Word Equations and Straight-Line Programs
Lecture 2: Various results for word equations

Artur Jeż

University of Wrocław

PhD Open
Warsaw 26.11.2021

Exponent of peridiocity

Definition (Exponent of periodicity)

For a word w, the exponent of periodicty $\mathrm{per}(w)$:
maximal k such that u^k is a substring of w (and $u \neq \varepsilon$).

Exponent of peridiocity

Definition (Exponent of periodicity)

For a word w, the exponent of periodicty $\mathrm{per}(w)$:
maximal k such that u^k is a substring of w (and $u \neq \varepsilon$).
Exponent of periodicity of an equation $U = V$:

$$\max\{\mathrm{per}(S(U)) \ : \ S \text{ is a length-minimal solution}\} \ .$$

Exponent of peridiocity

Definition (Exponent of periodicity)

For a word w, the exponent of periodicty $\mathrm{per}(w)$:
maximal k such that u^k is a substring of w (and $u \neq \varepsilon$).
Exponent of periodicity of an equation $U = V$:

$$\max\{\mathrm{per}(S(U)) \ : \ S \text{ is a length-minimal solution}\} \ .$$

Theorem (Kościelski, Pacholski '90)

The exponent of periodicity of a word equation is

$$|UV| \cdot e^{\mathcal{O}(|UV|)}$$

Exponent of peridiocity

Definition (Exponent of periodicity)

For a word w, the exponent of periodicty $\mathrm{per}(w)$:
maximal k such that u^k is a substring of w (and $u \neq \varepsilon$).
Exponent of periodicity of an equation $U = V$:

$$\max\{\mathrm{per}(S(U)) \ : \ S \text{ is a length-minimal solution}\} \ .$$

Theorem (Kościelski, Pacholski '90)

The exponent of periodicity of a word equation is

$$|UV| \cdot e^{\mathcal{O}(|UV|)}$$

Remark

An exponential lower bound clearly holds.

Maximal blocks

Remark

We are only using the bound, when the u is a letter (when bounding the length of maximal blocks).

Maximal blocks

Remark

We are only using the bound, when the u is a letter (when bounding the length of maximal blocks).

For the rest of the lecture: fix a length-minimal solution S and a letter a.

Maximal blocks

Remark

We are only using the bound, when the u is a letter (when bounding the length of maximal blocks).

For the rest of the lecture: fix a length-minimal solution S and a letter a.
ℓ_X, r_X: the lengths of the a-prefix and a-suffix of $S(X)$, for each variable X.

Maximal blocks

Remark

We are only using the bound, when the u is a letter (when bounding the length of maximal blocks).

For the rest of the lecture: fix a length-minimal solution S and a letter a.
ℓ_X, r_X: the lengths of the a-prefix and a-suffix of $S(X)$, for each variable X.
It could be that $\ell_X = 0$ or $r_X = 0$.
Convention: when $S(X)$ is an a-block then $r_X = 0$.

Maximal blocks

Remark

We are only using the bound, when the u is a letter
(when bounding the length of maximal blocks).

For the rest of the lecture: fix a length-minimal solution S and a letter a.
ℓ_X, r_X: the lengths of the a-prefix and a-suffix of $S(X)$, for each variable X.
It could be that $\ell_X = 0$ or $r_X = 0$.
Convention: when $S(X)$ is an a-block then $r_X = 0$.

If S is a length-minimal solution and e is a length of maximal a-block, then a^e has a maximal occurrence touching a cut.
(So using an explicit letter or an a-prefix or suffix). (Exercise)
In particular, there are at most $2|UV|$ such lengths.

Consider an equation

$$XabXXa = aXbYYY \ .$$

It is easy to show that the solutions of of the form $S(X) = a^{\ell_X}, S(Y) = a^{\ell_Y}$ if and only if

$$2\ell_X + 1 = 3\ell_Y \ .$$

Consider an equation

$$XabXXa = aXbYYY \ .$$

It is easy to show that the solutions of of the form $S(X) = a^{\ell_X}, S(Y) = a^{\ell_Y}$ if and only if

$$2\ell_X + 1 = 3\ell_Y \ .$$

The lengths are "arithmetic expressions" parametrized by lengths of a-prefixes and suffixes and those satisfy some system of linear equations.

Arithmetic expressions

Let $e_1, \ldots e_k$ be the lengths of maximal a blocks touching a cut in $S(U), S(V)$ in a left-to-right order, including the duplicates.

Arithmetic expressions

Let $e_1, \ldots e_k$ be the lengths of maximal a blocks touching a cut in $S(U), S(V)$ in a left-to-right order, including the duplicates.

Construct a set of arithmetic expressions in variables $\{L_X, R_X\}_{X \in \mathcal{X}}$, s.t.:

Arithmetic expressions

Let $e_1, \dots e_k$ be the lengths of maximal a blocks touching a cut in $S(U), S(V)$ in a left-to-right order, including the duplicates.

Construct a set of arithmetic expressions in variables $\{L_X, R_X\}_{X \in \mathcal{X}}$, s.t.:

- addition, positive constants, variables $\{L_X, R_X\}_{X \in \mathcal{X}}$ (multiplied by positive constants)

Arithmetic expressions

Let $e_1, \dots e_k$ be the lengths of maximal a blocks touching a cut in $S(U), S(V)$ in a left-to-right order, including the duplicates.

Construct a set of arithmetic expressions in variables $\{L_X, R_X\}_{X \in \mathcal{X}}$, s.t.:

- addition, positive constants, variables $\{L_X, R_X\}_{X \in \mathcal{X}}$ (multiplied by positive constants)
- the sum of constants in those expressions is at most $|UV|$
- the sum of constants at variable L_X (R_X) is $\leq |UV|_X$.

Arithmetic expressions

Let $e_1, \ldots e_k$ be the lengths of maximal a blocks touching a cut in $S(U), S(V)$ in a left-to-right order, including the duplicates.

Construct a set of arithmetic expressions in variables $\{L_X, R_X\}_{X \in \mathcal{X}}$, s.t.:

- addition, positive constants, variables $\{L_X, R_X\}_{X \in \mathcal{X}}$ (multiplied by positive constants)
- the sum of constants in those expressions is at most $|UV|$
- the sum of constants at variable L_X (R_X) is $\leq |UV|_X$.

$2L_X + 1$, $3L_Y$

Arithmetic expressions

Let $e_1, \dots e_k$ be the lengths of maximal a blocks touching a cut in $S(U), S(V)$ in a left-to-right order, including the duplicates.

Construct a set of arithmetic expressions in variables $\{L_X, R_X\}_{X \in \mathcal{X}}$, s.t.:

- addition, positive constants, variables $\{L_X, R_X\}_{X \in \mathcal{X}}$ (multiplied by positive constants)
- the sum of constants in those expressions is at most $|UV|$
- the sum of constants at variable L_X (R_X) is $\leq |UV|_X$.

$2L_X + 1$, $3L_Y$

For E depending on $\{L_X, R_X\}_{X \in \mathcal{X}}$
$E[\{\ell_X, r_X\}_{X \in \mathcal{X}}]$: the value obtained by substituting $\{\ell_X, r_X\}_{X \in \mathcal{X}}$ (positive natural numbers) for the variables.

Arithmetic expressions

Let $e_1, \dots e_k$ be the lengths of maximal a blocks touching a cut in $S(U), S(V)$ in a left-to-right order, including the duplicates.

Construct a set of arithmetic expressions in variables $\{L_X, R_X\}_{X \in \mathcal{X}}$, s.t.:

- addition, positive constants, variables $\{L_X, R_X\}_{X \in \mathcal{X}}$ (multiplied by positive constants)
- the sum of constants in those expressions is at most $|UV|$
- the sum of constants at variable L_X (R_X) is $\leq |UV|_X$.

$2L_X + 1,\ 3L_Y$

For E depending on $\{L_X, R_X\}_{X \in \mathcal{X}}$
$E[\{\ell_X, r_X\}_{X \in \mathcal{X}}]$: the value obtained by substituting $\{\ell_X, r_X\}_{X \in \mathcal{X}}$ (positive natural numbers) for the variables.

$2L_X + 1[L_X = \ell_X] = 2\ell_X + 1,\ 3L_Y[L_Y = 1] = 3$

Construction of expressions

A system of arithmetic expressions for $U = V$ and S:

- list the lengths of a-blocks touching a cut in $S(u)$ and $S(v)$: $e_1, \ldots, e_k$

Construction of expressions

A system of arithmetic expressions for $U = V$ and S:

- list the lengths of a-blocks touching a cut in $S(u)$ and $S(v)$: $e_1, \ldots, e_k$
- create expressions $E_1, \ldots, E_k$:

Construction of expressions

A system of arithmetic expressions for $U = V$ and S:

- list the lengths of a-blocks touching a cut in $S(u)$ and $S(v)$: $e_1, \ldots, e_k$
- create expressions $E_1, \ldots, E_k$:
- if e_i includes a prefix/suffix ℓ_X / r_X then include L_X / R_X in E_i.
  When e_i spans (in total) over m explicit letters a then add m to E_i.

Construction of expressions

A system of arithmetic expressions for $U = V$ and S:

- list the lengths of a-blocks touching a cut in $S(u)$ and $S(v)$: $e_1, \ldots, e_k$
- create expressions $E_1, \ldots, E_k$:
- if e_i includes a prefix/suffix ℓ_X / r_X then include L_X / R_X in E_i.
  When e_i spans (in total) over m explicit letters a then add m to E_i.

$$XabXXa = aXbYYY$$

yields $L_X + 1, 2L_X + 1, L_X + 1, 3L_Y$

Construction of expressions

A system of arithmetic expressions for $U = V$ and S:

- list the lengths of a-blocks touching a cut in $S(u)$ and $S(v)$: $e_1, \ldots, e_k$
- create expressions $E_1, \ldots, E_k$:
- if e_i includes a prefix/suffix ℓ_X / r_X then include L_X / R_X in E_i. When e_i spans (in total) over m explicit letters a then add m to E_i.

$$XabXXa = aXbYYY$$

yields $L_X + 1, 2L_X + 1, L_X + 1, 3L_Y$

Lemma

For a given word equation $U = V$ with variables $\mathcal{X}$ and lengths of touching blocks e_1, e_2, $\ldots$, e_k the constructed set of arithmetic expressions E_1, E_2, $\ldots$, E_k in variables $\{L_X, R_X\}_{X \in \mathcal{X}}$ satisfies the conditions given earlier. Moreover $e_i = E_i[\{\ell_X, r_X\}_{X \in \mathcal{X}}]$, where ℓ_X and r_X are the lengths of the a-prefix and a-suffix of $S(X)$.

Proof sketch

- addition, positive constants, variables $\{L_X, R_X\}_{X \in \mathcal{X}}$ (multiplied by positive constants)

Proof sketch

- addition, positive constants, variables $\{L_X, R_X\}_{X \in \mathcal{X}}$ (multiplied by positive constants)
- the sum of constants in those expressions is at most $|UV|$: we add 1 for each letter

Proof sketch

- addition, positive constants, variables $\{L_X, R_X\}_{X \in \mathcal{X}}$ (multiplied by positive constants)
- the sum of constants in those expressions is at most $|UV|$: we add 1 for each letter
- the sum of constants at variable L_X (R_X) is $\leq |UV|_X$: each a-prefix/suffix is considered once

Proof sketch

- addition, positive constants, variables $\{L_X, R_X\}_{X \in \mathcal{X}}$ (multiplied by positive constants)
- the sum of constants in those expressions is at most $|UV|$: we add 1 for each letter
- the sum of constants at variable L_X (R_X) is $\leq |UV|_X$: each a-prefix/suffix is considered once
- $e_i = E_i[\{\ell_X, r_X\}_{X \in \mathcal{X}}]$: we added L_X for ℓ_X, now re replace back

Constructing a system of equations

Given an equation $U = V$, a length-minimal solution S,
let $e_1, \ldots, e_k$ and $E_1, \ldots, E_k$ be as stated before.

Constructing a system of equations

Given an equation $U = V$, a length-minimal solution S,
let $e_1, \ldots, e_k$ and $E_1, \ldots, E_k$ be as stated before.

Construct a system of Diophantine equations:

- if $e_i = e_j$ then we add equation $E_i = Ej$
- remove useless equations (so $E_1 = E_2$, $E_2 = E_3$, $E_1 = E_3$ can loose an equation)
- add an equation $R_X = 0$ ($L_X = 0$) when $r_X = 0$ ($\ell_X = 0$)
- add inequality $r_X > 0$ ($\ell_X > 0$) otherwise.

Constructing a system of equations

Given an equation $U = V$, a length-minimal solution S,
let $e_1, \ldots, e_k$ and $E_1, \ldots, E_k$ be as stated before.

Construct a system of Diophantine equations:

- if $e_i = e_j$ then we add equation $E_i = Ej$
- remove useless equations (so $E_1 = E_2$, $E_2 = E_3$, $E_1 = E_3$ can loose an equation)
- add an equation $R_X = 0$ ($L_X = 0$) when $r_X = 0$ ($\ell_X = 0$)
- add inequality $r_X > 0$ ($\ell_X > 0$) otherwise.

Lemma

$\{\ell_X, r_X\}_{X \in \mathcal{X}}$ is a solution of the constructed system.

Constructing a system of equations

Given an equation $U = V$, a length-minimal solution S,
let $e_1, \ldots, e_k$ and $E_1, \ldots, E_k$ be as stated before.

Construct a system of Diophantine equations:

- if $e_i = e_j$ then we add equation $E_i = Ej$
- remove useless equations (so $E_1 = E_2$, $E_2 = E_3$, $E_1 = E_3$ can loose an equation)
- add an equation $R_X = 0$ ($L_X = 0$) when $r_X = 0$ ($\ell_X = 0$)
- add inequality $r_X > 0$ ($\ell_X > 0$) otherwise.

Lemma

$\{\ell_X, r_X\}_{X \in \mathcal{X}}$ is a solution of the constructed system.

Proof.

Recall that $e_i = E_i[\{\ell_X, r_X\}_{X \in \mathcal{X}}]$, the rest follows from construction. □

Solution for word equations from integer solutions

Let $\{\ell'_X, r'_X\}_{X\in\mathcal{X}}$ be a solution of the constructed system.
We construct a solution S'.

Solution for word equations from integer solutions

Let $\{\ell'_X, r'_X\}_{X\in\mathcal{X}}$ be a solution of the constructed system.
We construct a solution S'.
It is enough to define $S'(X)$ for a variable X.

- we replace the a-prefix and suffix a^{ℓ_X}, a^{r_X} with $a^{\ell'_X}, a^{r'_X}$
- we replace a maximal block of length e_j with $E_j[\{\ell'_X, r'_X\}_{X\in\mathcal{X}}]$

Solution for word equations from integer solutions

Let $\{\ell'_X, r'_X\}_{X\in\mathcal{X}}$ be a solution of the constructed system.
We construct a solution S'.
It is enough to define $S'(X)$ for a variable X.

- we replace the a-prefix and suffix a^{ℓ_X}, a^{r_X} with $a^{\ell'_X}, a^{r'_X}$
- we replace a maximal block of length e_j with $E_j[\{\ell'_X, r'_X\}_{X\in\mathcal{X}}]$

Lemma

$S'(U)$ is obtained by replacing in $S(U)$ each maximal a-block of length e_j with a maximal a-block of length $E_j[\{\ell'_X, r'_X\}_{X\in\mathcal{X}}]$.

Solution for word equations from integer solutions

Let $\{\ell'_X, r'_X\}_{X\in\mathcal{X}}$ be a solution of the constructed system.
We construct a solution S'.
It is enough to define $S'(X)$ for a variable X.

- we replace the a-prefix and suffix a^{ℓ_X}, a^{r_X} with $a^{\ell'_X}, a^{r'_X}$
- we replace a maximal block of length e_j with $E_j[\{\ell'_X, r'_X\}_{X\in\mathcal{X}}]$

Lemma

$S'(U)$ is obtained by replacing in $S(U)$ each maximal a-block of length e_j with a maximal a-block of length $E_j[\{\ell'_X, r'_X\}_{X\in\mathcal{X}}]$.

Proof.

Direct for blocks inside variables.
For all others: they are touching, so they have length $e_i = E_i[\{\ell_X, r_X\}_{X\in\mathcal{X}}]$
We replace each a-prefix a^{ℓ_X} and suffix a^{r_X} with $a^{\ell'_X}$ and $a^{r'_X}$, so indeed the block has length $E_i[\{\ell'_X, r'_X\}_{X\in\mathcal{X}}]$. □

Some linear algebra

Smallest solutions

Well-known: a system of linear equations has an exponential solution or is not is not satisfiable.

Some linear algebra

Smallest solutions

Well-known: a system of linear equations has an exponential solution or is not is not satisfiable. Not enough for our purposes.

Some linear algebra

Smallest solutions

Well-known: a system of linear equations has an exponential solution or is not is not satisfiable. Not enough for our purposes.

Minimal solutions

We compare solutions pointwise:

$$\{\ell'_X, r'_X\}_{X\in\mathcal{X}} \leq \{\ell_X, r_X\}_{X\in\mathcal{X}} \iff \forall_{X\in\mathcal{X}} \ell'_X \leq \ell_X, r'_X \leq r_X$$

$$\{\ell'_X, r'_X\}_{X\in\mathcal{X}} < \{\ell_X, r_X\}_{X\in\mathcal{X}} \iff \text{some inequality above is strict}$$

Some linear algebra

Smallest solutions

Well-known: a system of linear equations has an exponential solution or is not is not satisfiable. Not enough for our purposes.

Minimal solutions

We compare solutions pointwise:

$$\{\ell'_X, r'_X\}_{X\in\mathcal{X}} \leq \{\ell_X, r_X\}_{X\in\mathcal{X}} \iff \forall_{X\in\mathcal{X}} \ell'_X \leq \ell_X, r'_X \leq r_X$$

$$\{\ell'_X, r'_X\}_{X\in\mathcal{X}} < \{\ell_X, r_X\}_{X\in\mathcal{X}} \iff \text{some inequality above is strict}$$

Solution is minimal if it is minimal according to this (partial) order.

Some linear algebra

Smallest solutions

Well-known: a system of linear equations has an exponential solution or is not is not satisfiable. Not enough for our purposes.

Minimal solutions

We compare solutions pointwise:

$$\{\ell'_X, r'_X\}_{X\in\mathcal{X}} \leq \{\ell_X, r_X\}_{X\in\mathcal{X}} \iff \forall_{X\in\mathcal{X}} \ell'_X \leq \ell_X, r'_X \leq r_X$$

$$\{\ell'_X, r'_X\}_{X\in\mathcal{X}} < \{\ell_X, r_X\}_{X\in\mathcal{X}} \iff \text{some inequality above is strict}$$

Solution is minimal if it is minimal according to this (partial) order.

Theorem (Kościelski, Pacholski '90, adaptation of earlier proofs)

If $\{\ell_X, r_X\}_{X\in\mathcal{X}}$ is a minimal solution, then each coordinate is

$$\mathcal{O}\left(|UV| \cdot \left(\frac{|UV|_{\mathcal{X}}}{|\mathcal{X}|}\right)^{2|\mathcal{X}|}\right) \leq \mathcal{O}(|UV| e^{4|UV|/e})$$

Getting back to exponent of periodicity

- take a length-minimal solution, $\{\ell_X, r_X\}_{X \in \mathcal{X}}$

Getting back to exponent of periodicity

- take a length-minimal solution, $\{\ell_X, r_X\}_{X \in \mathcal{X}}$
- construct the system

Getting back to exponent of periodicity

- take a length-minimal solution, $\{\ell_X, r_X\}_{X \in \mathcal{X}}$
- construct the system
- we claim that $\{\ell_X, r_X\}_{X \in \mathcal{X}}$ is a minimal solution

Getting back to exponent of periodicity

- take a length-minimal solution, $\{\ell_X, r_X\}_{X\in\mathcal{X}}$
- construct the system
- we claim that $\{\ell_X, r_X\}_{X\in\mathcal{X}}$ is a minimal solution
- if not then let $\{\ell'_X, r'_X\}_{X\in\mathcal{X}} < \{\ell_X, r_X\}_{X\in\mathcal{X}}$

Getting back to exponent of periodicity

- take a length-minimal solution, $\{\ell_X, r_X\}_{X\in\mathcal{X}}$
- construct the system
- we claim that $\{\ell_X, r_X\}_{X\in\mathcal{X}}$ is a minimal solution
- if not then let $\{\ell'_X, r'_X\}_{X\in\mathcal{X}} < \{\ell_X, r_X\}_{X\in\mathcal{X}}$
- construct S' from it; it is shorter than S, contradiction

Getting back to exponent of periodicity

- take a length-minimal solution, $\{\ell_X, r_X\}_{X\in\mathcal{X}}$
- construct the system
- we claim that $\{\ell_X, r_X\}_{X\in\mathcal{X}}$ is a minimal solution
- if not then let $\{\ell'_X, r'_X\}_{X\in\mathcal{X}} < \{\ell_X, r_X\}_{X\in\mathcal{X}}$
- construct S' from it; it is shorter than S, contradiction
- so each ℓ_X, r_x is $\mathcal{O}(|UV|e^{4|UV|_{\mathcal{X}}/e})$

Getting back to exponent of periodicity

- take a length-minimal solution, $\{\ell_X, r_X\}_{X\in\mathcal{X}}$
- construct the system
- we claim that $\{\ell_X, r_X\}_{X\in\mathcal{X}}$ is a minimal solution
- if not then let $\{\ell'_X, r'_X\}_{X\in\mathcal{X}} < \{\ell_X, r_X\}_{X\in\mathcal{X}}$
- construct S' from it; it is shorter than S, contradiction
- so each ℓ_X, r_x is $\mathcal{O}(|UV|e^{4|UV|_{\mathcal{X}}/e})$
- so each touching a-block has length $\mathcal{O}(poly(|UV|)e^{4|UV|_{\mathcal{X}}/e})$

General case of exponent of periodicity

General case of exponent of periodicity

Definition

A word is primitive if it is not a (>1) power of another word.

It is enough to bound exponents of primitive words.

General case of exponent of periodicity

Definition

A word is primitive if it is not a (>1) power of another word.

It is enough to bound exponents of primitive words.

- A similar analysis for repetitions of powers of a primitive word.

General case of exponent of periodicity

Definition

A word is primitive if it is not a (>1) power of another word.

It is enough to bound exponents of primitive words.

- A similar analysis for repetitions of powers of a primitive word.
- maximal blocks cannot overlap
- powers of a primitive word w can overlap (a bit: shorter than w)

General case of exponent of periodicity

Definition

A word is primitive if it is not a (>1) power of another word.

It is enough to bound exponents of primitive words.

- A similar analysis for repetitions of powers of a primitive word.
- maximal blocks cannot overlap
- powers of a primitive word w can overlap (a bit: shorter than w)
- w-prefix and w-suffix less clear
- but it can be overcome (and this partially goes back to Makanin)

All solutions of a word equation

Algorithm uses the bound on the length of a-blocks in minimal solutions.

All solutions? No bound exists: $aXbXXa = XabYYY$.

All solutions of a word equation

Algorithm uses the bound on the length of a-blocks in minimal solutions.

All solutions? No bound exists: $aXbXXa = XabYYY$.

Use the approach

All solutions of a word equation

Algorithm uses the bound on the length of a-blocks in minimal solutions.

All solutions? No bound exists: $aXbXXa = XabYYY$.

Use the approach

We replace blocks of the same lengths.
We do not need the actual lengths:

All solutions of a word equation

Algorithm uses the bound on the length of a-blocks in minimal solutions.

All solutions? No bound exists: $aXbXXa = XabYYY$.

Use the approach

We replace blocks of the same lengths.
We do not need the actual lengths:

- guess the first/last letter
- the prefixes and suffixes have "lengths" L_X, R_X
- compute block lengths (arithmetic expressions in $\{L_X, R_X\}_{X \in \mathcal{X}}$)
- guess the system of equations (which blocks are equal)
- verify the system (satisfiability)
- replace the blocks (prefixes and suffixes are popped)