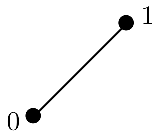
Twierdzenie o pełności – abstrakcja, czy konkret?

Adam KOLANY, Katowice

Czy jest coś bardziej konkretnego niż patyk? No może guz nim nabity na naszej głowie przez kolegę w dzieciństwie. Tak, czy owak, przyjrzyjmy mu się bliżej:

Ponieważ ma być abstrakcyjnie, wyabstrahujmy kształt konkretnego patyka, nadając przy okazji nazwy jego końcówkom:



I cóż my tu widzimy? To oczywiste: dwuelementową kratę, będącą przy okazji algebrą Boole'a, powszechnie zwaną $\mathcal{B}_2$. Takie „dwa w jednym". No i po co to komu? O tym za chwilę. Teraz odrobinę konkretów. Pamiętamy z liceum, co to są tautologie. Ot, takie *formuły zdaniowe*, w których – gdy za poszczególne zmienne wstawimy wartości „0" (fałsz) i „1" (prawda) – dostaniemy zawsze „1" (prawda). Mniejsza teraz o zastosowania tego rodzaju formuł (ludzie rozumni wiedzą, że stanowią one podstawę wszelkich poprawnych rozumowań). To co ważne, to to, że owo „wstawianie" zer i jedynek w miejsce zmiennych, to nic innego jak definiowanie pewnego homomorfizmu z tzw. algebry formuł zdaniowych w naszą $\mathcal{B}_2$ (abstrakcja?). Pójdźmy dalej. Chwila refleksji pozwala nam dostrzec, że jeśli tautologią jest pewna formuła α oraz pewna implikacja o poprzedniku α, to jej następnik też jest tautologią (tzw. reguła odrywania). Zapiszmy to schematycznie:

$$\frac{\alpha,\ \alpha \to \beta}{\beta},\ \text{gdzie } \alpha, \beta \text{ to formuły zdaniowe.}$$

Więcej, jeśli w tautologii za zmienne podstawimy (byle konsekwentnie) jakiekolwiek formuły zdaniowe, to w wyniku otrzymamy znowu tautologię (reguła podstawiania):

$$\frac{\alpha}{h(\alpha)},\ \text{gdzie } \alpha \text{ to formuła zdaniowa, } h \text{ – homomorfizm algebry formuł w siebie.}$$

Pokażemy w tym artykule, że istnieje skończona ilość formuł (konkret), z których korzystając jedynie z powyższych dwu reguł wywieść można wszystkie tautologie. Oczywiście za pomocą tych reguł nie da się z tautologii dostać czegokolwiek innego niż tautologia. To co jednak istotne, to to, że, jak za chwilę zobaczymy, **każdą** tautologię można uzyskać w ten sposób !!

Niech **Ax** oznacza następujący zbiór formuł zdaniowych

$\mathbf{Ax}_1 : \mathsf{p} \to (\mathsf{q} \to \mathsf{p})$ $\quad \mathbf{Ax}_2 : \big(\mathsf{p} \to (\mathsf{q} \to \mathsf{s})\big) \to \big((\mathsf{p} \to \mathsf{q}) \to (\mathsf{p} \to \mathsf{s})\big)$

$\mathbf{Ax}_3 : \mathsf{p} \to \mathsf{p} \vee \mathsf{q}$ $\quad \mathbf{Ax}_4 : \mathsf{q} \to \mathsf{p} \vee \mathsf{q}$ $\quad \mathbf{Ax}_5 : (\mathsf{p} \to \mathsf{s}) \to ((\mathsf{q} \to \mathsf{s}) \to (\mathsf{p} \vee \mathsf{q} \to \mathsf{s}))$

$\mathbf{Ax}_6 : \mathsf{p} \wedge \mathsf{q} \to \mathsf{p}$ $\quad \mathbf{Ax}_7 : \mathsf{p} \wedge \mathsf{q} \to \mathsf{p}$ $\quad \mathbf{Ax}_8 : (\mathsf{s} \to \mathsf{p}) \to ((\mathsf{s} \to \mathsf{q}) \to (\mathsf{s} \to \mathsf{p} \wedge \mathsf{q}))$

$\mathbf{Ax}_9 : (\mathsf{p} \iff \mathsf{q}) \to (\mathsf{p} \to \mathsf{q})$ $\quad \mathbf{Ax}_{10} : (\mathsf{p} \iff \mathsf{q}) \to (\mathsf{q} \to \mathsf{p})$ $\quad \mathbf{Ax}_{11} : (\mathsf{p} \to \mathsf{q}) \to ((\mathsf{q} \to \mathsf{p}) \to (\mathsf{p} \iff \mathsf{q}))$

$\mathbf{Ax}_{12} : \mathsf{p} \to (\neg\mathsf{p} \to \mathsf{q})$ $\quad \mathbf{Ax}_{13} : (\mathsf{p} \to \neg\mathsf{p}) \to \neg\mathsf{p}$ $\quad \mathbf{Ax}_{14} : \neg\neg\mathsf{p} \to \mathsf{p}$

Oczywiście wszystkie one są tautologiami. Niech dalej $\mathbf{Cn}^\star(\mathcal{X})$ oznacza te i tylko te formuły zdaniowe, które wywieść można ze zbioru $\mathcal{X}$ oraz **Ax** za pomocą reguły odrywania i podstawiania oraz niech $\mathbf{Cn}(\mathcal{X})$ oznacza dokładnie te formuły zdaniowe, które wywieść można ze zbioru $\mathcal{X}$ oraz $\mathbf{sb}(\mathbf{Ax})$ tylko za pomocą reguły odrywania $\big(\mathbf{sb}(\mathcal{Y})$ jest zbiorem wszystkich podstawień za zmienne formuł ze zbioru $\mathcal{Y}\big)$. Okazuje się, że $\mathbf{Cn}^\star(\mathcal{X}) = \mathbf{Cn}(\mathbf{sb}(\mathcal{X}))$. Innymi słowy mówiąc, zawsze wywód z $\mathcal{X}$ można przeprowadzić w ten sposób, że najpierw stosuje się regułę podstawiania, a potem odrywania.

Niech $\mathcal{X}$ będzie zbiorem formuł zdaniowych. Zdefiniujmy relację *równoważności Lindenbauma względem* $\mathcal{X}$ między formułami zdaniowymi następująco:

$$\alpha \equiv_{\mathcal{X}} \beta \ \leftrightarrow\ \alpha \iff \beta \in \mathbf{Cn}(\mathcal{X}),\ \text{gdzie } \alpha, \beta \text{ to formuły.}$$

Relacja ta okazuje się być relacją równoważnościową. Więcej, w zbiorze ilorazowym, można w naturalny sposób wprowadzić strukturę algebry (abstrakcja?). Mianowicie jeśli α i β są formułami, to definiujemy

$$\alpha/\mathcal{X} \sqcap \beta/\mathcal{X} = (\alpha \wedge \beta)/\mathcal{X} \text{oraz} \alpha/\mathcal{X} \sqcup \beta/\mathcal{X} = (\alpha \vee \beta)/\mathcal{X},$$

gdzie d $/\mathcal{X}$ jest klasą abstrakcji formuły d względem relacji $\equiv_{\mathcal{X}}$. Oczywiście należałoby jeszcze udowodnić, że definicje te są poprawne, ale to akurat jest prawda. Okazuje się, że otrzymana struktura jest algebrą Boole'a (konkret?), $\mathbf{Cn}(\mathcal{X})$ zaś jest jej największym elementem oraz, że porządek w tej algebrze wyznaczony jest przez implikację. Tzn.

$$\alpha/\mathcal{X} \leq \beta/\mathcal{X} \ \leftrightarrow\ \alpha \to \beta \in \mathbf{Cn}(\mathcal{X}),$$

dla dowolnych dwu formuł α i β. Algebrę tę nazywa się *algebrą Lindenbauma dla zbioru* $\mathcal{X}$. Oznaczymy ją sobie jako $\mathfrak{L}_{\mathcal{X}}$.

Przy użyciu Lematu Kuratowskiego-Zorna dowodzi się, że w każdej algebrze Boole istnieją tzw. *filtry* maksymalne, zwane inaczej *ultrafiltrami*. Tzn. takie domknięte na „$\sqcap$" właściwe podzbiory monotoniczne (tj. spełniające warunek: jeśli $a \in \mathcal{F}$ i $b \geq a$, to $b \in \mathcal{F}$), które już same nie są zawarte w innym filtrze. Więcej, przy wyborze ultrafiltra możemy nieco pomarudzić: mając różny od jedynki (czyli jej elementu największego) element algebry zawsze możemy domagać się, aby dany filtr tego elementu nie zawierał.

Filtry w algebrach Boole'a (a dokładniej w kratach — algebry Boole'a są szczególnymi przypadkami krat) pełnią podobną rolę, jak grupy normalne w grupach czy ideały w pierścieniach – można za ich pomocą definiować kongruencje, a potem przez te ostatnie dzielić. W przypadku filtra maksymalnego, ilorazowa algebra okazuje się być izomorficzna z algebrą dwuelementową — dokładnie tą, od której tę opowieść zaczęliśmy.

I co teraz?

Powiedzmy, że pewna formuła d nie daje się udowodnić ze zbioru założeń $\mathcal{X}$. Wówczas klasa $\Delta =$ d $/\mathcal{X}$ jest różna od jedynki algebry $\mathfrak{L}_{\mathcal{X}}$, którym jak pamiętamy jest $\mathbf{Cn}(\mathcal{X})$. Istnieje zatem ultrafiltr $\mathcal{F}$ w $\mathfrak{L}_{\mathcal{X}}$ omijający klasę Δ. Wówczas jednak w algebrze ilorazowej $\mathfrak{L}_{\mathcal{X}}/\mathcal{F}$ klasa $\Delta/\mathcal{F}$ jest zerem tej algebry. Niech teraz ( ) będzie tym oczywistym izomorfizmem algebry $\mathfrak{L}_{\mathcal{X}}/\mathcal{F}$ na $\mathcal{B}_2$ $\big((\mathcal{F}) = 1,\ (\Delta) = 0\big)$. Zauważmy wówczas, że odwzorowanie „$\alpha \mapsto \Big(\big(\alpha/\mathcal{X}\big)/\mathcal{F}\Big)$" jest homomorfizmem algebry formuł w $\mathcal{B}_2$. Ponieważ formuły ze zbioru $\mathcal{X}$ są w $\mathbf{Cn}(\mathcal{X})$, więc klasa każdej z nich, to dokładnie $\mathbf{Cn}(\mathcal{X})$, które jest jedynką algebry $\mathfrak{L}_{\mathcal{X}}$. Ponieważ jedynka algebry jest w każdym filtrze, wynika stąd, że wartością formuł z $\mathcal{X}$ na jest zawsze 1. Natomiast wartością d jest 0.

Tak więc pokazaliśmy, że jeśli formuła nie ma dowodu d z pewnego zbioru założeń, to istnieje wartościowanie zmiennych (homomorfizm algebry formuł w $\mathcal{B}_2$ – abstrakcja?), które wszystkim formułom tego zbioru przypisuje wartość 1, a formule d wartość 0, albo kontraponując: *jeśli formuła* d *jest prawdziwa ilekroć tylko prawdziwe są formuły z* $\mathcal{X}$, *to* d *daje się udowodnić ze zbioru* $\mathcal{X}$ (tzw. *silne twierdzenie o pełności*). Na odwrót zawsze być musi. W szczególnym przypadku, gdy $\mathcal{X}$ jest pusty, dostajemy tzw. *słabe twierdzenie o pełności*: *Każda tautologia ma dowód.*

W ten oto sposób, wychodząc od konkretu (dwuelementowej algebry Boole'a), poprzez abstrakcję (algebra Lindenbauma, ultrafiltry, algebra ilorazowa), wróciliśmy do konkretu — **twierdzenia o pełności**.

Czy aby na pewno?

Grzegorzewice – Sosnowiec, Sierpień 2008