Lista 2

Jakub Kuciński, prowadzący Andrzej Łukaszewski

26 czerwca 2020

Spis treści

1 Zadanie 1

Czas wysyłania ramki musi być większy równy niż dwa razy czas propagacji, bo wtedy albo ramka dotrze do odbiorcy albo dowiemy się o kolizji podczas jej nadawania. Czas propagacji możemy wyrazić wzorem:

$$\tau = \frac{d_{max}}{v} = \frac{2.5km}{10^8 \frac{m}{s}} = 2.5 \cdot 10^5 s \tag{1}$$

Czyli minimalny czas wysyłania ramki wynosi $T_{min} = 2 \cdot \tau = 5 \cdot 10^5 s$. Długość ramki to prędkość wysyłania razy czas wysyłania, czyli:

$$Frame = Ethernet\_speed \cdot T_{min} = 10^7 \frac{bit}{s} \cdot 5 \cdot 10^5 s = 500\, bit \tag{2}$$

Minimalny rozmiar ramki to 500 bitów.

2 Zadanie 2

Prawdopodobieństwo, że jednemu uczestnikowi uda się wysłać ramkę:

$$P(p, n) = n \cdot p \cdot (1 - p)^{n-1} \tag{3}$$

Uzasadnienie: Wybieramy na n sposobów któremu uczestnikowi uda się wysłać ramkę. Udało mu się to z pstwem p. Wtedy też każdemu innemu uczestnikowi musiało się to nie udać, czyli $n-1$ krotnie $1-p$.
Aby policzyć dla jakiego p wartość $P(p,n)$ jest maksymalizowana możemy policzyć pochodnią $P(p,n)$ po p i przyrównać ją do 0.

$$\frac{\partial P(p,n)}{\partial p} = n(1-p)^{n-1} - n(n-1)p(1-p)^{n-2} = 0 \tag{4}$$

$$n(1-p)^{n-2}((1-p) - (np-p)) = 0 \tag{5}$$

$$n(1-p)^{n-2}(1-np) = 0 \tag{6}$$

Z powyższego wynika, że $p = \frac{1}{n}$. Łatwo zauważyć, że pochodna jest dodatnia na $[0, \frac{1}{n}]$ i ujemna na $[\frac{1}{n}, 1]$. Zatem $p = \frac{1}{n}$ jest maksimum globalnym.
Pozostało policzyć granicę.

$$\lim_{n\to\infty} P(\frac{1}{n}, n) = \lim_{n\to\infty} n \cdot \frac{1}{n} \cdot (1-\frac{1}{n})^{n-1} = \lim_{n\to\infty} \left((1-\frac{1}{n})^{-n}\right)^{-\frac{n-1}{n}} = \frac{1}{e} \tag{7}$$

3 Zadanie 3

Ethernet capture polega na wykorzystaniu przepustowości łącza w większości przez jedno urządzenie. Załóżmy, że mamy urządzenie1 i urządzenie2. Oba próbują wysłać ramkę, ale następuje kolizja. Teraz obie losują wartość ze zbioru $\{0,1\}$ odpowiadające ile rund mają odczekać. Załóżmy, że urządzenie1 wylosowało 0, a urządzenie2 wylosowało 1. Urządzenie1 wysyła ramkę. Następnie oba urządzenia znowu próbują wysłać ramkę i powstaje kolizja. Tym razem urządzenie1 losuje ze zbioru $\{0,1\}$, a urządzenie2 ze zbioru $\{0,\ldots,3\}$. Istnieje większa szansa na to, że znowu urządzenie1 zacznie nadawać jako pierwsze. Jeśli tak się stanie to prawdopodobnie znowu powstanie kolizja, gdy urządzenie2 przestanie czekać i nada pakiet. Wówczas urządzenia ponownie będą losować liczbę rund do odczekania przy czym szansa, że urządzenie2 wylosuje wartość mniejszą niż urządzenie1 jest jeszcze mniejsza. Prawdopodobieństwo nadania ramki przez urządzenie2 jako pierwsze, czyli bez kolizji, będzie się stopniowo zmniejszało, przez co urządzenie2 może bardzo długo czekać na swoją kolej. Do uniknięcia takiej sytuacji wprowadza się resetowanie licznika po 16 nieudanych próbach wysłania ramki.

4 Zadanie 4

Wiadomość 1010 można zinterpretować jako wielomian x^3+x. Aby uzyskać sumę kontrolną musimy obliczyć resztę z dzielenia x^3+x przez x^2+x+1 i zamianę wielomianu znowu na postać bitową.

$$x^3 + x = (x-1)\cdot(x^2+x+1) + (x+1) \tag{8}$$

Zamieniając $x+1$ na bity dostajemy suma kontrolna CRC równą 10. Dla x^7+1 dostajemy po prostu x^3+x, czyli 00001010.

5 Zadanie 5

Zastanówmy się jak wygląda dzielenie wielomianu przez $x+1$. Niech $W(x) = b_k x^k + \ldots + b_0 x^0$, gdzie $b_i \in \{0,1\}$. Zauważmy, że dodawanie $b_i + b_j$ w świecie $\mathbb{Z}_2$ jest równoznaczne z operacją xor (będziemy zapisywać $\veebar$). Wtedy możemy zapisać:

$$(x+1)\left(b_k x^{k-1} + (b_k \veebar b_{k-1})x^{k-2} + \ldots + (b_k \veebar \ldots \veebar b_1)\cdot 1\right) + (b_k \veebar \ldots \veebar b_1 \veebar b_0) = \tag{9}$$

$$= x^k b_k + x^{k-1}(b_k \veebar b_{k-1} \veebar b_k) + \ldots + 1\cdot(b_k \veebar \ldots \veebar b_1 \veebar b_k \veebar \ldots \veebar b_1 \veebar b_0) = \tag{10}$$

$$= x^k b_k + x^{k-1} b_{k-1} + \ldots + 1 \cdot b_0 = W(x) \tag{11}$$

Widzimy stąd, że resztą z dzielenia $W(x)$ przez $x+1$ wynosi $b_k \veebar \ldots \veebar b_1 \veebar b_0$. Jest to xor wszystkich współczynników b_i, a skoro odpowiadają one zerom i jedynkom w reprezentacji bitowej, to jest to xor wszystkich bitów tworzących wiadomość. Oczywiście jeśli liczba zapalonych bitów jest nieparzysta to xor zwróci 1, wpp 0. Stąd po dołączeniu bitu odpowiadającemu temu xorowi do wiadomości dostaniemy parzystą liczbę zapalonych bitów, więc faktycznie działa dzielenie przez $x+1$ działa tak samo jak bit parzystości.

6 Zadanie 6

Oznaczmy wielomian wejściowy jako $W(x) = A(x) + B(x)x^k + C(x)x^{k+m}$ oraz wielomian po wykonanych zmianach jako $W'(x) = A(x) + B'(x)x^k + C(x)x^{k+m}$, gdzie k jest najmniejszym numerem bitu, w którym nastąpiła zmiana. Wiemy, że $G(x)|W(x)$. Zastanówmy się, czy może się zdarzyć, że $G(x)|W'(x)$. Jeśli tak, to wtedy $G(x)|W(x) + x^k(B(x) - B'(x))$ a stąd $G(x)|x^k(B(x) - B'(x))$. Zauważmy, że $G(x)$ jest względnie pierwsze z x^k. Stąd $G(x)|B(x) - B'(x)$. Wiemy, że $st(G(x)) = n > n-1 \geqslant st(B(x) - B'(x))$ oraz zarówno $G(x)$ jak i $B(x) - B'(x)$ zawierają x^0, więc $G(x)$ nie dzieli $B(x) - B'(x)$.
Jeśli $G(x)$ nie zawiera składnika równego x^0 to ta własność nie zachodzi. Wtedy w pewnym sensie wielomian $G(x)$ zachowuje się jakby miał stopień o jeden mniejszy.
Kontrprzykład: $G(x) = x$ oraz wiadomości wejściowej 100 i zmienionej 000. Doszło do zmiany 1 bitu (stopień $G(x)$ wynosi 1, więc powinien móc wykryć błąd) a obie wiadomości są podzielne przez $G(x)$, więc błąd nie zostanie wykryty.

7 Zadanie 7

Kod Hamminga(7,4): $p_1, p_2, b_3, p_4, b_5, b_6, b_7$, gdzie p_1, p_2 i p_4 są zdefiniowane następująco:

$$p_1 = b_3 \veebar b_5 \veebar b_7 \tag{12}$$

$$p_2 = b_3 \veebar b_6 \veebar b_7 \tag{13}$$

$$p_3 = b_5 \veebar b_6 \veebar b_7 \tag{14}$$

Musimy pokazać, że odległość Hamminga między dowolnymi dwoma kodami jest większa równa 3. Rozważmy przypadki:

1. Kody różnią się na 3 lub 4 z pól b_i. Oczywiste.

2. Kody różnią się na 1 z pól b_i.
   Znakiem x zaznaczam w tabeli które bity p_i będą się różniły dla wyrazów różniących się na polu b_i.

	b_3	b_5	b_6	b_7
p_1	x	x		x
p_2	x		x	x
p_4		x	x	x

   Widzimy, że jeśli kody różnią się na jednym polu b_i to różnią się też na przynajmniej dwóch polach p_i, czyli łącznie różnią się na przynajmniej 3 bitach.

3. Kody różnią się na 2 z pól b_i.
   Dla odpowiednich kombinacji b_i, b_j wpisuję, które wyrazy p_i będą się różniły.

	b_3	b_5	b_6	b_7
b_3	-	p_2, p_3	p_1, p_3	p_3
b_5		-	p_1, p_2	p_2
b_6			-	p_1
b_7				-

   Wyrazy poniżej przekątnej są symetryczne

Znowu dla dowolnych dwóch kodów różniących się na 2 polach b_i mamy również różnicę na przynajmniej jednym polu p_i, czyli odległość takich kodów wynosi przynajmniej 3.

Z powyższych przypadków wynika, że odległość Hamminga dowolnych (poprawnych) dwóch kodów wynosi przynajmniej 3, a stąd jesteśmy w stanie rozpoznać błąd przekłamania $3 - 1 = 2$ bitów i skorygować błąd $(3 - 1)/2 = 1$ bitów.

8 Zadanie 8

Niech $W(x)$ oznacza wejściowy wielomian oraz $W'(x) = W(x) + E(x)x^k$ wielomian z błędem (k to najmniejszy numer bitu z błędem). Wtedy $G(x) = x^3 + x + 1$ dzieli $W'(x)$ wtw gdy dzieli $E(x)$, gdzie $E(x) = x^i + 1$ dla $i \in \{1, 2, 3, 4, 5, 6\}$. Wystarczy sprawdzić jakie reszty z dzielenia przez $G(x)$ może dać wielomian $E(x)$. Otrzymujemy:

$E(x)$	Reszta z dzielenia
$x^6 + 1$	x^2
$x^5 + 1$	$x^2 + x$
$x^4 + 1$	$x^2 + x + 1$
$x^3 + 1$	x
$x^2 + 1$	$x^2 + 1$
$x^1 + 1$	$x + 1$

Widzimy, że żaden z wielomianów nie jest podzielny przez $G(x)$ zatem każdy z podwójnych błędów zostanie wykryty.

9 Zadanie 9

$W'(x) = W(x) + E(x)$. Zbadajmy jak zmienia się suma kontrolna w zależności od numeru zmienionego bitu.

Numer bitu	Reszta z dzielenia $E(x)$
6	$x^2 + 1$
5	$x^2 + x + 1$
4	$x^2 + x$
3	$x + 1$
2	x^2
1	x
0	1

Widzimy, że zmianie każdego bitu odpowiada inna zmiana sumy kontrolnej. Możemy zatem policzyć nową sumę kontrolną (dla otrzymanej wiadomości) i xorując ją z sumą kontrolną z wiadomości dostaniemy resztę z dzielenia $E(x)$, która jednoznacznie odpowiada pewnemu bitowi, który został zmieniony.

10 Zadanie 10

Aby wyliczyć prawdopodobieństwo, że wsród wylosowanych tekstów istnieją dwa o takiej samej wartości funkcji h można policzyć prawdopodobieństwo zdarzenia przeciwnego.

$$P(m) = 1 - P'(m) \tag{15}$$

$$P'(m) = \prod_{i=0}^{2^{\frac{m}{2}}-1} \frac{2^m - i}{2^m} = \frac{2^m!}{2^{m \cdot 2^{\frac{m}{2}}} \cdot (2^m - 2^{\frac{m}{2}})!} \tag{16}$$

Iloczyn po drugiej równości ma następującą interpretację. Liczymy prawdopodobieństwo, że kolejne teksty przejdą na inną wartość niż poprzednie, które mają już przypisane różne wartości. Dla i-tego tekstu mamy

prawdopodobieństwo $\frac{2^m-i}{2^m}$, że nie trafimy na już zajętą wartość, bo i wartości jest już zajętych.
Policzmy granicę $P'(m)$ w nieskończoności.

$$\lim_{m\to\infty} P'(m) = \lim_{m\to\infty} = \frac{2^m!}{2^{m\cdot 2^{\frac{m}{2}}}\cdot(2^m-2^{\frac{m}{2}})!} = \left|podstawienie\ x=2^m\right| = \lim_{x\to\infty}\frac{x!}{x^{\sqrt{x}}\cdot(x-\sqrt{x})!} = \tag{17}$$

$$= \lim_{x\to\infty}\frac{x!}{\sqrt{2\pi x}(\frac{x}{e})^x}\cdot\frac{\sqrt{2\pi(x-\sqrt{x})}(\frac{x-\sqrt{x}}{e})^{x-\sqrt{x}}}{(x-\sqrt{x})!}\cdot\frac{\sqrt{2\pi x}}{\sqrt{2\pi(x-\sqrt{x})}}\cdot\frac{(\frac{x}{e})^x}{(\frac{x-\sqrt{x}}{e})^{x-\sqrt{x}}\cdot x^{\sqrt{x}}} \tag{18}$$

Ze wzoru Stirlinga wiemy, że granica dwóch pierwszych ułamków wynosi 1. Wystarczy zatem policzyć granice dwóch ostatnich ułamków.
Pierwsza granica:

$$\lim_{x\to\infty}\frac{\sqrt{2\pi x}}{\sqrt{2\pi(x-\sqrt{x})}} = \lim_{x\to\infty}\sqrt{\frac{x}{x-\sqrt{x}}} = \lim_{x\to\infty}\sqrt{\frac{1}{1-\frac{1}{\sqrt{x}}}} = 1 \tag{19}$$

Druga granica jest bardziej skomplikowana:

$$\lim_{x\to\infty}\frac{(\frac{x}{e})^x}{(\frac{x-\sqrt{x}}{e})^{x-\sqrt{x}}\cdot x^{\sqrt{x}}} = \lim_{x\to\infty}\frac{e^{-\sqrt{x}}\cdot x^{x-\sqrt{x}}}{(x-\sqrt{x})^{x-\sqrt{x}}} = \lim_{x\to\infty} e^{-\sqrt{x}}\left(\frac{x}{x-\sqrt{x}}\right)^{x-\sqrt{x}} = \tag{20}$$

$$= \lim_{x\to\infty} e^{(x-\sqrt{x})\ln\left(\frac{x}{x-\sqrt{x}}\right)-\sqrt{x}} = e^{\lim\limits_{x\to\infty}(x-\sqrt{x})\ln\left(\frac{x}{x-\sqrt{x}}\right)-\sqrt{x}} \tag{21}$$

Policzmy granicę w wykładniku podstawiając $u=\sqrt{x}$:

$$\lim_{u\to\infty}\left[(u^2-u)\ln\left(\frac{u^2}{u^2-u}\right)-u\right] = \lim_{u\to\infty}\left[u^2\ln\left(\frac{u^2}{u^2-u}\right)-u-u\ln\left(\frac{u^2}{u^2-u}\right)\right] = \tag{22}$$

$$= \lim_{u\to\infty}\left[u\left(u\ln\left(\frac{u^2}{u^2-u}\right)-1\right)\right] - \lim_{u\to\infty}\left[u\ln\left(\frac{u^2}{u^2-u}\right)\right] \tag{23}$$

Policzmy drugą granicę:

$$\lim_{u\to\infty} u\ln\left(\frac{u^2}{u^2-u}\right) = \lim_{u\to\infty}\frac{\ln\left(\frac{u^2}{u^2-u}\right)}{\frac{1}{u}} = \left|de\ l'Hospital\right| = \lim_{u\to\infty}\frac{\frac{u^2-u}{u^2}\cdot\frac{2u(u^2-u)-u^2(2u-1)}{(u^2-u)^2}}{-\frac{1}{u^2}} \tag{24}$$

$$= \lim_{u\to\infty}\frac{\frac{2u-2-2u+1}{u^2-u}}{-\frac{1}{u^2}} = \lim_{u\to\infty}\frac{u^2}{u^2-u} = \lim_{u\to\infty}\frac{1}{1-\frac{1}{u}} = 1 \tag{25}$$

Policzmy pierwszą granicę:

$$\lim_{u\to\infty} u\left(u\ln\left(\frac{u^2}{u^2-u}\right)-1\right) = \lim_{u\to\infty}\frac{u\ln\left(\frac{u^2}{u^2-u}\right)-1}{\frac{1}{u}} = \left|de\ l'Hospital\right| = \lim_{u\to\infty}\frac{\ln\frac{u}{u-1}+u(-\frac{1}{u^2-u})}{-\frac{1}{u^2}} = \tag{26}$$

$$= \lim_{u\to\infty}\frac{\ln\frac{u}{u-1}-\frac{1}{u-1}}{-\frac{1}{u^2}} = \left|de\ l'Hospital\right| = \lim_{u\to\infty}\frac{\frac{1}{u-u^2}+\frac{1}{(1-u)^2}}{\frac{2}{u^3}} = \lim_{u\to\infty}\frac{\frac{1-u+u}{u(1-u)^2}}{\frac{2}{u^3}} = \lim_{u\to\infty}\frac{u^3}{2u(u-1)^2} = \frac{1}{2} \tag{27}$$

Zatem mamy:

$$\lim_{u\to\infty}\left[(u^2-u)\ln\left(\frac{u^2}{u^2-u}\right)-u\right] = \frac{1}{2}-1 = -\frac{1}{2} \tag{28}$$

$$\lim_{x\to\infty}\frac{(\frac{x}{e})^x}{(\frac{x-\sqrt{x}}{e})^{x-\sqrt{x}}\cdot x^{\sqrt{x}}} = e^{\lim\limits_{x\to\infty}(x-\sqrt{x})\ln\left(\frac{x}{x-\sqrt{x}}\right)-\sqrt{x}} = e^{-\frac{1}{2}} = \frac{1}{\sqrt{e}} \tag{29}$$

$$\lim_{m\to\infty} P'(m) = \lim_{m\to\infty} = \frac{2^m!}{2^{m\cdot 2^{\frac{m}{2}}}\cdot(2^m-2^{\frac{m}{2}})!} = \frac{1}{\sqrt{e}} \tag{30}$$

$$\lim_{m\to\infty} P(m) = \lim_{m\to\infty}(1-P'(m)) = 1-\frac{1}{\sqrt{e}} \tag{31}$$

Skoro w nieskończoności $P(m)$ ma granicę $1 - \frac{1}{\sqrt{e}}$ oraz wartości $P(m)$ są dodatnie, to istnieje dodatni kres dolny wartości $P(m)$.