A Word Reconstruction Problem for Polynomial Regular Language

Mehdi Golafshan, **Annika Huch**, Michel Rigo

University of Liège and Kiel University

What?

Introduction

Reconstruction &

Polynomial Regular Languages

Polynomials

for Reconstruction

Nice Case

Two Loops

General Case

and its problems

Let’s get started!

Introduction

Reconstruction &

Polynomial Regular Languages

Polynomials

for Reconstruction

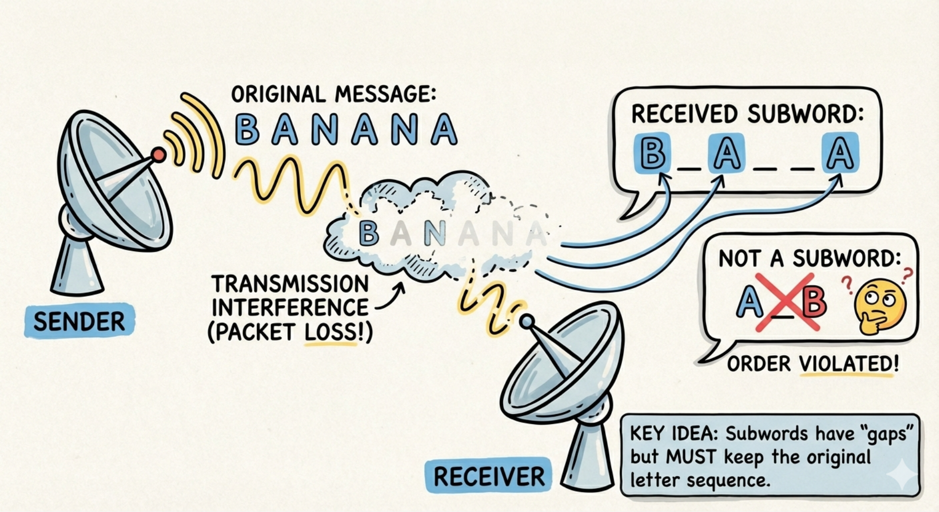
Nice Case

Two Loops

General Case

and its problems

(Scattered) Sub-words



Reconstruction

- Uniquely determine an unknown word from queries

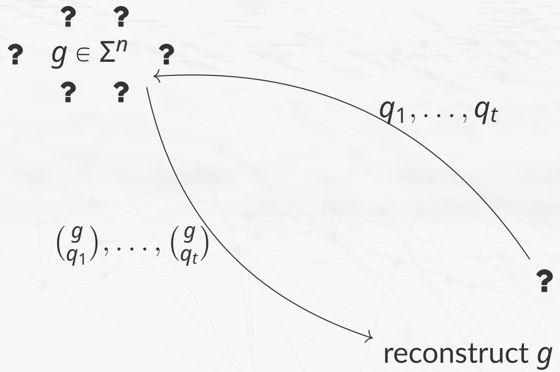
Reconstruction

Uniquely determine an unknown word from queries

Definition (Reconstruction Queries)

$$\binom{g}{q} = \#\{i_1 < \cdots < i_{|q|} \mid g[i_1]\cdots g[i_{|q|}] = q\} \quad \text{for } g, q \in \Sigma^*$$

Reconstruction



What is known?

query all $q \in \Sigma^{\ell}$
find least ℓ to reconstruct w

What is known?

Reconstruction

query all $q \in \Sigma^{\ell}$
find least ℓ to reconstruct w

$\ell \leqslant \exp(\Omega(\log^{1/2}(n)))$
(Dudík, Schulman)

What is known?

query all $q \in \Sigma^\ell$ find least ℓ to reconstruct w $\ell \leqslant \exp(\Omega(\log^{1/2}(n))$ (Dudík, Schulman)	adapt next query on the result of the previous ones

What is known?

query all $q \in \Sigma^\ell$ find least ℓ to reconstruct w	adapt next query on the result of the previous ones
$\ell \leqslant \exp(\Omega(\log^{1/2}(n)))$ (Dudík, Schulman)	$\mathcal{O}(k\sqrt{n\log_2(n)})$ queries (Richomme, Rosenfeld)

What is known?

query all $q \in \Sigma^\ell$
find least ℓ to reconstruct w

$\ell \leqslant \exp(\Omega(\log^{1/2}(n)))$
(Dudík, Schulman)

adapt next query on the
result of the previous ones

$\mathcal{O}(k\sqrt{n \log_2(n)})$ queries
(Richomme, Rosenfeld)

➔ reconstruction of a word from a specific regular language

What is known?

query all $q \in \Sigma^\ell$ find least ℓ to reconstruct w	adapt next query on the result of the previous ones
$\ell \leqslant \exp(\Omega(\log^{1/2}(n)))$ (Dudík, Schulman)	$\mathcal{O}(k\sqrt{n \log_2(n)})$ queries (Richomme, Rosenfeld)

→ reconstruction of a word from a specific regular language

regular languages with polynomial growth

Polynomial Regular Languages

Definition

A regular language L has **polynomial growth**

Polynomial Regular Languages

Definition

A regular language L has **polynomial growth** if $|L \cap \Sigma^n| \in O(n^k)$ for some $k \geqslant 0$.

Polynomial Regular Languages

Definition

A regular language L has **polynomial growth** if $|L \cap \Sigma^n| \in O(n^k)$ for some $k \geqslant 0$.

Theorem (Szilard *et al.* '92)

Every polynomial regular language is a finite union of languages of the form

Polynomial Regular Languages

Definition

A regular language L has **polynomial growth** if $|L \cap \Sigma^n| \in O(n^k)$ for some $k \geqslant 0$.

Theorem (Szilard *et al.* '92)

Every polynomial regular language is a finite union of languages of the form

$$L = u_1 v_1^* u_2 \cdots u_t v_t^* u_{t+1} \quad \textit{for } t \geqslant 1, v_1, \ldots, v_t \neq \varepsilon$$

Polynomial Regular Languages

Theorem (Szilard *et al.* ’92)

Every polynomial regular language is a finite union of languages of the form

$$L = u_1 v_1^* u_2 \cdots u_t v_t^* u_{t+1} \quad \text{for } t \geqslant 1, v_1, \ldots, v_t \neq \varepsilon$$

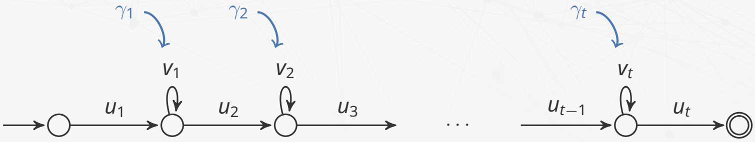
Polynomial Regular Languages

Automaton View

Theorem (Szilard *et al.* '92)

Every polynomial regular language is a finite union of languages of the form

$$L = u_1 v_1^* u_2 \cdots u_t v_t^* u_{t+1} \quad \text{for } t \geqslant 1, v_1, \ldots, v_t \neq \varepsilon$$



Polynomial Regular Languages

Reconstruction

$$g = u_1 v_1^{\gamma_1} u_2 \cdots u_t v_t^{\gamma_t} u_{t+1}$$

$q_1, \ldots, q_t$

$\binom{g}{q_1}, \ldots, \binom{g}{q_t}$

reconstruct g

$=$ uniquely determine $\gamma_1, \ldots, \gamma_t$

What?

Introduction

Basics & Initial Results

Polynomials

for Reconstruction

Nice Case

Two Loops

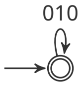
General Case

and its problems

Polynomial

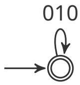
for loops

Example ($v = 010, u = 01$)



Polynomial

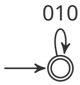
Example ($v = 010, u = 01$)



$$\binom{010^x}{01} = \binom{010}{01}\binom{x}{1} + \binom{010}{0}\binom{010}{1}\binom{x}{2}$$

Polynomial

Example ($v = 010, u = 01$)



$$\binom{010^x}{01} = \binom{010}{01}\binom{x}{1} + \binom{010}{0}\binom{010}{1}\binom{x}{2}$$

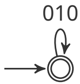
Lemma

For $v, u \in \Sigma^+$ and $x \in \mathbb{N}$, we have $\displaystyle\binom{v^x}{u} =$

Polynomial

for loops

Example ($v = 010, u = 01$)



$$\binom{010^x}{01} = \binom{010}{01}\binom{x}{1} + \binom{010}{0}\binom{010}{1}\binom{x}{2}$$

Lemma

For $v, u \in \Sigma^+$ and $x \in \mathbb{N}$, we have $\displaystyle\binom{v^x}{u} = \sum_{i=1}^{|u|} \sum_{\substack{u=u_1\cdots u_i \\ u_1,\ldots,u_i\in\Sigma^+}} \binom{v}{u_1}\cdots\binom{v}{u_i}\binom{x}{i}.$

Translation

to Polynomials

Step 1:

Translation

Step 1:

For $v \in \Sigma^+, u \in \Sigma^*, i \in \mathbb{N}$:

Translation

Step 1:

For $v \in \Sigma^+, u \in \Sigma^*, i \in \mathbb{N}$:

$$\alpha_i^{(v,u)} := \sum_{\substack{u = u_1 \cdots u_i \\ u_1, \ldots, u_i \in \Sigma^+}} \binom{v}{u_1} \cdots \binom{v}{u_i}$$

Translation

Step 1:

For $v \in \Sigma^+, u \in \Sigma^*, i \in \mathbb{N}$:

$$\alpha_i^{(v,u)} := \sum_{\substack{u = u_1 \cdots u_i \\ u_1, \ldots, u_i \in \Sigma^+}} \binom{v}{u_1} \cdots \binom{v}{u_i}$$

$$\Downarrow$$

coefficients for univariate polynomial

Translation

Step 1:

For $v \in \Sigma^+, u \in \Sigma^*, i \in \mathbb{N}$:

$$\alpha_i^{(v,u)} := \sum_{\substack{u = u_1 \cdots u_i \\ u_1, \ldots, u_i \in \Sigma^+}} \binom{v}{u_1} \cdots \binom{v}{u_i}$$

$$\Downarrow$$

coefficients for univariate polynomial

Step 2:

.

Translation

Step 1:

For $v \in \Sigma^+, u \in \Sigma^*, i \in \mathbb{N}$:

$$\alpha_i^{(v,u)} := \sum_{\substack{u = u_1 \cdots u_i \\ u_1, \ldots, u_i \in \Sigma^+}} \binom{v}{u_1} \cdots \binom{v}{u_i}$$

$$\Downarrow$$

coefficients for univariate polynomial

Step 2:

For $v \in \Sigma^+$:

.

Translation

Step 1:

For $v \in \Sigma^+, u \in \Sigma^*, i \in \mathbb{N}$:

$$\alpha_i^{(v,u)} := \sum_{\substack{u=u_1\cdots u_i \\ u_1,\ldots,u_i\in\Sigma^+}} \binom{v}{u_1}\cdots\binom{v}{u_i}$$

$\Downarrow$

coefficients for univariate polynomial

Step 2:

For $v \in \Sigma^+$:

$$B_{v,\varepsilon}(x) = 1$$

.

Translation

Step 1:

For $v \in \Sigma^+, u \in \Sigma^*, i \in \mathbb{N}$:

$$\alpha_i^{(v,u)} := \sum_{\substack{u=u_1\cdots u_i \\ u_1,\dots,u_i \in \Sigma^+}} \binom{v}{u_1} \cdots \binom{v}{u_i}$$

$\Downarrow$

coefficients for univariate polynomial

Step 2:

For $v \in \Sigma^+$:

$$B_{v,\varepsilon}(x) = 1$$

$$B_{v,u}(x) := \sum_{i=1}^{|u|} \alpha_i^{(v,u)} \binom{x}{i}$$

.

Translation

to Polynomials

Step 1:

For $v \in \Sigma^+, u \in \Sigma^*, i \in \mathbb{N}$:

$$\alpha_i^{(v,u)} := \sum_{\substack{u=u_1\cdots u_i\\ u_1,\dots,u_i\in\Sigma^+}} \binom{v}{u_1}\cdots\binom{v}{u_i}$$

$\Downarrow$

coefficients for univariate polynomial

Step 2:

For $v \in \Sigma^+$:

$$B_{v,\varepsilon}(x) = 1$$

$$B_{v,u}(x) := \sum_{i=1}^{|u|} \alpha_i^{(v,u)} \binom{x}{i}$$

If $\alpha_{|u|}^{(v,u)} \neq 0$, then $\deg(B_{v,u}) = |u|$.

$$L = u_1 v_1^* u_2 \cdots u_t v_t^* u_{t+1}$$

$$\binom{g}{q} =$$

$$L = u_1 v_1^* u_2 \cdots u_t v_t^* u_{t+1}$$

$$\binom{g}{q} = \sum_{\substack{q = e_1 f_1 e_2 \cdots e_t f_t e_{t+1} \\ e_i, f_i \in \Sigma^*}} \binom{u_1}{e_1} \binom{v_1^{x_1}}{f_1} \binom{u_2}{e_2} \cdots \binom{u_t}{e_t} \binom{v_t^{x_t}}{f_t} \binom{u_{t+1}}{e_{t+1}}$$

$$L = u_1 v_1^* u_2 \cdots u_t v_t^* u_{t+1}$$

Chu-Vandermonde

For all $w, z, u \in \Sigma^*$, we have

$$\binom{wz}{u} = \sum_{\substack{e,f \in A^* \\ u = ef}} \binom{w}{e} \binom{z}{f}.$$

$$\binom{g}{q} = \sum_{\substack{q = e_1 f_1 e_2 \cdots e_t f_t e_{t+1} \\ e_i, f_i \in \Sigma^*}} \binom{u_1}{e_1} \binom{v_1^{x_1}}{f_1} \binom{u_2}{e_2} \cdots \binom{u_t}{e_t} \binom{v_t^{x_t}}{f_t} \binom{u_{t+1}}{e_{t+1}}$$

$$L = u_1 v_1^* u_2 \cdots u_t v_t^* u_{t+1}$$

Chu-Vandermonde

For all $w, z, u \in \Sigma^*$, we have

$$\binom{wz}{u} = \sum_{\substack{e,f \in A^* \\ u = ef}} \binom{w}{e}\binom{z}{f}.$$

$$\binom{g}{q} = \sum_{\substack{q = e_1 f_1 e_2 \cdots e_t f_t e_{t+1} \\ e_i, f_i \in \Sigma^*}} \binom{u_1}{e_1}\binom{v_1^{x_1}}{f_1}\binom{u_2}{e_2}\cdots\binom{u_t}{e_t}\binom{v_t^{x_t}}{f_t}\binom{u_{t+1}}{e_{t+1}}$$

$$= \sum_{\substack{q = e_1 f_1 e_2 \cdots e_t f_t e_{t+1} \\ e_i, f_i \in \Sigma^*}} \prod_{j=1}^{t+1} \binom{u_j}{e_j}$$

$$L = u_1 v_1^* u_2 \cdots u_t v_t^* u_{t+1}$$

Chu-Vandermonde

For all $w, z, u \in \Sigma^*$, we have

$$\binom{wz}{u} = \sum_{\substack{e,f \in A^* \\ u = ef}} \binom{w}{e}\binom{z}{f}.$$

$$\binom{g}{q} = \sum_{\substack{q = e_1 f_1 e_2 \cdots e_t f_t e_{t+1} \\ e_i, f_i \in \Sigma^*}} \binom{u_1}{e_1}\binom{v_1^{x_1}}{f_1}\binom{u_2}{e_2}\cdots\binom{u_t}{e_t}\binom{v_t^{x_t}}{f_t}\binom{u_{t+1}}{e_{t+1}}$$

$$= \sum_{\substack{q = e_1 f_1 e_2 \cdots e_t f_t e_{t+1} \\ e_i, f_i \in \Sigma^*}} \prod_{j=1}^{t+1} \binom{u_j}{e_j} \prod_{j=1}^{t} B_{v_j, f_j}(x_j)$$

$$L = u_1 v_1^* u_2 \cdots u_t v_t^* u_{t+1}$$

Chu-Vandermonde

For all $w, z, u \in \Sigma^*$, we have

$$\binom{wz}{u} = \sum_{\substack{e,f \in A^* \\ u = ef}} \binom{w}{e}\binom{z}{f}.$$

$$\binom{g}{q} = \sum_{\substack{q = e_1 f_1 e_2 \cdots e_t f_t e_{t+1} \\ e_i, f_i \in \Sigma^*}} \binom{u_1}{e_1}\binom{v_1^{x_1}}{f_1}\binom{u_2}{e_2}\cdots\binom{u_t}{e_t}\binom{v_t^{x_t}}{f_t}\binom{u_{t+1}}{e_{t+1}}$$

$$= \sum_{\substack{q = e_1 f_1 e_2 \cdots e_t f_t e_{t+1} \\ e_i, f_i \in \Sigma^*}} \prod_{j=1}^{t+1} \binom{u_j}{e_j} \prod_{j=1}^{t} B_{v_j, f_j}(x_j) =: \mathrm{P}_q(x_1, \ldots, x_t)$$

$$L = u_1 v_1^* u_2 \cdots u_t v_t^* u_{t+1}$$

Chu-Vandermonde

For all $w, z, u \in \Sigma^*$, we have

$$\binom{wz}{u} = \sum_{\substack{e,f \in A^* \\ u = ef}} \binom{w}{e}\binom{z}{f}.$$

$$\binom{g}{q} = \sum_{\substack{q = e_1 f_1 e_2 \cdots e_t f_t e_{t+1} \\ e_i, f_i \in \Sigma^*}} \binom{u_1}{e_1}\binom{v_1^{x_1}}{f_1}\binom{u_2}{e_2} \cdots \binom{u_t}{e_t}\binom{v_t^{x_t}}{f_t}\binom{u_{t+1}}{e_{t+1}}$$

$$= \sum_{\substack{q = e_1 f_1 e_2 \cdots e_t f_t e_{t+1} \\ e_i, f_i \in \Sigma^*}} \prod_{j=1}^{t+1} \binom{u_j}{e_j} \prod_{j=1}^{t} B_{v_j, f_j}(x_j) =: \mathrm{P}_q(x_1, \ldots, x_t)$$

$\binom{g}{q}$ is a polynomial of degree at most $|q|$ and variables $x_1, \ldots, x_t$

$$L = u_1 v_1^* u_2 \cdots u_t v_t^* u_{t+1}$$

Chu-Vandermonde

For all $w, z, u \in \Sigma^*$, we have

$$\binom{wz}{u} = \sum_{\substack{e,f \in A^* \\ u = ef}} \binom{w}{e}\binom{z}{f}.$$

$$\binom{g}{q} = \sum_{\substack{q = e_1 f_1 e_2 \cdots e_t f_t e_{t+1} \\ e_i, f_i \in \Sigma^*}} \binom{u_1}{e_1}\binom{v_1^{x_1}}{f_1}\binom{u_2}{e_2} \cdots \binom{u_t}{e_t}\binom{v_t^{x_t}}{f_t}\binom{u_{t+1}}{e_{t+1}}$$

$$= \sum_{\substack{q = e_1 f_1 e_2 \cdots e_t f_t e_{t+1} \\ e_i, f_i \in \Sigma^*}} \prod_{j=1}^{t+1} \binom{u_j}{e_j} \prod_{j=1}^{t} B_{v_j, f_j}(x_j) =: \mathrm{P}_q(x_1, \ldots, x_t)$$

- $\binom{g}{q}$ is a polynomial of degree at most $|q|$ and variables $x_1, \ldots, x_t$
- $\mathrm{P}_q(x_1, \ldots, x_t)$ is independent of g

Equations

Definition

Let $q \in \Sigma^+$ and g from a polynomial regular language.

Equations

Definition

Let $q \in \Sigma^+$ and g from a polynomial regular language. Consider the polynomial in $\mathbb{Q}[x_1, \ldots, x_t]$

$$\mathrm{Eq}_{g,q} := \mathrm{P}_q(x_1, \ldots, x_t) - \binom{g}{q}.$$

Equations

Definition

Let $q \in \Sigma^+$ and g from a polynomial regular language. Consider the polynomial in $\mathbb{Q}[x_1, \ldots, x_t]$

$$\mathrm{Eq}_{g,q} := \mathrm{P}_q(x_1, \ldots, x_t) - \binom{g}{q}.$$

Theorem

Let $g = u_1 v_1^{\gamma_1} u_2 \cdots u_t v_t^{\gamma_t} u_{t+1}$ from a polynomial regular language.

Equations

Definition

Let $q \in \Sigma^+$ and g from a polynomial regular language. Consider the polynomial in $\mathbb{Q}[x_1, \ldots, x_t]$

$$\mathrm{Eq}_{g,q} := \mathrm{P}_q(x_1, \ldots, x_t) - \binom{g}{q}.$$

Theorem

Let $g = u_1 v_1^{\gamma_1} u_2 \cdots u_t v_t^{\gamma_t} u_{t+1}$ from a polynomial regular language. For all $q \in \Sigma^+$, the t-uple $(\gamma_1, \ldots, \gamma_t)$ of non-negative integers

Equations

Definition

Let $q \in \Sigma^+$ and g from a polynomial regular language. Consider the polynomial in $\mathbb{Q}[x_1, \ldots, x_t]$

$$\mathrm{Eq}_{g,q} := \mathrm{P}_q(x_1, \ldots, x_t) - \binom{g}{q}.$$

Theorem

Let $g = u_1 v_1^{\gamma_1} u_2 \cdots u_t v_t^{\gamma_t} u_{t+1}$ from a polynomial regular language. For all $q \in \Sigma^+$, the t-uple $(\gamma_1, \ldots, \gamma_t)$ of non-negative integers is a solution of the equation $\mathrm{Eq}_{g,q} = 0$.

Equations

Definition

Let $q \in \Sigma^+$ and g from a polynomial regular language. Consider the polynomial in $\mathbb{Q}[x_1, \ldots, x_t]$

$$\mathrm{Eq}_{g,q} := \mathrm{P}_q(x_1, \ldots, x_t) - \binom{g}{q}.$$

Theorem

Let $g = u_1 v_1^{\gamma_1} u_2 \cdots u_t v_t^{\gamma_t} u_{t+1}$ from a polynomial regular language. For all $q \in \Sigma^+$, the t-uple $(\gamma_1, \ldots, \gamma_t)$ of non-negative integers is a solution of the equation $\mathrm{Eq}_{g,q} = 0$.

➔ Problem reduces:

Equations

Definition

Let $q \in \Sigma^+$ and g from a polynomial regular language. Consider the polynomial in $\mathbb{Q}[x_1, \ldots, x_t]$

$$\mathrm{Eq}_{g,q} := \mathrm{P}_q(x_1, \ldots, x_t) - \binom{g}{q}.$$

Theorem

Let $g = u_1 v_1^{\gamma_1} u_2 \cdots u_t v_t^{\gamma_t} u_{t+1}$ from a polynomial regular language. For all $q \in \Sigma^+$, the t-uple $(\gamma_1, \ldots, \gamma_t)$ of non-negative integers is a solution of the equation $\mathrm{Eq}_{g,q} = 0$.

➜ Problem reduces: finding a **set of queries**

Equations

Definition

Let $q \in \Sigma^+$ and g from a polynomial regular language. Consider the polynomial in $\mathbb{Q}[x_1, \dots, x_t]$

$$\mathrm{Eq}_{g,q} := \mathrm{P}_q(x_1, \dots, x_t) - \binom{g}{q}.$$

Theorem

Let $g = u_1 v_1^{\gamma_1} u_2 \cdots u_t v_t^{\gamma_t} u_{t+1}$ from a polynomial regular language. For all $q \in \Sigma^+$, the t-uple $(\gamma_1, \dots, \gamma_t)$ of non-negative integers is a solution of the equation $\mathrm{Eq}_{g,q} = 0$.

➔ Problem reduces: finding a **set of queries** such that **system of equations** has **unique integer solution !**

Example

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2}$$

Example

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \begin{pmatrix} g \\ 0 \end{pmatrix}$$

Example

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{0} \gg 21$$

Example

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{0} \gg 21$$

$$\binom{g}{0}$$

Example

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{0} \gg 21$$

$$\binom{g}{0} = \binom{u_1}{0}$$

Example

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{0} \gg 21$$

$$\binom{g}{0} = \binom{u_1}{0} + \binom{v_1}{0}x$$

Example

$$L = \underbrace{0}_{u_1}\ \underbrace{(10010)^*}_{v_1}\ \underbrace{010}_{u_2}\ \underbrace{(010)^*}_{v_2} \qquad \binom{g}{0} \gg 21$$

$$\binom{g}{0} = \binom{u_1}{0} + \binom{v_1}{0}x + \binom{u_2}{0}$$

Example

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{0} \gg 21$$

$$\binom{g}{0} = \binom{u_1}{0} + \binom{v_1}{0}x + \binom{u_2}{0} + \binom{v_2}{0}y$$

Example

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{0} \gg 21$$

$$\binom{g}{0} = \binom{u_1}{0} + \binom{v_1}{0}x + \binom{u_2}{0} + \binom{v_2}{0}y$$

$$=1$$

Example

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{0} \gg 21$$

$$\binom{g}{0} = \binom{u_1}{0} + \binom{v_1}{0}x + \binom{u_2}{0} + \binom{v_2}{0}y$$
$$= 1 + 3x$$

Example

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \begin{pmatrix} g \\ 0 \end{pmatrix} \gg \; 21$$

$$\begin{pmatrix} g \\ 0 \end{pmatrix} = \begin{pmatrix} u_1 \\ 0 \end{pmatrix} + \begin{pmatrix} v_1 \\ 0 \end{pmatrix} x + \begin{pmatrix} u_2 \\ 0 \end{pmatrix} + \begin{pmatrix} v_2 \\ 0 \end{pmatrix} y$$

$$= 1 + 3x + 2$$

Example

$$L = \underbrace{0}_{u_1}\ \underbrace{(10010)^*}_{v_1}\ \underbrace{010}_{u_2}\ \underbrace{(010)^*}_{v_2} \qquad \binom{g}{0} \gg 21$$

$$\begin{aligned}\binom{g}{0} &= \binom{u_1}{0} + \binom{v_1}{0}x + \binom{u_2}{0} + \binom{v_2}{0}y \\ &= 1 + 3x + 2 + 2y\end{aligned}$$

Example

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{0} \gg 21$$

$$\begin{aligned}\binom{g}{0} &= \binom{u_1}{0} + \binom{v_1}{0}x + \binom{u_2}{0} + \binom{v_2}{0}y \\ &= 1 + 3x + 2 + 2y \\ &= 3x\end{aligned}$$

Example

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{0} \gg 21$$

$$\begin{aligned}\binom{g}{0} &= \binom{u_1}{0} + \binom{v_1}{0}x + \binom{u_2}{0} + \binom{v_2}{0}y \\ &= 1 + 3x + 2 + 2y \\ &= 3x + 2y\end{aligned}$$

Example

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{0} \gg 21$$

$$\begin{aligned}\binom{g}{0} &= \binom{u_1}{0} + \binom{v_1}{0}x + \binom{u_2}{0} + \binom{v_2}{0}y \\ &= 1 + 3x + 2 + 2y \\ &= 3x + 2y + 3\end{aligned}$$

Example

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{0} \gg 21$$

$$\begin{aligned}\binom{g}{0} &= \binom{u_1}{0} + \binom{v_1}{0}x + \binom{u_2}{0} + \binom{v_2}{0}y \\ &= 1 + 3x + 2 + 2y \\ &= 3x + 2y + 3\end{aligned}$$

$$\mathrm{Eq}_{g,0} = 3x + 2y + 3 - 21$$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{10}$$

$$=$$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2}$$

$$\binom{g}{10} \gg 132$$

$=$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2}$$

$$\binom{g}{10} \gg 132$$

$$\binom{g}{10}$$

$$=$$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2}$$

$$\binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\qquad\qquad\qquad\qquad}_{\text{both letters from the same factor}}$$

$$\underbrace{\qquad\qquad\qquad\qquad}$$

$$= \underbrace{\qquad\qquad}\quad\underbrace{\qquad\qquad}$$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2}$$

$$\binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10}\qquad\qquad\qquad\qquad\qquad\qquad}_{\text{both letters from the same factor}}$$

$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad}$$

$$= \underbrace{\qquad\qquad\qquad\qquad}\quad\underbrace{\qquad\qquad\qquad}$$

Example

continued

$$L = \underbrace{0}_{u_1}\ \underbrace{(10010)^*}_{v_1}\ \underbrace{010}_{u_2}\ \underbrace{(010)^*}_{v_2} \qquad \binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x \qquad\qquad\qquad\qquad\qquad\qquad}_{\text{both letters from the same factor}}$$

$$=$$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x + \binom{v_1}{1}\binom{v_1}{0}\binom{x}{2}}_{\text{both letters from the same factor}}$$

$$=$$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x + \binom{v_1}{1}\binom{v_1}{0}\binom{x}{2} + \binom{u_2}{10}}_{\text{both letters from the same factor}}$$

$$=$$

Example

continued

$$L = \underbrace{0}_{u_1}\ \underbrace{(10010)^*}_{v_1}\ \underbrace{010}_{u_2}\ \underbrace{(010)^*}_{v_2} \qquad \binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x + \binom{v_1}{1}\binom{v_1}{0}\binom{x}{2} + \binom{u_2}{10} + \binom{v_2}{10}y}_{\text{both letters from the same factor}}$$

$$=$$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x + \binom{v_1}{1}\binom{v_1}{0}\binom{x}{2} + \binom{u_2}{10} + \binom{v_2}{10}y + \binom{v_2}{1}\binom{v_2}{0}\binom{y}{2}}_{\text{both letters from the same factor}}$$

$$=$$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2}$$

$$\binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x + \binom{v_1}{1}\binom{v_1}{0}\binom{x}{2} + \binom{u_2}{10} + \binom{v_2}{10}y + \binom{v_2}{1}\binom{v_2}{0}\binom{y}{2}}_{\text{both letters from the same factor}}$$

$$+ \underbrace{\qquad\qquad}_{\text{letters from different factors}}$$

$$= \underbrace{\qquad\qquad}\quad \underbrace{\qquad\qquad}$$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x + \binom{v_1}{1}\binom{v_1}{0}\binom{x}{2} + \binom{u_2}{10} + \binom{v_2}{10}y + \binom{v_2}{1}\binom{v_2}{0}\binom{y}{2}}_{\text{both letters from the same factor}}$$

$$+ \underbrace{\binom{u_1}{1}\binom{v_1}{0}x \qquad\qquad\qquad\qquad\qquad\qquad}_{\text{letters from different factors}}$$

$$=$$

Example

continued

$$L = \underbrace{0}_{u_1}\ \underbrace{(10010)^*}_{v_1}\ \underbrace{010}_{u_2}\ \underbrace{(010)^*}_{v_2} \qquad \binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x + \binom{v_1}{1}\binom{v_1}{0}\binom{x}{2} + \binom{u_2}{10} + \binom{v_2}{10}y + \binom{v_2}{1}\binom{v_2}{0}\binom{y}{2}}_{\text{both letters from the same factor}}$$

$$+ \underbrace{\binom{u_1}{1}\binom{v_1}{0}x + \binom{v_1}{1}\binom{u_2}{0}x}_{\text{letters from different factors}}$$

$$=$$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2}$$

$$\binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x + \binom{v_1}{1}\binom{v_1}{0}\binom{x}{2} + \binom{u_2}{10} + \binom{v_2}{10}y + \binom{v_2}{1}\binom{v_2}{0}\binom{y}{2}}_{\text{both letters from the same factor}}$$

$$+ \underbrace{\binom{u_1}{1}\binom{v_1}{0}x + \binom{v_1}{1}\binom{u_2}{0}x + \binom{v_1}{1}\binom{v_2}{0}xy}_{\text{letters from different factors}}$$

$$=$$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x + \binom{v_1}{1}\binom{v_1}{0}\binom{x}{2} + \binom{u_2}{10} + \binom{v_2}{10}y + \binom{v_2}{1}\binom{v_2}{0}\binom{y}{2}}_{\text{both letters from the same factor}}$$

$$+ \underbrace{\binom{u_1}{1}\binom{v_1}{0}x + \binom{v_1}{1}\binom{u_2}{0}x + \binom{v_1}{1}\binom{v_2}{0}xy + \binom{u_2}{1}\binom{v_2}{0}y}_{\text{letters from different factors}}$$

$$=$$

Example

continued

$$L = \underbrace{0}_{u_1}\,\underbrace{(10010)^*}_{v_1}\,\underbrace{010}_{u_2}\,\underbrace{(010)^*}_{v_2} \qquad \binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x + \binom{v_1}{1}\binom{v_1}{0}\binom{x}{2} + \binom{u_2}{10} + \binom{v_2}{10}y + \binom{v_2}{1}\binom{v_2}{0}\binom{y}{2}}_{\text{both letters from the same factor}}$$

$$+ \underbrace{\binom{u_1}{1}\binom{v_1}{0}x + \binom{v_1}{1}\binom{u_2}{0}x + \binom{v_1}{1}\binom{v_2}{0}xy + \binom{u_2}{1}\binom{v_2}{0}y}_{\text{letters from different factors}}$$

$$= 0$$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x + \binom{v_1}{1}\binom{v_1}{0}\binom{x}{2} + \binom{u_2}{10} + \binom{v_2}{10}y + \binom{v_2}{1}\binom{v_2}{0}\binom{y}{2}}_{\text{both letters from the same factor}}$$

$$+ \underbrace{\binom{u_1}{1}\binom{v_1}{0}x + \binom{v_1}{1}\binom{u_2}{0}x + \binom{v_1}{1}\binom{v_2}{0}xy + \binom{u_2}{1}\binom{v_2}{0}y}_{\text{letters from different factors}}$$

$$= 0 + 4x$$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x + \binom{v_1}{1}\binom{v_1}{0}\binom{x}{2} + \binom{u_2}{10} + \binom{v_2}{10}y + \binom{v_2}{1}\binom{v_2}{0}\binom{y}{2}}_{\text{both letters from the same factor}}$$

$$+ \underbrace{\binom{u_1}{1}\binom{v_1}{0}x + \binom{v_1}{1}\binom{u_2}{0}x + \binom{v_1}{1}\binom{v_2}{0}xy + \binom{u_2}{1}\binom{v_2}{0}y}_{\text{letters from different factors}}$$

$$= \underbrace{0 + 4x + 2 \cdot 3\frac{x^2 - x}{2}}_{}$$

Example

continued

$$L = \underbrace{0}_{u_1}\ \underbrace{(10010)^*}_{v_1}\ \underbrace{010}_{u_2}\ \underbrace{(010)^*}_{v_2} \qquad \binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x + \binom{v_1}{1}\binom{v_1}{0}\binom{x}{2} + \binom{u_2}{10} + \binom{v_2}{10}y + \binom{v_2}{1}\binom{v_2}{0}\binom{y}{2}}_{\text{both letters from the same factor}}$$

$$+ \underbrace{\binom{u_1}{1}\binom{v_1}{0}x + \binom{v_1}{1}\binom{u_2}{0}x + \binom{v_1}{1}\binom{v_2}{0}xy + \binom{u_2}{1}\binom{v_2}{0}y}_{\text{letters from different factors}}$$

$$= \underbrace{0 + 4x + 2 \cdot 3\frac{x^2 - x}{2} + 1}$$

Example

continued

$$L = \underbrace{0}_{u_1}\ \underbrace{(10010)^*}_{v_1}\ \underbrace{010}_{u_2}\ \underbrace{(010)^*}_{v_2} \qquad \binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x + \binom{v_1}{1}\binom{v_1}{0}\binom{x}{2} + \binom{u_2}{10} + \binom{v_2}{10}y + \binom{v_2}{1}\binom{v_2}{0}\binom{y}{2}}_{\text{both letters from the same factor}}$$

$$+ \underbrace{\binom{u_1}{1}\binom{v_1}{0}x + \binom{v_1}{1}\binom{u_2}{0}x + \binom{v_1}{1}\binom{v_2}{0}xy + \binom{u_2}{1}\binom{v_2}{0}y}_{\text{letters from different factors}}$$

$$= \underbrace{0 + 4x + 2 \cdot 3\frac{x^2 - x}{2} + 1 + y}$$

Example

continued

$$L = \underbrace{0}_{u_1}\ \underbrace{(10010)^*}_{v_1}\ \underbrace{010}_{u_2}\ \underbrace{(010)^*}_{v_2} \qquad \binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x + \binom{v_1}{1}\binom{v_1}{0}\binom{x}{2} + \binom{u_2}{10} + \binom{v_2}{10}y + \binom{v_2}{1}\binom{v_2}{0}\binom{y}{2}}_{\text{both letters from the same factor}}$$

$$+ \underbrace{\binom{u_1}{1}\binom{v_1}{0}x + \binom{v_1}{1}\binom{u_2}{0}x + \binom{v_1}{1}\binom{v_2}{0}xy + \binom{u_2}{1}\binom{v_2}{0}y}_{\text{letters from different factors}}$$

$$= \underbrace{0 + 4x + 2\cdot 3\frac{x^2 - x}{2} + 1 + y + 1\cdot 2\frac{y^2 - y}{2}}$$

Example

continued

$$L = \underbrace{0}_{u_1}\ \underbrace{(10010)^*}_{v_1}\ \underbrace{010}_{u_2}\ \underbrace{(010)^*}_{v_2} \qquad \binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x + \binom{v_1}{1}\binom{v_1}{0}\binom{x}{2} + \binom{u_2}{10} + \binom{v_2}{10}y + \binom{v_2}{1}\binom{v_2}{0}\binom{y}{2}}_{\text{both letters from the same factor}}$$

$$+ \underbrace{\binom{u_1}{1}\binom{v_1}{0}x + \binom{v_1}{1}\binom{u_2}{0}x + \binom{v_1}{1}\binom{v_2}{0}xy + \binom{u_2}{1}\binom{v_2}{0}y}_{\text{letters from different factors}}$$

$$= \underbrace{0 + 4x + 2\cdot 3\frac{x^2-x}{2} + 1 + y + 1\cdot 2\frac{y^2-y}{2}} + \underbrace{\qquad\qquad\qquad}$$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x + \binom{v_1}{1}\binom{v_1}{0}\binom{x}{2} + \binom{u_2}{10} + \binom{v_2}{10}y + \binom{v_2}{1}\binom{v_2}{0}\binom{y}{2}}_{\text{both letters from the same factor}}$$

$$+ \underbrace{\binom{u_1}{1}\binom{v_1}{0}x + \binom{v_1}{1}\binom{u_2}{0}x + \binom{v_1}{1}\binom{v_2}{0}xy + \binom{u_2}{1}\binom{v_2}{0}y}_{\text{letters from different factors}}$$

$$= \underbrace{0 + 4x + 2\cdot 3\frac{x^2 - x}{2} + 1 + y + 1\cdot 2\frac{y^2 - y}{2}} + \underbrace{0 \qquad\qquad}$$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x + \binom{v_1}{1}\binom{v_1}{0}\binom{x}{2} + \binom{u_2}{10} + \binom{v_2}{10}y + \binom{v_2}{1}\binom{v_2}{0}\binom{y}{2}}_{\text{both letters from the same factor}}$$

$$+ \underbrace{\binom{u_1}{1}\binom{v_1}{0}x + \binom{v_1}{1}\binom{u_2}{0}x + \binom{v_1}{1}\binom{v_2}{0}xy + \binom{u_2}{1}\binom{v_2}{0}y}_{\text{letters from different factors}}$$

$$= \underbrace{0 + 4x + 2 \cdot 3\frac{x^2 - x}{2} + 1 + y + 1 \cdot 2\frac{y^2 - y}{2}}_{} + \underbrace{0 + 2 \cdot 2x \qquad\qquad}_{}$$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x + \binom{v_1}{1}\binom{v_1}{0}\binom{x}{2} + \binom{u_2}{10} + \binom{v_2}{10}y + \binom{v_2}{1}\binom{v_2}{0}\binom{y}{2}}_{\text{both letters from the same factor}}$$

$$+ \underbrace{\binom{u_1}{1}\binom{v_1}{0}x + \binom{v_1}{1}\binom{u_2}{0}x + \binom{v_1}{1}\binom{v_2}{0}xy + \binom{u_2}{1}\binom{v_2}{0}y}_{\text{letters from different factors}}$$

$$= \underbrace{0 + 4x + 2 \cdot 3\frac{x^2 - x}{2} + 1 + y + 1 \cdot 2\frac{y^2 - y}{2}}_{} + \underbrace{0 + 2 \cdot 2x + 2 \cdot 2xy}_{}$$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2} \qquad \binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x + \binom{v_1}{1}\binom{v_1}{0}\binom{x}{2} + \binom{u_2}{10} + \binom{v_2}{10}y + \binom{v_2}{1}\binom{v_2}{0}\binom{y}{2}}_{\text{both letters from the same factor}}$$

$$+ \underbrace{\binom{u_1}{1}\binom{v_1}{0}x + \binom{v_1}{1}\binom{u_2}{0}x + \binom{v_1}{1}\binom{v_2}{0}xy + \binom{u_2}{1}\binom{v_2}{0}y}_{\text{letters from different factors}}$$

$$= \underbrace{0 + 4x + 2 \cdot 3\frac{x^2 - x}{2} + 1 + y + 1 \cdot 2\frac{y^2 - y}{2}} + \underbrace{0 + 2 \cdot 2x + 2 \cdot 2xy + 1 \cdot 2y}$$

Example

continued

$$L = \underbrace{0}_{u_1}\ \underbrace{(10010)^*}_{v_1}\ \underbrace{010}_{u_2}\ \underbrace{(010)^*}_{v_2} \qquad \binom{g}{10} \gg 132$$

$$\binom{g}{10} = \underbrace{\binom{u_1}{10} + \binom{v_1}{10}x + \binom{v_1}{1}\binom{v_1}{0}\binom{x}{2} + \binom{u_2}{10} + \binom{v_2}{10}y + \binom{v_2}{1}\binom{v_2}{0}\binom{y}{2}}_{\text{both letters from the same factor}}$$

$$+ \underbrace{\binom{u_1}{1}\binom{v_1}{0}x + \binom{v_1}{1}\binom{u_2}{0}x + \binom{v_1}{1}\binom{v_2}{0}xy + \binom{u_2}{1}\binom{v_2}{0}y}_{\text{letters from different factors}}$$

$$= \underbrace{0 + 4x + 2\cdot 3\frac{x^2-x}{2} + 1 + y + 1\cdot 2\frac{y^2-y}{2}} + \underbrace{0 + 2\cdot 2x + 2\cdot 2xy + 1\cdot 2y}$$

$$= 3x^2 + 4xy + 5x + y^2 + 2y + 1$$

Example

continued

$$L = \underbrace{0}_{u_1} \underbrace{(10010)^*}_{v_1} \underbrace{010}_{u_2} \underbrace{(010)^*}_{v_2}$$

q	$\mathrm{P}_q(x, y)$	$\binom{g}{q}$

Example

continued

$$L = \underbrace{0}_{u_1}\ \underbrace{(10010)^*}_{v_1}\ \underbrace{010}_{u_2}\ \underbrace{(010)^*}_{v_2}$$

q	$\mathrm{P}_q(x,y)$	$\binom{g}{q}$
0	$3x+2y+3$	21

Example

continued

$$L = \underbrace{0}_{u_1}\ \underbrace{(10010)^*}_{v_1}\ \underbrace{010}_{u_2}\ \underbrace{(010)^*}_{v_2}$$

q	$P_q(x,y)$	$\binom{g}{q}$
0	$3x + 2y + 3$	21
10	$3x^2 + 4xy + 5x + y^2 + 2y + 1$	132

Example

continued

$$L = \underbrace{0}_{u_1}\ \underbrace{(10010)^*}_{v_1}\ \underbrace{010}_{u_2}\ \underbrace{(010)^*}_{v_2}$$

q	$\mathrm{P}_q(x,y)$	$\binom{g}{q}$
0	$3x + 2y + 3$	21
10	$3x^2 + 4xy + 5x + y^2 + 2y + 1$	132
011	$2x^3 + 3x^2y + \frac{5x^2}{2} + \frac{3xy^2}{2} + \frac{5xy}{2} + \frac{x}{2} + \frac{y^3}{3} + y^2 + \frac{2y}{3}$	418

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2}$$

$$\begin{cases} \mathrm{Eq}_{g,0} & : & 3x + 2y - 18 & = & 0 \\ \mathrm{Eq}_{g,10} & : & 3x^2 + 4xy + 5x + y^2 + 2y - 131 & = & 0 \end{cases}$$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2}$$

$$\begin{cases} \mathrm{Eq}_{g,0} & : & 3x + 2y - 18 & = & 0 \\ \mathrm{Eq}_{g,10} & : & 3x^2 + 4xy + 5x + y^2 + 2y - 131 & = & 0 \end{cases}$$

➔ two solutions $(x, y) = (4, 3)$ or $(32/7, -7)$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2}$$

$$\begin{cases} \mathrm{Eq}_{g,0} & : & 3x + 2y - 18 & = & 0 \\ \mathrm{Eq}_{g,10} & : & 3x^2 + 4xy + 5x + y^2 + 2y - 131 & = & 0 \end{cases}$$

➔ two solutions $(x, y) = (4, 3)$ or $(32/7, -7)$

✚ $\mathrm{P}_{011}(x, y)$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2}$$

$$\begin{cases} \mathrm{Eq}_{g,0} & : & 3x + 2y - 18 & = & 0 \\ \mathrm{Eq}_{g,10} & : & 3x^2 + 4xy + 5x + y^2 + 2y - 131 & = & 0 \end{cases}$$

➔ two solutions $(x, y) = (4, 3)$ or $(32/7, -7)$

✚ $\mathrm{P}_{011}(x, y)$ ➔ unique solution

Example

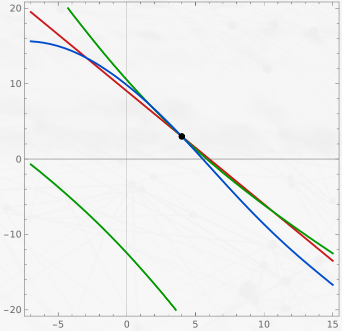
continued

$$L = \underbrace{0}_{u_1}\ \underbrace{(10010)^*}_{v_1}\ \underbrace{010}_{u_2}\ \underbrace{(010)^*}_{v_2}$$

$$\begin{cases} \mathrm{Eq}_{g,0} : & 3x + 2y - 18 = 0 \\ \mathrm{Eq}_{g,10} : & 3x^2 + 4xy + 5x + y^2 + 2y - 131 = 0 \end{cases}$$

➔ two solutions $(x, y) = (4, 3)$ or $(32/7, -7)$

✚ $\mathrm{P}_{011}(x, y)$ ➔ unique solution



Example

continued

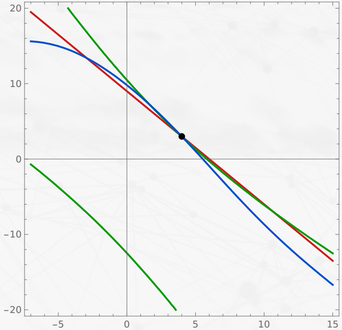
$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_2}$$

$$\begin{cases} \mathrm{Eq}_{g,0} : & 3x + 2y - 18 = 0 \\ \mathrm{Eq}_{g,10} : & 3x^2 + 4xy + 5x + y^2 + 2y - 131 = 0 \end{cases}$$

→ two solutions $(x, y) = (4, 3)$ or $(32/7, -7)$

+ $\mathrm{P}_{011}(x, y)$ → unique solution

$g = 0(10010)^4 010(010)^3$



Two Loops

Introduction

Basics & Initial Results

Polynomials

for Reconstruction

Nice Case

Two Loops

General Case

and its problems

Setting

Lan-
guage

Setting

Lan-
guage

$L = u_1 v_1^* u_2 v_2^* u_3$ with $v_1, v_2 \in \Sigma^+$

Setting

Lan-
guage

$L = u_1 v_1^* u_2 v_2^* u_3$ with $v_1, v_2 \in \Sigma^+$

Guess

Setting

Lan-
guage

$L = u_1 v_1^* u_2 v_2^* u_3$ with $v_1, v_2 \in \Sigma^+$

Guess

$g = u_1 v_1^x u_2 v_2^y u_3$

Setting

Lan-
guage

$L = u_1 v_1^* u_2 v_2^* u_3$ with $v_1, v_2 \in \Sigma^+$

Guess

$g = u_1 v_1^x u_2 v_2^y u_3$

Equa-
tion

Setting

Lan-guage

$$L = u_1 v_1^* u_2 v_2^* u_3 \text{ with } v_1, v_2 \in \Sigma^+$$

Guess

$$g = u_1 v_1^x u_2 v_2^y u_3$$

Equa-tion

$$\binom{g}{q} = \sum_{\substack{q = e_1 f_1 e_2 \cdots e_t f_t e_{t+1} \\ e_i, f_i \in \Sigma^*}} \left(\prod_{j=1}^{3} \binom{u_j}{e_j} \right) B_{v_1, f_1}(x) B_{v_2, f_2}(y)$$

Setting

Language

$$L = u_1 v_1^* u_2 v_2^* u_3 \text{ with } v_1, v_2 \in \Sigma^+$$

Guess

$$g = u_1 v_1^x u_2 v_2^y u_3$$

Equation

$$\binom{g}{q} = \sum_{\substack{q=e_1 f_1 e_2 \cdots e_t f_t e_{t+1} \\ e_i, f_i \in \Sigma^*}} \left(\prod_{j=1}^{3} \binom{u_j}{e_j} \right) B_{v_1, f_1}(x) B_{v_2, f_2}(y)$$

for letters

Setting

Lan-guage

$$L = u_1 v_1^* u_2 v_2^* u_3 \text{ with } v_1, v_2 \in \Sigma^+$$

Guess

$$g = u_1 v_1^x u_2 v_2^y u_3$$

Equa-tion

$$\binom{g}{q} = \sum_{\substack{q = e_1 f_1 e_2 \cdots e_t f_t e_{t+1} \\ e_i, f_i \in \Sigma^*}} \left(\prod_{j=1}^{3} \binom{u_j}{e_j} \right) B_{v_1, f_1}(x) B_{v_2, f_2}(y)$$

for letters

$$\binom{g}{a} = |v_1|_a x + |v_2|_a y + |u_1 u_2 u_3|_a$$

Setting

Language

$$L = u_1 v_1^* u_2 v_2^* u_3 \text{ with } v_1, v_2 \in \Sigma^+$$

Guess

$$g = u_1 v_1^x u_2 v_2^y u_3$$

Equation

$$\binom{g}{q} = \sum_{\substack{q = e_1 f_1 e_2 \cdots e_t f_t e_{t+1} \\ e_i, f_i \in \Sigma^*}} \left(\prod_{j=1}^{3} \binom{u_j}{e_j} \right) B_{v_1, f_1}(x) B_{v_2, f_2}(y)$$

for letters

$$\binom{g}{a} = |v_1|_a x + |v_2|_a y + |u_1 u_2 u_3|_a$$

Linearly Independent

Lemma

Let $L = u_1 v_1^* u_2 v_2^* u_3$ *be a language where* $v_1, v_2 \in \Sigma^+$ *and* $u_1, u_2, u_3 \in \Sigma^*$ *are given.*

Linearly Independent

Lemma

Let $L = u_1 v_1^* u_2 v_2^* u_3$ *be a language where* $v_1, v_2 \in \Sigma^+$ *and* $u_1, u_2, u_3 \in \Sigma^*$ *are given.*

$\Psi(v_1), \Psi(v_2)$ *linearly independent over* $\mathbb{Q}$

Linearly Independent

Lemma

Let $L = u_1 v_1^* u_2 v_2^* u_3$ *be a language where* $v_1, v_2 \in \Sigma^+$ *and* $u_1, u_2, u_3 \in \Sigma^*$ *are given.*

$\Psi(v_1), \Psi(v_2)$ *linearly independent over* $\mathbb{Q}$ $\implies$

Linearly Independent

Lemma

Let $L = u_1 v_1^* u_2 v_2^* u_3$ *be a language where* $v_1, v_2 \in \Sigma^+$ *and* $u_1, u_2, u_3 \in \Sigma^*$ *are given.*

$\Psi(v_1), \Psi(v_2)$ *linearly independent over* $\mathbb{Q}$ $\Longrightarrow$ *a word in* L *(of unknown length) uniquely reconstructable with two queries (of length 1)*

Linearly Independent

Lemma

Let $L = u_1 v_1^* u_2 v_2^* u_3$ *be a language where* $v_1, v_2 \in \Sigma^+$ *and* $u_1, u_2, u_3 \in \Sigma^*$ *are given.*

$\Psi(v_1), \Psi(v_2)$ *linearly independent over* $\mathbb{Q}$ $\Longrightarrow$ *a word in* L *(of unknown length) uniquely reconstructable with two queries (of length* 1*)*

Sketch of a Proof.

$\square$

Linearly Independent

Lemma

Let $L = u_1 v_1^* u_2 v_2^* u_3$ *be a language where* $v_1, v_2 \in \Sigma^+$ *and* $u_1, u_2, u_3 \in \Sigma^*$ *are given.*

$\Psi(v_1), \Psi(v_2)$ *linearly independent over* $\mathbb{Q}$ $\Longrightarrow$ *a word in* L *(of unknown length) uniquely reconstructable with two queries (of length 1)*

Sketch of a Proof.

$$\binom{g}{a} = |v_1|_a x + |v_2|_a y + |u_1 u_2 u_3|_a$$

□

Linearly Independent

Lemma

Let $L = u_1 v_1^* u_2 v_2^* u_3$ *be a language where* $v_1, v_2 \in \Sigma^+$ *and* $u_1, u_2, u_3 \in \Sigma^*$ *are given.*

$\Psi(v_1), \Psi(v_2)$ linearly independent over $\mathbb{Q}$ $\Longrightarrow$ *a word in L (of unknown length) uniquely reconstructable with two queries (of length 1)*

Sketch of a Proof.

$$\binom{g}{a} = |v_1|_a x + |v_2|_a y + |u_1 u_2 u_3|_a \text{ and } \binom{g}{b} = |v_1|_b x + |v_2|_b y + |u_1 u_2 u_3|_b$$

$\square$

Linearly Independent

Lemma

Let $L = u_1 v_1^* u_2 v_2^* u_3$ *be a language where* $v_1, v_2 \in \Sigma^+$ *and* $u_1, u_2, u_3 \in \Sigma^*$ *are given.*

$\Psi(v_1), \Psi(v_2)$ *linearly independent over* $\mathbb{Q}$	$\Longrightarrow$	*a word in* L *(of unknown length) uniquely reconstructable with two queries (of length 1)*

Sketch of a Proof.

$\binom{g}{a} = |v_1|_a x + |v_2|_a y + |u_1 u_2 u_3|_a$ and $\binom{g}{b} = |v_1|_b x + |v_2|_b y + |u_1 u_2 u_3|_b$ are linear equations with one point of intersection $\square$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_1} \qquad g = 0(10010)^4010(010)^3 \qquad (\gamma_1, \gamma_2) = (4, 3)$$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_1} \qquad g = 0(10010)^4010(010)^3 \qquad (\gamma_1, \gamma_2) = (4, 3)$$

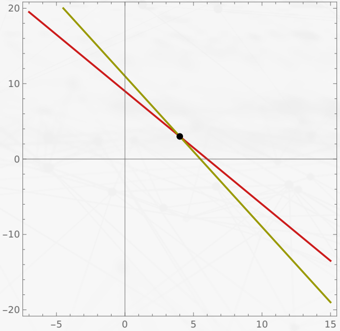
$$\begin{cases} \mathrm{Eq}_{g,0} & : & 3x + 2y - 18 & = & 0 \\ \mathrm{Eq}_{g,1} & : & 2x + y - 11 & = & 0 \end{cases}$$

Example

continued

$$L = \underbrace{0}_{u_1}\underbrace{(10010)^*}_{v_1}\underbrace{010}_{u_2}\underbrace{(010)^*}_{v_1} \qquad g = 0(10010)^4 010(010)^3 \qquad (\gamma_1, \gamma_2) = (4,3)$$

$$\begin{cases} \mathrm{Eq}_{g,0} & : & 3x + 2y - 18 & = & 0 \\ \mathrm{Eq}_{g,1} & : & 2x + y - 11 & = & 0 \end{cases}$$



Linearly Dependent

$$\alpha\Psi(v_1) = \beta\Psi(v_2)$$

Linearly Dependent

$$\alpha\Psi(v_1) = \beta\Psi(v_2)$$

⚠ $\mathrm{Eq}_{g,a}(x,y) = 0$ and $\mathrm{Eq}_{g,b}(x,y) = 0$ are equivalent

Linearly Dependent

$$\alpha\Psi(v_1) = \beta\Psi(v_2)$$

⚠ $\mathrm{Eq}_{g,a}(x,y) = 0$ and $\mathrm{Eq}_{g,b}(x,y) = 0$ are equivalent → query $\binom{g}{a}$ and $\binom{g}{ab}$

Linearly Dependent

$$\alpha\Psi(v_1) = \beta\Psi(v_2)$$

⚠ $\mathrm{Eq}_{g,a}(x,y) = 0$ and $\mathrm{Eq}_{g,b}(x,y) = 0$ are equivalent ➔ query $\binom{g}{a}$ and $\binom{g}{ab}$

Lemma

Let $L = u_1 v_1^* u_2 v_2^* u_3$ be a language where $v_1, v_2 \in \Sigma^+$ and $u_1, u_2, u_3 \in \Sigma^*$ are given

Linearly Dependent

$\alpha\Psi(v_1) = \beta\Psi(v_2)$

⚠ $\mathrm{Eq}_{g,a}(x,y) = 0$ and $\mathrm{Eq}_{g,b}(x,y) = 0$ are equivalent ➜ query $\binom{g}{a}$ and $\binom{g}{ab}$

Lemma

Let $L = u_1 v_1^* u_2 v_2^* u_3$ be a language where $v_1, v_2 \in \Sigma^+$ and $u_1, u_2, u_3 \in \Sigma^*$ are given and $v_1^\alpha \sim_1 v_2^\beta$ for some coprime integers $\alpha, \beta \geqslant 1$.

Linearly Dependent

$$\alpha\Psi(v_1) = \beta\Psi(v_2)$$

⚠ $\mathrm{Eq}_{g,a}(x,y) = 0$ and $\mathrm{Eq}_{g,b}(x,y) = 0$ are equivalent ➔ query $\binom{g}{a}$ and $\binom{g}{ab}$

Lemma

Let $L = u_1 v_1^* u_2 v_2^* u_3$ be a language where $v_1, v_2 \in \Sigma^+$ and $u_1, u_2, u_3 \in \Sigma^*$ are given and $v_1^\alpha \sim_1 v_2^\beta$ for some coprime integers $\alpha, \beta \geqslant 1$. If there exist $a, b \in \Sigma$ such that the quantity

Linearly Dependent

$\alpha\Psi(v_1) = \beta\Psi(v_2)$

⚠ $\mathrm{Eq}_{g,a}(x,y) = 0$ and $\mathrm{Eq}_{g,b}(x,y) = 0$ are equivalent ➔ query $\binom{g}{a}$ and $\binom{g}{ab}$

Lemma

Let $L = u_1 v_1^* u_2 v_2^* u_3$ be a language where $v_1, v_2 \in \Sigma^+$ and $u_1, u_2, u_3 \in \Sigma^*$ are given and $v_1^\alpha \sim_1 v_2^\beta$ for some coprime integers $\alpha, \beta \geqslant 1$. If there exist $a, b \in \Sigma$ such that the quantity

$$|v_1^\alpha|_b |u_2|_a - |v_1^\alpha|_a |u_2|_b + \binom{v_2^\beta}{ab} - \binom{v_1^\alpha}{ab}$$

is non-zero

Linearly Dependent

$\alpha\Psi(v_1) = \beta\Psi(v_2)$

⚠ $\mathrm{Eq}_{g,a}(x,y) = 0$ and $\mathrm{Eq}_{g,b}(x,y) = 0$ are equivalent ➔ query $\binom{g}{a}$ and $\binom{g}{ab}$

Lemma

Let $L = u_1 v_1^* u_2 v_2^* u_3$ be a language where $v_1, v_2 \in \Sigma^+$ and $u_1, u_2, u_3 \in \Sigma^*$ are given and $v_1^\alpha \sim_1 v_2^\beta$ for some coprime integers $\alpha, \beta \geqslant 1$. If there exist $a, b \in \Sigma$ such that the quantity

$$|v_1^\alpha|_b |u_2|_a - |v_1^\alpha|_a |u_2|_b + \binom{v_2^\beta}{ab} - \binom{v_1^\alpha}{ab}$$

is non-zero , then a word in L (of unknown length) can be uniquely reconstructed

Linearly Dependent

$$\alpha\Psi(v_1) = \beta\Psi(v_2)$$

⚠ $\mathrm{Eq}_{g,a}(x,y) = 0$ and $\mathrm{Eq}_{g,b}(x,y) = 0$ are equivalent ➔ query $\binom{g}{a}$ and $\binom{g}{ab}$

Lemma

Let $L = u_1 v_1^* u_2 v_2^* u_3$ be a language where $v_1, v_2 \in \Sigma^+$ and $u_1, u_2, u_3 \in \Sigma^*$ are given and $v_1^\alpha \sim_1 v_2^\beta$ for some coprime integers $\alpha, \beta \geqslant 1$. If there exist $a, b \in \Sigma$ such that the quantity

$$|v_1^\alpha|_b |u_2|_a - |v_1^\alpha|_a |u_2|_b + \binom{v_2^\beta}{ab} - \binom{v_1^\alpha}{ab}$$

is non-zero , then a word in L (of unknown length) can be uniquely reconstructed with two queries (of length 1 and 2 respectively).

Equation

in detail

For all $a, b \in \Sigma$:

$$|v_1^\alpha|_b |u_2|_a - |v_1^\alpha|_a |u_2|_b + \binom{v_2^\beta}{ab} - \binom{v_1^\alpha}{ab} = 0$$

$\downarrow$ $\downarrow$

$x \sim_k y$ for $k \in \mathbb{N}$ iff
$\binom{x}{w} = \binom{y}{w}$ for all $w \in \Sigma^k$

Equation

in detail

For all $a, b \in \Sigma$:

$$|v_1^\alpha|_b |u_2|_a - |v_1^\alpha|_a |u_2|_b + \binom{v_2^\beta}{ab} - \binom{v_1^\alpha}{ab} = 0$$

$\downarrow$

$$\binom{v_1^\alpha}{ab} = \binom{v_2^\beta}{ab}$$

and

$$|v_1^\alpha|_b |u_2|_a = |v_1^\alpha|_a |u_2|_b$$

$\downarrow$

$x \sim_k y$ for $k \in \mathbb{N}$ iff
$\binom{x}{w} = \binom{y}{w}$ for all $w \in \Sigma^k$

Equation

in detail

For all $a, b \in \Sigma$:

$$|v_1^\alpha|_b |u_2|_a - |v_1^\alpha|_a |u_2|_b + \binom{v_2^\beta}{ab} - \binom{v_1^\alpha}{ab} = 0$$

$\Downarrow$ $\Downarrow$

$$\binom{v_1^\alpha}{ab} = \binom{v_2^\beta}{ab}$$

and

$$|v_1^\alpha|_b |u_2|_a = |v_1^\alpha|_a |u_2|_b$$

$$\Longleftrightarrow$$

$v_1^\alpha \sim_2 v_2^\beta$ and $\Psi(v_1^\alpha), \Psi(u_2)$ lin. dependent

$x \sim_k y$ for $k \in \mathbb{N}$ iff
$\binom{x}{w} = \binom{y}{w}$ for all $w \in \Sigma^k$

Equation

in detail

For all $a, b \in \Sigma$:

$$|v_1^\alpha|_b |u_2|_a - |v_1^\alpha|_a |u_2|_b + \binom{v_2^\beta}{ab} - \binom{v_1^\alpha}{ab} = 0$$

$\Downarrow$

$$\binom{v_1^\alpha}{ab} = \binom{v_2^\beta}{ab}$$

and

$$|v_1^\alpha|_b |u_2|_a = |v_1^\alpha|_a |u_2|_b$$

$$\Longleftrightarrow$$

$v_1^\alpha \sim_2 v_2^\beta$ and $\Psi(v_1^\alpha), \Psi(u_2)$ lin. dependent

$\Downarrow$

$$|v_1^\alpha|_b |u_2|_a - |v_1^\alpha|_a |u_2|_b$$

$$= \binom{v_1^\alpha}{ab} - \binom{v_2^\beta}{ab}$$

$$\neq 0$$

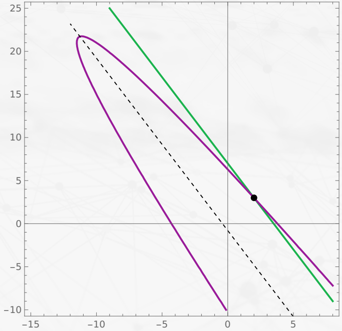
$x \sim_k y$ for $k \in \mathbb{N}$ iff $\binom{x}{w} = \binom{y}{w}$ for all $w \in \Sigma^k$

Example

new

$$L = \underbrace{0}_{u_1}\underbrace{(11000)^*}_{v_1}\underbrace{001}_{u_2}\underbrace{(010)^*}_{v_1}$$

$$\begin{cases} \mathrm{Eq}_{g,0} : & 2x + y - 7 = 0 \\ \mathrm{Eq}_{g,1} : & 2y + y - 7 = 0 \\ \mathrm{Eq}_{g,01} : & 4x^2 + 4xy + 2x + y^2 + 4y - 65 = 0 \end{cases}$$



Consequence

for short queries

Theorem

Let $L = u_1 v_1^* u_2 v_2^* u_3$ *and*

Consequence

for short queries

Theorem

Let $L = u_1 v_1^* u_2 v_2^* u_3$ *and*

- $v_1^\alpha \sim_1 v_2^\beta$ *for some coprime integers* $\alpha, \beta \geqslant 1$

Consequence

for short queries

Theorem

Let $L = u_1 v_1^* u_2 v_2^* u_3$ *and*

- $v_1^\alpha \sim_1 v_2^\beta$ *for some coprime integers* $\alpha, \beta \geqslant 1$
- $k \geqslant 2$

Consequence

for short queries

Theorem

Let $L = u_1 v_1^* u_2 v_2^* u_3$ *and*

- $v_1^{\alpha} \sim_1 v_2^{\beta}$ *for some coprime integers* $\alpha, \beta \geqslant 1$
- $k \geqslant 2$
- $g = u_1 v_1^{\gamma_1} u_2 v_2^{\gamma_2} u_3$ *to guess is long enough such that* $\lfloor \gamma_1/\alpha \rfloor + \lfloor \gamma_2/\beta \rfloor \geqslant k$

For all queries q *such that* $2 \leqslant |q| \leqslant k$*:*

Consequence

for short queries

Theorem

Let $L = u_1 v_1^* u_2 v_2^* u_3$ *and*

- $v_1^{\alpha} \sim_1 v_2^{\beta}$ *for some coprime integers* $\alpha, \beta \geqslant 1$
- $k \geqslant 2$
- $g = u_1 v_1^{\gamma_1} u_2 v_2^{\gamma_2} u_3$ *to guess is long enough such that* $\lfloor \gamma_1/\alpha \rfloor + \lfloor \gamma_2/\beta \rfloor \geqslant k$

For all queries q *such that* $2 \leqslant |q| \leqslant k$:

$$\{\mathrm{Eq}_{g,a} = 0\} \textit{ and } \{\mathrm{Eq}_{g,q} = 0 \mid 1 \leqslant |q| \leqslant k\} \iff v_1^{\alpha} u_2 \sim_k u_2 v_2^{\beta}$$

same sets of solutions

Consequence

for short queries

Theorem

Let $L = u_1 v_1^* u_2 v_2^* u_3$ *and*

- $v_1^\alpha \sim_1 v_2^\beta$ *for some coprime integers* $\alpha, \beta \geqslant 1$
- $k \geqslant 2$
- $g = u_1 v_1^{\gamma_1} u_2 v_2^{\gamma_2} u_3$ *to guess is long enough such that* $\lfloor \gamma_1/\alpha \rfloor + \lfloor \gamma_2/\beta \rfloor \geqslant k$

For all queries q *such that* $2 \leqslant |q| \leqslant k$:

$$\{\mathrm{Eq}_{g,a} = 0\} \text{ and } \{\mathrm{Eq}_{g,q} = 0 \mid 1 \leqslant |q| \leqslant k\} \quad \Longleftrightarrow \quad v_1^\alpha u_2 \sim_k u_2 v_2^\beta$$

same sets of solutions

➔ there exists a largest K such that $v_1^\alpha u_2 \sim_K u_2 v_2^\beta$ and $v_1^\alpha u_2 \nsim_{K+1} u_2 v_2^\beta$.

Query for K

no short queries

Lemma

If $v_1^{\alpha} u_2 \sim_k u_2 v_2^{\beta}$ one can determine a K

Query for K

no short queries

Lemma

If $v_1^\alpha u_2 \sim_k u_2 v_2^\beta$ one can determine a K such that, a word in L (of unknown length) can be uniquely reconstructed

Query for K

no short queries

Lemma

If $v_1^{\alpha} u_2 \sim_k u_2 v_2^{\beta}$ one can determine a K such that, a word in L (of unknown length) can be uniquely reconstructed with two queries (of length 1 and $K+1$ respectively).

Complete Picture

for two loops

Are $\Psi(v_1), \Psi(v_2)$
linearly independent?

<u>Step 1</u>
yes: $|q_1| = 1, |q_2| = 1$
2 linear equations suffice

no: $v_1^{\alpha} \sim_1 v_2^{\beta}$
$\exists a, b \in \Sigma$:
$(*)$ is non-zero?

<u>Step 2</u>
yes: $|q_1| = 1, |q_2| = 2$
2 equations suffice

<u>Step 3</u>
no: $|q_1| = 1, |q_2| = K + 1$
$v_1^{\alpha} u_2 \sim_2 u_2 v_2^{\beta}$
2 equations suffice

More Loops

Introduction

Basics & Initial Results

Polynomials

for Reconstruction

Nice Case

Two Loops

General Case

and its problems

More Loops

More Loops

- more queries: $q_1, \ldots, q_m \in \Sigma^+$

More Loops

- more queries: $q_1, \ldots, q_m \in \Sigma^+$
- system of m equations $\mathrm{Eq}_{g,q_i} = 0$

More Loops

- more queries: $q_1, \ldots, q_m \in \Sigma^+$
- system of m equations $\mathrm{Eq}_{g,q_i} = 0$

there exists **at least one non-negative integer solution** $(\gamma_1, \ldots, \gamma_t)$

More Loops

- more queries: $q_1, \ldots, q_m \in \Sigma^+$
- system of m equations $\mathrm{Eq}_{g,q_i} = 0$

there exists **at least one non-negative integer solution** $(\gamma_1, \ldots, \gamma_t)$

Goal.

Show that

$$F : \mathbb{N}^t \to \mathbb{N}^m, \ \mathbf{x} = (x_1, \ldots, x_t) \mapsto (\mathrm{P}_{q_1}(\mathbf{x}), \ldots, \mathrm{P}_{q_m}(\mathbf{x}))$$

is injective. $\square$

Tarski-Seidenberg

$F : \mathbb{N}^t \to \mathbb{N}^m,$

$\mathbf{x} = (x_1, \ldots, x_t) \mapsto (\mathrm{P}_{q_1}(\mathbf{x}), \ldots, \mathrm{P}_{q_m}(\mathbf{x}))$

Tarski-Seidenberg

$F : \mathbb{N}^t \to \mathbb{N}^m,$

$\mathbf{x} = (x_1, \ldots, x_t) \mapsto (\mathrm{P}_{q_1}(\mathbf{x}), \ldots, \mathrm{P}_{q_m}(\mathbf{x}))$

extend the domain to real numbers

Tarski-Seidenberg

$F : \mathbb{N}^t \to \mathbb{N}^m,$

$\mathbf{x} = (x_1, \ldots, x_t) \mapsto (\mathrm{P}_{q_1}(\mathbf{x}), \ldots, \mathrm{P}_{q_m}(\mathbf{x}))$

extend the domain to real numbers

$G : \mathbb{R}^t_{\geqslant 0} \to \mathbb{R}^m_{\geqslant 0},$

$\mathbf{x} = (x_1, \ldots, x_t) \mapsto (\mathrm{P}_{q_1}(\mathbf{x}), \ldots, \mathrm{P}_{q_m}(\mathbf{x}))$

Tarski-Seidenberg

$F : \mathbb{N}^t \to \mathbb{N}^m,$

$\mathbf{x} = (x_1, \ldots, x_t) \mapsto (\mathrm{P}_{q_1}(\mathbf{x}), \ldots, \mathrm{P}_{q_m}(\mathbf{x}))$

extend the domain to real numbers

$\Downarrow$

$G : \mathbb{R}^t_{\geqslant 0} \to \mathbb{R}^m_{\geqslant 0},$

$\mathbf{x} = (x_1, \ldots, x_t) \mapsto (\mathrm{P}_{q_1}(\mathbf{x}), \ldots, \mathrm{P}_{q_m}(\mathbf{x}))$

$\Downarrow$

$$\neg \left(\exists x_1, \ldots, x_t, y_1, \ldots, y_t \geqslant 0 : \bigvee_{j=1}^{t} x_j \neq y_j \Rightarrow G(x_1, \ldots, x_t) \neq G(y_1, \ldots, y_t) \right).$$

Tarski-Seidenberg

$F : \mathbb{N}^t \to \mathbb{N}^m,$

$\mathbf{x} = (x_1, \dots, x_t) \mapsto (\mathrm{P}_{q_1}(\mathbf{x}), \dots, \mathrm{P}_{q_m}(\mathbf{x}))$

extend the domain to real numbers

↓

$G : \mathbb{R}^t_{\geqslant 0} \to \mathbb{R}^m_{\geqslant 0},$

$\mathbf{x} = (x_1, \dots, x_t) \mapsto (\mathrm{P}_{q_1}(\mathbf{x}), \dots, \mathrm{P}_{q_m}(\mathbf{x}))$

Theorem (Tarski-Seidenberg)

For every first-order formula over the real field, there exists an equivalent quantifier-free formula. Furthermore, there is an explicit algorithm to compute this quantifier-free formula.

↓

$$\neg\left(\exists x_1, \dots, x_t, y_1, \dots, y_t \geqslant 0 : \bigvee_{j=1}^{t} x_j \neq y_j \Rightarrow G(x_1, \dots, x_t) \neq G(y_1, \dots, y_t)\right).$$

Tarski-Seidenberg

Theorem

Let

- $q_1, \ldots, q_m$ *be queries*

Tarski-Seidenberg

Theorem

Let

- $q_1, \ldots, q_m$ *be queries*
- $G(\mathbf{x}) = (\mathrm{P}_{q_1}(\mathbf{x}), \ldots, \mathrm{P}_{q_m}(\mathbf{x}))$ *be the corresponding polynomial map*

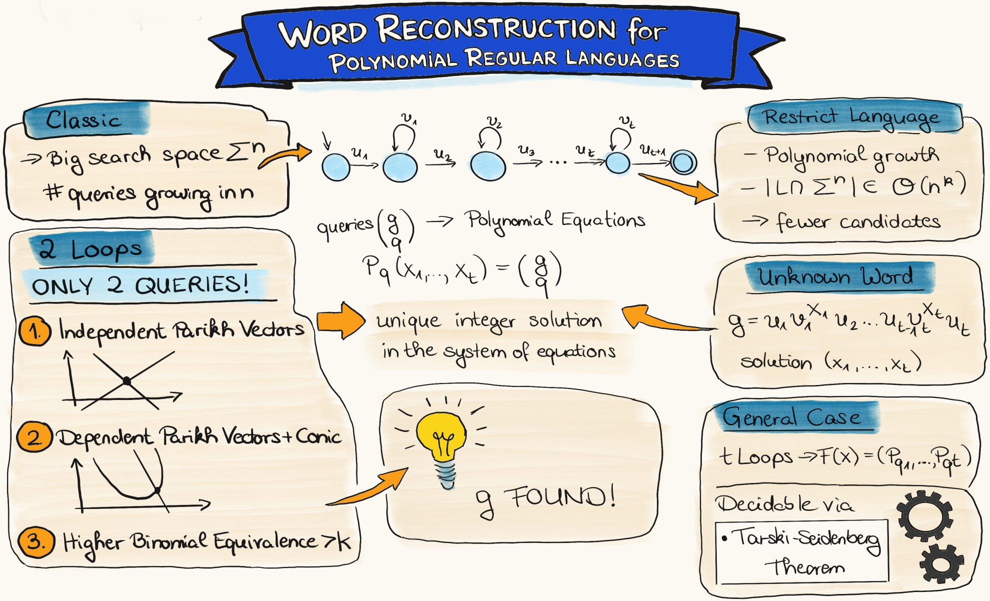
Tarski-Seidenberg

Theorem

Let

- $q_1, \ldots, q_m$ *be queries*
- $G(\mathbf{x}) = (\mathrm{P}_{q_1}(\mathbf{x}), \ldots, \mathrm{P}_{q_m}(\mathbf{x}))$ *be the corresponding polynomial map*

quantifier elimination of the formula returns `True` $\Longrightarrow$ *any word in the language can be reconstructed in a constant number of m queries*


Word Reconstruction for
Polynomial Regular Languages
Classic
→ Big search space Σ^n
queries growing in n
v1 v2 vt
u1 u2 u3 … ut ut+1
queries (g q) → Polynomial Equations
Pq(x1,…, xt) = (g q)
Restrict Language
– Polynomial growth
– |L ∩ Σ^n| ∈ O(n^k)
→ fewer candidates
2 Loops
ONLY 2 QUERIES!
1. Independent Parikh Vectors
2. Dependent Parikh Vectors + Conic
3. Higher Binomial Equivalence > k
unique integer solution
in the system of equations
Unknown Word
g = u1 v1^x1 u2 … ut-1 vt^xt ut
solution (x1, …, xt)
g FOUND!
General Case
t Loops → F(x) = (Pq1, …, Pqt)
Decidable via
• Tarski-Seidenberg Theorem