Obwody logiczne a zbiory borelowskie

Adam Radziwończyk-Syta Michał Skrzypczak

3 czerwca 2009

Spis treści

Streszczenie

Poniższy referat wprowadza pojęcie obwodów logicznych o nieskończonej głębokości. Obwody takie okazują się mieć ścisły związek z rodziną borelowskich podzbiorów zbioru Cantora. Metodami teorii obwodów logicznych wskazujemy nieborelowski podzbiór zbioru Cantora.

1 Wprowadzenie

Obwody logiczne stanowią jeden z modeli obliczeń. Klasyczny obwód składa się z pewnej liczby bramek wejściowych, skończenie wielu warstw zawierających bramki *and* i *or*, oraz pewnej liczby bramek wyjściowych. Obwód taki dostaje na wejściu pewną liczbę bitów, dane te zostają przetworzone przez kolejne warstwy, aż do uzyskania wyniku. Istotnymi własnościami każdego obwodu jest jego rozmiar (sumaryczna liczba bramek), oraz głębokość (liczba warstw).

W tym referacie koncentrujemy się na obwodach nieskończonych, o nieskończonej liczbie wejść. Rozszerzamy tę klasę obwodów do klasy obwodów uogólnionych o potencjalnie nieskończonej głębokości.

Badania nieskończonych obwodów borelowskich skończonej głębokości i twierdzenie o nieistnieniu takiego obwodu dla funkcji parzystości, stały się inspiracją dla słynnego twierdzenia Fursta-Saxe-Sipsera o separacji klas AC_0 i NC_1.

Celem referatu jest wskazanie analogii pomiędzy uogólnionymi obwodami logicznymi, a podzbiorami borelowskiemi zbioru Cantora. Głównym wynikiem poniższej pracy jest dowód własności jaką spełniają wszystkie uogólnione obwody logiczne. Wskazane są przykłady funkcji, które tej własności nie mają, więc nie są obliczane przez żaden uogólniony obwód logiczny. Funkcje te indukują nieborelowskie podzbiory zbioru Cantora.

2 Topologia

2.1 Zbiór Cantora

Każdy uogólniony obwód logiczny indukuje w naturalny sposób funkcję, która każdemu ciągowi zero-jedynkowemu przypisuje wartość w zbiorze $\{0, 1\}$. Naturalnym modelem zbioru nieskończonych ciągów binarnych jest zbiór Cantora.

Definicja 2.1. *Zbiór Cantora* $\mathbb{K}$ *jest to zbiór* $\{0, 1\}^\omega$*, z naturalną topologią produktową.*

Przypomnijmy, że topologia produktowa (Tichonowa), to topologia w której zbiory bazowe są to tzw. cylindry. Cylinder $C_{a_0,a_1,\ldots,a_n}$ to zbiór

$$\{x \in \mathbb{K} : x_0 = a_0, x_1 = a_1, \ldots, x_n = a_n\}.$$

Jak łatwo sprawdzić, zdefiniowany powyżej zbiór $\mathbb{K}$ jest homeomorficzny ze znanym z analizy matematycznej podzbiorem odcinka jednostkowego.

2.2 Hierarchia borelowska

W pewnych zastosowaniach (np. w teorii miary) topologia danej przestrzeni jest niewystarczająca, gdyż okazuje się, że badane zbiory są bardziej złożone niż zbiory otwarte, czy domknięte. W takiej sytuacji często rozpatrywanym pojęciem są zbiory borelowskie.

Definicja 2.2. *σ-ciałem zbiorów nazywamy dowolną rodzinę podzbiorów danego zbioru, która jest zamknięta ze względu na dopełnienia, przeliczalne sumy i przeliczalne przecięcia.*

Definicja 2.3. *Dla danej przestrzeni topologicznej X, rodziną zbiorów borelowskich $\mathcal{B}(X)$ nazywamy najmniejsze σ-ciało w X, zawierające wszystkie zbiory otwarte X.*

Istnieje równoważna, bardziej konstruktywna definicja rodziny zbiorów borelowskich.

Definicja 2.4. *Weźmy dowolną przestrzeń topologiczną X. Oznaczmy przed Σ^0_1 (Π^0_1) rodzinę zbiorów otwartych (domkniętych) w X Przez indukcję pozaskończoną, dla każdego $1 < \alpha < \omega_1$, zdefiniujmy Σ^0_α (Π^0_α) jako rodzinę wszystkich zbiorów powstałych jako przeliczalne sumy (przecięcia) zbiorów leżących w $\bigcup_{0<\beta<\alpha} \Pi^0_\beta$ ($\bigcup_{0<\beta<\alpha} \Sigma^0_\beta$). Wreszcie niech*

$$\mathcal{B}(X) = \bigcup_{0<\beta<\omega_1} \Sigma^0_\beta \cup \Pi^0_\beta,$$

oraz

$$\Delta^0_\alpha = \Sigma^0_\alpha \cap \Pi^0_\alpha.$$

Definicja ta wskazuje na naturalną hierarchię zbiorów borelowskich dowolnej przestrzeni.

W przypadku zbioru Cantora powyższa hierarchia ma pewną dodatkową własność. Można ją mianowicie rozszerzyć wstecz, definiując Π^0_0 jako zbiór wszystkich cylindrów w $\mathbb{K}$, oraz analogicznie Σ^0_0 dopełnienia cylindrów. Ponieważ wszystkich cylindrów jest przeliczalnie wiele, więc każdy zbiór otwarty (odp. domknięty) jest sumą (odp. przecięciem) przeliczalnej rodziny cylindrów (odp. dopełnień cylindrów). Wreszcie niech $\Delta_0 = \Sigma^0_0 \cap \Pi^0_0$. Jak łatwo sprawdzić elementy Δ^0_0 to cylindry długości 1.

3 Uogólnione obwody logiczne

Każdy uogólniony obwód logiczny posiada nieskończenie wiele wejść $(x_0, x_1, \ldots)$. Dla każdego wejścia x_i, istnieje też wejście dualne (o wartości przeciwnej) oznaczone $\overline{x_i}$. Każdy uogólniony obwód logiczny ma jedno wyjście powstałe poprzez $\bigvee$, lub $\bigwedge$ przeliczalnej rodziny[1] prostszych obwodów.

[1]Określeniem *przeliczalnie wiele* określamy zarówno skończenie wiele, jak też $\aleph_0$.

Obwody logiczne tworzą hierarchię analogiczną do hierarchii borelowskiej. Poniżej znajduje się indukcyjna definicja kolejnych rodzin obwodów w tej hierarchii.

- Niech Δ_0 będzie rodziną obwodów będących pojedynczymi wejściami (lub wejściami dualnymi). Przykład takiego obwodu, to x_7, czy $\overline{x_{25}}$.
- Następnie, niech Σ_0 (Π_0) będzie rodziną obwodów będących $\bigvee$ ($\bigwedge$) skończonej (potencjalnie pustej) rodziny obwodów należących do Δ_0. Przykład takiego obwodu, to $x_1 \vee \overline{x_4} \vee x_7$ ($\overline{x_0} \wedge \overline{x_5} \wedge x_{1235}$).
- Wreszcie dla $0 < \alpha < \omega_1$, niech Σ_α (Π_α) będzie rodziną obwodów będących $\bigvee$ ($\bigwedge$) przeliczalnej rodziny obwodów typów Π_{β_i} (Σ_{β_i}), dla $0 \leqslant \beta_i < \alpha$. Przykład takiego obwodu, to $C = \bigvee_i C_i$ ($D = \bigwedge_i D_i$), gdzie indeksy i przebiegają jakiś przeliczalny zbiór. Obwody C_i (D_i) z przykładu nazywać będziemy dziećmi obwodu C (D).

Definicja 3.1. *Przez uogólniony obwód logiczny rozumiemy dowolny element zbioru* $\mathcal{C} = \bigcup_{0 \leqslant \beta < \omega_1} \Sigma_\beta \cup \Pi_\beta$.

Relacja *wchodzenia w skład* danego obwodu, jest to domknięcie przechodnie relacji *bycia dzieckiem* obwodu. Jako rozmiar uogólnionego obwodu logicznego przyjmujemy moc zbioru obwodów wchodzących w jego skład. Przez ścieżkę w obwodzie C nazywamy ciąg obwodów $C_0, C_1, \ldots, C_n$, gdzie $C_0 = C$, $C_n \in \Delta_0$, oraz C_{i+1} jest dzieckiem C_i.

Łatwo sprawdzić przez indukcję pozaskończoną, że każdy uogólniony obwód logiczny C ma następujące własności:

- C ma rozmiar przeliczalny,
- każda ścieżka w C ma skończoną długość,
- dla każdego $x \in \mathbb{K}$, wartość $Cx \in \{0, 1\}$ jest dobrze określona w naturalny sposób.

Wobec tego każdy uogólniony obwód logiczny C indukuje funkcję $f_C \colon \mathbb{K} \to \{0, 1\}$, $f_C(x) = Cx$, oraz zbiór $s_C \subseteq \mathbb{K}$ $s_C = f_C^{-1}(1)$.

Powiemy, że dwa obwody są *równoważne*, jeśli indukują te same funkcje.

Rozpatrzmy dowolny obwód logiczny C. Załóżmy, że α jest najmniejszą z liczb porządkowych takich, że $C \in \Sigma_\alpha \cup \Pi_\alpha$. Wtedy powiemy, że obwód C ma *wysokość* $\alpha + 1$.

3.1 Równoważność obwodów i zbiorów borelowskich

Operacja zbioru indukowanego przez obwód s_C zadaje w naturalny sposób funkcję $\int \colon \mathcal{C} \to \mathcal{P}(\mathbb{K})$, $\int(C) = s_C$. Okazuje się, że funkcja ta zachowuje hierarchię układów/borelowską i w ramach tych hierarchii jest „na”. Ściśle rzecz biorąc.

Twierdzenie 3.2. *Dla każdej liczby porządkowej $0 \leqslant \alpha < \omega_1$, funkcja $\int|_{\Sigma_\alpha}$ (odpowiednio $\int|_{\Pi_\alpha}$) prowadzi w Σ^0_α (Π^0_α) i jest „na". Oczywiście symbole Σ, Π jako dziedziny funkcji $\int$ oznaczają rodziny uogólnionych obwodów logicznych, a jako jej przeciwdziedziny oznaczają rodziny zbiorów odpowiedniego poziomu w hierarchii borelowskiej $\mathbb{K}$.*

Dowód. Łatwa indukcja. ■

3.2 Restrykcje

Definicja 3.3. *Restrykcją nazywamy funkcję $\rho\colon \mathbb{N} \to \{0, 1, \star\}$, która zawiera nieskończenie wiele gwiazdek.*

Podstawową operacją związaną z restrykcjami jest ograniczanie nimi funkcji i obwodów. Uściślają to następujące definicje:

Definicja 3.4. *Dla restrykcji ρ i funkcji $f\colon \{0,1\}^\omega \to \{0,1\}$ określamy funkcję $f|_\rho\colon \{0,1\}^\omega \to \{0,1\}$ jako $f|_\rho(\mathbf{x}) = f(\mathbf{y})$, gdzie $\mathbf{y}$ jest równe ρ z zastąpioną i-tą gwiazdką przez x_i.*

Definicja 3.5. *Dla restrykcji ρ i obwodu C określamy obwód $C|_\rho$ jako obwód, w którym zamiast wejścia x_i jest $\rho(i)$ dla $\rho(i) \neq \star$, a zamiast wejścia x_i jest wejście y_j, jeśli $\rho(i)$ jest j-tą gwiazdka w ρ.*

Łatwo sprawdzić, że jeżeli obwód C oblicza funkcję f, to obwód $C|_\rho$ oblicza funkcję $f|_\rho$.

Główną ideą naszego dowodu jest znajdowanie restrykcji, które będą minimalizowały wielkość obwodu $C|_\rho$. Motywuje to następującą definicję:

Definicja 3.6. *Restrykcja ρ jest dobra dla danego obwodu C, jeśli $C|_\rho$ zależy od skończenie wielu pozycji, tzn. istnieje skończony podzbiór $A \subset \mathbb{N}$ taki, że $\forall i \in A\ x_i = y_i \ \Rightarrow C|_\rho(\mathbf{x}) = C|_\rho(\mathbf{y})$.*

Zauważmy, że własność bycia dobrym dla C nie zależy od kształtu obwodu C, a jedynie od funkcji przez niego obliczanej. Korzystając z poniższego faktu możemy podczas konstruowania restrykcji swobodnie zamieniać w obwodzie pewne jego podobwody na równoważne im podobwody innego kształtu.

Twierdzenie 3.7. *Jeśli obwody C i C' obliczają ta samą funkcję i ρ jest dobra dla C, to jest również dobra dla C'.*

Definicja 3.8. *Dla restrykcji ρ i ρ' powiemy, że ρ' jest rozszerzeniem ρ jeżeli $\rho_i \in \{0,1\} \ \Rightarrow \ \rho'(i) = \rho(i)$, tzn. jeśli ρ' powstała przez zastąpienie pewnej liczby gwiazdek przez 0 lub 1 w ρ.*

Oczywiście rozszerzenie rozszerzenia restrykcji jest także jej rozszerzeniem, co będziemy wykorzystywać przy indukcyjnym procesie budowania restrykcji. Ponadto jeśli restrykcja jest dobra dla C, to jej dowolne rozszerzenie także jest.

3.3 Główne twierdzenie

Twierdzenie 3.9. *Dla każdego uogólnionego obwodu logicznego C, restrykcji ρ i skończonego zbioru liczb A, takiego że $\rho(A) = \{\star\}$, istnieje rozszerzenie restrykcji ρ, $\overline{\rho}$, które jest dobre dla C i $\overline{\rho}(A) = \{\star\}$.*

Najpierw wykażemy lemat pomocniczy.

Lemat 3.10. *Dla danego uogólnionego obwodu logicznego C, restrykcji ρ, oraz skończonego zbioru liczb A, takich że $\rho(A) = \{\star\}$, jeśli $C|_\rho$ jest równoważne obwodowi którego wszystkie dzieci są skończone, to istnieje rozszerzenie ρ do $\overline{\rho}$, dobre dla C, o własności $\overline{\rho}|_A = \{\star\}$.*

Dowód. Ponumerujmy wszystkie możliwe funkcje z A do $\{0, 1\}$ jako $(\eta_i)_{i=1,\ldots,k}$, dla pewnego k. Będziemy konstruować ciąg ρ_i indukcyjnie.

Na początku kładziemy $\rho_0 = \rho$. W celu zdefiniowania ρ_{i+1} rozpatrujemy η_i i ρ_i. Jeśli układ C ma ustaloną wartość przy podstawieniu za zmienne wyznaczone przez A wartości wyznaczonych przez η_i, to definiujemy $\rho_{i+1} = \rho_i$. W przeciwnym przypadku pewien z podukładów C_i musi nie mieć wyznaczonej wartości. Zatem istnieją podstawienia pewnych wartości za zmienne przyjmujące wartość $\star$ w ρ_i i spoza A, które ustalają wartość podukładu odpowiednio na 0 lub 1. Ponieważ podukład jest skończony, to te podstawienia mogą dotyczyć tylko skończenie wielu zmiennych. W zależności od typu całego układu C wybieramy to przypisanie, które ustala jego wartość (np. jeżeli C jest typu $\vee$ wybieramy przypisanie ustalające wartość C_i na 1).

Ostatecznie kładziemy $\overline{\rho} = \rho_{k+1}$, gdzie k to ilość funkcji η. Ponieważ w każdym kroku usuwamy skończenie wiele gwiazdek z ρ, to w $\overline{\rho}$ jest ich nieskończenie wiele. W żadnym momencie nie podstawiamy nic za gwiazdki z A, więc także $\overline{\rho}|_A = \{\star\}$. Ponadto wartość układu C zależy jedynie wartości zmiennych wyznaczonych przez A. Jest tak, gdyż przy każdym możliwym przypisaniu wartości zmiennych zadbaliśmy, w kroku odpowiadającym temu przypisaniu, by układ miał ustaloną wartość. ■

Dowód twierdzenia przebiegać będzie przez indukcję pozaskończoną.

Dowód. Oczywiście teza twierdzenia jest prawdziwa dla obwodów wysokości 1, gdyż obwody te są skończone.

Załóżmy, że teza twierdzenia jest prawdziwa dla obwodów o wysokości mniejszej niż pewna liczba porządkowa $1 < \alpha < \omega_1$. Weźmy dowolny obwód C, wysokości α. Weźmy dowolną restrykcję ρ_0, oraz zbiór skończony A_0, taki że $\rho_0(A) = \{\star\}$. Załóżmy, że dzieci obwodu C, to obwody $C_1, C_2, \ldots$. Z założenia indukcyjnego teza twierdzenia jest spełniona dla wszystkich obwodów $C_1, C_2, \ldots$.

Postępujemy przez indukcję, w kroku $i = 1, 2, \ldots$ ustalona jest restrykcja ρ_{i-1}, oraz zbiór skończony A_{i-1}, takie że $\rho_{i-1}(A_{i-1}) = \{\star\}$, oraz restrykcja ρ_{i-1} jest dobra dla obwodów $C_1, C_2, \ldots, C_{i-1}$.

Ponieważ obwód C_i spełnia tezę twierdzenia, to istnieje restrykcja ρ_i, będąca rozszerzeniem ρ_{i-1}, która jest dobra dla C_i i $\rho_i(A_{i-1}) = \{\star\}$. Wiemy też, że istnieje liczba $a_i \notin A_{i-1}$, taka że $\rho_i(a_i) = \star$. Rozpatrzmy $A_i = A_{i-1} \cup \{a_i\}$. Określiliśmy w ten sposób kolejną parę ρ_i, A_i.

Zdefiniujmy $A = \bigcup_i A_i$. Oczywiście zbiór A jest nieskończony, jako suma wstępującej rodziny zbiorów A_i, takich że $\sharp A_i \geqslant i$. Zauważmy dodatkowo, że w ciągu restrykcji ρ_i, kolejne wyrazy powstają z poprzednich, poprzez rozszerzenie (czyli zamianę pewnych gwiazdek na liczby $0, 1$). Wobec tego istnieje funkcja graniczna $\rho\colon \mathbb{N} \to \{0, 1, \star\}$, określona w naturalny sposób. Zauważmy dodatkowo, że $\rho(A) = \{\star\}$, więc ρ jest restrykcją, gdyż zbiór A jest nieskończony. Ponadto ρ jest rozszerzeniem wszystkich restrykcji ρ_i, więc jest dobre dla wszystkich obwodów C_i jednocześnie.

Rozpatrzmy obwód $C|_\rho$. Ponieważ restrykcja ρ jest dobra dla wszystkich dzieci obwodu C, to istnieje obwód C' o dzieciach $C'_1, C'_2, \ldots$, takich że wszystkie obwody C'_i są skończone, oraz $C|_\rho$ jest równoważny C'.

Wystarczy teraz zastosować powyższy lemat, do obwodu C, restrykcji ρ i zbioru A_0, by otrzymać rozszerzenie ρ do restrykcji $\overline{\rho}$, z zachowaniem warunku $\overline{\rho}(A_0) = \{\star\}$. $\overline{\rho}$ jest szukanym rozszerzeniem ρ_0. ■

Treść powyższego lematu jest zmodyfikowanym rozumowaniem pochodzącym z nieopublikowanej pracy Sipsera. Lemat ten pozwalał udowodnić twierdzenie podobne do powyższego, dla obwodów o skończonej wysokości. Nowym wkładem jest rozumowanie poprzez indukcję pozaskończoną, które dowodzi twierdzenia dla uogólnionych obwodów logicznych.

Można wymagać, by skonstruowana w dowodzie powyższego twierdzenia restrykcja $\overline{\rho}$, miała tę własność, że $C_{\overline{\rho}}$ zależy dokładnie od zmiennych ze zbioru A_0.

4 Wnioski

Sformułowanie głównego twierdzenia jest w podanej postaci, by możliwie uprościć jego dowód indukcyjny. Jednak w jego stosowaniu zwykle wystarczy posłużyć się podaną poniżej prostszą wersją twierdzenia.

Twierdzenie 4.1. *Dla każdego uogólnionego obwodu logicznego C i restrykcji ρ, istnieje rozszerzenie ρ, $\overline{\rho}$ takie, że $C|_{\overline{\rho}}$ indukuje funkcję stałą.*

Powyższe twierdzenie pozwala w łatwy sposób dowodzić, że określone funkcje nie mogą być obliczane przez żadne obwody logiczne. Podstawowym przykładem takich funkcji są funkcje parzystości.

Definicja 4.2. *Funkcją parzystości nazwiemy dowolną funkcję $p\colon \mathbb{K} \to \{0, 1\}$, o własności:*

Dla każdych $x \in \mathbb{K}$, oraz $x' \in \mathbb{K}$, różniących się na dokładnie jednej pozycji, zachodzi

$$p(x) \neq p(x').$$

Jak łatwo sprawdzić korzystając z aksjomatu wyboru, funkcje parzystości istnieją.

Niech p będzie dowolną funkcją parzystości. Jednocześnie, nie istnieje restrykcja ρ, taka by $p|_\rho$ było funkcją stałą, wobec czego p nie jest obliczane przez żaden uogólniony obwód logiczny. A co za tym idzie $P = p^{-1}(1)$ nie jest zbiorem borelowskim w $\mathbb{K}$.

Przy okazji, ponieważ zbiór Cantora jest domkniętym podzbiorem prostej $\mathbb{R}$, więc też P nie jest borelowskim podzbiorem $\mathbb{R}$.

Literatura

[1] M. Sipser, *On polynomial vs. exponential growth*, unpublished (1981).