

Kod z ostatniego wykładu:

```
int gcd(int x, int y) {  
  while (x != y) {  
    if (x > y) { x = x - y; }  
    else { y = y - x; }  
  }  
  return x;  
}
```

$$f((x, y)) = x + y$$

$$(x, y) \rightsquigarrow (x', y') \Rightarrow f((x', y')) < f(x, y)$$

CEL: pokazanie
bezpieczności

Przestrz. stanów

$$\Omega = \mathbb{N}^+ \times \mathbb{N}^+$$

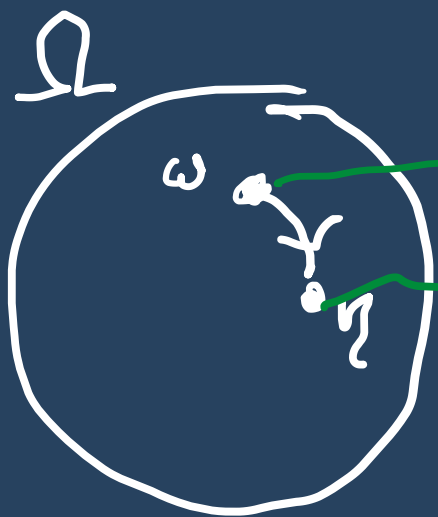
$$\begin{aligned} (17, 5) &\rightsquigarrow (12, 5) \rightsquigarrow (7, 5) \rightsquigarrow \\ &\rightsquigarrow (2, 5) \rightsquigarrow (2, 3) \rightsquigarrow (2, 1) \\ &\rightsquigarrow (1, 1) \end{aligned}$$

Wniosek: gdyby pętla obrotowa nieskończenie
długo, to otrzymalibyśmy ciąg

$$(x_n, y_n) \in \Omega \text{ t. j.}$$

$$(x_n) (f(x_n, y_n) > f(x_{n+1}, y_{n+1}))$$

A TO NIE JEST MOŻLIWE.



$(x, y) - d. \text{wpisz.}$

$f(\omega)$
 \vee
 $f(\eta)$

Ogólna
strategia
dowodzenia
w teorii algorytmów.

Dowód popr. algebraicznie:

FAKT: $\left. \begin{array}{l} x, y \in \mathbb{N}^+ \\ x < y \end{array} \right\} \rightarrow \text{NWD}(x, y) = \text{NWD}(x, y-x)$

$(12, 4) \rightarrow (8, 4) \rightarrow (4, 4) \rightarrow 4$
 $\text{NWD}(8, 4) = a \quad \text{NWD} = a \quad \text{reszta } a$

$a = \text{NWD}(12, 4)$

Inne: funkcja (matem.) NWD

jest niezmiennikiem wewn.
petli

Powtórka z poprzedz. wykładu:

Tw. Jeśli $n, m \in \mathbb{N}$ oraz

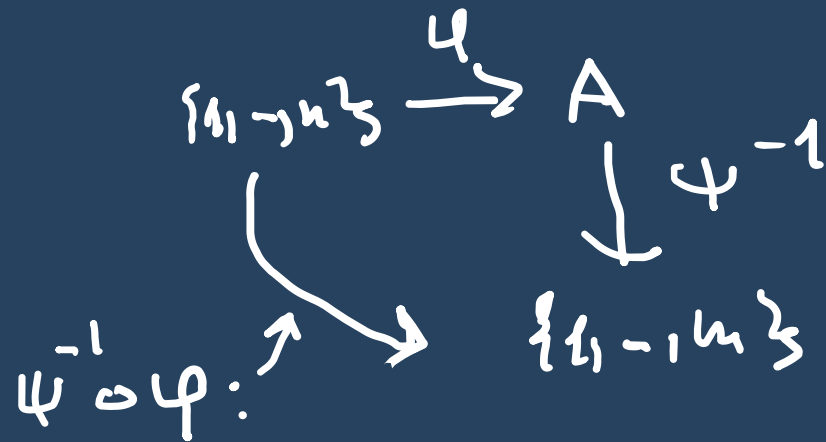
$$\left(\exists \varphi : \{1, \dots, n\} \xrightarrow{1-1} \{1, \dots, m\} \right) \wedge \left(\exists \psi : \{1, \dots, m\} \xrightarrow{1-1} \{1, \dots, n\} \right) \iff n = m.$$

Wniosek. Pojęcie $|A| = n$ jest dobrze określone.

D-d. Wskaz. że $|A| = n, |A| = m \quad (n, m \geq 1)$

• $\varphi : \{1, \dots, n\} \xrightarrow{1-1} A$

• $\psi : \{1, \dots, m\} \xrightarrow{1-1} A$



by. zatem $n = m$.

D-ol, luid po m_2 .

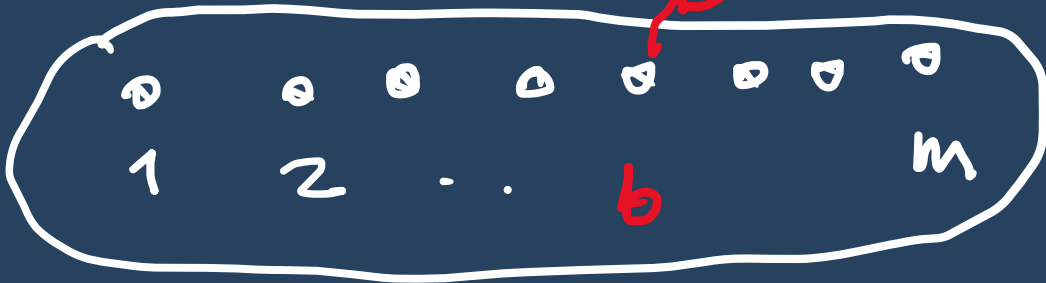
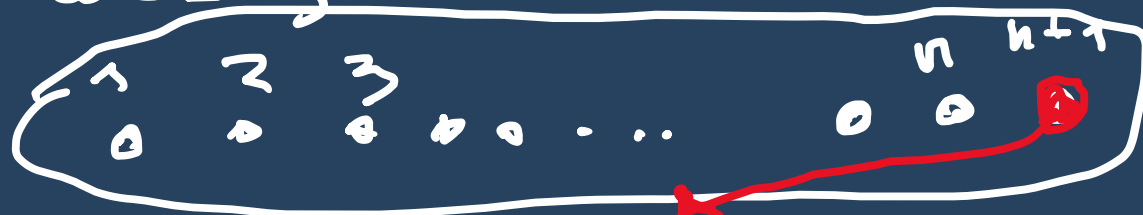
$$\varphi(n) =$$

$$\left(\forall m \right) \left[\left(\exists \tilde{\varphi} \right) \left(\tilde{\varphi} : \{1, \dots, n\} \xrightarrow[n_0]{l-1} \{1, \dots, m\} \right) \rightarrow m = n \right]$$

• $n=1$: OK

• waz. ze wiemy, ze $\varphi(n)$.

wezmy dowolne m , waz. $f : \{1, \dots, n+1\} \xrightarrow[n_0]{l-1} \{1, \dots, m\}$

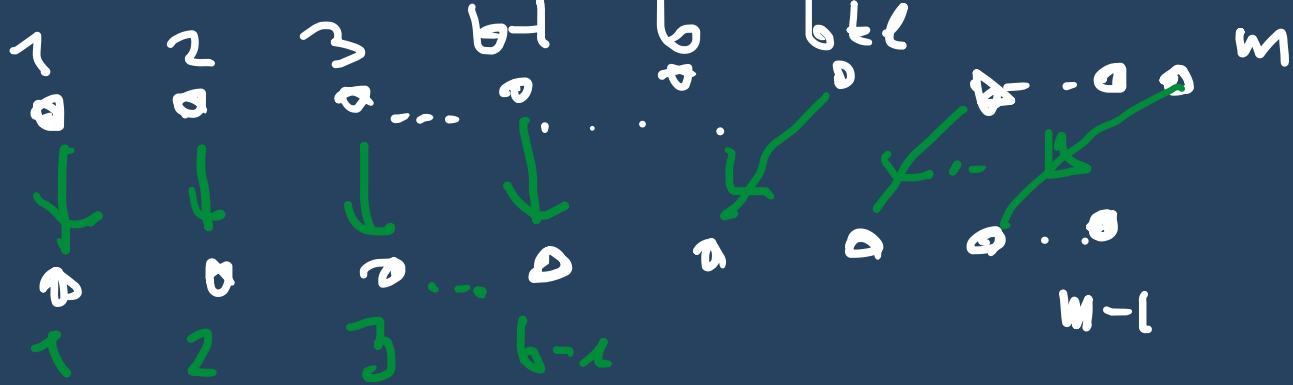


$$b = f(n+1)$$

$$f^* = f \upharpoonright \{1, \dots, n\}$$

$$f^* : \{1, \dots, n\} \xrightarrow[n_0]{l-1}$$

$$\{1, \dots, m\} \setminus \{b\}$$



$$\alpha(x) = \begin{cases} x & : x < b \\ x-1 & : x \in \{b+1, \dots, m\} \end{cases}$$

$$\alpha : \underbrace{\{1, \dots, m\}}_{\substack{\uparrow f^* \\ \{1, \dots, n\}}} \setminus \{b\} \xrightarrow[\alpha \circ f^*]{l-1, u\alpha} \underbrace{\{1, \dots, m-1\}}_{n-1, u\alpha}$$

\geq ЗАК. ИНД. МАМЧ $n = m - 1$

ЗАТЕМ $n+1 = (m-1)+1 = m$ \square

Zadanie: Pole \mathbb{R} i A, B - skłonicz.

$|A|=|B|$; $f: A \rightarrow B$: WTEDY \Leftrightarrow

1) f jest iniekcją

2) f jest surcją

wsk. 1) \rightarrow 2) : czysto

2) \rightarrow 1) : nieprost.

PORZĄDEK LEKSYKOGRAFICZNY NA SŁOWACH.

Otoczka Kleene'go.

X - ustalony zbiór, $X \neq \emptyset$

$$X^* = \bigcup_{n \geq 0} X^n \quad X^n = \underbrace{X X \dots X}_n$$

↑ otoczka Kleene'go zbioru X .

"zbiór wszystkich słówicz. ciągów elem. X

$$X^0 = \{ \varepsilon \} \quad \varepsilon \leftarrow \text{ciąg długości } 0.$$

$$\text{len}(x) = \text{długość słowa } x \in X^*$$

- konkatenacja

$$x = (x_1, \dots, x_n)$$

$$y = (y_1, \dots, y_m)$$

$$x * y = (x_1, \dots, x_n, y_1, \dots, y_m)$$

TO JEST BINARNE DZIAŁANIE NA X^*

- $$\left. \begin{array}{l} x * \varepsilon = x \\ \varepsilon * x = x \end{array} \right\} \equiv \varepsilon \text{ jest elem. neutralnym.}$$

- $$(x * y) * z = x * (y * z) \quad \text{Łączność}$$

Def. (A, \circ, e) jest MONOIDEM

\Leftrightarrow
 \circ jest łącznym działaniem na X , e jest elementem neutralnym.

Ⓟ $(\mathbb{N}, +, 0) \in \text{monoid}$

$(\mathbb{N}^+, \cdot, 1) \in$

$(X^*, \cdot, \varepsilon)$

DEF. Dla $x, y \in X^*$:

$$x \sqsubseteq y \equiv (\exists z \in X^*) (y = x * z)$$

FAKT. (X^*, \sqsubseteq) jest cz. porządkiem

D-d. indukcie.

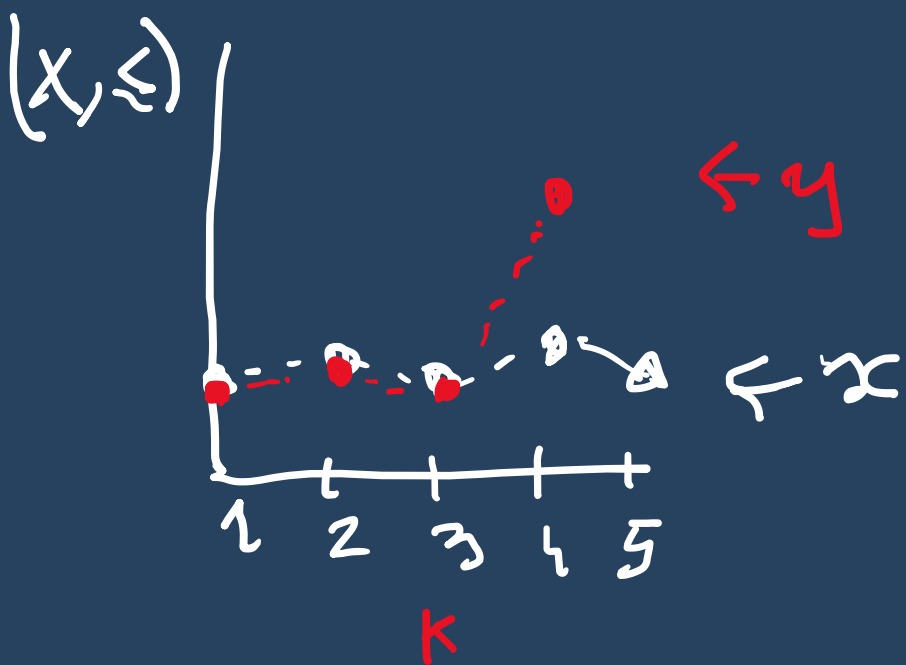
$$\begin{cases} x * \varepsilon = x \\ \text{czyli} \\ x \sqsubseteq x \end{cases}$$

Porz. leksykal.

Na zbiorze X mamy liniowy porządek \leq .

DEF.

$$x \preceq_{\text{lek}} y \equiv (x \sqsubseteq y) \vee (\exists k) \left((1 \leq k \leq \min(\ell(x), \ell(y))) \wedge \right. \\ \left. (\forall i) (1 \leq i < k \rightarrow x_i = y_i) \wedge (x_k < y_k) \right)$$



Przykład : ASCII

$\underbrace{a a a a a}_{x} \prec_{lex} \underbrace{a a b a}_y$

$a < b$

CEL :

\prec_{lex}

jest liniowym

porządkiem na X^*

na X^*

① ZWROTUŚĆ : $X \leq_{\text{lex}} X$ |

DL: bo $X \subseteq X$.

② ZAT. ie $X \leq_{\text{lex}} Y$ i $Y \leq_{\text{lex}} X$,

$$D = \{i : 1 \leq i \leq \min\{l(x), l(y)\} \wedge x_i \neq y_i\}$$

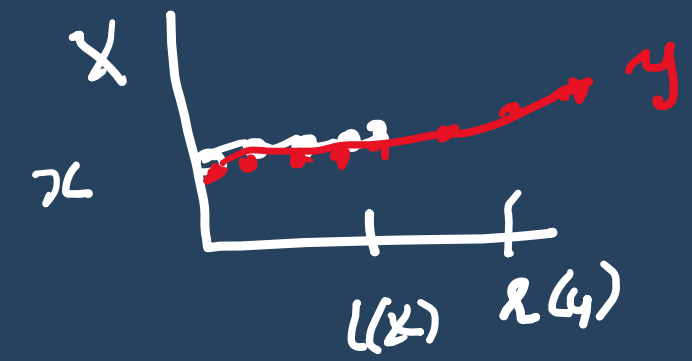
• P1: ($D = \emptyset$). $1 \leq i \leq \min(l(x), l(y)) \rightarrow x_i = y_i$

P1a. ZAT. ie $l(x) \leq l(y)$

wtedy $X \subseteq Y$

P1b. ZAT. ie $l(x) > l(y)$

wtedy $Y \subseteq X$.



✓
 $X=Y$.

• P2 ($D \neq \emptyset$)

Niech $k = \min(D)$.

• $1 \leq i < k \rightarrow x_i = y_i$

• $X \leq_{\text{lex}} Y \rightarrow x_k < y_k$ } sprz.

• $Y \leq_{\text{lex}} X \rightarrow y_k < x_k$ }

$$\textcircled{3} \quad x \leq_{\text{lex}} y \wedge y \leq_{\text{lex}} z$$

$$D = \{i : 1 \leq i \leq \min\{\ell(x), \ell(y)\} \wedge x_i \neq y_i\}$$

$$E = \{i : 1 \leq i \leq \min\{\ell(y), \ell(z)\} \wedge y_i \neq z_i\}.$$

P1. $D = \emptyset \wedge E = \emptyset$. wtedy $x \subseteq y$ i $y \subseteq z$
 zatem $x \subseteq z$ więc $x \leq_{\text{lex}} z$.

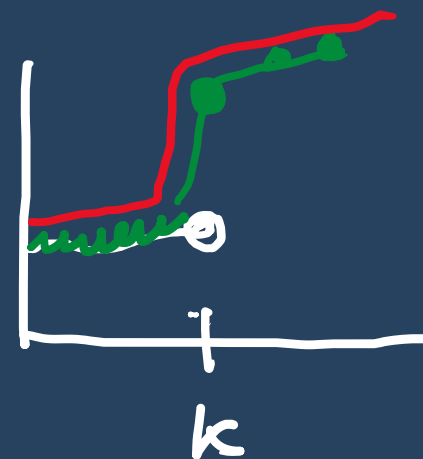
P2. $D \neq \emptyset \wedge E = \emptyset$: mamy $y \subseteq z$.

$$k = \min(D); \quad x_k < y_k$$

ale $z \supseteq y$, więc $y_k = z_k > x_k$

$$1 \leq l < k \rightarrow x_l = y_l = z_l$$

zatem $x \leq_{\text{lex}} z$.



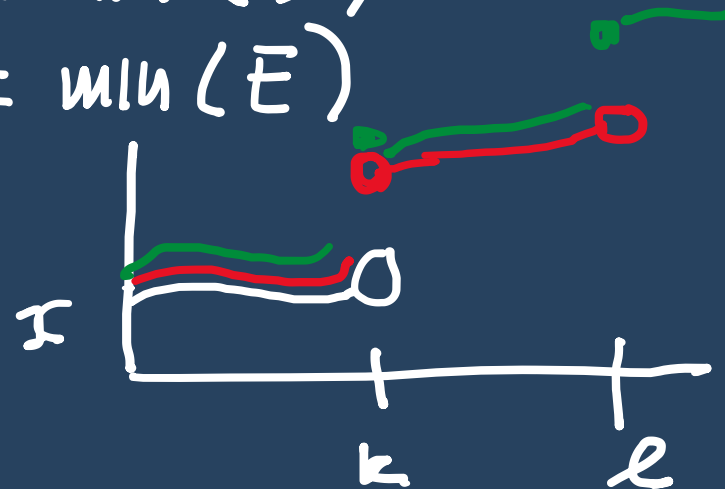
P3. $D = \phi \wedge E \neq \phi$: $z_{\text{max}} \in E$

P4. $D \neq \phi \wedge E \neq \phi$: $k = \min(D)$
 $l = \min(E)$

P4a. $k < l$

$$x_k < z_k$$

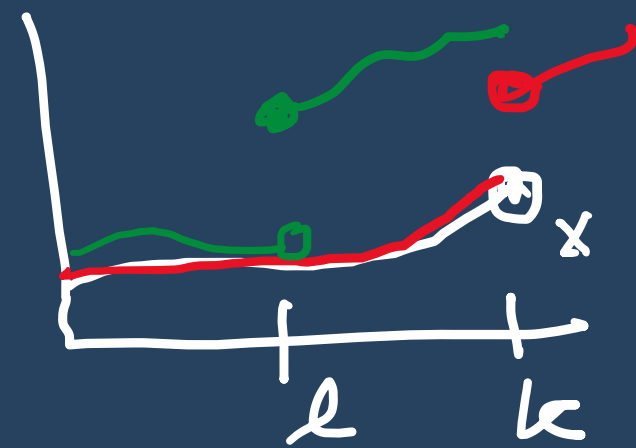
$$1 \leq l < k \rightarrow x_l = z_l$$



P4b. $k > l$

$$1 \leq l < k \rightarrow x_l = z_l$$

$$x_l < z_l$$



P4c. $k = l$

• Uniqueness: For any $x, y \in X^*$.

$$D = \{i : 1 \leq i \leq \min\{l(x), l(y)\} \wedge$$

$$D = \emptyset : \begin{array}{l} l(x) \leq l(y) \rightarrow x \subseteq y \rightarrow x \preceq_{\text{lex}} y \\ l(y) \leq l(x) \rightarrow y \subseteq x \rightarrow y \preceq_{\text{lex}} x \end{array} \quad \left. \begin{array}{l} x_i \neq y_i \end{array} \right\}$$

• $D \neq \emptyset$:

$$k = \min(D) \quad 1 \leq i < k \rightarrow x_i = y_i.$$

• $x_k < y_k \rightarrow x \preceq_{\text{lex}} y$

• $y_k < x_k \rightarrow y \preceq_{\text{lex}} x$

