O automatach i gęstości liczb

Jakub Różycki

Uniwersytet Warszawski

Koło Pasjonatów Matematyki

21 grudnia 2020

Spis treści

Formuły logiczne

Kilka przykładów formuł logicznych:

Formuły logiczne

Kilka przykładów formuł logicznych:

$$\forall x \forall y \forall z : (x \cdot y) \cdot z = x \cdot (y \cdot z)$$

$$\forall x : e \cdot x = x \cdot e = x$$

$$\forall x \exists y : x \cdot y = y \cdot x = e$$

$$\exists y : x = y^2$$

$$\exists a, b, c, d : x = a^2 + b^2 + c^2 + d^2$$

$$\forall \epsilon > 0 \exists \delta > 0 \forall a, b : |a - b| < \delta \rightarrow |f(a) - f(b)| < \epsilon$$

Formuły logiczne

Kilka przykładów formuł logicznych:

$$\forall x \forall y \forall z : (x \cdot y) \cdot z = x \cdot (y \cdot z) \qquad (G, \cdot)$$

$$\forall x : e \cdot x = x \cdot e = x \qquad (G, \cdot)$$

$$\forall x \exists y : x \cdot y = y \cdot x = e \qquad (G, \cdot)$$

$$\exists y : x = y^2 \qquad (\mathbb{R}, +, \cdot)$$

$$\exists a, b, c, d : x = a^2 + b^2 + c^2 + d^2 \qquad (\mathbb{Z}, +, \cdot)$$

$$\forall \epsilon > 0 \exists \delta > 0 \forall a, b : |a - b| < \delta \rightarrow |f(a) - f(b)| < \epsilon \qquad (\mathbb{R}, +, \cdot)$$

Formuły logiczne

Kilka przykładów formuł logicznych:

$$\forall x \forall y \forall z : (x \cdot y) \cdot z = x \cdot (y \cdot z) \qquad (G, \cdot)$$

$$\forall x : e \cdot x = x \cdot e = x \qquad (G, \cdot)$$

$$\forall x \exists y : x \cdot y = y \cdot x = e \qquad (G, \cdot)$$

$$\exists y : x = y^2 \qquad (\mathbb{R}, +, \cdot)$$

$$\exists a, b, c, d : x = a^2 + b^2 + c^2 + d^2 \qquad (\mathbb{Z}, +, \cdot)$$

$$\forall \epsilon > 0 \exists \delta > 0 \forall a, b : |a - b| < \delta \rightarrow |f(a) - f(b)| < \epsilon \qquad (\mathbb{R}, +, \cdot)$$

Uwaga! W każdej formule logicznej zakładam, że:

Formuły logiczne

Kilka przykładów formuł logicznych:

$$\forall x \forall y \forall z : (x \cdot y) \cdot z = x \cdot (y \cdot z) \qquad (G, \cdot)$$

$$\forall x : e \cdot x = x \cdot e = x \qquad (G, \cdot)$$

$$\forall x \exists y : x \cdot y = y \cdot x = e \qquad (G, \cdot)$$

$$\exists y : x = y^2 \qquad (\mathbb{R}, +, \cdot)$$

$$\exists a, b, c, d : x = a^2 + b^2 + c^2 + d^2 \qquad (\mathbb{Z}, +, \cdot)$$

$$\forall \epsilon > 0 \exists \delta > 0 \forall a, b : |a - b| < \delta \rightarrow |f(a) - f(b)| < \epsilon \qquad (\mathbb{R}, +, \cdot)$$

Uwaga! W każdej formule logicznej zakładam, że:

- Wszystkie kwantyfikatory są na początku.

Formuły logiczne

Kilka przykładów formuł logicznych:

$$\forall x \forall y \forall z : (x \cdot y) \cdot z = x \cdot (y \cdot z) \qquad (G, \cdot)$$

$$\forall x : e \cdot x = x \cdot e = x \qquad (G, \cdot)$$

$$\forall x \exists y : x \cdot y = y \cdot x = e \qquad (G, \cdot)$$

$$\exists y : x = y^2 \qquad (\mathbb{R}, +, \cdot)$$

$$\exists a, b, c, d : x = a^2 + b^2 + c^2 + d^2 \qquad (\mathbb{Z}, +, \cdot)$$

$$\forall \epsilon > 0 \exists \delta > 0 \forall a, b : |a - b| < \delta \rightarrow |f(a) - f(b)| < \epsilon \qquad (\mathbb{R}, +, \cdot)$$

Uwaga! W każdej formule logicznej zakładam, że:

- Wszystkie kwantyfikatory są na początku.
- Zmienne są kwantyfikowane po całym zbiorze.

Kwantyfikatory

Obserwacja

Formuły logiczne w którym często przeplatają się kwantyfikatory $\forall$ oraz $\exists$ są skomplikowane.

Kwantyfikatory

Obserwacja

Formuły logiczne w którym często przeplatają się kwantyfikatory $\forall$ oraz $\exists$ są skomplikowane.

Jeżeli formuła ψ jest postaci:

- $\psi(x) = \exists x_1 \dots x_n : \phi(x, x_1 \dots x_n)$, gdzie ϕ nie ma kwantyfikatorów, to $\psi \in \exists^*$.
- $\psi(x) = \exists x_1 \dots x_n \forall y_1 \dots y_m : \phi(x, x_1 \dots x_n, y_1 \dots y_m)$, gdzie ϕ nie ma kwantyfikatorów, to $\psi \in \exists^* \forall^*$.

Kwantyfikatory

Obserwacja

Formuły logiczne w którym często przeplatają się kwantyfikatory $\forall$ oraz $\exists$ są skomplikowane.

Jeżeli formuła ψ jest postaci:

- $\psi(x) = \exists x_1 \dots x_n : \phi(x, x_1 \dots x_n)$, gdzie ϕ nie ma kwantyfikatorów, to $\psi \in \exists^*$.
- $\psi(x) = \exists x_1 \dots x_n \forall y_1 \dots y_m : \phi(x, x_1 \dots x_n, y_1 \dots y_m)$, gdzie ϕ nie ma kwantyfikatorów, to $\psi \in \exists^* \forall^*$.

Uwaga!

Od tej pory będziemy mówić o formułach z jednym parametrem.

Arytmetyka Büchiego

Niech $p > 1$ będzie ustaloną liczbą naturalną.

Arytmetyka Büchiego

Niech $p > 1$ będzie ustaloną liczbą naturalną.
Będziemy rozważać dwa światy:

Arytmetyka Büchiego

Niech $p > 1$ będzie ustaloną liczbą naturalną.
Będziemy rozważać dwa światy:

- $(\mathbb{N}, +)$

Arytmetyka Büchiego

Niech $p > 1$ będzie ustaloną liczbą naturalną.
Będziemy rozważać dwa światy:

- $(\mathbb{N}, +)$
- $(\mathbb{N}, +, V_p(\cdot, \cdot))$, gdzie $V_p(x, y)$ zachodzi wtedy i tylko wtedy, gdy $x = p^k$ oraz $p^k | y$ i $p^{k+1} \nmid y$ dla pewnego k.

Arytmetyka Büchiego

Niech $p > 1$ będzie ustaloną liczbą naturalną.
Będziemy rozważać dwa światy:

- $(\mathbb{N}, +)$
- $(\mathbb{N}, +, V_p(\cdot, \cdot))$, gdzie $V_p(x, y)$ zachodzi wtedy i tylko wtedy, gdy $x = p^k$ oraz $p^k | y$ i $p^{k+1} \nmid y$ dla pewnego k. Ten świat to *arytmetyka Büchiego*.

Arytmetyka Büchiego

Niech $p > 1$ będzie ustaloną liczbą naturalną.
Będziemy rozważać dwa światy:

- $(\mathbb{N}, +)$
- $(\mathbb{N}, +, V_p(\cdot, \cdot))$, gdzie $V_p(x, y)$ zachodzi wtedy i tylko wtedy, gdy $x = p^k$ oraz $p^k | y$ i $p^{k+1} \nmid y$ dla pewnego k. Ten świat to *arytmetyka Büchiego*.

Uwaga!

O liczbach w arytmetyce Büchiego wygodnie jest myśleć jak o liczbach zapisanych w systemie o podstawie p. Wtedy $V_p(x, y)$ zachodzi wtedy i tylko wtedy, gdy $x = 1\underbrace{0 \ldots 0}_{k}$ oraz $y = a\underbrace{0 \ldots 0}_{k}$, gdzie a kończy się cyfrą inną niż 0.

Języki i automaty

Naszymi literami będą cyfry $\{0, 1 \dots p-1\}$. *Alfabetem* nazywamy zbiór wszystkich liter. *Słowem* nazwiemy dowolny ciąg liter. *Językiem* nazwiemy zbiór słów.

Języki i automaty

Naszymi literami będą cyfry $\{0, 1 \ldots p-1\}$. *Alfabetem* nazywamy zbiór wszystkich liter. *Słowem* nazwiemy dowolny ciąg liter. *Językiem* nazwiemy zbiór słów.

Definicja

Automat to graf skierowany, którego krawędzie są indeksowane literami. Dodatkowo w automatach wyróżniamy wierzchołek początkowy i końcowy.

Języki i automaty

Naszymi literami będą cyfry $\{0, 1 \dots p-1\}$. *Alfabetem* nazywamy zbiór wszystkich liter. *Słowem* nazwiemy dowolny ciąg liter. *Językiem* nazwiemy zbiór słów.

Definicja

Automat to graf skierowany, którego krawędzie są indeksowane literami. Dodatkowo w automatach wyróżniamy wierzchołek początkowy i końcowy.

Przykłady automatów:

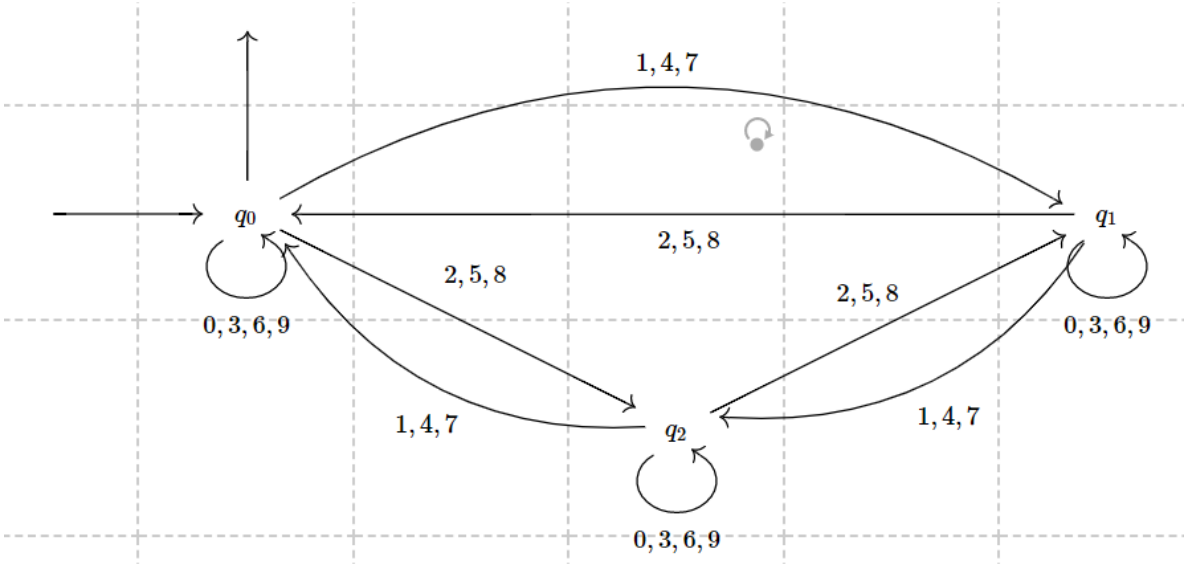
Języki i automaty

Naszymi literami będą cyfry $\{0, 1 \ldots p-1\}$. *Alfabetem* nazywamy zbiór wszystkich liter. *Słowem* nazwiemy dowolny ciąg liter. *Językiem* nazwiemy zbiór słów.

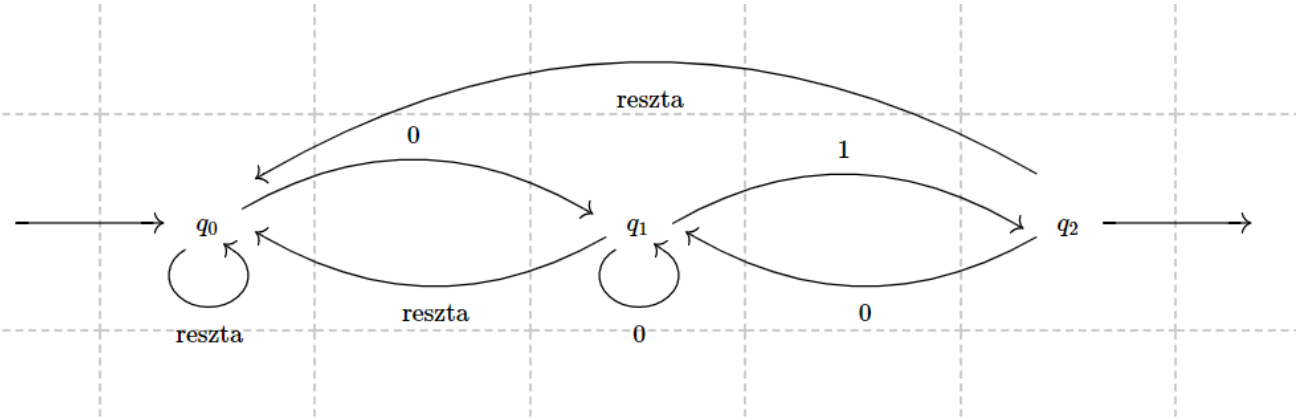
Definicja

Automat to graf skierowany, którego krawędzie są indeksowane literami. Dodatkowo w automatach wyróżniamy wierzchołek początkowy i końcowy.

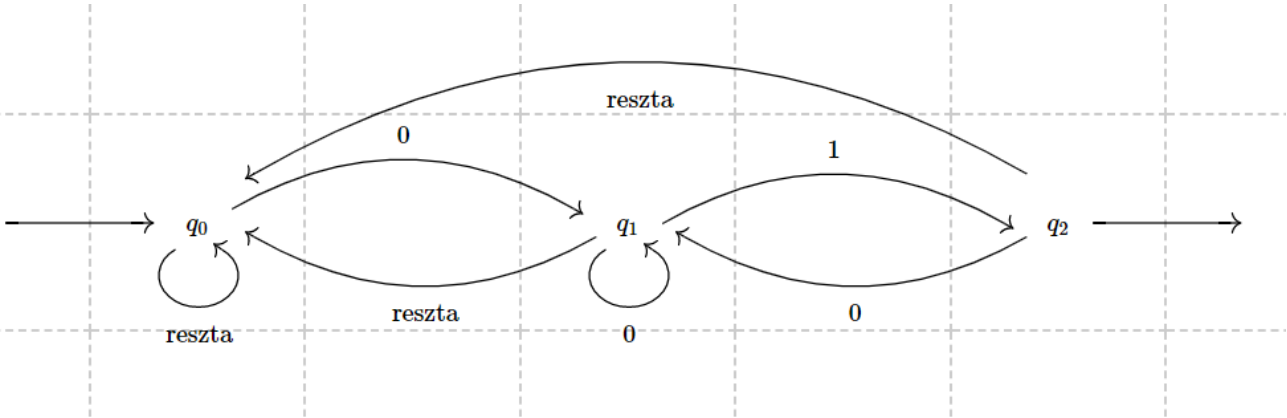
Przykłady automatów:



Automaty cd.



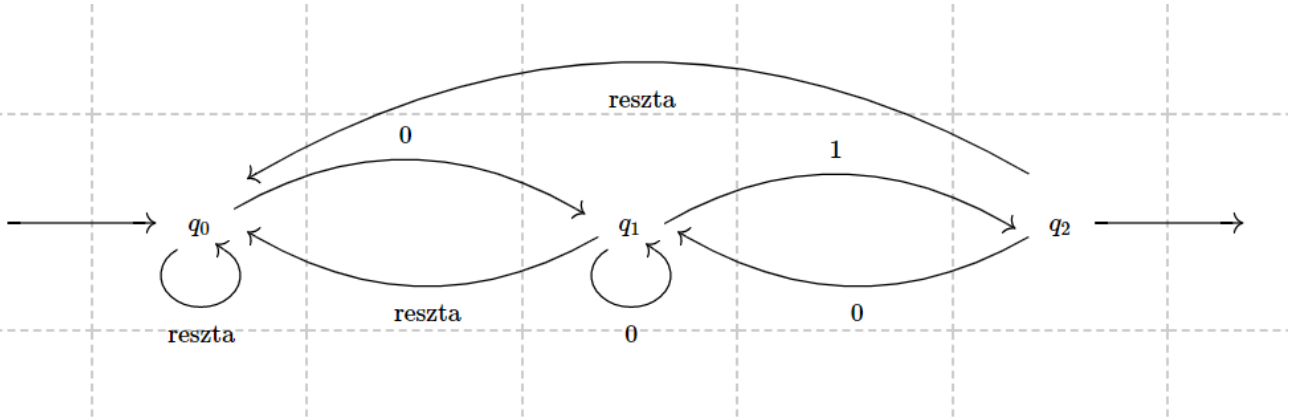
Automaty cd.



Definicja

Automat *akceptuje* słowo w jeśli istnieje w nim ścieżka indeksowana kolejnymi literami słowa w, która zaczyna się w wierzchołku początkowym i kończy w wierzchołku końcowym.

Automaty cd.



Definicja

Automat *akceptuje* słowo w jeśli istnieje w nim ścieżka indeksowana kolejnymi literami słowa w, która zaczyna się w wierzchołku początkowym i kończy w wierzchołku końcowym.

Definicja

Powiemy, że automat A akceptuje język L gdy dla dowolnego słowa w, w należy do L wtedy i tylko wtedy, gdy A akceptuje w.

Arytmetyka Büchiego a automaty

Zachodzi fajne i ważne twierdzenie:

Arytmetyka Büchiego a automaty

Zachodzi fajne i ważne twierdzenie:

Twierdzenie

Ustalmy język L. Następujące warunki są równoważne:

Arytmetyka Büchiego a automaty

Zachodzi fajne i ważne twierdzenie:

Twierdzenie

Ustalmy język L. Następujące warunki są równoważne:

- Istnieje automat A, który akceptuje L.

Arytmetyka Büchiego a automaty

Zachodzi fajne i ważne twierdzenie:

Twierdzenie

Ustalmy język L. Następujące warunki są równoważne:

- Istnieje automat A, który akceptuje L.
- Istnieje formuła arytmetyki Büchiego ϕ taka, że $L = \{w \text{ - słowo} : \phi(w)\}$.

Arytmetyka Büchiego a automaty

Zachodzi fajne i ważne twierdzenie:

Twierdzenie

Ustalmy język L. Następujące warunki są równoważne:

- Istnieje automat A, który akceptuje L.
- Istnieje formuła arytmetyki Büchiego ϕ taka, że $L = \{w \text{ - słowo} : \phi(w)\}$.
- (Dla osób, które wiedzą więcej) L jest językiem regularnym.

Analogia do $(\mathbb{N}, +)$

Twierdzenie

Niech $\phi(x)$ będzie formułą w świecie $(\mathbb{N}, +)$. Wtedy istnieje formuła $\psi(x) \in \exists^*$ taka, że $\phi(x) \iff \psi(x)$.

Analogia do $(\mathbb{N}, +)$

Twierdzenie

Niech $\phi(x)$ będzie formułą w świecie $(\mathbb{N}, +)$. Wtedy istnieje formuła $\psi(x) \in \exists^*$ taka, że $\phi(x) \iff \psi(x)$.

Z poprzednich prac wiadomo, że:

Analogia do $(\mathbb{N}, +)$

Twierdzenie

Niech $\phi(x)$ będzie formułą w świecie $(\mathbb{N}, +)$. Wtedy istnieje formuła $\psi(x) \in \exists^*$ taka, że $\phi(x) \iff \psi(x)$.

Z poprzednich prac wiadomo, że:

Twierdzenie

Niech $\phi(x)$ będzie formułą arytmetyki Büchiego. Wtedy istnieje formuła $\psi(x) \in \exists^*\forall^*$ taka, że $\phi(x) \iff \psi(x)$.

Analogia do $(\mathbb{N}, +)$

Twierdzenie

Niech $\phi(x)$ będzie formułą w świecie $(\mathbb{N}, +)$. Wtedy istnieje formuła $\psi(x) \in \exists^*$ taka, że $\phi(x) \iff \psi(x)$.

Z poprzednich prac wiadomo, że:

Twierdzenie

Niech $\phi(x)$ będzie formułą arytmetyki Büchiego. Wtedy istnieje formuła $\psi(x) \in \exists^*\forall^*$ taka, że $\phi(x) \iff \psi(x)$.

Pytanie

Czy dla każdej formuły $\phi(x)$ arytmetyki Büchiego istnieje formuła $\psi(x) \in \exists^*$ taka, że $\phi(x) \iff \psi(x)$?
Jeśli nie, to czy potrafimy scharakteryzować jakoś języki, które dają się zdefiniować formułą z klasy $\exists^*$?

Główne twierdzenie

Twierdzenie

Jeżeli $\phi(x)$ jest formułą arytmetyki Büchiego oraz $\phi(x) \in \exists^*$, to zachodzi jeden z dwóch przypadków:

(1) $|\{x \in \mathbb{N} : \phi(x)\} \cap [p^{n-1}, p^n)| \geqslant cp^n$ dla pewnej stałej $c > 0$ i nieskończenie wielu $n \in \mathbb{N}$.

(2) $|\{x \in \mathbb{N} : \phi(x)\} \cap [p^{n-1}, p^n)| \leqslant q(n)$ dla pewnego wielomianu q i wszystkich $n \in \mathbb{N}$.

Główne twierdzenie

Twierdzenie

Jeżeli $\phi(x)$ jest formułą arytmetyki Büchiego oraz $\phi(x) \in \exists^*$, to zachodzi jeden z dwóch przypadków:

(1) $|\{x \in \mathbb{N} : \phi(x)\} \cap [p^{n-1}, p^n)| \geqslant cp^n$ dla pewnej stałej $c > 0$ i nieskończenie wielu $n \in \mathbb{N}$.

(2) $|\{x \in \mathbb{N} : \phi(x)\} \cap [p^{n-1}, p^n)| \leqslant q(n)$ dla pewnego wielomianu q i wszystkich $n \in \mathbb{N}$.

Wniosek

Jeżeli znajdziemy w arytmetyce Büchiego formułę $\phi(x)$, która spełnia $ap^k \leqslant |\{x \in \mathbb{N} : \phi(x)\} \cap [p^{n-1}, p^n)| \leqslant bp^l$ dla pewnych stałych $a, b, k > 0, l < n$, to dla dowolnej formuły $\psi(x)$ takiej że $\psi(x) \iff \phi(x)$ zajdzie $\psi(x) \notin \exists^*$.

Przeformułowanie twierdzenia

Twierdzę, że dowolną formułę arytmetyki Büchiego można sprowadzić do alternatywy wyrażeń postaci

$$A \cdot \vec{x} = \vec{c} \bigwedge_i V_p(t_i, s_i) \quad (*)$$

gdzie A jest macierzą oraz $\vec{x}, \vec{c}$ są wektorami.

Przeformułowanie twierdzenia

Twierdzę, że dowolną formułę arytmetyki Büchiego można sprowadzić do alternatywy wyrażeń postaci

$$A \cdot \vec{x} = \vec{c} \bigwedge_i V_p(t_i, s_i) \quad (*)$$

gdzie A jest macierzą oraz $\vec{x}, \vec{c}$ są wektorami.

Obserwacja

Wystarczy pokazać, że dla każdej formuły postaci $(*)$ zachodzi główne twierdzenie.

Przeformułowanie twierdzenia

Twierdzę, że dowolną formułę arytmetyki Büchiego można sprowadzić do alternatywy wyrażeń postaci

$$A \cdot \vec{x} = \vec{c} \bigwedge_i V_p(t_i, s_i) \quad (*)$$

gdzie A jest macierzą oraz $\vec{x}, \vec{c}$ są wektorami.

Obserwacja

Wystarczy pokazać, że dla każdej formuły postaci $(*)$ zachodzi główne twierdzenie.

Dowód. Jeżeli jedna z formuł w alternatywie spełnia przypadek (1) z głównego twierdzenia, to cała formuła też.

Przeformułowanie twierdzenia

Twierdzę, że dowolną formułę arytmetyki Büchiego można sprowadzić do alternatywy wyrażeń postaci

$$A \cdot \vec{x} = \vec{c} \bigwedge_i V_p(t_i, s_i) \quad (*)$$

gdzie A jest macierzą oraz $\vec{x}, \vec{c}$ są wektorami.

Obserwacja

Wystarczy pokazać, że dla każdej formuły postaci $(*)$ zachodzi główne twierdzenie.

Dowód. Jeżeli jedna z formuł w alternatywie spełnia przypadek (1) z głównego twierdzenia, to cała formuła też. Jeżeli natomiast wszystkie formuły spełniają (2), to ich alternatywa szacuje się przez sumę wielomianów, czyli wielomian.

Konstrukcja automatu

Skonstruujemy automat $\mathcal{A}$, który akceptuje rozwiązania układu równań $A \cdot \vec{x} = \vec{c}$. Niech:

Konstrukcja automatu

Skonstruujemy automat $\mathcal{A}$, który akceptuje rozwiązania układu równań $A \cdot \vec{x} = \vec{c}$. Niech:

- Zbiór wierzchołków $V = \mathbb{Z}^n$, gdzie n jest długością wektora $\vec{c}$.

Konstrukcja automatu

Skonstruujemy automat $\mathcal{A}$, który akceptuje rozwiązania układu równań $A \cdot \vec{x} = \vec{c}$. Niech:

- Zbiór wierzchołków $V = \mathbb{Z}^n$, gdzie n jest długością wektora $\vec{c}$.
- $\vec{s} \xrightarrow{\vec{a}} \vec{t}$ wtedy i tylko wtedy, gdy $\vec{t} = p \cdot \vec{s} + A \cdot \vec{a}$.

Konstrukcja automatu

Skonstruujemy automat $\mathcal{A}$, który akceptuje rozwiązania układu równań $A \cdot \vec{x} = \vec{c}$. Niech:

- Zbiór wierzchołków $V = \mathbb{Z}^n$, gdzie n jest długością wektora $\vec{c}$.
- $\vec{s} \xrightarrow{\vec{a}} \vec{t}$ wtedy i tylko wtedy, gdy $\vec{t} = p \cdot \vec{s} + A \cdot \vec{a}$.
- Początek jest w $\vec{0}$.

Konstrukcja automatu

Skonstruujemy automat $\mathcal{A}$, który akceptuje rozwiązania układu równań $A \cdot \vec{x} = \vec{c}$. Niech:

- Zbiór wierzchołków $V = \mathbb{Z}^n$, gdzie n jest długością wektora $\vec{c}$.
- $\vec{s} \xrightarrow{\vec{a}} \vec{t}$ wtedy i tylko wtedy, gdy $\vec{t} = p \cdot \vec{s} + A \cdot \vec{a}$.
- Początek jest w $\vec{0}$.
- Koniec jest w $\vec{c}$.

Konstrukcja automatu

Skonstruujemy automat $\mathcal{A}$, który akceptuje rozwiązania układu równań $A \cdot \vec{x} = \vec{c}$. Niech:

- Zbiór wierzchołków $V = \mathbb{Z}^n$, gdzie n jest długością wektora $\vec{c}$.
- $\vec{s} \xrightarrow{\vec{a}} \vec{t}$ wtedy i tylko wtedy, gdy $\vec{t} = p \cdot \vec{s} + A \cdot \vec{a}$.
- Początek jest w $\vec{0}$.
- Koniec jest w $\vec{c}$.

Fakt

W powyżej zdefiniowanym automacie istnieje skończenie wiele wierzchołków, z których można trafić do wierzchołka końcowego.

Równania liniowe

Stwierdzenie

Niech $\vec{w}$ będzie wektorem słów, gdzie każde słowo jest długości m. W automacie $\mathcal{A}$ istnieje ścieżka $\vec{s} \xrightarrow{\vec{w}} \vec{t}$ wtedy i tylko wtedy gdy

$$\vec{t} = p^m \cdot \vec{s} + A \cdot \vec{w}$$

Równania liniowe

Stwierdzenie

Niech $\vec{w}$ będzie wektorem słów, gdzie każde słowo jest długości m. W automacie $\mathcal{A}$ istnieje ścieżka $\vec{s} \xrightarrow{\vec{w}} \vec{t}$ wtedy i tylko wtedy gdy

$$\vec{t} = p^m \cdot \vec{s} + A \cdot \vec{w}$$

Będziemy chcieli patrzeć na pętle w automacie $\mathcal{A}$. Niech x będzie współrzędną odpowiadającą pewnej zmiennej w wektorach słów, którymi karmimy $\mathcal{A}$. Wprowadźmy oznaczenie:

Równania liniowe

Stwierdzenie

Niech $\vec{w}$ będzie wektorem słów, gdzie każde słowo jest długości m. W automacie $\mathcal{A}$ istnieje ścieżka $\vec{s} \xrightarrow{\vec{w}} \vec{t}$ wtedy i tylko wtedy gdy

$$\vec{t} = p^m \cdot \vec{s} + A \cdot \vec{w}$$

Będziemy chcieli patrzeć na pętle w automacie $\mathcal{A}$. Niech x będzie współrzędną odpowiadającą pewnej zmiennej w wektorach słów, którymi karmimy $\mathcal{A}$. Wprowadźmy oznaczenie:

$$C_{v,x}(n) = |\{\pi_x(\vec{w}) : \vec{v} \xrightarrow{\vec{w}} \vec{v}, \text{słowa wektora } \vec{w} \text{ są długości } n\}|$$

gdzie $\pi_x(\vec{w})$ jest rzutowaniem wektora $\vec{w}$ na współrzędną x.

Pętle

Lemat

Dla każdego wierzchołka v automatu $\mathcal{A}$ oraz współrzędnej słów x istnieją funkcje liniowe $f_1, f_2 \dots f_k$ takie, że $C_{v,x}(n) = f_i(p^n)$ dla pewnego $i \leqslant k$.

Pętle

Lemat

Dla każdego wierzchołka v automatu $\mathcal{A}$ oraz współrzędnej słów x istnieją funkcje liniowe $f_1, f_2 \dots f_k$ takie, że $C_{v,x}(n) = f_i(p^n)$ dla pewnego $i \leqslant k$.

Szkic dowodu. Tak naprawdę zastanawiamy się, ile jest rozwiązań układu równań liniowych:

$$\vec{v} = p^n \cdot \vec{v} + A \cdot \vec{w}$$

ze względu na pewną zmienną wektora $\vec{w}$, nie przekraczających p^n.

Pętle

Lemat

Dla każdego wierzchołka v automatu $\mathcal{A}$ oraz współrzędnej słów x istnieją funkcje liniowe $f_1, f_2 \dots f_k$ takie, że $C_{v,x}(n) = f_i(p^n)$ dla pewnego $i \leqslant k$.

Szkic dowodu. Tak naprawdę zastanawiamy się, ile jest rozwiązań układu równań liniowych:

$$\vec{v} = p^n \cdot \vec{v} + A \cdot \vec{w}$$

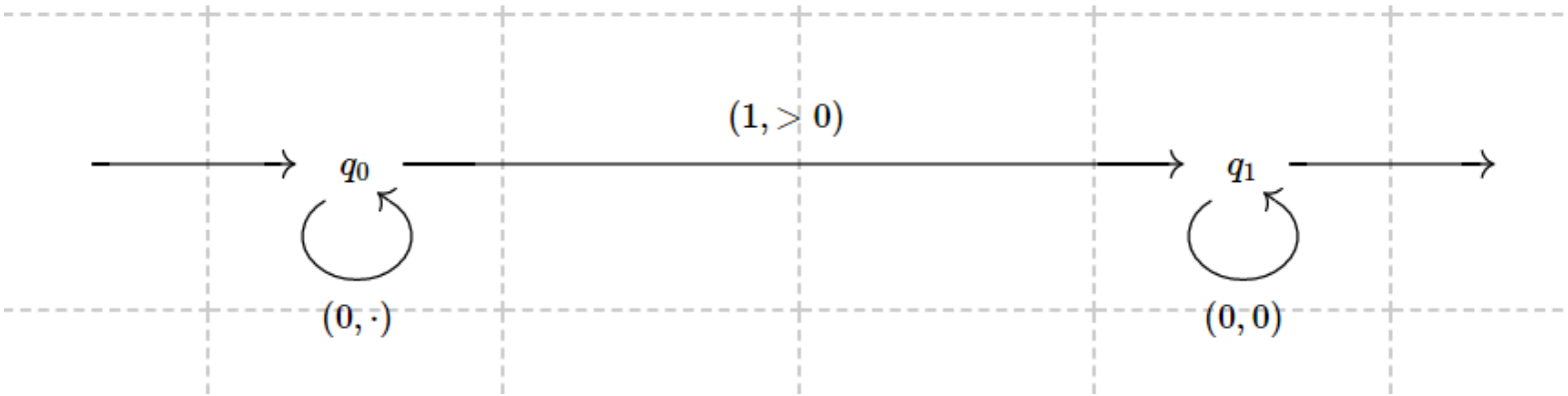
ze względu na pewną zmienną wektora $\vec{w}$, nie przekraczających p^n.
Jako że rozwiązania układów równań liniowych są przestrzeniami liniowymi (czy też afinicznymi, jak kto woli), to taka funkcja musi zachowywać się mniej więcej liniowo.

Automaty reprezentujące $V_p(x, y)$

Automaty sprawdzające, czy zachodzi $V_p(x, y)$ zdefiniujemy za pomocą rysunku:

Automaty reprezentujące $V_p(x, y)$

Automaty sprawdzające, czy zachodzi $V_p(x, y)$ zdefiniujemy za pomocą rysunku:



Automat produktowy

Stwierdzenie

Dla dowolnych automatów $\mathcal{B}$ oraz $\mathcal{C}$ istnieje ich produkt $\mathcal{B} \times \mathcal{C}$.

Automat produktowy

Stwierdzenie

Dla dowolnych automatów $\mathcal{B}$ oraz $\mathcal{C}$ istnieje ich produkt $\mathcal{B} \times \mathcal{C}$.

Nasza intuicja produktu automatów będzie taka, że będziemy jednocześnie podawać to samo słowo wszystkim automatom. Uznamy słowo za zaakceptowane, jeżeli zostało zaakceptowane we wszystkich automatach z osobna.

Automat produktowy

Stwierdzenie

Dla dowolnych automatów $\mathcal{B}$ oraz $\mathcal{C}$ istnieje ich produkt $\mathcal{B} \times \mathcal{C}$.

Nasza intuicja produktu automatów będzie taka, że będziemy jednocześnie podawać to samo słowo wszystkim automatom. Uznamy słowo za zaakceptowane, jeżeli zostało zaakceptowane we wszystkich automatach z osobna.

Oznaczmy $\mathcal{C} = \mathcal{A} \times \prod_i \mathcal{B}_i$, gdzie $\mathcal{B}_i$ to automaty odpowiadające formułom $V_p(\cdot, \cdot)$ w badanej formule.

Automat produktowy

Stwierdzenie

Dla dowolnych automatów $\mathcal{B}$ oraz $\mathcal{C}$ istnieje ich produkt $\mathcal{B} \times \mathcal{C}$.

Nasza intuicja produktu automatów będzie taka, że będziemy jednocześnie podawać to samo słowo wszystkim automatom. Uznamy słowo za zaakceptowane, jeżeli zostało zaakceptowane we wszystkich automatach z osobna.

Oznaczmy $\mathcal{C} = \mathcal{A} \times \prod_i \mathcal{B}_i$, gdzie $\mathcal{B}_i$ to automaty odpowiadające formułom $V_p(\cdot, \cdot)$ w badanej formule.

Zdefiniujmy też funkcję:

$$C'_{v,x}(n) = |\{\pi_x(\vec{w}) : \vec{v} \xrightarrow{\vec{w}} \vec{v}, \text{słowa wektora } \vec{w} \text{ są długości } n\}|$$

która używa wierzchołków $\mathcal{C}$.

Pętle w automacie produktowym

Będziemy chcieli teraz policzyć pętle w tak zdefiniowanym automacie produktowym. Konkretniej udowodnimy:

Pętle w automacie produktowym

Będziemy chcieli teraz policzyć pętle w tak zdefiniowanym automacie produktowym. Konkretniej udowodnimy:

Lemat

Dla każdego wierzchołka v automatu $\mathcal{C}$ oraz współrzędnej słów x istnieją funkcje liniowe $f_1, f_2 \dots f_k$ takie, że $C'_{v,x}(n) = f_i(p^n)$ dla pewnego $i \leqslant k$.

Pętle w automacie produktowym

Będziemy chcieli teraz policzyć pętle w tak zdefiniowanym automacie produktowym. Konkretniej udowodnimy:

Lemat

Dla każdego wierzchołka v automatu $\mathcal{C}$ oraz współrzędnej słów x istnieją funkcje liniowe $f_1, f_2 \dots f_k$ takie, że $C'_{v,x}(n) = f_i(p^n)$ dla pewnego $i \leqslant k$.

Dowód. W automacie produktowym mamy do czynienia z pętlą, jeżeli mamy do czynienia z pętlą w każdym z małych automatów.

Pętle w automacie produktowym

Będziemy chcieli teraz policzyć pętle w tak zdefiniowanym automacie produktowym. Konkretniej udowodnimy:

Lemat

Dla każdego wierzchołka v automatu $\mathcal{C}$ oraz współrzędnej słów x istnieją funkcje liniowe $f_1, f_2 \dots f_k$ takie, że $C'_{v,x}(n) = f_i(p^n)$ dla pewnego $i \leqslant k$.

Dowód. W automacie produktowym mamy do czynienia z pętlą, jeżeli mamy do czynienia z pętlą w każdym z małych automatów. Pętle w automacie $\mathcal{B}_i$ odpowiadającym formule $V_p(x_i, y_i)$ są zadane jednak przez warunek $x_i = 0$ lub warunek $x_i = 0 \wedge y_i = 0$ w zależności od tego, w którym wierzchołku $\mathcal{B}_i$ jesteśmy. Wobec tego pętle w $\mathcal{C}$ są zadane przez warunek:

Pętle w automacie produktowym

Będziemy chcieli teraz policzyć pętle w tak zdefiniowanym automacie produktowym. Konkretniej udowodnimy:

Lemat

Dla każdego wierzchołka v automatu $\mathcal{C}$ oraz współrzędnej słów x istnieją funkcje liniowe $f_1, f_2 \dots f_k$ takie, że $C'_{v,x}(n) = f_i(p^n)$ dla pewnego $i \leqslant k$.

Dowód. W automacie produktowym mamy do czynienia z pętlą, jeżeli mamy do czynienia z pętlą w każdym z małych automatów. Pętle w automacie $\mathcal{B}_i$ odpowiadającym formule $V_p(x_i, y_i)$ są zadane jednak przez warunek $x_i = 0$ lub warunek $x_i = 0 \wedge y_i = 0$ w zależności od tego, w którym wierzchołku $\mathcal{B}_i$ jesteśmy. Wobec tego pętle w $\mathcal{C}$ są zadane przez warunek:

$$\text{pętla w } \mathcal{A} \bigwedge_i x_i = 0 \qquad \bigwedge_{i,\mathcal{B}_i \text{ jest w prawym wierzchołku}} y_i = 0$$

Pętle w automacie produktowym

Będziemy chcieli teraz policzyć pętle w tak zdefiniowanym automacie produktowym. Konkretniej udowodnimy:

Lemat

Dla każdego wierzchołka v automatu $\mathcal{C}$ oraz współrzędnej słów x istnieją funkcje liniowe $f_1, f_2 \dots f_k$ takie, że $C'_{v,x}(n) = f_i(p^n)$ dla pewnego $i \leqslant k$.

Dowód. W automacie produktowym mamy do czynienia z pętlą, jeżeli mamy do czynienia z pętlą w każdym z małych automatów. Pętle w automacie $\mathcal{B}_i$ odpowiadającym formule $V_p(x_i, y_i)$ są zadane jednak przez warunek $x_i = 0$ lub warunek $x_i = 0 \wedge y_i = 0$ w zależności od tego, w którym wierzchołku $\mathcal{B}_i$ jesteśmy. Wobec tego pętle w $\mathcal{C}$ są zadane przez warunek:

$$\text{pętla w } \mathcal{A} \bigwedge_i x_i = 0 \qquad \bigwedge_{i,\mathcal{B}_i \text{ jest w prawym wierzchołku}} y_i = 0$$

Warunek na pętlę w $\mathcal{A}$ był układem równań liniowych, zatem całość jest układem równań liniowych. Stąd z odpowiedniego lematu dla świata

Dwa przypadki

Lemat

Dla ustalonej zmiennej x zachodzi jeden z dwóch przypadków:

(i) Istnieje wierzechołek v w $\mathcal{C}$ oraz funkcja liniowa f takie, że $f(p^n) = C'_{v,x}(n)$ dla nieskończenie wielu n.

(ii) Istnieje $d \in \mathbb{N}$ takie, że $C'_{v,x}(n) \leqslant d$ dla każdych v, n.

Dwa przypadki

Lemat

Dla ustalonej zmiennej x zachodzi jeden z dwóch przypadków:

(i) Istnieje wierzechołek v w $\mathcal{C}$ oraz funkcja liniowa f takie, że $f(p^n) = C'_{v,x}(n)$ dla nieskończenie wielu n.

(ii) Istnieje $d \in \mathbb{N}$ takie, że $C'_{v,x}(n) \leqslant d$ dla każdych v, n.

Dowód. Ustalmy v, x. Pokazaliśmy, że istnieją funkcje liniowe $f_1 \dots f_k$ takie, że $C'_{v,x}(n) = f_i(p^n)$ dla każdego $n \in \mathbb{N}$.

Dwa przypadki

Lemat

Dla ustalonej zmiennej x zachodzi jeden z dwóch przypadków:

(i) Istnieje wierzechołek v w $\mathcal{C}$ oraz funkcja liniowa f takie, że $f(p^n) = C'_{v,x}(n)$ dla nieskończenie wielu n.

(ii) Istnieje $d \in \mathbb{N}$ takie, że $C'_{v,x}(n) \leqslant d$ dla każdych v, n.

Dowód. Ustalmy v, x. Pokazaliśmy, że istnieją funkcje liniowe $f_1 \dots f_k$ takie, że $C'_{v,x}(n) = f_i(p^n)$ dla każdego $n \in \mathbb{N}$. Odrzućmy te funkcje, które spełniają powyższą równość na co najwyżej skończenie wielu miejscach. Wśród pozostałych:

1. Albo istnieje funkcja nieograniczona i wtedy zachodzi (i).
2. Albo wszystkie są stałe.

Jeśli 2. zachodzi dla wszystkich v, to wtedy zachodzi (ii).

Dwa przypadki cd.

Lemat

Niech L będzie językiem automatu $\mathcal{C}$. Zachodzi jeden z dwóch przypadków:

(1) $|L \cap [p^{n-1}, p^n)| \geqslant cp^n$ dla pewnej stałej $c > 0$ i nieskończenie wielu $n \in \mathbb{N}$.

(2) $|L \cap [p^{n-1}, p^n)| \leqslant q(n)$ dla pewnego wielomianu q i wszystkich $n \in \mathbb{N}$.

Dwa przypadki cd.

Lemat

Niech L będzie językiem automatu $\mathcal{C}$. Zachodzi jeden z dwóch przypadków:

(1) $|L \cap [p^{n-1}, p^n)| \geqslant cp^n$ dla pewnej stałej $c > 0$ i nieskończenie wielu $n \in \mathbb{N}$.

(2) $|L \cap [p^{n-1}, p^n)| \leqslant q(n)$ dla pewnego wielomianu q i wszystkich $n \in \mathbb{N}$.

Dowód. Niech q_0 będzie wierzchołkiem początkowym automatu $\mathcal{C}$ oraz niech q_f będzie jego wierzchołkiem końcowym. Przyjmijmy, że x jest zmienną, względem której parametryzowana jest oryginalna formuła. Oznaczmy też $d_L(n) = |L \cap [p^{n-1}, p^n)|$.

Dwa przypadki cd.

Lemat

Niech L będzie językiem automatu $\mathcal{C}$. Zachodzi jeden z dwóch przypadków:

(1) $|L \cap [p^{n-1}, p^n)| \geqslant cp^n$ dla pewnej stałej $c > 0$ i nieskończenie wielu $n \in \mathbb{N}$.

(2) $|L \cap [p^{n-1}, p^n)| \leqslant q(n)$ dla pewnego wielomianu q i wszystkich $n \in \mathbb{N}$.

Dowód. Niech q_0 będzie wierzchołkiem początkowym automatu $\mathcal{C}$ oraz niech q_f będzie jego wierzchołkiem końcowym. Przyjmijmy, że x jest zmienną, względem której parametryzowana jest oryginalna formuła. Oznaczmy też $d_L(n) = |L \cap [p^{n-1}, p^n)|$.
Załóżmy najpierw że zachodzi punkt (i) z lematu z poprzedniego slajdu. Niech v będzie wierzchołkiem oraz f funkcją liniową nieograniczoną i taką, że $f(p^n) = C'_{v,x}(n)$ dla nieskończenie wielu n.

Dwa przypadki cd.

Lemat

Niech L będzie językiem automatu $\mathcal{C}$. Zachodzi jeden z dwóch przypadków:

(1) $|L \cap [p^{n-1}, p^n)| \geqslant cp^n$ dla pewnej stałej $c > 0$ i nieskończenie wielu $n \in \mathbb{N}$.

(2) $|L \cap [p^{n-1}, p^n)| \leqslant q(n)$ dla pewnego wielomianu q i wszystkich $n \in \mathbb{N}$.

Dowód. Niech q_0 będzie wierzchołkiem początkowym automatu $\mathcal{C}$ oraz niech q_f będzie jego wierzchołkiem końcowym. Przyjmijmy, że x jest zmienną, względem której parametryzowana jest oryginalna formuła. Oznaczmy też $d_L(n) = |L \cap [p^{n-1}, p^n)|$.
Załóżmy najpierw że zachodzi punkt (i) z lematu z poprzedniego slajdu. Niech v będzie wierzchołkiem oraz f funkcją liniową nieograniczoną i taką, że $f(p^n) = C'_{v,x}(n)$ dla nieskończenie wielu n. Rozważmy ścieżkę $q_0 \xrightarrow{w_1} v \xrightarrow{w_2} q_f$. Niech k_1, k_2 będą długościami słów w_1, w_2. Dla nieskończenie wielu, dostatecznie dużych n zachodzi:

Końcowe szacowania

$$d_L(n + k_1 + k_2) \geqslant a \cdot p^n + b \geqslant c \cdot p^{n+k_1+k_2}$$

Końcowe szacowania

$$d_L(n + k_1 + k_2) \geqslant a \cdot p^n + b \geqslant c \cdot p^{n+k_1+k_2}$$

Załóżmy teraz, że zachodzi punkt (ii) ze wspomnianego lematu, czyli dla każdych v, n zachodzi $C'_{v,x}(n) \leqslant d$ dla pewnej stałej d.

Końcowe szacowania

$$d_L(n + k_1 + k_2) \geqslant a \cdot p^n + b \geqslant c \cdot p^{n+k_1+k_2}$$

Załóżmy teraz, że zachodzi punkt (ii) ze wspomnianego lematu, czyli dla każdych v, n zachodzi $C'_{v,x}(n) \leqslant d$ dla pewnej stałej d. Każde słowo w długości n może być rozłożone jako $w = u_0 w_1 u_1 \dots w_m$ dla pewnego $m \leqslant |V|$ tak, aby:

Końcowe szacowania

$$d_L(n + k_1 + k_2) \geqslant a \cdot p^n + b \geqslant c \cdot p^{n+k_1+k_2}$$

Załóżmy teraz, że zachodzi punkt (ii) ze wspomnianego lematu, czyli dla każdych v, n zachodzi $C'_{v,x}(n) \leqslant d$ dla pewnej stałej d. Każde słowo w długości n może być rozłożone jako $w = u_0 w_1 u_1 \dots w_m$ dla pewnego $m \leqslant |V|$ tak, aby:

$$q_0 \xrightarrow{u_0} q_{a_1} \xrightarrow{w_1} q_{a_1} \xrightarrow{u_1} \dots \xrightarrow{w_m} q_{a_m} \xrightarrow{u_m} q_{a_m}$$

gdzie $q_{a_i} \neq q_{a_j}$, $q_{a_m} = q_f$ oraz każda ścieżka $q_{a_i} \xrightarrow{u_i} q_{a_{i+1}}$ jest bez pętli.

Końcowe szacowania

$$d_L(n + k_1 + k_2) \geqslant a \cdot p^n + b \geqslant c \cdot p^{n+k_1+k_2}$$

Załóżmy teraz, że zachodzi punkt (ii) ze wspomnianego lematu, czyli dla każdych v, n zachodzi $C'_{v,x}(n) \leqslant d$ dla pewnej stałej d. Każde słowo w długości n może być rozłożone jako $w = u_0 w_1 u_1 \dots w_m$ dla pewnego $m \leqslant |V|$ tak, aby:

$$q_0 \xrightarrow{u_0} q_{a_1} \xrightarrow{w_1} q_{a_1} \xrightarrow{u_1} \dots \xrightarrow{w_m} q_{a_m} \xrightarrow{u_m} q_{a_m}$$

gdzie $q_{a_i} \neq q_{a_j}$, $q_{a_m} = q_f$ oraz każda ścieżka $q_{a_i} \xrightarrow{u_i} q_{a_{i+1}}$ jest bez pętli. Za pomocą nietrudnej kombinatoryki dostajemy:

Końcowe szacowania

$$d_L(n + k_1 + k_2) \geqslant a \cdot p^n + b \geqslant c \cdot p^{n+k_1+k_2}$$

Załóżmy teraz, że zachodzi punkt (ii) ze wspomnianego lematu, czyli dla każdych v, n zachodzi $C'_{v,x}(n) \leqslant d$ dla pewnej stałej d. Każde słowo w długości n może być rozłożone jako $w = u_0 w_1 u_1 \dots w_m$ dla pewnego $m \leqslant |V|$ tak, aby:

$$q_0 \xrightarrow{u_0} q_{a_1} \xrightarrow{w_1} q_{a_1} \xrightarrow{u_1} \dots \xrightarrow{w_m} q_{a_m} \xrightarrow{u_m} q_{a_m}$$

gdzie $q_{a_i} \neq q_{a_j}$, $q_{a_m} = q_f$ oraz każda ścieżka $q_{a_i} \xrightarrow{u_i} q_{a_{i+1}}$ jest bez pętli. Za pomocą nietrudnej kombinatoryki dostajemy:

$$d_L(n) \leqslant |V|^{|V|} \cdot n^{2 \cdot |V|} \cdot d^{|V|} \leqslant q(n)$$

Miejsce na pytania i notatki

Bibliografia

- P. Wolper, B. Boigelot "On the construction of automata from linear arithmetic"
- F. Guèpin, C. Haase, and J. Worrell "On the existential theories of Büchi arithmetic and linear p-adic fields constraints"
- V. Bruyère, G. Hansel, C. Michaux, and R. Villemaire "Logic and p-recognizable sets of integers"
- K. Woods "The unreasonable ubiquitousness of quasi-polynomials"