Systemy algebraiczne

Materiały pomocnicze do wykładu

uczelnia: **PJWSTK**
przedmiot: **Matematyka Dyskretna 1**
wykładowca: **dr Magdalena Kacprzak**

Struktury danych
–
struktury algebraiczne

Przykład

Rozważmy następujący algorytm

```
{
  y:=1; s:= 1; k:= 1;
  while k < 100 do
       y := operacja1(y, 2);
       s := operacja2(s, y);
       k := operacja3(k,1);
  od;
 }
```

Czy można powiedzieć co robi ten algorytm?

Przykład

Jeśli założymy, że wszystkie trzy operacje, to po prostu dodawanie w zbiorze liczb naturalnych, to algorytm w każdej iteracji

- do zmiennej y dodaje 2,
- do zmiennej s dodaje y,
- do k dodaje 1.

Łatwo teraz wywnioskujemy, że k jest licznikiem iteracji, y przyjmuje jako wartość kolejne liczby nieparzyste postaci 2k+1, a s sumuje je.

Przykład

Gdybyśmy jednak zinterpretowali operacje pierwszą i drugą jako dodawanie, a operację trzecią jako mnożenie, wówczas zmienna k nie zmieniałaby wartości (stale k=1) i pętla w naszym algorytmie nigdy nie zakończyłaby się.

Intuicje

Wynika stąd, że aby zrozumieć co robi algorytm (program) musimy znać strukturę danych, w której wykonywane są instrukcje.
Musimy wiedzieć jakiego typu są zmienne występujące w tym algorytmie, wiedzieć jak interpretowane są relacje i operacje w nim występujące.

Intuicje

Intuicyjnie możemy powiedzieć, że

struktura danych

jest to trójka

Zbiór + operacje + relacje.

Taki system nazywa się

systemem algebraicznym.

Intuicje

Przypomnijmy, że operacja n-argumentowa w zbiorze X, to wieloargumentowa funkcja określona na elementach produktu kartezjańskiego X^n i o wartościach w X.

W szczególnym przypadku rozważa się też operacje zeroargumentowe, tzn. stałe.

Definicja

O zbiorze X powiemy, że jest

zamknięty

ze względu na n-argumentową operację **o** wtedy i tylko wtedy, gdy wynik operacji **o** dla dowolnych argumentów wziętych z X należy do X:

jeśli $x_1 \in X$, $x_2 \in X$, ..., $x_n \in X$, to $\mathbf{o}(x_1, x_2, \ldots, x_n) \in X$.

Przykład

Czy zbiór liczb naturalnych jest zamknięty ze względu na operację odejmowania?

NIE, bo np. $4-5=-1 \notin N$

Czy zbiór liczb całkowitych jest zamknięty ze względu na operację dzielenia?

NIE, bo np. $4/5 \notin Z$

Przykład

Czy zbiór liczb pierwszych jest zamknięty ze względu na operację mnożenia?

NIE, bo np. 2*3 nie jest liczbą pierwszą

Czy zbiór liczb całkowitych jest zamknięty ze względu na operację mnożenia?

TAK

Intuicje

Operacje, z którymi mamy do czynienia w praktyce, są często funkcjami częściowymi, tzn. ich wartość nie zawsze jest określona dla wszystkich możliwych układów danych.

Taką operacją jest np. dzielenie w zbiorze liczb rzeczywistych, czy pierwiastkowanie.

Definicja struktury algebraicznej

Systemem (strukturą) algebraicznym (relacyjnym)

nazywamy układ

$$< A, o_1, o_2,\ldots, o_n ; r_1, r_2, \ldots, r_m >$$

w którym

- A jest niepustym zbiorem, zwanym **uniwersum** systemu,
- $o_1, o_2,\ldots, o_n$ są **operacjami** w A, (zbiór A jest domknięty ze względu na operacje $o_1,\ldots, o_n$)
- $r_1,r_2,\ldots,r_m$ są **relacjami** w A.

Uwagi

Jeśli uniwersum systemu składa się z obiektów różnych typów, to mówimy o systemie **wielosortowym**.

Każda operacja systemu relacyjnego ma określony typ, tzn. liczbę i typy argumentów oraz typ wyniku. Podobnie, każda relacja systemu ma określony typ, tzn. liczbę i typy argumentów.

Na relację w systemie relacyjnym będziemy zwykle patrzyli jako na funkcję charakterystyczną zbioru reprezentowanego przez tę relację. Zatem typ wyniku takiej funkcji jest booleowski.

Uwagi

Typy operacji i relacji systemu algebraicznego tworzą razem

sygnaturę systemu.

Systemy algebraiczne o takiej samej sygnaturze nazywa się

podobnymi.

Uwagi

Podobieństwo to jest czysto formalne tzn. dwa systemy podobne mają tyle samo relacji i tyle samo operacji, a odpowiadające sobie operacje i relacje mają takie same **arności** (liczby argumentów).

Algebra

Jeśli w systemie nie rozważa się relacji, to wówczas mówimy po prostu o

algebrze.

Przykłady

Zbiór liczb naturalnych z dodawaniem i mnożeniem tworzy system algebraiczny (algebrę)

$<N, +, * >$

Rzeczywiście wynik dodawania i mnożenia dwóch liczb naturalnych zawsze jest liczbą naturalną. Dodawanie i mnożenie są operacjami dwuargumentowymi w N, czyli sygnatura tego systemu składa się z dwóch dwuargumentowych operacji:

$$+ : N \times N \to N$$

$$* : N \times N \to N$$

Przykłady

Podobnie, zbiór liczb parzystych z dodawaniem i mnożeniem też jest algebrą

<P,+,*>

bo suma dwóch liczb parzystych jest liczbą parzystą i iloczyn dwóch liczb parzystych jest liczbą parzystą:

$$+ : P \times P \to P$$

$$* : P \times P \to P$$

Przykłady

Systemy

$$<N,+,*> \text{ i } <P,+,* >$$

są podobne: oba mają po dwie dwuargumentowe operacje.

Przykłady

Zbiór liczb nieparzystych NP z dodawaniem nie jest strukturą algebraiczną, bo suma dwóch liczb nieparzystych nie jest liczbą nieparzystą.

Wynika stąd, że dodawanie nie jest dobrze określoną operacją w zbiorze NP.

Przykłady

Przykładem systemu algebraicznego jest też krata

<A,inf,sup,r>

tzn. zbiór A uporządkowany przez relację r
z dwoma operacjami dwuargumentowymi
inf i sup określonymi dla dowolnych $x,y \in A$
następująco:

inf(x,y) =kres dolny zbioru {x,y} w sensie porządku r,

sup(x,y)=kres górny zbioru {x,y} ze względu na porządek r.

Przykłady systemów algebraicznych

Dwuelementowa algebra Boole'a

Zbiór {true, false} z działaniami

$\neg$: {true, false} $\rightarrow$ {true, false}

$\vee$: {true, false} $\times$ {true, false} $\rightarrow$ {true, false},

$\wedge$: {true, false} $\times$ {true, false} $\rightarrow$ {true, false}

określonymi następująco

$\neg$ true = false, $\neg$ false = true,

true $\vee$ a = true i false $\vee$ a = a dla a $\in$ {true, false}

true $\wedge$ a = a i false $\wedge$ a = false dla a $\in$ {true, false}

tworzy system algebraiczny

$$\mathbf{B_0 = \langle \{true, false\}, \neg, \vee, \wedge, false, true \rangle.}$$

Zwróćmy uwagę, że działania tu przedstawione pokrywają się z operacjami logicznymi. B_0 jest dwuelementową algebrą Boole'a.

Algebra zbiorów

Niech X będzie ustalonym zbiorem. Rozważmy zbiór wszystkich jego podzbiorów z operacjami teoriomnogościowymi uzupełnienia w X, sumy i przecięcia zbiorów. System

$$\langle P(X), -, \cup, \cap, \emptyset, X \rangle$$

jest algebrą: wyniki wszystkich działań zastosowane do podzbiorów zbioru X dają w wyniku podzbiór zbioru X.

Algebra zbiorów

Zwróćmy uwagę, że powyższe struktury (dwuelementowa algebra Boole'a i algebra zbiorów) są podobne.
Każdy z tych algebr ma jedną operację jednoargumentową, dwie operacje dwuargumentowe i dwie stałe.
Rzeczywiście sygnatury tych dwóch systemów są takie same.

Algebra relacji

Niech U będzie niepustym zbiorem. System

$$\langle P(U \times U), \circ, {}^{-1} \rangle,$$

którego uniwersum stanowi zbiór wszystkich relacji binarnych w U, a operacjami są operacja składania i operacja odwracania relacji, jest przykładem systemu algebraicznego.

Sygnatura tego systemu składa się z dwu operacji: jedna z nich, ${}^{-1}$, jest jednoargumentowa, a druga $\circ$ jest operacją dwuargumentową. Zarówno operacja składania relacji binarnych jak i operacja odwracania, zastosowane do relacji binarnych w zbiorze U, prowadzą do relacji binarnej w zbiorze U.

Standardowa struktura stosów

Rozważmy niepusty zbiór E i zbiór S ciągów skończonych, których elementy należą do E.
Zakładamy, że w zbiorze S znajduje się ciąg pusty oznaczony tu przez 'empty', $empty \in S$.
Niech w zbiorze $S \cup E$ będą określone operacje **push**, **pop**, **top** o sygnaturze

$$push: S \times E \to S$$
$$pop: S \to S$$
$$top : S \to E$$

Standardowa struktura stosów

Dla dowolnego ciągu $s = (e_1,e_2,...,e_n)$ i dowolnego elementu $e \in E$, przyjmujemy:

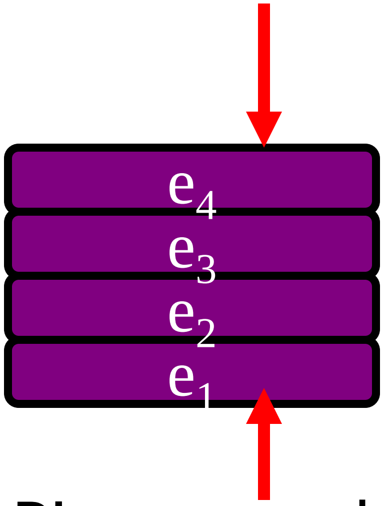
$push((e_1,e_2,...,e_n), e) = (e_1,e_2,...,e_n,e)$ dla wszystkich $n \geq 0$,
$pop((e_1,e_2,...,e_n)) = (e_1,...,e_{n-1})$ o ile $n>0$,
$top((e_1,e_2,...,e_n)) = e_n$ o ile $n>0$.

Operacje pop i top są operacjami częściowymi, bo nie są określone dla elementu 'empty'.

Standardowa struktura stosów

$push((e_1,e_2,e_3,e_4), e) = (e_1,e_2,e_3,e_4,e)$

Ostatni ułożony element

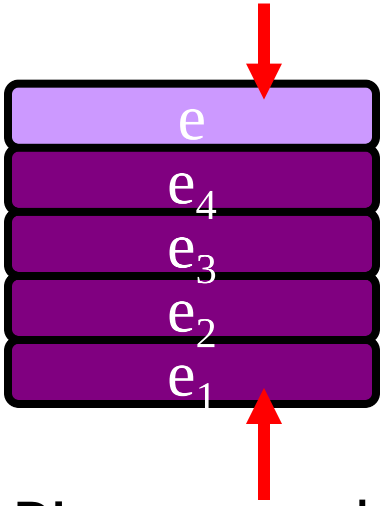


Pierwszy ułożony element

Standardowa struktura stosów

push((e_1,e_2,e_3,e_4), e) = (e_1,e_2 ,e_3,e_4,e)

Ostatni ułożony element



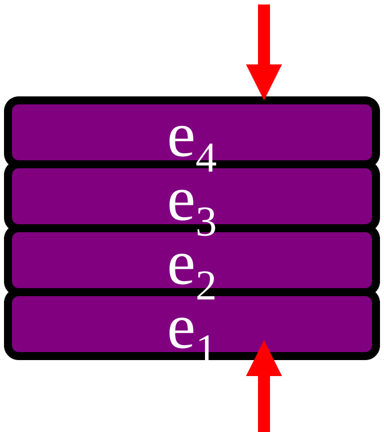
Pierwszy ułożony element

Zauważmy, że argumenty operacji push mają różne typy: jednym z argumentów jest ciąg, a drugim element zbioru E. Jest to więc struktura dwusortowa.

Standardowa struktura stosów

$\mathrm{pop}((e_1,e_2,e_3,e_4)) = (e_1,e_2,e_3)$

Ostatni ułożony element

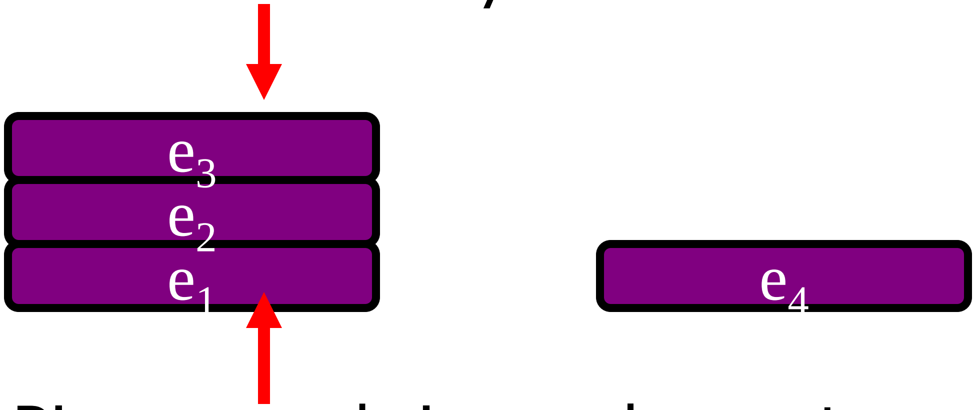


Pierwszy ułożony element

Standardowa struktura stosów

$pop((e_1,e_2,e_3,e_4)) = (e_1,e_2,e_3)$

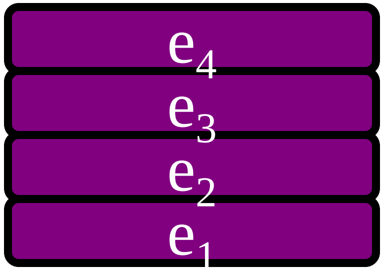
Ostatni ułożony element



Pierwszy ułożony element

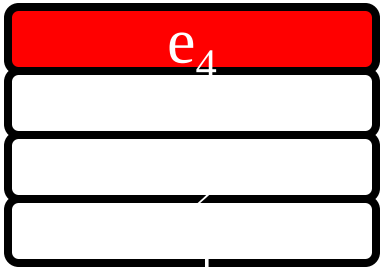
Standardowa struktura stosów

$top((e_1,e_2,e_3,e_4)) = e_4$



Standardowa struktura stosów

$top((e_1,e_2,e_3,e_4)) = e_4$



Standardowa struktura stosów

Wtedy

$<S \cup E$, push, pop, top, empty, $= >$

jest systemem algebraicznym.

System ten nazywamy

standardową strukturą stosów.

Standardowa struktura kolejek

Niech E będzie niepustym zbiorem, a S zbiorem ciągów skończonych o wyrazach należących do E. Zakładamy, tak jak poprzednio, że w zbiorze S znajduje się ciąg pusty oznaczony przez 'empty', empty$\in$S. W zbiorze S$\cup$E definiujemy dwuargumentową operację **in** i dwie jednoargumentowe operacje częściowe **out** i **first** o sygnaturze:

$$in: S \times E \to S,$$

$$out: S \to S,$$

$$first : S \to E.$$

Standardowa struktura kolejek

Dla dowolnego ciągu $(e_1,\ldots,e_n)$ i dowolnego elementu $e \in E$,

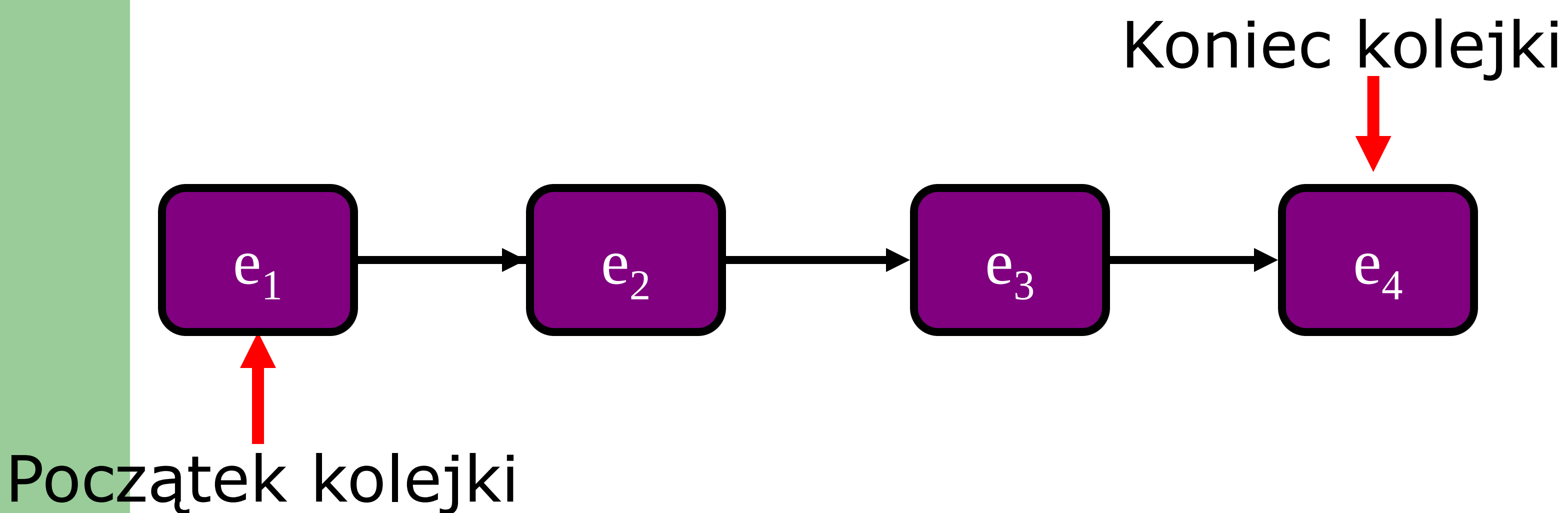
$in((e_1,\ldots,e_n),e)=(e_1,\ldots,e_n,e)$ dla wszystkich $n \geq 0$,

$out((e_1,e_2,\ldots,e_n))=(e_2,\ldots,e_n)$, o ile $n>0$,
i nieokreślone w przeciwnym przypadku,

$first((e_1,e_2,\ldots,e_n))=e_1$, o ile $n>0$, i nieokreślone w przeciwnym przypadku

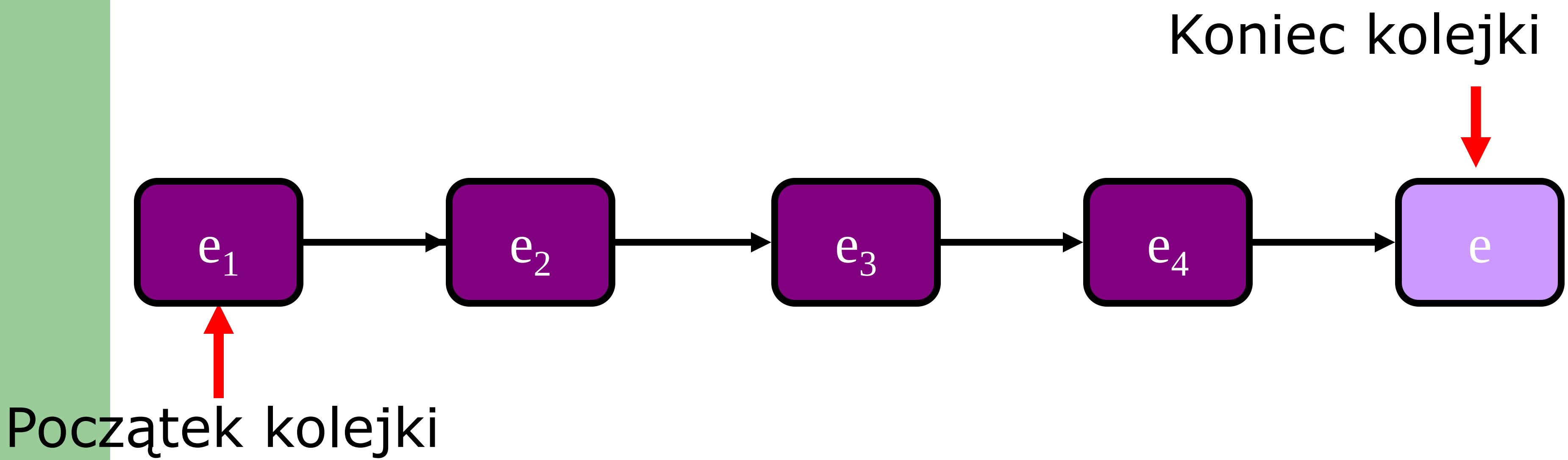
Standardowa struktura kolejek

$in((e_1,e_2,e_3,e_4),e)=(e_1,e_2,e_3,e_4,e)$



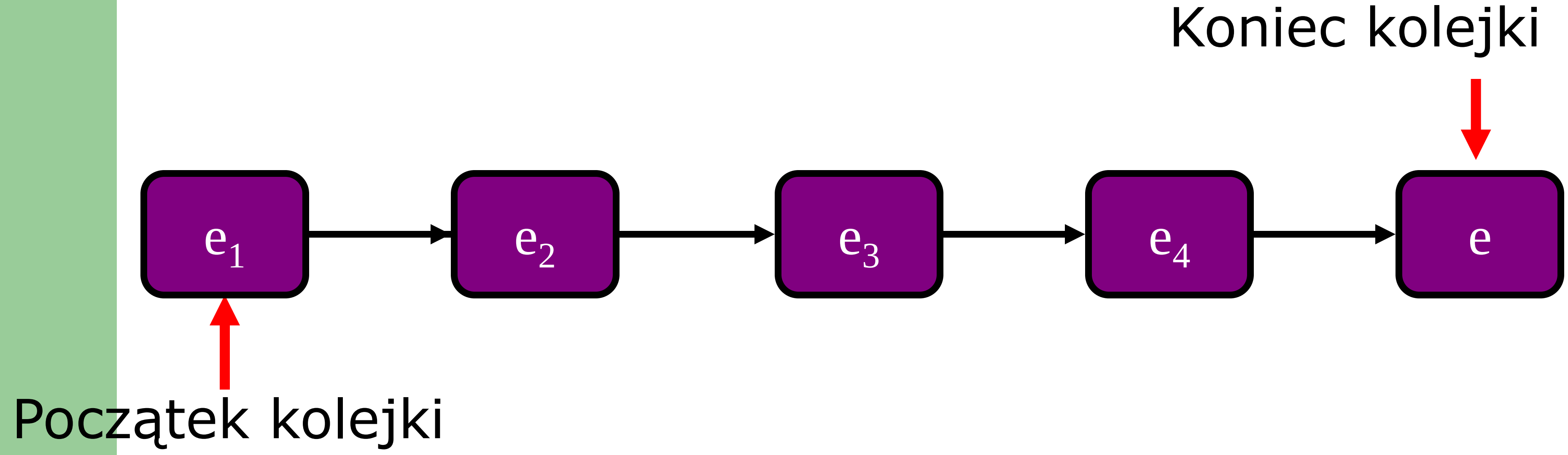
Standardowa struktura kolejek

$in((e_1,e_2,e_3,e_4),e)=(e_1,e_2,e_3,e_4,e)$



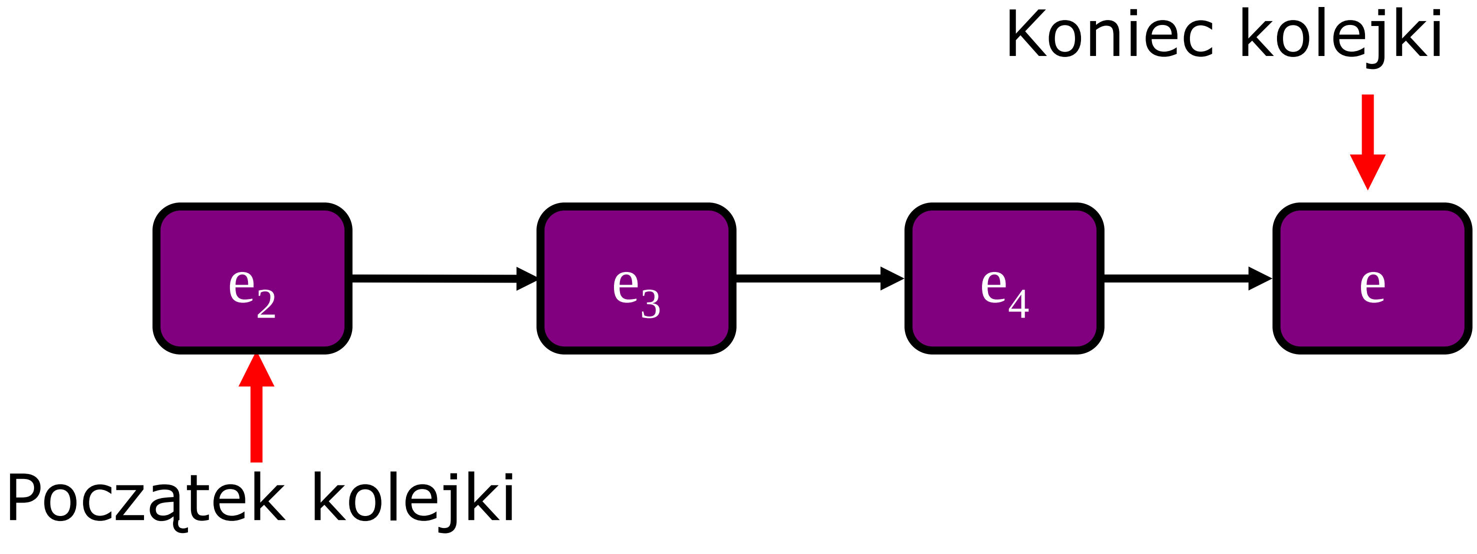
Standardowa struktura kolejek

$\mathrm{out}((e_1,e_2,e_3,e_4))=(e_2,e_3,e_4)$



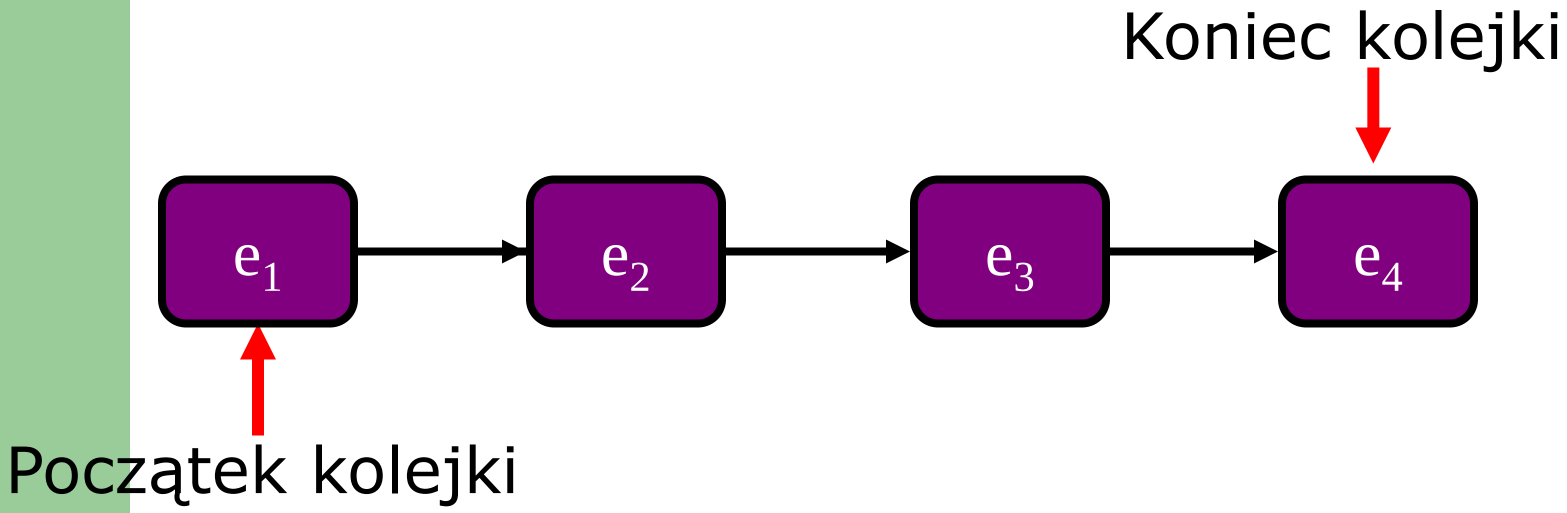
Standardowa struktura kolejek

$out((e_1,e_2,e_3,e_4))=(e_2,e_3,e_4)$



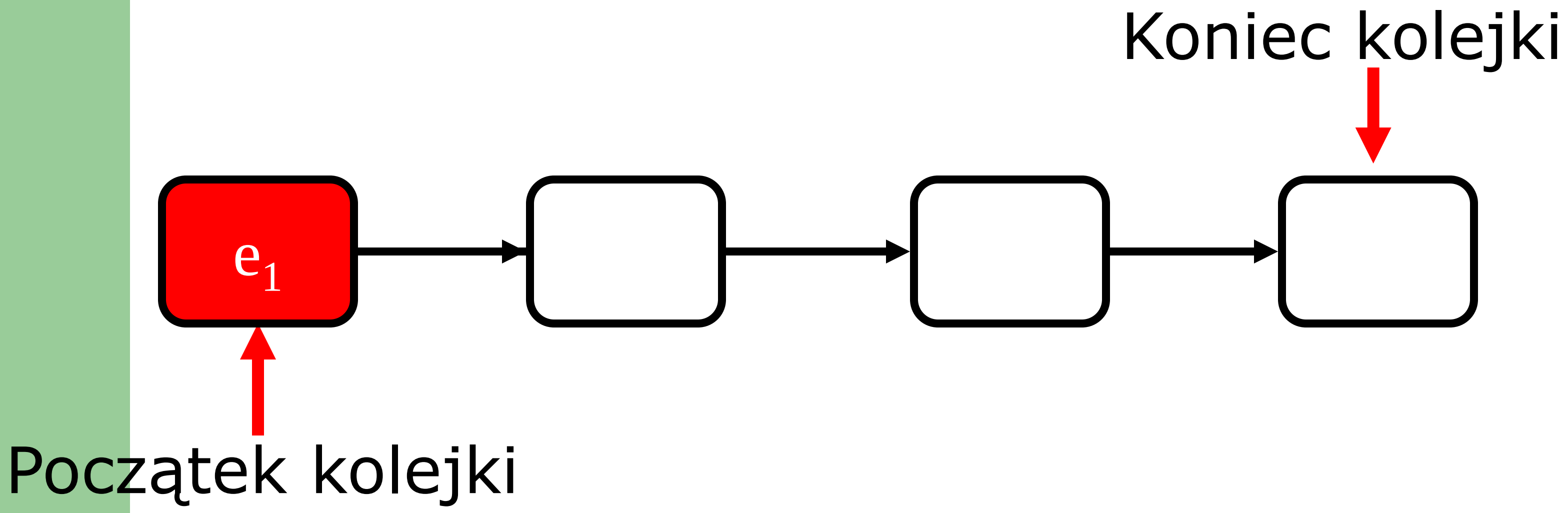
Standardowa struktura kolejek

$first((e_1,e_2,e_3,e_4)) = e_1$



Standardowa struktura kolejek

$\text{first}((e_1, e_2, e_3, e_4)) = e_1$



Standardowa struktura kolejek

System

$< S \cup E, in, out, first, empty, = >$

jest przykładem dwusortowego systemu algebraicznego. Nazywamy go

standardową strukturą kolejek.

Struktura stosów i struktura kolejek mają taką samą sygnaturę. Są to struktury podobne.

Generatory algebr

Intuicje

Niech **A=**< A, o_1, o_2,..., o_n > będzie algebrą.
Jakie elementy zbioru A są konieczne,
by zdefiniować (wygenerować) przy ich pomocy i przy pomocy operacji algebry **A** wszystkie inne elementy uniwersum algebry?

Rozważmy na przykład algebrę <N,+,*>.
Zauważmy, że 2=1+1, 3=1+1+1 itd.

Intuicje

Najmniejszy podzbiór A, który wystarczy do określenia wszystkich innych obiektów, nazywa się zbiorem generatorów algebry.

Podalgebra

Niech **A** = <A,o_1,o_2,...,o_n> będzie algebrą i A' niepustym podzbiorem zbioru A.

Wówczas **A'**=<A',o_1,o_2,...,o_n> nazywamy **podalgebrą** algebry A, jeżeli zbiór A' jest zamknięty ze względu na operacje o_1, o_2,..., o_n.

Podsystem

Jeśli w zbiorze A określone są relacje r_1, r_2, ..., r_m, to są one też określone w podzbiorze A'. Zatem definicję podalgebry możemy rozszerzyć na systemy relacyjne przyjmując, że

$$\mathbf{A'}=<A',o_1,o_2,\ldots,o_n;r_1,r_2,\ldots,r_m>$$

jest **podsystemem** systemu

$$\mathbf{A}=<A,o_1,\ldots,o_n;r_1,\ldots,r_m>$$

wtedy i tylko wtedy, gdy A' $\subseteq$ A i zbiór A' jest zamknięty ze względu na wszystkie operacje o_1, o_2,..., o_n systemu A.

Podsystem

W gruncie rzeczy, operacje i relacje w systemie A' są obcięciami funkcji i relacji systemu A, do zbioru A'.

Przykład

Rozważmy algebrę $<R,+,*>$ jaką tworzy zbiór liczb rzeczywistych z operacjami dodawania i mnożenia. Systemy

$$<R^{+},+,*>, <Q,+,*>, <N,+,*>,$$
$$<P,+,*>, <\{3k:k \in N\},+,*>$$

z operacjami dodawania i mnożenia obciętymi do odpowiednich uniwersów są różnymi podalgebrami systemu $<R,+,*>$.

Intuicje

Łatwo zauważyć, że przecięcie dwóch zbiorów zamkniętych ze względu na pewną operację jest też zamknięte na tę operację. Rzeczywiście, jeśli rozważane zbiory to A i B, i rozważana operacja n-argumentowa o ma własność :
dla dowolnych $a_1,\ldots,a_n \in A$, $o(a_1,\ldots,a_n) \in A$ i
dla dowolnych $b_1,\ldots,b_n \in B$, $o(b_1,\ldots,b_n) \in B$,
to dla $x_1,\ldots,x_n \in A \cap B$, mamy $o(x_1,\ldots,x_n) \in A$
i $o(x_1,\ldots,x_n) \in B$, czyli $o(x_1,\ldots,x_n) \in A \cap B$.

Lemat

Przecięcie dowolnego zbioru podalgebr dowolnej algebry albo jest puste albo samo jest podalgebrą tej algebry.

Definicja generatorów algebr

Niepusty podzbiór G zbioru A nazywamy zbiorem **generatorów** algebry $<A,o_1,o_2,...,o_n>$ wtedy i tylko wtedy, gdy najmniejszą podalgebrą zawierającą G jest sama algebra $<A, o_1, o_2, ..., o_n>$.

O zbiorze G mówimy, że generuje zbiór A.

Uwagi

Z Lematu wynika, że jeśli rozważymy rodzinę podalgebr pewnej algebry zawierających jakiś ustalony niepusty zbiór G, to ich przecięcie też zawiera zbiór G i jest podalgebrą A. Przecięcie wszystkich podalgebr zawierających G jest najmniejszą podalgebrą zawierającą G.

Uwagi

Jeżeli ta najmniejsza podalgebra zawierająca G ma być identyczna z A, to znaczy, że każdy element zbioru A da się otrzymać jako wynik działania pewnej operacji systemu na argumentach z G. Każdy element algebry A można wygenerować z elementów zbioru G stosując odpowiednie operacje systemu.

Przykłady

Zbiorem generatorów algebry

<N,suc,0>

gdzie suc jest operacją następnika w N,
jest zbiór **{0}**.

Rzeczywiście, każda liczba naturalna może być otrzymana z zera przez dodawanie jedynki.
Mamy suc(0)= 1, suc(suc(0))= 2,
suc(suc(suc(0))) = 3 itd.

Przykłady

Zbiorem generatorów algebry

<N,+,*>

jest zbiór **{0,1}**.

Zauważmy, że samo zero ani sama jedynka nie wystarczą.

Przykłady

Zbiorem generatorów algebry

<Z,+,*>

jest zbiór **{-1}**.

Rzeczywiście,
+1 otrzymamy w wyniku mnożenia (-1)*(-1),
a 0 w wyniku dodawania (-1)+(+1).
Każdą dodatnią liczbą całkowitą otrzymamy z zera przez dodawanie 1. Każdą liczbę całkowitą ujemną otrzymamy z 0 przez dodawanie (-1).

Przykłady

Zbiorem generatorów dla struktury stosów

<S∪E,push,pop,top,empty,=>

jest zbiór

{empty}∪E

bo każdy stos możemy utworzyć ze stosu pustego przez włożenie przy pomocy operacji push odpowiednich elementów.

Homomorfizmy i izomorfizmy

Definicja homomorfizmu

Dane są podobne systemy algebraiczne

$$A=<A,o_1,o_2,\ldots,o_n,r_1,r_2,\ldots,r_m>,$$
$$B=<B,o'_1,o'_2,\ldots,o'_n,r'_1,r'_2,\ldots,r'_m>,$$

gdzie o_i i o'_i są odpowiadającymi sobie operacjami oraz r_j i r'_j są odpowiadającymi sobie relacjami.

Definicja homomorfizmu

Homomorfizmem systemu **A** w system podobny **B** nazywamy odwzorowanie h: A $\rightarrow$ B takie, że dla dowolnej k_i-argumentowej operacji o_i w A oraz dla dowolnej k_j-argumentowej relacji r_j i dla dowolnych argumentów a_1, a_2 , ... ze zbioru A mamy

- $h(o_i(a_1,\ldots,a_{ki})) = o'_i(h(a_1),\ldots,h(a_{ki}))$,
- $r_j(a_1,\ldots,a_{kj})$ wttw $r'_j(h(a_1),\ldots,h(a_{kj}))$.

Przykład

Funkcja h przyporządkowująca podzbiorowi zbioru liczb naturalnych wartość 1 (tzn. wartość prawda) tylko wtedy gdy liczba 1 jest jego elementem, tzn. dla dowolnego zbioru $X \subseteq N$,

$$h(X) = 1, \text{ gdy } 1 \in X \text{ i } h(X) = 0, \text{ gdy } 1 \notin X$$

jest homomorfizmem algebry

$$< 2^N, \cup, \cap, - >$$

w dwuelementową algebrę Boole'a

$$< \{0,1\}, \vee, \wedge, \neg >.$$

Przykład

Rzeczywiście, dla dowolnych zbiorów X i Y będących podzbiorami N,

$h(X \cup Y)=1$ wttw $1 \in X \cup Y$ wttw $1 \in X$ lub $1 \in Y$ wttw $h(X)=1$ lub $h(Y)=1$ wttw $h(X) \vee h(Y)=1$.

Zatem $h(X \cup Y)= h(X) \vee h(Y)$.

Przykład

$h(X \cap Y)=1$ wttw $1 \in X \cap Y$ wttw $1 \in X$ i $1 \in Y$ wttw $h(X)=1$ i $h(Y)=1$ wttw $h(X) \wedge h(Y)=1$.

Zatem $h(X \cap Y)=h(X) \wedge h(Y)$.

$h(-X)=1$ wttw $1 \in -X$ wttw $1 \notin X$ wttw $h(X)=0$ wttw $\neg h(X)=1$.

Zatem $h(-X) = \neg h(X)$.

Przykład

Niech E będzie zbiorem cyfr $\{0,1,2,3,\ldots,9\}$.
Rozważmy dwa podobne systemy algebraiczne:
standardową strukturę stosów

$$<S \cup E, push, pop, top, empty>$$

i strukturę

$$<N \cup E, włóż, usuń, pierwszy, 0>,$$

gdzie $0 \in E$, w których operacje są określone następująco: dla dowolnych $e_1, e_2, \ldots, e_n, e \in E$ i $n \in N$, włóż$(n,e)=(n+1)*10+e$,

usuń$(n)=n$ div $10-1$, dla $n>0$,

pierwszy$(n)=n$ mod 10.

Przykład

Funkcja h,

$$h(\text{empty}) = 0,$$
$$h(e) = e,$$
$$h(e_1,e_2...,e_n)=\text{włóż}(h(e_1,e_2...,e_{n-1}),h(e_n))$$

określona dla dowolnych elementów $e_1,e_2,...,e_n,e$ ze zbioru E odwzorowuje zbiór ciągów skończonych S w zbiór liczb naturalnych i ustala homomorfizm między tymi systemami.

Definicja izomorfizmu

Jeżeli h jest homomorfizmem odwzorowującym system **A** w system podobny **B** oraz **h** jest **bijekcją**, to h nazywamy **izomorfizmem**.

Jeśli istnieje izomorfizm odwzorowujący A na B, to systemy **A** i **B** nazywamy izomorficznymi.

Przykład

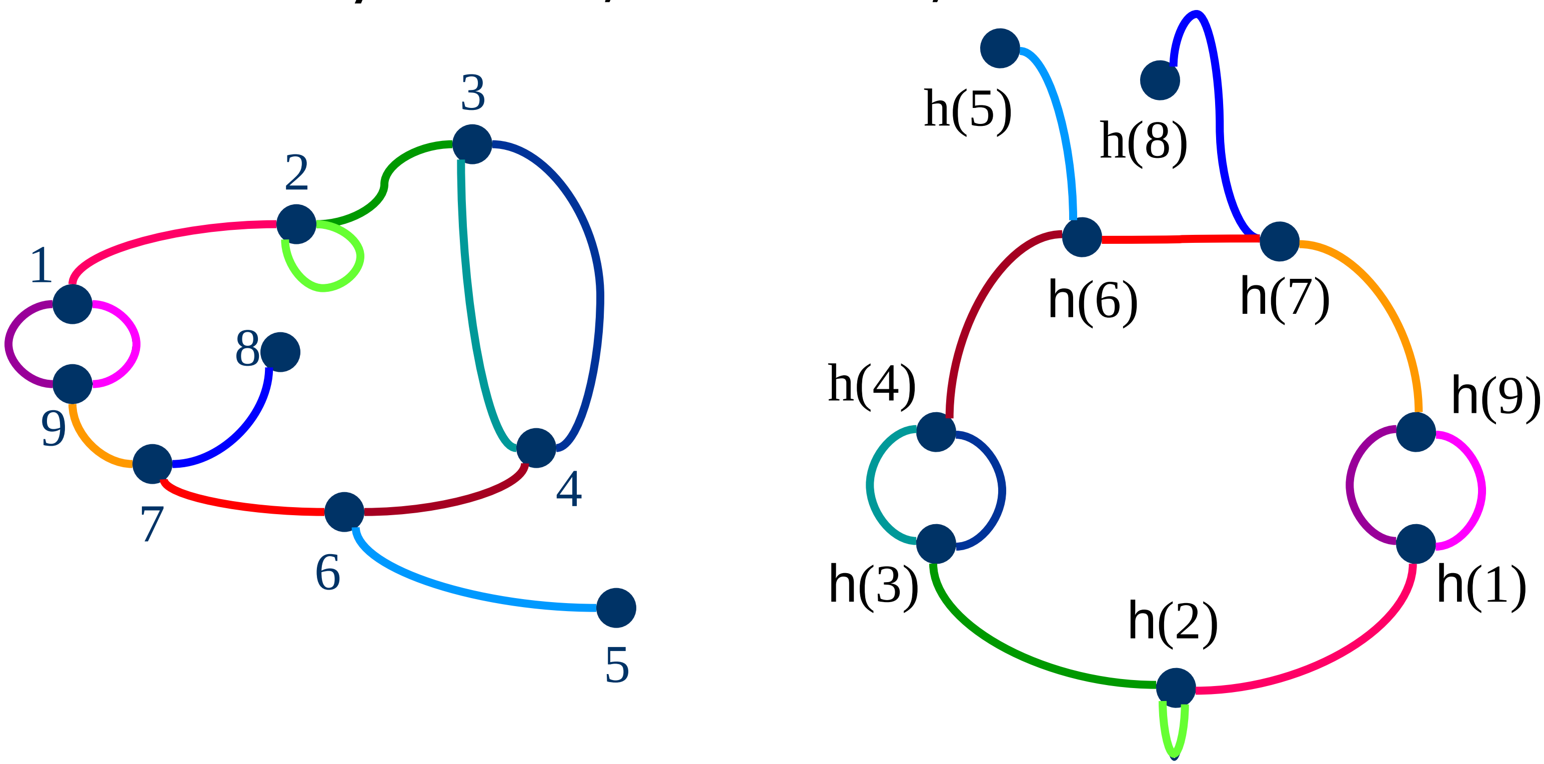
Każdy graf

$$G=\langle V,E\rangle$$

jest przykładem systemu relacyjnego, z jedną relacją binarną.

Przykład

Na rysunku przedstawiliśmy przykład grafów izomorficznych <G',E'> i <G",E">.



Przykład

Funkcja h, która wierzchołkom 1,2,...,9 grafu G' przypisuje odpowiednio wierzchołki h(1),h(2),...,h(9) grafu G", ustala izomorfizm między tymi grafami.

Warunek zachowywania relacji sprowadza się w tym przypadku do równoważności:
dla dowolnych wierzchołków x,y grafu G,

$$(x,y)\in E' \text{ wttw } (h(x),h(y))\in E''.$$

Przykład

Funkcja

$$f(x)=2x$$

odwzorowująca zbiór liczb naturalnych w zbiór liczb parzystych nieujemnych ustala izomorfizm struktur

$$\langle N,+\rangle \text{ i } \langle P^{+},+\rangle.$$

Funkcja f jest różnowartościowa i odwzorowuje liczby naturalne na zbiór liczb parzystych, bo jeśli $x \neq y$, to $2x \neq 2y$ i jeśli $x \in P^{+}$, to $x/2 \in N$ oraz $f(x/2)=x$.

Przykład

Ponadto,

$$f(x+y)=2(x+y)=2x+2y=f(x)+f(y)$$

dla dowolnych liczb naturalnych x i y.

Wynika stąd, że f jest izomorfizmem odwzorowującym system algebraiczny $\langle N,+\rangle$ na system algebraiczny $\langle P^+,+\rangle$.

Własności homomorfizmów i izomorfizmów

Niech h będzie homomorfizmem odwzorowującym system **A** w system algebraiczny **B**.

1. Jeżeli g jest homomorfizmem odwzorowującym system **B** w system algebraiczny **C,** to złożenie ($h \circ g$) jest homomorfizmem odwzorowującym system **A** w system algebraiczny **C**.
2. Obraz homomorficzny uniwersum systemu **A**, h(A), tworzy podalgebrę systemu **B**.

Własności homomorfizmów i izomorfizmów

3. Jeśli zbiór A_0 jest zbiorem generatorów algebry **A** i h jest izomorfizmem, to obraz zbioru generatorów $h(A_0)$ jest zbiorem generatorów algebry **B**.

4. Jeśli h jest izomorfizmem, to systemy **A** i **B** mają taką samą moc, $|A| = |B|$.

Wniosek

Jeżeli h jest izomorfizmem odwzorowującym system **A** na system algebraiczny **B** oraz g jest izomorfizmem odwzorowującym system **B** na system algebraiczny **C,** to złożenie $(h \circ g)$ jest izomorfizmem odwzorowującym system **A** na system algebraiczny **C**.

Twierdzenie

Jeśli dwa homomorfizmy są zgodne (przyjmują te same wartości) na zbiorze generatorów systemu algebraicznego, to są identyczne.

Twierdzenie o izomorfiźmie

Jeżeli h jest izomorfizmem odwzorowującym system algebraiczny **A** na system algebraiczny **B** o sygnaturze S, to dla dowolnej formuły rachunku predykatów α, w której występują tylko operacje i relacje z rozważanej sygnatury

A $\models \alpha$ wtedy i tylko wtedy, gdy **B** $\models \alpha$.

Twierdzenie o izomorfiźmie - intuicje

Systemy izomorficzne są nieodróżnialne przez własności zapisane jako formuły logiki predykatów.

W praktyce oznacza to, że jeśli jakiś warunek jest spełniony w systemie A, to będzie też spełniony w każdym systemie z nim izomorficznym.

Kongruencje

Definicja kongruencji

Niech $A=<A,o_1,o_2,...,o_n,r_1,r_2,...,r_m>$ będzie dowolnym danym systemem algebraicznym. Relację równoważności ~ w A nazywamy

kongruencją

wtedy i tylko wtedy, gdy dla dowolnej n-argumentowej operacji o i relacji r oraz dla dowolnych elementów $a_1, a_2,...,a_n$,

jeżeli $a_1 \sim a'_1$, $a_2 \sim a'_2$, ..., $a_n \sim a'_n$, to

- $o(a_1,a_2 ...,a_n) \sim o(a'_1,a'_2 ,...,a'_n)$,
- $r(a_1,a_2 ,...,a_n)$ wttw $r(a'_1,a'_2 ,..., a'_n)$.

Intuicje

Warunki podane w definicji można interpretować intuicyjnie następująco:

jeżeli argumenty operacji są równoważne,
to wyniki operacji są też równoważne oraz

jeśli jakaś relacja zachodzi dla danych argumentów, to również zachodzi dla argumentów równoważnych.

Przykład

Relacja przystawania modulo p określona w systemie algebraicznym <N,+> jako

$$n \equiv n' \text{ wttw } n \bmod p = n' \bmod p$$

jest kongruencją, bo gdy $a \equiv a'$ oraz $b \equiv b'$, to mamy

$$a \bmod p = a' \bmod p,$$

czyli dla pewnych liczb k i k',

$$a = k \cdot p + c \text{ i } a' = k' \cdot p + c$$

oraz

Przykład

$$b \bmod p = b' \bmod p,$$

czyli dla pewnych m i m',

$$b = m \cdot p + d \text{ i } b' = m' \cdot p + d.$$

Stąd

$$a+b=(k+m)p+(c+d)$$

oraz

$$a'+b'=(k'+m')p+(c+d).$$

Czyli

$$(a+b) \bmod p = (a'+b') \bmod p.$$

Lemat

Niech h będzie homomorfizmem odwzorowującym system algebraiczny **A** w system podobny **B**.
Wtedy relacja:

$$a \sim a' \text{ wttw } h(a) = h(a') \text{ dla } a, a' \in A,$$

jest kongruencją w systemie **A**.

Systemy ilorazowe

Definicja systemu ilorazowego

Niech dany będzie system algebraiczny

$$\mathbf{A} = \langle A, o_1, o_2, \ldots, o_n, r_1, r_2, \ldots, r_m \rangle$$

i niech relacja ~ będzie kongruencją w A. Wtedy system

$$\mathbf{A}/\sim \; = \langle A/\sim, o^*_1, o^*_2, \ldots, o^*_n, r^*_1, r^*_2, \ldots, r^*_m \rangle$$

którego uniwersum stanowi zbiór wszystkich klas abstrakcji relacji ~, a operacje i relacje są zdefiniowane przez następujące równości

- $o^*([a_1],\ldots,[a_n]) =^{df} [o(a_1,\ldots,a_n)]$ dla dowolnej n-argumentowej operacji o^* i dowolnych $a_1,\ldots,a_n$
- $r^*([a_1],\ldots,[a_m])$ wttw $r(a_1,\ldots,a_m)$ dla dowolnej m-argumentowej relacji r^* i dowolnych $a_1,\ldots,a_m$

nazywamy **systemem ilorazowym**.

Przykład

Rozważmy relację $\equiv$ przystawania modulo p (p>0) w zbiorze liczb całkowitych Z. Relacja ta jest kongruencją w algebrze $<Z,+,\times>$. Zbiór klas abstrakcji relacji przystawania modulo p, stanowią klasy reszt modulo p, tzn.

$$[0], [1],\ldots,[p-1].$$

Określmy dwie operacje $\oplus$, $\otimes$ na klasach abstrakcji, dla dowolnych x, y $\in$ Z,

$$[x] \oplus [y] =^{def} [x+y]$$

$$[x] \otimes [y] =^{def} [x \times y]$$

System $\mathbf{<Z/\equiv,\oplus,\otimes>}$ jest systemem ilorazowym otrzymanym z algebry liczb całkowitych przez podzielenie jej przez relację kongruencji modulo p.

Lemat

System ilorazowy **A**/~ jest podobny do **A**,
a odwzorowanie h(a) =^{df} [a] ustala homomorfizm systemów **A** i **A**/~ .

Taki homomorfizm nazywamy
homomorfizmem naturalnym.