1. Czas propagacji $\tau \leq 2.5km : 10^8 \frac{m}{s} =$

$$= 2500m : 10^8 \frac{m}{s} =$$

$$= 2.5 \cdot 10^{-5} s$$

Czyli czas wysyłania ramki s musi być

$$s \geq 2 \cdot \tau \geq 5 \cdot 10^{-5} s$$

Czyli ramka musi mieć conajmniej

$$5 \cdot 10^{-5} s \cdot 10 \frac{Mb}{s} = \underline{500 b}$$

2. Dla wybranego hosta ppr sukcesu to $p\cdot(1-p)^{n-1}$ a ponieważ mamy ich n to prawdopodobieństwo sukcesu w rundzie to $\binom{n}{1}\cdot p\cdot(1-p)^{n-1} = P(p,n)$

czyli $P(p,n) = n\cdot p\cdot(1-p)^{n-1}$.

Pochodna po p

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

$\frac{\partial P}{\partial p}$ dla $p=\frac{1}{n}$: $n\left(1-\frac{1}{n}\right)^{n-1} - n\cdot\frac{1}{n}(n-1)\left(1-\frac{1}{n}\right)^{n-2} =$

$$= n\left(\frac{n-1}{n}\right)^{n-1} - (n-1)\left(\frac{n-1}{n}\right)^{n-2} =$$

$$= \frac{(n-1)^{n-1}}{n^{n-2}} - \frac{(n-1)^{n-1}}{n^{n-2}} = 0$$

Druga pochodna:

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

dla $\frac{1}{n} = p$ wartość jest ujemna czyli mamy maximum

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

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

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

3. Opis CSMA/CD

Dla każdej ramki do wysłania:

1. $m \leftarrow 1$
2. Poczekaj aż kanał będzie pusty i zacznij nadawać.
3. Podczas nadawania, nasłuchuj. Jeśli usłyszysz kolizję:
   - skończ nadawać,
   - wylosuj k ze zbioru $\{ 0, \dots, 2^m - 1 \}$ i odczekaj k rund,
   - $m \leftarrow m + 1$,
   - wróć do kroku 2.

Opis Ethernet capture.

Jest to zjawisko, które powstaje podczas używania CSMA/CD. Mamy przykładowo 2 komputery w sieci, które mają do wysłania dużo ramek. Oba próbują wysłać, dostają kolizje i liczbę rund które będą czekały zgodnie z algorytmem.
Może się okazać, że jeden z komputerów dostanie krótszy czas i on szybciej odczeka swój czas i zacznie wysyłać swoje ramki. Kiedy drugiemu komputerowi skończą się rundy i będzie próbował wysyłać swoją ramke znów oba komputery zauważą kolizję i znów losować będą czas jaki będą czekały (pula rund drugiego komputera jest już dwa razy większa). Znów się może zdarzyć że pierwszy komputer wylosuje bardzo mały czas, a drugi duży. Ta sytuacja może dziać się długo, aż np nie przedawni się ramka.
W takiej sytuacji mówi się że pierwszy komputer przejął kontrole nad kanałem.

$m = 1010 \qquad M(x) = x^3 + x$

a) $G(x) = x^2 + x + 1$

Chcemy takie $S(x)$, że $M(x) \cdot x^2 + S(x)$ dzieli się przez $G(x)$

Wiemy, że $S(x) = R(x)$, gdzie $R(x)$ to reszta dzielenia $M(x) \cdot x^2$ przez $G(x)$

$$M(x) \cdot x^2 = x^5 + x^3$$

$$\frac{x^5 + x^3}{x^2 + x + 1} = x^3 - x^2 + x - \frac{x}{x^2 + x + 1}$$

Czyli $S(x) = -x = x \mod 2$

Czyli $B(x) = 1010\underbrace{10}$

b) $G(x) = x^7 + 1$

$$M(x) \cdot x^7 = x^{10} + x^8$$

$$\frac{x^{10} + x^8}{x^7 + 1} = x^3 + x + \frac{(-x^3 - x)}{x^7 + 1}$$

Czyli $S(x) = x^3 + x$

$B(x) = 1010\underbrace{0000101010}_{\text{suma kontrolna}}$

5\. Wiemy że suma kontrolna będzie długości 1, czyli będzie to albo 1 albo 0.
Zrobimy indukcję po długości wiadomości.

Dla n = 1

Jeśli $m = 1$, $M(x) = 1$

to $\dfrac{M(x) \cdot x}{x+1} = 1 - \dfrac{1}{x+1}$

czyli $S(x) = 1$

Jeśli $m = 0$, $M(x) = 0$

$\dfrac{M(x) \cdot x}{x+1} = 0$

czyli $S(x) = 0$

Zgadza się.

Krok indukcyjny:

Załóżmy że suma kontrolna działa dla wszystkich wiadomości długości n.
Weźmy dowolną wiadomość o długości n+1. Mamy dwa przypadki.

Jeśli początek wiadomości to 0, to nasz wielomian się nie zmienia, parzystość też się nie zmienia, czyli suma kontrolna taka sama i prawidłowa.

Jeśli początek wiadomości to 1.

Mamy wiadomość $M' = 1\#M$, czyli $M'(x) = x^n + M(x)$

liczymy sume kontrolną:

$$\frac{M'(x)}{x+1} = \frac{x^n + M(x)}{x+1} = \underbrace{\frac{x^n}{x+1}}_{1)} + \underbrace{\frac{M(x)}{x+1}}_{2)}$$

z 1) wyjdzie nam reszta 1

z 2) wyjdzie poprawne dla $M(x)$ $S(x)$

dodamy do $S(x)$ reszte 1 i dostaniemy $(S(x)+1) \bmod 2$

jako sume kontrolną, co jest poprawne. ∎

6. $G(n) = x^n + \ldots + 1$

Mamy $M(x)$ i modyfikujemy go dowolnie dla jakiegoś okna n.

czyli $M'(x) = M(x) + x^j(x^0 + x^1 + \ldots + x^{n-1})$

Teraz pytanie czy $G(x) \mid M'(x)$

czyli czy $G(x) \mid x^j(x^0 + x^1 + \ldots + x^{n-1})$

$G(x) \nmid (x^0 + x^1 + \ldots + x^{n-1})$ bo tu zawsze będzie reszta (właśnie przez to x^0).

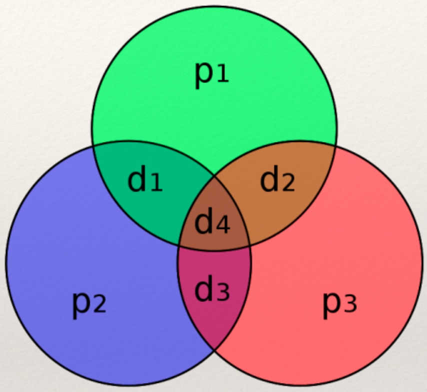
Oraz $G(x)$ i x^j są względnie pierwsze

czyli: $G(x) \nmid (x^0 + x^1 + \ldots + x^{n-1})$

- jeśli $G(x)$ nie zawiera x^0 to $G(x)$ mogłoby dzielić nawias.

7.

- 4 bity danych: d_1, d_2, d_3, d_4
- 3 bity parzystości: p_1, p_2, p_3 (każdy dla innych 3 bitów danych).
- Odległość Hamminga między dowolnymi dwoma kodami ≥ 3 *(ćwiczenie).*
- Znacznie wyższa efektywność niż naiwny (3,1)-kod.



Obrazek ze strony
https://en.wikipedia.org/wiki/Hamming(7,4)}

Jeśli dowolne dwa ciągi różnią się jednym bitem, to będzie to uwzględnione w 2 bitach parzystości, czyli będą się różniły 3 bitami.

Jeśli dwa ciągi różnią się dwoma bitami to będzie taki bit parzystości, że jednego z tych bitów nie uwzględniamy, więc będą się różniły o 1 + 2 = 3

Jeśli dwa ciągi różnią się trzema lub czterama bitami no to oczywiście własność zachodzi.

8. Podobnie co w 6 zadaniu.

Mamy $M'(x) = M(x) + x^j(1+x^k)$, $k \in \{1,2,\dots,6\}$

oczywiście $g(x) \nmid x^j$ więc trzeba pokazać że

$g(x) \nmid (1+x^k)$, $k \in \{1,2,3,4,5,6\}$

$k=1,2,3$ oczywiste bo za mały wielomian

$$k=4: \quad \frac{1+x^4}{x^3+x+1} = x + \frac{(-x^2-x+1)}{x^3+x+1}$$

$$k=5 \quad \frac{1+x^5}{x^3+x+1} = x^2-1 + \frac{(-x^2+x+2)}{x^3+x+1}$$

$$k=6 \quad \frac{1+x^6}{x^3+x+1} = x^3-x-1 + \frac{x^2+2x+2}{x^3+x+1}$$

$\blacksquare$

9. żeby wykryć, wystarczy że sprawdzimy czy to co dostaliśmy dzieli się przez $g(x)$. Było to omawiane w poprzednich zadaniach.

Jak to skorygować?

Sprawdzić które zamienienie bitu w naszej wiadomości sprawi, że będzie ona podzielna przez $g(x)$. Będzie to nasza wiadomość.