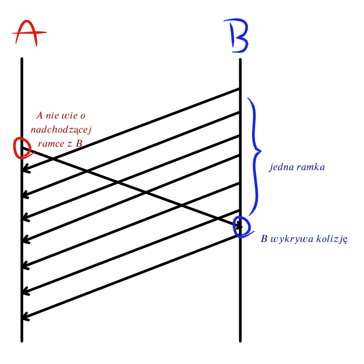
Zadanie 1

Ramka powinna być wystarczająco duża, by w momencie wykrycia kolizji nie było wątpliwości, że to podczas waśnie jej transmisji wystąpiła kolizja.



Czas propagacji = 0.000025s
Czas rundy >= 2*czas propagacji = 0.00005s
Przesyłamy z prędkością 10Mbit/s = 10^7 bitów na sekundę
Minimalny rozmiar ramki = 10^7 * 0.00005s
rozmiar ramki >= 500 bitów = 63 bajty
(po zaokrąglaniu 45 bajtów na dane)

Zadanie 2

$$P(p,n) = np(1-p)^{n-1}$$

$$P'(p) = -n(1-p)^{n-2}(np-1)$$

$$P'(p) = 0 \mapsto p = 1 \lor p = \frac{1}{n}$$

$$P''(p) = n(n-1)(np-2)(1-p)^{n-3}$$

$$P''\left(n^{-1}\right) < 0$$

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

Zadanie 3

Rozważmy sytuację, w której zarówno A i B próbują nadawać przez obecnie cichy kanał. Oboje wykrywają kolizję i losują swoje czasy oczekiwania (np. między 0 i 1). Przypuśćmy, że czas oczekiwania wypadł krótszy dla A, który zaczyna nadawać podczas gdy B wciąż oczekuje po czym próbuje nadać swoją ramkę przypuszczalnie doprowadzając do kolejnej kolizji. Ponieważ jest to już druga kolizja z rzędu dla B tym razem jego losowany czas oczekiwania będzie dłuższy (np. między 0 i 3).
Można sobie wyobrazić, że taka sytuacja powtórzy się wielokrotnie przez co B uzbiera wyjątkowo długi czas oczekiwania i A "przejmie kontrolę" nad kanałem.

Zadanie 4

$m = 1010$
$S(x)$ – suma kontrolna
$M(x) = x^3 + x$

$G_1(x) = x^2 + x + 1$
$G_1(x) \mid M(x)\,x^2 + S_1(x)$

$$\begin{array}{l} \quad x^3 + x^2 + x \\ \hline x^5 + x^3 : x^2 + x + 1 \\ + x^5 + x^4 + x^3 \\ \hline = x^4 \\ + x^4 + x^3 + x^2 \\ \hline = x^3 + x^2 \\ + x^3 + x^2 + x \\ \hline = x \end{array}$$

$S_1(x) = x \to m \oplus 10$

$G_2(x) = x^7 + 1$
$G_2(x) \mid M(x)\,x^7 + S_2(x)$

$$\begin{array}{l} \quad x^3 + x \\ \hline x^{10} + x^8 : x^7 + 1 \\ + x^{10} + x^3 \\ \hline = x^8 + x^3 \\ + x^8 + x \\ \hline = x^3 + x \end{array}$$

$S_2(x) = x^3 + x \to m \oplus 0001010$

Zadanie 5

$G(x) = x + 1$

$G(x) \mid M(x)\,x + S(x)$

Remainder theorem

$P(x) \bmod (x - r) = P(r) \iff P(r) = 0$

$P(x) = M(x)\,x \land r = 1$

$$P(1) \overset{*}{=} \begin{cases} 0, & \text{jeśli } P \text{ jest bitowo parzyste} \\ 1, & \text{wpp.} \end{cases}$$

Zadanie 6

$x^0 \in G(x)$, $st(G) = n$

$E(x) = e(x)\,x^i$, $e(x) = b_0 x^0 + b_1 x^1 + \ldots + b_{n-1} x^{n-1}$

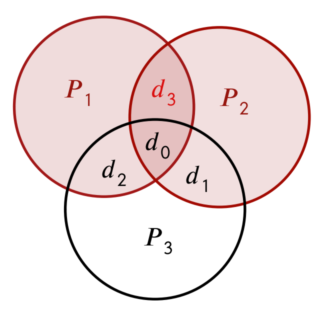
Pokażmy, że $G \nmid E$

- G jest względnie pierwsze z x^i (bo $x^0 \in G(x)$)
- $G \nmid e$, ponieważ $st(G) = n \land st(e) \leq n - 1$

Zadanie 7

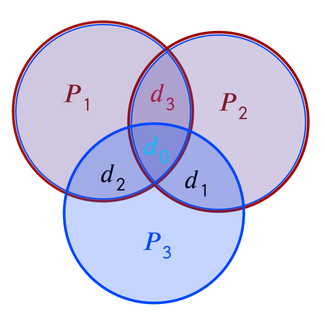
Interesują nas tylko poprawane kody Hamminga. Wystarczy więc rozważyć tylko kody różniące się na jednym lub dwóch databitach.

Różnica na dokładnie jednym databicie



Zauważmy, że jeśli zmienimy któryś z databitów d_i to kod nie będzie poprawny dopóki nie przewrócimy co najmniej dwóch dodatkowych bitów (bitów parzystości, którymi objęty jest zmieniony bit).

Różnica na dokładnie dwóch databitach



Każdy zmieniony bit jest objęty co najmniej dwoma bitami parzystości. Co więcej skoro zmieniamy dokładnie dwa bity to co najmniej jeden bit parzystości jest dla nich rozłączny, czyli będziemy musieli go przewrócić, aby zachować poprawność kodu co łącznie daje nam co najmniej trzy zmienione bity.

Różnice na trzech databitach trywialnie są w Hammingowej odległości nie mniejszej niż 3.

Zadanie 8

$G(x) = x^3 + x + 1$

$E(x) = x^i + x^j = (x^{j-i} + 1)\,x^i$, $n = j - i \leq 6$

- G jest względnie pierwsze z x^i
- Pozostaje pokazać, że $G \nmid (x^n + 1)$ dla $n \in [1, 6]$
  - $n \in [1, 3]$ to $st(G) > st(x^n + 1)$
  - $(x^4 + 1) \bmod G = x^2 + x + 1$
  - $(x^5 + 1) \bmod G = x^2 + x$
  - $(x^6 + 1) \bmod G = x^2$

Zadanie 10

$\#\text{teksty} = t = 2^{m/2}$

$\#\text{hashe} = q = 2^m$

$$P(m) = 1 - P\left(\begin{matrix}\text{wszystkie teksty mają} \\ \text{różną wartość wzgl. } h\end{matrix}\right)$$

$$= \frac{q!}{(q-t)!\,q^t}$$

$$\lim_{m \to \infty} P(m) = 1 - \frac{1}{\sqrt{e}} \approx 0.4$$