q-deformations of binomial coefficients of words

Antoine Renard

Joint work with Michel Rigo and Markus A. Whiteland

Département de Mathématique, Université de Liège

27th June 2023

Outline

Outline

Definitions I

An ***alphabet*** is a finite set of symbols. For example,

$$A = \{a, b, c, d\}, \quad B = \{0, 1\} \quad \text{and} \quad C = \{\clubsuit, \blacklozenge, \heartsuit, \spadesuit\}$$

are alphabets.

The elements of an alphabet are called ***letters***, and a ***word*** is a finite or infinite sequence of letters. For instance,

$$u = abbcabc, \quad v = 010010100 \quad \text{and} \quad w = \clubsuit\spadesuit\heartsuit\clubsuit\clubsuit\heartsuit$$

are finite words over the alphabets A, B and C respectively.
The word

$$\mathbf{f} = abaababaabaababaabab\cdots$$

is an infinite word called the ***Fibonacci word***.

Definitions I

An ***alphabet*** is a finite set of symbols. For example,

$$A = \{a, b, c, d\}, \quad B = \{0, 1\} \quad \text{and} \quad C = \{\clubsuit, \blacklozenge, \heartsuit, \spadesuit\}$$

are alphabets.

The elements of an alphabet are called ***letters***, and a ***word*** is a finite or infinite sequence of letters. For instance,

$$u = abbcabc, \quad v = 010010100 \quad \text{and} \quad w = \clubsuit\spadesuit\heartsuit\clubsuit\clubsuit\heartsuit$$

are finite words over the alphabets A, B and C respectively.
The word

$$\mathbf{f} = abaababaabaababaabab\cdots$$

is an infinite word called the ***Fibonacci word***.

Definitions II

In this talk, we shall only consider finite words.

Let A be an alphabet. We denote by A^* the set of all finite words over A. This set, along with the ***empty word*** ε as identity and the ***concatenation product***, is a monoid.

The ***length*** of a word w, denoted by $|w|$, is the number of its letters. Hence, if $w = w_n \cdots w_1$ $(w_i \in A)$, we write $|w| = n$.

If there exist some finite words x, y, z such that $w = xyz$, we say that

- x is a ***prefix*** of w $(x \in \mathrm{Pref}(w))$,
- y is a ***factor*** of w $(y \in \mathrm{Fac}(w))$,
- z is a ***suffix*** of w $(z \in \mathrm{Suff}(w))$.

Definitions II

In this talk, we shall only consider finite words.

Let A be an alphabet. We denote by A^* the set of all finite words over A. This set, along with the ***empty word*** ε as identity and the ***concatenation product***, is a monoid.

The ***length*** of a word w, denoted by $|w|$, is the number of its letters. Hence, if $w = w_n \cdots w_1$ $(w_i \in A)$, we write $|w| = n$.

If there exist some finite words x, y, z such that $w = xyz$, we say that

- x is a ***prefix*** of w $(x \in \mathrm{Pref}(w))$,
- y is a ***factor*** of w $(y \in \mathrm{Fac}(w))$,
- z is a ***suffix*** of w $(z \in \mathrm{Suff}(w))$.

Definitions II

In this talk, we shall only consider finite words.

Let A be an alphabet. We denote by A^* the set of all finite words over A. This set, along with the ***empty word*** ε as identity and the ***concatenation product***, is a monoid.

The ***length*** of a word w, denoted by $|w|$, is the number of its letters. Hence, if $w = w_n \cdots w_1$ $(w_i \in A)$, we write $|w| = n$.

If there exist some finite words x, y, z such that $w = xyz$, we say that

- x is a ***prefix*** of w $(x \in \mathrm{Pref}(w))$,
- y is a ***factor*** of w $(y \in \mathrm{Fac}(w))$,
- z is a ***suffix*** of w $(z \in \mathrm{Suff}(w))$.

Outline

Introduction

Binomial coefficient $\binom{u}{v}$ of two words: counts the number of occurrences of v as a subword of u

Ex:

$$\binom{abbab}{ab} = 4$$

$abbab$ $abbab$
$abbab$ $abbab$

Gaussian binomial coefficient $\binom{m}{r}_q$ of two positive integers:

$$\binom{m}{r}_q = \frac{(1-q^m)\cdots(1-q^{m-r+1})}{(1-q^r)\cdots(1-q)}$$

$\longrightarrow$ ***What if we merge these two objects?***

Introduction

Binomial coefficient $\binom{u}{v}$ of two words: counts the number of occurrences of v as a subword of u

Ex:

$$\binom{abbab}{ab} = 4$$

$abbab$ $abbab$
$abbab$ $abbab$

Gaussian binomial coefficient $\binom{m}{r}_q$ of two positive integers:

$$\binom{m}{r}_q = \frac{(1-q^m)\cdots(1-q^{m-r+1})}{(1-q^r)\cdots(1-q)}$$

$\longrightarrow$ ***What if we merge these two objects?***

Introduction

Binomial coefficient $\binom{u}{v}$ of two words: counts the number of occurrences of v as a subword of u

Ex:

$$\binom{abbab}{ab} = 4$$

$abbab$ $abbab$
$abbab$ $abbab$

Gaussian binomial coefficient $\binom{m}{r}_q$ of two positive integers:

$$\binom{m}{r}_q = \frac{(1-q^m)\cdots(1-q^{m-r+1})}{(1-q^r)\cdots(1-q)}$$

$\longrightarrow$ ***What if we merge these two objects?***

How to define this q-deformation?

Two recursive definitions for the "classical" coefficients:

Coefficients on words:

$$\binom{ua}{vb} = \binom{u}{vb} + \delta_{a,b}\binom{u}{v}$$

Gaussian coefficients:

$$\binom{m+1}{r+1}_q = \binom{m}{r+1}_q \cdot q^{r+1} + \binom{m}{r}_q$$

$\longrightarrow$ ***We are going to mix these two!***

How to define this q-deformation?

Two recursive definitions for the "classical" coefficients:

Coefficients on words:

$$\binom{ua}{vb} = \binom{u}{vb} + \delta_{a,b}\binom{u}{v}$$

Gaussian coefficients:

$$\binom{m+1}{r+1}_q = \binom{m}{r+1}_q \cdot q^{r+1} + \binom{m}{r}_q$$

$\longrightarrow$ ***We are going to mix these two!***

How to define this q-deformation?

Two recursive definitions for the "classical" coefficients:

Coefficients on words:

$$\binom{ua}{vb} = \binom{u}{vb} + \delta_{a,b}\binom{u}{v}$$

Gaussian coefficients:

$$\binom{m+1}{r+1}_q = \binom{m}{r+1}_q \cdot q^{r+1} + \binom{m}{r}_q$$

$\longrightarrow$ ***We are going to mix these two!***

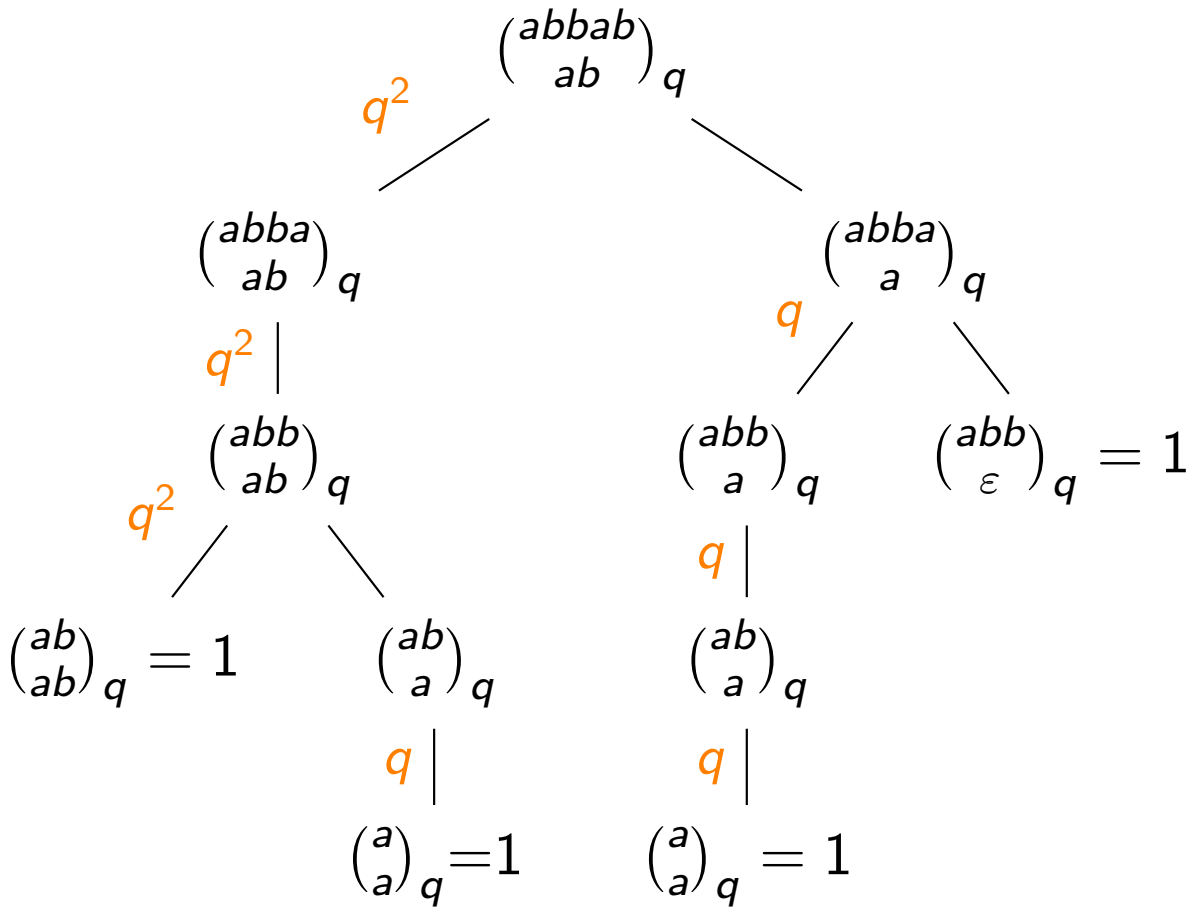
q-deformed binomial coefficients of words

The ***q-deformation*** $\binom{\cdot}{\cdot}_q$ of binomial coefficients of words is a polynomial in $\mathbb{N}[q]$ defined as follows: for all $u, v \in A^*$ and $a, b \in A$,

$$\binom{u}{\varepsilon}_q = 1, \quad \binom{\varepsilon}{v}_q = 0 \text{ if } v \neq \varepsilon,$$

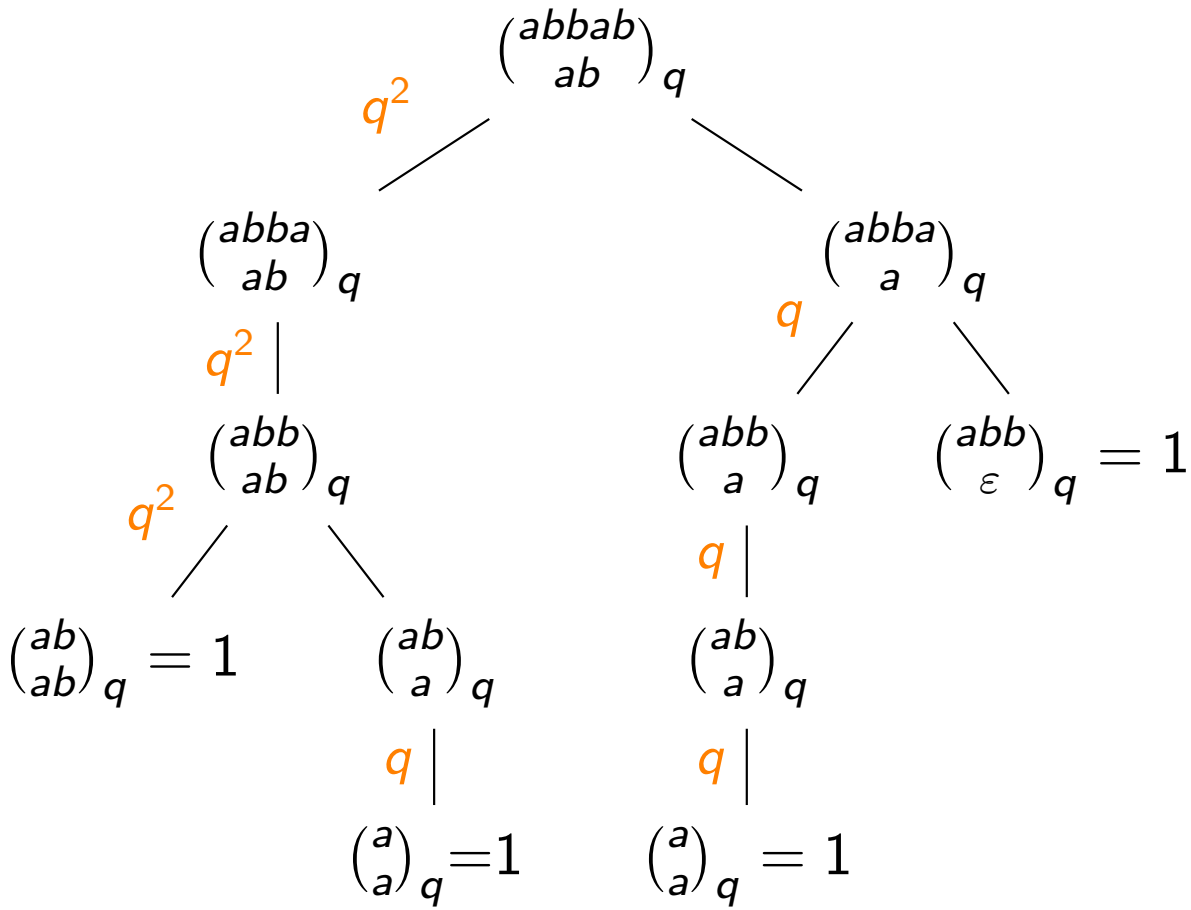
$$\binom{ua}{vb}_q = \binom{u}{vb}_q \cdot q^{|vb|} + \delta_{a,b} \binom{u}{v}_q .$$

Example: an easy way to compute q-binomials



$$\longrightarrow \binom{abbab}{ab}_q = q^6 + q^5 + q^3 + 1$$

Example: an easy way to compute q-binomials



$$\longrightarrow \binom{abbab}{ab}_q = q^6 + q^5 + q^3 + 1$$

Basic properties

Directly from definition, we can show that $\forall u, v \in A^*$,

- $\binom{u}{u}_q = 1$,
- $\binom{u}{v}_q = 0 \Leftrightarrow v$ does not occur as a subword of u.

We can also link our q-coefficients to the classical ones:

- $\binom{u}{v}_q(1) = \binom{u}{v}$,
- $\binom{a^k}{a^l}_q = \binom{k}{l}_q$.

Outline

Main theorem

Theorem (R., Rigo, Whiteland, 2023)

Let $u = u_n \cdots u_1$ and $v = v_k \cdots v_1$ be words. Then

$$\binom{u}{v}_q = \sum_{Y \in A_{n,k}} q^{s(Y) - \frac{k(k+1)}{2}}$$

where $A_{n,k} = \{n \geq y_k > \cdots > y_1 \geq 1 \mid u_{y_k} \cdots u_{y_1} = v\}$
$s(Y) := \sum_{y \in Y} y, \forall Y \in A_{n,k}$

For example, the occurences of ab in $abbab$ give

$$\begin{array}{lcll} \overset{5\ 4\ 3\ 2\ 1}{abbab} & \longrightarrow & \overset{-(1+2)}{5+4-3=6} & \longrightarrow & q^6 \\ abbab & \longrightarrow & 5+3-3=5 & \longrightarrow & q^5 \\ abbab & \longrightarrow & 5+1-3=3 & \longrightarrow & q^3 \\ abbab & \longrightarrow & 1+2-3=0 & \longrightarrow & q^0 \end{array}$$

Main theorem

Theorem (R., Rigo, Whiteland, 2023)

Let $u = u_n \cdots u_1$ and $v = v_k \cdots v_1$ be words. Then

$$\binom{u}{v}_q = \sum_{Y \in A_{n,k}} q^{s(Y) - \frac{k(k+1)}{2}}$$

where $A_{n,k} = \{n \geq y_k > \cdots > y_1 \geq 1 \mid u_{y_k} \cdots u_{y_1} = v\}$
$s(Y) := \sum_{y \in Y} y, \forall Y \in A_{n,k}$

For example, the occurences of ab in $abbab$ give

$$\begin{array}{lcll} \overset{5\ 4\ 3\ 2\ 1}{abbab} & \longrightarrow & \overset{-(1+2)}{5+4-3} = 6 & \longrightarrow q^6 \\ abbab & \longrightarrow & 5+3-3 = 5 & \longrightarrow q^5 \\ abbab & \longrightarrow & 5+1-3 = 3 & \longrightarrow q^3 \\ abbab & \longrightarrow & 1+2-3 = 0 & \longrightarrow q^0 \end{array}$$

Alternative interpretation

More "convenient" interpretation of the powers of q:

Each occurrence of v in u contributes to $\binom{u}{v}_q$ with a term q^α, where α is the sum over all letters of v of the number of letters at the right of them and that are not part of this particular occurrence of v.

Let's clear this up using our example:

$$\underset{\downarrow}{ab\overline{bab}} \quad \underset{\downarrow}{a\underline{b}b\overline{ab}} \quad \underset{\downarrow}{a\underline{bba}b} \quad \underset{\downarrow}{abbab}$$

$$q^{3+3} + q^{2+3} + q^{0+3} + q^{0+0} = \binom{abbab}{ab}_q$$

$\longrightarrow$ the powers of q encode the positions of the letters of v in its occurrences in u

Alternative interpretation

More "convenient" interpretation of the powers of q:

Each occurrence of v in u contributes to $\binom{u}{v}_q$ with a term q^α, where α is the sum over all letters of v of the number of letters at the right of them and that are not part of this particular occurrence of v.

Let's clear this up using our example:

$$\begin{array}{ccccccccc} ab\overline{\underline{bab}} & & a\underline{b}b\overline{\underline{ab}} & & a\underline{bba}b & & abbab & & \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ q^{3+3} & + & q^{2+3} & + & q^{0+3} & + & q^{0+0} & = & \binom{abbab}{ab}_q \end{array}$$

$\longrightarrow$ the powers of q encode the positions of the letters of v in its occurrences in u

Alternative interpretation

More "convenient" interpretation of the powers of q:

Each occurrence of v in u contributes to $\binom{u}{v}_q$ with a term q^α, where α is the sum over all letters of v of the number of letters at the right of them and that are not part of this particular occurrence of v.

Let's clear this up using our example:

$$\begin{array}{ccccccccc} ab\overline{\underline{bab}} & & a\underline{b}b\overline{\underline{ab}} & & a\underline{bba}b & & abbab & & \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ q^{3+3} & + & q^{2+3} & + & q^{0+3} & + & q^{0+0} & = & \binom{abbab}{ab}_q \end{array}$$

$\longrightarrow$ the powers of q encode the positions of the letters of v in its occurrences in u

Information within the coefficients

This interpretation of q-deformed binomials gives us some information about coefficients.

Corollary

For all words u, v, the polynomial $\binom{u}{v}_q$ is monic, and the coefficient of the least degree non-zero term is 1. In particular,

- $\binom{u}{v}_q(0) = \begin{cases} 1, & \text{if } v \text{ is a suffix of } u, \\ 0, & \text{otherwise.} \end{cases}$
- $\binom{u}{v}_q \left[q^{|v|(|u|-|v|)} \right] = \begin{cases} 1, & \text{if } v \text{ is a prefix of } u, \\ 0, & \text{otherwise.} \end{cases}$

Outline

Classical formulas revisited

Some formulas/theorems working for classical coefficients have their q-analogs:

$$\binom{m+n}{k}_q = \sum_{j=0}^{k} q^{j(m-k+j)} \binom{m}{k-j}_q \binom{n}{j}_q \quad \to \quad \binom{xy}{v}_q = \sum_{\substack{v=v_1v_2 \\ v_1,v_2\in A^*}} q^{|v_1|(|y|-|v_2|)} \binom{x}{v_1}_q \binom{y}{v_2}_q$$

$$\sum_{v\in A^n} \binom{u}{v} = \binom{|u|}{n} \quad \to \quad \sum_{v\in A^n} \binom{u}{v}_q = \binom{|u|}{n}_q$$

$$\sum_{u\in A^n} \binom{u}{v} = (\#A)^{n-|v|} \binom{n}{|v|} \quad \to \quad \sum_{u\in A^n} \binom{u}{v}_q = (\#A)^{n-|v|} \binom{n}{|v|}_q$$

$$\binom{|u|-|x|}{k-|x|}\binom{u}{x} = \sum_{t\in A^k} \binom{u}{t}\binom{t}{x} \quad \to \quad \binom{|u|-|x|}{k-|x|}_q \binom{u}{x}_q = \sum_{t\in A^k} \binom{u}{t}_q \binom{t}{x}_q$$

q-shuffle I

Usual shuffle $\sqcup\!\sqcup$ of two words $=$ polynomial in $\mathbb{N}\langle A^* \rangle$

Example:

$$aba \sqcup\!\sqcup a = abaa + abaa + aaba + aaba$$
$$= 2aba^2 + 2a^2ba$$

For the q-shuffle, the coefficients are no longer integers, but polynomials in q. It is defined recursively as follows:

$$u \sqcup\!\sqcup_q \varepsilon = \varepsilon \sqcup\!\sqcup_q u = 1.u,$$

$$ua \sqcup\!\sqcup_q vb = (u \sqcup\!\sqcup_q vb)a + q^{|ua|}(ua \sqcup\!\sqcup_q v)b.$$

$\longrightarrow$ can be seen as a formal series in $\mathbb{N}[q]\langle\langle A^* \rangle\rangle$

q-shuffle I

Usual shuffle $\sqcup\!\sqcup$ of two words $=$ polynomial in $\mathbb{N}\langle A^*\rangle$

Example:

$$aba \sqcup\!\sqcup a = abaa + abaa + aaba + aaba$$
$$= 2aba^2 + 2a^2ba$$

For the q-shuffle, the coefficients are no longer integers, but polynomials in q. It is defined recursively as follows:

$$u \sqcup\!\sqcup_q \varepsilon = \varepsilon \sqcup\!\sqcup_q u = 1.u,$$

$$ua \sqcup\!\sqcup_q vb = (u \sqcup\!\sqcup_q vb)a + q^{|ua|}(ua \sqcup\!\sqcup_q v)b.$$

$\longrightarrow$ can be seen as a formal series in $\mathbb{N}[q]\langle\langle A^*\rangle\rangle$

q-shuffle and q-binomial

What is it useful for? For instance, we have $\forall u, w \in A^*$

$$\langle u \sqcup\!\sqcup_q A^*, w \rangle = \binom{w}{u}_q$$

where A^* is the characteristic formal series whose coefficients are all equal to 1, *i.e.*

$$u \sqcup\!\sqcup_q A^* = u \sqcup\!\sqcup_q \sum_{v \in A^*} v = \sum_{v \in A^*} u \sqcup\!\sqcup_q v,$$

and $\langle S, w \rangle$ denotes the coefficient of w in the series S.

q-infiltration

Usual infiltration $\uparrow$ of two words $=$ polynomial in $\mathbb{N}\langle A^* \rangle$

Example:

$$\begin{aligned} aba \uparrow a &= abaa + abaa + aaba + aaba + aba + aba \\ &= 2aba^2 + 2a^2ba + 2aba \end{aligned}$$

As for the q-shuffle, the coefficients of q-infiltration are polynomials in q.
It could be defined recursively as follows:

$$u \uparrow_q \varepsilon = \varepsilon \uparrow_q u = 1 \cdot u,$$

$$ua \uparrow_q vb = (u \uparrow_q vb)a + q^{|ua|}(ua \uparrow_q v)b + q^{\alpha(ua,vb)}\delta_{a,b}(u \uparrow_q v)a.$$

where $\alpha : A^* \times A^* \to \mathbb{N}$ is a chosen map.

One that "works well": $\alpha(ua, vb) = |ua|$.

q-infiltration

Usual infiltration $\uparrow$ of two words $=$ polynomial in $\mathbb{N}\langle A^* \rangle$

Example:

$$aba \uparrow a = abaa + abaa + aaba + aaba + aba + aba$$
$$= 2aba^2 + 2a^2ba + 2aba$$

As for the q-shuffle, the coefficients of q-infiltration are polynomials in q. It could be defined recursively as follows:

$$u \uparrow_q \varepsilon = \varepsilon \uparrow_q u = 1 \cdot u,$$

$$ua \uparrow_q vb = (u \uparrow_q vb)a + q^{|ua|}(ua \uparrow_q v)b + q^{\alpha(ua,vb)}\delta_{a,b}(u \uparrow_q v)a.$$

where $\alpha : A^* \times A^* \to \mathbb{N}$ is a chosen map.

One that "works well": $\alpha(ua, vb) = |ua|$.

q-infiltration

Usual infiltration $\uparrow$ of two words $=$ polynomial in $\mathbb{N}\langle A^* \rangle$

Example:

$$aba \uparrow a = abaa + abaa + aaba + aaba + aba + aba$$
$$= 2aba^2 + 2a^2ba + 2aba$$

As for the q-shuffle, the coefficients of q-infiltration are polynomials in q. It could be defined recursively as follows:

$$u \uparrow_q \varepsilon = \varepsilon \uparrow_q u = 1 \cdot u,$$

$$ua \uparrow_q vb = (u \uparrow_q vb)a + q^{|ua|}(ua \uparrow_q v)b + q^{\alpha(ua,vb)}\delta_{a,b}(u \uparrow_q v)a.$$

where $\alpha : A^* \times A^* \to \mathbb{N}$ is a chosen map.

One that "works well": $\alpha(ua, vb) = |ua|$.

Some properties of q-infiltration

We have some interesting properties:

- There exists a polynomial $P_{u,v}$ of degree less than $|u| + |v|$ such that

$$u \uparrow_q v = u \sqcup\!\sqcup_q v + P_{u,v}.$$

- If $|u| \geq |v|, |w|$,

$$\langle w \uparrow_q (v \uparrow_q u), u \rangle = q^{|w|(|w|+1)/2+|v|(|v|+1)/2} \binom{u}{w}_q \binom{u}{v}_q.$$

However: whatever is the definition of α,

- not associative (unlike the classical infiltration),
- can't generalize the Chen-Fox-Lyndon relation

$$\binom{h}{f}\binom{h}{g} = \sum_{w \in A^*} \langle f \uparrow g, w \rangle \binom{h}{w} \quad \forall f, g, h \in A^*.$$

Some properties of q-infiltration

We have some interesting properties:

- There exists a polynomial $P_{u,v}$ of degree less than $|u| + |v|$ such that

$$u \uparrow_q v = u \sqcup\!\sqcup_q v + P_{u,v}.$$

- If $|u| \geq |v|, |w|$,

$$\langle w \uparrow_q (v \uparrow_q u), u \rangle = q^{|w|(|w|+1)/2+|v|(|v|+1)/2} \binom{u}{w}_q \binom{u}{v}_q.$$

However: whatever is the definition of α,

- not associative (unlike the classical infiltration),
- can't generalize the Chen-Fox-Lyndon relation

$$\binom{h}{f}\binom{h}{g} = \sum_{w \in A^*} \langle f \uparrow g, w \rangle \binom{h}{w} \quad \forall f, g, h \in A^*.$$

Outline

Recognizable and p-group languages

We say that a language is ***recognizable*** if and only if there exist

- a finite monoid M,
- a subset $S \subset M$,
- a monoid morphism $\varphi : A^* \to M$,

such that $L = \varphi^{-1}(S)$. A language recognized by a p-group is a ***p-group language***, where p is a prime.

Theorem (Eilenberg, 1976)

Let p be a prime. A language is a p-group language if and only if it is a Boolean combination of languages of the form

$$L_{v,r,p} := \left\{ u \in A^* \mid \binom{u}{v} \equiv r \pmod{p} \right\}.$$

$\longrightarrow$ ***Can we generalize this result using our q-deformed coefficients?***

Recognizable and p-group languages

We say that a language is ***recognizable*** if and only if there exist

- a finite monoid M,
- a subset $S \subset M$,
- a monoid morphism $\varphi : A^* \to M$,

such that $L = \varphi^{-1}(S)$. A language recognized by a p-group is a ***p-group language***, where p is a prime.

Theorem (Eilenberg, 1976)

Let p be a prime. A language is a p-group language if and only if it is a Boolean combination of languages of the form

$$L_{v,r,p} := \left\{ u \in A^* \mid \binom{u}{v} \equiv r \pmod{p} \right\}.$$

$\longrightarrow$ ***Can we generalize this result using our q-deformed coefficients?***

Recognizable and p-group languages

We say that a language is ***recognizable*** if and only if there exist

- a finite monoid M,
- a subset $S \subset M$,
- a monoid morphism $\varphi : A^* \to M$,

such that $L = \varphi^{-1}(S)$. A language recognized by a p-group is a ***p-group language***, where p is a prime.

Theorem (Eilenberg, 1976)

Let p be a prime. A language is a p-group language if and only if it is a Boolean combination of languages of the form

$$L_{v,r,p} := \left\{ u \in A^* \mid \binom{u}{v} \equiv r \pmod{p} \right\}.$$

$\longrightarrow$ ***Can we generalize this result using our q-deformed coefficients?***

Towards a new theorem

Let p be a prime, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ be the field of integers modulo p and $\mathfrak{M}$ be a non-zero polynomial in $\mathbb{F}_p[q]$. We denote $\mathbb{K} = \mathbb{F}_p[q]/\langle \mathfrak{M} \rangle$
Quite naturally, we will consider languages of the form

$$L_{v,\mathfrak{R},\mathfrak{M}} := \left\{ u \in A^* \mid \binom{u}{v}_q \equiv \mathfrak{R} \pmod{\mathfrak{M}} \right\}.$$

Idea: To prove the theorem, we are going to define a congruence $\cong$, so that $A^*/\cong$ is a finite monoid, and thus have regular languages.

Towards a new theorem

Let p be a prime, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ be the field of integers modulo p and $\mathfrak{M}$ be a non-zero polynomial in $\mathbb{F}_p[q]$. We denote $\mathbb{K} = \mathbb{F}_p[q]/\langle \mathfrak{M} \rangle$
Quite naturally, we will consider languages of the form

$$L_{v,\mathfrak{R},\mathfrak{M}} := \left\{ u \in A^* \mid \binom{u}{v}_q \equiv \mathfrak{R} \pmod{\mathfrak{M}} \right\}.$$

Idea: To prove the theorem, we are going to define a congruence $\cong$, so that $A^*/\cong$ is a finite monoid, and thus have regular languages.

Equivalence relation $\sim_{u,\mathfrak{M}}$

Let $u \in A^*$ and $\mathfrak{M} \in \mathbb{F}_p[q]$. Two finite words $w_1, w_2 \in A^*$ are $(u, \mathfrak{M})$-***binomially equivalent*** and we write $w_1 \sim_{u,\mathfrak{M}} w_2$ whenever

$$\forall v \in \mathrm{Fac}(u) : \binom{w_1}{v}_q \equiv \binom{w_2}{v}_q \pmod{\mathfrak{M}}.$$

$\longrightarrow$ # classes $\leq \#\mathbb{K}^{(\#\,\mathrm{Fac}(u)-1)}$

$\longrightarrow$ $A^*/\sim_{u,\mathfrak{M}}$ is finite

Problem: $\sim_{u,\mathfrak{M}}$ is not always a congruence...

We will consider a congruence $\cong$ which is a ***refinement*** of $\sim_{u,\mathfrak{M}}$, *i.e.*

$$w_1 \cong w_2 \Rightarrow w_1 \sim_{u,\mathfrak{M}} w_2.$$

We also say that $\sim_{u,\mathfrak{M}}$ is ***coarser*** than $\cong$.

Equivalence relation $\sim_{u,\mathfrak{M}}$

Let $u \in A^*$ and $\mathfrak{M} \in \mathbb{F}_p[q]$. Two finite words $w_1, w_2 \in A^*$ are $(u, \mathfrak{M})$-***binomially equivalent*** and we write $w_1 \sim_{u,\mathfrak{M}} w_2$ whenever

$$\forall v \in \mathrm{Fac}(u) : \binom{w_1}{v}_q \equiv \binom{w_2}{v}_q \pmod{\mathfrak{M}}.$$

$\longrightarrow$ # classes $\leq \#\mathbb{K}^{(\#\,\mathrm{Fac}(u)-1)}$

$\longrightarrow$ $A^*/\sim_{u,\mathfrak{M}}$ is finite

Problem: $\sim_{u,\mathfrak{M}}$ is not always a congruence...

We will consider a congruence $\cong$ which is a ***refinement*** of $\sim_{u,\mathfrak{M}}$, *i.e.*

$$w_1 \cong w_2 \Rightarrow w_1 \sim_{u,\mathfrak{M}} w_2.$$

We also say that $\sim_{u,\mathfrak{M}}$ is ***coarser*** than $\cong$.

Equivalence relation $\sim_{u,\mathfrak{M}}$

Let $u \in A^*$ and $\mathfrak{M} \in \mathbb{F}_p[q]$. Two finite words $w_1, w_2 \in A^*$ are $(u, \mathfrak{M})$-***binomially equivalent*** and we write $w_1 \sim_{u,\mathfrak{M}} w_2$ whenever

$$\forall v \in \mathrm{Fac}(u) : \binom{w_1}{v}_q \equiv \binom{w_2}{v}_q \pmod{\mathfrak{M}}.$$

$\longrightarrow$ # classes $\leq \#\mathbb{K}^{(\#\,\mathrm{Fac}(u)-1)}$

$\longrightarrow$ $A^*/\sim_{u,\mathfrak{M}}$ is finite

Problem: $\sim_{u,\mathfrak{M}}$ is not always a congruence...

We will consider a congruence $\cong$ which is a ***refinement*** of $\sim_{u,\mathfrak{M}}$, *i.e.*

$$w_1 \cong w_2 \Rightarrow w_1 \sim_{u,\mathfrak{M}} w_2.$$

We also say that $\sim_{u,\mathfrak{M}}$ is ***coarser*** than $\cong$.

Equivalence relation $\sim_{u,\mathfrak{M}}$

Let $u \in A^*$ and $\mathfrak{M} \in \mathbb{F}_p[q]$. Two finite words $w_1, w_2 \in A^*$ are $(u, \mathfrak{M})$-***binomially equivalent*** and we write $w_1 \sim_{u,\mathfrak{M}} w_2$ whenever

$$\forall v \in \mathrm{Fac}(u) \ : \ \binom{w_1}{v}_q \equiv \binom{w_2}{v}_q \pmod{\mathfrak{M}}.$$

$\longrightarrow$ # classes $\leq \#\mathbb{K}^{(\#\,\mathrm{Fac}(u)-1)}$

$\longrightarrow$ $A^*/\sim_{u,\mathfrak{M}}$ is finite

Problem: $\sim_{u,\mathfrak{M}}$ is not always a congruence...

We will consider a congruence $\cong$ which is a ***refinement*** of $\sim_{u,\mathfrak{M}}$, *i.e.*

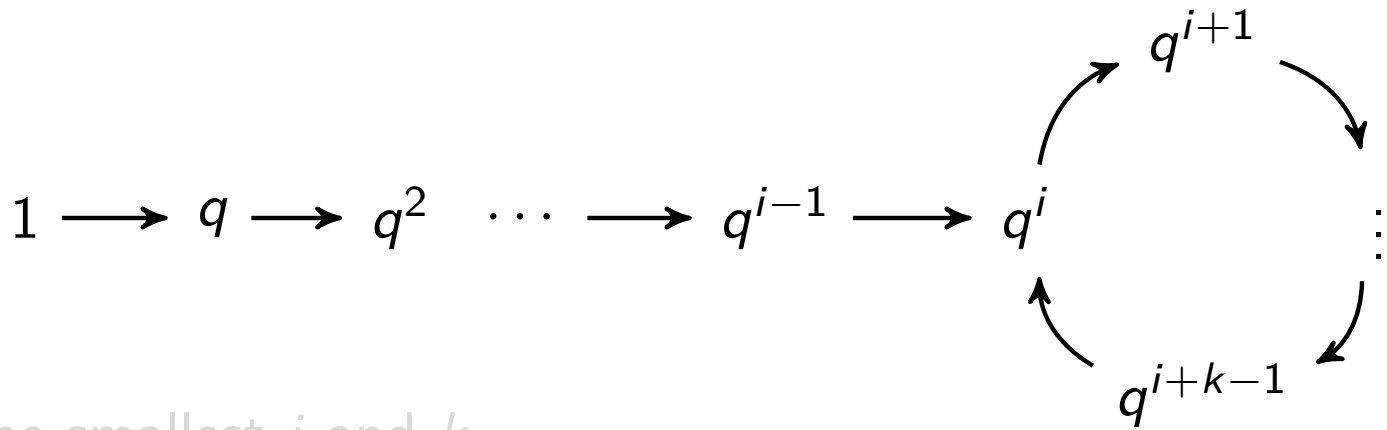
$$w_1 \cong w_2 \Rightarrow w_1 \sim_{u,\mathfrak{M}} w_2.$$

We also say that $\sim_{u,\mathfrak{M}}$ is ***coarser*** than $\cong$.

Properties of q in $\mathbb{K}$

As $\mathbb{K} = \mathbb{F}_p[q]/\langle \mathfrak{M} \rangle$ is finite, there exist $i \geq 0$, $k \geq 1$ such that

$$q^i \equiv q^{i+k} \pmod{\mathfrak{M}}.$$



Taking the smallest i and k,

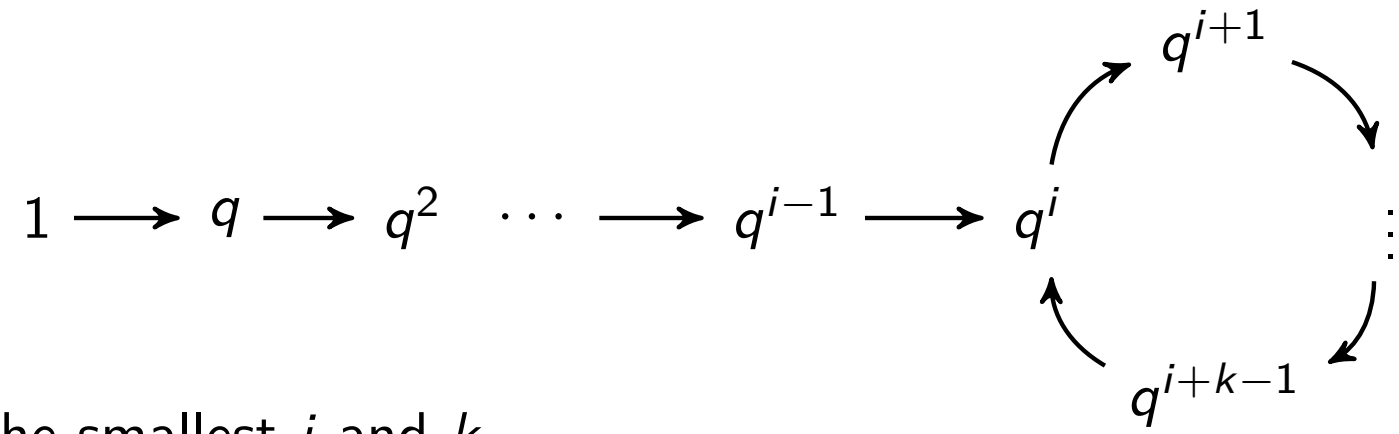
- i is the ***index*** of q,
- k is the ***period*** of q.

Notice that, if q is invertible in $\mathbb{K}$, then $i = 0$ and $k = \mathrm{ord}(q)$.

Properties of q in $\mathbb{K}$

As $\mathbb{K} = \mathbb{F}_p[q]/\langle \mathfrak{M} \rangle$ is finite, there exist $i \geq 0$, $k \geq 1$ such that

$$q^i \equiv q^{i+k} \pmod{\mathfrak{M}}.$$



Taking the smallest i and k,

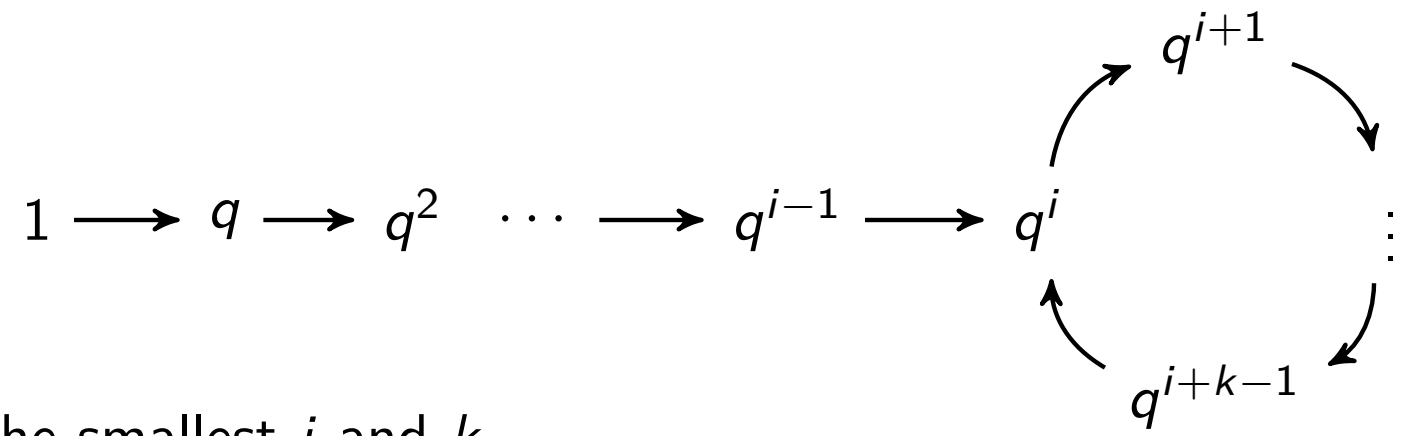
- i is the ***index*** of q,
- k is the ***period*** of q.

Notice that, if q is invertible in $\mathbb{K}$, then $i = 0$ and $k = \mathrm{ord}(q)$.

Properties of q in $\mathbb{K}$

As $\mathbb{K} = \mathbb{F}_p[q]/\langle \mathfrak{M} \rangle$ is finite, there exist $i \geq 0$, $k \geq 1$ such that

$$q^i \equiv q^{i+k} \pmod{\mathfrak{M}}.$$



Taking the smallest i and k,

- i is the ***index*** of q,
- k is the ***period*** of q.

Notice that, if q is invertible in $\mathbb{K}$, then $i = 0$ and $k = \mathrm{ord}(q)$.

Structure of $A^*/\cong$: q is not invertible

If q is not a unit of $\mathbb{K}$, we have the following:

Proposition (R., Rigo, Whiteland, 2023)

Let $u \in A^*$, $\mathfrak{M} \in \mathbb{F}_p[q]$ and $\cong$ be a congruence that refines $\sim_{u,\mathfrak{M}}$. If q is not a unit of $\mathbb{K}$, then the monoid $A^*/\cong$ is a not group. In particular, no element except for the identity is invertible.

Structure of $A^*/\cong$: q is invertible

If q is a unit of $\mathbb{K}$, we can look for the ***coarsest*** congruence refining $\sim_{u,\mathfrak{M}}$.

We show that $\sim_{u,\mathfrak{M}} \cap \sim_{\mathrm{ord}(p)}$, where

$$w_1 \sim_{\mathrm{ord}(q)} w_2 \Leftrightarrow |w_1| \equiv |w_2| \pmod{\mathrm{ord}(q)},$$

and denoted $\equiv_{u,\mathfrak{M}}$ is the coarsest congruence refining $\sim_{u,\mathfrak{M}}$.

Theorem (R., Rigo, Whiteland, 2023)

Let $u \in A^*$, $\mathfrak{M} \in \mathbb{F}_p[q]$. If q is a unit in $\mathbb{K}$, $A^*/\equiv_{u,\mathfrak{M}}$ is a group whose order divides $\mathrm{ord}(q) \cdot p^{|u|}$.

Structure of $A^*/\cong$: q is invertible

If q is a unit of $\mathbb{K}$, we can look for the ***coarsest*** congruence refining $\sim_{u,\mathfrak{M}}$.

We show that $\sim_{u,\mathfrak{M}} \cap \sim_{\mathrm{ord}(p)}$, where

$$w_1 \sim_{\mathrm{ord}(q)} w_2 \Leftrightarrow |w_1| \equiv |w_2| \pmod{\mathrm{ord}(q)},$$

and denoted $\equiv_{u,\mathfrak{M}}$ is the coarsest congruence refining $\sim_{u,\mathfrak{M}}$.

Theorem (R., Rigo, Whiteland, 2023)

Let $u \in A^*$, $\mathfrak{M} \in \mathbb{F}_p[q]$. If q is a unit in $\mathbb{K}$, $A^*/\equiv_{u,\mathfrak{M}}$ is a group whose order divides $\mathrm{ord}(q) \cdot p^{|u|}$.

Structure of $A^*/\cong$: q is invertible

If q is a unit of $\mathbb{K}$, we can look for the ***coarsest*** congruence refining $\sim_{u,\mathfrak{M}}$.

We show that $\sim_{u,\mathfrak{M}} \cap \sim_{\mathrm{ord}(p)}$, where

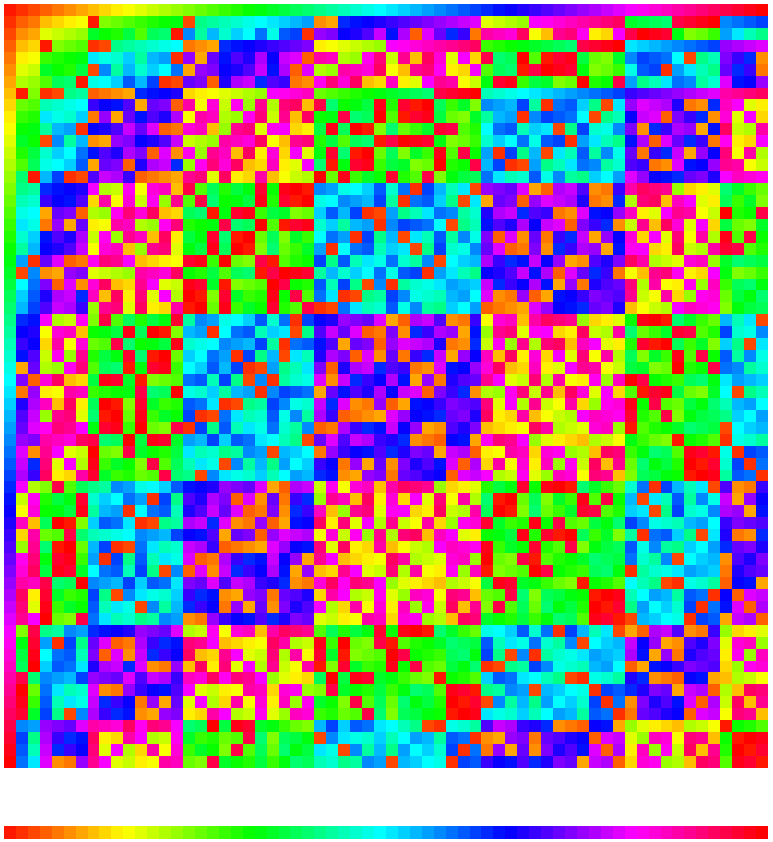
$$w_1 \sim_{\mathrm{ord}(q)} w_2 \Leftrightarrow |w_1| \equiv |w_2| \pmod{\mathrm{ord}(q)},$$

and denoted $\equiv_{u,\mathfrak{M}}$ is the coarsest congruence refining $\sim_{u,\mathfrak{M}}$.

Theorem (R., Rigo, Whiteland, 2023)

Let $u \in A^*$, $\mathfrak{M} \in \mathbb{F}_p[q]$. If q is a unit in $\mathbb{K}$, $A^*/\equiv_{u,\mathfrak{M}}$ is a group whose order divides $\mathrm{ord}(q) \cdot p^{|u|}$.

A beautiful example



Multiplication table for the group $\{a, b\}^*/\sim_{ab,q^2+1}$ with 64 elements.

A generalization of Eilenberg's theorem

Corollary (R., Rigo, Whiteland, 2023)

Let v be a word and $\mathfrak{M} = a(q-1)^d$ for some integer $d \geq 1$. The language

$$L_{v,\mathfrak{R},\mathfrak{M}} = \left\{ u \in A^* \mid \binom{u}{v}_q \equiv \mathfrak{R} \pmod{\mathfrak{M}} \right\}$$

is a p-group language.

Theorem (R., Rigo, Whiteland, 2023)

Let p be a prime and $\mathfrak{M} = a(q-1)^d$ with $d \geq 1$ an integer. A language is a p-group language if and only if it is a Boolean combination of languages of the form

$$L_{v,\mathfrak{R},\mathfrak{M}} = \left\{ u \in A^* \mid \binom{u}{v}_q \equiv \mathfrak{R} \pmod{\mathfrak{M}} \right\}.$$

A generalization of Eilenberg's theorem

Corollary (R., Rigo, Whiteland, 2023)

Let v be a word and $\mathfrak{M} = a(q-1)^d$ for some integer $d \geq 1$. The language

$$L_{v,\mathfrak{R},\mathfrak{M}} = \left\{ u \in A^* \mid \binom{u}{v}_q \equiv \mathfrak{R} \pmod{\mathfrak{M}} \right\}$$

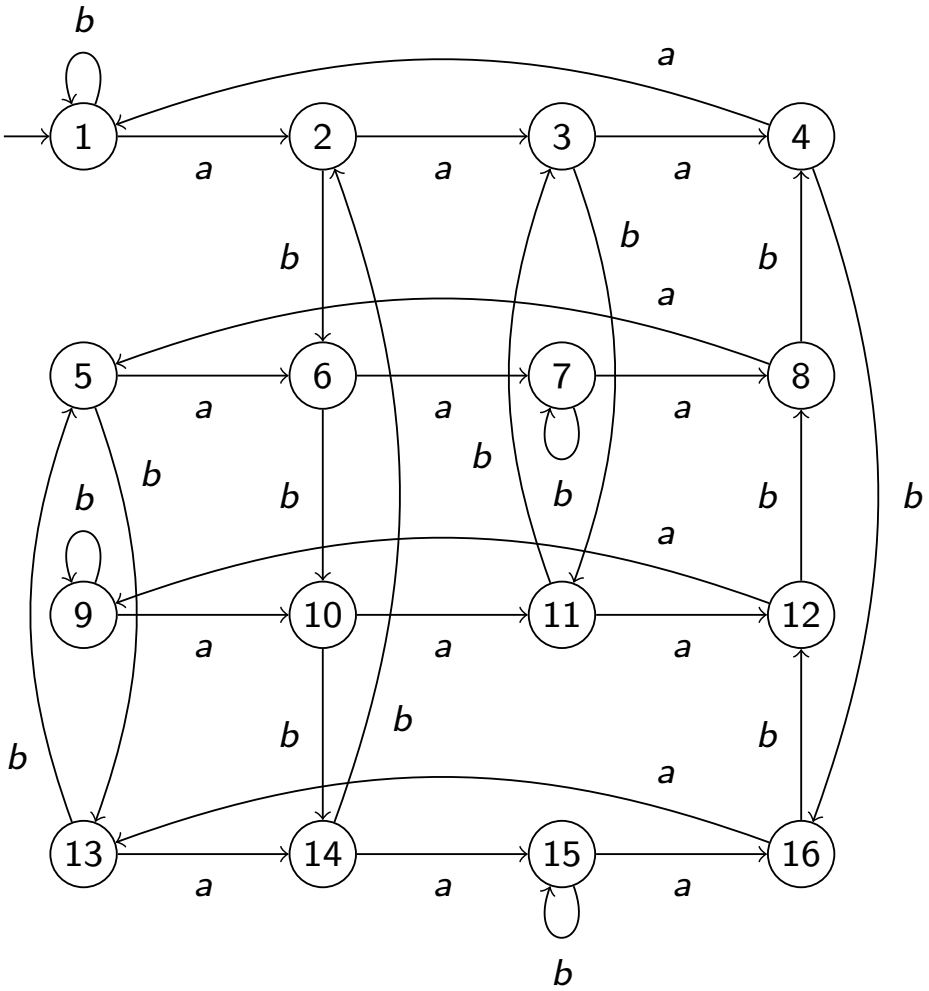
is a p-group language.

Theorem (R., Rigo, Whiteland, 2023)

Let p be a prime and $\mathfrak{M} = a(q-1)^d$ with $d \geq 1$ an integer. A language is a p-group language if and only if it is a Boolean combination of languages of the form

$$L_{v,\mathfrak{R},\mathfrak{M}} = \left\{ u \in A^* \mid \binom{u}{v}_q \equiv \mathfrak{R} \pmod{\mathfrak{M}} \right\}.$$

Example of regular language



The minimal automaton of $L_{ab,\mathfrak{R},q^2+1}$.

Open questions/Future research

- Can we give a combinatorial interpretation of all coefficients of $\binom{u}{v}_q$?
- What if we evaluate $\binom{u}{v}_q$ to some particular value?
- Can we give another definition of the infiltration product that will suit the missing properties?
- The structure of $A^*/\cong$ when q is not a unit is very particular (none of the element is invertible). Can we say more about it?
- When q is invertible, the group is non-abelian, but there are lots of symmetries. What kind of group is this? Can we compute its order exactly?
- Links with Christoffel words, q-rationals.

Thank you for your attention!

q-shuffle

For a more convenient computation, one can use the following result.

Lemma (R., Rigo, Whiteland, 2023)

We have

$$u \sqcup\!\sqcup_q v = \sum_{\substack{u=u_1\cdots u_n u_{n+1},\ u_i\in A^* \\ v=v_1\cdots v_n,\ v_i\in A}} \left(\prod_{i=1}^{n} q^{|u_1\cdots u_i|}\right) u_1 v_1 u_2 v_2 \cdots u_n v_n u_{n+1}.$$

q-shuffle: an example

Let's clarify with an example:

$$aba \sqcup\!\sqcup_q aa = q^6\, \overline{\underline{aba}}aa + q^5\, \overline{\underline{ab}}\underline{a}aa + q^4\, \bar{\underline{a}}a\underline{ba}a + q^3\, a\underline{aba}a + q^4\, \overline{\underline{ab}}aaa +$$

$$q^3\, \bar{\underline{a}}a\underline{b}aa + q^2\, a\underline{ab}aa + q^2\, \bar{\underline{a}}aaba + q\, a\underline{a}aba + 1\, aaaba.$$

$$= (q^6 + q^5 + q^4)aba^3 + (q^2 + 2q^3 + q^4)a^2ba^2 +$$
$$(q^2 + q + 1)a^3ba$$

$\longrightarrow$ roughly speaking, one has to count for each coloured letter, how many black letters are on the left of it, and then sum all of these to get the exponent

$\longrightarrow$ there exists a similar result where the letters you have to count are the ones at the right of the coloured letter