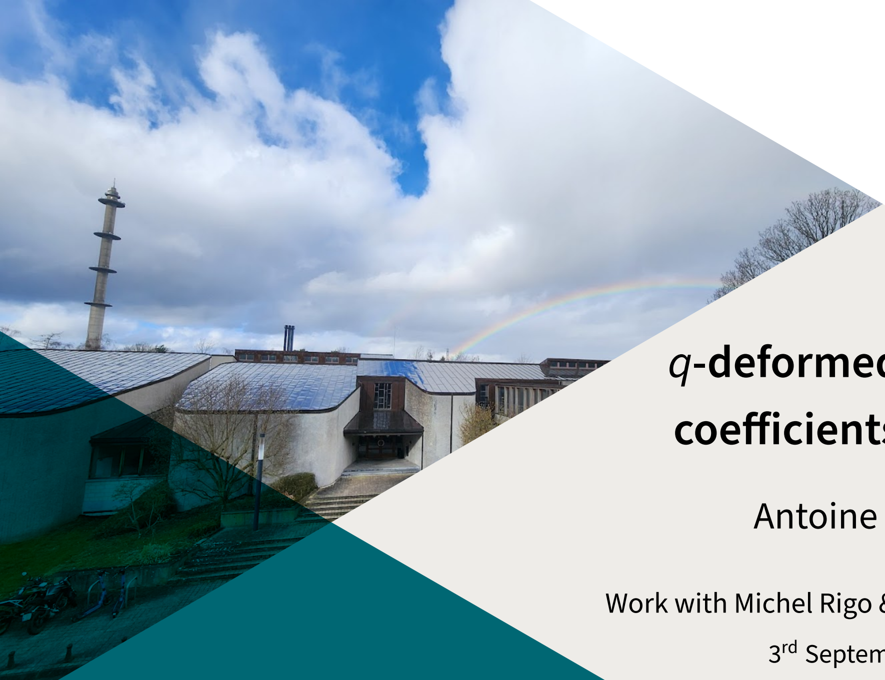


q-deformed binomial coefficients of words

Antoine Renard

Work with Michel Rigo & Markus A. Whiteland

3rd September 2024

Overview

1. Definition and examples
2. Combinatorial interpretation
3. *p*-group languages
4. *q*-Parikh matrices

Definition and examples

Definition and examples

q-deformations

A ***q-deformation*** or ***q-analog*** is a generalisation of some mathematical object involving a new parameter q, such that the limit for $q \to 1$ gives back the original object.

Definition and examples

q-deformations

A ***q-deformation*** or ***q-analog*** is a generalisation of some mathematical object involving a new parameter q, such that the limit for $q \to 1$ gives back the original object.

Ex:

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

Definition and examples

q-deformations

A ***q-deformation*** or ***q-analog*** is a generalisation of some mathematical object involving a new parameter q, such that the limit for $q \to 1$ gives back the original object.

Ex:

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

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

Definition and examples

Binomial coefficients

The ***binomial coefficient*** $\binom{u}{v}$ of two words counts the number of occurrences of v as a subword of u

Ex:

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

$abbab \quad abbab$

$abbab \quad abbab$

Definition and examples

Binomial coefficients

The ***binomial coefficient*** $\binom{u}{v}$ of two words counts the number of occurrences of v as a subword of u

Ex:

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

$abbab \quad abbab$

$abbab \quad abbab$

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

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

$\rightarrow$ counts the number of subspaces of dimension k in a vector space of dimension n over $\mathbb{F}_q$.

Definition and examples

Binomial coefficients

The ***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:

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

$\rightarrow$ counts the number of subspaces of dimension k in a vector space of dimension n over $\mathbb{F}_q$.

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

Definition and examples

q-deformed binomial coefficients of words

Two recursive definitions for the "classical" coefficients:

Definition and examples

q-deformed binomial coefficients of words

Two recursive definitions for the “classical” coefficients:

Coefficients on words:

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

Gaussian coefficients:

$$\binom{n+1}{k+1}_q = \binom{n}{k+1}_q \cdot q^{k+1} + \binom{n}{k}_q$$

Definition and examples

q-deformed binomial coefficients of words

Two recursive definitions for the "classical" coefficients:

Coefficients on words:

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

Gaussian coefficients:

$$\binom{n+1}{k+1}_q = \binom{n}{k+1}_q \cdot q^{k+1} + \binom{n}{k}_q$$

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

Definition and examples

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 $a, b \in A$ (where A is a finite alphabet),

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

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

Definition and examples

Basic properties

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

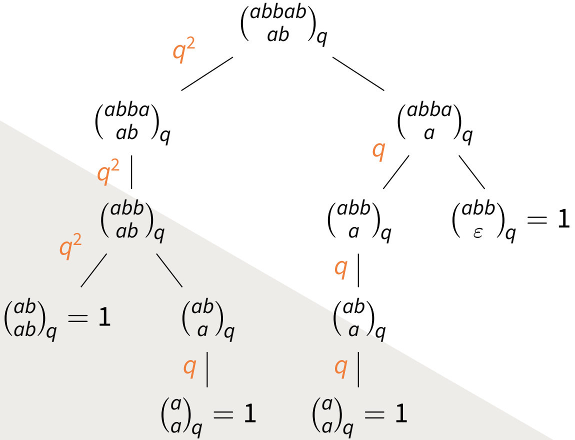
- $\binom{u}{u}_q = 1$,
- $\binom{u}{v}_q = 0 \Leftrightarrow v$ does not occur as a subword of u.

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

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

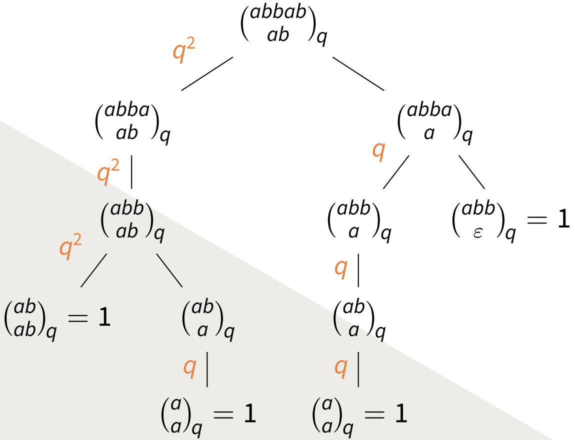
Definition and examples

Example: an easy way to compute q-binomials



Definition and examples

Example: an easy way to compute q-binomials



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

Combinatorial interpretation

Combinatorial interpretation

Main result

Theorem (R., Rigo, Whiteland, 2024)

Let u be a word over A, $k \geq 0$, and $a_1, \ldots, a_k \in A$. Then

$$\binom{u}{a_1 \cdots a_k}_q = \sum_{\substack{u_0, u_1, \ldots, u_k \in A^* \\ u = u_0 a_1 \cdots u_{k-1} a_k u_k}} q^{\sum_{i=1}^{k} i|u_i|}.$$

Combinatorial interpretation

Main result

If we take back our favourite example

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

we have to consider all factorisations of *abbab* of the form $u_0 a u_1 b u_2$:

	abbab	*abbab*	*abbab*	*abbab*
(u_1, u_2)	(ε, bab)	(b, ab)	(bba, ε)	$(\varepsilon, \varepsilon)$
$\lvert u_1\rvert + 2\lvert u_2\rvert$	6	5	3	0

Combinatorial interpretation

Main result

In other words, for a fixed occurrence of v in u, one has to count, for each letter of v, the number of letters of u that are at its right and not part of this specific occurrence. Summing these numbers gives the corresponding power of q.

Combinatorial interpretation

Main result

In other words, for a fixed occurrence of v in u, one has to count, for each letter of v, the number of letters of u that are at its right and not part of this specific occurrence. Summing these numbers gives the corresponding power of q.

To quote a famous Swedish band, “here I go again”:

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

Combinatorial interpretation

Main result

In other words, for a fixed occurrence of v in u, one has to count, for each letter of v, the number of letters of u that are at its right and not part of this specific occurrence. Summing these numbers gives the corresponding power of q.

To quote a famous Swedish band, “here I go again”:

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

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

Combinatorial interpretation

Information within the coefficients

From the combinatorial interpretation, we get some information about coefficients.

Corollary (R., Rigo, Whiteland, 2024)

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,

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

p-group languages

p-group languages

Definitions

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

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

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

p-group languages

Definitions

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

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

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

The language L is said to be ***recognisable*** if it is recognised by a <u>finite</u> monoid.

p-group languages

Definitions

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

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

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

The language L is said to be ***recognisable*** if it is recognised by a finite monoid.

Finally, a language recognised 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.

p-group languages

Definitions

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

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

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

The language L is said to be ***recognisable*** if it is recognised by a finite monoid.

Finally, a language recognised 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.

N.B.: Regular languages = recognisable languages

p-group languages

Characterising 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

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

p-group languages

Characterising 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

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

Theorem (R., Rigo, Whiteland, 2024)

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

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

q-Parikh matrices

q-Parikh matrices

"Classical" Parikh matrices

Introduced by Şerbănuţă in 2004, *Parikh matrices induced by a word* $z = z_1 \cdots z_n$ are upper triangular matrices of size $(n+1) \times (n+1)$, containing elements of the form $\binom{u}{v}$ for words v of the form $z_i \, z_{i+1} \cdots z_j$, $1 \leq i \leq j \leq |z|$.

q-Parikh matrices

"Classical" Parikh matrices

Introduced by Şerbănuţă in 2004, ***Parikh matrices induced by a word*** $z = z_1 \cdots z_n$ are upper triangular matrices of size $(n+1) \times (n+1)$, containing elements of the form $\binom{u}{v}$ for words v of the form $z_i\, z_{i+1} \cdots z_j$, $1 \leq i \leq j \leq |z|$.

The Parikh matrix mapping is a monoid morphism $\Psi_{A,z} : A^* \to \mathbb{N}^{(n+1)\times(n+1)}$ defined by

$$[\Psi_{A,z}(a)]_{i,j} = \begin{cases} 1 & j = i \\ \delta_{a,z_i} & j = i+1 \\ 0 & \text{otherwise} \end{cases} \qquad \text{for all } a \in A.$$

q-Parikh matrices

An example

Fix $z = aba$ and $u = abbaba$. We have

$$\Psi_{A,z}(a) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \Psi_{A,z}(b) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

so that $\Psi_{A,z}(u) = \Psi_{A,z}(a)\Psi_{A,z}(b)\Psi_{A,z}(b)\Psi_{A,z}(a)\Psi_{A,z}(b)\Psi_{A,z}(a)$, *i.e.*

$$\Psi_{A,z}(u) = \begin{pmatrix} 1 & 3 & 4 & 6 \\ 0 & 1 & 3 & 5 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \binom{u}{a} & \binom{u}{ab} & \binom{u}{aba} \\ 0 & 1 & \binom{u}{b} & \binom{u}{ba} \\ 0 & 0 & 1 & \binom{u}{a} \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

q-Parikh matrices

q-deformed Parikh matrices

Let $z = z_1 \cdots z_n$ be a word and A be the alphabet of z, *i.e.* the set of letters occurring in z. For $a \in A$ and $\ell \geq 0$, we let $\mathcal{M}_{a,\ell}$ denote the upper triangular matrix defined by

$$[\mathcal{M}_{a,\ell}]_{i,j} = \begin{cases} 1 & j = i \\ \delta_{a,z_i} q^\ell & j = i+1 \\ 0 & \text{otherwise} \end{cases} .$$

We now define the map

$$\mathcal{P}_z : A^* \to (\mathbb{N}[q])^{(n+1)\times(n+1)} : u_k u_{k-1} \cdots u_1 u_0 \mapsto \mathcal{M}_{u_k,k} \cdots \mathcal{M}_{u_0,0}.$$

q-Parikh matrices

q-deformed Parikh matrices

Let $z = z_1 \cdots z_n$ be a word and A be the alphabet of z, *i.e.* the set of letters occurring in z.
For $a \in A$ and $\ell \geq 0$, we let $\mathcal{M}_{a,\ell}$ denote the upper triangular matrix defined by

$$[\mathcal{M}_{a,\ell}]_{i,j} = \begin{cases} 1 & j = i \\ \delta_{a,z_i} q^\ell & j = i+1 \\ 0 & \text{otherwise} \end{cases}.$$

We now define the map

$$\mathcal{P}_z : A^* \to (\mathbb{N}[q])^{(n+1)\times(n+1)} : u_k u_{k-1} \cdots u_1 u_0 \mapsto \mathcal{M}_{u_k,k} \cdots \mathcal{M}_{u_0,0}.$$

Unfortunately, **this is not a monoid morphism anymore**.

q-Parikh matrices

q-deformed Parikh matrices

Here, we have the following:

Theorem (R., Rigo, Whiteland, 2024)

Let z be a word of length $n \geq 1$ whose alphabet is A. Let $u \in A^*$. The corresponding $(n+1) \times (n+1)$ q-Parikh matrix is such that

- $[\mathcal{P}_z(u)]_{i,j} = 0$, *for all* $1 \leq j < i \leq n+1$,
- $[\mathcal{P}_z(u)]_{i,i} = 1$, *for all* $1 \leq i \leq n+1$.
- *Let* $r \in \{1, \dots, n\}$. *For all* $1 \leq i \leq n-r+1$, $[\mathcal{P}_z(u)]_{i,i+r} = q^{\mathrm{s}(r-1)} \binom{u}{z_i\, z_{i+1} \cdots z_{i+r-1}}_q$, *where* $\mathrm{s}(\ell) = \sum_{k=1}^{\ell} k$.

q-Parikh matrices

An example (again)

Back with our friends $z = aba$ and $u = abbaba$, we have

$$\mathcal{M}_{a,\ell} = \begin{pmatrix} 1 & q^\ell & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & q^\ell \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathcal{M}_{b,\ell} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & q^\ell & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

q-Parikh matrices

An example (again)

Thus,

$$\mathcal{P}_z(u) = \mathcal{M}_{a,5}\mathcal{M}_{b,4}\mathcal{M}_{b,3}\mathcal{M}_{a,2}\mathcal{M}_{b,1}\mathcal{M}_{a,0}$$

$$= \begin{pmatrix} 1 & q^5+q^2+1 & q^9+q^8+q^6+q^3 & q^{11}+q^{10}+q^9+q^8+q^6+q^3 \\ 0 & 1 & q^4+q^3+q & q^6+q^5+q^4+q^3+q \\ 0 & 0 & 1 & q^5+q^2+1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \binom{u}{a}_q & q\binom{u}{ab}_q & q^3\binom{u}{aba}_q \\ 0 & 1 & \binom{u}{b}_q & q\binom{u}{ba}_q \\ 0 & 0 & 1 & \binom{u}{a}_q \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

q-Parikh matrices

Consequences

- Alternative way to compute q-binomials;
- New identities, *e.g.*

$$\sum_{\substack{z=xy \\ x,y\in A^*}} (-1)^{|y|} q^{\mathsf{s}(|x|-1)+\mathsf{s}(|y|-1)} \binom{u}{x}_q \binom{u}{\widetilde{y}}_q = 0$$

  for words z with no equal consecutive letters;
- Information on the behaviour of $\binom{u^n}{z}_q$ as $n \to +\infty$: converges to a formal power series whose coefficients can be effectively computed;
- etc.

Thank you for your attention!

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):

$$aabaaa \quad \text{and} \quad aabaaa \longrightarrow 2q^4$$
$$aabaaa \quad \text{and} \quad aabaaa \longrightarrow 2q^5$$

Reconstructing words

Theorem (R., Rigo, Whiteland, 2024)

Let k be an integer, u, x words such that $|u| \geq k \geq |x|$. We have

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

Corollary (R., Rigo, Whiteland, 2024)

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.

p-groups

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.

p-groups

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

p-groups

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 $a \sim_{u,\mathfrak{M}} abbbaa$ and $b \sim_{u,\mathfrak{M}} bb$:

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

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

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

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

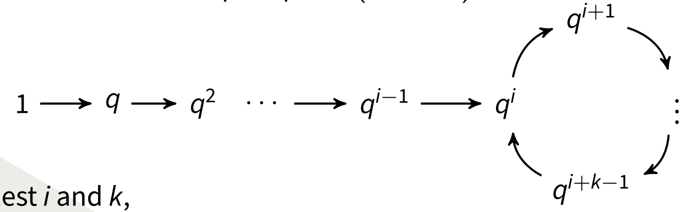
$$w_1 \cong w_2 \Rightarrow w_1 \sim_{u,\mathfrak{M}} w_2.$$

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

p-groups

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

p-groups

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

Proposition (R., Rigo, Whiteland, 2024)

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.

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

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

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

p-groups

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

We showed that $\sim_{u,\mathfrak{M}} \cap \sim_{\mathrm{ord}(p)}$, 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, 2024)

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

p-groups

Corollary (R., Rigo, Whiteland, 2024)

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

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

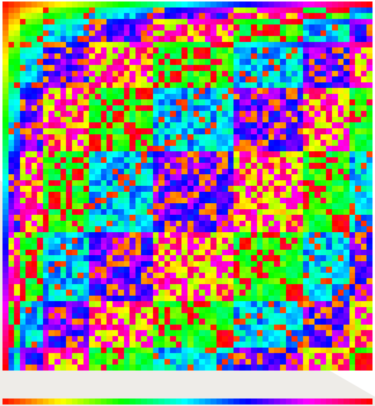
is a p-group language.

Theorem (R., Rigo, Whiteland, 2024))

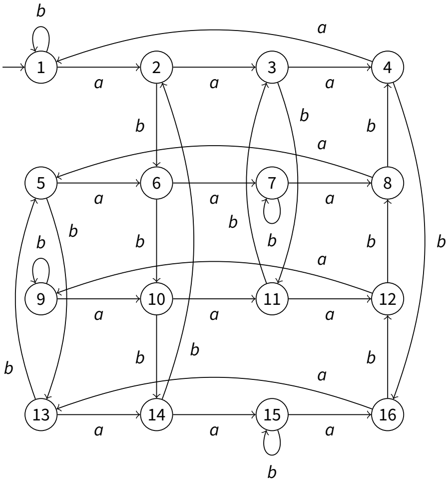
Let p be a prime and $\mathfrak{M} = a(q-1)^d$ with $d \geq 1$ an integer. A language is a p-group language if and only if it is a Boolean combination of languages of the form

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

p-groups



$$\{a,b\}^*/\sim_{ab,q^2+1}$$



$$L_{ab,\mathfrak{R},q^2+1}$$