Zadanie 1 Minimalny rozmiar ramki jest określany na podstawie czasu wysyłania ramki, która zapewni nam, że będziemy wiedzieli czy ramka dotarła czy nastąpiła kolizja podczas nadawania ramki. Czas wysyłania ramki musi być dwukrotnie większy od czasy propagacji.

$$T_s \geq T_p$$

Czas propagacji możemy obliczyć na podstawie maksymalnej odległości $dist_{max} = 2,5km$ oraz prędkości rozchodzenia się sygnału $v = 10^8 m/s$

$$T_p = \frac{dist_{max}}{v}$$

Więc $T_p = 2,5 * 10^{-5}s$ czyli minimalny czas wysyłania musi wynosić $T_{smin} = 5 * 10^{-5}s$. Nasz kabel wysyła $E = 10^7 bit/s$ więc wzór na wielkość ramki jest następujący:

$$S_{frame} = E * T_{smin} = 5 * 10^2 bit.$$

Zadanie 2 Przypadek, że jakiejś stacji udało się nadać pakiet nastąpi wtedy kiedy tylko jedna stacja wyśle pakiet, więc

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

gdzie $p(1-p)^{n-1}$ oznacza prawdopodobieństwo, że tylko i-ty komputer próbował coś wysłać, a mnożymy razy n, ponieważ może być n takich komputerów. Aby obliczyć dla jakiej wartości p funkcja $P(p, n)$ przyjmuje największą wartość liczymy pochodną po p:

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

Pierwsze dwa wyrazy są zawsze dodatnie (z ograniczenia p i n), więc interesuje nas tylko $(1-np)$ i funkcja P(p,n) dla $p \in (0, \frac{1}{n})$ rośnie, a dla dla $p \in (\frac{1}{n}, 1)$ maleje, więc z tego wynika, że dla $p = \frac{1}{n}$ przyjmuje największą wartość.

$$\lim_{n\to\infty}[P(\frac{1}{n}, n) = \frac{1}{n}(1-\frac{1}{n})^{n-1} * n = (\frac{n-1}{n})^{n-1}] = \frac{1}{e}$$

Zadanie 3 Zjawisko to polega na zdominowaniu łącza przez jeden komputer. Przykład powstania to np. mamy 2 komputery A i B, które w tym samym czasie chcą nadać ramkę. Oba komputery nadają ramkę, ale wykrywają kolizję, więc losują liczbę z przedziału [0,1], A wylosowało 0, a B wylosowało 1, następnie A znów wysyła ramkę. B skończył się czas A i B znów próbują wysłać ramkę i im się nie udaje, ale tym razem A losuje liczbę z przedziału [0,1], a B z przedziału [0,3]. Przykładowo A wylosował 1, a B wylosował 3, więc A znów się uda wysłać ramki i ta sytuacja może się powiększać (tzn. im więcej nieudanych prób B tym większe prawdopodobieństwo, że następne próby się nie udadzą) dopóki B nie wylosuje liczby mniejszej od A lub B uda się wysłać ramkę. Warto dodać, że istnieje mechanizm, który przeciwdziała temu zjawisku i po 16 takich sytuacjach B startuje licznik od nowa.

Zadanie 4 Wykonujemy pewien rodzaj dzielenia pisemnego na bitach wiadomości (dzielna) i na zapisie wielomianu w formie bitowej (dzielnik), ale zamiast odejmowania wykonujemy operację XOR (inaczej wykonujemy operacje odejmowania w Z_2), a naszą sumą kontrolną będzie reszta. Dla $x^2 + x + 1$ otrzymujemy sumę kontrolną 10, a dla $x^7 + 1$ wynosi ona 0001010.

Zadanie 5 Przeprowadze dowód indukcyjny po liczbie bitów.

Teza: Dla słowa o n bitach, jeśli liczba zapalonych bitów jest parzysta to suma kontrolna CRC-1 wynosi 0, wpp. wynosi 1.

Baza indukcji - n=1

Jeśli bit jest zapalony to otrzymujemy wynik 1, a jeśli jest zgaszony otrzymujemy 0, więc teza jest spełniona dla n.

ZI: Dla n jest spełniona teza. (przy czym $n \geq 2$)

TI: Dla n+1 jest spełniona teza.

Rozpatrzmy 4 przypadki początku naszej wiadomości:

1) 10 po pierwszej operacji otrzymamy 01, więc liczba zapalonych bitów się nie zmieni (jeden gasimy drugi zapalamy), a otrzymaliśmy słowo o mniejszej ilości bitów (możemy "uciąć"początkowy bit) czyli korzystając z ZI otrzymujemy, że TI będzie spełniona dla tego przypadku.

2) 11 po pierwszej operacji otrzymamy 00, więc liczba zapalonych bitów się zmniejszy, ale o 2 więc parzystość zapalonych bitów nie ulegnie zmianie i podobnie jak powyżej można "uciąć"pierwszy bit i skorzystać z ZI, więc TI będzie spełniona.

3) i 4) Zaczynają się od 0, więc można "uciąć"pierwszy bit i korzystając z ZI, zostaje spełniona TI.

Więc na mocy zasady o indukcji spełniona jest teza.

Zadanie 6 Działania na wielomianach w Z_2. Równoważna jest interpretacja bitowa nasza ciągu z wielomianami.

Niech $G(x) = x^n + ... + 1$, a $W(x)$ będzie naszym wielomianem początkowym, a $W'(x) = W(x) + E(x)$, będzie wielomianem reprezentujący ciąg z zmienionymi bitami na spójnym odcinku o długości n. Czyli $E(x) = x^k(a_{n-1}x^{n-1} + ... + a_0)$ jest reprezentacją zmienionych bitów.

Wykrycie błędu będzie możliwe jedynie jeśli suma kontrolna się nie będzie zgadzała czyli wtedy, kiedy $E(x) mod G(x)! = 0$, a ponieważ wiemy, że $G(x)$ jest względnie pierwsze z x^k oraz $(a_{n-1}x^{n-1} + ... + a_0) mod G(x)! = 0$ ($(a_{n-1}x^{n-1} + ... + a_0)$ ma stopień mniejszy od $G(x)$.), więc z tego wynika, że $E(x) mod G(x)! = 0$ czyli jesteśmy w stanie wykryć błąd.

Jeśli G(x) nie zawiera x^0 to ta własność nie jest zachowana, ponieważ na naszym przedziale można wykonać operację XOR wraz z reprezentacją bitową naszego wielomianu i wynik nasz się nie zmieni, ponieważ ma to skutek lokalny. Przykładowo dla n = 3 odcinki 000 i 111 dla $x^3 + x^2 + x$ zwrócą tą samą wartość i nie zmienią bitów następujących po nich, a operacje zmiany i-tego bitu odcinku wynikające z operacji na wcześniejszych bitach są symetryczne.

Zadanie 7 Dla kodowanie Hamminga(7,4) mamy trzy bity kontrolne na pozycjach potęgi 2 oraz 4 bity informacyjne

$$b_1 b_2 b_3 b_4 b_5 b_6 b_7$$

Bity kontrolne są wyliczane na podstawie bitów informacyjnych:

$$b_4 = (b_5 + b_6 + b_7) mod 2$$

$$b_2 = (b_3 + b_6 + b_7) mod 2$$

$$b_1 = (b_3 + b_5 + b_7) mod 2$$

Wybierzmy dwa dowolne ciągi 4 bitów informacyjnych i pokażmy, że dla kodowania Hamminga każde mają odległość przynajmniej 3.

Najpierw rozważmy, że różnią się na jednej pozycji:

- b_3 to zmieni się b_2 i b_1 więc w sumie zmienią się 3 bity
- b_5 to zmieni się b_4 i b_1 więc w sumie zmienią się 4 bity
- b_6 to zmieni się b_4 i b_2 więc w sumie zmienią się 3 bity
- b_7 to zmieni się b_4, b_2 i b_1 więc w sumie zmienią się 4 bity

Różnią się na dwóch pozycjach, to wtedy chcemy pokazać, że któryś bit kontrolny ulegnie zmianie.

- Bit kontrolny b_1 ulegnie zmianie jeśli różnią się na bitach (b_3 i b_6), (b_5 i b_6), (b_7 i b_6).
- Bit kontrolny b_2 ulegnie zmianie jeśli różnią się na bitach (b_3 i b_5), (b_6 i b_6), (b_7 i b_5).
- Bit kontrolny b_4 ulegnie zmianie jeśli różnią się na bitach (b_5 i b_3), (b_6 i b_3), (b_7 i b_3).

czyli wszystkie pary bitów informacyjnych zostały pokryte i różnica dwóch bitów, wiąże się z odległością 3.

Dla większej liczby różnic odległość trzy jest zapewniona.

Więc w przypadku kodowania Hamminga(7,4) odległość między kodowaniami wynosi co najmniej 3, więc jesteśmy w stanie skorygować błąd.

Zadanie 8 Chcemy pokazać, że stosując wielomian $G(x) = x^3 + x + 1$ wykryjemy wszystkie podwójne, które nie są oddalone od siebie o więcej niż 6 bitów. Będę udowadniał to na wielomianach w Z_2. Zakładam, że w wielomianie taki podwójny błąd występuje tylko raz.

Niech początkowy wielomian będzie wielomian $W(x)$, a wielomian z błędem będzie postaci $W'(x) = W(x) + E(x)$, gdzie $E(x) = x^k(x^m + 1)$ jest wielomianem naszego błedu, a $m \in [1, ..., 6]$.

Rozpiszmy reszty dla $x^m + 1 \bmod G(x)$ dla każdego m:

m	reszta
1	$x + 1$
2	$x^2 + 1$
3	x
4	$x^2 + x + 1$
5	$x^2 + x$
6	x^2

Każda z reszt jest niezerowa i różna, dzięki czemu, że wiemy o tym, że x^k jest względnie pierwsze z $G(x)$ więc $x^k(x^m + 1) \bmod G(x)! = 0$, co pozwala nam wykryć błąd poprzez wyliczenie sumy kontrolnej i porównaniu jej z otrzymaną.

Zadanie 9 Podobnie jak wcześniej rozważyłem problem jako dzielenie wielomianu modul G(x) w Z_2. Rozpisałem jak przekłamanie bitu wpłynie na różnicę sum kontrolnych pomiędzy suma kontrolną otrzymaną, a sumą kontrolną, która możemy wyliczyć. Wyliczyliśmy

nr bitu	różnica sum kontrolnych
0	001
1	100
2	011
3	110
4	110
5	111
6	101

Widzimy, że w zależności od zmiany jednego bitu suma kontrolna zmienia się inaczej, więc porównując wyliczoną suma kontrolne z dostarczoną i XORując możemy sprawdzić, jak się różnią przez co który bit należy poprawić (zgodnie z tabelką.

Zadanie 10 Prawdopodobieństwo zdarzenia przeciwnego, czyli wszystkie hasła otrzymane są różne wynosi:

$$P'(m) = \frac{(2^m)!}{(2^m - 2^{m/2})! * 2^{m*2^{m/2}}}$$

Więc na podstawie otrzymujemy wzór na szukane prawdopodobieństwo:

$$P(m) = 1 - P'(m)$$

Aby pokazać, że $P(m) = \Theta(1)$, trzeba pokazać, że od pewnego m jest ograniczona przez niezerowe c_1 od dołu i c_2 od góry. Wiemy, że prawdopodobieństwo nie może być większe niż 1, więc ograniczenie z góry już mamy.

Licząc granicę, gdzie za 2^m podstawiamy x i korzystając ze wzorów Stirlinga:

$$\lim_{x->\infty} P'(m) = \lim_{x->\infty} \frac{x!}{x^{\sqrt{x}}(x-\sqrt{x})!} = \lim_{x->\infty} \frac{(\frac{x}{e})^x\sqrt{2\pi x}}{x^{\sqrt{x}}(\frac{x-\sqrt{x}}{e})^{x-\sqrt{x}}\sqrt{2\pi(x-\sqrt{x})}} =$$

$$\lim_{x->\infty} \frac{(\frac{x}{e})^x}{x^{\sqrt{x}}(\frac{x-\sqrt{x}}{e})^{x-\sqrt{x}}} * \lim_{x->\infty} \frac{\sqrt{x}}{\sqrt{x-\sqrt{x}}} = \lim_{x->\infty} \frac{x^{x-\sqrt{x}}}{(x-\sqrt{x})^{x-\sqrt{x}}e^{\sqrt{x}}} =$$

$$\lim_{x->\infty} e^{(x-\sqrt{x})\ln\frac{x}{x-\sqrt{x}}-\sqrt{x}}$$

Licząc granicę w wykładniku:

$$\lim_{x->\infty} (x-\sqrt{x})\ln\frac{x}{x-\sqrt{x}} - \sqrt{x} = \lim_{x->\infty} (\sqrt{x}(\sqrt{x}\ln\frac{x}{x-\sqrt{x}} - 1)) - \sqrt{x}\ln\frac{x}{x-\sqrt{x}}$$

Podstawiając (dzięki sugestii wolframa) y = $\sqrt{x}$ otrzymujemy

$$\lim_{y->\infty} (y(y\ln\frac{y^2}{y^2-y} - 1)) - \lim_{x->\infty} y\ln\frac{y^2}{y^2-y} =$$

$$\lim_{y->\infty} \frac{y \ln \frac{y^2}{y^2-y} - 1}{\frac{1}{y}} - \lim_{y->\infty} \frac{ln \frac{y^2}{y^2-y}}{\frac{1}{y}}$$

Korzystając z reguły de L'Hospitala dla obu granic (dla pierwszej dwukrotnie) otrzymujemy:

$$\lim_{y->\infty} \frac{\frac{1}{(1-y^2} + \frac{1}{y-y^2}}{\frac{2}{y^3}} - \lim_{y->\infty} \frac{\frac{y^2-y}{y^2} \frac{(u^2-y)2y-y^2(2y-1)}{(y^2-y)^2}}{\frac{-1}{y^2}}$$

Po zredukowaniu wyrazów:

$$\lim_{y->\infty} \frac{y^3}{2y(y-1)^2} - \lim_{y->\infty} \frac{y}{y-1} = \frac{1}{2} - 1 = 1/2$$

Czyli $\lim_{y->\infty} P'(m) = \frac{1}{\sqrt{e}}$

Więc $\lim_{y->\infty} P(m) = 1 - \frac{1}{\sqrt{e}}$

Korzystając z definicji Cauchy'ego dla granicy otrzymujemy nasze szukane $c_1 = 1 - \frac{1}{\sqrt{e}} - \epsilon$. Gdzie ϵ może byc np, 10^{-1000}, ważne aby było dodatnie. Więc udowodniliśmy to co chcieliśmy.