Dydaktyczny symulator wybranych rozwiązań warstwy fizycznej sieci Ethernet

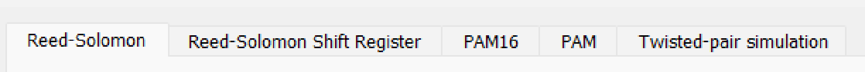
Michał Iwanicki, Mateusz Bauer, Marcin Garnowski

Politechnika Gdańska

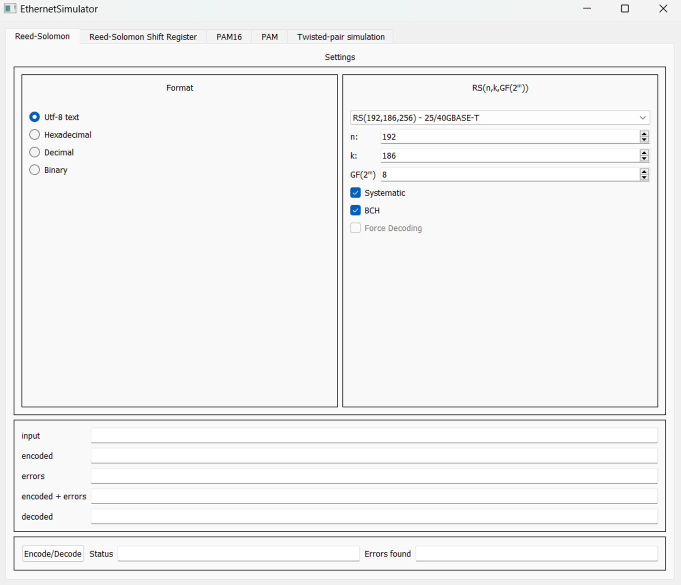
5 grudnia 2023

Uruchamianie

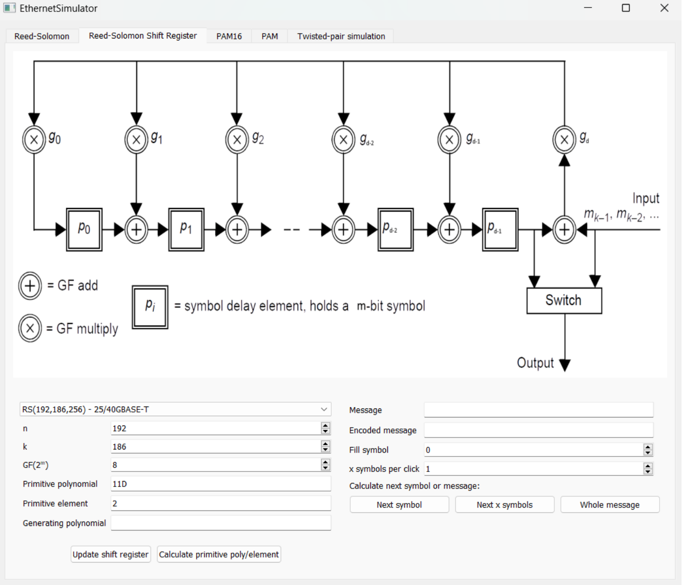
Poruszanie się po symulatorze



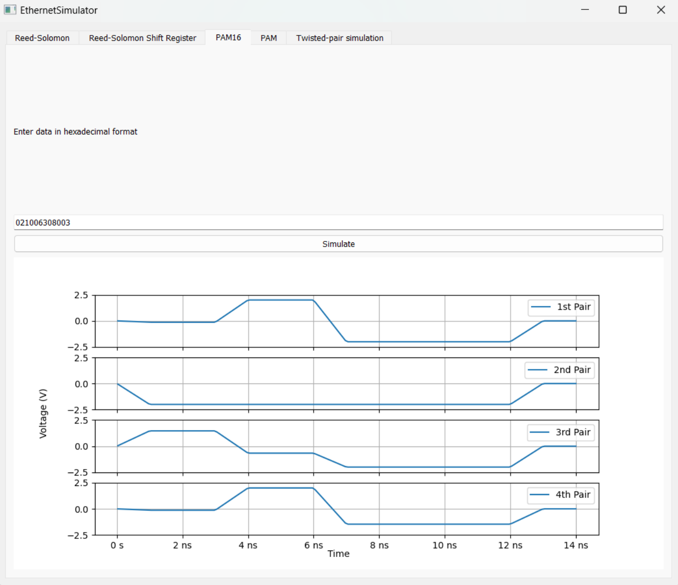
Reed-Solomon



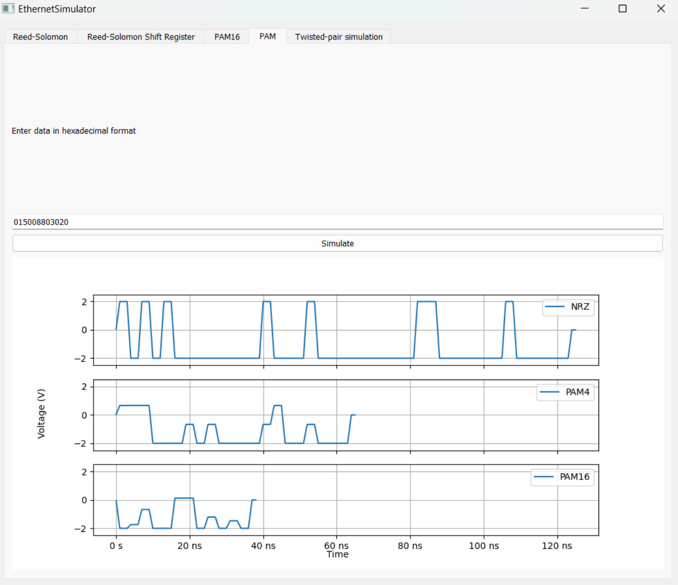
Reed-Solomon Shift Register

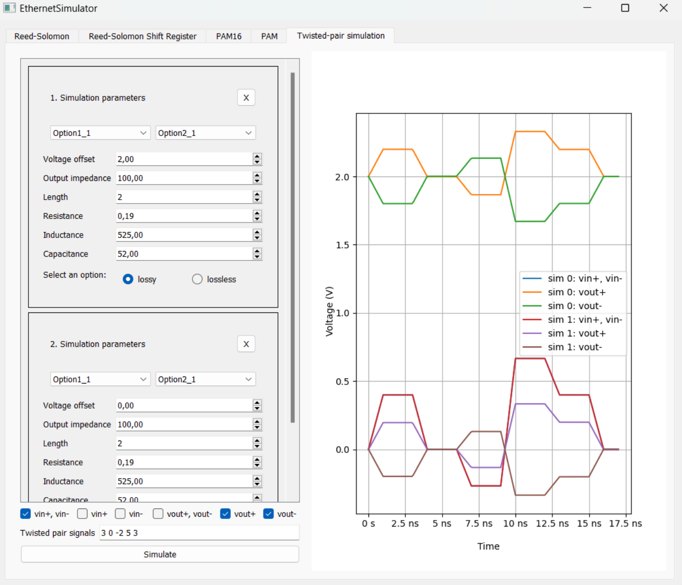


PAM16


EthernetSimulator
Reed-Solomon
Reed-Solomon Shift Register
PAM16
PAM
Twisted-pair simulation
Enter data in hexadecimal format
021006308003
Simulate
1st Pair
2nd Pair
3rd Pair
4th Pair
Voltage (V)
Time
0 s
2 ns
4 ns
6 ns
8 ns
10 ns
12 ns
14 ns

PAM


EthernetSimulator
Reed-Solomon
Reed-Solomon Shift Register
PAM16
PAM
Twisted-pair simulation
Enter data in hexadecimal format
015008803020
Simulate
NRZ
PAM4
PAM16
Voltage (V)
Time
0 s
20 ns
40 ns
60 ns
80 ns
100 ns
120 ns
2
0
−2



EthernetSimulator
Reed-Solomon
Reed-Solomon Shift Register
PAM16
PAM
Twisted-pair simulation
1. Simulation parameters
X
Option1_1
Option2_1
Voltage offset 2,00
Output impedance 100,00
Length 2
Resistance 0,19
Inductance 525,00
Capacitance 52,00
Select an option:
lossy
lossless
2. Simulation parameters
X
Option1_1
Option2_1
Voltage offset 0,00
Output impedance 100,00
Length 2
Resistance 0,19
Inductance 525,00
Capacitance 52,00
vin+, vin-
vin+
vin-
vout+, vout-
vout+
vout-
Twisted pair signals 3 0 -2 5 3
Simulate
2.0
1.5
1.0
0.5
0.0
Voltage (V)
0 s
2.5 ns
5 ns
7.5 ns
10 ns
12.5 ns
15 ns
17.5 ns
Time
sim 0: vin+, vin-
sim 0: vout+
sim 0: vout-
sim 1: vin+, vin-
sim 1: vout+
sim 1: vout-

Reed-Solomon

Kod Reeda-Solomona

Kodowanie korekcyjne Reeda-Solomona zostało stworzone przez Irvina S. Reeda oraz Gustava Solomona w 1960 roku.
Kody Reeda-Solomona charakteryzują się kilkoma parametrami:

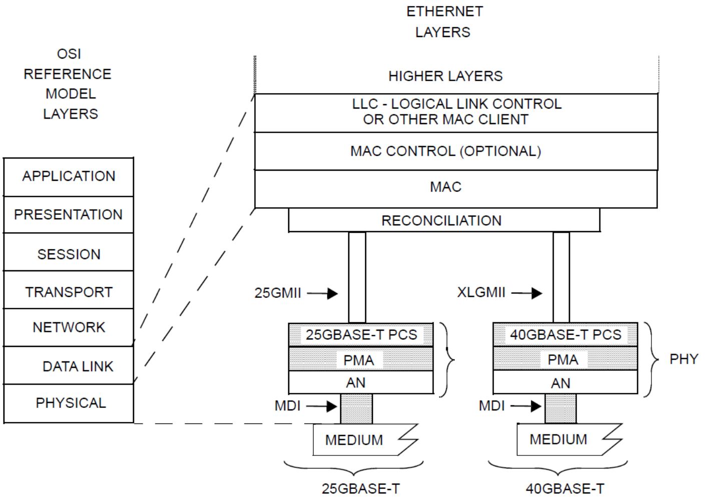
- Ciałem skończonym $\mathbb{F}_q$, $q = 2^m$, $m \in \{2, 3, \ldots\}$ w którym wykonywane są działania.
- długością wiadomości do zakodowania k
- długością słowa kodowego n gdzie $k < n \leq q$

Reed-Solomon

Przykładowe kodowania RS(n,k,$\mathbb{F}_{2^m}$) w różnych standardach

Kodowanie RS	Standardy
RS(544, 514, $\mathbb{F}_{2^{10}}$)	50GBASE-R, 100GBASE-KP4, 200GBASE-R, 400GBASE-R
RS(528, 514, $\mathbb{F}_{2^{10}}$)	10GBASE-R, 25GBASE-R, 100GBASE-CR4
RS(450, 406, $\mathbb{F}_{2^9}$)	1000BASE-T1
RS(360, 326, $\mathbb{F}_{2^{10}}$)	2.5GBASE-T1, 5GBASE-T1, 10GBASE-T1
RS(192, 186, $\mathbb{F}_{2^8}$)	25GBASE-T, 40GBASE-T

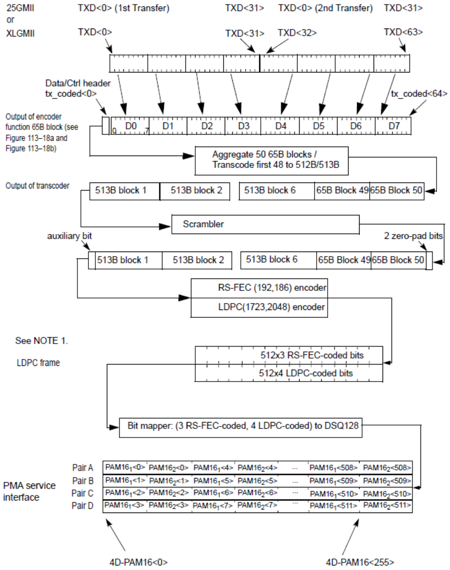
Warstwy Ethernet



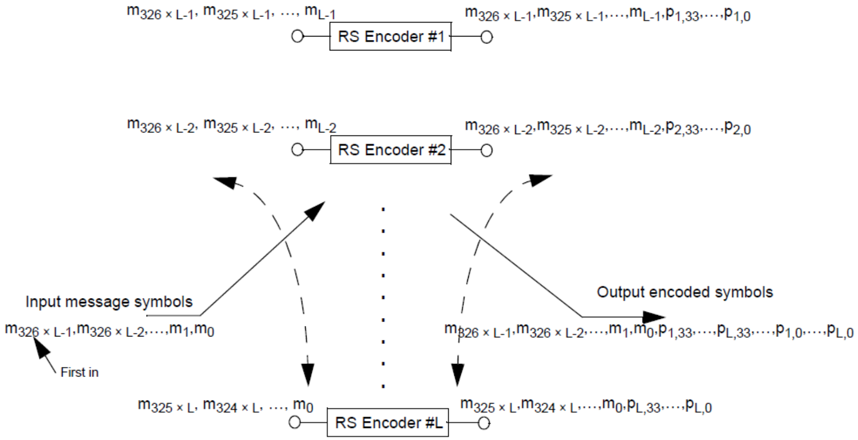
AN = AUTO-NEGOTIATION
MAC = MEDIA ACCESS CONTROL
MDI = MEDIUM DEPENDENT INTERFACE
PCS = PHYSICAL CODING SUBLAYER

PHY = PHYSICAL LAYER DEVICE
PMA = PHYSICAL MEDIUM ATTACHMENT
25GMII = 25 Gb/s MEDIA INDEPENDENT INTERFACE
XLGMII = 40 Gb/s MEDIA INDEPENDENT INTERFACE

25/40GBASE-T PCS



2.5/5/10GBASE-T1 RS Encoder



Czym jest ciało

Ciało K jest to struktura algebraiczna $(K, +, \cdot, 0, 1)$ definiująca działania $+$ i $\cdot$ nazywane dodawaniem i mnożeniem. Działania te muszą spełniać kilka warunków:

- dodawanie i mnożenie jest łączne, przemienne oraz zawiera elementy neutralne
- każdy element musi posiadać element odwrotny względem dodawania
- każdy element oprócz 0 musi posiadać element odwrotny względem mnożenia
- mnożenie jest rozdzielne względem dodawania

Definicja ciała

Formalnie ciało (K, +, ·, 0, 1) definiuje się za pomocą kilku aksjomatów.

Aksjomaty ciała

$$a + (b + c) = (a + b) + c \qquad \forall a, b, c \in K \tag{1}$$

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \qquad \forall a, b, c \in K \tag{2}$$

$$a + b = b + a \qquad \forall a, b \in K \tag{3}$$

$$a \cdot b = b \cdot a \qquad \forall a, b \in K \tag{4}$$

$$a + 0 = a \qquad \forall a \in K \tag{5}$$

$$a \cdot 1 = a \qquad \forall a \in K \tag{6}$$

$$a + (-a) = 0 \qquad \forall a \in K\ \exists -a \in K \tag{7}$$

$$a \cdot a^{-1} = 1 \qquad \forall a \in K \setminus \{0\}\ \exists a^{-1} \in K \tag{8}$$

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \qquad \forall a, b, c \in K \tag{9}$$

Ciało skończone

Czym jest ciało skończone

Ciało skończone to po prostu ciało o skończonej liczbie elementów. Oznaczane jest zwykle jako $\mathbb{F}_q$ gdzie q to liczba elementów. Aby ciało skończone istniało q musi być liczbą pierwszą p bądź potęgą takiej liczby $q = p^m$, $m \in \{2, 3, \ldots\}$

Definicja ciała skończonego

Najprościej ciało skończone $\mathbb{F}_p$ gdzie p to liczba pierwsza można zdefiniować jako pierścień klas reszt $\mathbb{Z}_p$.

Definicja tego pierścienia

$$\mathbb{Z}_p = \{[0]_p, [1]_p, [2]_p, \ldots, [p-1]_p\}$$
$$[a]_p = \{a + k \cdot p | k \in \mathbb{Z}\}$$

$$[a]_p + [b]_p = [a+b]_p$$
$$[a]_p \cdot [b]_p = [a \cdot b]_p$$

Ciało skończone $\mathbb{F}_2$

Jednym z najczęściej używanych ciał skończonych w informatyce jest ciało $\mathbb{F}_2$ zawierające 2 elementy $\{0, 1\}$ w którym działania $+$ i $\cdot$ są równoważne operacjom logicznym XOR oraz AND

Dodawanie i mnożenie w $\mathbb{F}_2$

a	b	$+$	$\cdot$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

Ciało skończone $\mathbb{F}_{2^m}$

Elementami ciała skończonego $\mathbb{F}_{2^m}$, $m \in \{2, 3, \ldots\}$ są wielomiany o postaci

$$\sum_{n=0}^{m-1} c_n \alpha^n = c_0 + c_1 \alpha + c_2 \alpha^2 + \cdots + c_{m-1} \alpha^{m-1}, c_n \in \{0, 1\}$$

Przykładowe elementy $\mathbb{F}_{2^3}$

$$\mathbb{F}_{2^3} = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}$$
$$\mathbb{F}_{2^3} = \{000_2, 001_2, 010_2, 011_2, 100_2, 101_2, 110_2, 111_2\}$$
$$\mathbb{F}_{2^3} = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

Dodawanie w $\mathbb{F}_{2^m}$

Dodawanie dwóch elementów ciała $\mathbb{F}_{2^m}$ jest po prostu obliczeniem XOR z ich reprezentacji binarnej

Przykład dodawania w $\mathbb{F}_{2^3}$

$$a = \alpha^2 + \alpha = 110_2$$
$$b = \alpha + 1 = 011_2$$
$$a + b = 110_2 \oplus 011_2$$

$$\begin{array}{r} 110_2 \\ \oplus\ 011_2 \\ \hline 101_2 \end{array}$$

Mnożenie w $\mathbb{F}_{2^m}$

Aby zdefiniować mnożenie w $\mathbb{F}_{2^m}$ potrzebujemy najpierw znaleźć nierozkładalny wielomian $p(x)$ stopnia m o współczynnikach w $\mathbb{F}_p$. Wynikiem mnożenia elementów ciała $\mathbb{F}_{2^m}$ będzie reszta z dzielenia iloczynu tych elementów przez wielomian $p(x)$

Przykład mnożenia w $\mathbb{F}_{2^3}$

$$
\begin{aligned}
p(x) &= x^3 + x + 1 \\
a &= \alpha^2 + 1 \\
b &= \alpha + 1 \\
a \cdot b &= (\alpha^2 + 1) \cdot (\alpha + 1) && \mod x^3 + x + 1 \\
a \cdot b &= \alpha^3 + \alpha^2 + \alpha + 1 && \mod x^3 + x + 1 \\
a \cdot b &= \alpha^2
\end{aligned}
$$

Mnożenie w $\mathbb{F}_{2^m}$

Reszta z dzielenia przez $p(x)$

$a \cdot b = \alpha^3 + \alpha^2 + \alpha + 1 = 1111_2$
$p(x) = x^3 + x + 1 = 1011_2$

$$
\begin{array}{l}
1 \\
\hline
1111 : 1011 \\
\oplus\ 1011 \\
\hline
100 = \alpha^2
\end{array}
$$

Właściwości

Kody Reeda-Solomona cechują się możliwością korekty $\lfloor \frac{n-k}{2} \rfloor$ lub wykrycia $n - k$ błędnych symboli. Symbol w ciele $\mathbb{F}_{2^m}$ składa się z m bitów co w przypadku błędów grupowych daje możliwość korekty maksymalnie $m \cdot \lfloor \frac{n-k}{2} \rfloor$ bitów bądź detekcji $m(n-k)$ przekłamanych bitów

Oryginalny sposób kodowania

Sposób kodowania przedstawiony w pracy Reeda i Solomona polega na stworzeniu wielomianu $p_m(x) = \sum_{i=0}^{k-1} m_i x^i$, gdzie $m_i \in \mathbb{F}_q$ to i-ty element wiadomości, po czym za pomocą tego wielomianu obliczane jest słowo kodowe $C(m) = (p_m(a_0), p_m(a_1), \ldots, p_m(a_{n-1}))$ gdzie a_i to różne elementy ciała $\mathbb{F}_q$.

Kod systematyczny

Za pomocą niewielkiej modyfikacji można stworzyć kod systematyczny czyli taki w którym słowo kodowe zawiera w sobie kodowaną wiadomość. Żeby stworzyć kod systematyczny musimy zmodyfikować sposób tworzenia wielomianu w taki sposób by $p_m(x_i) = m_i$ dla $i \in \{0, 1, \ldots, k-1\}$.
Jednym ze sposobów stworzenia takiego wielomianu jest użycie metody interpolacji wielomianów. Słowo kodowe wygenerowane z tego wielomianu będzie zawierało wiadomość w pierwszych k elementach.

$$\begin{aligned} C(m) &= (p_m(a_0), p_m(a_1), \ldots, p_m(a_{n-1})) \\ &= (m_0, m_1, \ldots, m_{k-1}, p_m(a_k), p_m(a_{k+1}), \ldots, p_m(a_{n-1})) \end{aligned}$$

Kod BCH

Kody BCH (Bose-Chaudhuri-Hocquenghem) są kodami cyklicznymi co oznacza że każde przesunięcie słowa kodowego jest także słowem kodowym.
Aby zbudować kod BCH Reeda-Solomona potrzebujemy najpierw funkcji minimalnej pierwiastka α, czyli takiego minimalnego wielomianu nierozkładalnego $p(x)$ stopnia m dla którego istnieje element prymitywny α który pozwala wygenerować całe ciało skończone

$$\mathbb{F}_{2^m} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^m-1}\}$$

Obliczanie kodu BCH

Mając taki element prymitywny jesteśmy w stanie stworzyć wielomian generujący $g(x)$ używając wzoru

$$t = n - k$$

$$g(x) = \prod_{i=0}^{t-1}(x - \alpha^i) = g_t x^t + g_{t-1}x^{t-1} + \cdots + g_1 x + g_0$$

Aby utworzyć słowo kodowe wystarczy pomnożyć wielomian $p_m(x)$ przez wielomian generujący $g(x)$

Aby uzyskać systematyczne słowo kodowe $s(x)$ musimy obliczyć:

$$s_r(x) = p_m(x) \cdot x^t \mod g(x)$$

$$s(x) = p_m(x) \cdot x^t - s_r(x)$$