Topologia zbioru Cantora a obwody logiczne

Adam Radziwończyk-Syta   Michał Skrzypczak

Uniwersytet Warszawski

1 lipca 2009

http://students.mimuw.edu.pl/~mskrzypczak/dokumenty/obwody.pdf

Zbiór Cantora

Definicja

Przez zbiór Cantora K oznaczamy obraz zbioru $\{0,2\}^{\mathbb{N}}$ przy funkcji

$$(x_0, x_1, \ldots) \mapsto \sum_{i=0}^{\infty} x_i \frac{1}{3^{i+1}}.$$

Zbiór Cantora

Fakt

$$\mathbb{K} \simeq_{\mathsf{Top}} \{0,1\}^{\mathbb{N}}$$

Hierarchia borelowska

Definicja indukcyjna dla $\alpha < \omega_1$ i w odniesieniu do zbioru Cantora. W ogólnej przestrzeni top. jest tak samo, ale zaczyna się od 1.

Definicja

- Σ^0_0 – *skończone sumy zbiorów* $\{x_i = b_i\}$, *dla* $b_i \in \{0, 1\}$,
- Π^0_0 – *skończone przecięcia zbiorów* $\{x_i = b_i\}$, *dla* $b_i \in \{0, 1\}$,
- Σ^0_α – *przeliczalne sumy zbiorów z* $\bigcup_{\beta<\alpha} \Pi^0_\beta$,
- Π^0_α – *dopełnienia zbiorów z* Σ^0_α,
- $\Delta^0_\alpha = \Sigma^0_\alpha \cap \Pi^0_\alpha$.

$$
\begin{tikzcd}
 & \mathbf{\Sigma}^0_0 \arrow[dr] & & \mathbf{\Sigma}^0_1 \arrow[dr] & & \mathbf{\Sigma}^0_2 & \cdots & & \mathbf{\Sigma}^0_\alpha \arrow[dr] & & \cdots \\
\mathbf{\Delta}^0_0 \arrow[ur] \arrow[dr] & & \mathbf{\Delta}^0_1 \arrow[ur] \arrow[dr] & & \mathbf{\Delta}^0_2 \arrow[ur] \arrow[dr] & & \cdots & \mathbf{\Delta}^0_\alpha \arrow[ur] \arrow[dr] & & \mathbf{\Delta}^0_{\alpha+1} & \cdots \\
 & \mathbf{\Pi}^0_0 \arrow[ur] & & \mathbf{\Pi}^0_1 \arrow[ur] & & \mathbf{\Pi}^0_2 & \cdots & & \mathbf{\Pi}^0_\alpha \arrow[ur] & & \cdots
\end{tikzcd}
$$

Zbiory borelowskie

Definicja

Przez $\mathcal{B}$ oznaczamy rodzinę

$$\bigcup_{\alpha<\omega_1} \Sigma^0_\alpha \cup \Pi^0_\alpha.$$

Zbiory te nazywamy borelowskimi podzbiorami zbioru Cantora.

Definicja

Każdy zbiór borelowski B ma dobrze określoną pozycję w hierarchii (swoją złożoność), jako najmniejszą liczbę porządkową α, że $B \in \Sigma^0_\alpha \cup \Pi^0_\alpha$.

Zbiory borelowskie – własności

Fakt

Rodzina zbiorów borelowskich jest zamknięta ze względu na przeliczalne sumy, przecięcia i dopełnienia.

Fakt

Hierarchia borelowska jest ścisła – żadna inkluzja na poniższym obrazku nie jest równością. Więc istnieją zbiory borelowskie o dowolnie dużych złożonościach ($< \omega_1$).

$$\begin{tikzcd}
& \mathbf{\Sigma}^0_0 \arrow[dr] & & \mathbf{\Sigma}^0_1 \arrow[dr] & & \mathbf{\Sigma}^0_2 & \cdots & & \mathbf{\Sigma}^0_\alpha \arrow[dr] & & \cdots \\
\mathbf{\Delta}^0_0 \arrow[ur] \arrow[dr] & & \mathbf{\Delta}^0_1 \arrow[ur] \arrow[dr] & & \mathbf{\Delta}^0_2 \arrow[ur] \arrow[dr] & & \cdots & \mathbf{\Delta}^0_\alpha \arrow[ur] \arrow[dr] & & \mathbf{\Delta}^0_{\alpha+1} & \cdots \\
& \mathbf{\Pi}^0_0 \arrow[ur] & & \mathbf{\Pi}^0_1 \arrow[ur] & & \mathbf{\Pi}^0_2 & \cdots & & \mathbf{\Pi}^0_\alpha \arrow[ur] & & \cdots
\end{tikzcd}$$

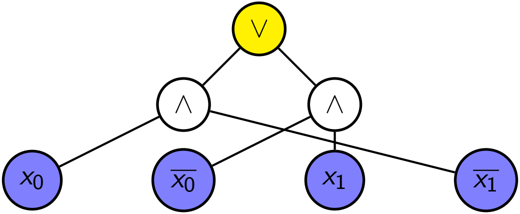
Obwody logiczne

Obwód C o n wejściach:

- bramki wejściowe $x_0, x_2, \ldots, x_{n-1}$,
- jedna bramka wyjściowa,
- bramki typu $\vee$, $\wedge$, $\neg$,
- wyznacza $f_C \colon \{0,1\}^n \to \{0,1\}$.

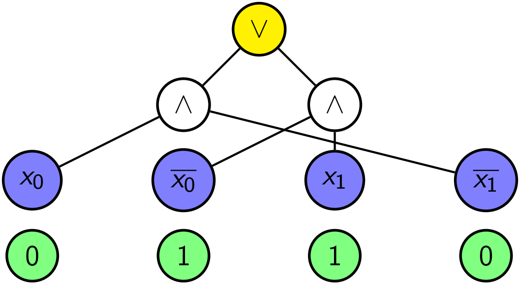
Obwody logiczne – przykład

Obwód obliczający $x_0 \ \mathrm{XOR} \ x_1$:



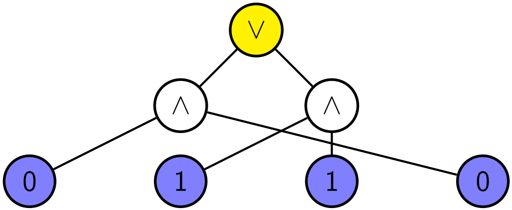
Obwody logiczne – przykład

Obwód obliczający $x_0 \text{ XOR } x_1$ – obliczenie dla $x_0 = 0$ i $x_1 = 1$:



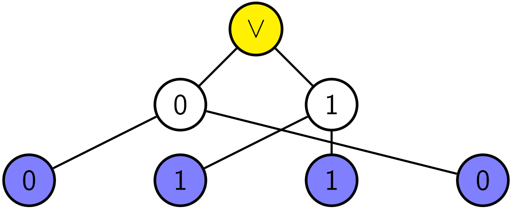
Obwody logiczne – przykład

Obwód obliczający $x_0 \ \mathrm{XOR} \ x_1$ – obliczenie dla $x_0 = 0$ i $x_1 = 1$:



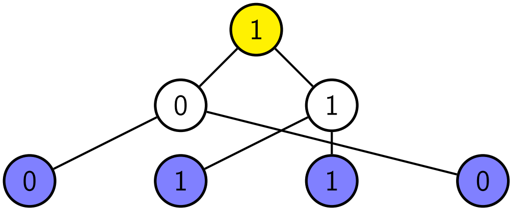
Obwody logiczne – przykład

Obwód obliczający $x_0 \ \mathrm{XOR} \ x_1$ – obliczenie dla $x_0 = 0$ i $x_1 = 1$:



Obwody logiczne – przykład

Obwód obliczający $x_0 \ \mathrm{XOR} \ x_1$ – obliczenie dla $x_0 = 0$ i $x_1 = 1$:



Własności obwodów logicznych

Parametry:

- głębokość (długość najdłuższej ścieżki),
- rozmiar (ilość bramek),
- nieograniczone stopnie wejściowe vs. ograniczone stopnie wejściowe.

Własności obwodów logicznych

Parametry:

- głębokość (długość najdłuższej ścieżki),
- rozmiar (ilość bramek),
- nieograniczone stopnie wejściowe vs. ograniczone stopnie wejściowe.

Własności:

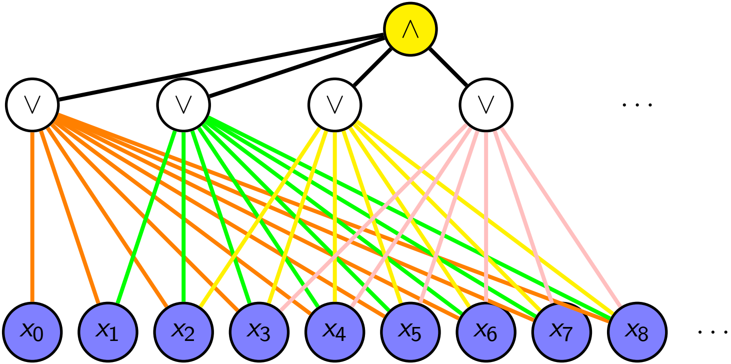
- negacje można przesunąć w dół do zmiennych,
- obwody odpowiadają formułom boolowskim,
- ciąg obwodów $(C_i)_{i\in\mathbb{N}}$ gdzie C_n ma n wejść $\approx$ model maszyny rozpoznającej słowa nad $\Sigma = \{0, 1\}$.

Nieskończone obwody logiczne (Sipser)

- nieskończenie wiele wejść $x_0, x_1, \ldots$,
- nieskończone stopnie wejściowe,
- skończenie wiele warstw,
- dane dla obwodu to nieskończone ciągi $0, 1$ – elementy zbioru Cantora.

Przykład

Nieskończony obwód rozpoznający słowa z nsk. wieloma 1:



Uogólnione obwody logiczne

- nieskończenie wiele wejść $x_0, x_1, \ldots$,
- nieskończone stopnie wejściowe,
- niekoniecznie skończona wysokość.

Uogólnione obwody logiczne

- nieskończenie wiele wejść $x_0, x_1, \ldots$,
- nieskończone stopnie wejściowe,
- niekoniecznie skończona wysokość.

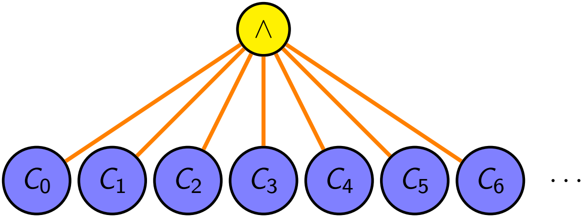
Definicja indukcyjna (dla $\alpha < \omega_1$):

- Σ_0 – skończona alternatywa zmiennych lub ich negacji,
- Π_0 – skończona koniunkcja zmiennych lub ich negacji,
- Σ_α – przeliczalna alternatywa obwodów należących do $\bigcup_{\beta<\alpha} \Pi_\beta$,
- Π_α – przeliczalna koniunkcja obwodów należących do $\bigcup_{\beta<\alpha} \Sigma_\beta$,

Analogicznie jak u Sipsera, ale wysokość obwodu jest dowolną liczbą porządkową!

Przykład

Obwód wysokości ω:



Gdzie C_n jest obwodem wysokości n.
Generalnie istnieją obwody dowolnie dużej wysokości mniejszej niż ω_1.

Odpowiedniość

Fakt

- *Jeśli obwód* $C \in \Sigma_\alpha$, *to* $f_C^{-1}(\{1\}) \in \Sigma^0_\alpha$.
- *Jeśli zbiór* $A \in \Sigma^0_\alpha$, *to istnieje obwód* $C \in \Sigma_\alpha$ *taki, że* $f_C = \Xi_A$.

Odpowiedniość

Fakt

- *Jeśli obwód* $C \in \Sigma_\alpha$, *to* $f_C^{-1}(\{1\}) \in \Sigma^0_\alpha$.
- *Jeśli zbiór* $A \in \Sigma^0_\alpha$, *to istnieje obwód* $C \in \Sigma_\alpha$ *taki, że* $f_C = \Xi_A$.

Wniosek

Hierarchia borelowska i hierarchia obwodów są w odpowiedniej odpowiedniości.
Więc m.in. hierarchia obwodów jest ścisła!

Restrykcje

Definicja

Restrykcją nazywamy dowolny nieskończony ciąg symboli ze zbioru $\{0, 1, \star\}$*, zawierający nieskończenie wiele znaków* $\star$*.*

Restrykcje

Definicja

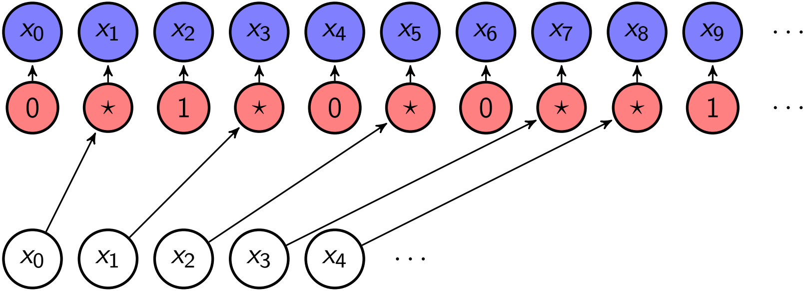
Restrykcją nazywamy dowolny nieskończony ciąg symboli ze zbioru $\{0, 1, \star\}$, *zawierający nieskończenie wiele znaków* $\star$.

Definicja

Dla danego obwodu C, *oraz restrykcji* ρ, *przez* $C|_\rho$ *oznaczamy obwód, w którym za poszczególne zmienne zostały podstawione symbole* ρ. *Tam gdzie w* ρ *występuje* $\star$, *zostają wpisane nowe zmienne.*

Obcięcie obwodu restrykcją

Mamy obwód C (pokazane są tylko jego wejścia, z pominiętymi negacjami), oraz restrykcję ρ:



Powstaje nowy obwód $C|_\rho$.

Fakt

Zamiast obcinać restrykcją obwód, można obciąć funkcję przez niego obliczaną i to komutuje:
Jeśli $f_C = f_{C'}$, *to*

$$f_{C|_\rho} = f_{C'|_\rho} = (f_C)|_\rho.$$

Fakt

Zamiast obcinać restrykcją obwód, można obciąć funkcję przez niego obliczaną i to komutuje:
Jeśli $f_C = f_{C'}$, *to*

$$f_{C|_\rho} = f_{C'|_\rho} = (f_C)|_\rho.$$

Fakt

Dla danych ρ_1, ρ_2, *istnieje restrykcja* $\rho_1 \circ \rho_2$ *taka że dla każdego obwodu* $(C|_{\rho_1})|_{\rho_2} \equiv C|_{\rho_1 \circ \rho_2}$. *Powstaje ona przez podstawienie symboli* ρ_1 *w gwiazdki* ρ_2.

Fakt

Zamiast obcinać restrykcją obwód, można obciąć funkcję przez niego obliczaną i to komutuje:
Jeśli $f_C = f_{C'}$*, to*

$$f_{C|_\rho} = f_{C'|_\rho} = (f_C)|_\rho.$$

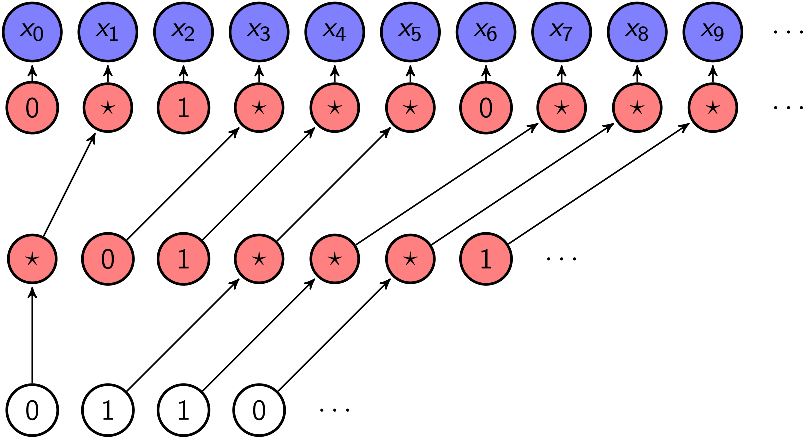
Fakt

Dla danych ρ_1, ρ_2*, istnieje restrykcja* $\rho_1 \circ \rho_2$ *taka że dla każdego obwodu* $(C|_{\rho_1})|_{\rho_2} \equiv C|_{\rho_1 \circ \rho_2}$*. Powstaje ona przez podstawienie symboli* ρ_1 *w gwiazdki* ρ_2*.*

Definicja

Restrykcja ρ_2 *jest rozszerzeniem* ρ_1*, jeśli powstaje z* ρ_1 *przez zastąpienie pewnych gwiazdek cyframi* $\{0, 1\}$*.*

Przykład


x_0
x_1
x_2
x_3
x_4
x_5
x_6
x_7
x_8
x_9
...
0
$\star$
1
$\star$
$\star$
$\star$
0
$\star$
$\star$
$\star$
...
$\star$
0
1
$\star$
$\star$
$\star$
1
...
0
1
1
0
...

Dobre restrykcje

Definicja

Restrykcja ρ jest dobra dla obwodu C, jeśli wartość $C|_\rho$ zależy tylko od skończenie wielu zmiennych.

Fakt

Rozszerzenie restrykcji dobrej dla danego obwodu też jest dla niego dobre.

Fakt

Jeśli ρ jest dobre dla C, to istnieje rozszerzenie ρ ustalające wartość C.

Główne twierdzenie

Twierdzenie

Dla każdego uogólnionego obwodu logicznego C, istnieje restrykcja ρ, taka że $C|_\rho$ ma stałą wartość (niezależną od wejść).

Główne twierdzenie

Twierdzenie

Dla każdego uogólnionego obwodu logicznego C, istnieje restrykcja ρ, taka że $C|_\rho$ ma stałą wartość (niezależną od wejść).

Dowód składa się z dwóch części:

- Lemat pozwala znaleźć restrykcję dobrą dla dowolnego nieskończonego obwodu, którego wszystkie dzieci są skończone.

Główne twierdzenie

Twierdzenie

Dla każdego uogólnionego obwodu logicznego C, istnieje restrykcja ρ, taka że $C|_\rho$ ma stałą wartość (niezależną od wejść).

Dowód składa się z dwóch części:

- Lemat pozwala znaleźć restrykcję dobrą dla dowolnego nieskończonego obwodu, którego wszystkie dzieci są skończone.
- Główne rozumowanie dowodzi indukcyjnie ze względu na wysokość obwodu tezy. Jednym z kroków rozumowania jest skorzystanie z lematu.

Lemat pochodzący od Sipsera

Lemat

Dla dowolnego obwodu C którego wszystkie dzieci są skończone, oraz skończonego zbioru A, istnieje restrykcja ρ, taka że $\rho(A) = \{\star\}$ i ρ jest dobre dla C.

Lemat pochodzący od Sipsera

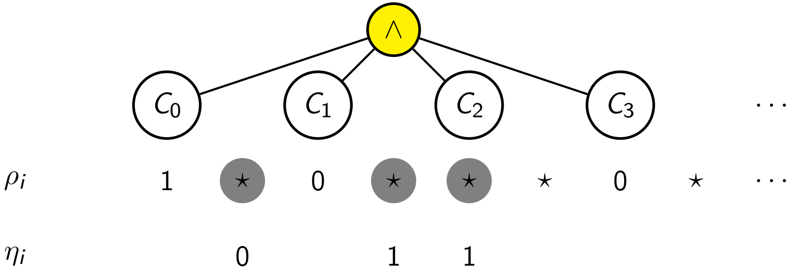
Lemat

Dla dowolnego obwodu C którego wszystkie dzieci są skończone, oraz skończonego zbioru A, istnieje restrykcja ρ, taka że $\rho(A) = \{\star\}$ i ρ jest dobre dla C.

Idea dowodu

Staramy się by wartości wejść ze zbioru A jednoznacznie wyznaczały wartość całego obwodu. Robimy to *po kolei*, dla wszystkich możliwych wartościowań na A. Dla każdego wartościowania rozszerzamy dotychczasową restrykcję by była przy tym wartościowaniu dobra.

Numerujemy wartościowania na A: $\eta_0, \eta_1, \ldots, \eta_k$. Zaczynamy od $\rho_0 = (\star, \star, \star, \ldots)$. W kolejnym kroku rozpatrujemy $C|_{\rho_i \cup \eta_i}$. Jeśli ten obwód ma nieustaloną wartość, to któreś (skończone) C_j ma nieustaloną wartość. Wtedy rozszerzamy na skończenie wielu pozycjach ρ_i do ρ_{i+1} by C_j zdeterminowało wartość C. Wpp. kładziemy $\rho_{i+1} = \rho_i$.



Teza indukcyjna

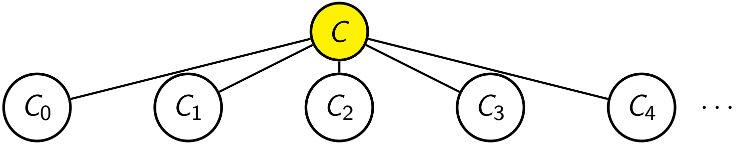
Teza

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 $\overline{\rho}(A) = \{\star\}$.

Indukcja

Dowód przebiega indukcyjnie ze względu na wysokość obwodu. Obwody wysokości 1 są skończone, więc każda restrykcja jest dla nich dobra. Zakładamy, że teza jest prawdziwa dla obwodów wysokości mniejszej niż α i dowodzimy tezy dla dowolnego obwodu C wysokości α.

Konstruujemy ciągi ρ_i i A_i korzystając z tezy indukcyjnej. Zaczynamy od danych ρ i A. ρ_{i+1} jest rozszerzeniem ρ_i i A_{i+1} jest o jeden większy niż A_i.



$\rho_0 \quad \rho_1 \quad \rho_2 \quad \rho_3 \quad \rho_4 \quad \cdots$

$A_0 \quad A_1 \quad A_2 \quad A_3 \quad A_4 \quad \cdots$

Istnieje funkcja $\overline{\rho}$ będąca granicą ciągu (ρ_i). Jednocześnie $\rho_i(A_i) = \{\star\}$, więc $\overline{\rho}(\bigcup A_i) = \{\star\}$. Więc $\overline{\rho}$ jest restrykcją dobrą dla wszystkich dzieci danego obwodu. Więc $C|_{\overline{\rho}}$ jest równoważne obwodowi którego wszystkie dzieci są skończone. Więc z lematu, istnieje ρ' rozszerzające $\overline{\rho}$, dobre dla C i $\rho'(A) = \{\star\}$.

W rezultacie otrzymujemy tezę indukcyjną dla wszystkich obwodów logicznych. Możemy ją następnie uprościć:

- ustalamy zbiór $A = \emptyset$,
- ustalamy restrykcję $\rho = (\star, \star, \star, \ldots)$,
- rozszerzamy wynikową restrykcję, by nie tylko była dobra, lecz by ustalała wartość obwodu,

otrzymując wniosek:

Twierdzenie uproszczone

Dla każdego obwodu logicznego C istnieje restrykcja ρ, taka że $C|_\rho$ ma stałą wartość niezależną od wejść.

Wnioski

Powyższy wniosek można wyrazić w języku topologii:

Inne sformułowanie

Dla każdego borelowskiego podzbioru zbioru Cantora B istnieje zanurzenie zbioru Cantora w siebie indukowane przez restrykcję, takie że jego obraz zawiera się w B, lub jest z nim rozłączny.

Otrzymana teza jest podobna do twierdzenia Ellentucka, z dodatkowym warunkiem by odpowiednie zanurzenie pochodziło od restrykcji.

Funkcje parzystości

Definicja

Funkcja parzystości to dowolna funkcja $P\colon \{0,1\}^{\mathbb{N}} \to \{0,1\}$, *taka że* $P(x) \neq P(y)$, *jeśli* x *i* y *różnią się na dokładnie jednej pozycji.*

Funkcje parzystości

Definicja

Funkcja parzystości to dowolna funkcja $P\colon \{0,1\}^{\mathbb{N}} \to \{0,1\}$, *taka że* $P(x) \neq P(y)$, *jeśli* x *i* y *różnią się na dokładnie jednej pozycji.*

Fakt

Oczywiście dla każdej restrykcji ρ, $P|_\rho$ *nie jest funkcją stałą (bo* ρ *zawiera jakąś gwiazdkę).*

Funkcje parzystości

Definicja

Funkcja parzystości to dowolna funkcja $P\colon \{0,1\}^{\mathbb{N}} \to \{0,1\}$*, taka że* $P(x) \neq P(y)$*, jeśli* x *i* y *różnią się na dokładnie jednej pozycji.*

Fakt

Oczywiście dla każdej restrykcji ρ*,* $P|_\rho$ *nie jest funkcją stałą (bo* ρ *zawiera jakąś gwiazdkę).*

Wniosek

Dla każdej funkcji parzystości P*, nie istnieje uogólniony obwód logiczny* C *obliczający* P*.*

Dziękuję za uwagę, czy są jakieś pytania?