Dowód twierdzenia Razborowa

Rafał Wojtczuk, na podstawie wykładu
"Teoria złożoności" dr hab. Damiana Niwińskiego

22 maja 2005 roku

1 Treść twierdzenia

Twierdzenie (Razborowa). *Istnieje $c > 0$ takie, że dla prawie wszystkich n, każdy obwód monotoniczny rozpoznający $CLIQUE_{n,\sqrt[4]{n}}$ ma co najmniej $2^{c\sqrt[8]{n}}$ bramek.*

Wniosek 1. Nie istnieje ciąg monotonicznych obwodów rozmiaru wielomianowego rozpoznający język $CLIQUE$.

2 Notacje, definicje

PRZYPOMNIENIE. Nieskierowany graf $G = \langle V, E\rangle$ możemy zakodować słowem w długości $\binom{n}{2}$ nad alfabetem {0,1}, gdzie n to liczba wierzchołków G. Należy w tym celu ustalić bijekcję β_n, mającą jako dziedzinę zbiór par wierzchołków $\{i, j\}$, a jako przeciwdziedzinę zbiór $\{1, \ldots, \binom{n}{2}\}$. Litera w słowie w na pozycji $\beta_n(\{i, j\})$ określa, czy między parą wierzchołków i i j jest krawędź.

PRZYPOMNIENIE. $CLIQUE_{n,k} = \{w \in \{0,1\}^{\binom{n}{2}} : w$ koduje graf o n wierzchołkach z k-kliką $\}$

Definicja 1. W dalszym toku dowodu przyjmiemy następujące oznaczenia:
$k = \sqrt[4]{n}, l = \sqrt[8]{n}, p = l \cdot \log n, M = (p-1)^l \cdot l!$

Zauważmy, że $M = (l \cdot \log n - 1)^l \cdot l! = (8l \cdot \log l - 1)^l \cdot l^l < l^{\frac{4}{3}\cdot l} \cdot l^l = l^{\frac{7}{3}\cdot l}$
dlatego $M^2 < l^{\frac{14}{3}\cdot l} < l^{\frac{16}{3}\cdot l} = (l^8)^{\frac{2}{3}\cdot l}$
czyli

$$M^2 < n^{\frac{2}{3}\cdot l} \tag{1}$$

Definicja 2. Dla $X_i \subseteq \{1..n\}$ obwodem surowym $CC(X_1, \ldots, X_t)$ nazywamy monotoniczny obwód logiczny postaci
$CC(X_1, \ldots, X_t) = \bigvee_{1\leqslant i\leqslant t} CC(X_i)$

gdzie $CC(X) = \bigwedge_{\substack{i,j \in X \\ i \neq j}} x_{\{i,j\}}$

Ponadto wymagamy aby $|X_i| \leqslant l$ oraz $t \leqslant M$.

MOTYWACJA. Zmienna $x_{\{i,j\}}$ odpowiada literze w słowie w kodującej istnienie krawędzi pomiędzy wierzchołkami i i j. Widać, że obwód powyższej postaci jest dość naturalną próbą implementacji obwodu rozpoznającego graf z kliką - każda koniunkcja $CC(X_i)$ przyjmuje wartość PRAWDA, gdy wierzchołki należące do X_i tworzą klikę. Ograniczenia na rozmiar obwodu będą kluczowe w dalszej części dowodu.

Definicja 3. "Przykład pozytywne" to k-elementowe podzbiory zbioru {1,. . . ,n}. Każdy przykład pozytywny X wyznacza graf G_X, który ma klikę rozmiaru k. Graf G_X ma postać
$G_X = \langle \{1 \ldots n\}, E_X \rangle, \quad E_X(i,j) \iff i,j \in X$
Jak widać, wszystkie krawędzie w G_X należą do kliki. Istnieje $\binom{n}{k}$ przykładów pozytywnych.

Definicja 4. "Przykłady negatywne" funkcje α postaci
$\alpha\colon \{1 \ldots n\} \to \{1 \ldots k-1\}$
Każda funkcja α wyznacza graf G_α, który nie ma kliki rozmiaru k. Graf G_α ma postać:
$G_\alpha = \langle \{1 \ldots n\}, E_\alpha \rangle, \quad E_\alpha(i,j) \iff \alpha(i) \neq \alpha(j)$
Istnieje $(k-1)^n$ przykładów negatywnych.

MOTYWACJA. Jak łatwo zauważyć, poprawność powyższej konstrukcja ma związek z kolorowaniem grafu $k-1$ kolorami; krawędzie istnieją tylko pomiędzy wierzchołkami o różnych kolorach. W takim grafie nie ma kliki rozmiaru k, gdyż wszystkie wierzchołki z dowolnej kliki mają parami różny kolor.
Zauważmy, że różne funkcje α mogą wyznaczać te same grafy - nie będzie to przeszkodą w dalszym ciągu dowodu.

NOTACJA. C[w] to wynik działania obwodu logicznego C dla wejścia będącego słowem w.

NOTACJA. $C[[X]] = C[w_{G_X}]$

NOTACJA. $C[[\alpha]] = C[w_{G_\alpha}]$

NOTACJA. $|C|$ to liczba bramek w obwodzie C.

3 Podstawowy lemat o obwodach surowych

Lemat 1. *Każdy obwód surowy jest tożsamościowo równy FALSE lub myli się przynajmniej dla połowy przykładów negatywnych.*

Dowód lematu. Zdefiniujmy przestrzeń probabilistyczną P

- zdarzeniem elementarnym jest wybór funkcji α
- dla każdego zdarzenia elementarnego e, prawdopodobieństwo e jest takie samo i wynosi $\frac{1}{(k-1)^n}$

Intuicyjnie, dla przestrzeni P zdarzeniem jest pokolorowanie n wierzchołków co najwyżej $k-1$ kolorami. W dalszym ciągu rozumowania, przy ustalonych $1 \leqslant v \leqslant n$ i $1 \leqslant c \leqslant k-1$, na określenie zdarzenia
$z = \{\alpha : \alpha(v) = c\}$
będzie używany skrót "zdarzenie takie, że wierzchołek v ma kolor c".
Zauważmy, że prawdopodobieństwo, że dany wierzchołek ma dany kolor, wynosi $\frac{1}{k-1}$ (z symetrii). Podobnie, prawdopodobieństwo, że 2 ustalone wierzchołki są tego samego koloru jest równe $\frac{1}{k-1}$. A zatem, prawdopodobieństwo, że w zbiorze X istnieją 2 punkty o tym samym kolorze jest nie większe niż $\frac{\binom{|X|}{2}}{k-1}$.
Załóżmy, że obwód surowy nie jest tożsamościowo równy FALSE. Zauważmy, że $CC(X)$ na przykładzie negatywnym α da poprawną odpowiedź (czyli FALSE) wtedy i tylko wtedy, jeśli w zbiorze X istnieją dwa wierzchołki i, j takie, że $\alpha(i) = \alpha(j)$. Prawdopodobieństwo, że tak się stanie jest nie większe niż
$\frac{\binom{|X|}{2}}{k-1} = \frac{l\cdot(l-1)}{2\cdot(l^2-1)} < \frac{1}{2}$
Skorzystaliśmy tu z definicji k i mocy zbioru X definiującego element obwodu surowego. Zatem CC(X) z prawdopodobieństwem $> \frac{1}{2}$ akceptuje przykład negatywny. Ponieważ obwód surowy CC to alternatywa $\bigvee CC(X_i)$, to prawdopodobieństwo, że CC akceptuje przykład negatywny jest nie mniejsze. □

4 Uogólnienie powyższego lematu

Lemat 2. *Niech $X \subset \{1, \ldots, n\}$, $|X| \leqslant l$, $A \subseteq X$. Przyjmijmy przestrzeń probabilistyczną jak w poprzednim lemacie. Niech R(Z) - zdarzenie, że w Z są dwa punkty tego samego koloru. Wtedy*
$p(R(X)|\neg R(A)) < \frac{1}{2}$

Dowód lematu. Przyjmijmy $B = X - A$, $|B| = b$. Jakie kolorowania B są sprzyjające? Są dwie możliwości:

- W B są dwa punkty tego samego koloru; prawdopodobieństwo takiego zdarzenia jest $< \frac{\binom{|B|}{2}}{k-1}$
- W B jest punkt takiego samego koloru, co pewien punkt z A; prawdopodobieństwo takiego zdarzenia jest $< \frac{|A|}{k-1} \cdot |B|$

Zatem
$p(R(X)|\neg R(A)) < \frac{\binom{|B|}{2}}{k-1} + \frac{|A|}{k-1} \cdot |B| =$
$\frac{\frac{1}{2}\cdot|B|\cdot(|B|-1)}{k-1} + \frac{|X|-|B|}{k-1} \cdot |B| < \frac{\frac{1}{2}\cdot|B|\cdot(|B|-1)}{k-1} + \frac{l-|B|}{k-1} \cdot |B| = \frac{\frac{1}{2}\cdot b^2 - \frac{1}{2}\cdot b + l\cdot b - b^2}{l^2-1} =$
$\frac{(l-\frac{1}{2})\cdot b - \frac{1}{2}\cdot b^2}{l^2-1} \leqslant$
[funkcja $f(b)$ ma maksimum dla $b = l - \frac{1}{2}$]
$\frac{1}{2} \cdot \frac{(l-\frac{1}{2})^2}{l^2-1} <$
[dla $l \geqslant 2$]
$< \frac{1}{2}$

□

5 O słonecznikach

PRZYPOMNIENIE. "Słonecznikiem" nazywamy rodzinę zbiorów $\{Z_1, \ldots, Z_s\}$ jeśli $\forall z \in \bigcup Z_i : z \in \bigcap Z_i \vee (\exists\, dok\text{ł}adnie\, jedno\, i\, takie,\, \text{ż}e\, z \in Z_i)$

Lemat 3 (Erdösa-Rado). *Aby rodzina $\mathbb{Z}$ zbiorów co najwyżej l-elementowych zawierała słonecznik mocy p, wystarcza, by $|\mathbb{Z}| > (p-1)^l \cdot l!$*

Dowód lematu. Przez indukcję po l. Dla $l = 1$ teza jest prawdziwa: każde p zbiorów co najwyżej 1-elementowych tworzy słonecznik. Krok indukcyjny: niech teza będzie prawdziwa dla $l-1$. Ustalmy $\mathbb{Z}$ o mocy $> (p-1)^l \cdot l!$. Rozpatrzmy dwa przypadki:

- Istnieje rodzina zbiorów $\mathbb{Z}'$, $\mathbb{Z}' \subseteq \mathbb{Z}$, $|\mathbb{Z}'| > (p-1)^{(l-1)} \cdot (l-1)!$, taka, że część wspólna wszystkich zbiorów z $\mathbb{Z}'$ jest niepusta (oznaczmy ją przez W).
  W takim przypadku, zdefiniujmy
  $\mathbb{Z}'' = \{Z - W : Z \in \mathbb{Z}'\}$
  czyli z każdego zbioru z $\mathbb{Z}'$ odejmiemy ich część wspólną. $\mathbb{Z}''$ spełnia założenie kroku indukcyjnego. Zatem można z tej rodziny wybrać słonecznik S'' mocy p. Utwórzmy zbiór S' dodając W do każdego zbioru z S''. Jak łatwo zauważyć, S' też jest słonecznikiem, a ponadto każdy zbiór z S' należy do $\mathbb{Z}'$, a więc także do $\mathbb{Z}$. Tak więc S' jest szukanym słonecznikiem.

- Nie istnieje rodzina zbiorów $\mathbb{Z}'$, $\mathbb{Z}' \subseteq \mathbb{Z}$, $|\mathbb{Z}'| > (p-1)^{(l-1)} \cdot (l-1)!$, taka, że część wspólna wszystkich zbiorów z $\mathbb{Z}'$ jest niepusta.
  W takim przypadku podamy algorytm na wybranie z $\mathbb{Z}$ p parami rozłącznych zbiorów (które tworzą słonecznik). Zauważmy najpierw, że dla dowolnego zbioru Z_i i dowolnego jego elementu z, istnieje co najwyżej $(p-1)^{(l-1)} \cdot (l-1)!$ zbiorów z $\mathbb{Z}$ zawierających z (gdyż w przeciwnym przypadku założenie tego podpunktu nie byłoby prawdziwe). Ponieważ $|Z_i| \leqslant l$, to istnieje co najwyżej $l \cdot (p-1)^{(l-1)} \cdot (l-1)! = (p-1)^{(l-1)} \cdot l!$ zbiorów mających część wspólną z $|Z_i|$. Zatem nasz algorytm ma postać:

  1. $\mathbb{Z}_{tmp} := \mathbb{Z}$; $\mathbb{S} := \emptyset$; $licznik := 0$
  2. wybierz dowolny zbiór Z z $\mathbb{Z}_{tmp}$
  3. $\mathbb{S} := \mathbb{S} \cup \{Z\}$
  4. wyrzucamy z $\mathbb{Z}_{tmp}$ Z i wszystkie zbiory mające część wspólną z Z
  5. $licznik := licznik + 1$
  6. jeśli $licznik < p-1$, idź do 2
  7. wybierz dowolny zbiór Z z $\mathbb{Z}_{tmp}$ i dodaj go do $\mathbb{S}$

  Krok 4 jest wykonany $p-1$ razy. Ponieważ w kroku 4 moc $\mathbb{Z}_{tmp}$ zmniejsza się o nie więcej niż $(p-1)^{(l-1)} \cdot l!$, to po $p-1$ iteracjach moc $\mathbb{Z}_{tmp}$ zmniejszy się co najwyżej o
  $(p-1) \cdot (p-1)^{(l-1)} \cdot l! = (p-1)^l \cdot l! < |\mathbb{Z}|$
  tak więc w kroku 7 $\mathbb{Z}_{tmp}$ będzie niepusty i będzie można wybrać z niego p-ty element słonecznika $\mathbb{S}$.

$\square$

Definicja 5. $pluck(\mathbb{Z})$ - niedeterministyczna operacja, która z rodziny $\mathbb{Z}$ o mocy $> M$ wybiera słonecznik mocy p i zastępuje go "środkiem słonecznika" (czyli częścią wspólną wszystkich zbiorów ze słonecznika wybranego z $\mathbb{Z}$).

Zauważmy, że operacja *pluck* zmniejsza moc zbioru $\mathbb{Z}$ o $p-1$. Ponadto, operacja *pluck* może spowodować, że w $\mathbb{Z}$ będzie zbiór pusty; przyjmujemy, że $CC(\emptyset)$ jest tożsamościowo równy PRAWDA.

Definicja 6. $pluck^{+}(\mathbb{Z})$ - operacja, która polega na powtórzeniu operacji *pluck* tyle razy, aby moc zbioru $\mathbb{Z}$ stała się $\leqslant M$

6 Definicja aproksymatora surowego

Niech będą dane dwa obwody surowe $CC(\mathbb{X})$ i $CC(\mathbb{Y})$. Obwód, który jest koniunkcją (lub alternatywą) $CC(\mathbb{X})$ i $CC(\mathbb{Y})$ nie ma postaci obwodu surowego. Zdefiniujemy obwody surowe, które zachowują się w przybliżeniu tak, jak koniunkcja (lub alternatywa) tych dwóch obwodów.

Definicja 7. Niech będą dane dwa obwody surowe $CC(\mathbb{X})$ i $CC(\mathbb{Y})$. Aproksymatory surowe definiujemy następujaco:
$App_{\vee}(CC(\mathbb{X}), CC(\mathbb{Y})) = CC(pluck^{+}(\mathbb{X} \cup \mathbb{Y}))$
$App_{\wedge}(CC(\mathbb{X}), CC(\mathbb{Y})) = CC(pluck^{+}(\mathbb{V}))$
$gdzie\, \mathbb{V} = \{X_i \cup Y_j, X_i \in \mathbb{X}, Y_j \in \mathbb{Y}, |X_i \cup Y_j| < l\}$

MOTYWACJA. Łatwo jest znormalizować alternatywę $CC(\mathbb{X})$ i $CC(\mathbb{Y})$ tak, aby otrzymać równoważny obwód, który jest alternatywą koniunkcji:

Definicja 8. $Norm_{\vee}(CC(\mathbb{X}), CC(\mathbb{Y})) = CC(\mathbb{X} \cup \mathbb{Y})$

Podobnie, zauważmy, że

$$CC(X_i \cup Y_j) \leqslant CC(X_i) \wedge CC(Y_j) \tag{2}$$

(ponieważ w koniunkcji po lewej stronie równania występują zmienne kodujące krawędzie między parą wierzchołków $\{w_1, w_2\}$, gdzie $w_1 \in X_i$, a $w_2 \in Y_j$; takich zmiennych nie ma po prawej stronie). Zatem możemy zdefiniować następujący obwód, który zwraca wartości nie większe niż koniunkcja $CC(\mathbb{X})$ i $CC(\mathbb{Y})$:

Definicja 9. $Norm_{\wedge}(CC(\mathbb{X}), CC(\mathbb{Y})) = CC(\{X_i \cup Y_j, X_i \in \mathbb{X}, Y_j \in \mathbb{Y}\})$

Zauważmy także, że dla wejścia kodującego przykład pozytywny p mamy równość

$$Norm_{\wedge}(CC(\mathbb{X}), CC(\mathbb{Y}))[[p]] = CC(\mathbb{X})[[p]] \wedge CC(\mathbb{Y})[[p]] \tag{3}$$

ponieważ przykład pozytywny składa się z jednej kliki, więc jeśli jest krawędź pomiędzy parą wierzchołków $\{w_1, w_2\}$ i jest krawędź pomiędzy parą wierzchołków $\{w_3, w_4\}$, to jest również krawędź pomiędzy parą wierzchołków $\{w_1, w_3\}$;

dlatego w rozumowaniu uzasadniającym (2) mamy równość zamiast nierówności.
Własności (2) i (3) uzasadniają przyjęcie $Norm_\wedge$ jako przybliżenia koniunkcji obwodów surowych.
Jednakże $Norm_\vee$ może być definiowany przez zbyt dużo zbiorów, aby spełniać ogranicznia nakładane na obwód surowy. Podobnie, $Norm_\wedge$ może nie być obwodem surowym, gdyż może być definiowany przez zbyt dużo zbiorów, a ponadto mogą one być za duże. Operacja $pluck^+$ (i usuwanie za dużych zbiorów $X_i \cup Y_j$) rozwiązuje te problemy, ale za to wprowadza błędy. Jednak jak zobaczymy, własności słonecznika gwarantują, że liczba błędów powstałych w wyniku obcinania zbiorów będzie dostatecznie mała.

7 Dwa kluczowe lematy

Lemat 4 (o przegranych pozytywach). *Niech $CC(\mathbb{X})$, $CC(\mathbb{Y})$ to obwody surowe. Oznaczmy przez FN zbiór zbiorów X, $X \subseteq \{1 \dots n\}$, $|X| = k$ (czyli zbiór przykładów pozytywnych), dla których aproksymator surowy popełnia błąd zwracając "fałsz", to znaczy*
niech $\Box \in \{\vee, \wedge\}$
$FN = \{X : App_\Box(CC(\mathbb{X}), CC(\mathbb{Y}))[[X]] <$
$\Box(CC(\mathbb{X})[[X]], CC(\mathbb{Y})[[X]])\}$
Wtedy $|FN| < M^2 \cdot \binom{n-l-1}{k-l-1}$

Dowód lematu. Zauważmy najpierw, że "oskubywanie słonecznika" (czyli operacja *pluck*) nie może spowodować powstania przegranego pozytywu. Jest tak dlatego, że operacja *pluck* zastępuje fragment postaci $\bigvee_{1 \leqslant i \leqslant p} CC(X_i)$ przez $CC(\bigcap_{1 \leqslant i \leqslant p} X_i)$ Jak łatwo zauważyć, z poprzedniego wyrażenia wynika ostatnie.
Ponadto, mamy równość (3). Dlatego błąd może powstać tylko w $App_\wedge$, kiedy do funkcji *pluck*() podstawimy nie wszystkie zbiory $X_i \cup Y_j$ - to znaczy kiedy usuniemy któryś z nich, ponieważ ma za dużo elementów (więcej niż l). Ile błędów może wprowadzić usunięcie jednej pary $X_i \cup Y_j$? Inaczej, ile mamy takich zbiorów X mocy k, że $CC(X_i \cup Y_j)[[X]] = PRAWDA$? Taki zbiór X musi zawierać $|X_i \cup Y_j|$ wierzchołków należących do przecięcia tych zbiorów, a pozostałe $k - |X_i \cup Y_j|$ wierzchołków wybieramy dowolnie. Zatem takich zbiorów jest
$\binom{n-|X_i \cup Y_j|}{k-|X_i \cup Y_j|} \leqslant$ [funkcja $f(x) = \binom{n-x}{k-x}$ jest malejąca] $\leqslant \binom{n-l-1}{k-l-1}$
Ponieważ mamy co najwyżej M^2 par $X_i \cup Y_j$, dostajemy żądane oszacowanie. □

Lemat 5 (o wygranych negatywach). *Niech $CC(\mathbb{X})$, $CC(\mathbb{Y})$ to obwody surowe. Oznaczmy przez FP zbiór funkcji α (czyli zbiór przykładów negatywnych), dla których aproksymator surowy popełnia błąd zwracając "prawda", to znaczy*
niech $\Box \in \{\vee, \wedge\}$
$FP = \{\alpha : App_\Box(CC(\mathbb{X}), CC(\mathbb{Y}))[[\alpha]] >$

$\square(CC(\mathbb{X})[[\alpha]], CC(\mathbb{Y})[[\alpha]])\}$
Wtedy $|FP| < M^2 \cdot 2^{-p} \cdot (k-1)^n$

Dowód lematu. Zauważmy najpierw, że usunięcie zbioru $X_i \cup Y_j$, który miał za dużo elementów, nie może spowodować powstania wygranego negatywu, ponieważ ta operacja usuwa człony alternatywy z wynikowego obwodu, nie może więc zmienić wartości tej alternatywy z 0 na 1. Ponadto mamy własność (2). Dlatego tylko operacja *pluck* generuje błędy. Przyjmijmy przestrzeń probabilistyczną taką samą, jak w lemacie 1. Niech R(X) to zdarzenie, że w X są powtarzające się kolory.

Przypuśćmy, że w wyniku operacji *pluck* słonecznik $Z_1, \ldots, Z_p$ zastąpiliśmy przez przecięcie $S(\mathbb{Z}) = \bigcap Z_i$. Wtedy prawdopodobieństwo powstania sytuacji wygranego negatywu wynosi
$p(R(Z_1) \wedge \ldots \wedge R(Z_p) \wedge \neg R(S(\mathbb{Z}))) \leqslant$
[prawdopodobieństwo warunkowe]
$\leqslant p(R(Z_1) \wedge \ldots \wedge R(Z_p) | \neg R(S(\mathbb{Z}))) =$
[ponieważ z definicji słonecznika zbiory $Z_i - S(\mathbb{Z})$ są rozłączne]
$= \prod_{1 \leqslant i \leqslant p} p(R(Z_i) | \neg R(S(\mathbb{Z})) \leqslant$
[ponieważ z lematu 2, $p(R(Z_i) | \neg R(S(\mathbb{Z}) \leqslant \frac{1}{2}$]
$\leqslant (\frac{1}{2})^p$
Tak więc wykonanie operacji *pluck* powoduje powstanie nie więcej niż $(\frac{1}{2})^p \cdot (k-1)^n$ wygranych negatywów. Ponieważ operacja $pluck^+$ wykonuje nie więcej niż $(M^2 - M)/(p-1) < M^2$ operacji *pluck*, dostajemy żądane oszacowanie.

□

8 Dowód twierdzenia Razborowa

Niech **C** - obwód monotoniczny rozpoznający $CLIQUE_{n, \sqrt[4]{n}}$. Dla każdej bramki g obwodu **C**, niech C_g to obwód, gdzie g jest wyjściem, a bramki poniżej g są takie same jak w obwodzie **C**.
Dla każdej bramki g obwodu **C** określamy obwód surowy CC_g, aproksymujacy C_g. Konstrukcja przebiega indukcyjnie, począwszy od liści obwodu:

- Pojedyńcza zmienna jest obwodem surowym.
- Dla bramki g, która ma jako wejście bramki g_1 i g_2, i wykonuje na nich operację $\square, \square \in \{\vee, \wedge\}$,
  $CC_g = App_{\square}(CC_{g_1}, CC_{g_2})$

Przyjmijmy też $\mathbf{CC} = CC_{g_\omega}$, gdzie g_ω to ostatnia bramka C; tak więc **CC** aproksymuje cały obwód **C**.
Rozpatrzmy teraz dwa przypadki.

8.1 CC jest tożsamościowo równe FALSE

Ustalmy p ze zbioru przykładów pozytywnych. Musi istnieć bramka g_e o wejściach g_1 i g_2 taka, że

$$App_{\square}(CC_{g_1}, CC_{g_2})[[p]] < \square(CC_{g_1}[[p]], CC_{g_2}[[p]]) \tag{4}$$

Załóżmy tezę przeciwną. Wtedy przez indukcję możnaby dowieść, że dla każdej bramki g zachodzi

$$CC_g[[p]] \geqslant C_g[[p]] \tag{5}$$

Ta nierówność byłaby prawdziwa w liściach obwodu, a potem działa indukcja korzystając z indukcyjnej definicji CC_g; krok indukcyjny ma postać
$CC_g[[p]] = App_{\square}(CC_{g_1}, CC_{g_2})[[p]] \geqslant$
[na podstawie zanegowanego (4)]
$\geqslant \square(CC_{g_1}[[p]], CC_{g_2}[[p]]) \geqslant$
[założenie indukcyjne (5) i monotoniczność $\wedge$ i $\vee$]
$\geqslant \square(C_{g_1}[[p]], C_{g_2}[[p]]) = C_g[[p]]$

Ponieważ (5) nie zgadza się dla bramki g_ω, dlatego (4) musi być prawdziwe dla pewnej bramki g.
Zatem, na mocy (4), dla każdego p istnieje bramka, dla której aproksymator surowy popełnia błąd dla p. Tak więc istnieje bramka taka, że aproksymator CC_g popełnia $\geqslant \frac{\binom{n}{k}}{|C|}$ błędów dla przykładów pozytywnych (z zasady szufladkowej). Po podstawieniu tego wyrażenia do tezy lematu o przegranych pozytywach dostajemy
$\frac{\binom{n}{k}}{|C|} \leqslant M^2 \cdot \binom{n-l-1}{k-l-1}$
Czyli:
$|C| \geqslant \frac{\binom{n}{k}}{M^2 \cdot \binom{n-l-1}{k-l-1}} \geqslant (\frac{n-l}{k})^l \cdot \frac{1}{M^2} \geqslant$ [na podstawie (1)] $\geqslant (\frac{n-l}{k \cdot n^{\frac{2}{3}}})^l \geqslant (\frac{n-l}{n^{\frac{1}{4}} \cdot n^{\frac{2}{3}}})^l$
Ponieważ $\frac{1}{4} + \frac{2}{3} < 1$, to widać, że teza głównego twierdzenia jest spełniona.

8.2 CC myli się na połowie przykładów negatywnych

Analogiczne rozumowanie prowadzi do nierówności
$\frac{1}{2} \cdot (k-1)^n \leqslant |C| \cdot M^2 \cdot 2^{-p} \cdot (k-l)^n$
Zatem
$|C| \geqslant \frac{\frac{1}{2} \cdot (k-1)^n \cdot 2^p}{M^2 \cdot (k-l)^n} \geqslant \frac{1}{2} \cdot 2^p \cdot \frac{1}{M^2} =$ [z definicji p] $= \frac{1}{2} n^l \cdot \frac{1}{M^2} \geqslant$ [na podstawie (1)]
$\geqslant \frac{1}{2} n^l \cdot n^{-\frac{2}{3} \cdot l}$
Również w tym przypadku z ostatniej nierówności wynika teza głównego twierdzenia. $\square$

9 Bibliografia

- Ch. H. Papadimitriou, "Złożoność obliczeniowa", WNT, Warszawa 2002