



Wrocław University of Technology

Podstawy Telekomunikacji Teoria informacji i kodowania

dr Robert Borowiec

Politechnika Wrocławska

Instytut Telekomunikacji, Teleinformatyki i Akustyki

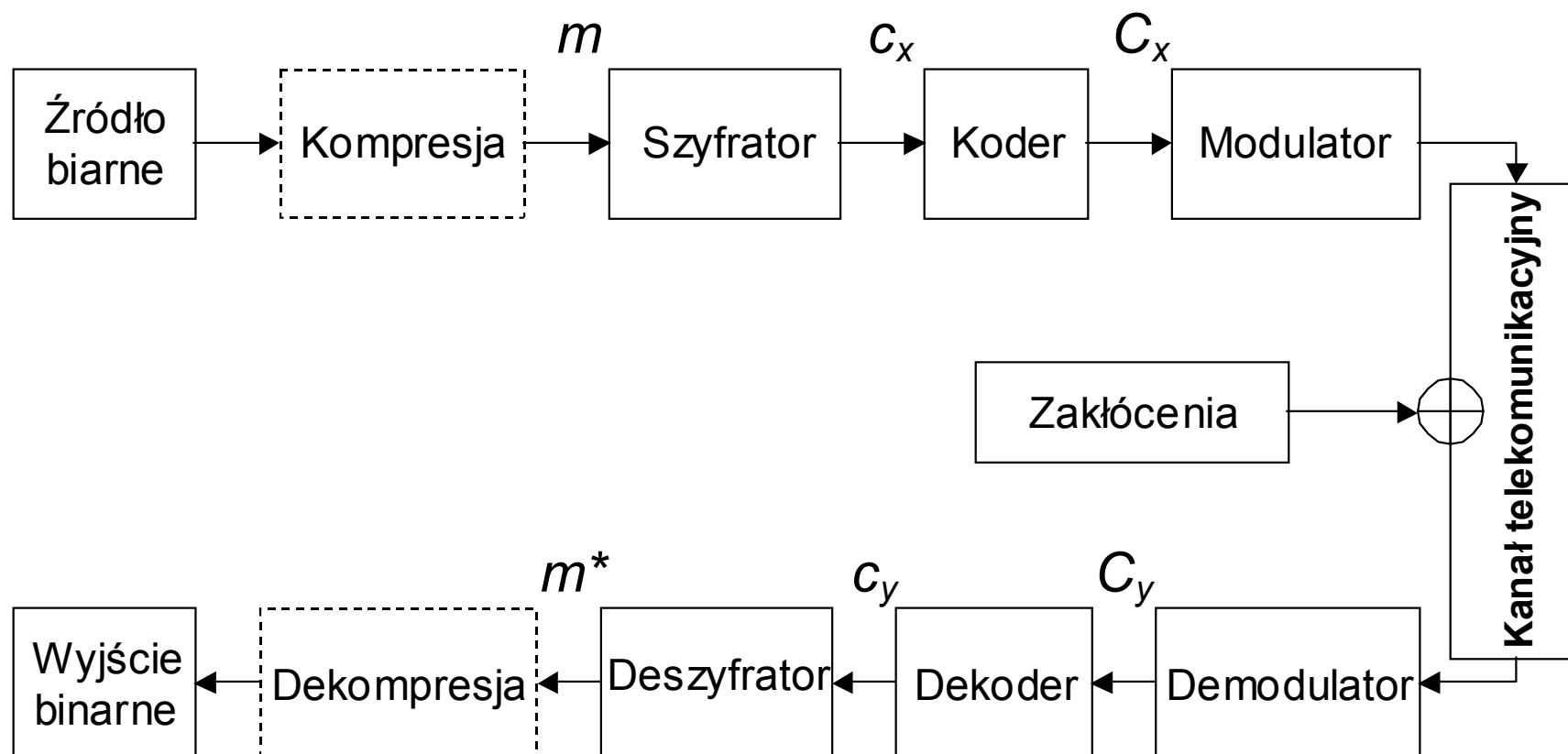
pokój 909, C-5

tel. 3203083

e-mail: Robert.Borowiec@pwr.wroc.pl

www: <https://kursy.pwr.wroc.pl/>

Cyfrowy system transmisyjny





Pojęcia podstawowe

Kompresja danych - stosowana jest po to, aby zmniejszyć ilość przesyłanych danych bez uszczerbku dla zawartej w nich informacji. Rozróżniamy dwa podstawowe sposoby kompresji:

- ☐ ilościowa (bezstratna)
- ☐ jakościowa

Kompresja ilościowa - wykorzystuje redundancję (nadmiarowość) źródła informacji.

Kompresja jakościowa - wykorzystuje ułomność zmysłów człowieka (zgadzamy się na niezauważalną utratę ilości informacji).



Pojęcia podstawowe

Szyfrowanie - stosowane jest po to, aby zapewnić:

⇒ **poufność informacji (prywatność)**

⇒ **autentyczność informacji (integralność)**

Szyfrator ma za zadanie tak zmienić informację, aby była ona niezrozumiała dla osoby nieuprawnionej do odczytania wiadomości. Odtworzenie jawnej treści informacji następuje dopiero w **deszyfratorze**, którego zadaniem jest również stwierdzenie czy wiadomość jest autentyczna.

Szyfrowanie nie zwiększa ilości bitów w informacji.



Pojęcia podstawowe

Modulacja – nadanie sygnałowi elektrycznemu cech charakterystycznych w celu przesłania informacji.

Modulator odwzorowuje zbiór symboli (słów binarnych) na zbiór sygnałów odpowiednich do przesłania w medium transmisyjnym.

Demodulator przeprowadza demodulację i detekcję odebranych sygnałów. Podejmuje decyzję, który symbol (słowo binarne) zostało nadane.



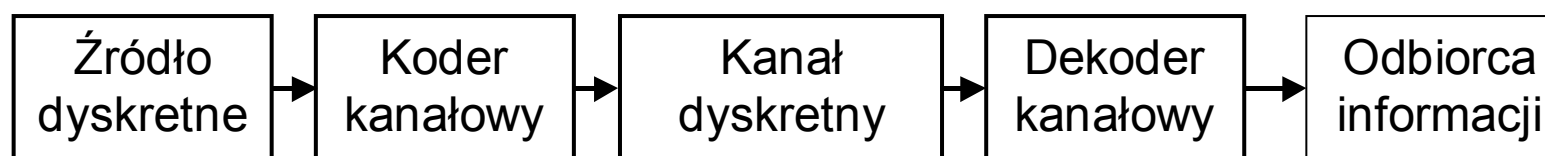
Pojęcia podstawowe

Kodowanie kanałowe - stosowane jest po to, aby zapewnić przy określonym stosunku E_b/N_o (energii bitu do energii szumu) odpowiednią jakość transmisji. Kodowanie jest procesem wprowadzania informacji nadmiarowej, którą potem dekodery wykorzystuje do oceny odebranych informacji.

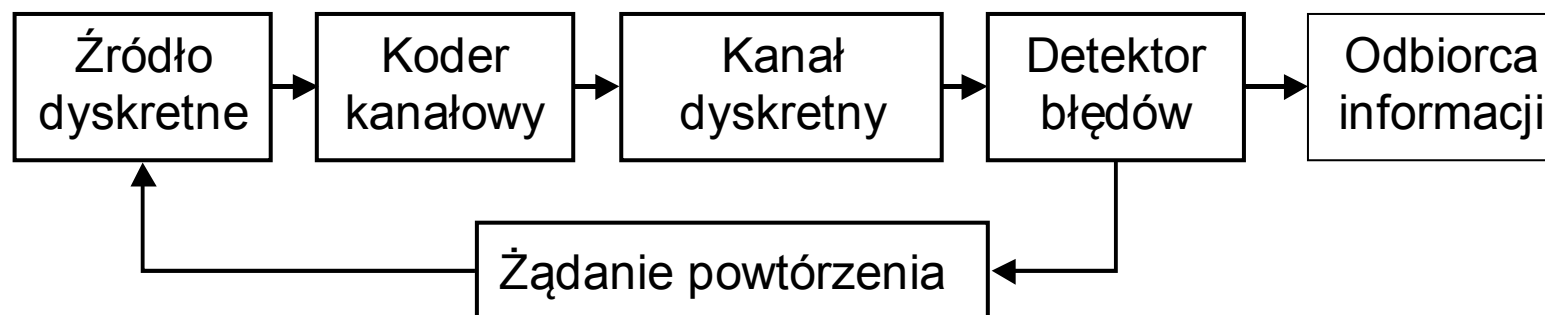
Układ **koder-dekoder** ma, więc za zadanie zmniejszenie wpływu szumu na jakość transmisji. Wprowadzenie informacji nadmiarowej (bitów kontrolnych) implikuje **wzrost prędkości strumienia bitów, a więc i szerokości pasma sygnału.**

Poprawa jakości transmisji

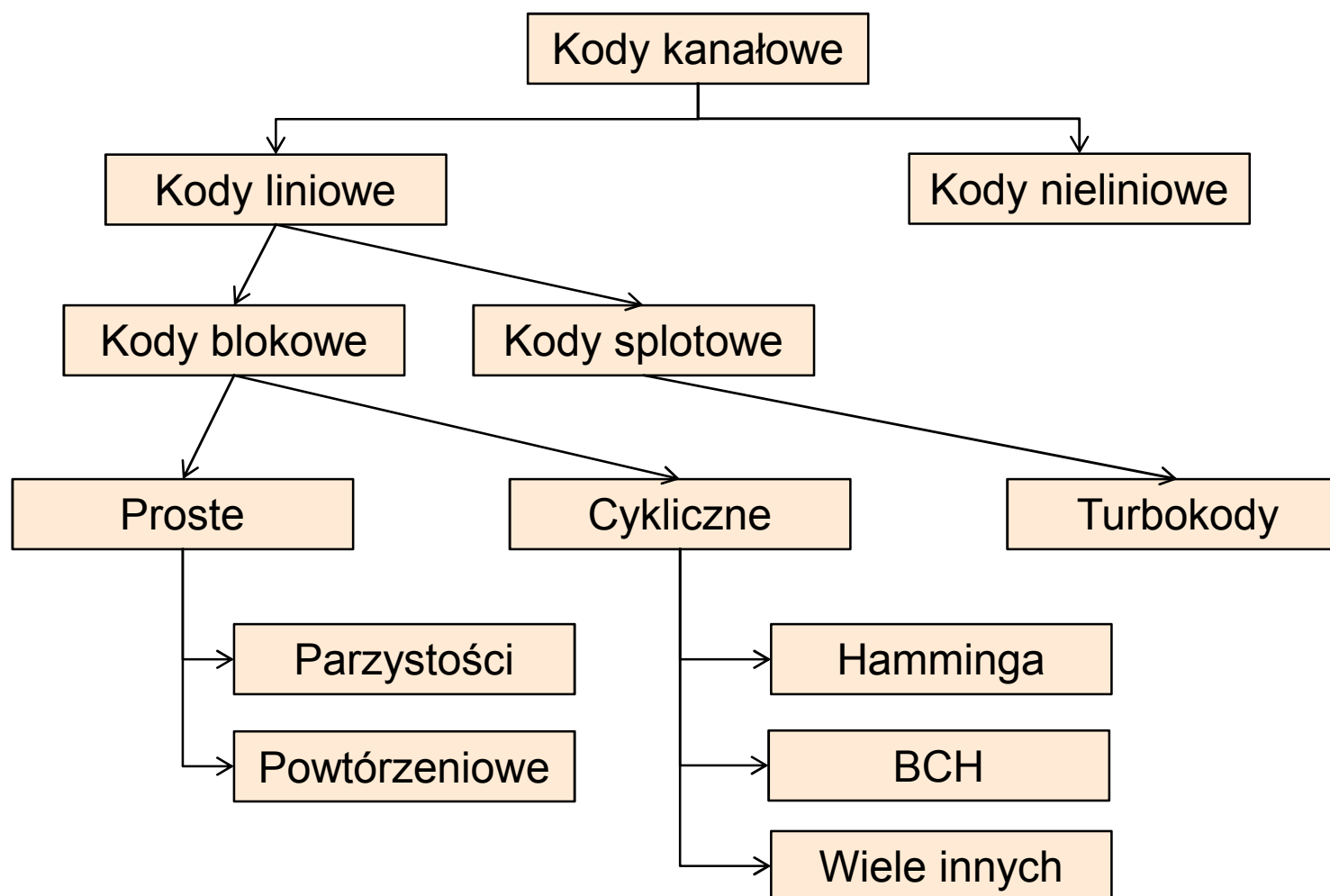
Korekcja błędów w przód (ang. FEC)



Automatyczne żądanie powtórzenia (ang. ARQ)



Podział kodów





Podział kodów

W ujęciu historycznym kody dzieli się na:

- blokowe
- splotowe

Kodowanie blokowe polega na wprowadzeniu na wejście kodera bloków informacji binarnej o długości k bitów i dodaniu do nich $n-k$ bitów nadmiarowych (parzystości).

Przy **kodowaniu splotowym** informacja bitowa z wejścia jest przetwarzana w sposób ciągły. Koder dokonuje dyskretnego splotu strumienia informacji bitowej z odpowiedzią impulsową kodera.



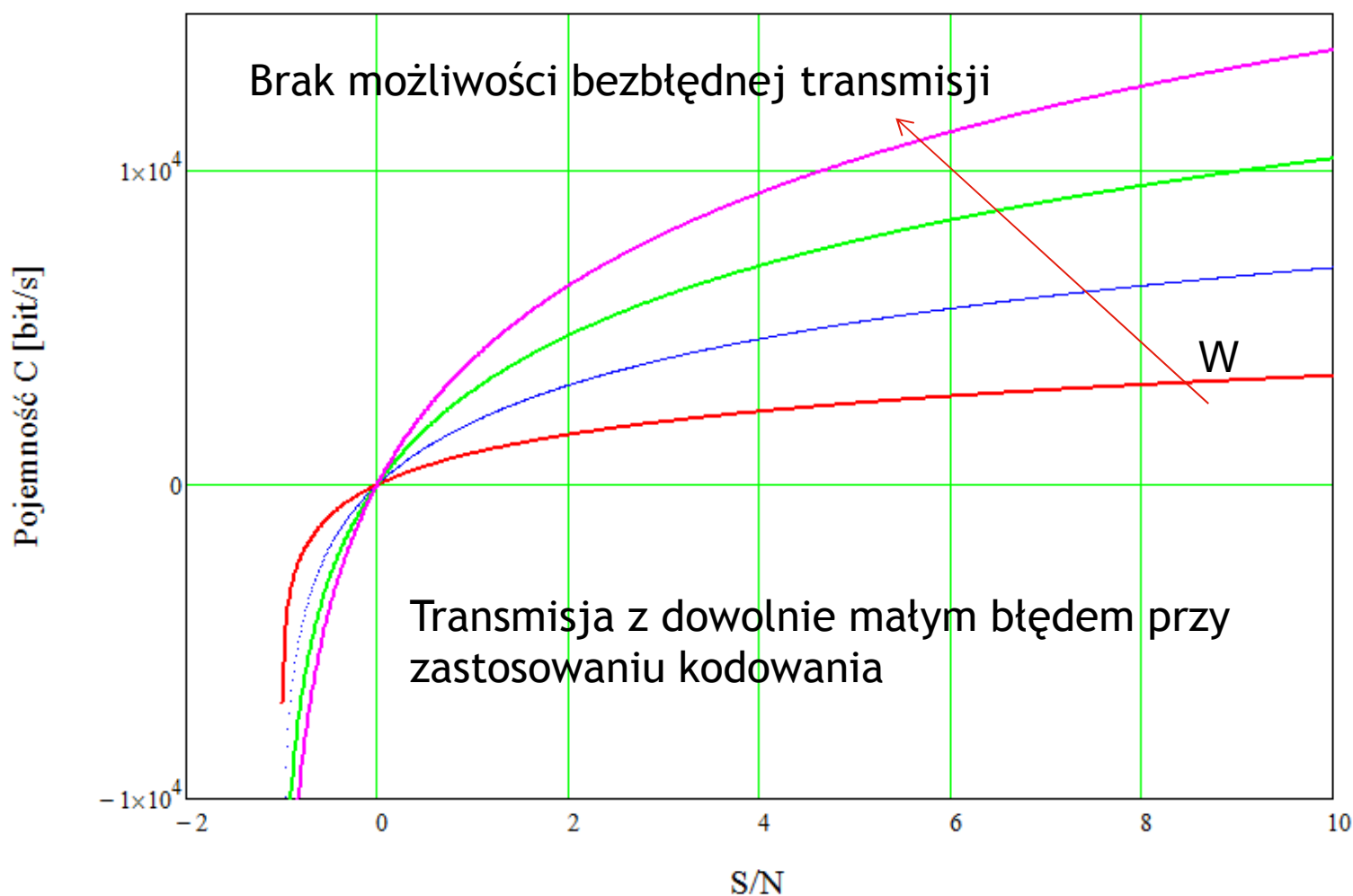
Pojemność kanału-Twierdzenia Shanona-Hartleya

$$C = W \log_2 \left(\frac{S}{N} + 1 \right)$$

gdzie:

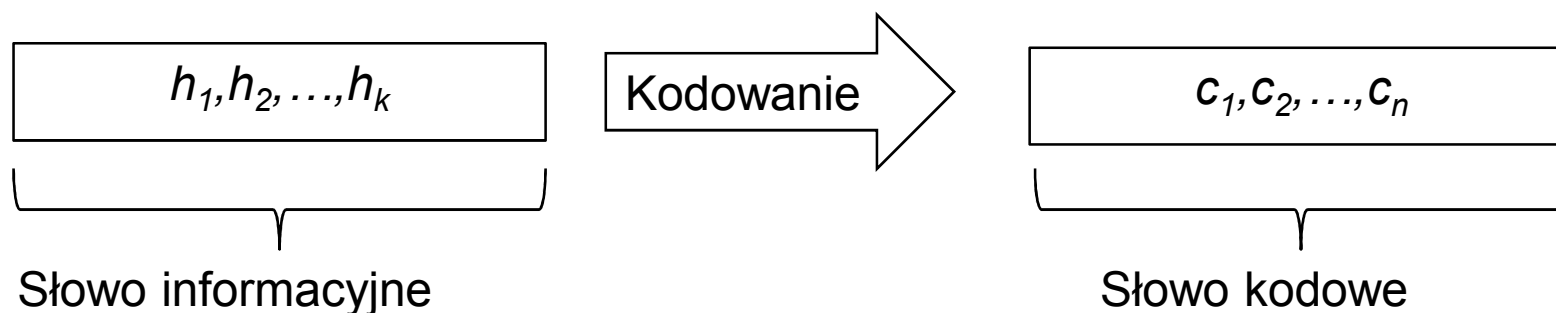
- C -pojemność kanału
- S/N -stosunek sygnał szum w kanale
- W -szerokość pasma kanału

Pojemność kanału-Twierdzenia Shanona-Hartleya



Definicja blokowego kodu liniowego

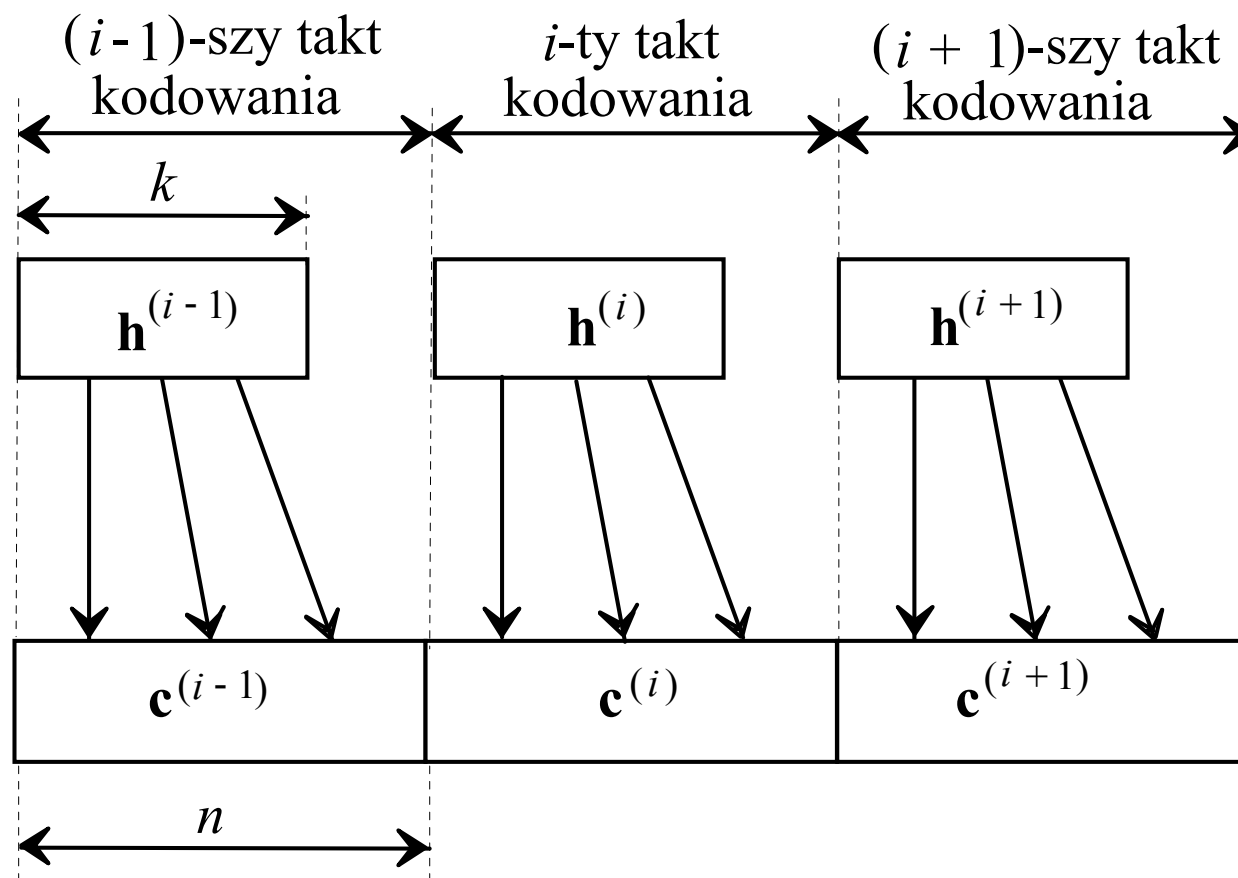
Kodowanie blokowe polega na przekształceniu k -pozycyjnych q -narnych ciągów informacyjnych $\mathbf{h}=(h_1, h_2, \dots, h_k)$ w n -pozycyjne q -narne ciągi kodowe $\mathbf{c}=(c_1, c_2, \dots, c_n)$



Formalnie proces kodowania blokowego można zapisać:

$$\bigwedge_{\mathbf{h}_i \in \{\mathbf{h}\}} \bigvee_{\mathbf{c}_i \in \{\mathbf{c}\}} f : \mathbf{h}_i \rightarrow \mathbf{c}_i \quad , \text{ przy czym } \quad f : \mathbf{h} \Leftrightarrow \mathbf{c}$$

Proces kodowania blokowego



Parametry kodu blokowego

Blokowy kod nadmiarowy oznaczamy symbolem (n, k) . Jednoznaczne określenie kodu (n, k) wymaga podania zbiorów $\{\mathbf{h}\}$ i $\{\mathbf{c}\}$ oraz funkcji f , a więc

Parametry kodu blokowego

$$(n, k) \equiv (\{\mathbf{h}\}, \{\mathbf{c}\}, f).$$

Nadmiar kodowy

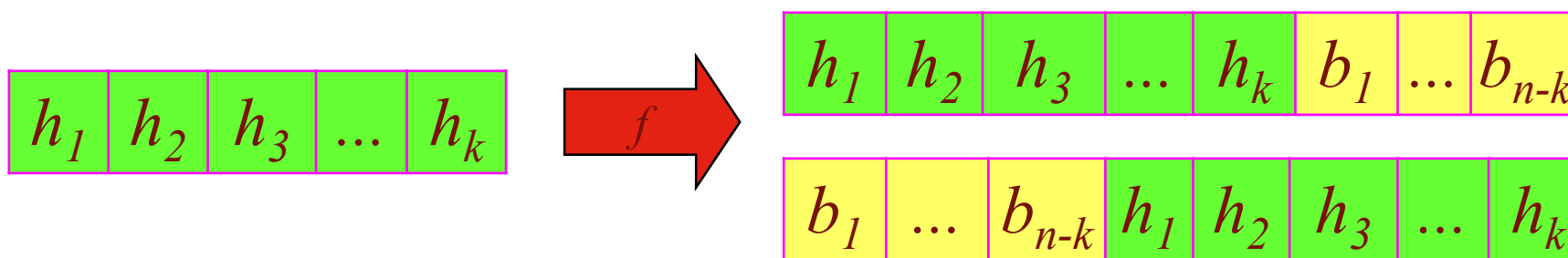
$$\rho_k = \frac{n-k}{n} = 1 - \frac{k}{n}$$

Sprawność

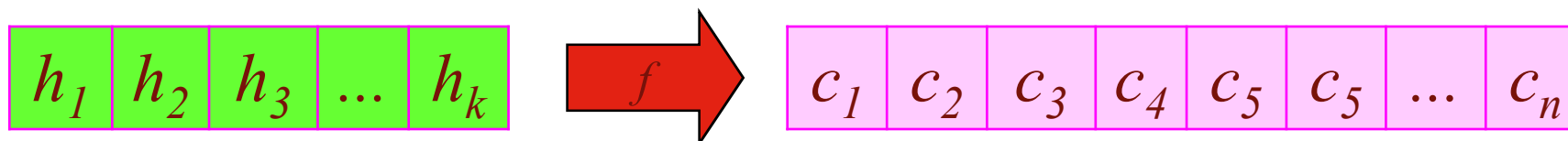
$$\eta_k = \frac{k}{n} = 1 - \rho_k$$

Podział kodów

Kod systematyczny rozdzielny



Kod niesystematyczny

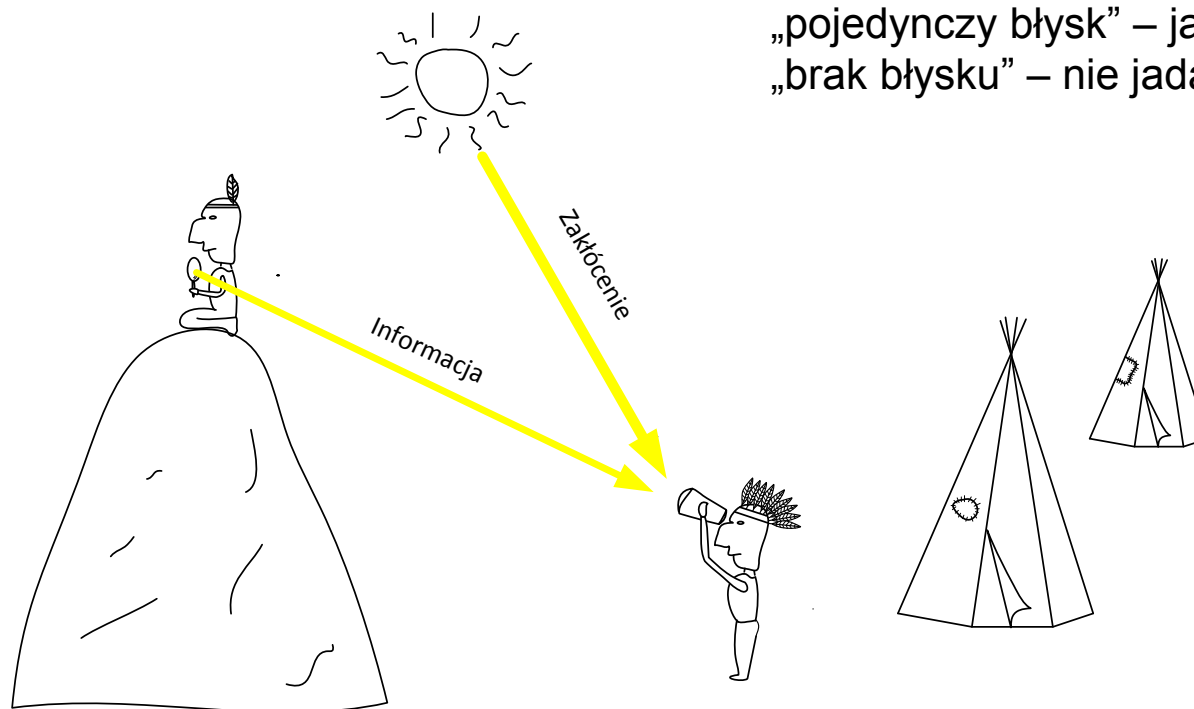


Przykład kodowania

Możliwe zdarzenia i sygnały:

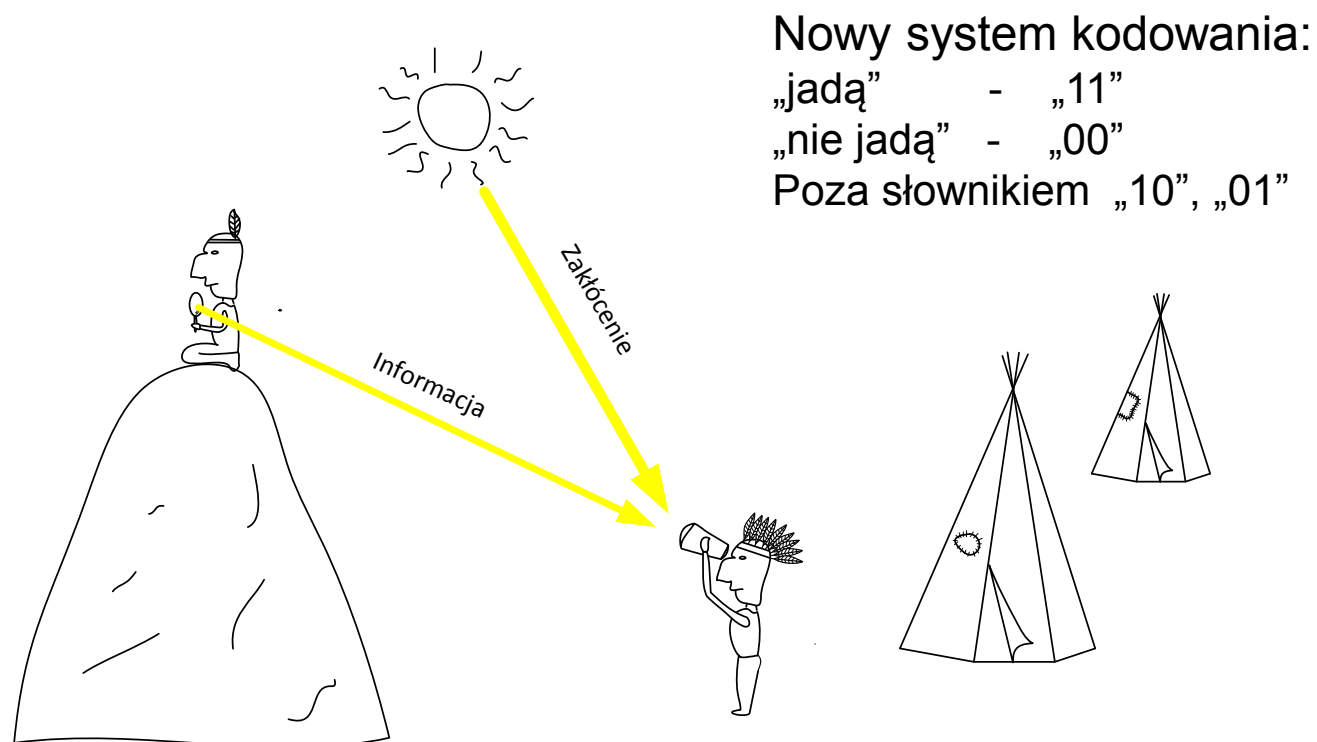
„pojedynczy błysk” – jadą „1”

„brak błysku” – nie jadą „0”



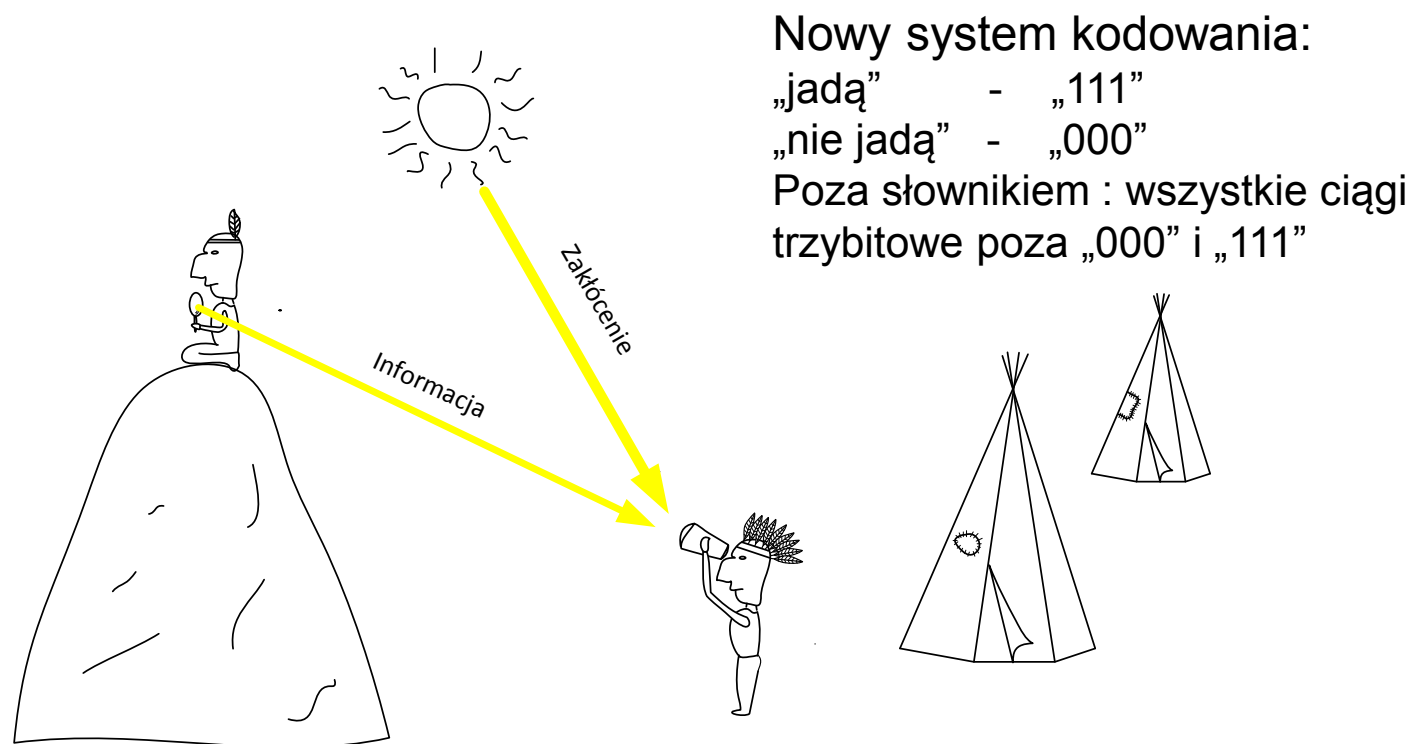
W wyniku refleksów świetlnych powodowanych przez słońce dużo fałszywych alarmów. Brak możliwości rozróżnienia alarmów fałszywych od prawdziwych

Przykład kodowania



Zmniejszyliśmy ilość fałszywych alarmów, ale nie jesteśmy w stanie ocenić, w przypadku pojedynczego błędu transmisji, jaka powinna być poprawna wiadomość, gdyż odległość błędnego słowa 01 lub 10 od poprawnego 00 lub 11 jest taka sama. Konieczne jest powtórzenie wiadomości (ARQ).

Przykład kodowania



Zmniejszyliśmy nie tylko fałszywych alarmów, ale możemy się już pokusić o wskazanie prawidłowego zdarzenia mimo przekłamanego pojedynczego bitu. Kodowanie FEC.



Jak dokładać informację nadmiarową

Zdarzenie	Słowo informacyjne	Słowo kodowe		
Zdarzenie	Symbole	N krotne powtórzenie	Dołożenie N „0”	Dołożenie N „1”
jadą	0	00000	00000	01111
nie jadą	1	11111	10000	11111



Kodowanie w życiu codziennym

- Język jakim się posługujemy to w istocie kod o zmiennej długości o dużym nadmiarze.
- Polski alfabet - 32 litery
 - a ą b c ć d e ę f g h i j k l ł m n Ń o ó p r s ś t u
w y z ż ż
- Ilość słów:
 - jednoliterowych = $32 = 32$
 - dwuliterowych = $32^2 = 1.024$
 - trzyliterowych = $32^3 = 32.768$
 - czteroliterowych = $32^4 = 1.048.576$

Po co używamy tak długich nazw jak „politechnika”

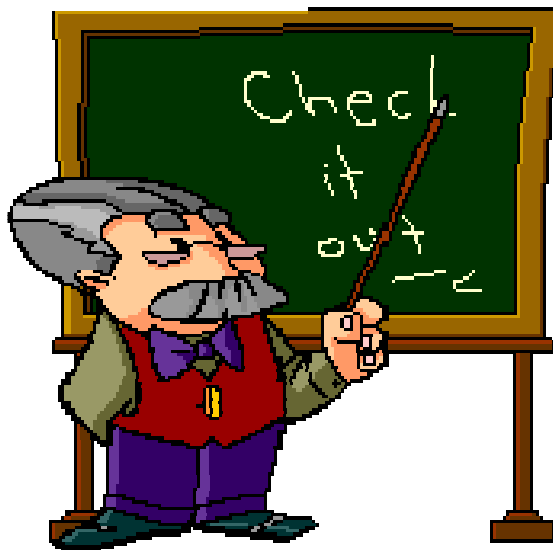
- Po co używamy tak długich nazw jak „politechnika” skoro do opisu wszystkiego wystarczyły by nam słowa o długości 4 liter

Przykład słowa w języku czteroliterowym	Przypisane znaczenie w jęz. polskim
nwjk	politechnika
mwjk	przedszkole

- Łatwo o błąd „transmisji” podczas rozmowy, gdy słowa o różnym znaczeniu różnią się na niewielkiej ilości liter.

Przykłady wyznaczania entropii

- Wyznaczanie entropii źródła informacji na temat płci
- Wyznaczanie entropii dla źródeł o różnym prawdopodobieństwie symboli
- Kompresja bezstratna



Entropia-przypomnienie

Entropia jest dana zależnością:

$$H(X) = - \sum_{i=1}^n p(X_i) \cdot \log_2 p(X_i)$$

gdzie: X_1, \dots, X_n będą wariantami treści wiadomości występującymi z prawdopodobieństwami: $p(X_1), \dots, p(X_n)$ oraz:

$$\sum_{i=1}^n p(X_i) = 1$$

Uwzględniając wszystkie wiadomości X , mamy:

$$H(X) = - \sum_X p(X) \log_2 p(X) = \sum_X p(X) \log_2 \left(\frac{1}{p(X)} \right)$$



Po co stosować koder źródłowy

- Koder źródłowy stosujemy, aby zminimalizować ilość przesyłanych bitów w kanale telekomunikacyjnym
- Przesyłanie informacji o płci kodem ASCII wymaga przesłania:
 - 7 bajtów -kobieta
 - 9 bajtów-mężczyzna
- W postaci binarnej tylko 1 bitu
 - „0”-kobieta
 - „1”-mężczyzna

Optymalne kodowanie informacji

- Optymalną ilość bitów do zakodowania zdarzenia o prawdopodobieństwie p wyraża zależność

$$\log_2\left(\frac{1}{p}\right) \text{ bitów}$$

- Zależność nie mówi nic o sposobie jej zakodowania, a tylko o ilości bitów

Kod Huffmana

- Optymalne zakodowanie zdarzeń na bitach można uzyskać za pomocą kodu Huffmana.
- Mamy zdarzenia A, B, C, D, E, F o prawdopodobieństwach:
 - $P(A)=0,4$, to $\log_2(1/0,4) = 1,32 \cong 1$
 - $P(B)=0,3$, to $\log_2(1/0,3) = 1,73 \cong 2$
 - $P(C)=0,16$, to $\log_2(1/0,16) = 2,64 \cong 3$
 - $P(D)=0,07$, to $\log_2(1/0,07) = 3,83 \cong 4$
 - $P(E)=0,036$, to $\log_2(1/0,036) = 4,79 \cong 5$
 - $P(F)=0,016$, to $\log_2(1/0,016) = 5,96 \cong 6$
 - $P(G)=0,01$, to $\log_2(1/0,01) = 6,64 \cong 7$
 - $P(H)=0,008$, to $\log_2(1/0,008) = 6.96 \cong 7$

$$H(X)=0.4*1,32+0,3*1,73+.....+0,008*6,96 \cong 2.13 \text{ bita/zd.}$$

Kod Huffmana

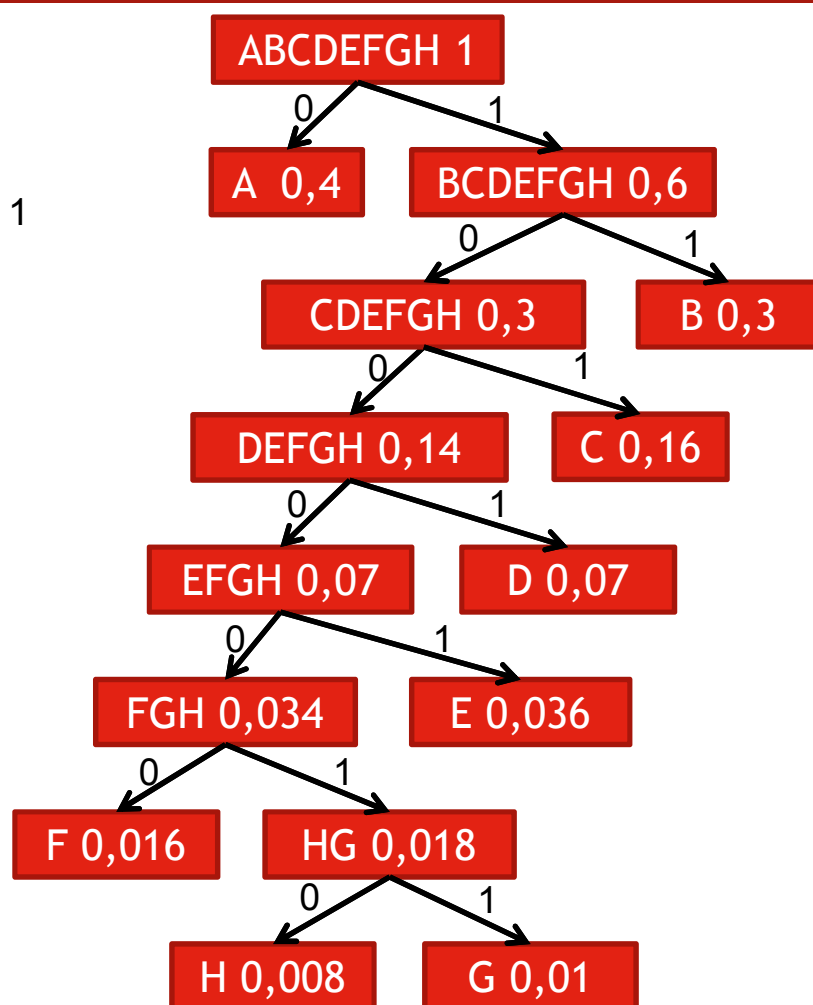
Posortuj zdarzenia od najmniejszej prawdopodobnego do najbardziej prawdopodobnego

H 0,008	G 0,01	F 0,016	E 0,036	D 0,07	C 0,16	B 0,3	A 0,4
------------	-----------	------------	------------	-----------	-----------	----------	----------

Połącz zdarzenia najmniej prawdopodobne i ponownie posortuj



Kod Huffmana



Powtarzaj operację łączenia najmniej prawdopodobnych zdarzeń i sortowanie ich układu, aż do uzyskania drzewa. Następnie lewym gałęziom przypisz „0”, a prawym „1”, lub odwrotnie. Sekwencję binarną optymalną do zakodowania zdarzenia uzyskujemy poprzez odczyt wartości ścieżek od węzła głównego do poszczególnych zdarzeń



Optymalne przyporządkowanie

Zdarzenie	Sekwencja binarna
A	0
B	11
C	101
D	1001
E	10001
F	100000
G	1000011
H	1000010

Zysk z kompresji

Założmy, że nastąpiło $N=500$ zdarzeń x_i :

1. Jeśli nie uwzględnimy statystyki występowania symboli alfabetu wtedy każdy z nich musimy zapisać na 3 bitach i objętość wiadomości wyniesie 1500bitów.
2. Jeśli uwzględnimy statystyki występowania symboli alfabetu wtedy, każdy z nich musimy zapisujemy na innej ilości bitów L , co w efekcie daje nam objętość wiadomości 1081 bitów.

Zdarzenie x_i	$p(x_i)$	$N \times p(x_i)$	L	$N \times L$
A	0,4	200	1	200
B	0,3	150	2	300
C	0,16	80	3	240
D	0,07	35	4	140
E	0,036	18	5	90
F	0,016	8	6	48
G	0,01	5	7	35
H	0,008	4	7	28
Razem	1	500	średnio 2	1081



KONIEC

Dziękuję za uwagę