Kongruencie v modernej algebre

Miroslav Ploščica

PF UPJŠ Košice, MÚ SAV Košice

November 24, 2008

Kongruencie

Na $\mathbb{Z}$:

$$a \equiv b \ (\mathrm{mod}\, m) \quad \text{ak} \quad m|(a-b)$$

Kľúčová vlastnosť:

$$a \equiv b \ (\mathrm{mod}\, m), \ c \equiv d \ (\mathrm{mod}\, m)$$

implikuje

$$a + c \equiv b + d \ (\mathrm{mod}\, m),$$

$$ac \equiv bd \ (\mathrm{mod}\, m).$$

Algebry

Algebra = množina s operáciami:

$$\mathbf{A} = (A, \{f_i \mid i \in I\})$$

n-árna operácia na množine A: funkcia $A^n \to A$;

Príklady: grupy, okruhy, vektorové priestory, Booleovské algebry, zväzy...

Kongruencie všeobecne

Kongruencia na algebre **A** je relácia ekvivalencie θ na množine A, ktorú zachovávajú všetky základné operácie algebry $\mathbf{A}$, t.j.

$$(a_1, b_1) \in \theta,\ (a_2, b_2) \in \theta, \ldots, (a_n, b_n) \in \theta$$

implikuje

$$(f(a_1, \ldots, a_n), f(b_1, \ldots, b_n) \in \theta))$$

(pre f n-árnu).

Význam kongruencií

Kongruencie umožňujú *faktorizáciu*:
Na množine θ-tried definujeme operácie pomocou reprezentantov:

$$f(a_1/\theta, \ldots, a_n/\theta) = f(a_1, \ldots, a_n)/\theta.$$

Vznikne nová algebra, rovnakého typu ako $\mathbf{A}$, ktorá je zjednodušeným obrazom algebry A.

Napríklad: $\mathbb{Z}/(\mathrm{mod}\, n) = \mathbb{Z}_n$.

Príklad: grupy

A ... komutatívna grupa;
Každá podgrupa B grupy A určuje kongruenciu

$$\theta = \{(a, b) \in A^2 \mid ab^{-1} \in B\}.$$

(Preto hovoríme o faktorizácii grupy podgrupou.)

Podobne: okruhy, vektorové priestory

Príklad: Booleove algebry

$\mathbf{B} = (B; \cup, \cap, ', 0, 1)$
$(B \subseteq \mathcal{P}(X))$;
Ideál: podmnožina $I \subseteq B$ taká, že

- ak $M \in I$, $N \subseteq M$, tak $M \in I$;
- ak $M, N \in I$, tak $M \cup N \in I$.

Každý ideál určuje kongruenciu (a naopak):

$$\theta = \{(M, N) \in B^2 \mid (M \cap N') \cup (M' \cap N) \in I\}.$$

Príklad: reťazce

Uvažujme $(\mathbb{Z}, \max, \min)$ (distributívny zväz)
Platí: Kongruencia je taká ekvivalencia, ktorej každá trieda je interval.

Plán prednášky

- polynómy a kompatibilné funkcie;
- zväzy kongruencií;
- minimálne algebry.

Kompatibilné funkcie 1

n-árna funkcia na algebre $\mathbf{A}$ sa nazýva *kompatibilná*, ak zachováva všetky kongruencie.
Takže: každá základná operácia algebry $\mathbf{A}$ je kompatibilná.
Okrem toho: každá konštantná funkcia je kompatibilná;
Všeobecne: každá polynomická funkcia (zloženie konštánt, projekcií a základných operácií) je kompatibilná.

Kompatibilné funkcie 2

Existujú aj nepolynomické kompatibilné funkcie?
Vo všeobecnosti áno, ale napríklad

Theorem

Na každej Boooleovej algebre je každá kompatibilná funkcia polynomická.

(Dobre známe pre 2-prvkové B. a.)

Kompatibilné funkcie na $\mathbb{Z}$

$f_0(x) = x;$
$f_1(x) = (x-1)x(x+1);$
$f_2(x) = (x-2)(x-1)x(x+1)(x+2);$
$\ldots$

$$F(x) = \sum_{n=0}^{\infty} f_n(x)$$

je kompatibilná (lokálne polynomická), ale nie polynomická.

Kompatibilné funkcie na $\mathbb{Z}$

Fakt 1: Každý (lokálny) polynóm $f(x)$ na $\mathbb{Z}$ spĺňa $8| \ (f(0) - 2f(2) + f(4))$.

Fakt 2: Existuje kompatibilná funkcia $f : \ \mathbb{Z} \to \mathbb{Z}$, ktorá spĺňa $f(0) = 4, \ f(2) = 2, \ f(4) = 4$.

Distributívne zväzy

$\mathbf{D} = (D; \cup, \cap)$
$(B \subseteq \mathcal{P}(X))$;
Typický príklad: $D =$ všetky konečné podmnožiny $\mathbb{N}$
Ktoré (nepolynomické) funkcie sú kompatibilné?

Distributívne zväzy

- špeciálne projekcie:

$$F(X) = X \cap A,$$

kde A je nejaká nekonečná podmnožina $\mathbb{N}$;
(funkcie sú lokálne polynomické)

Distributívne zväzy

- Intervalové komplementácie: pre každé konečné $A \subseteq B$ definujeme

$$c(X) = [(X \cup A) \cap B]';$$

(nie sú lokálne polynomické)

Distributívne zväzy

- množinový rozdiel:

$$f(X, Y) = X \setminus Y.$$

- funkcie, ktoré vzniknú zložením hore uvedených (+polynómov).

Zväzy kongruencií

Kongruencie na algebre $\mathbf{A}$ možno usporiadať reláciou "zjemnenia (= množinovej inklúzie):

$$\varphi \leq \theta \text{ ak } (x\varphi y \text{ implikuje } x\theta y).$$

Vznikne tým usporiadaná množina Con$\mathbf{A}$, v ktorej každé 2 prvky majú najväčšie dolné a najmenšie horné ohraničenie - *zväz*. Con$\mathbf{A}$ vždy obsahuje najmenší aj najväčší prvok.

Zväzy kongruencií

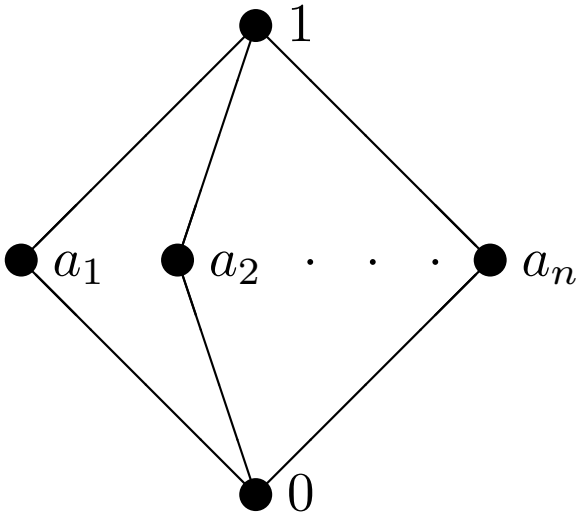
Pre $(\mathbb{Z}, +, \cdot)$:

$$(\mathrm{mod}\, n) \leq (\mathrm{mod}\, m) \quad \text{ak } m|n.$$

Takže: najmenší prvok je $(\mathrm{mod}\, 0)$, najväčší $(\mathrm{mod}\, 1)$, najväčšie dolné ohraničenie (infimum) zodpovedá NSN, najmenšie horné ohraničenie (supremum) je NSD.

Zväzy kongruencií

Nech $\mathbf{A}$ je 2-rozmerný vektorový priestor nad poľom F Každá netriviálna kongruencia vyzerá tak, že jej triedy sú navzájom rovnobežné priamky. Preto zväz $\mathrm{Con}\,\mathbf{A}$ vyzerá nasledovne:



Počet prvkov v strednej vrstve je rovný počtu priamok prechádzajúcich počiatkom. Pre konečné F je $n = |F| + 1$.

Zväzy kongruencií

Je každý zväz izomorfný so zväzom kongruencií nejakej algebry?

Theorem

Zväz je izomorfný so zväzom kongruencií nejakej algebry práve vtedy, keď je algebraický.

Ako vyzerajú zväzy kongruencií špeciálnych druhov algebier?

Zväzy kongruencií

Otvorený problém: Je každý *konečný* zväz (izomorfný so) zväzom kongruencií nejakej *konečnej* algebry?

Ekvivalentná grupová formulácia: Je každý *konečný* zväz (izomorfný s) intervalom vo zväze podgrúp nejakej *konečnej* grupy?

Zväzy kongruencií

Vyriešený problém: Je každý *distributívny* algebraický zväz (izomorfný so) zväzom kongruencií nejakého zväzu?

Odpoveď: nie (F. Wehrung 2005)

Minimálne algebry

Nech konečná algebra $\mathbf{A}$ je jednoduchá. (Nemá netriviálne kongruencie.) Množina $U \subseteq A$ sa nazýva *minimálna*, ak je minimálna medzi všetkými množinami tvaru $f(A)$, kde f je nekonštantný unárny polynóm.
Na U definujeme algebraickú štruktúru tak, že za základné operácie zoberieme všetky polynomické operácie algebry $\mathbf{A}$, voči ktorým je U uzavretá.

Minimálne algebry

Theorem

Pre danú algebru $\mathbf{A}$ sú všetky minimálne algebry navzájom izomorfné a sú ekvivalentné algebre niektorého z piatich nasledujúcich typov:

- *unárna algebra,ktorej každá operácia je permutácia;*
- *vektorový priestor;*
- *2-prvková Booleova algebra;*
- *2-prvkový zväz;*
- *2-prvkový polozväz.*