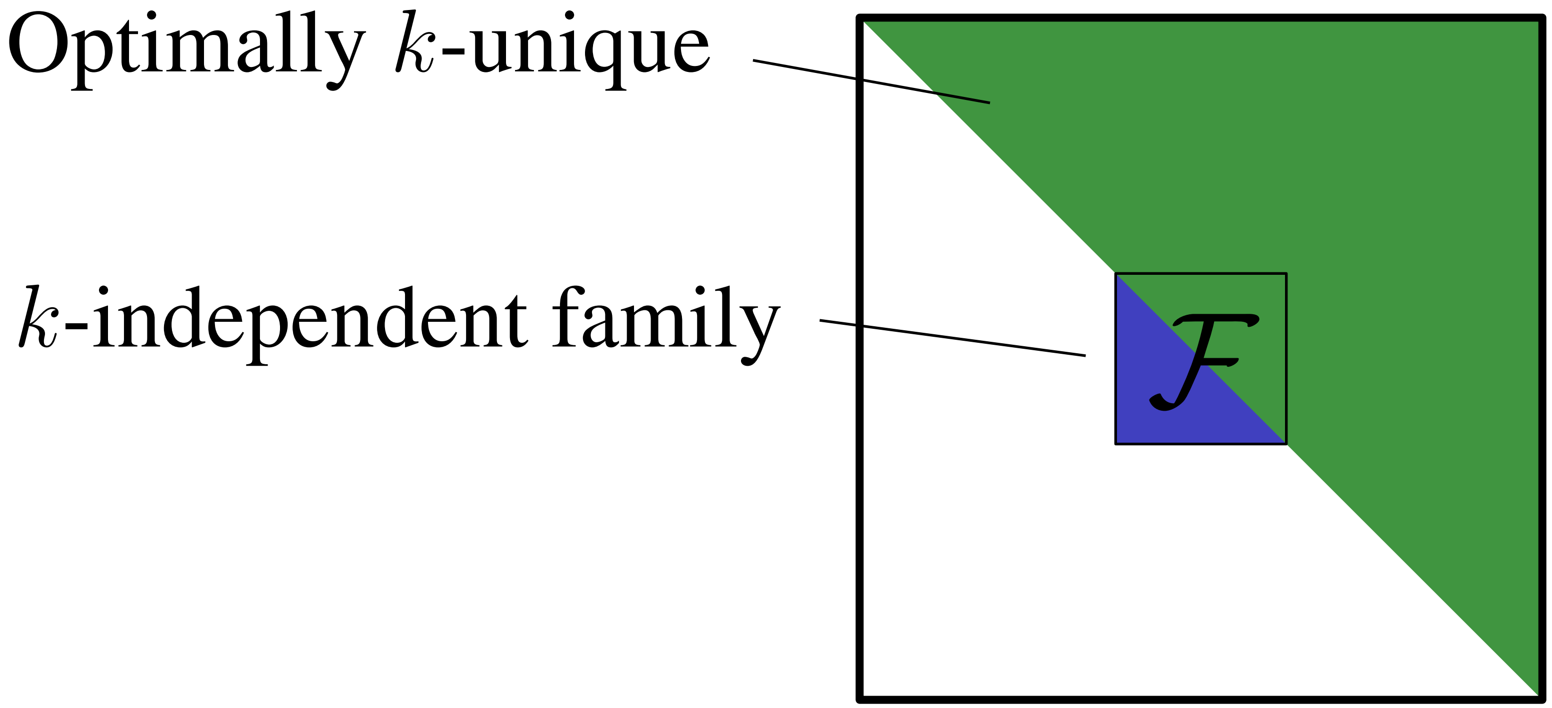


Set of all functions $\Gamma : U \to V^d$



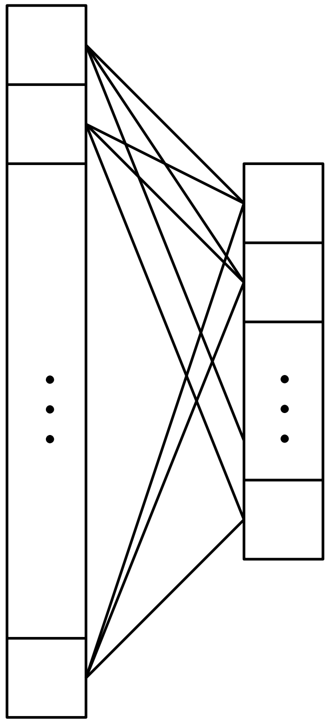
Lemma A k-independent function $\Gamma : U \to V^d$ with $|U| = u$, $|V| = O(ku^{1/t}t)$ and $d = O(t)$ is k-unique with high probability.

Set of all functions $\Gamma : U \to V^d$

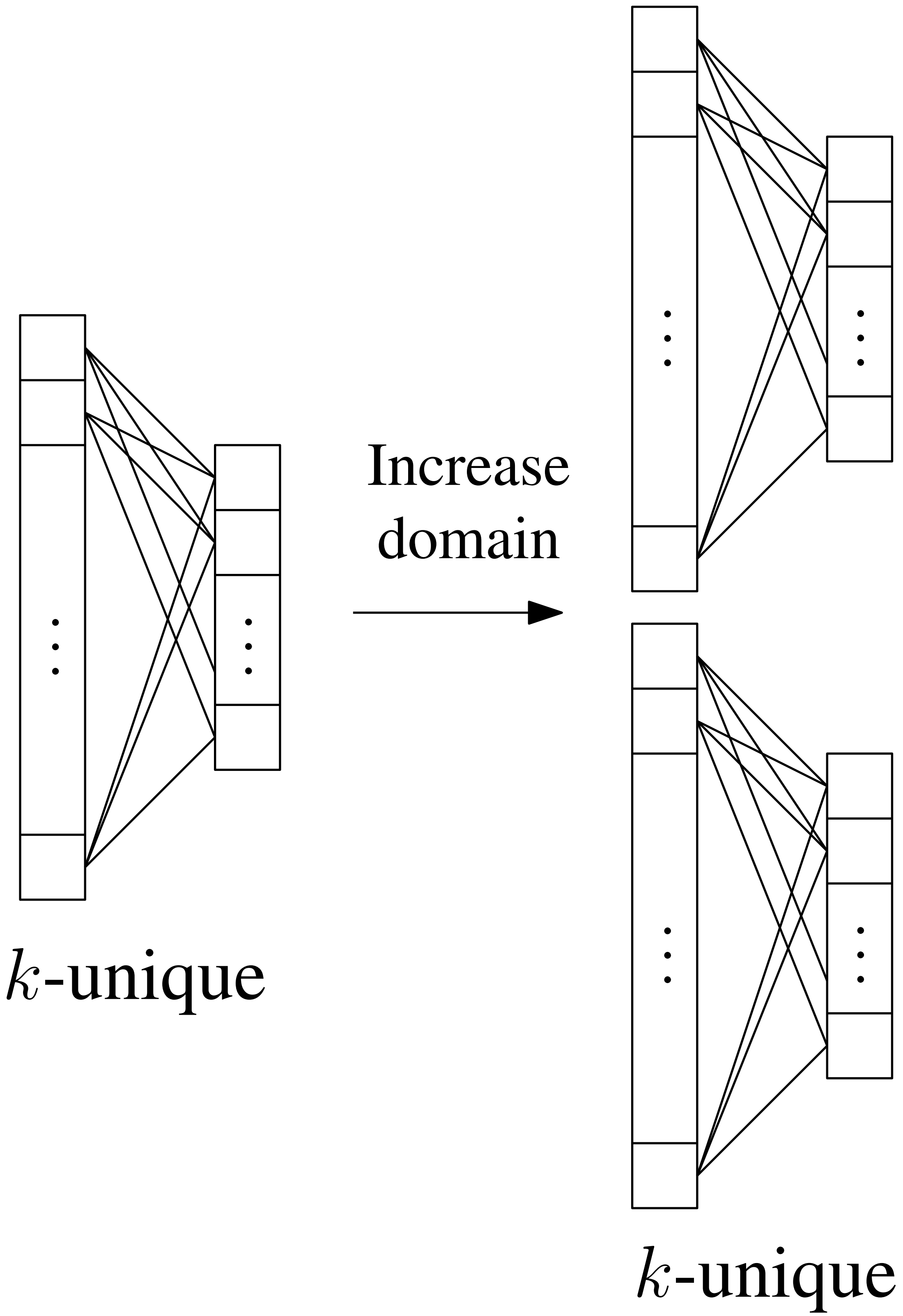


Lemma A k-independent function $\Gamma : U \to V^d$ with $|U| = u$, $|V| = O(ku^{1/t}t)$ and $d = O(t)$ is k-unique with high probability.

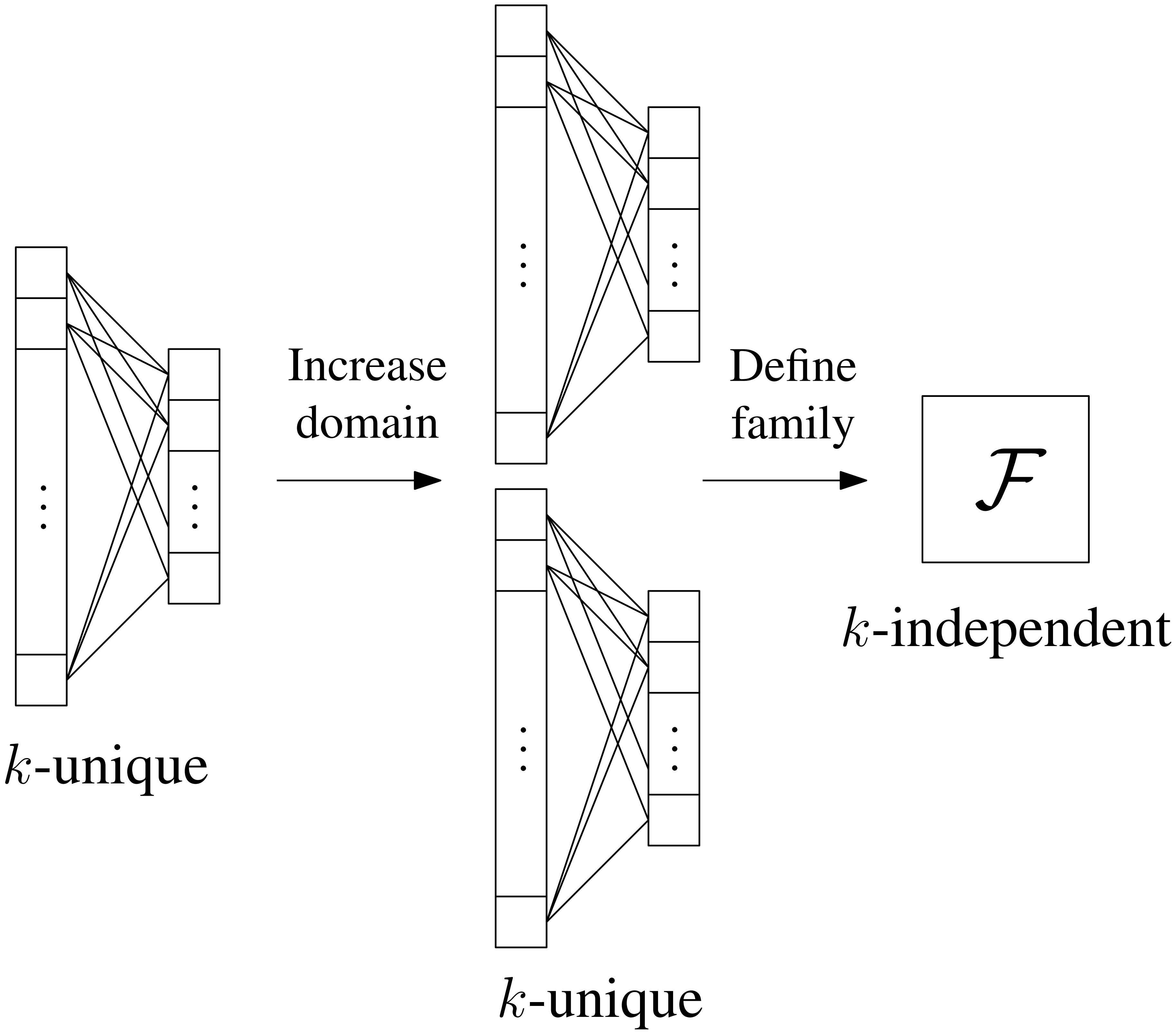
k-unique		k-independent family		k-unique whp.
Γ	$\longrightarrow$	$\mathcal{F}$	$\longrightarrow$	$\Gamma \in \mathcal{F}$

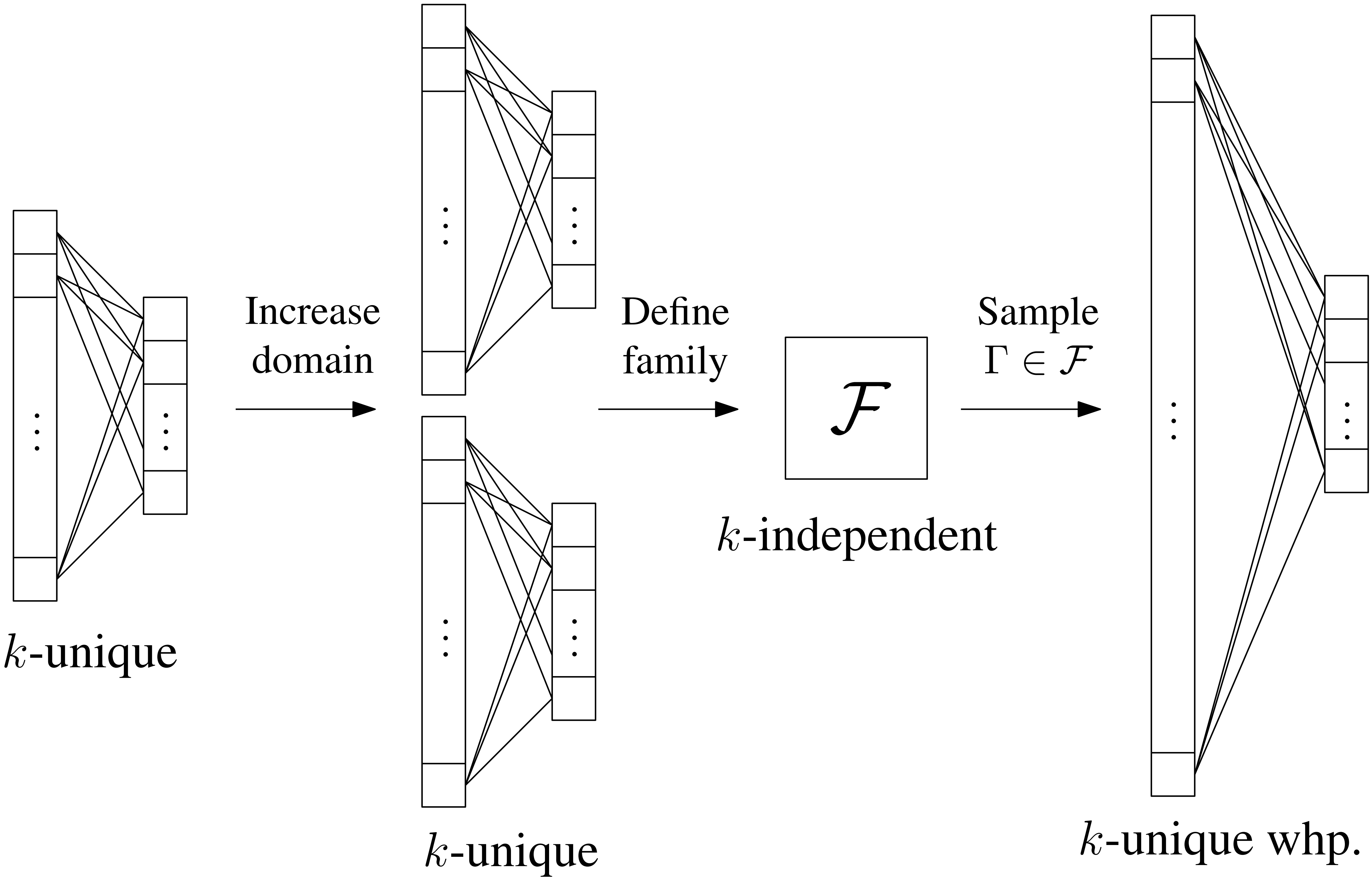


k-unique



k-unique
Increase domain
k-unique


Increase
domain
Define
family
$\mathcal{F}$
k-unique
k-unique
k-independent



k-unique
Increase domain
k-unique
Define family
$\mathcal{F}$
k-independent
Sample $\Gamma \in \mathcal{F}$
k-unique whp.

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

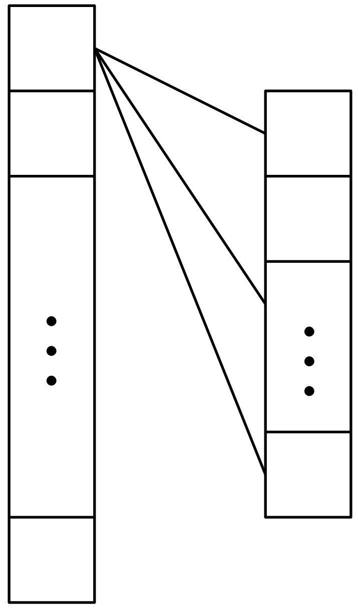
$$\Gamma(ax) = \bigoplus_i h(a, \Gamma(x)_i), \qquad a \in \Sigma, ax \in \Sigma^*$$

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

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

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

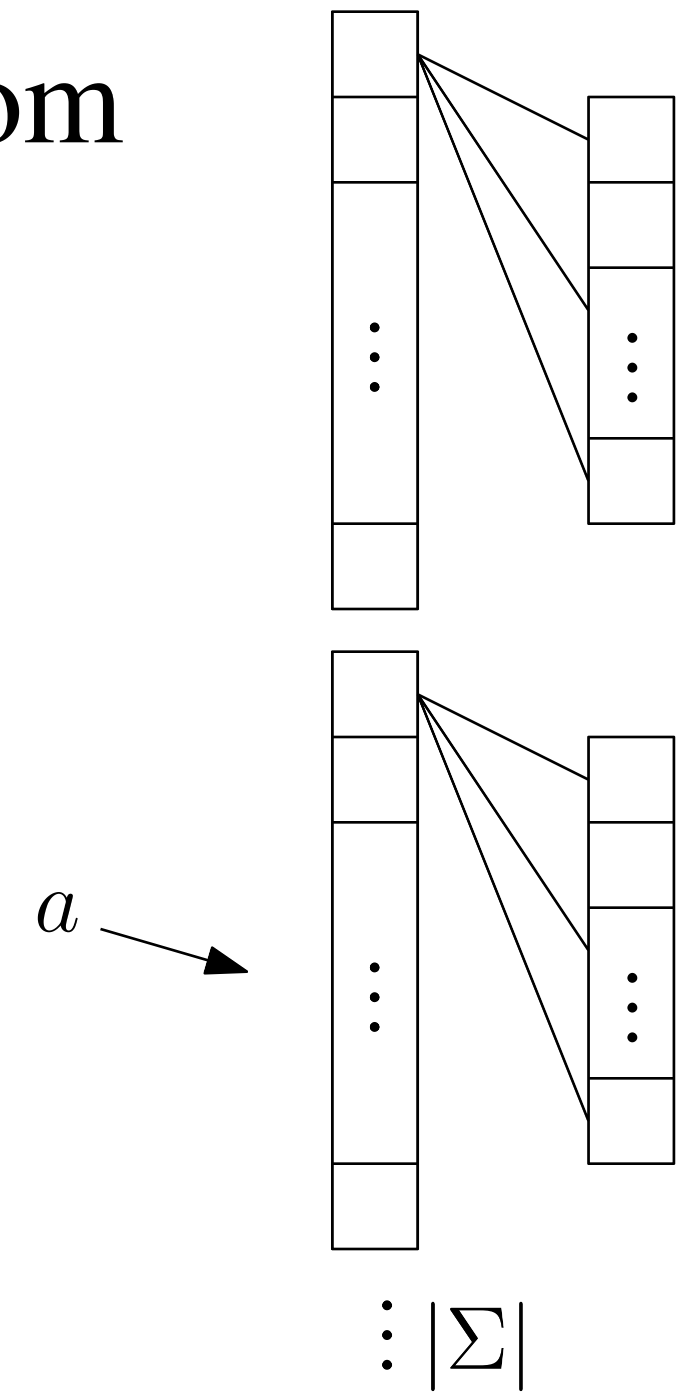
$h : \Sigma \times V \to V^d$ is random



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

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

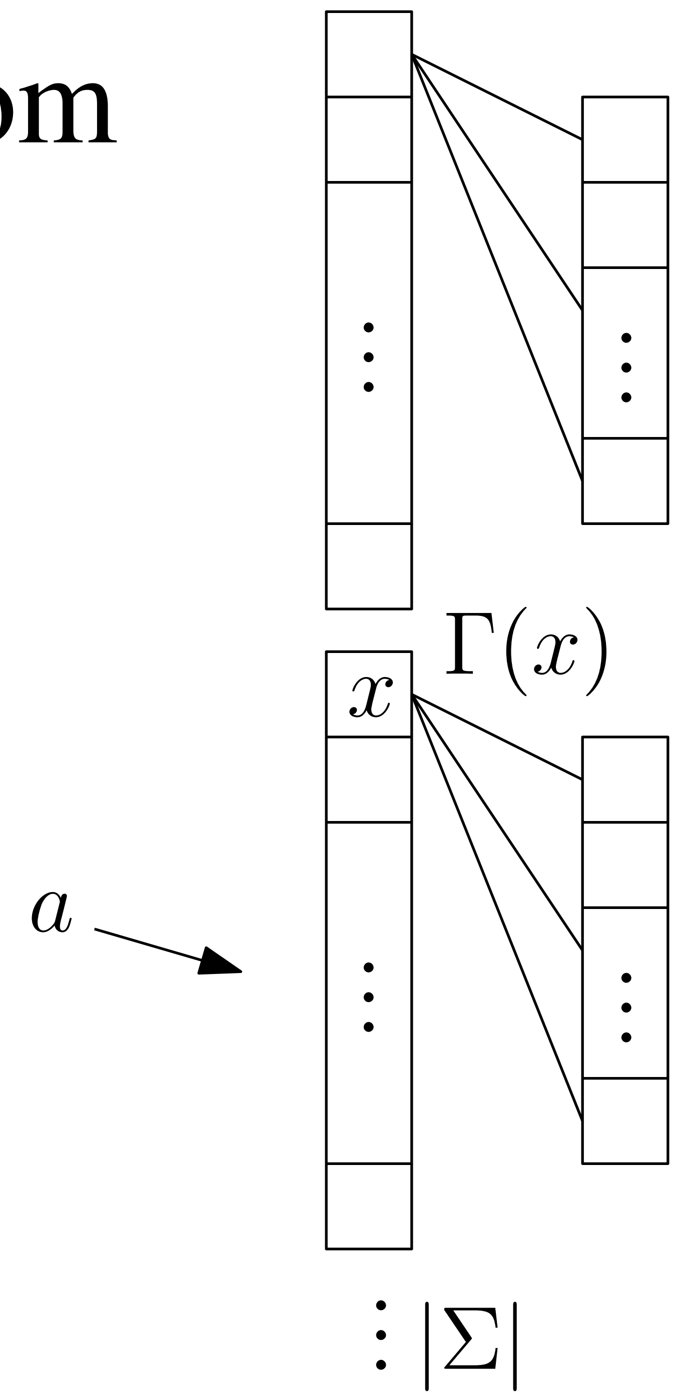
$h : \Sigma \times V \to V^d$ is random



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

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

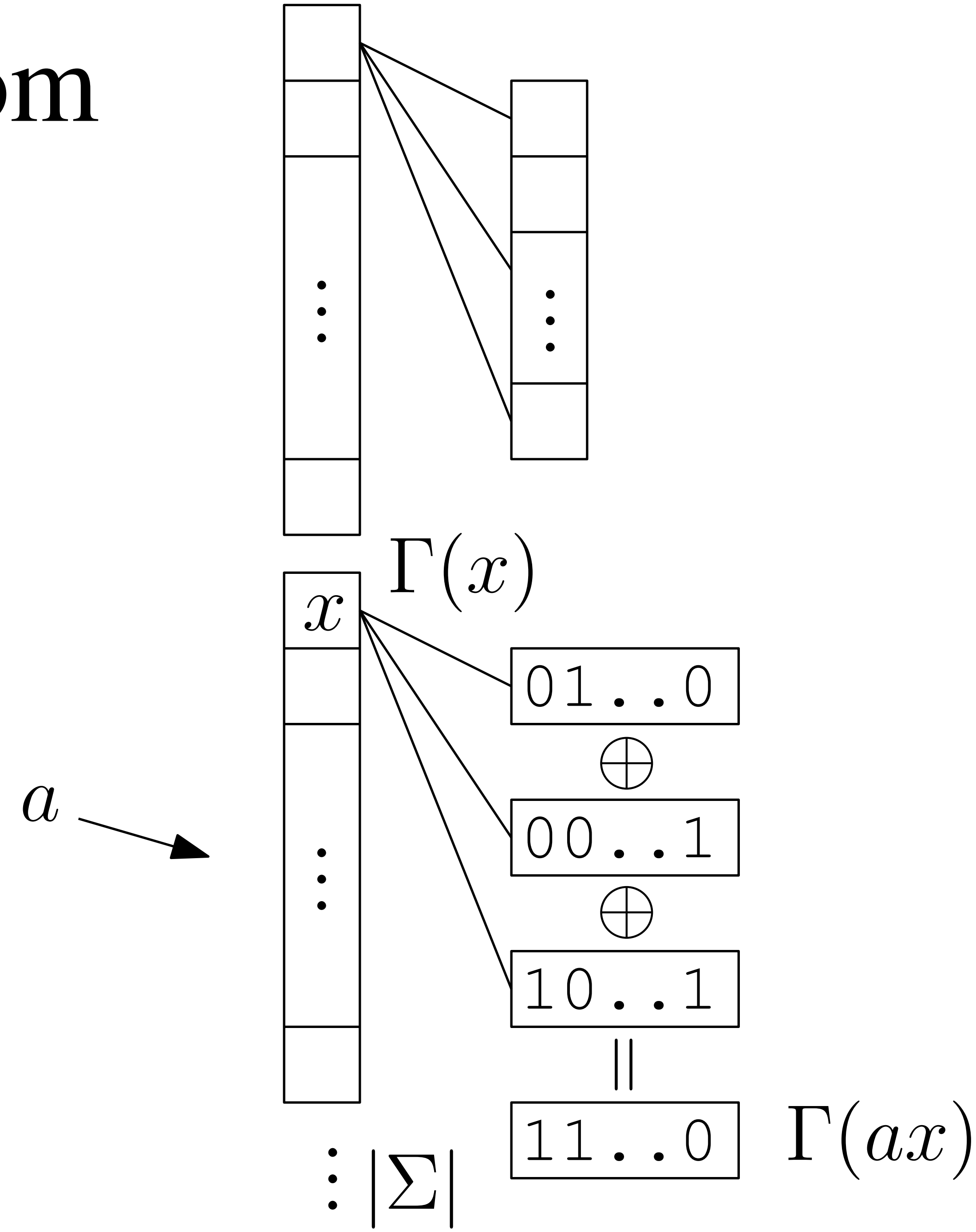
$h : \Sigma \times V \to V^d$ is random



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

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

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

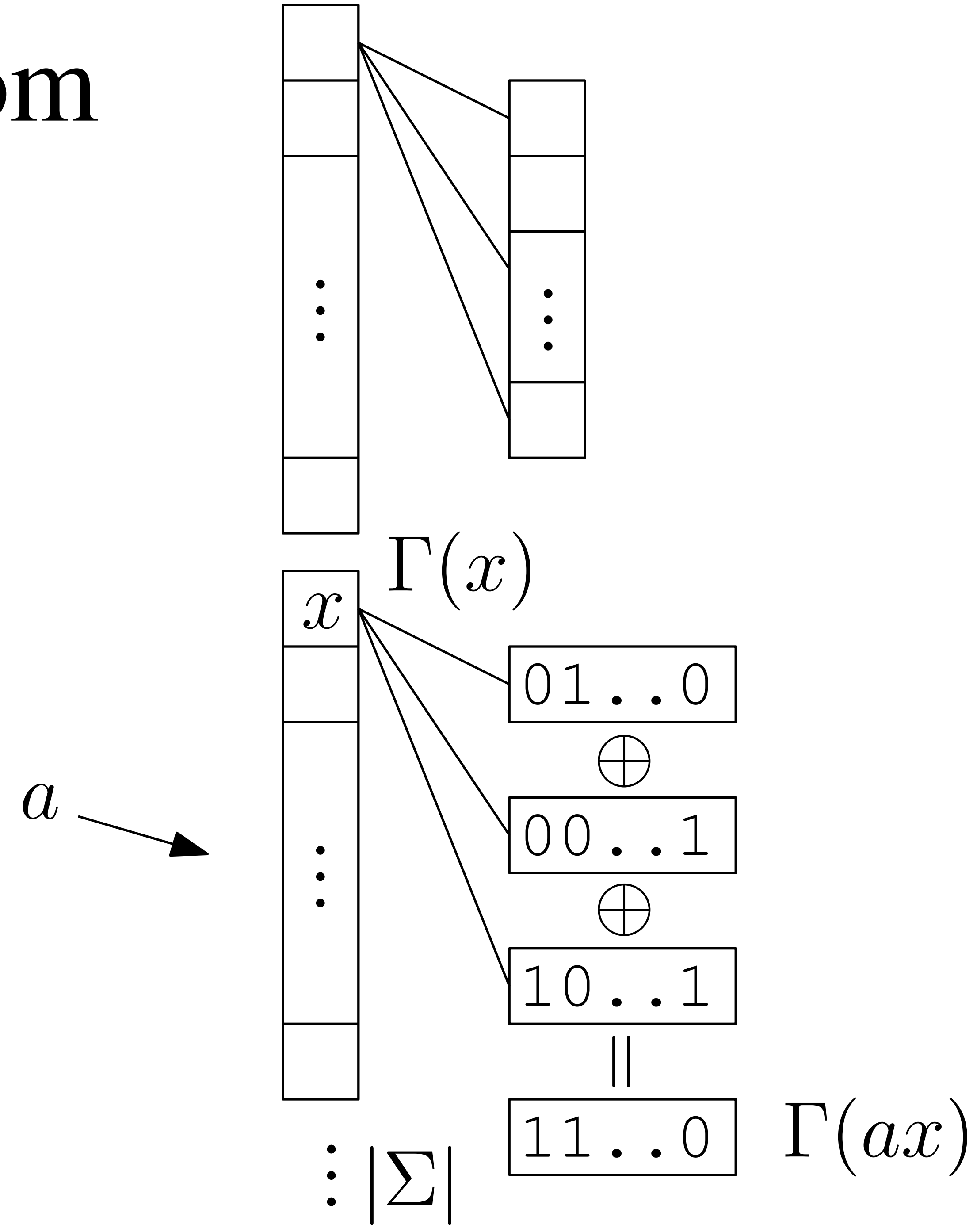


- View $x \in [u]$ as a string of characters from an alphabet Σ

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

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

Lemma Γ is k-unique over Σ^j
$\Rightarrow \Gamma$ is k-independent over Σ^{j+1}
$\Rightarrow \Gamma$ is k-unique over Σ^{j+1} whp.



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

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

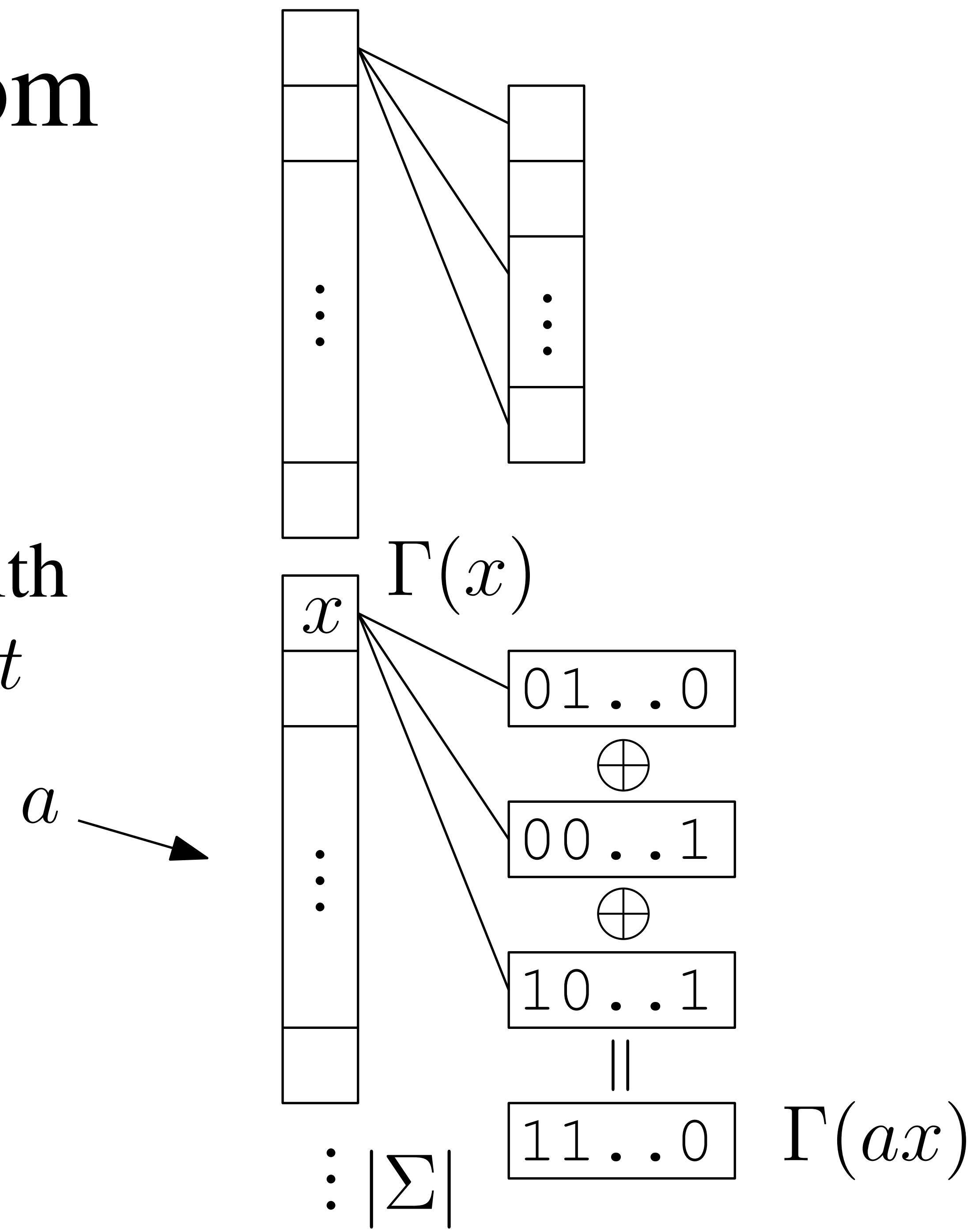
$h : \Sigma \times V \to V^d$ is random

Lemma Γ is k-unique over Σ^j
$\Rightarrow$ Γ is k-independent over Σ^{j+1}
$\Rightarrow$ Γ is k-unique over Σ^{j+1} whp.

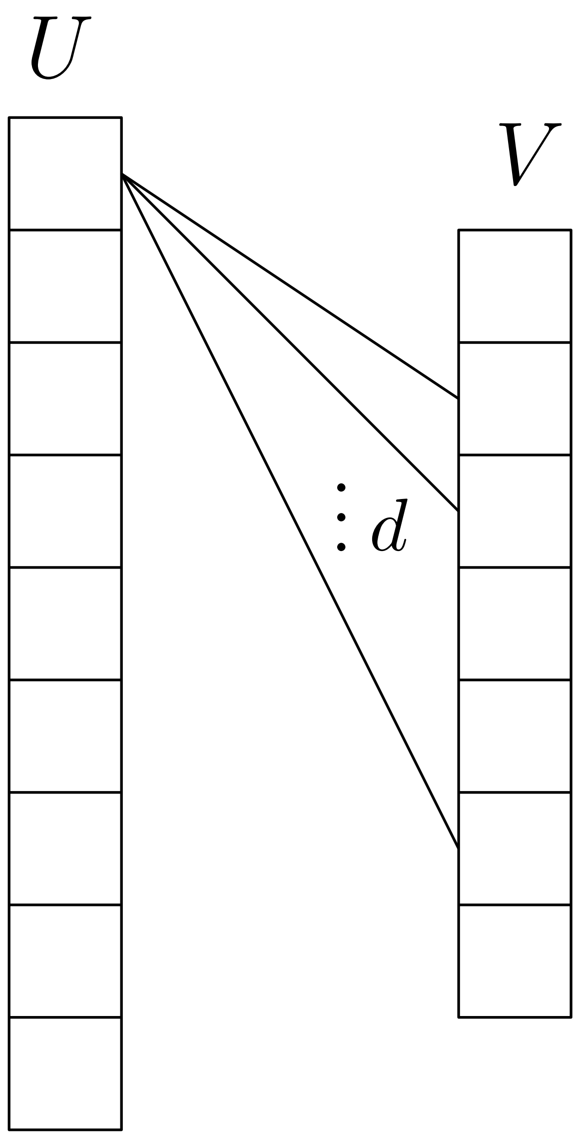
- Parameterizing for k-independence with domain size u and tradeoff parameter t

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

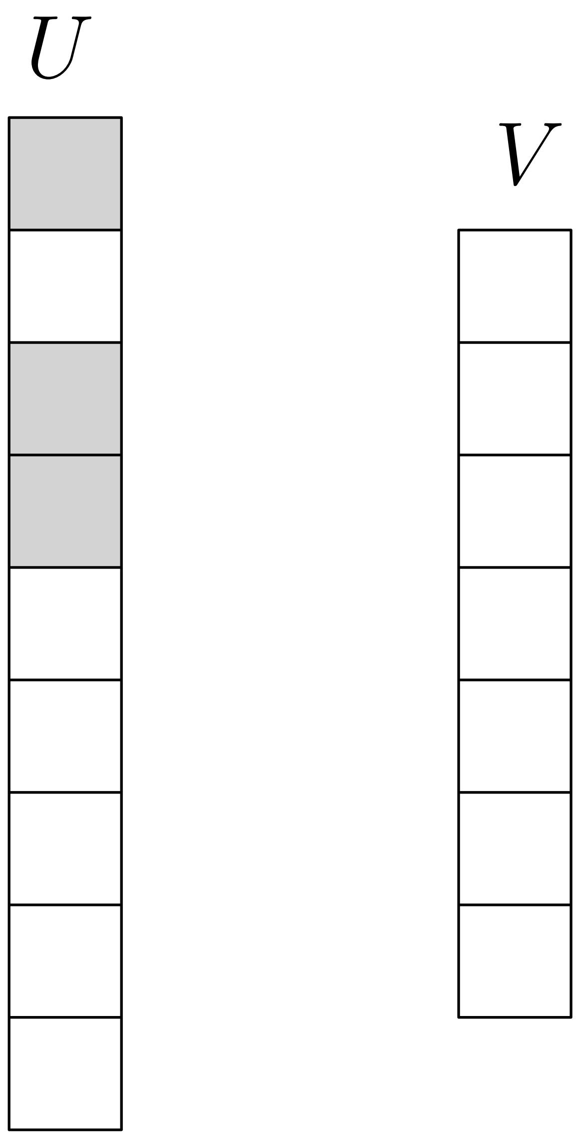
- Space $O(ku^{1/t}t^2)$. Time $O(t^2)$.



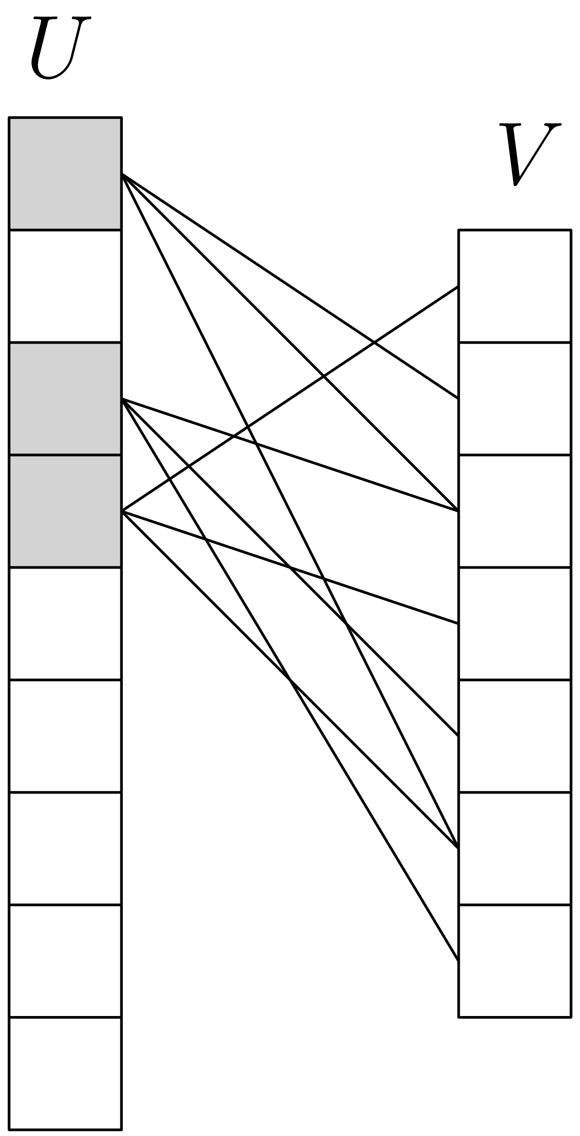
Definition A bipartite graph Γ is k-majority-unique if for every $S \subseteq U$ with $|S| \leq k$ there exists $x \in S$ such that the majority of vertices in $\Gamma(\{x\})$ have exactly one neighbor in S



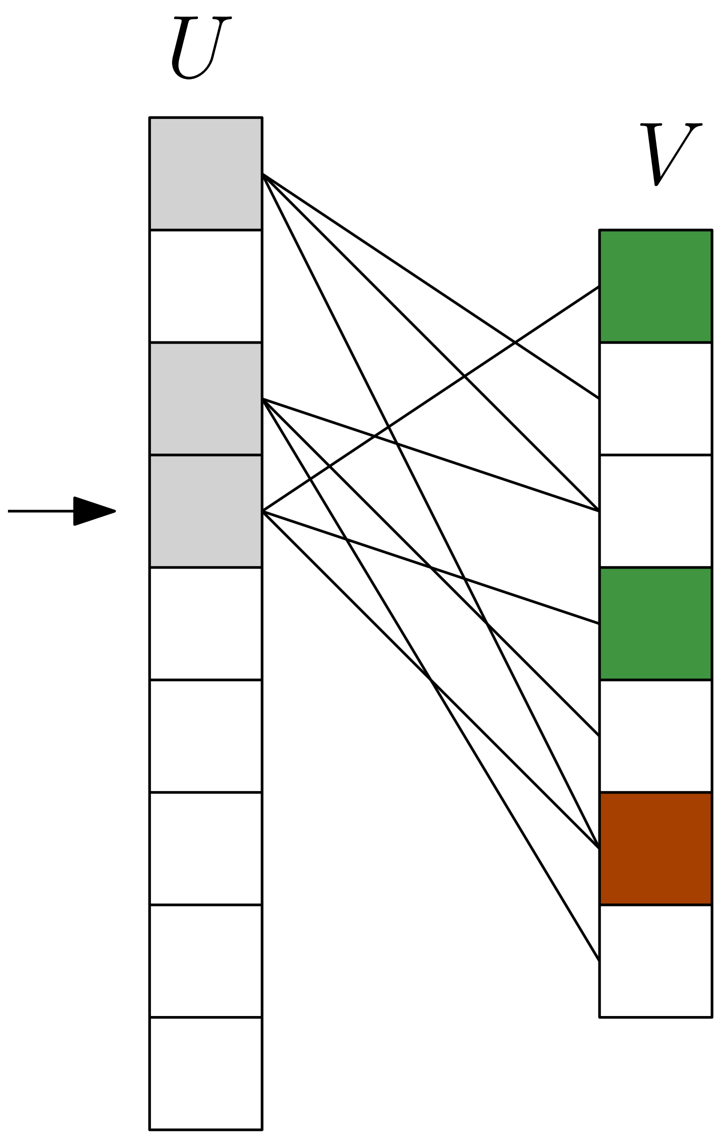
Definition A bipartite graph Γ is k-majority-unique if for every $S \subseteq U$ with $|S| \leq k$ there exists $x \in S$ such that the majority of vertices in $\Gamma(\{x\})$ have exactly one neighbor in S



Definition A bipartite graph Γ 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



Definition A bipartite graph Γ 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



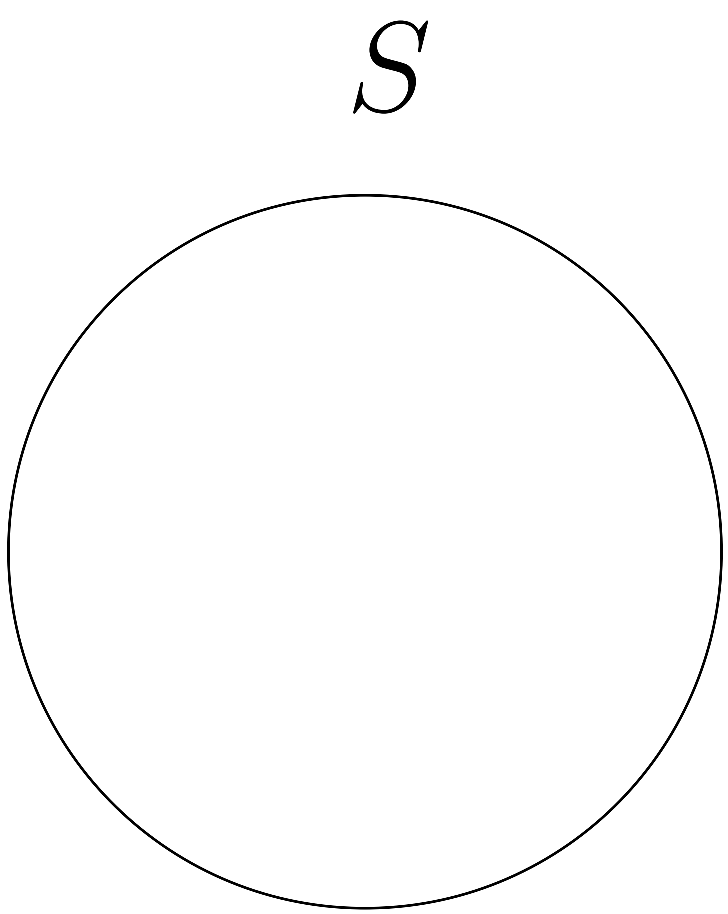
Lemma Let Γ be k-majority-unique over an alphabet Σ. Then the function defined by $\Gamma(x_1x_2)_i = \Gamma(x_1)_i\Gamma(x_2)_i$ is k-unique over Σ^2.

A graph product based on component-wise concatenation

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

Proof:

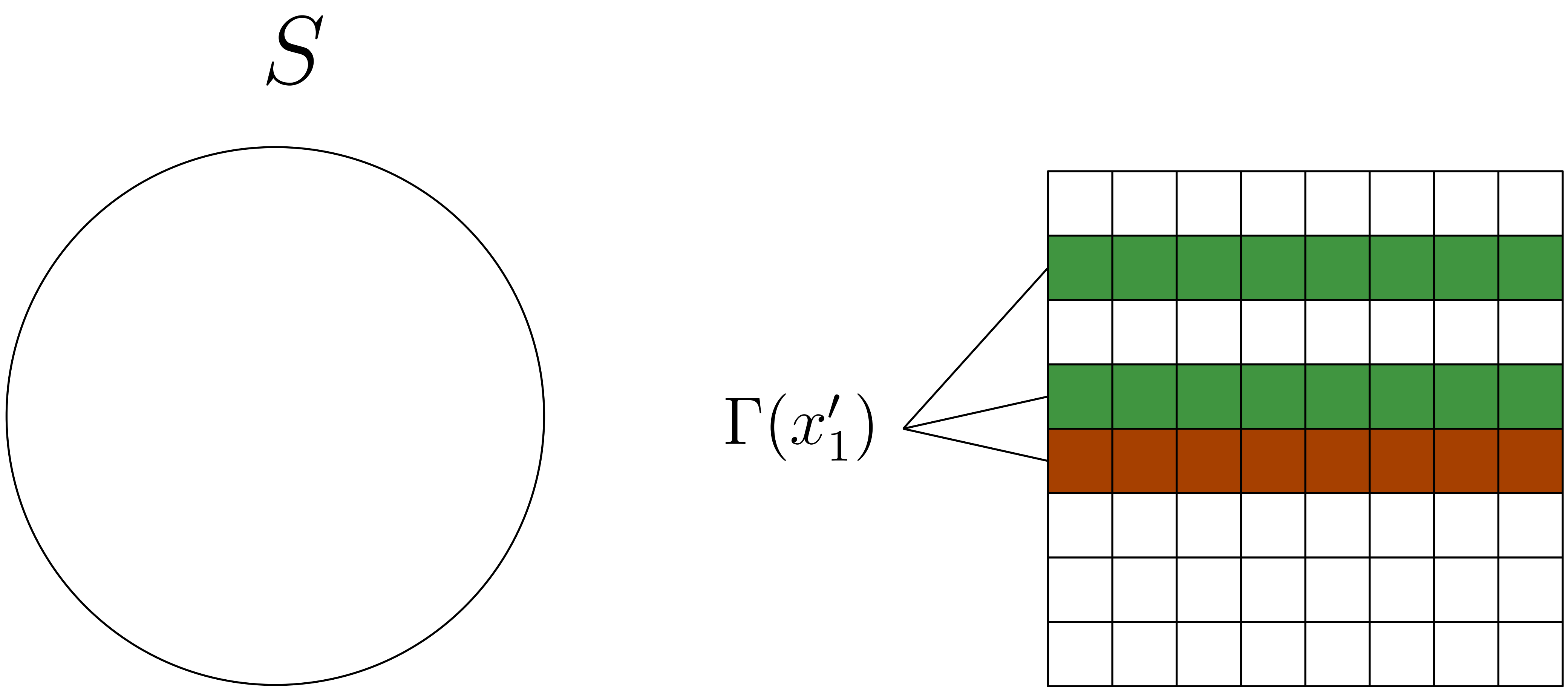
- Goal: Find a key $x'_1 x'_2 \in S \subseteq \Sigma^2$ that has a unique neighbor



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

Proof:

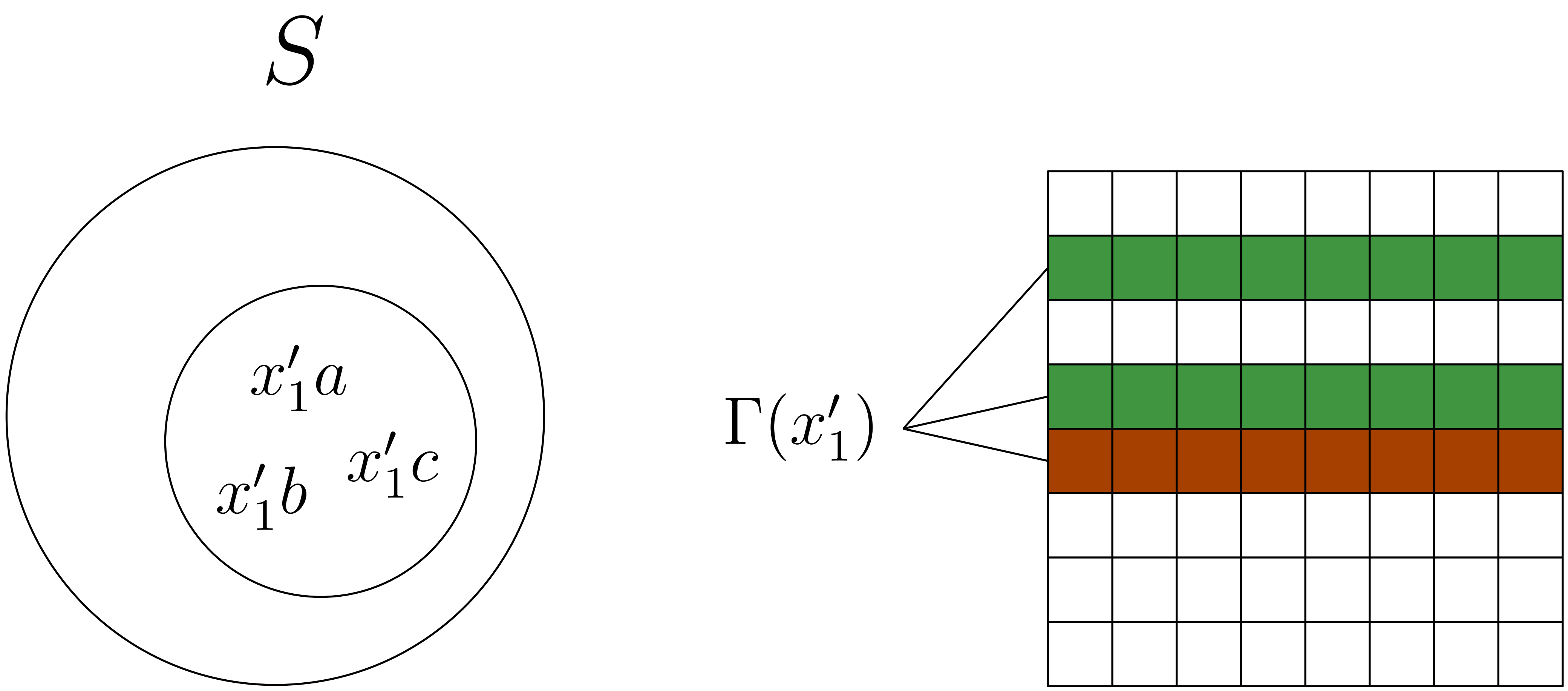
- Goal: Find a key $x'_1x'_2 \in S \subseteq \Sigma^2$ that has a unique neighbor
- There exists $x'_1 \in \{x_1 \mid x_1x_2 \in S\}$ with $> d/2$ unique neighbors



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

Proof:

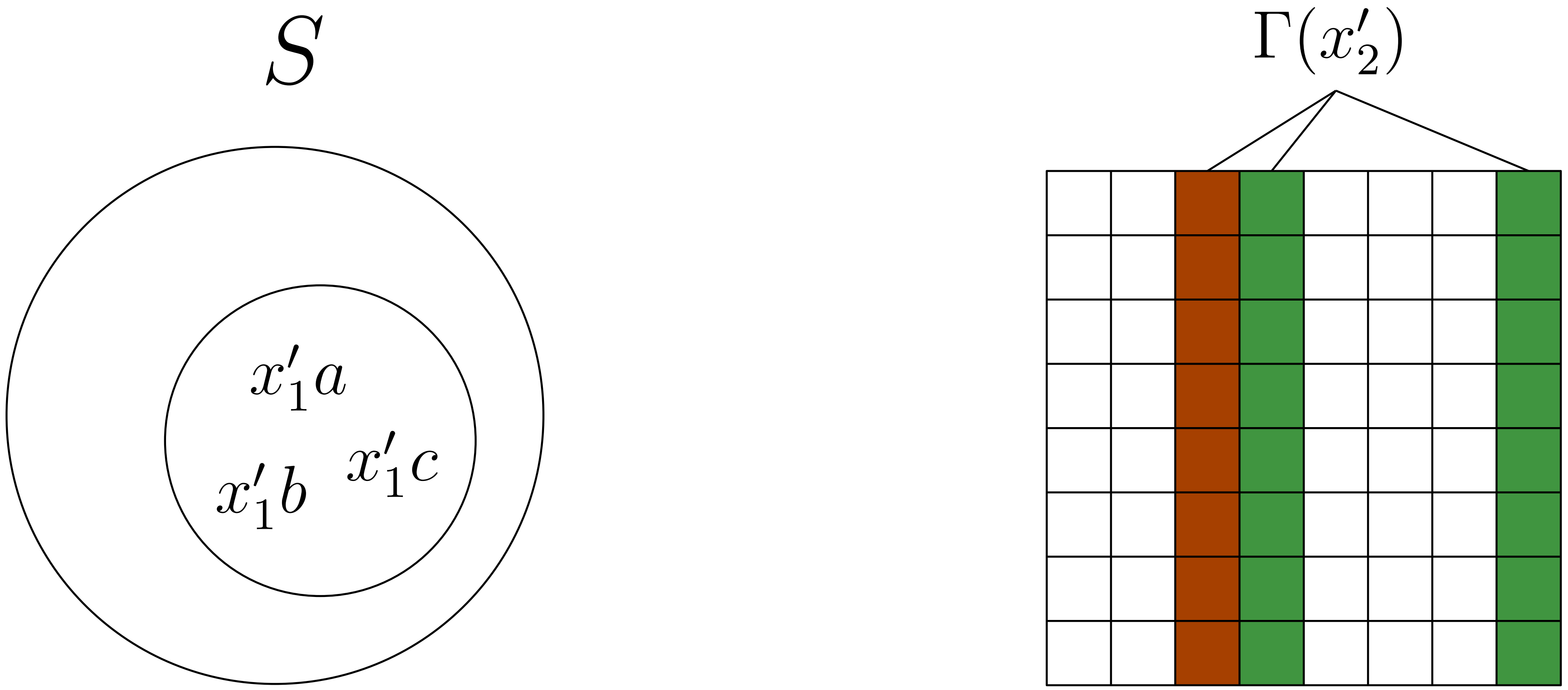
- Goal: Find a key $x'_1x'_2 \in S \subseteq \Sigma^2$ that has a unique neighbor
- There exists $x'_1 \in \{x_1 \mid x_1x_2 \in S\}$ with $> d/2$ unique neighbors



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

Proof:

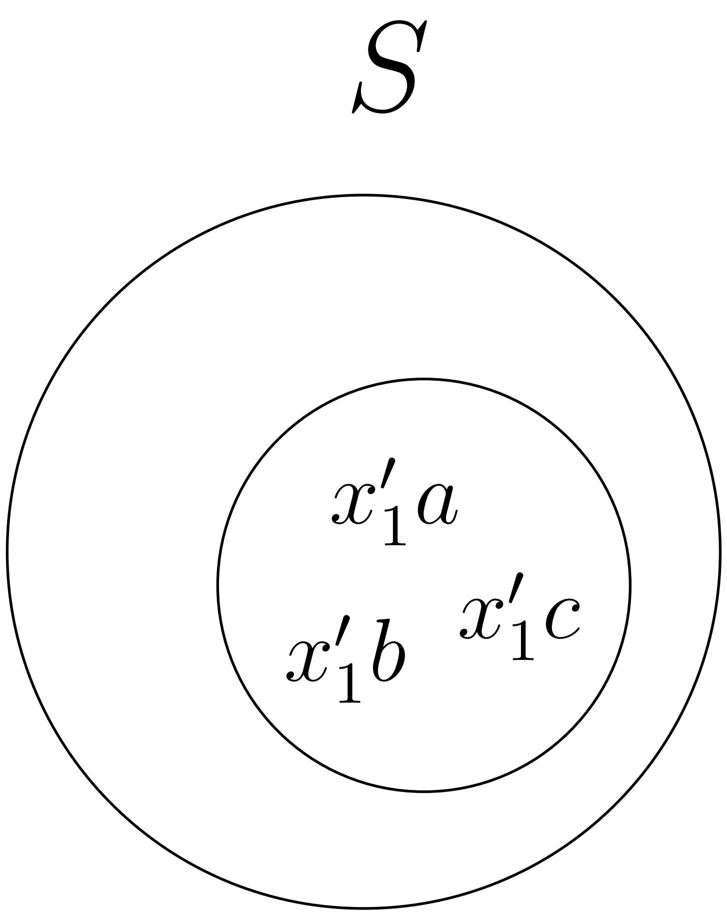
- Goal: Find a key $x'_1 x'_2 \in S \subseteq \Sigma^2$ that has a unique neighbor
- There exists $x'_1 \in \{x_1 \mid x_1 x_2 \in S\}$ with $> d/2$ unique neighbors
- There exists $x'_2 \in \{x_2 \mid x'_1 x_2 \in S\}$ with $> d/2$ unique neighbors

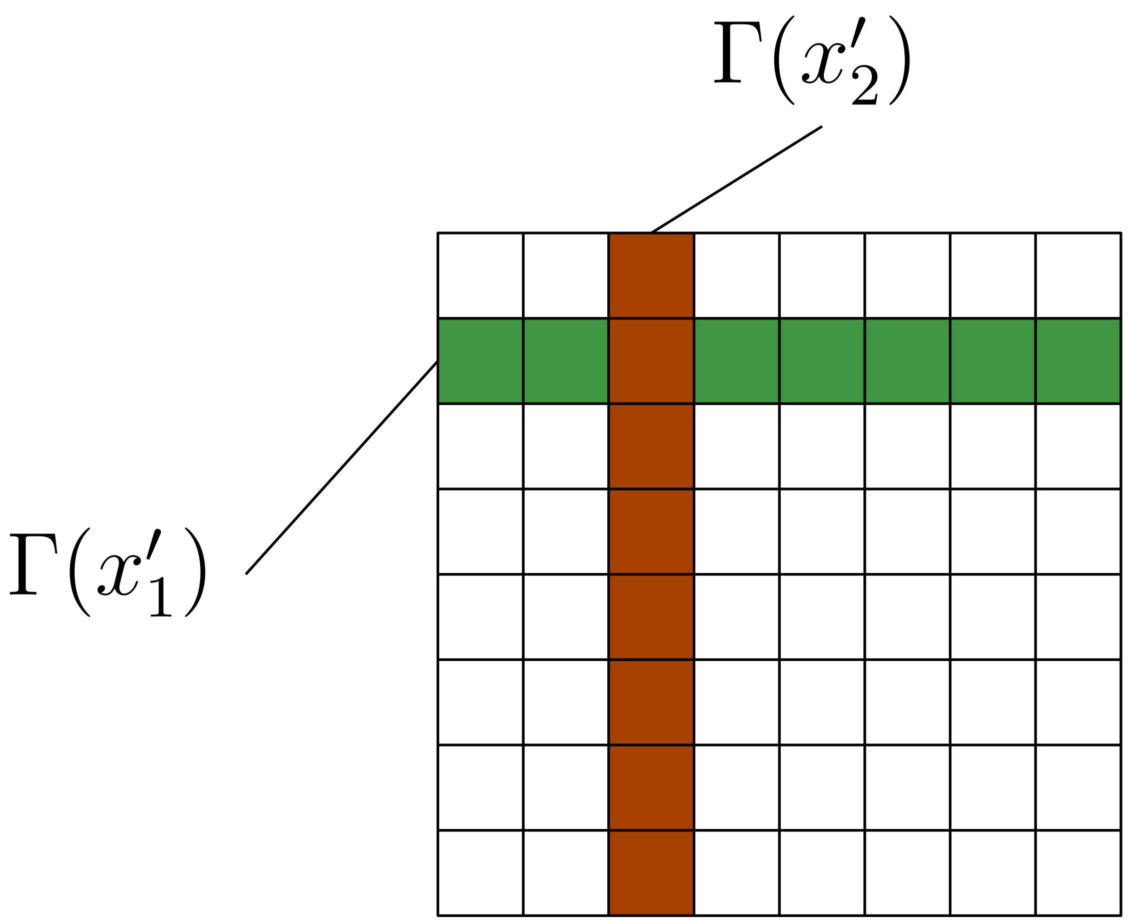


Lemma Let Γ be k-majority-unique over an alphabet Σ. Then the function defined by $\Gamma(x_1x_2)_i = \Gamma(x_1)_i\Gamma(x_2)_i$ is k-unique over Σ^2.

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

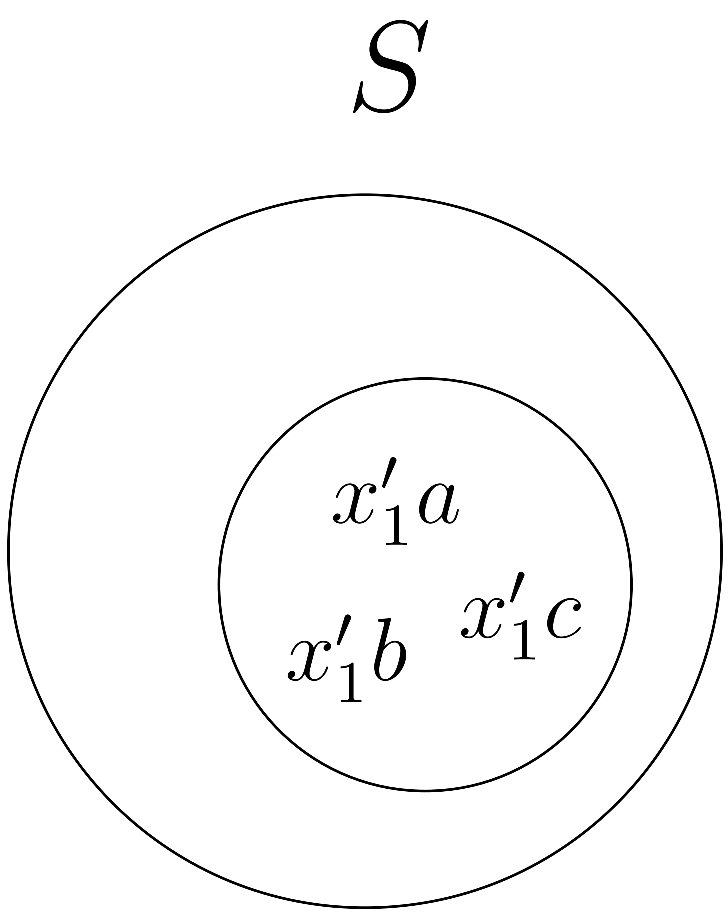


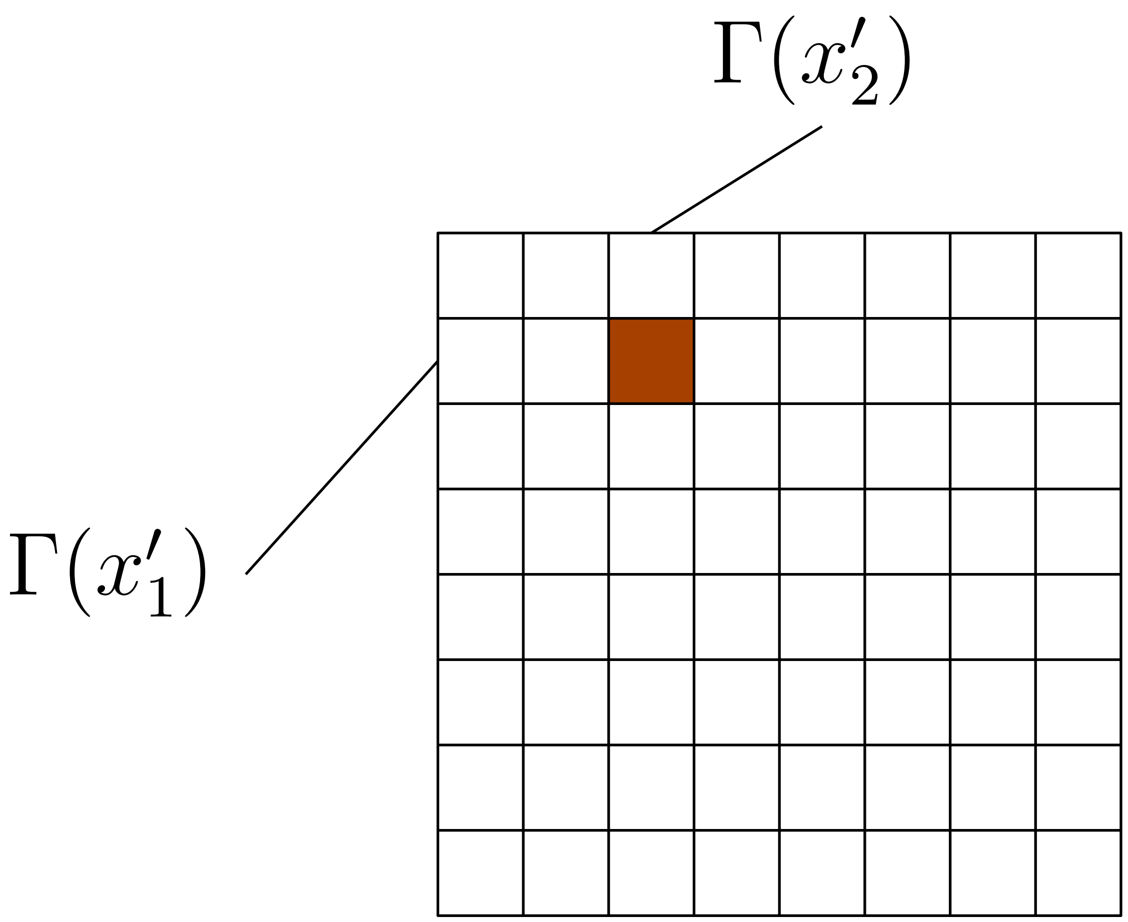


Lemma Let Γ be k-majority-unique over an alphabet Σ. Then the function defined by $\Gamma(x_1 x_2)_i = \Gamma(x_1)_i \Gamma(x_2)_i$ is k-unique over Σ^2.

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

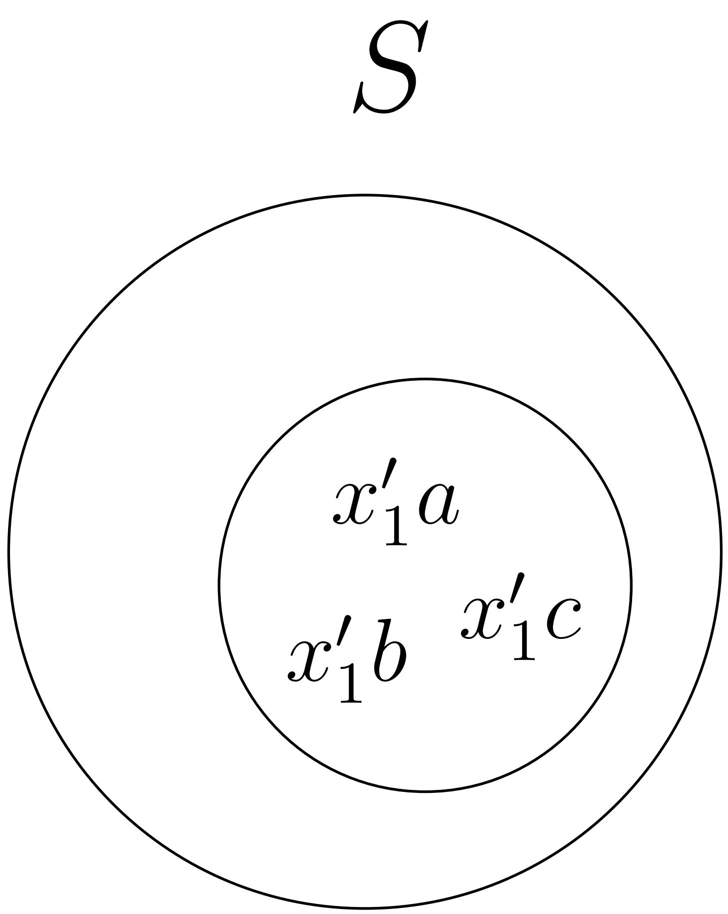


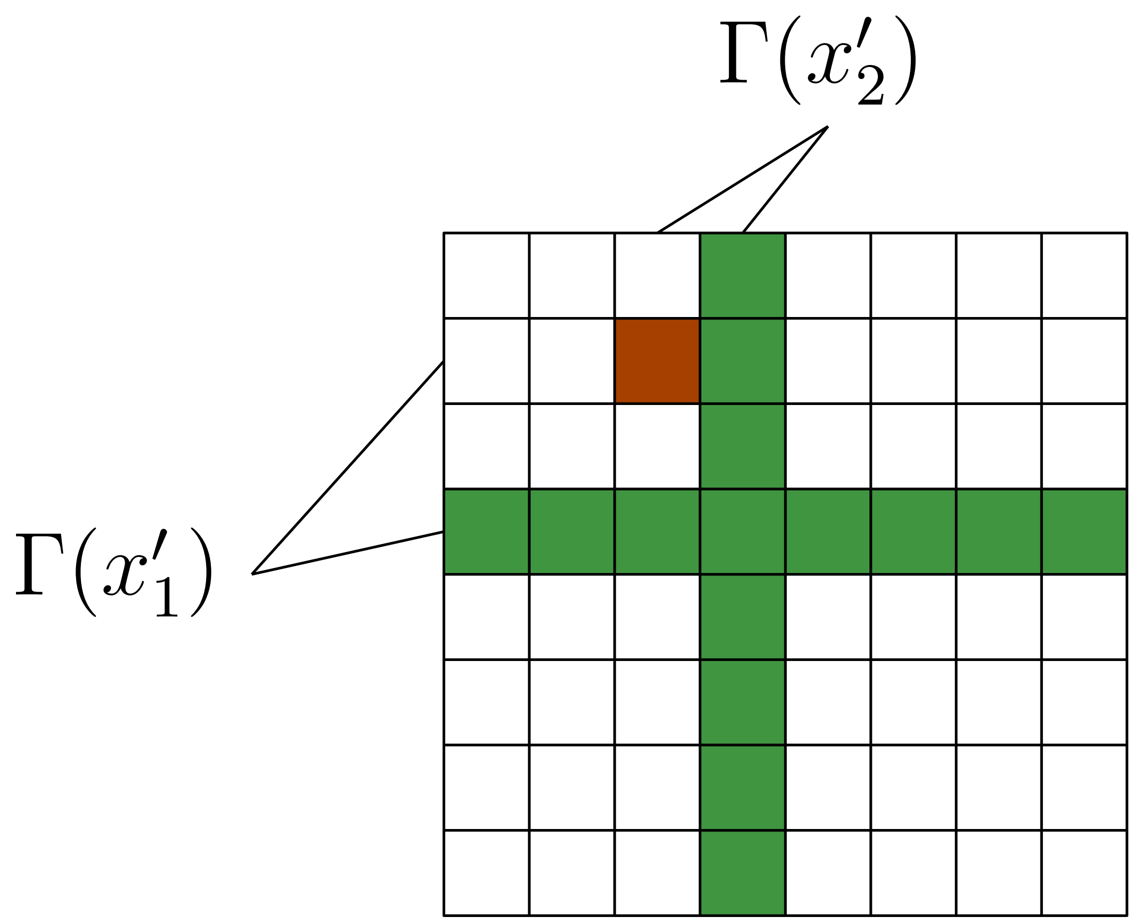


Lemma Let Γ be k-majority-unique over an alphabet Σ. Then the function defined by $\Gamma(x_1x_2)_i = \Gamma(x_1)_i\Gamma(x_2)_i$ is k-unique over Σ^2.

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 $x_2' \in \{x_2 \mid x_1'x_2 \in S\}$ with $> d/2$ unique neighbors

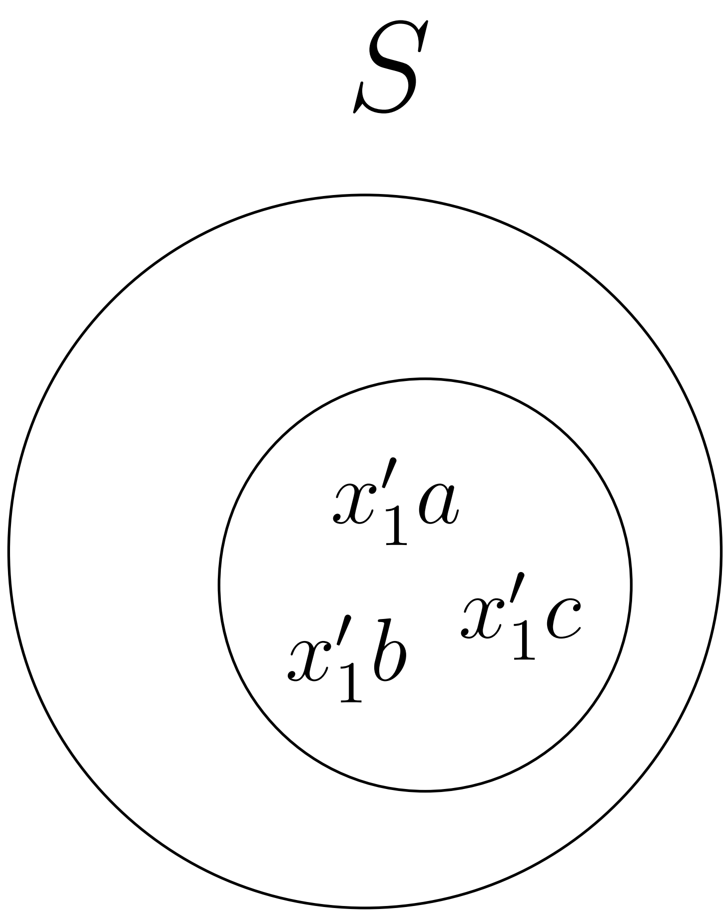


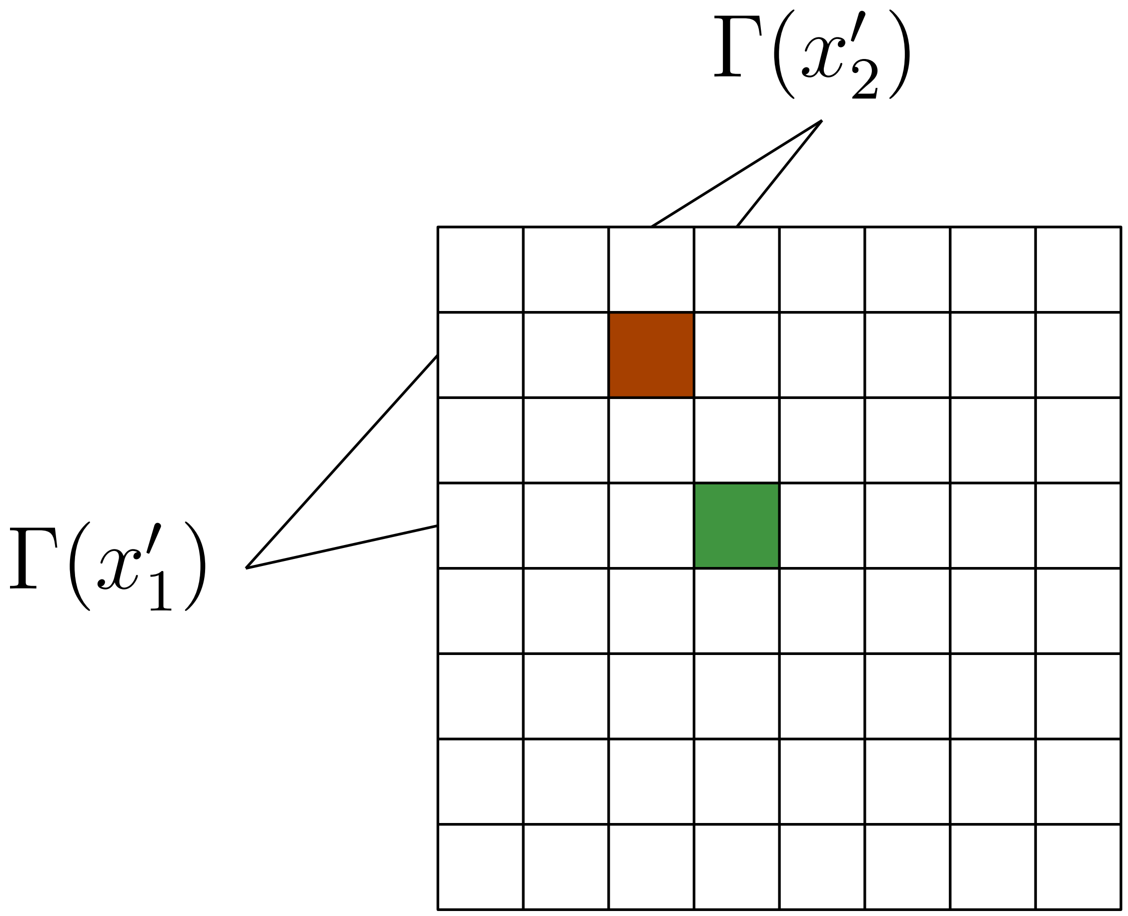


Lemma Let Γ be k-majority-unique over an alphabet Σ. Then the function defined by $\Gamma(x_1x_2)_i = \Gamma(x_1)_i\Gamma(x_2)_i$ is k-unique over Σ^2.

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

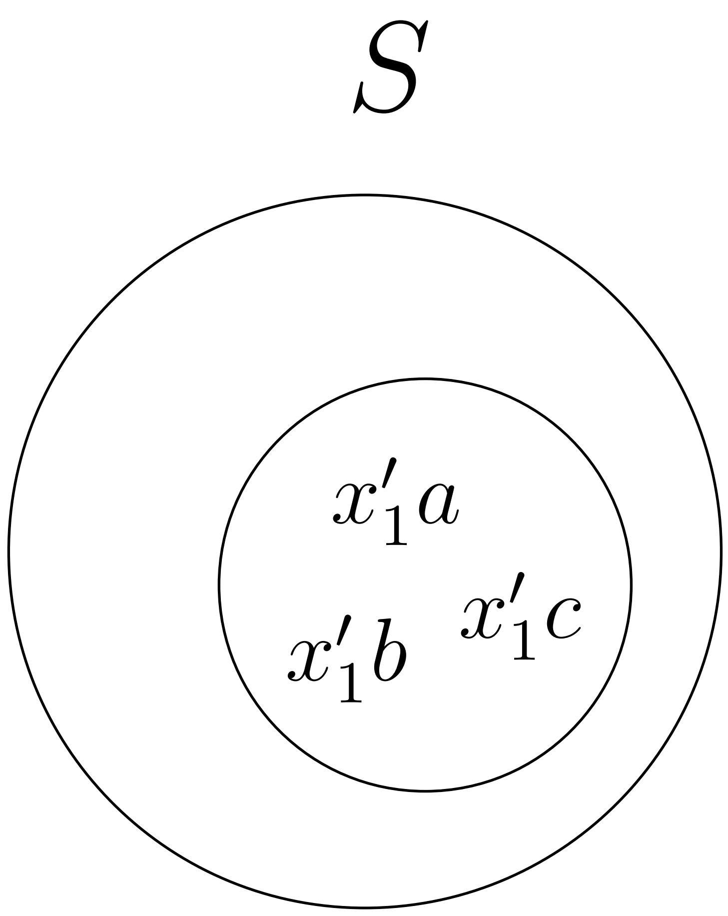


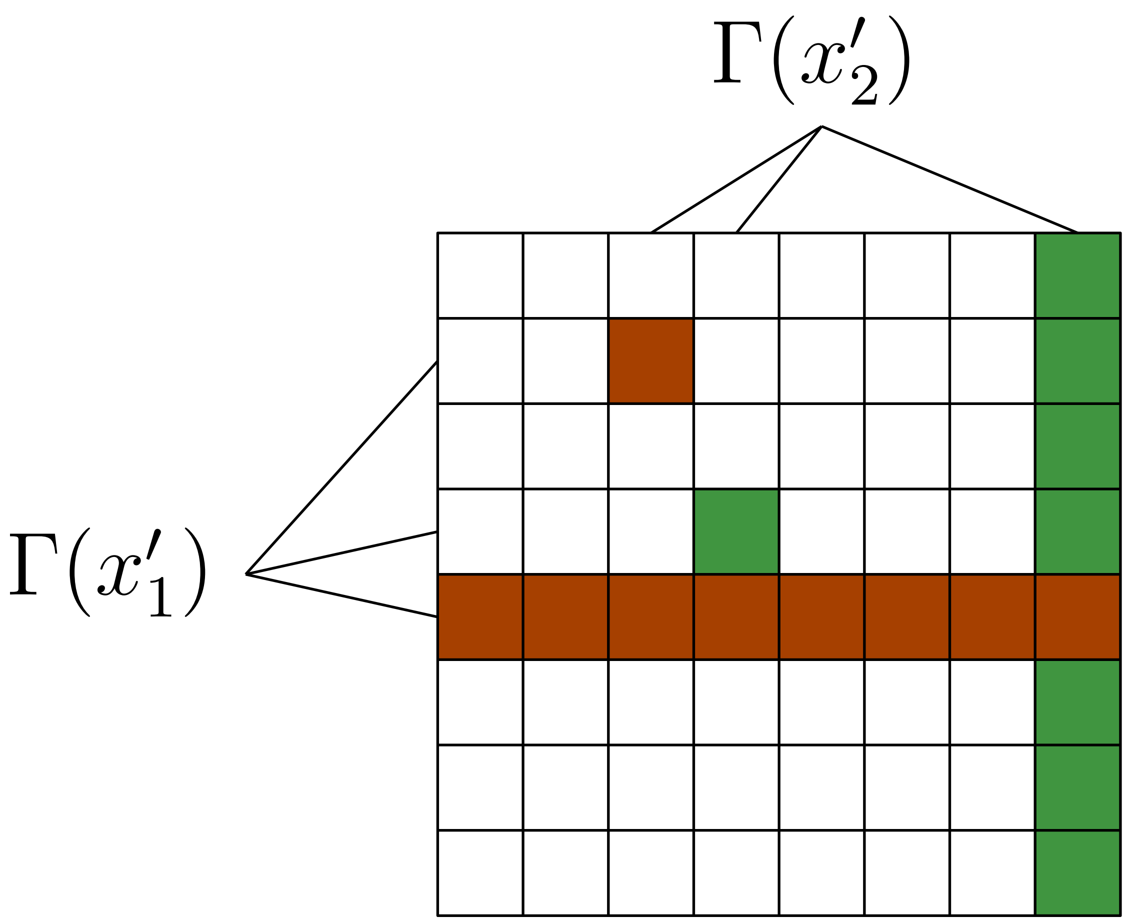


Lemma Let Γ be k-majority-unique over an alphabet Σ. Then the function defined by $\Gamma(x_1x_2)_i = \Gamma(x_1)_i\Gamma(x_2)_i$ is k-unique over Σ^2.

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

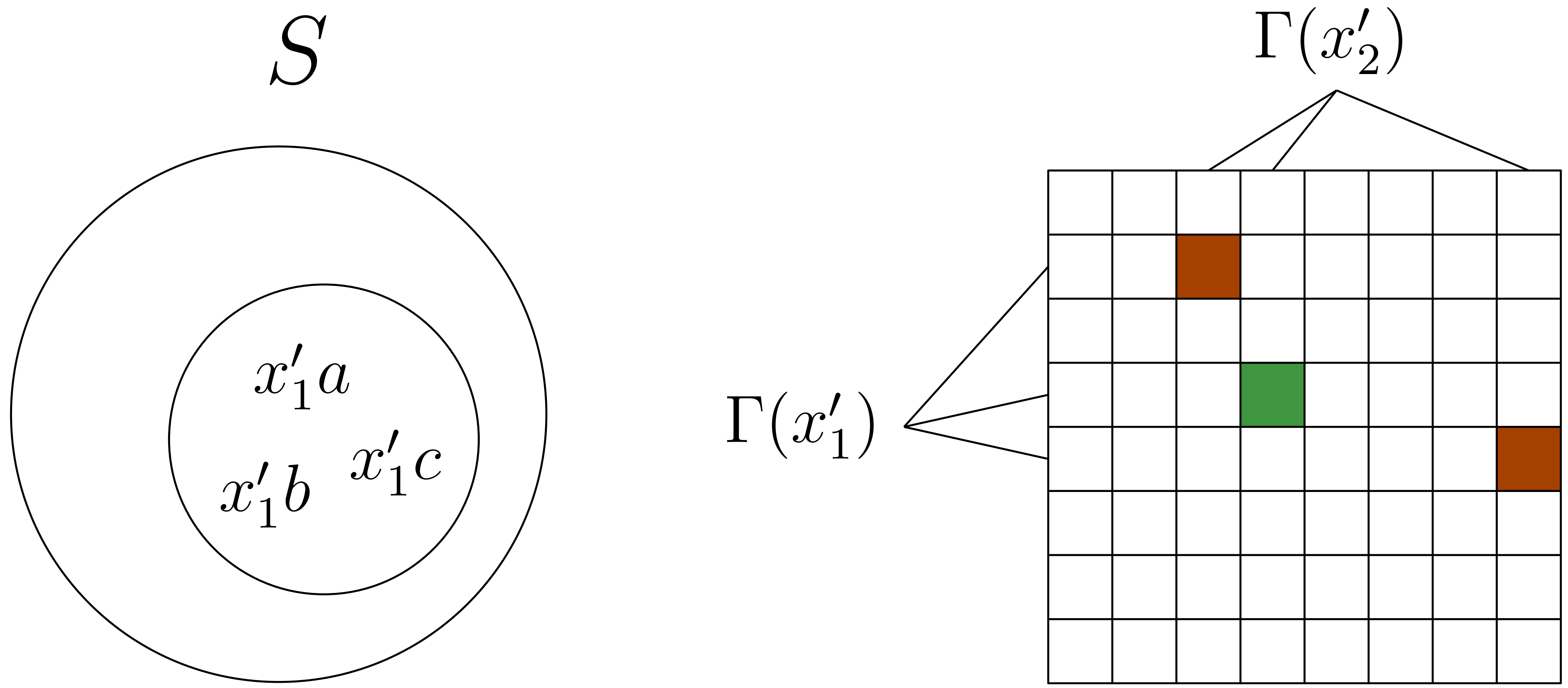




Lemma Let Γ be k-majority-unique over an alphabet Σ. Then the function defined by $\Gamma(x_1x_2)_i = \Gamma(x_1)_i\Gamma(x_2)_i$ is k-unique over Σ^2.

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 $x_2' \in \{x_2 \mid x_1'x_2 \in S\}$ with $> d/2$ unique neighbors



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

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

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

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

	Universe	Degree
$\Gamma(x)$	u	d

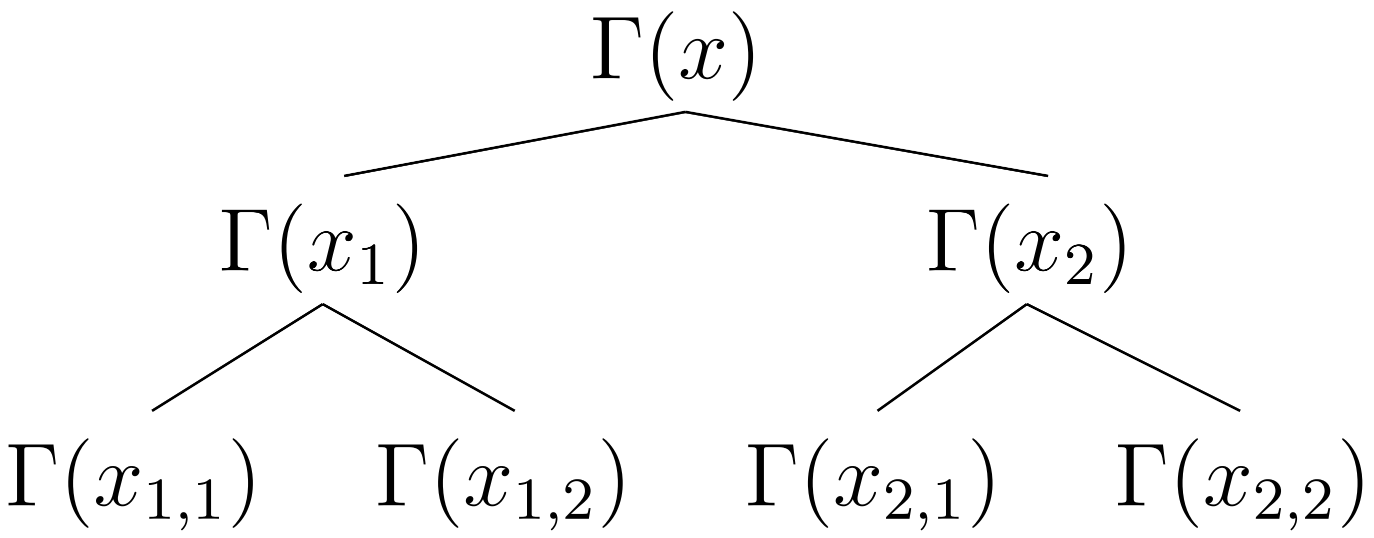
- View $x \in [u]$ as a string of two characters and recurse on each

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

		Universe	Degree
$\Gamma(x)$		u	d
$\Gamma(x_1)$	$\Gamma(x_2)$	$u^{1/2}$	$d/2$

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

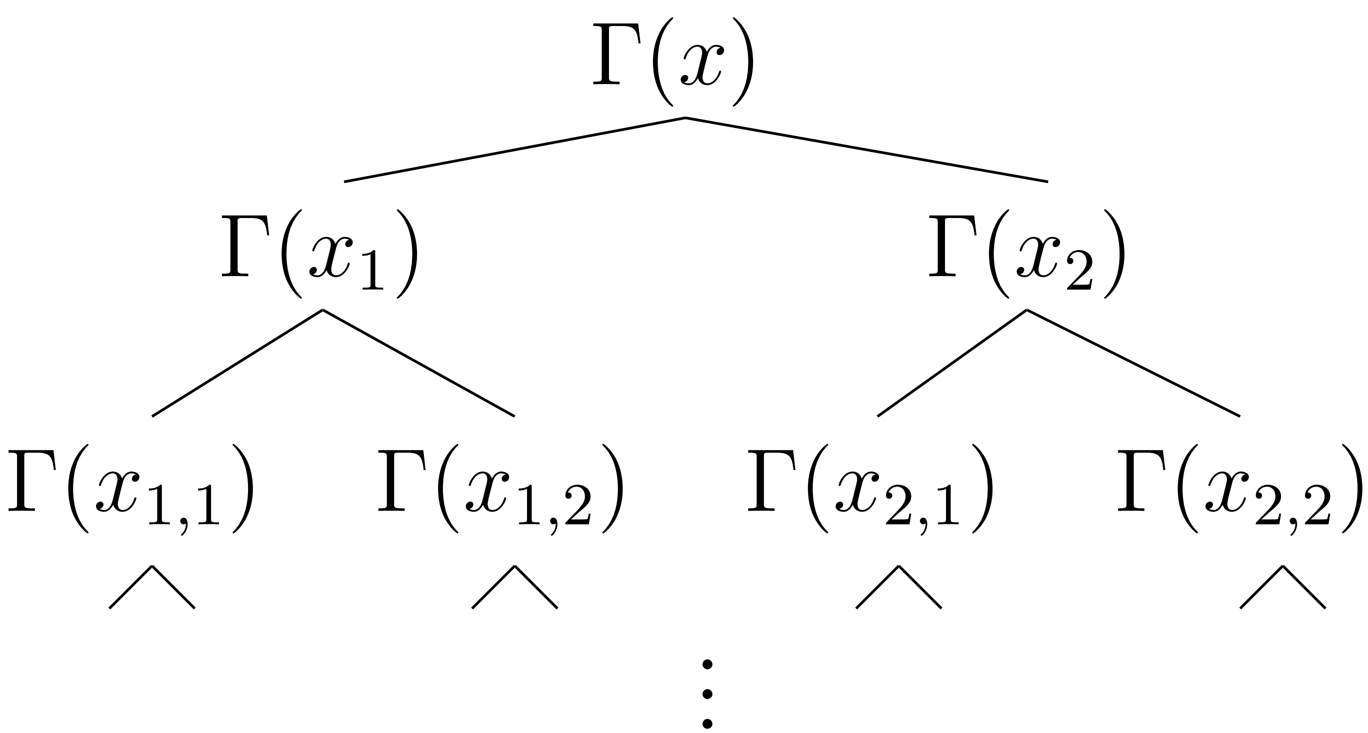
$$\Gamma(x_1 x_2) = \bigoplus_i h(\Gamma(x_1)_i, \Gamma(x_2)_i)$$



Universe	Degree
u	d
$u^{1/2}$	$d/2$
$u^{1/4}$	$d/4$

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

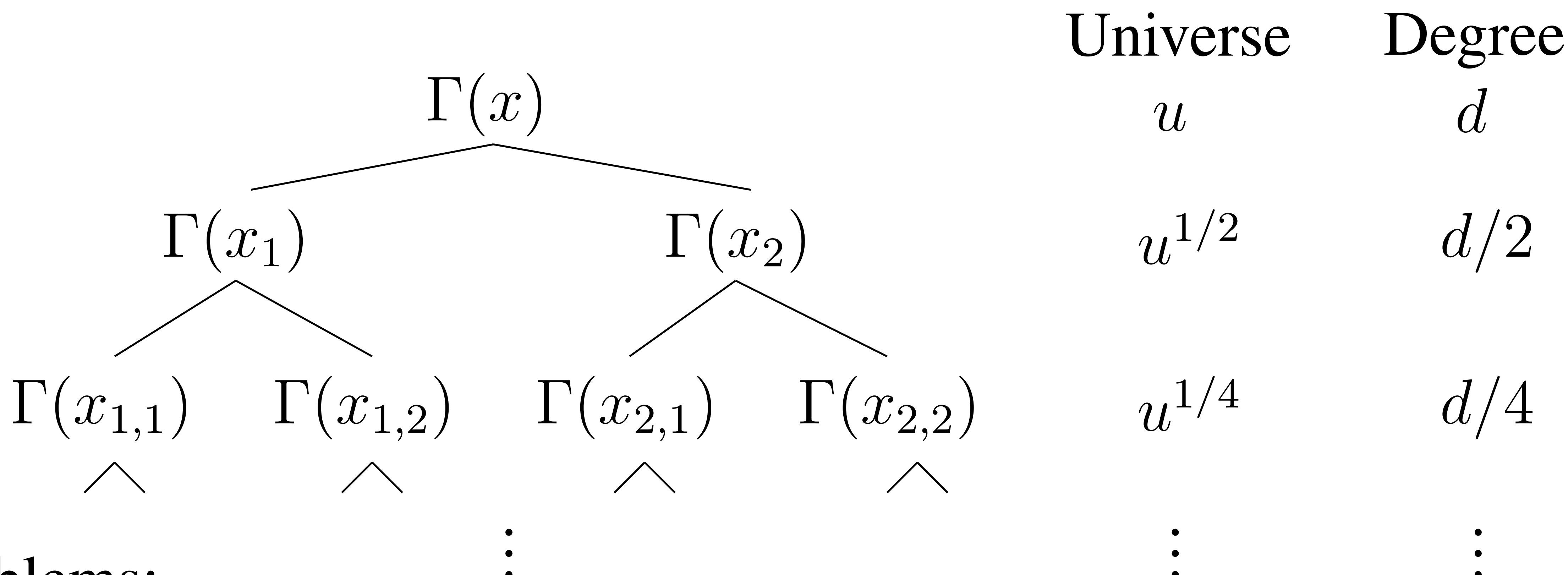
$$\Gamma(x_1 x_2) = \bigoplus_i h(\Gamma(x_1)_i, \Gamma(x_2)_i)$$



Universe	Degree
u	d
$u^{1/2}$	$d/2$
$u^{1/4}$	$d/4$
$\vdots$	$\vdots$

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

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



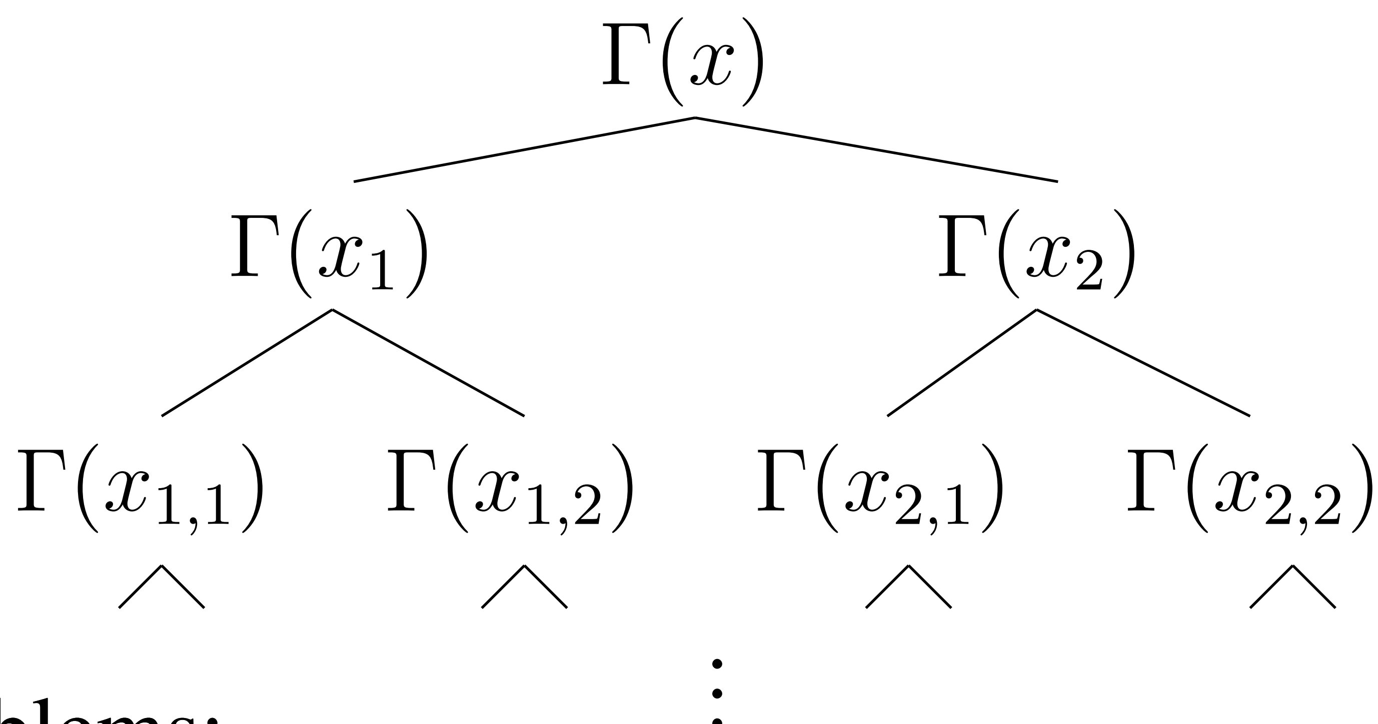
Problems:

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

A divide-and-conquer recursion

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

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



Universe	Degree
u	d
$u^{1/2}$	$d/2$
$u^{1/4}$	$d/4$
$\vdots$	$\vdots$

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

Result:

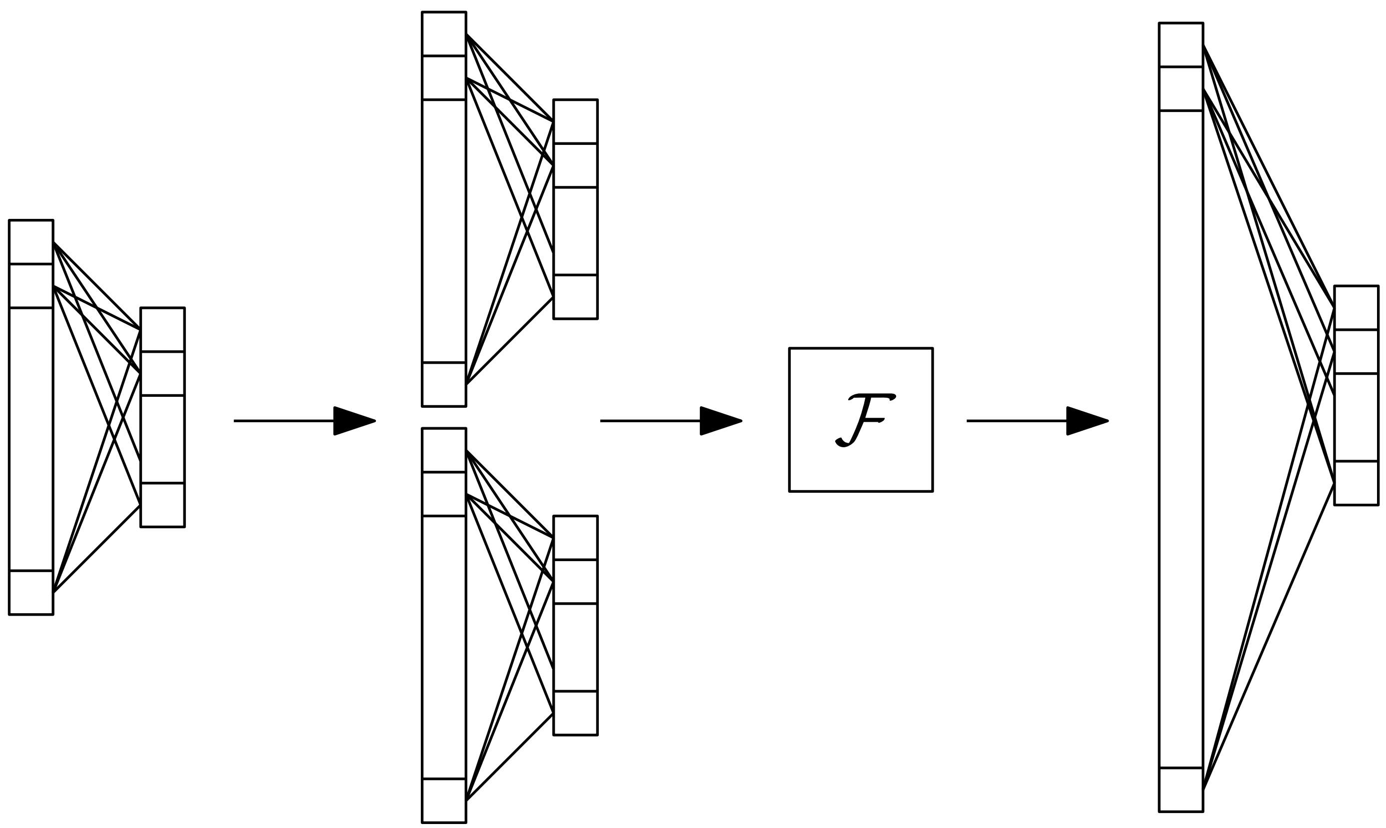
- Near-optimal space-time tradeoff for k-independent functions

Result:

- Near-optimal space-time tradeoff for k-independent functions

Technique:

- Graph products and alternating between expansion and independence

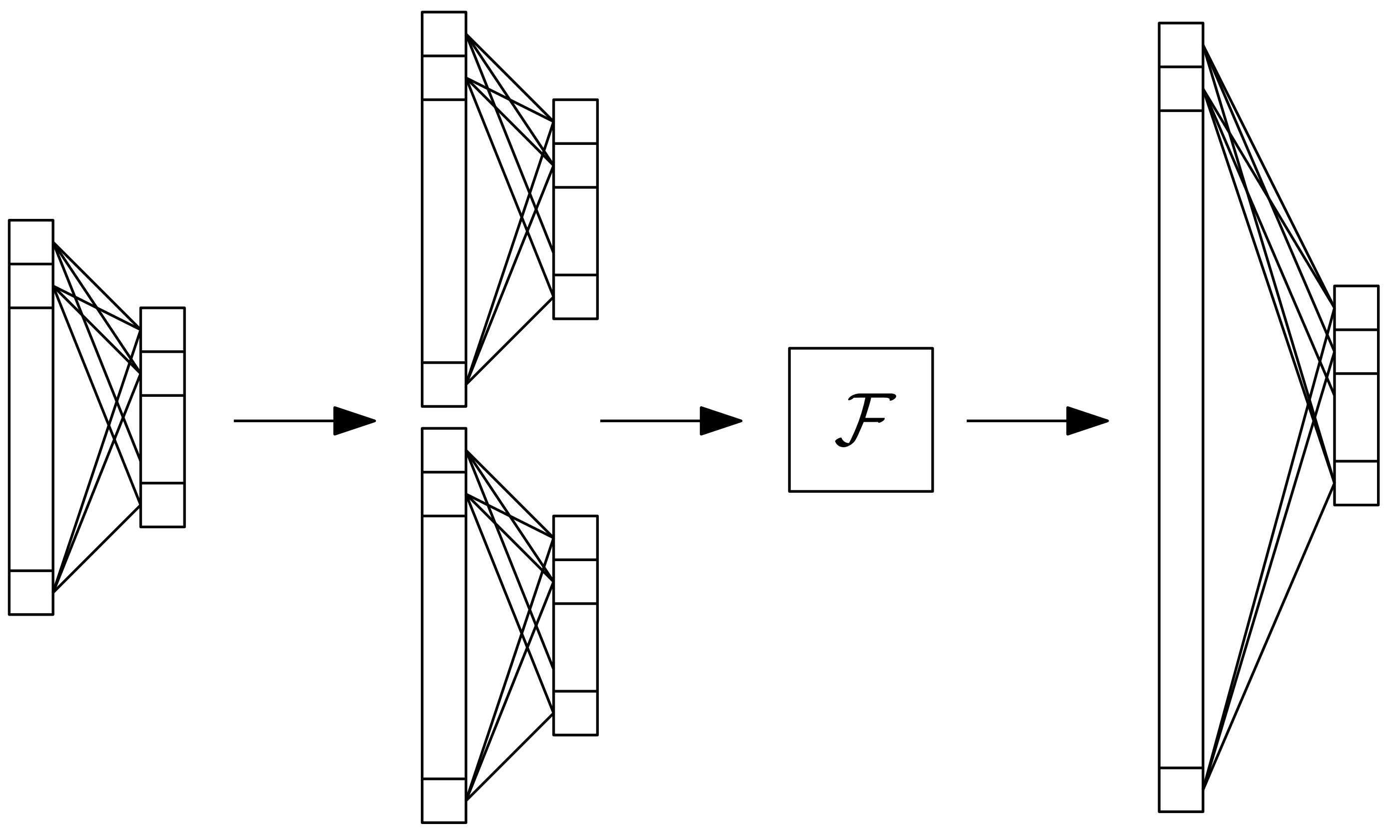


Result:

- Near-optimal space-time tradeoff for k-independent functions

Technique:

- Graph products and alternating between expansion and independence



Open questions:

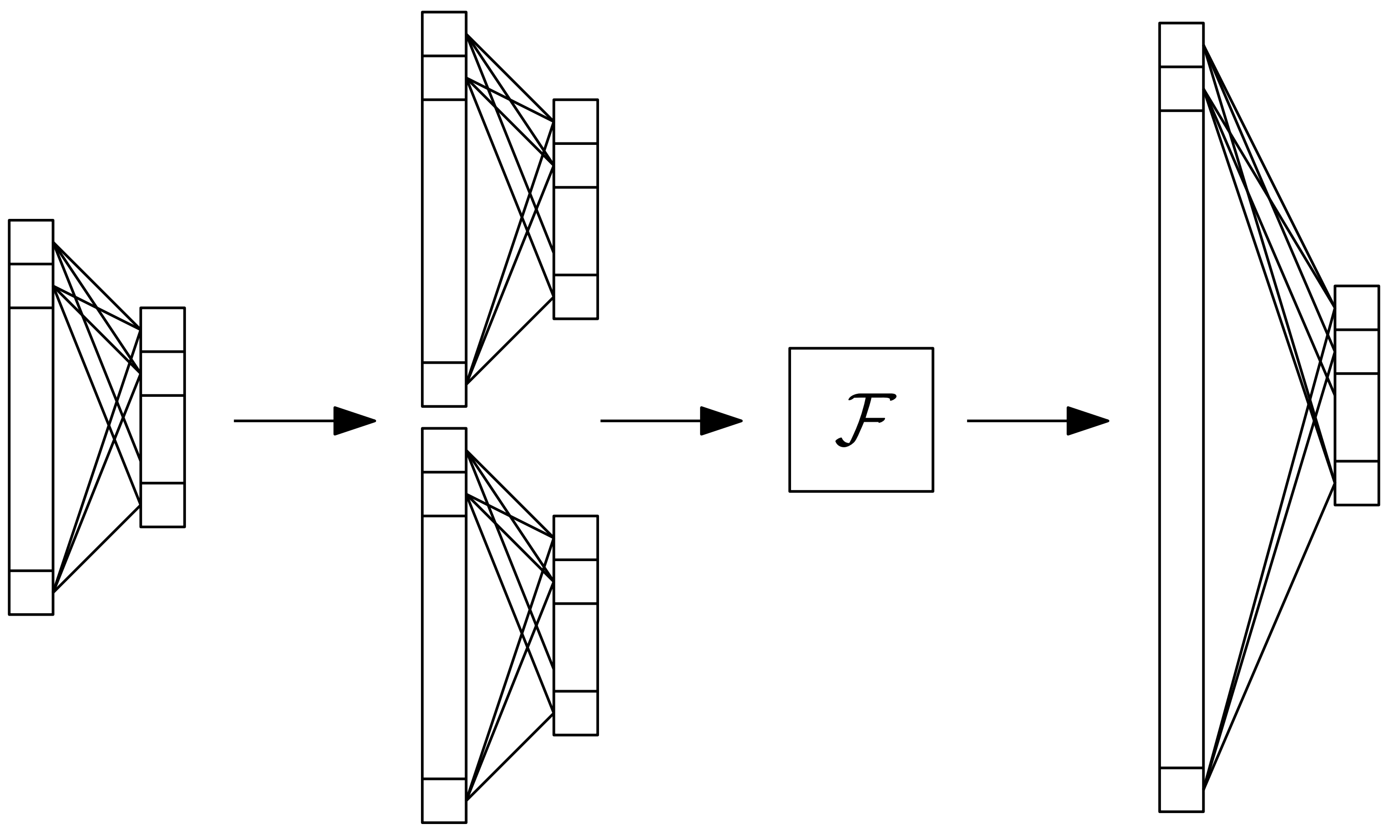
- Optimal expanders without k-independence

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!