

q -deformations of binomial coefficients of words

Antoine Renard

Joint work with Michel Rigo and Markus A. Whiteland

Département de Mathématique, Université de Liège



11th April 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

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

Ex:

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

ab bab ab bab
 ab ba b ab ba b

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

→ *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:

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

→ *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:

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

→ ***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:

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

→ *We are going to mix these two!*

How to define this *q*-deformation?

Two recursive definitions for the "classical" coefficients:

Coefficients on words:

Gaussian coefficients:

$$\begin{pmatrix} ua \\ vb \end{pmatrix} = \begin{pmatrix} u \\ vb \end{pmatrix} + \delta_{a,b} \begin{pmatrix} u \\ v \end{pmatrix} \quad \begin{pmatrix} m+1 \\ r+1 \end{pmatrix}_q = \begin{pmatrix} m \\ r+1 \end{pmatrix}_q \cdot q^{r+1} + \begin{pmatrix} m \\ r \end{pmatrix}_q$$

→ *We are going to mix these two!*

How to define this *q*-deformation?

Two recursive definitions for the "classical" coefficients:

Coefficients on words:

Gaussian coefficients:

$$\begin{pmatrix} ua \\ vb \end{pmatrix} = \begin{pmatrix} u \\ vb \end{pmatrix} + \delta_{a,b} \begin{pmatrix} u \\ v \end{pmatrix} \quad \begin{pmatrix} m+1 \\ r+1 \end{pmatrix}_q = \begin{pmatrix} m \\ r+1 \end{pmatrix}_q \cdot q^{r+1} + \begin{pmatrix} m \\ r \end{pmatrix}_q$$

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

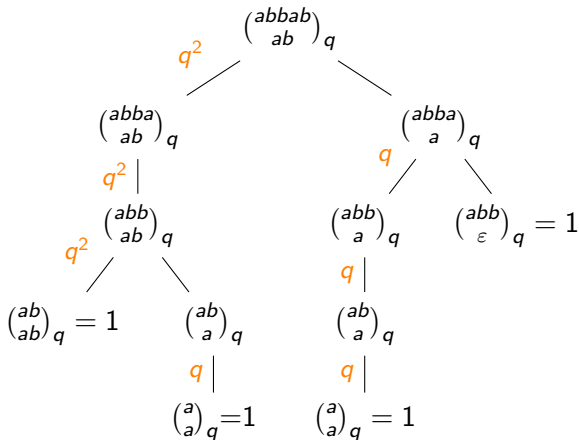
q -deformed binomial coefficients of words

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 $a, b \in A$,

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

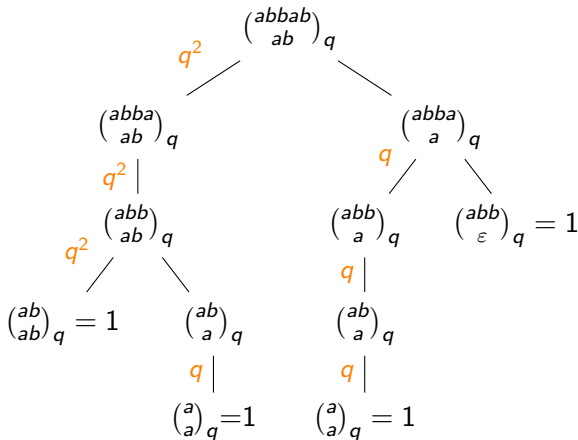
$$\binom{ua}{vb}_q = \binom{u}{vb}_q \cdot q^{|vb|} + \delta_{a,b} \binom{u}{v}_q.$$

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

In other words, the powers of q in $\binom{u}{v}_q$ encode the positions of letters of v of its occurrences in u .

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

Y	$(5, 4)$	$(5, 3)$	$(5, 1)$	$(2, 1)$
$s(Y) - 3$	6	5	3	0

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

In other words, the powers of q in $\binom{u}{v}_q$ encode the positions of letters of v of its occurrences in u .

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

Y	$(5, 4)$	$(5, 3)$	$(5, 1)$	$(2, 1)$
$s(Y) - 3$	6	5	3	0

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

In other words, the powers of q in $\binom{u}{v}_q$ encode the positions of letters of v of its occurrences in u .

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

Y	$(5, 4)$	$(5, 3)$	$(5, 1)$	$(2, 1)$
$s(Y) - 3$	6	5	3	0

Alternative interpretation I

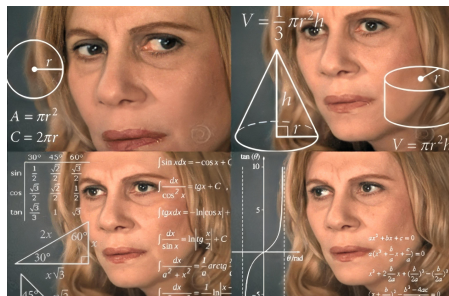
More "convenient" interpretation of the powers of q :

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 .

Alternative interpretation I

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 .



Alternative interpretation II

Let's clear this up using our example:

$$\begin{array}{c} \overline{ab}bab \\ \downarrow \\ q^{3+3} \end{array} + \begin{array}{c} a\overline{bb}ab \\ \downarrow \\ q^{2+3} \end{array} + \begin{array}{c} ab\overline{bab} \\ \downarrow \\ q^{0+3} \end{array} + \begin{array}{c} abb\overline{ab} \\ \downarrow \\ q^{0+0} \end{array} = \binom{abab}{ab}_q$$

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

Alternative interpretation II

Let's clear this up using our example:

$$\begin{array}{ccccccc}
 \textcolor{brown}{a}\textcolor{green}{b}\overline{\textcolor{brown}{b}\textcolor{green}{a}\textcolor{brown}{b}} & & \textcolor{brown}{a}\overline{\textcolor{brown}{b}\textcolor{green}{b}\textcolor{brown}{a}} & & \textcolor{brown}{a}\overline{\textcolor{brown}{b}\textcolor{green}{b}\textcolor{brown}{a}} & & \textcolor{brown}{a}\textcolor{green}{b}\textcolor{brown}{b}\textcolor{green}{a}\textcolor{brown}{b} \\
 \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 q^{3+\textcolor{green}{3}} & + & q^{2+\textcolor{green}{3}} & + & q^{0+\textcolor{green}{3}} & + & q^{0+0} = \left(\begin{smallmatrix} \textcolor{brown}{a}\textcolor{green}{b}\textcolor{brown}{a}\textcolor{green}{b} \\ \textcolor{brown}{a}\textcolor{green}{b} \end{smallmatrix} \right)_q
 \end{array}$$

→ 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. 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

- 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:

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

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

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

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

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 $\mathbb{N}[q]\langle\langle A^* \rangle\rangle$

→ not that convenient to compute...

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 $\mathbb{N}[q]\langle\langle A^* \rangle\rangle$

→ not that convenient to compute...

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 $\mathbb{N}[q]\langle\langle A^* \rangle\rangle$

→ not that convenient to compute...

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 $\mathbb{N}[q]\langle\langle A^* \rangle\rangle$

→ not that convenient to compute...

q -shuffle II

Lemma (R., Rigo, Whiteland, 2023)

We have

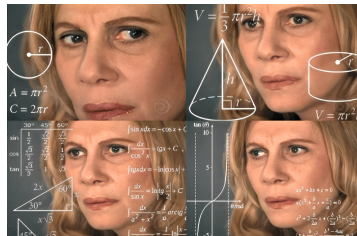
$$u \sqcup_q v = \sum_{\substack{u=u_1 \cdots u_n u_{n+1}, \ u_i \in A^* \\ v=v_1 \cdots v_n, \ v_i \in A}} \left(\prod_{i=1}^n q^{|u_1 \cdots u_i|} \right) u_1 v_1 u_2 v_2 \cdots u_n v_n u_{n+1}.$$

q -shuffle II

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:

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

→ 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: an example

Let's clarify with an example:

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

→ 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: an example

Let's clarify with an example:

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

→ 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 is defined recursively as follows:

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

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

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 is defined recursively as follows:

$$\begin{aligned} u \uparrow_q \varepsilon &= \varepsilon \uparrow_q u = 1 \cdot u, \\ ua \uparrow_q vb &= (u \uparrow_q vb)a + q^{|ua|} [(ua \uparrow_q v)b + \delta_{a,b}(u \uparrow_q v)a]. \end{aligned}$$

Some properties of q -infiltration

We have some interesting properties:

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

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

Moreover, $P_{u,v} = 0$ if and only if u and v are on disjoint alphabets.

- Let u, v, w be words such that $|u| \geq |v|, |w|$. We have

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

However, we can't generalize the Chen-Fox-Lyndon relation

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

even if we consider a generalized definition of $\uparrow_q$

Some properties of q -infiltration

We have some interesting properties:

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

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

Moreover, $P_{u,v} = 0$ if and only if u and v are on disjoint alphabets.

- Let u, v, w be words such that $|u| \geq |v|, |w|$. We have

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

However, we can't generalize the Chen-Fox-Lyndon relation

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

even if we consider a generalized definition of $\uparrow_q$:

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 **recognizable** if and only if there exist

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

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

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

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

Recognizable and p -group languages

Recall that a language is **recognizable** if and only if there exist

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

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

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

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

Recognizable and p -group languages

Recall that a language is **recognizable** if and only if there exist

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

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

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

→ ***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 $\mathfrak{M}(q)$ 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 $\mathfrak{M}(q)$ 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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.

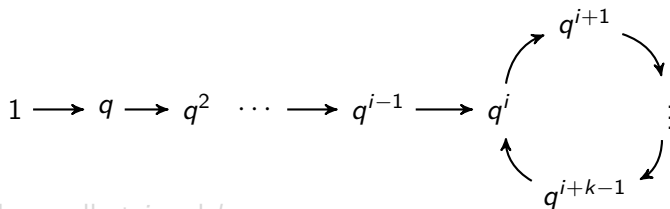
$$w_1 \cong w_2 \Rightarrow w_1 \sim_{u,\mathfrak{M}} w_2.$$

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 ,

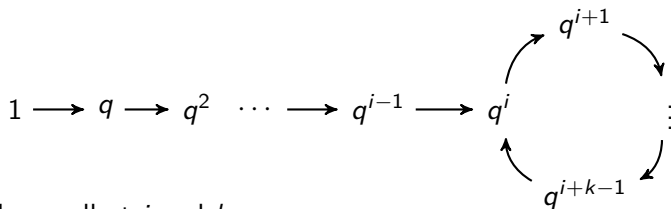
- i is the *index* of q ,
- k is the *period* of q .

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

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 ,

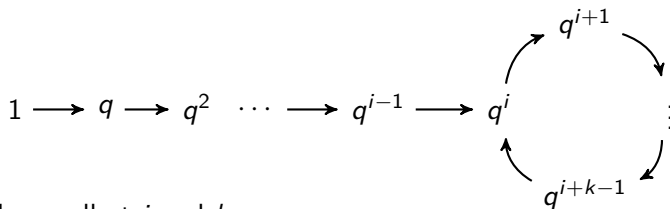
- i is the **index** of q ,
- k is the **period** of q .

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 $A^*/\cong$

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.*

If q is a unit of $\mathbb{K}$, we can show that $\sim_{u,\mathfrak{M}} \cap \sim_{\text{ord}(p)}$, where

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

is a congruence. We denote it $\equiv_{u,\mathfrak{M}}$, and it can be shown that this 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 $A^*/\cong$

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.*

If q is a unit of $\mathbb{K}$, we can show that $\sim_{u,\mathfrak{M}} \cap \sim_{\text{ord}(p)}$, where

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

is a congruence. We denote it $\equiv_{u,\mathfrak{M}}$, and it can be shown that this 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 $A^*/\cong$

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.*

If q is a unit of $\mathbb{K}$, we can show that $\sim_{u,\mathfrak{M}} \cap \sim_{\text{ord}(p)}$, where

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

is a congruence. We denote it $\equiv_{u,\mathfrak{M}}$, and it can be shown that this 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

Corollary (R., Rigo, Whiteland, 2023)

Let v be a word and $\mathfrak{N} = q^{p^t} - 1$ for some integer $t \geq 1$. The language $L_{v, \mathfrak{N}, \mathfrak{N}}$ is a p -group language.

Theorem (R., Rigo, Whiteland, 2023)

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

$$L_{v, \mathfrak{R}, q^p - 1} = \{u \in A^* \mid \binom{u}{v}_q \equiv \mathfrak{R} \pmod{q^p - 1}\}.$$

Sketch of proof. $\Leftarrow$ Comes from the corollary.

$\Rightarrow$ We can show that languages $L_{v, r, p}$ are finite unions of languages of the form $L_{v, \mathfrak{R}, q^p - 1}$.

A generalization of Eilenberg's theorem

Corollary (R., Rigo, Whiteland, 2023)

Let v be a word and $\mathfrak{N} = q^{p^t} - 1$ for some integer $t \geq 1$. The language $L_{v, \mathfrak{N}, \mathfrak{N}}$ is a p -group language.

Theorem (R., Rigo, Whiteland, 2023)

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

$$L_{v, \mathfrak{N}, q^p - 1} = \{u \in A^* \mid \binom{u}{v}_q \equiv \mathfrak{N} \pmod{q^p - 1}\}.$$

Sketch of proof. $\Leftarrow$ Comes from the corollary.

$\Rightarrow$ We can show that languages $L_{v, r, p}$ are finite unions of languages of the form $L_{v, \mathfrak{N}, q^p - 1}$.

A generalization of Eilenberg's theorem

Corollary (R., Rigo, Whiteland, 2023)

Let v be a word and $\mathfrak{N} = q^{p^t} - 1$ for some integer $t \geq 1$. The language $L_{v, \mathfrak{N}, \mathfrak{N}}$ is a p -group language.

Theorem (R., Rigo, Whiteland, 2023)

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

$$L_{v, \mathfrak{N}, q^p - 1} = \{u \in A^* \mid \binom{u}{v}_q \equiv \mathfrak{N} \pmod{q^p - 1}\}.$$

Sketch of proof. $\Leftarrow$ Comes from the corollary.

$\Rightarrow$ We can show that languages $L_{v, r, p}$ are finite unions of languages of the form $L_{v, \mathfrak{N}, q^p - 1}$.

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?

Thank you for your attention!