O weryfikacji tautologii logicznych przy użyciu przekształceń algebraicznych

Adam Lubiński

II Liceum Ogólnokształcące im. Marii Skłodowskiej-Currie w Gorzowie Wielkopolskim w Zespole Szkół Ogólnokształcących nr 2
adam.mariusz.lubinski@gmail.com

30 kwietnia 2024

Streszczenie

W poniższej pracy wprowadzam metodę sprowadzania weryfikacji tautologii logicznych do przekształceń algebraicznych. W tym celu definiuję pojęcie funkcji charakterystycznej zdania logicznego i dowodzę jej własności. Natępnie pokazuję jak je wykorzystać w dowodach tautologii logicznych

1 Wstęp

Lev Kourliandtchik w pierwszym rozdziale książki *Impresje liczbowe* [1] przedstawia niezwykle ciekawy i efektywny sposób dowodzenia równości rachunku zbiorów. Polega on na zdefiniowaniu funkcji charakterystycznej danego zbioru A jako

$$\chi_A(x) = \begin{cases} 1 & \text{dla } x \in A, \\ 0 & \text{dla } x \notin A, \end{cases}$$

co po wyznaczeniu wzorów na funkcje charakterystyczne sum, iloczynów czy różnic teoriomnogościowych, daje mocne narzędzie w dowodzeniu równości dwóch zbiorów, pozwalając na sprowadzenie ich dowodów do serii przekształceń algebraicznych. Po lekkiej modyfikacji tę metodę można także z powodzeniem wykorzystać do sprawdzania prawdziwości tautologii logicznych, czym zajmę się w tej pracy.

2 Definicja

Dla dowolnego zdania logicznego p określmy *funkcję charakterystyczną* χ *zdania* p przez

$$\chi(p) = \begin{cases} 1, & \text{gdy zdanie } p \text{ jest prawdziwe} \\ 0, & \text{gdy zdanie } p \text{ jest nieprawdziwe.} \end{cases}$$

Aby zrobić z niej użytek udowodnimy twierdzenie pozwalające wyznaczać funkcje charakterystyczne zdań połączonych funktorami.

Twierdzenie 1 (O funkcjach charakterystycznych funktorów zdaniotwórczych)**.** *Oznaczmy przez p i q dowolne zdania logiczne. Niech funktory $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$, oznaczają odpowiednio negację, koniukcję, alternatywę, implikację i równoważność zdań. Wtedy:*

(N) $\chi(\neg p) = 1 - \chi(p)$

(K) $\chi(p \wedge q) = \chi(p)\chi(q)$

(A) $\chi(p \vee q) = \chi(p) + \chi(q) - \chi(p)\chi(q)$

(Im) $\chi(p \Rightarrow q) = \chi(p)\chi(q) - \chi(p) + 1$

(R) $\chi(p \Leftrightarrow q) = 2\chi(p)\chi(q) - \chi(p) - \chi(q) + 1$

Dowód. Dla dowodu podpunktu (N) wystarczy zauważyć, że zdania p i $\neg p$, podobnie jak ich funkcje charakterystyczne, przyjmują różne wartości logiczne, czy liczbowe.
By udowodnić pozostałe równości, przyjrzyjmy się tabelom logicznym, które przedstawiają prawdziwość odpowiednich złożeń zdań w zależności od prawdziwości ich składowych i sprawdzimy, że dla wszystkich czterech konfiguracji wartości logicznych zdań p i q powyższe równości zachodzą.

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

p	q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0

p	q	$p \Rightarrow q$
1	1	1
1	0	0
0	1	1
0	0	1

p	q	$p \Leftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

Iloczyn dwóch liczb rzeczywistych jest różny od zera wtedy i tylko wtedy, gdy obie są różne od zera, zatem równość (K) jest prawdziwa. Istotnie, gdy któreś ze zdań p i q jest nieprawdziwe, to któraś z funkcji $\chi(p)$, $\chi(q)$ przyjmuje wartość 0, więc zerem jest wtedy także ich iloczyn. Gdy prawdziwe są oba zdania p i q, to $\chi(p) = \chi(q) = 1$, więc także w tym przypadku równość (K) zachodzi. Podobnie przebiega dowód równości (A). Gdy zdania p i q są prawdziwe, to $\chi(p) + \chi(q) - \chi(p)\chi(q) = 1 + 1 - 1 = 1$, co się zgadza, bo w tym przypadku zdanie $p \vee q$ jest prawdziwe. Gdy zdanie p jest prawdziwe, a zdanie q nie, to $\chi(p) + \chi(q) - \chi(p)\chi(q) = 1 + 0 - 0 = 1$, co zgadza się z tabelą. Podobnie gdy p jest nieprawdziwe, a q jest prawdziwe, dzięki symetrii. Gdy oba zdania p i q są nieprawdziwe, to $\chi(p) + \chi(q) - \chi(p)\chi(q) = 0 + 0 - 0 = 0$, więc równość (A) jest prawdziwa. Analogicznie postępujemy w dowodzie równości (Im). Gdy zdania p i q są prawdziwe, to $\chi(p)\chi(q) + 1 - \chi(p) = 1 + 1 - 1 = 1$, co odpowiada tabeli. Gdy p jest prawdziwe, a q nie, to $\chi(p)\chi(q) + 1 - \chi(p) = 0 + 1 - 1 = 0$, co zgadza się z nieprawdziwością zdania $p \Rightarrow q$ w tym przypadku. Gdy z kolei zdanie p jest nieprawdziwe, a zdanie q jest prawdziwe, to $\chi(p)\chi(q) + 1 - \chi(p) = 0 + 1 - 0 = 1$, co też się zgadza. Jeśli zdania p i q są nieprawdziwe, to $\chi(p)\chi(q) + 1 - \chi(p) = 0 + 1 - 0 = 1$, czyli tak, jak ma być. Pozostało udowodnić równość (R). Jeśli zdania p i q są prawdziwe, to $2\chi(p)\chi(q) - \chi(p) - \chi(q) + 1 = 2 - 1 - 1 + 1 = 1$, co jest zgodne z tabelą. Jeśli jednak p jest prawdziwe, a q nie, to $2\chi(p)\chi(q) - \chi(p) - \chi(q) + 1 = 0 - 1 - 0 + 1 = 0$, co też pasuje. Gdy p jest fałszywe, a q prawdziwe, to $2\chi(p)\chi(q) - \chi(p) - \chi(q) + 1 = 0 - 0 - 1 + 1 = 0$. Jeśli zdania p i q są nieprawdziwe, to $2\chi(p)\chi(q) - \chi(p) - \chi(q) + 1 = 0 - 0 - 0 + 1 = 1$. To kończy dowód wszystkich równości. $\square$

Zanotujmy jeszcze równość $\chi(p)^2 = \chi(p)$, prawdziwą dla dowolnego zdania logicznego p. Wynika ona z tego, że funkcja χ przyjmuje tylko wartości 0 lub 1, będące punktami stałymi podnoszenia do kwadratu. Będziemy z niej korzystać w dalszej części tej pracy.

3 Zastosowanie

Wypróbujmy nasz arsenał w dowodzie *modus tollendo tollens*, czyli tautologii postaci

$$[(p \Rightarrow q) \wedge \neg q] \Rightarrow \neg p.$$

Aby ją udowodnić wystarczy sprawdzić, że

$$\chi\Big([(p \Rightarrow q) \wedge \neg q] \Rightarrow \neg p\Big) = 1,$$

niezależnie od prawdziwości p i q. Zgodnie z równością (Im) otrzymujemy

$$\chi\Big([(p \Rightarrow q) \wedge \neg q] \Rightarrow \neg p\Big) = \chi\Big((p \Rightarrow q) \wedge \neg q\Big)\chi(\neg p) - \chi\Big((p \Rightarrow q) \wedge \neg q\Big) + 1. \quad (\heartsuit)$$

Korzystając z (K), a potem z (N) i z (Im) dostaniemy

$$\begin{aligned} \chi\Big((p \Rightarrow q) \wedge \neg q\Big) &= \chi(p \Rightarrow q)\chi(\neg q) = \Big(\chi(p)\chi(q) - \chi(p) + 1\Big)\Big(1 - \chi(q)\Big) = \\ &= \chi(p)\chi(q) - \chi(p) + 1 - \chi(p)\chi(q)^2 + \chi(p)\chi(q) - \chi(q) = \\ &= \chi(p)\chi(q) - \chi(p) + 1 - \chi(p)\chi(q) + \chi(p)\chi(q) - \chi(q) = \\ &= \chi(p)\chi(q) - \chi(p) - \chi(q) + 1. \end{aligned}$$

Wstawiając to wyrażenie w miejsce $\chi\Big([(p \Rightarrow q) \wedge \neg q]\Big)$ do (♥) otrzymujemy ostatecznie

$$\begin{aligned}
&\chi\Big((p \Rightarrow q) \wedge \neg q\Big)\chi(\neg p) - \chi\Big((p \Rightarrow q) \wedge \neg q\Big)+1 = \\
&= (\chi(p)\chi(q) - \chi(p) - \chi(q) + 1)(1 - \chi(p)) - \chi(p)\chi(q) + \chi(p) + \chi(q) - 1 + 1 = \\
&= \chi(p)\chi(q) - \chi(p) - \chi(q) + 1 - \chi(p)^2\chi(q) + \chi(p)^2 + \chi(p)\chi(q) - \chi(p) - \\
&- \chi(p)\chi(q) + \chi(p) + \chi(q) - 1 + 1 = \\
&= \chi(p)\chi(q) - \chi(p) - \chi(q) + 1 - \chi(p)\chi(q) + \chi(p) + \chi(p)\chi(q) - \chi(p) - \\
&- \chi(p)\chi(q) + \chi(p) + \chi(q) - 1 + 1 = \\
&= 1,
\end{aligned}$$

co kończy weryfikację rozważanej tautologii.

Przy pomocy przedstawianej metody udowodnimy teraz I prawo De Morgana postaci

$$\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q),$$

co jest równoważne z pokazaniem, że

$$\chi\Big(\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)\Big) = 1,$$

niezależnie od wartości logicznych zdań p i q. Dostajemy

$$\chi\Big(\neg(p \wedge q)\Big) = 1 - \chi(p \wedge q) = 1 - \chi(p)\chi(q),$$

najpierw korzystając z (N), a potem z (K). Podobnie

$$\chi\Big((\neg p)\vee(\neg q)\Big) = \chi(\neg p)+\chi(\neg q)-\chi(\neg p)\chi(\neg q) = 1-\chi(p)+1-\chi(p)+(1-\chi(p))(1-\chi(q)) =$$

$$= 1 - \chi(p)\chi(q).$$

Dla przejrzystości wprowadźmy oznaczenia $a = \chi\Big(\neg(p\wedge q)\Big)$ i $b = \chi\Big((\neg p) \vee (\neg q)\Big)$. Widzimy, że dla dowolnych zdań logicznych p i q

$$a = \chi\Big(\neg(p \wedge q)\Big) = \chi\Big((\neg p) \vee (\neg q)\Big) = b.$$

Stąd, korzystając z (R) i z tego, że $a^2 = a = b$, kończymy dowód

$$\chi\Big(\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)\Big) = 2ab - a - b + 1 = 2a^2 - 2a + 1 = 2a - 2a + 1 = 1.$$

4 Czy ta metoda zawsze działa?

W powyższych rozumowaniach korzystaliśmy jedynie z tego, że $\chi(p)^2 = \chi(p)$, co po szkolnych przekształceniach algebraicznych pozwalało bezpośrednio pokazać, że funkcja charakterystyczna dowodzonej tautologii jest tożsamościowo równa 1, z gracją kończąc dowód. Czy zawsze można to zrobić? Czy zawsze jedynie bezmyślnie wymnażając wszystkie nawiasy i stosując własność $\chi(p)^2 = \chi(p)$ wszystkie wyrazy się zredukują i otrzymamy samotną jedynkę? Okazuje się, że tak. W celu udowodnienia tego, wykorzystamy pewien lemat.

Lemat 1. *Niech $F \in \mathbb{R}[X_1, X_2, ..., X_n]$ będzie wielomianem n zmiennych o współczynnikach rzeczywistych oraz*

$$F(X_1, X_2, ..., X_n) = \sum f_{k_1,k_2,...,k_n} X_1^{k_1} X_2^{k_2} ... X_n^{k_n},$$

a $k_i \in \{0, 1\}$ dla wszystkich $i \in \{1, ..., n\}$. Wtedy, jeśli wielomian F przyjmuje wartość 0 dla każdego wyboru $X_1, X_2 ..., X_n \in \{0, 1\}$, to F jest wielomianem zerowym.

Dowód. Nazwijmy l-krotnym jednomian w wielomianie F będący iloczynem l zmiennych: $X_{i_1} X_{i_2} ... X_{i_l}$. Dowiodę tezy przez *silną* indukcję ze względu na krotność współczynników. Bazą indukcji będzie zerowość współczynnika przy jedynym 0-krotnym jednomianie, czyli wyrazie wolnym. Oznaczmy go przez w. Mamy

$$w = F(0, ..., 0) = 0.$$

Załóżmy teraz, że wszystkie współczynniki przy jednomianach o krotności niewiększej niż pewne $s < n$ są równe zero. Niech f_C będzie dowolnym współczynnikiem przy $(s + 1)$-krotnym jednomianie, gdzie C jest pewnym ciągiem binarnym o jedynkach na $s + 1$ miejscach. Wtedy

$$0 = F(C) = f_C,$$

dlatego że na mocy założenia indukcyjnego wszystkie współczynniki przy jednomianach o krotności mniejszej niż $s+1$ są równe 0, a we wszystkich jednomianach o krotności większej lub równej $s + 1$, poza jednomianem przy f_C, za którąś ze zmiennych podstawione zostało zero. Krok indukcyjny jest zatem prawdziwy, co na mocy zasady indukcji matematycznej kończy dowód. □

Teraz możemy przejść do dowodu twierdzenia odpowiadającego na postawione na początku tego ustępu pytanie.

Twierdzenie 2. *Niech P będzie tautologią, powstałą ze zdań $p_1, p_2, ..., p_n$ przy pomocy funktorów zdaniotwórczych z Twierdzenia 1. Wtedy, korzystając jedynie z tego, że $\chi(p)^2 = \chi(p)$ dla dowolnego zdania p można, przeprowadzając szkolne przekształcenia algebraiczne, bezpośrednio pokazać, że $\chi(P) = 1$.*

Dowód. Wyrażenie $\chi(P)$ można potraktować jako wielomian od funkcji charakterystycznych zdań $p_1, p_2, ..., p_n$. Wynika to z tego, że funkcje charakterystyczne zdań połączonych funktorami zdaniotwórczymi są wielomianami od funkcji charakterystycznych tych zdań. Wielokrotnie korzystając z tego, że $\chi(p)^2 = \chi(p)$ dla dowolnego zdania p, otrzymamy wielomian, w którym wszystkie zmienne występują w potędze nie większej niż 1. Oznaczmy ten wielomian przez H. Wielomian $G = H - 1$ spełnia założenia Lematu 1, bo

$$H(X_1, X_2, ..., X_n) = 1$$

dla dowolnego wyboru $X_1, X_2, ..., X_n \in \{0, 1\}$. Zatem $G = 0$, więc $H = 1$, co kończy dowód. □

5 Kwantyfikatory

Zastosujemy teraz opisywaną metodę do badania zdań zawierających kwantyfikatory $\forall$ i $\exists$, ograniczone do zbiorów skończonych.

Twierdzenie 3 (O funkcjach charakterystycznych kwantyfikatorów)**.** *Niech $\varphi(x)$ będzie dowolną funkcją zdaniową, a skończony zbiór X jej dziedziną. Wtedy*

(F) $\chi\Big(\forall_{x\in X}\, \varphi(x)\Big) = \prod_{x\in X} \chi(\varphi(x))$,

(E) $\chi\Big(\exists_{x\in X}\, \varphi(x)\Big) = 1 - \prod_{x\in X}\Big(1 - \chi(\varphi(x))\Big)$.

Dowód. Jeśli $\varphi(x)$ staje się fałszem dla jakiegoś $x_1 \in X$, to $\chi(\varphi(x_1)) = 0$, zatem wtedy iloczyn z podpunktu (F) przyjmuje wartość zero. Jeśli z kolei $\varphi(x)$ jest prawdą dla wszystkich $x \in X$, to $\chi(\varphi(x)) = 1$ dla wszystkich $x \in X$, zatem w tym przypadku iloczyn z podpunktu (F) przyjmuje wartość 1. Zatem podpunkt (F) Twierdzenia 3 jest udowodniony. W przypadku gdy zdanie $\varphi(x)$ jest fałszywe dla wszystkich $x \in X$, to iloczyn obecny w podpunkcie (E) przyjmuje wartość 1, więc lewa strona równości (E) staje się równa 0. Wtedy też zdanie $\exists_{x\in X}\, \varphi(x)$ jest nieprawdziwe, czyli równość zachodzi. Jeśli jednak istnieje taki $x_2 \in X$, że zdanie $\varphi(x_2)$ jest prawdziwe, to prawdziwe jest zdanie $\exists_{x\in X}\, \varphi(x)$, a wyrażenie po prawej stronie równości (E) przyjmuje wartość 1. Dowód Twierdzenia 3 jest zatem zakończony. □

Przetestujmy powyższe twierdzenie w dowodzie prawa de Morgana rachunku kwantyfikatorów:

$$\neg\forall_{x\in X}\, \varphi(x) \Leftrightarrow \exists_{x\in X}\, \neg\varphi(x).$$

Mamy

$$\chi\Big(\neg\forall_{x\in X}\, \varphi(x)\Big) = 1 - \chi\Big(\forall_{x\in X}\, \varphi(x)\Big) = 1 - \prod_{x\in X} \chi(\varphi(x))$$

oraz

$$\chi\Big(\exists_{x\in X}\neg\varphi(x)\Big) = 1 - \prod_{x\in X}\Big(1 - \chi(\neg\varphi(x))\Big) = 1 - \prod_{x\in X} \chi(\varphi(x)).$$

To kończy dowód, gdyż wyrażenia po obu stronach równoważności mają takie same funkcje charakterystyczne. Gdy bowiem oznaczymy je przez a, to otrzymamy

$$\chi\Big(\neg\forall_{x\in X}\, \varphi(x) \Leftrightarrow \exists_{x\in X}\, \neg\varphi(x)\Big) = 2a^2 - a - a + 1 = 2a - a - a + 1 = 1.$$

Zastosowanie funkcji charaketrystycznych pozwala równie łatwo dowieść rozdzielności $\forall$ względem $\wedge$:

$$\forall_{x\in X}(\varphi(x) \wedge \psi(x)) \Leftrightarrow \forall_{x\in X}\, \varphi(x) \wedge \forall_{x\in X}\, \psi(x),$$

gdzie $\varphi(x)$ i $\psi(x)$ to funkcje zdaniowe. Mamy bowiem

$$\begin{aligned}\chi\Big(\forall_{x\in X}(\varphi(x) \wedge \psi(x))\Big) &= \prod_{x\in X} \chi(\varphi(x) \wedge \psi(x)) = \prod_{x\in X} \chi(\varphi(x)) \cdot \chi(\psi(x)) = \\ &= \prod_{x\in X} \chi(\varphi(x)) \cdot \prod_{x\in X} \chi(\psi(x)) = \\ &= \chi\Big(\forall_{x\in X}\, \varphi(x)\Big) \cdot \chi\Big(\forall_{x\in X}\, \psi(x)\Big) = \\ &= \chi\Big(\forall_{x\in X}\, \varphi(x) \wedge \forall_{x\in X}\, \psi(x)\Big).\end{aligned}$$

Funkcje charakterystyczne obu wyrażeń są identyczne, co, tak jak poprzednio, kończy dowód.

6 Dalsze kierunki badań

Możliwe, że zastosowanie funkcji charakterystycznych można dalej rozwijać. Obiecującymi wydają się następujące kierunki badań:

- Zastosowanie opisywanej metody w logice wielowartościowej.
- Analizowanie możliwości stosowania funkcji charakterystycznych w innych działach matematyki.

Literatura

[1] Kourliandtchik Lev, *Impresje Liczbowe. Od Cyfry Do Szeregu*, (Oficyna Wydawnicza Tutor, 2001).