Ćwiczenia z Sieci komputerowych
Lista 2

1. W kablu koncentrycznym używanym w standardowym 10-Mbitowym Ethernecie[1] sygnał rozchodzi się z prędkością 10^8 m/s. Standard ustala, że maksymalna odległość między dwoma komputerami może wynosić co najwyżej 2,5 km. Oblicz, jaka jest minimalna długość ramki (wraz z nagłówkami).[2]

2. Rozważmy rundowy protokół Aloha we współdzielonym kanale, tj. w każdej rundzie każdy z n uczestników usiłuje wysłać ramkę z prawdopodobieństwem p. Jakie jest prawdopodobieństwo $P(p, n)$, że jednej stacji uda się nadać (tj. że nie wystąpi kolizja)? Pokaż, że $P(p, n)$ jest maksymalizowane dla $p = 1/n$. Ile wynosi $\lim_{n\to\infty} P(1/n, n)$?

3. Wyszukaj w sieci informację na temat zjawiska *Ethernet capture* i wytłumacz w jaki sposób ono powstaje. (Tym mianem określa się sytuację, w której jedna ze stacji nadaje znacznie częściej, choć wszystkie stacje używają algorytmu CSMA/CD.)

4. Jaka suma kontrolna CRC zostanie dołączona do wiadomości `1010` przy założeniu że CRC używa wielomianu $x^2 + x + 1$? A jaka jeśli używa wielomianu $x^7 + 1$?

5. Pokaż, że CRC-1, czyli 1-bitowa suma obliczana na podstawie wielomianu $G(x) = x + 1$, działa identycznie jak bit parzystości.

6. Załóżmy, że wielomian $G(x)$ stopnia n stosowany w CRC zawiera składnik x^0. Pokaż, że jeśli wybierzemy dowolny odcinek długości n z wiadomości i dowolnie go zmodyfikujemy (zmienimy dowolną niezerową liczbę bitów w nim), to zostanie to wykryte. Czy taka własność zachodzi, jeśli $G(x)$ nie zawiera składnika równego x^0?

7. Pokaż, że kodowanie Hamming(7,4) umożliwia skorygowanie jednego przekłamanego bitu. Wskazówka: wystarczy pokazać, że odległość Hamminga między dwoma kodami wynosi co najmniej 3.

8. Pokaż, że suma CRC stosująca wielomian $G(x) = x^3 + x + 1$ wykryje wszystkie podwójne błędy (zmianę wartości dwóch bitów), które są oddalone od siebie o nie więcej niż 6 bitów (tj. pomiędzy dwoma zmienianymi bitami jest nie więcej niż 5 innych bitów).

9. Załóżmy, że wyliczamy sumę CRC dla 4-bitowej wiadomości używając wielomianu $G(x) = x^3 + x + 1$; wtedy wiadomość wraz z sumą ma długość 7 bitów. Załóżmy, że co najwyżej jeden z tych 7 bitów został przekłamany. Pokaż, jak odbiorca takiego komunikatu może wykryć i skorygować takie przekłamanie.

10. Dana jest deterministyczna funkcja skrótu h zwracająca na podstawie tekstu liczbę m-bitową. Losujemy $2^{m/2}$ tekstów i obliczamy na nich funkcję h. Zakładamy tutaj, że przy takim losowaniu tekstu x, $h(x)$ jest losową (wybraną z rozkładem jednostajnym) liczbą m-bitową. Pokaż, że prawdopodobieństwo, że wsród wylosowanych tekstów istnieją dwa o takiej samej wartości funkcji h jest $\Omega(1)$.[3]

Materiały do kursu znajdują się w systemie Canvas: https://canvas.ii.uni.wroc.pl/.

Marcin Bieńkowski

[1] Można założyć, że 10 Mbit = 10^7 bit

[2] W rzeczywistości sygnał rozchodzi się ok. 2 razy szybciej, ale opóźnienia występują nie tylko w kablu.

[3] Dlaczego ten fakt jest istotny okaże się na wykładzie o kryptografii. Albo już się okazało.