(1) 10Mbit $\rightarrow 10^7 bit/s = d$

$v = 10^8 m/s$

$K_1 \longleftrightarrow K_2$

$2{,}5km = 2500m = s$ $\quad K_1 \rightarrow K_2 : t = \frac{s}{v} = \frac{2500m}{10^8 m/s} = 2{,}5 \cdot 10^{-5} s$

Chcemy wykryć kolizję zanim wyślemy całą ramkę

$K_1 \rightarrow K_2 \rightarrow K_1$ tj. $2t$

$2 t_d = 2 \cdot 2{,}5 \cdot 10^{-5} \cancel{s} \cdot 10^7 \frac{bit}{\cancel{s}} = 5 \cdot 10^2 bit = 500$ bitów

512 bitów to 64 bajty więc się zgadza

(2) - dzielimy czas na rundy
- jeśli mam ramkę to wysyłam ją z pdp. $1/p$
- sukces gdy tylko 1 nadaje

n uczestników, pdp. p

- $P(p,n)$ - bez kolizji

X_i - i-ty wysłał

tylko 1 wysłał — takie samo

$$P(p,n) = P(X_1=1, X_2=0, \dots, X_n=0) + P(X_1=0, X_2=1, \dots, X_n=0) + \dots + P(X_1=0, \dots, X_n=1)$$
$$= n P(X_1=1, \dots, X_n=0) = n \underset{\text{1 wysłał}}{p} (1-p)^{n-1}$$
więc $(1-p)$ że nie wyśle

- liczymy pochodną po p: Miejsce zerowe w $p = 1/n \to$ ekstremum
liczymy 2 pochodną i podstawiamy $p = 1/n$ dostajemy ujemną wartość
więc mamy maksimum w $1/n$

- $p = 1/n$ więc $\cancel{n} \cdot \frac{1}{\cancel{n}}\left(1 - \frac{1}{n}\right)^{n-1} = \left(1-\frac{1}{n}\right)^{n-1}$

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

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

$\lim\limits_{n\to\infty}\left(1+\frac{1}{n-1}\right)^n = e$ więc $\lim\limits_{n\to\infty}\left(1-\frac{1}{n}\right)^n = \frac{1}{e}$

czyli $\lim\limits_{n\to\infty}\left(1-\frac{1}{n}\right)^{n-1} = \frac{1}{e}$

③ algorytm ~~ALOHA~~: CSMA/CD

1. $m \leftarrow 1$
2. czekaj na pusty kanał
3. nasłuchuj kolizji:
   - skończ nadawać
   - losuj k z $\{0, \ldots, 2^m - 1\}$ i czekaj k rund
   - $m \leftarrow m + 1$
   - wróć do kroku 2

Ethernet capture → 1 cały czas „wygrywa" dostęp do nadawania

np. w $t = 0$ A i B chcą nadawać i losują z $\{0, 1\}$

A wysyła, B czeka, $t = 0$

teraz A i B znowu chcą nadawać, ale A losuje z $\{0, 1\}$ a B już z $\{0, 1, 2, 3\}$

itd. szansa B maleje

po 16 rundach mówimy o channel capture, B się wycofuje na dłużej

im więcej użytkowników → mniejsza szansa na przechwycenie

(4) $M(x) = x^3 + x$ $\quad (1010)$
$\quad\quad x^3 x^2 x^1 x^0$

- $G(x) = x^2 + x + 1$, $r = 2$

w F_2 : $-1 \equiv +1$, $2 \equiv 0$ etc.

$x^r M(x) : G(x)$

$$\underline{x^3 + x^2 + x} \to Q(x)$$
$$x^5 + 0 + x^3 + 0 + 0 + 0 : x^2 + x + 1$$
$$\underline{x^5 + x^4 + x^3}$$
$$x^4$$
$$\underline{x^4 + x^3 + x^2}$$
$$x^3 + x^2$$
$$\underline{x^3 + x^2 + x}$$
$$x \to R(x)$$

$$x^r M(x) = \underbrace{(x^3 + x^2 + x)}_{Q(x)} \underbrace{(x^2 + x + 1)}_{G(x)} + \underbrace{x}_{\substack{\text{cr} \\ R(x) = S(x)}} \to \underset{x^1 x^0}{10} \to \text{KOD CRC}$$

- $G(x) = x^7 + 1$, $r = 7$

$x^r M(x) = x^{10} + x^8$

$$(x^7 + 1)(x^3 + x) \underbrace{- x^3 - x}_{R(x)} \to R(x) = x^3 + x = S(x)$$

$x^7 \downarrow$ $\quad x^8 \downarrow$

0001010 $\to$ kod CRC

$\underbrace{00}_{r=7}\, x^3 x^2 x^1 x^0$

(5) CRC-1 to bit parzystości

$G(x) = x + 1$, wiadomość m

$$S(x) = \begin{cases} 1, & m \text{ ma nieparzyście '1'} \\ 0, & m \text{ ma parzyście '1'} \end{cases}$$

T: Dla każdego wielomianu nad F_2 jest on podzielny bez reszty przez $x+1$ jeśli liczba jedynek jest parzysta

$W(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 x^0 \quad 2 \mid \sum_{i=0}^{n} a_i \iff G(x) \mid W(x)$

$a_i \in \{0, 1\}$

w F_2 dzielenie przez $(x+1)$ to to samo co dzielenie przez $(x-1)$

Weźmy dwa dowolne zapalone bity ($a_i = 1$) wielomianu $W(x)$

wtedy mamy x^b i x^c, $b > c$

dodajemy: $x^b + x^c = x^c \underbrace{(x^{b-c} + 1)}_{x^d + 1}$, $d = b - c$

$x^d + 1 = x^d - 1 = (x-1) Q(x) \to$ z szeregu geometrycznego

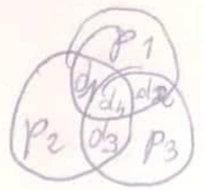
dowód: $x^d - 1 = \underbrace{(x-1)(x^{d-1} + x^{d-2} + \ldots + 1)}$

$$\begin{array}{rl} & x^d + x^{d-1} + \ldots + x \\ + & \quad\;\; x^{d-1} + \ldots + x - 1 \\ \hline & x^d - 1 \end{array}$$

więc dowolne pary $(x^b + x^c)$ dzieli się przez $G(x) = x+1$ bez reszty

- jeśli mamy parzyście jedynek $\to$ grupujemy w pary $\to$ każda para się dzieli
- jeśli mamy nieparzyście $\to$ zostanie jedynka bez pary $\to$ zostanie reszta 1

7 Hamming (7,4)



d - dane $d_1 d_2 d_3 d_4$

p - parity $p_1 p_2 p_3$

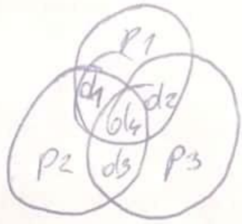
	p_1	p_2	d_1	p_3	d_2	d_3	d_4
p_1	1	0	1	0	1	0	1
p_2	0	1	1	0	0	1	1
p_3	0	0	0	1	1	1	1

$p_1 p_2 d_1 p_3 d_2 d_3 d_4$

$\overline{0}\ \overline{1}\ \ \ \overline{2}$ → potęgi 2

odl ≥ 3 tj. dla dowolnych dwóch kodów minimalna liczba zamian bitów ~~ag~~ by zamienić jeden kod w drugi

d_1	d_2	d_3	d_4	p_1	p_2	p_3
0	0	0	0	0	0	0
0	0	0	1	1	1	1
0	0	1	1	1	0	0
0	0	1	0	0	1	1
0	1	1	0	1	1	0
0	1	1	1	0	0	1
0	1	0	1	0	1	1
0	1	0	0	1	0	1
1	1	0	0	0	1	1
1	1	0	1	1	0	0
1	1	1	1	1	1	1
1	1	1	0	0	0	0
1	0	1	0	1	0	1
1	0	1	1	0	1	0
1	0	0	1	0	0	1
1	0	0	0	1	1	0



dla d przyjmujemy 1 bit różnicy

dla p:

- powtarzające się → różnią się w d na 3
- odległe o 1 → trzeba sprawdzić czy odl. o 2
- odległe o 2 → wystarczy odl ≥ 3

(10) h: f. haszująca

tekst $\rightarrow$ m bitów

$2^{m/2}$ tekstów, 2^m możliwych haszy

podobnie jak paradoks dnia urodzin:

(osoba $\rightarrow$ urodziny
tekst $\rightarrow$ hasz)

$P(A)$ - prawdop. że przynajmniej dwa teksty mają ten sam hasz

$P(A')$ - prawdop. że wszystkie teksty dostały unikatowy hasz

wzajemnie wykluczone: $1 = P(A) + P(A')$

a $P(A')$ łatwiej policzyć

---

prawdop. wylosowania k unikatowych liczb z N możliwych

załóżmy że wybraliśmy 1, wtedy pozostaje N-1 więc dla 2 liczb prawdop. to

$\frac{N-1}{N}$, dla 3: $\frac{N-1}{N} \cdot \frac{N-2}{N}$ $\rightarrow$ pomijamy dwie pierwsze

i tak dla k:

$$\frac{N-1}{N} \cdot \frac{N-2}{N} \cdot \ldots \cdot \frac{N-(k-1)}{N} \overset{\text{stirling}}{\approx} e^{\frac{-k(k-1)}{2N}} \approx e^{\frac{-k^2}{2N}}$$

więc $P(A) = 1 - P(A') = 1 - e^{-k^2/2N}$

---

u nas: $N = 2^m$, $k = 2^{m/2}$

$$P(A) = 1 - e^{-(2^{m/2})^2/2(2^m)} = 1 - e^{-(2^m)/(2^{m+1})}$$

$$= 1 - e^{-1/2} = 1 - \underbrace{\frac{1}{\sqrt{e}}}_{\approx 0.60653} \approx 0.39346$$

ok 40% szansy na kolizję

$\Omega(1) \iff \exists n_0 \in \mathbb{N}, c > 0 \quad h(n) \geq c$