Ćwiczenia 2

Dawid Dieu
302052

Zadanie 1

W kablu koncentrycznym używanym w standardowym 10-Mbitowym Ethernecie sygnał rozchodzi się z prędkością $10^8 m/s$. Standard ustala, że maksymalna odległość między dwoma komputerami może wynosić co najwyżej $2{,}5 km$. Oblicz, jaka jest minimalna długość ramki (wraz z nagłówkami).

- s = $2500m$
- V = $10^8 m/s$
- b (bandwidth) = $10Mb$ = 10^7 bitów
- d (propagation delay) = $s/V = 2.5 * 10^{-5} s$

- długośc ramki = $b*2*d = 5*10^2 = 500$ bitów

Zadanie 2

Rozważmy rundowy protokół Aloha we współdzielonym kanale, tj. w każdej rundzie każdy z n uczestników usiłuje wysłać ramkę z prawdopodobieństwem p. Jakie jest prawdopodobieństwo $P(p,n)$, że jednej stacji uda się nadać (tj. że nie wystąpi kolizja)?

Pokaż, że $P(p,n)$ jest maksymalizowane dla $p = \frac{1}{n}$.

Ile wynosi $\lim_{x \to \infty} P(\frac{1}{n}, n)$?

1. Zakładam, że mi uda się wysłać moją ramkę.
2. Zakładam, że innym $n-1$ uczestników nie uda się wysłać ramki.
3. Takich przypadków, że komuś udało się wysłać, a reszcie nie jest n.

Zatem $P(p,n)=n*p*(1-p)^{n-1}$.

Liczymy pochodną po p.

YOUR INPUT:
$f(p) =$

$$n(1-p)^{n-1}p$$

Note: Your input has been rewritten/simplified.

Roots/zeros found at:

$$p = 1$$

$$p = 0$$

Simplify

FIRST DERIVATIVE:
$\frac{d}{dp}[f(p)] = f'(p) =$

$$n(1-p)^{n-1} - (n-1)\,n(1-p)^{n-2}p$$

Simplify/rewrite:

$$-\frac{n(1-p)^{n}(np-1)}{(p-1)^{2}}$$

Root/zero found at:

$$p = \frac{1}{n}$$

Simplify Show steps

NEXT DERIVATIVE:

Calculate next higher derivative

Differentiate last result w. r. t.: n

Jak widać miejsce zerowe pochodnej jest w 1n, czyli mamy ekstremum.

SECOND DERIVATIVE:

$$\frac{d^2}{dp^2}[f(p)] = f''(p) =$$

$$\frac{n^2(1-p)^{n-1}(np-1)}{(p-1)^2} + \frac{2n(1-p)^n(np-1)}{(p-1)^3} - \frac{n^2(1-p)^n}{(p-1)^2}$$

Simplify/rewrite:

$$-\frac{(n-1)\,n(1-p)^n(np-2)}{(p-1)^3}$$

Root/zero found at:

$$p = \frac{2}{n}$$

Simplify | Show steps

Podstawiając p= 1n do 2 pochodnej otrzymujemy coś ujemnego, dlatego wiemy, że to maksimum.

- $\lim_{x\to\infty} P($ 1n $,n)=$ 1e .

$$\lim_{n\to\infty}\left(\left(1-\frac{1}{n}\right)^{n-1}\right)$$

Go

Graph » Examples »

Solution

Keep Practicing >

Show Steps

$$\lim_{n\to\infty}\left(\left(1-\frac{1}{n}\right)^{n-1}\right) = \frac{1}{e} \quad (\text{Decimal:} \quad 0.36787\ldots)$$

Steps

$\lim_{n\to\infty}\left(\left(1-\frac{1}{n}\right)^{n-1}\right)$

$\left(1-\frac{1}{n}\right)^{n-1}=\left(1-\frac{1}{n}\right)^{n}\left(1-\frac{1}{n}\right)^{-1}$

$=\lim_{n\to\infty}\left(\left(1-\frac{1}{n}\right)^{n}\left(1-\frac{1}{n}\right)^{-1}\right)$

$\lim_{x\to a}[f(x)\cdot g(x)]=\lim_{x\to a}f(x)\cdot\lim_{x\to a}g(x)$

With the exception of indeterminate form

$=\lim_{n\to\infty}\left(\left(\left(1-\frac{1}{n}\right)^{n}\right)\cdot\lim_{n\to\infty}\left(\left(1-\frac{1}{n}\right)^{-1}\right)\right)$

$\lim_{n\to\infty}\left(\left(1-\frac{1}{n}\right)^{n}\right)=\frac{1}{e}$ *Show Steps*

$\lim_{n\to\infty}\left(\left(1-\frac{1}{n}\right)^{-1}\right)=1$ *Show Steps*

$=\frac{1}{e}\cdot 1$

Simplify

$=\frac{1}{e}$

click here to practice limits »

Zadanie 3

Wyszukaj w sieci informację na temat zjawiska Ethernet capture i wytłumacz w jaki sposób ono powstaje.

(Tym mianem określa się sytuację, w której jedna ze stacji nadaje znacznie częściej, choć wszystkie stacje używają algorytmu CSMA/CD.)

Dzieje się to dlatego, że wierzchołki w sieci ustępują wysłania danych na rzecz innego wierzchołka, a potem próbują wysłać swoje dane ponownie.

Ethernet capture w algorytmie CSMA/CD

- Załóżmy, że każdy wierzchołek w sieci LAN ma jakieś dane do przesłania.
- Kiedy dwa wierzchołki próbują coś wysłać w tym samym czasie następuje kolizja i każdy z nich czeka jakiś losowy okres czasu zanim spróbuje wysłać ponownie.
- Ale ten losowy okres czasu jest proporcjonalny do liczby udanych prób wysłania pakietu.
- Jednak kiedy jeden wierzchołek zaczyna wysyłać znacznie większą liczbę pakietów może zdominować całą sieć.
- ...
- Niech A i B próbują wysłać coś w tym samym czasie.
- Mamy kolizję i oboje czekaja [0, 1] jednostek czasu.
- Załóżmy, że czas czekania A jest mniejszy.
- Wtedy A wysyła co miał wysłać.
- Jeżeli A ma dalej coś do wysłania mamy znowu kolizję.
- Ale teraz A czeka [0, 1] jednostek czasu, a B [0, 3] jednostek, ponieważ to już druga próba wysłania pakietu przez B.
- Czyli za każdym razem jak B przegrywa walke o wysłanie, szansa, że uda mu się wysłac spada dokładnie dwukrotnie.
- Po 16 przegranych kolizjach B wycofa się na dłuższy czas lub np. odrzuci pakiet i będzie próbowało wysłac następny.
- Wtedy mówimy, że A przejęło kanał (“capture”).

Zadanie 4

Jaka suma kontrolna CRC zostanie dołączona do wiadomości *1010* przy założeniu że CRC używa wielomianu x^2+x+1?
A jaka jeśli używa wielomianu x^7+1?

CRC

Ustalamy r i wielomian $G(x)$ stopnia r (znany nadawcy i odbiorcy).

- W Ethernecie: $r = 32$, $G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x^1 + 1$.

Generowanie r-bitowej sumy kontrolnej s:

- Mamy wiadomość m ↔ M(x).
- Wysyłamy ciąg $b = m\#s \leftrightarrow B(x) = x^r \cdot M(x) + S(x)$,
  gdzie **s wybieramy tak, żeby $B(x)$ był podzielny przez $G(x)$**.

Odbiorca otrzymuje b′ ↔ B′(x)

- Odbiorca sprawdza, czy $G(x) \mid B'(x)$.
  - Nie → musiało wystąpić przekłamanie.
  - Tak → **zakładamy**, że dane zostały przesłane poprawnie.

- wiadomość $m=1010 \Leftrightarrow M(x)=x^3+x$
- żyjemy w świecie mod 2

1. $G(x)=x^2+x+1 \Leftrightarrow g=111(\text{bin}), r=2$
2. Dzielimy $x^r * M(x)=x^5+x^3=101000(\text{bin})$ przez $G(x)$
3. $x^5+x^3 x^2+x+1 = x^3+x^2+x$ Reszty x
4. Reszta, czyli $S(x)=x$
5. suma kontrolna powinna mieć $st(G)=2$ bity, czyli $s=10$

1. $G(x)=x^7+1 \Longleftrightarrow g=10000001(bin), r=7$
2. Dzielimy $x^r * M(x)=x^{10}+x^8=10100000000(bin)$ przez $G(x)$
3. $x^{10}+x^8 x^7+1 = x^3+x$ Reszty x^3+x
4. Reszta, czyli $S(x)=x^3+x$
5. suma kontrolna powinna mieć $st(G)=7$ bitów, czyli $s=0001010$

Zadanie 5

Pokaż, że CRC-1, czyli 1-bitowa suma obliczana na podstawie wielomianu $G(x)=x+1$, działa identycznie jak bit parzystości.

1. Teza: Jeżeli liczba zapalonych bitów w słowie maszynowym jest parzysta dzielenie przez $x+1$ da resztę 0, wpp 1.
2. Czyli musimy pokazać, że $x+1$ dzieli bez reszty wszystkie wielomiany o parzystej liczbie składników (w F_2).

Każdy wielomian postaci $x^n - x^k == x^n + x^k$ w F_2,
czyli w szczególności $x-1=x+1$.

$x^n+x^k=x^k(x^{n-k}+1)$, zakładając że $n>=k$
Wystarczy pokazać, że x^m+1 jest podzielne przez $x+1$.

Dla $m=0,1$ trywialne.
Załóżmy, że dla $m=k$, gdzie k całkowite:
$x^k-1=(x-1)*P(x)$, gdzie P to wielomian.

Weźmy $m=k+1$:
$x^{k+1}-1=(x-1)*Q(x)$, gdzie Q to wielomian.
$x^{k+1}-1=...$

$...=(x-1)*x^k+x^k-1$

$...=(x-1)*x^k+(x-1)*P(x)$, z założenia indukcyjnego

$...=(x-1)(x^k+P(x))$

$...=(x-1)(x^k+\frac{x^k-1}{x-1})$

$...=(x-1)(\frac{x^k*(x-1)+x^k-1}{x-1})$

$...=(x-1)(\frac{x^{k+1}-x^k+x^k-1}{x-1})$

$...=(x-1)Q(x)$

Teraz mając wielomian o parzystej liczbie składników dzielimy te składniki w pary.
Wiedząc, że każda para postaci x^n+x^k dzieli się przez $x+1$ cały wielomian też się dzieli bez reszty.

Jeżeli liczba składników jest nieparzysta zawsze zostanie jeden z nich zostanie bez pary, czyli zostanie reszta. Dzielimy przez wielomian stopnia 1, więc reszta jest 1.

Zadanie 7

Pokaż, że kodowanie Hamming(7,4) umożliwia skorygowanie jednego przekłamanego bitu.

> Wskazówka:
> wystarczy pokazać, że odległość Hamminga między dwoma kodami wynosi co najmniej 3.

Załóżmy, że x,y to dwa kody kodowania Hamminga C z macierzą kontroli parzystości M.
Wtedy $x-y \in C$.

1. Jeżeli $dist(x,y)=1$, to $M(x:y)$ to kolumna z M.
   Wszystkie kolumny w M są niezerowe, ale jeśli $(x-y)$ to kod Hamminga, to $M(x-y)=0$ --> **sprzeczność**.

2. Jeżeli $dist(x,y)=2$, to $M(x:y)=0$ wtedy i tylko wtedy gdy w M są dwie kolumny liniowo zależne. Ale tak nie może być w Hammingu. --> **sprzeczność**.

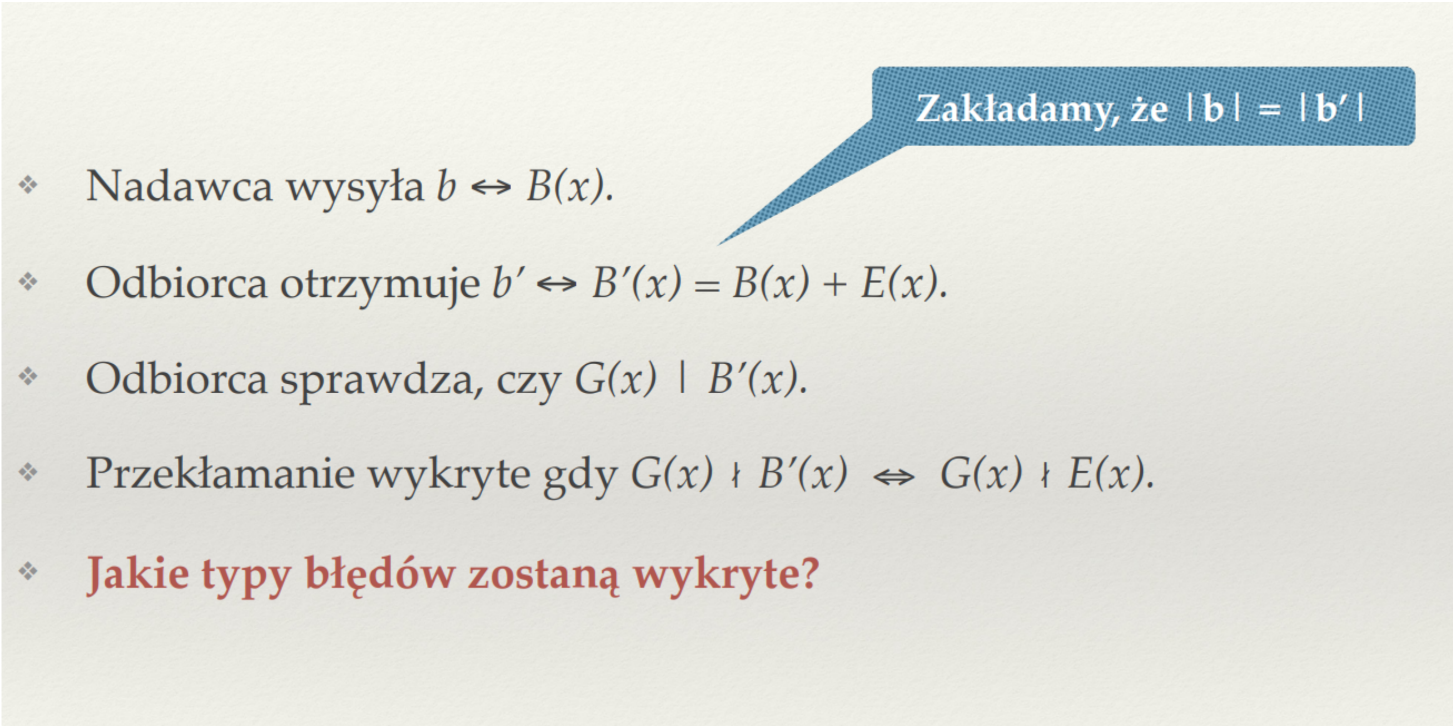
Zatem dist(x,y)>=3 dla wszystkich kodów x,y.

Zadanie 8

Należy sprawdzić 6 przypadków odległości bitów.
Sprawdzanie tak samo jak w zadaniu 9.

Zadanie 9

Załóżmy, że wyliczamy sumę CRC dla 4-bitowej wiadomości używając wielomianu $G(x)=x^3+x+1$. Wtedy wiadomość wraz z sumą ma długość 7 bitów. Załóżmy, że co najwyżej jeden z tych 7 bitów został przekłamany. Pokaż, jak odbiorca takiego komunikatu może wykryć i skorygować takie przekłamanie.



1. Liczymy sobie sumę kontrolną s dla jakieś wiadomości m przy użyciu G.
2. Łączymy tę wiadomość razem z sumą kontrolną, która nam wyszła i mamy m#s.

3. Dzielimy $m\#s$ tak jak bysmy chcieli wygenerować nową sumę kontrolną.
4. Powinno wyjść nam 0. Wpp Jakis bit został przekłamany i dostaniemy coś niezerowego.

Zadanie 10

Dana jest deterministyczna funkcja skrótu h zwracająca na podstawie tekstu liczbę m-bitową. Losujemy $2^{m/2}$ tekstów i obliczamy na nich funkcję h. Zakładamy tutaj, że przy takim losowaniu tekstu x, $h(x)$ jest losową (wybraną z rozkładem jednostajnym) liczbą m-bitową. Pokaż, że prawdopodobieństwo, że wsród wylosowanych tekstów istnieją dwa o takiej samej wartości funkcji h jest Ω(1).

- Łatwo zauważymy, że problem ten sprowadza się do *birthday paradox*.
- Ciężko obliczyć ppd. że conajmniej 2 teksty będą miały ten sam hasz, ale łatwo policzyć ppd zdażenia przeciwnego, czyli że wszystkie hasze będą różne.
- Czyli interesuje nas $1-\frac{2^m}{2^m}*\frac{2^m-1}{2^m}*\ldots*\frac{2^m-2^{\frac{m}{2}}}{2^m}$
- Możemy użyc tutaj sprawnej aproksymacji:$p(n,d)\approx1-e^{-\frac{n^2}{2*d}}$,gdzie n to liczba haszy, które losujemy, a d to liczba wszystkich możliwych haszy.
- Czyli w naszym przypadku wynik to:

  $p(n,d)\approx1-e^{-\frac{\left(2^{\frac{m}{2}}\right)^2}{2*2^m}}=e^{-\frac{2^m}{2*2^m}}=1-e^{-\frac{1}{2}}=0.3934693\approx40\%$