

q -deformations of binomial coefficients of words

Antoine Renard

Joint work with Michel Rigo and Markus A. Whiteland

Département de Mathématique, Université de Liège



10th November 2023

Outline

- 1 q -deformed coefficients
- 2 Combinatorial interpretation
- 3 Formulas and other generalizations
- 4 p -group languages

Outline

- 1 q -deformed coefficients
- 2 Combinatorial interpretation
- 3 Formulas and other generalizations
- 4 p -group languages

q-deformations

A *q*-**deformation** or *q*-**analog** is a generalization of some mathematical object, such that the limit for $q \rightarrow 1$ gives back the original object.

Ex:

- *q*-natural numbers: $[n]_q = \frac{1 - q^n}{1 - q} = 1 + q + \cdots + q^{n-1}$,
- *q*-factorial: $[n]_q! = [n]_q [n-1]_q \cdots [2]_q [1]_q$,
- *q*-binomial coefficients: $\binom{n}{k}_q = \frac{[n]_q!}{[n-k]_q! [k]_q!}$

But also: *q*-rational numbers, *q*-derivative, Gaussian *q*-distribution, etc.

q -deformations

A **q -deformation** or **q -analog** is a generalization of some mathematical object, such that the limit for $q \rightarrow 1$ gives back the original object.

Ex:

- q -natural numbers: $[n]_q = \frac{1 - q^n}{1 - q} = 1 + q + \cdots + q^{n-1}$,
- q -factorial: $[n]_q! = [n]_q [n-1]_q \cdots [2]_q [1]_q$,
- q -binomial coefficients: $\binom{n}{k}_q = \frac{[n]_q!}{[n-k]_q! [k]_q!}$

But also: q -rational numbers, q -derivative, Gaussian q -distribution, etc.

q -deformations

A q -**deformation** or q -**analog** is a generalization of some mathematical object, such that the limit for $q \rightarrow 1$ gives back the original object.

Ex:

- q -natural numbers: $[n]_q = \frac{1 - q^n}{1 - q} = 1 + q + \cdots + q^{n-1}$,
- q -factorial: $[n]_q! = [n]_q [n-1]_q \cdots [2]_q [1]_q$,
- q -binomial coefficients: $\binom{n}{k}_q = \frac{[n]_q!}{[n-k]_q! [k]_q!}$

But also: q -rational numbers, q -derivative, Gaussian q -distribution, etc.

Why *q*-deformed stuff in combinatorics? I

Combinatorial *q*-deformations should

- "count" something,
- generalize some (if not all) algebraic properties of the original object,
- and/or bring new combinatorial properties.

Ex: *q*-deformed binomial coefficients

On one side, $\binom{n}{k}$ counts the number of words over $\{0, 1\}^*$ of length n containing exactly k 1's. For example, there are

$$\binom{4}{2} = 6$$

words of length 4 containing 2 1's : 0011, 0101, 0110, 1001, 1010, 1100.

Why q -deformed stuff in combinatorics? I

Combinatorial q -deformations should

- "count" something,
- generalize some (if not all) algebraic properties of the original object,
- and/or bring new combinatorial properties.

Ex: q -deformed binomial coefficients

On one side, $\binom{n}{k}$ counts the number of words over $\{0, 1\}^*$ of length n containing exactly k 1's. For example, there are

$$\binom{4}{2} = 6$$

words of length 4 containing 2 1's : 0011, 0101, 0110, 1001, 1010, 1100.

Why q -deformed stuff in combinatorics? II

On another, the coefficients of the polynomial $\binom{n}{k}_q$ count the number of inversions (*i.e.* number of 1's before 0's) in words over $\{0, 1\}^*$ of length n containing exactly k 1's. For instance,

$$\binom{4}{2}_q = q^4 + q^3 + 2q^2 + q + 1,$$

because there are

- 0 inversion in 0011,
- 1 inversion in 0101,
- 2 inversions in 0110 and 1001,
- 3 inversions in 1010,
- 4 inversions in 1100.

Why q -deformed stuff in combinatorics? III

And that's not all! The coefficient $\binom{n}{k}_q$ is also used to count:

- the number of ways of throwing d balls into m bins having a maximal capacity equal to n balls: this is exactly the coefficient of q^d of $\binom{m+n}{m}_q$;
- if $q = p^d$ for some prime p and integer $d > 0$, the number of points of the Grassmanian $\text{Gr}(k, \mathbb{F}_q^n)$, i.e. the number of k -dimensional vector subspaces of a n -dimensional vector space over $\mathbb{F}_q$;
- the number of partitions of an integer $d > 0$ into a sum of m terms which are all smaller than or equal to n : this is exactly the coefficient of q^d of $\binom{m+n}{m}_q$.
Equivalently, this counts the number of partitions of d whose Young tableau fits in a $m \times n$ box;
- etc.

Why q -deformed stuff in combinatorics? III

And that's not all! The coefficient $\binom{n}{k}_q$ is also used to count:

- the number of ways of throwing d balls into m bins having a maximal capacity equal to n balls: this is exactly the coefficient of q^d of $\binom{m+n}{m}_q$;
- if $q = p^d$ for some prime p and integer $d > 0$, the number of points of the Grassmanian $\text{Gr}(k, \mathbb{F}_q^n)$, i.e. the number of k -dimensional vector subspaces of a n -dimensional vector space over $\mathbb{F}_q$;
- the number of partitions of an integer $d > 0$ into a sum of m terms which are all smaller than or equal to n : this is exactly the coefficient of q^d of $\binom{m+n}{m}_q$.
Equivalently, this counts the number of partitions of d whose Young tableau fits in a $m \times n$ box;
- etc.

Why q -deformed stuff in combinatorics? III

And that's not all! The coefficient $\binom{n}{k}_q$ is also used to count:

- the number of ways of throwing d balls into m bins having a maximal capacity equal to n balls: this is exactly the coefficient of q^d of $\binom{m+n}{m}_q$;
- if $q = p^d$ for some prime p and integer $d > 0$, the number of points of the Grassmanian $\text{Gr}(k, \mathbb{F}_q^n)$, i.e. the number of k -dimensional vector subspaces of a n -dimensional vector space over $\mathbb{F}_q$;
- the number of partitions of an integer $d > 0$ into a sum of m terms which are all smaller than or equal to n : this is exactly the coefficient of q^d of $\binom{m+n}{m}_q$.
Equivalently, this counts the number of partitions of d whose Young tableau fits in a $m \times n$ box;
- etc.

"Classical" binomial coefficients

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
 $\binom{n}{k}_q$ of two positive integers:

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

→ *What if we merge these two objects?*

"Classical" binomial coefficients

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
 $\binom{n}{k}_q$ of two positive integers:

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

→ *What if we merge these two objects?*

"Classical" binomial coefficients

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
 $\binom{n}{k}_q$ of two positive integers:

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

→ ***What if we merge these two objects?***

How to define this *q*-deformation?

Two recursive definitions for the "classical" coefficients:

Coefficients on words:

$$\begin{pmatrix} ua \\ vb \end{pmatrix} = \begin{pmatrix} u \\ vb \end{pmatrix} + \delta_{a,b} \begin{pmatrix} u \\ v \end{pmatrix}$$

Gaussian coefficients:

$$\begin{pmatrix} n+1 \\ k+1 \end{pmatrix}_q = \begin{pmatrix} n \\ k+1 \end{pmatrix}_q \cdot q^{k+1} + \begin{pmatrix} n \\ k \end{pmatrix}_q$$

→ *We are going to mix these two!*

How to define this q -deformation?

Two recursive definitions for the "classical" coefficients:

Coefficients on words:

$$\begin{pmatrix} ua \\ vb \end{pmatrix} = \begin{pmatrix} u \\ vb \end{pmatrix} + \delta_{a,b} \begin{pmatrix} u \\ v \end{pmatrix}$$

Gaussian coefficients:

$$\begin{pmatrix} n+1 \\ k+1 \end{pmatrix}_q = \begin{pmatrix} n \\ k+1 \end{pmatrix}_q \cdot q^{k+1} + \begin{pmatrix} n \\ k \end{pmatrix}_q$$

→ *We are going to mix these two!*

How to define this q -deformation?

Two recursive definitions for the "classical" coefficients:

Coefficients on words:

$$\begin{pmatrix} ua \\ vb \end{pmatrix} = \begin{pmatrix} u \\ vb \end{pmatrix} + \delta_{a,b} \begin{pmatrix} u \\ v \end{pmatrix}$$

Gaussian coefficients:

$$\begin{pmatrix} n+1 \\ k+1 \end{pmatrix}_q = \begin{pmatrix} n \\ k+1 \end{pmatrix}_q \cdot q^{k+1} + \begin{pmatrix} n \\ k \end{pmatrix}_q$$

→ ***We are going to mix these two!***

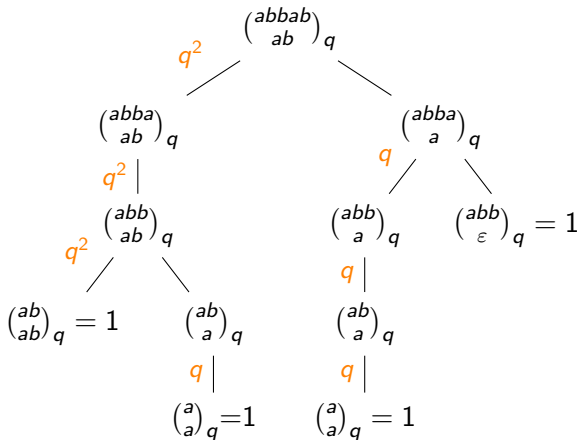
q -deformed binomial coefficients of words

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 $a, b \in A$,

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

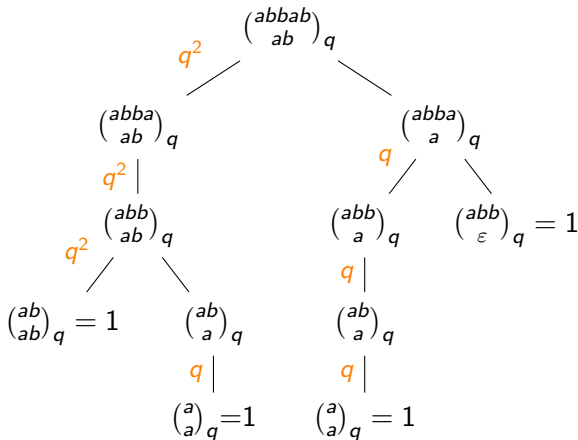
$$\binom{ua}{vb}_q = \binom{u}{vb}_q \cdot q^{|vb|} + \delta_{a,b} \binom{u}{v}_q.$$

Example: an easy way to compute q -binomials



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

Example: an easy way to compute q -binomials



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

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

- 1 q -deformed coefficients
- 2 Combinatorial interpretation
- 3 Formulas and other generalizations
- 4 p -group languages

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 occurrences of ab in $abbab$ give

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

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 occurrences of ab in $abbab$ give

$$\begin{array}{lclclcl} & 5 & 4 & 3 & 2 & 1 & & \\ ab & ab & ab & & & & \longrightarrow & 5 + 4 - 3 = 6 & \longrightarrow & q^6 \\ ab & & ab & ab & & & \longrightarrow & 5 + 3 - 3 = 5 & \longrightarrow & q^5 \\ ab & & & ab & ab & & \longrightarrow & 5 + 1 - 3 = 3 & \longrightarrow & q^3 \\ ab & & & & ab & ab & \longrightarrow & 1 + 2 - 3 = 0 & \longrightarrow & q^0 \end{array}$$

Alternative interpretation

More "convenient" interpretation of the powers of q :

Fix an occurrence of v in u : this will contribute to $\binom{u}{v}_q$ with a term q^α .
For each letter of v , count the number of letters at the right of it and that are not part of this particular occurrence of v . Sum the results for all letters of v , this gives you α .

Let's clear this up using our example:

$$\begin{array}{ccccccc}
 \overline{ab}bab & & \overline{abb}ab & & \overline{abba}b & & abba\overline{b} \\
 \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 q^{3+3} & + & q^{3+2} & + & q^{3+0} & + & q^{0+0} = \binom{abba\overline{b}}{\overline{ab}ab}_q
 \end{array}$$

→ 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 :

Fix an occurrence of v in u : this will contribute to $\binom{u}{v}_q$ with a term q^α .
For each letter of v , count the number of letters at the right of it and that are not part of this particular occurrence of v . Sum the results for all letters of v , this gives you α .

Let's clear this up using our example:

$$\begin{array}{ccccccc}
 \text{a}\overline{\text{b}\text{b}\text{a}\text{b}} & & \text{a}\overline{\text{b}\text{b}\text{a}\text{b}} & & \text{a}\overline{\text{b}\text{b}\text{a}\text{b}} & & \text{a}\overline{\text{b}\text{b}\text{a}\text{b}} \\
 \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 q^{3+3} & + & q^{3+2} & + & q^{3+0} & + & q^{0+0} = \binom{\text{abbab}}{\text{ab}}_q
 \end{array}$$

→ 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 :

Fix an occurrence of v in u : this will contribute to $\binom{u}{v}_q$ with a term q^α .
For each letter of v , count the number of letters at the right of it and that are not part of this particular occurrence of v . Sum the results for all letters of v , this gives you α .

Let's clear this up using our example:

$$\begin{array}{ccccccc}
 \text{a}\overline{\text{b}\text{b}\text{a}\text{b}} & & \text{a}\overline{\text{b}\text{b}\text{a}\text{b}} & & \text{a}\overline{\text{b}\text{b}\text{a}\text{b}} & & \text{a}\overline{\text{b}\text{b}\text{a}\text{b}} \\
 \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 q^{3+3} & + & q^{3+2} & + & q^{3+0} & + & q^{0+0} = \binom{\text{abbab}}{\text{ab}}_q
 \end{array}$$

→ the powers of q encode the positions of the letters of v in its occurrences in u

Information within the coefficients

Therefore, 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 non-zero coefficient of the monomial of least degree is 1. In particular,

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

Another example

Of course, other coefficients may be different than 1. For instance,

$$\binom{aabaaa}{aa}_q = q^8 + q^6 + 2q^5 + 2q^4 + q^3 + q^2 + q + 1.$$

Here, the 2's mean that there exist two occurrences of aa in $aabaaa$ such that the sum of positions equals 7 (resp. 8):

$$aabaaa \text{ and } aabaaa \longrightarrow 2q^4$$

$$aaba aa \text{ and } aaba aa \longrightarrow 2q^5$$

Outline

- 1 q -deformed coefficients
- 2 Combinatorial interpretation
- 3 Formulas and other generalizations
- 4 p -group languages

Classical formulas revisited

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

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

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

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

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

A nice property

As a consequence of the last formula, we have the following:

Corollary (R., Rigo, Whiteland, 2023)

Let $u \in A^$ and $1 \leq k \leq |u|$. The sequence $\left(\binom{u}{x}_q \right)_{x \in A^k}$ uniquely determines the word u .*

Proof. It is true for $k = 1$. For larger k , using the previous formula allows us to find the polynomials

$$\binom{|u| - 1}{k - 1}_q \binom{u}{a}_q$$

for each $a \in A$.

A nice property

As a consequence of the last formula, we have the following:

Corollary (R., Rigo, Whiteland, 2023)

Let $u \in A^$ and $1 \leq k \leq |u|$. The sequence $\left(\binom{u}{x}_q\right)_{x \in A^k}$ uniquely determines the word u .*

Proof. It is true for $k = 1$. For larger k , using the previous formula allows us to find the polynomials

$$\binom{|u| - 1}{k - 1}_q \binom{u}{a}_q$$

for each $a \in A$.

Outline

- 1 q -deformed coefficients
- 2 Combinatorial interpretation
- 3 Formulas and other generalizations
- 4 p -group languages

Recognizable and p -group languages

Recall that a language is **recognized** by a monoid M if there exist

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

such that $L = \varphi^{-1}(S)$.

The language L is said to be **recognizable** if it is recognized by a finite monoid.

Theorem

A language is regular if and only if it is recognizable.

Finally, a language recognized by a p -group (i.e. a group whose elements have order which is a power of p) is a **p -group language**, where p is a prime.

Recognizable and p -group languages

Recall that a language is **recognized** by a monoid M if there exist

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

such that $L = \varphi^{-1}(S)$.

The language L is said to be **recognizable** if it is recognized by a finite monoid.

Theorem

A language is regular if and only if it is recognizable.

Finally, a language recognized by a p -group (i.e. a group whose elements have order which is a power of p) is a **p -group language**, where p is a prime.

Recognizable and p -group languages

Recall that a language is **recognized** by a monoid M if there exist

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

such that $L = \varphi^{-1}(S)$.

The language L is said to be **recognizable** if it is recognized by a finite monoid.

Theorem

A language is regular if and only if it is recognizable.

Finally, a language recognized by a p -group (i.e. a group whose elements have order which is a power of p) is a **p -group language**, where p is a prime.

Recognizable and p -group languages

Recall that a language is **recognized** by a monoid M if there exist

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

such that $L = \varphi^{-1}(S)$.

The language L is said to be **recognizable** if it is recognized by a finite monoid.

Theorem

A language is regular if and only if it is recognizable.

Finally, a language recognized by a p -group (i.e. a group whose elements have order which is a power of p) is a **p -group language**, where p is a prime.

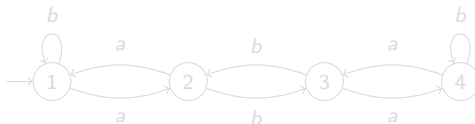
Characterizing p -group languages

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

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

For example, here is the structure of the minimal automaton of $L_{ab,r,2}$:



→ *Can we generalize this result using our q -deformed coefficients?*

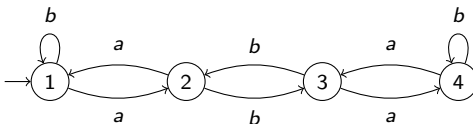
Characterizing p -group languages

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

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

For example, here is the structure of the minimal automaton of $L_{ab,r,2}$:



→ *Can we generalize this result using our q -deformed coefficients?*

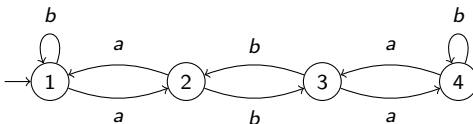
Characterizing p -group languages

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

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

For example, here is the structure of the minimal automaton of $L_{ab,r,2}$:



→ ***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

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

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

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

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 $\sim_{u,\mathfrak{M}}$ I

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

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

→ # classes $\leq \#\mathbb{K}(\#\text{Fac}(u)-1)$

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

Ex: For $p = 2$, $\mathfrak{M} = q^2 + 1$, $A = \{a, b\}$ and $u = ab$, we have $bba \sim_{u,\mathfrak{M}} bbabbbb$, for

$$\binom{bba}{a}_q \equiv 1 \equiv \binom{bbabbbb}{a}_q \pmod{\mathfrak{M}},$$

$$\binom{bba}{b}_q \equiv 1 + q \equiv \binom{bbabbbb}{b}_q \pmod{\mathfrak{M}},$$

$$\text{and } \binom{bba}{ab}_q \equiv 0 \equiv \binom{bbabbbb}{ab}_q \pmod{\mathfrak{M}}.$$

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

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

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

→ # classes $\leq \#\mathbb{K}(\#\text{Fac}(u)-1)$

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

Ex: For $p = 2$, $\mathfrak{M} = q^2 + 1$, $A = \{a, b\}$ and $u = ab$, we have $bba \sim_{u,\mathfrak{M}} bbabbbb$, for

$$\binom{bba}{a}_q \equiv 1 \equiv \binom{bbabbbb}{a}_q \pmod{\mathfrak{M}},$$

$$\binom{bba}{b}_q \equiv 1 + q \equiv \binom{bbabbbb}{b}_q \pmod{\mathfrak{M}},$$

$$\text{and } \binom{bba}{ab}_q \equiv 0 \equiv \binom{bbabbbb}{ab}_q \pmod{\mathfrak{M}}.$$

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

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

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

→ # classes $\leq \#\mathbb{K}(\#\text{Fac}(u)-1)$

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

Ex: For $p = 2$, $\mathfrak{M} = q^2 + 1$, $A = \{a, b\}$ and $u = ab$, we have $bba \sim_{u,\mathfrak{M}} bbabbbb$, for

$$\binom{bba}{a}_q \equiv 1 \equiv \binom{bbabbbb}{a}_q \pmod{\mathfrak{M}},$$

$$\binom{bba}{b}_q \equiv 1 + q \equiv \binom{bbabbbb}{b}_q \pmod{\mathfrak{M}},$$

$$\text{and } \binom{bba}{ab}_q \equiv 0 \equiv \binom{bbabbbb}{ab}_q \pmod{\mathfrak{M}}.$$

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

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

Ex: For $p = 2$, $\mathfrak{M} = q^2 + 1$, $A = \{a, b\}$ and $u = a$, we have $a \sim_{u,\mathfrak{M}} abbbbaa$ and $b \sim_{u,\mathfrak{M}} bb$:

$$\binom{a}{a}_q \equiv 1 \equiv \binom{abbbbaa}{a}_q \pmod{\mathfrak{M}} \quad \text{and} \quad \binom{b}{a}_q \equiv 0 \equiv \binom{bb}{a}_q \pmod{\mathfrak{M}}$$

but $ab \not\sim_{u,\mathfrak{M}} abbbbaabb$:

$$\binom{ab}{a}_q \equiv q \not\equiv 1 \equiv \binom{abbbbaabb}{a}_q \pmod{\mathfrak{M}}$$

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 $\sim_{u,\mathfrak{M}}$ II

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

Ex: For $p = 2$, $\mathfrak{M} = q^2 + 1$, $A = \{a, b\}$ and $u = a$, we have $a \sim_{u,\mathfrak{M}} abbbbaa$ and $b \sim_{u,\mathfrak{M}} bb$:

$$\binom{a}{a}_q \equiv 1 \equiv \binom{abbbbaa}{a}_q \pmod{\mathfrak{M}} \quad \text{and} \quad \binom{b}{a}_q \equiv 0 \equiv \binom{bb}{a}_q \pmod{\mathfrak{M}}$$

but $ab \not\sim_{u,\mathfrak{M}} abbbbaabb$:

$$\binom{ab}{a}_q \equiv q \not\equiv 1 \equiv \binom{abbbbaabb}{a}_q \pmod{\mathfrak{M}}$$

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 $\sim_{u,\mathfrak{M}}$ II

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

Ex: For $p = 2$, $\mathfrak{M} = q^2 + 1$, $A = \{a, b\}$ and $u = a$, we have $a \sim_{u,\mathfrak{M}} abbbbaa$ and $b \sim_{u,\mathfrak{M}} bb$:

$$\binom{a}{a}_q \equiv 1 \equiv \binom{abbbbaa}{a}_q \pmod{\mathfrak{M}} \quad \text{and} \quad \binom{b}{a}_q \equiv 0 \equiv \binom{bb}{a}_q \pmod{\mathfrak{M}}$$

but $ab \not\sim_{u,\mathfrak{M}} abbbbaabb$:

$$\binom{ab}{a}_q \equiv q \not\equiv 1 \equiv \binom{abbbbaabb}{a}_q \pmod{\mathfrak{M}}$$

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

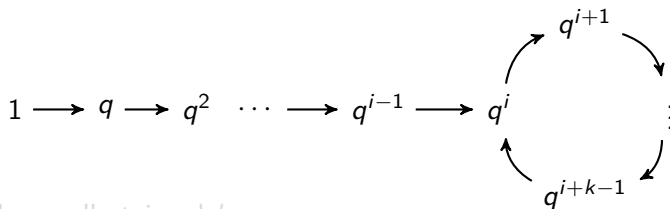
$$w_1 \cong w_2 \Rightarrow w_1 \sim_{u,\mathfrak{M}} w_2.$$

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 ,

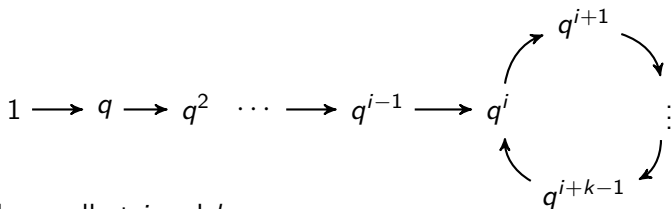
- i is the **index** of q ,
- k is the **period** of q .

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

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 ,

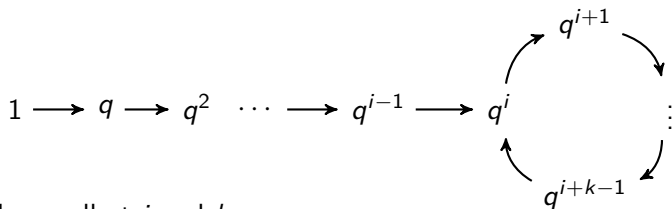
- i is the **index** of q ,
- k is the **period** of q .

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

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 $k = \text{ord}(q)$.

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 not a group. In particular, no element except for the identity is invertible.*

Why? We managed to show that for any congruence $\cong$ refining $\sim_{u,\mathfrak{M}}$, we have

$$w_1 \cong w_2 \Rightarrow |w_1| = |w_2| \text{ or } (|w_1|, |w_2| \geq \text{ind}(q) \wedge \dots)$$

So when q is not a unit of $\mathbb{K}$, $\text{ind}(q) \geq 1$, and $[\varepsilon]$ is a singleton, so that $[w] \cdot [x] = [wx] \neq [\varepsilon]$ for all $w, x \in A^+$.

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 not a group. In particular, no element except for the identity is invertible.*

Why? We managed to show that for any congruence $\cong$ refining $\sim_{u,\mathfrak{M}}$, we have

$$w_1 \cong w_2 \Rightarrow |w_1| = |w_2| \text{ or } (|w_1|, |w_2| \geq \text{ind}(q) \wedge \dots)$$

So when q is not a unit of $\mathbb{K}$, $\text{ind}(q) \geq 1$, and $[\varepsilon]$ is a singleton, so that $[w] \cdot [x] = [wx] \neq [\varepsilon]$ for all $w, x \in A^+$.

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 showed that $\sim_{u,\mathfrak{M}} \cap \sim_{\text{ord}(p)}$, where

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

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 $\text{ord}(q) \cdot p^{|u|}$.*

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 showed that $\sim_{u, \mathfrak{M}} \cap \sim_{\text{ord}(p)}$, where

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

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 $\text{ord}(q) \cdot p^{|u|}$.*

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 showed that $\sim_{u, \mathfrak{M}} \cap \sim_{\text{ord}(p)}$, where

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

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 $\text{ord}(q) \cdot p^{|u|}$.*

A beautiful example



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

A generalization of Eilenberg's theorem I

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.

Sketch of proof. Given such polynomial $\mathfrak{M}$, we have $\text{ind}(q) = 0$ and $\text{per}(q) = \text{ord}(q) = p^t$ for some integer $t > 0$. Thus, $A^* / \equiv_{u,\mathfrak{M}}$ is a p -group (since its order divides a power of p).

Now, considering

$$\pi : A^* \rightarrow A^* / \equiv_{u,\mathfrak{M}} : x \mapsto [x] \quad \text{and} \quad S = \left\{ [u] : \binom{u}{v}_q \equiv \mathfrak{R} \pmod{\mathfrak{M}} \right\},$$

we have $L_{v,\mathfrak{R},\mathfrak{M}} = \pi^{-1}(S)$.

A generalization of Eilenberg's theorem I

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.

Sketch of proof. Given such polynomial $\mathfrak{M}$, we have $\text{ind}(q) = 0$ and $\text{per}(q) = \text{ord}(q) = p^t$ for some integer $t > 0$. Thus, $A^* / \equiv_{u,\mathfrak{M}}$ is a p -group (since its order divides a power of p).

Now, considering

$$\pi : A^* \rightarrow A^* / \equiv_{u,\mathfrak{M}} : x \mapsto [x] \quad \text{and} \quad S = \left\{ [u] : \binom{u}{v}_q \equiv \mathfrak{R} \pmod{\mathfrak{M}} \right\},$$

we have $L_{v,\mathfrak{R},\mathfrak{M}} = \pi^{-1}(S)$.

A generalization of Eilenberg's theorem II

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

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

Sketch of proof. $\Rightarrow$ We showed that languages of the form $L_{v,r,p}$ are disjoint unions of languages of the form $L_{v,\mathfrak{R},\mathfrak{M}}$, for polynomials $\mathfrak{R}$ such that $\mathfrak{R}(1) = r$ modulo p .

$\Leftarrow$ Comes from the previous corollary.

A generalization of Eilenberg's theorem II

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

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

Sketch of proof. $\Rightarrow$ We showed that languages of the form $L_{v,r,p}$ are disjoint unions of languages of the form $L_{v,\mathfrak{R},\mathfrak{M}}$, for polynomials $\mathfrak{R}$ such that $\mathfrak{R}(1) = r$ modulo p .

$\Leftarrow$ Comes from the previous corollary.

An example

Taking back our example, we have

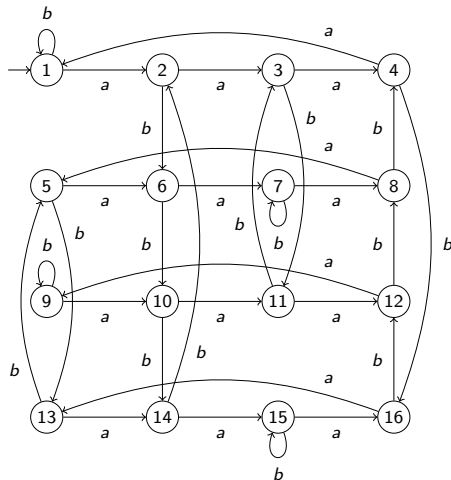
$$L_{v,0,2} = \{u \in A^* \mid \binom{u}{v}_q \equiv 0 \pmod{q^2 - 1}\} \\ \cup \{u \in A^* \mid \binom{u}{v}_q \equiv q + 1 \pmod{q^2 - 1}\},$$

since $q + 1$ at $q = 1$ evaluates to 0 modulo 2, and

$$L_{v,1,2} = \{u \in A^* \mid \binom{u}{v}_q \equiv 1 \pmod{q^2 - 1}\} \\ \cup \{u \in A^* \mid \binom{u}{v}_q \equiv q \pmod{q^2 - 1}\},$$

since q at $q = 1$ evaluates to 1 modulo 2.

Example of regular language



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

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?
- 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.
- q -Parikh matrices

Thank you for your attention!

q -shuffle I

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

Example:

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

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

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

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

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

q -shuffle II

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

Lemma (R., Rigo, Whiteland, 2023)

We have

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

q-shuffle: an example

Let's clarify with an example:

$$\begin{aligned}
 aba \sqcup_q aa &= q^6 \overline{aba}aa + q^5 \overline{ab}aaa + q^4 \overline{a}abaa + q^3 a\overline{aba}a + q^4 \overline{ab}aaa + \\
 &\quad q^3 \overline{a}abaa + q^2 a\overline{ab}aa + q^2 \overline{a}aaba + q a\overline{a}aba + 1 a\overline{a}aba. \\
 &= (q^6 + q^5 + q^4)aba^3 + (q^2 + 2q^3 + q^4)a^2ba^2 + \\
 &\quad (q^2 + q + 1)a^3ba
 \end{aligned}$$

→ 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

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

q -shuffle and q -binomial

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

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

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

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

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 $\alpha : A^* \times A^* \rightarrow \mathbb{N}$ 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

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

- 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

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