

Kodowanie i kryptografia

Kody cykliczne

dr Robert Borowiec

Politechnika Wrocławska

Instytut Telekomunikacji i Akustyki

pokój 908, C-5

tel. 3203083

e-mail: robert.borowiec@ita.pwr.wroc.pl

www: lstwww.ita.pwr.wroc.pl/~RB/

Wykład V

6-godzin

Plan wykładu

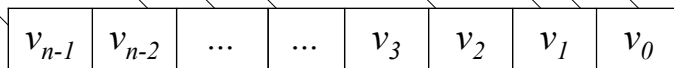
- Historia
- Przesunięcie cykliczne
- Sposoby kodowania informacji
- Tworzenie kodu
- Kody dualne
- Metryka przestrzeni
- Zdolność korekcyjna kodu
- Przykłady wybranych kodów liniowych

Wprowadzenie do kodów cyklicznych

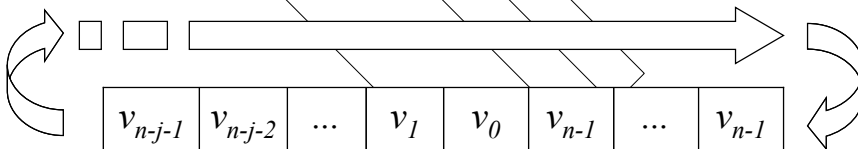
Kody cykliczne zostały wprowadzone po raz pierwszy przez Prange'a w roku 1957. Stanowią one najważniejszą klasę blokowych kodów liniowych. Wyodrębnienie ich, spośród innych kodów liniowych, wiąże się ściśle z wprowadzeniem zapisu wielomianowego ciągów oraz z zastosowaniem algebry wielomianów do analizy algorytmów kodowania i dekodowania. Definicja blokowego kodu cyklicznego jest związana z pojęciem *cyklicznego przesunięcia* ciągu.

Przesunięcie cykliczne

ciąg kodowy \mathbf{v}



$\mathbf{v}^{(j)}$ przesunięty ciąg kodowy o j pozycji w lewo



Definicja kodu cyklicznego

w oparciu o cykliczne przesunięcie

Zbiór $\{\mathbf{c}\}$ n -pozycyjnych ciągów q -narnych jest zbiorem ciągów kodowych cyklicznego kodu (n, k) , jeśli spełnione są następujące warunki:

1. zbiór $\{\mathbf{c}\}$ jest grupą abelową względem operacji dodawania n -pozycyjnych ciągów;
2. dla dowolnego $\mathbf{c} \in \{\mathbf{c}\}$ oraz $j = 1, 2, \dots, n-1$ zachodzi

$$\mathbf{c}^{(j)} \in \{\mathbf{c}\}$$

Interpretacja ciągu kodowego

Niech \mathbf{v} będzie n -pozycyjnym ciągiem kodowym

$$\mathbf{v} = (v_{n-1}, v_{n-2}, \dots, v_1, v_0)$$

Wprowadza się przekształcenie

$$F(\mathbf{v}) \equiv \sum_{i=0}^{n-1} v_i x^i$$

$$v(x) = v_{n-1}x^{n-1} + v_{n-2}x^{n-2} + \dots + v_1x^1 + v_0x^0$$



Interpretacja ciągu kodowego



Robert Borowiec

Kodowanie i kryptografia
Wykład V, strona 7/62

Operacja równoważna do przesunięcia cyklicznego

Dochodzimy do zależności

$$\frac{x^j v(x)}{x^n + 1} = q(x) + \frac{v^{(j)}(x)}{x^n + 1}$$

z której wynika, że

$$v^{(j)}(x) = R_{x^n + 1} [x^j v(x)]$$

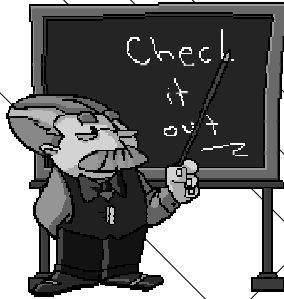
przy czym $R_{f(x)}[\bullet]$ jest resztą z podziału $[\bullet]$ przez $f(x)$ modulo $f(x)$.

Robert Borowiec

Kodowanie i kryptografia
Wykład V, strona 8/62

Przykład 3.1

Na wyznaczenie przesuniętego ciągu
kodowego



Robert Borowiec

Kodowanie i kryptografia
Wykład V, strona 9/62

Kod cykliczny

Wielomian $(x^n + 1)$ oraz jego składowe odgrywają istotną rolę w generacji kodów cyklicznych.

W algebrze wielomianów modulo wielomian $(x^n + 1)$ zbiór wielomianów $\{c(x)\}$ może stanowić zbiór ciągów kodowych, gdy dowolny wielomian $c(x) \in \{c(x)\}$ jest wielokrotnością pewnego wielomianu $g(x)$, a więc

$$c(x) = a(x) \cdot g(x)$$

i spełniony jest warunek

$$R_{g(x)}[x^n + 1] = 0$$

Robert Borowiec

Kodowanie i kryptografia
Wykład V, strona 10/62

Wielomian generujący

Zbiór $\{c(x)\}$ wielomianów stopnia nie większego niż $(n-1)$ o współczynnikach z ciała $CG(q)$ jest równoważny zbiorowi q -narnego kodu cyklicznego (n, k) , gdy dla dowolnego $c(x) \in \{c(x)\}$ zachodzi

$$R_{g(x)}[c(x)] = 0$$



$$c(x) = h(x) \cdot g(x)$$

Wielomian generujący

Wielomian $g(x)$ nazywamy *wielomianem generującym kod cykliczny*, Stopień wielomianu $g(x)$ określa liczbę pozycji kontrolnych kodu.

Właściwości wielomianu $g(x)$

$$R_{g(x)}[x^n + 1] = 0 \quad \text{wielomian } g(x) \text{ jest składową wielomianu } (x^n + 1)$$

$$\deg g(x) = r = n - k$$

Macierzowe przedstawienie kodów cyklicznych

Przyporządkujmy wielomianowi $x^{(k-1)}g(x)$ ciąg \mathbf{g} ; możemy wówczas macierz \mathbf{G} generującą kod liniowy, równoważny kodowi cyklicznemu generowanemu przez wielomian $g(x)$, zapisać w postaci

$$\mathbf{G} = \begin{bmatrix} \mathbf{g} \\ \mathbf{g}^{(-1)} \\ \vdots \\ \mathbf{g}^{(-k+2)} \\ \mathbf{g}^{(-k+1)} \end{bmatrix}$$

$\mathbf{g}^{(-j)}$ - oznacza ciąg przesunięty o j pozycji w prawo, np.:

$$\mathbf{c} = 0101100$$

$$\mathbf{c}^{(-2)} = 0001011$$

Kod dualny kodu cyklicznego

Jeśli $\{c(x)\}$ jest zbiorem wielomianów kodowych kodu cyklicznego (n,k) generowanego przez wielomian $g(x)$, a $\{v(x)\}$ jest zbiorem wielomianów kodowych dualnego kodu cyklicznego $(n,n-k)$ generowanego przez wielomian $q(x)$, to warunek ortogonalności wielomianów $c(x)$ i $v(x)$ przybiera postać

$$R_{(x^n+1)}[c(x)v(x)] = 0$$

Macierz generująca kod dualny (macierz kontrolna kodu)

Wielomian generujący cykliczny kod dualny $(n, n-k)$ określa zależność

$$q(x) = \frac{x^n + 1}{g(x)}$$

Macierz \mathbf{H} generująca kod dualny ma postać

$$\mathbf{H} = \begin{bmatrix} \mathbf{q} \\ \mathbf{q}^{(-1)} \\ \vdots \\ \mathbf{q}^{(-r+2)} \\ \mathbf{q}^{(-r+1)} \end{bmatrix},$$



$$\mathbf{q} \equiv x^{r-1} q'(x)$$

$\mathbf{q}^{(-j)}$ oznacza ciąg \mathbf{q} przesunięty o j pozycji w prawo

$$q'(x)$$

Wielomian $q(x)$ o odwróconej kolejności współczynników.

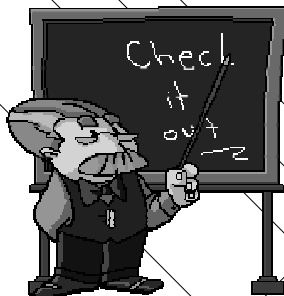
Jeżeli $q(x) = 100100$,

to $q'(x) = 001001$.



Przykład 3.2

Kod cykliczny



Macierz generująca systematyczny kod cykliczny (n, k)

$$G = \begin{bmatrix} \mathbf{u}_{n-1} \\ \mathbf{u}_{n-2} \\ \vdots \\ \mathbf{u}_{n-k+1} \end{bmatrix} \quad \leftarrow \quad \mathbf{u}_i = R_{g(x)}[x^i]$$

Przykład:

Dla kodu cyklicznego $(7,4)$ generowanego przez wielomian $g(x) = x^3 + x + 1$ mamy

$$\mathbf{u}_{n-1} = \mathbf{u}_6 \Leftrightarrow R_{g(x)}[x^6] = x^2 + 1 \Leftrightarrow 101,$$

$$\mathbf{u}_{n-2} = \mathbf{u}_5 \Leftrightarrow R_{g(x)}[x^5] = x^2 + x + 1 \Leftrightarrow 111,$$

$$\mathbf{u}_{n-3} = \mathbf{u}_4 \Leftrightarrow R_{g(x)}[x^4] = x^2 + x \Leftrightarrow 110,$$

$$\mathbf{u}_{n-4} = \mathbf{u}_3 \Leftrightarrow R_{g(x)}[x^3] = x + 1 \Leftrightarrow 011.$$



Skrócony kod cykliczny

Kody cykliczne istnieją tylko dla niektórych wartości n , na przykład:

$$n = p^m - 1$$

$$n = p^{2m} + p^m + 1$$

przy czym p jest liczbą pierwszą, a m - liczbą naturalną



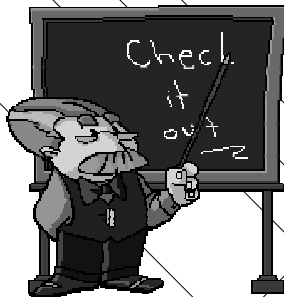
Skrócony kod cykliczny (kod pseudocykliczny)

Procedura skracania kodu (n, k) do kodu (n', k') , gdzie $n > n'$:

1. Znajdujemy kod o długości ciągów najbliższej naszego projektowanego kodu.
2. Ze zbioru ciągów kodowych wybieramy ciągi, które na pierwszych $n - n'$ pozycjach mają zera.
3. Z wybranych ciągów usuwamy $n - n'$ pierwszych zer
4. Wybrane i skrócone ciągi tworzą nowy zbiór ciągów kodowych $\{c'(x)\}$



Przykład 3.3 Skrócony kod cykliczny



Skrócony kod cykliczny (właściwości)

1. W skróconych kodach cyklicznych nie jest spełniony warunek, że dla dowolnego $\mathbf{c} \in \{\mathbf{c}\}$ oraz $j = 1, 2, \dots, n' - 1$ zachodzi
$$\mathbf{c}^{(j)} \in \{\mathbf{c}\}$$
2. Oznaczenie kodu skróconego ma postać $[n', k - (n - n')]$
3. Jeżeli wyjściowy kod (n, k) ma odległość d_{min} , to odległość minimalna d'_{min} kodu skróconego ma odległość nie mniejszą niż d_{min} .

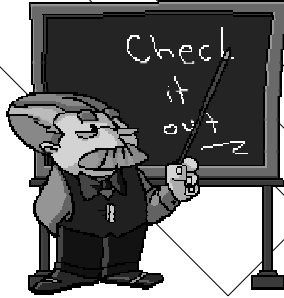
Kodowanie za pomocą kodów cyklicznych

1. Prosta reguła kodowania daje w wyniku kod niesystematyczny
Jeżeli $h(x)$ jest wielomianem informacyjnym, a $g(x)$ jest wielomianem generującym kod, to wielomian kodowy jest równy
$$c(x) = h(x) \cdot g(x)$$
2. Uzyskanie systematycznego kodu cyklicznego zapewnia następująca reguła kodowania

$$c(x) = x^r h(x) - R_{g(z)}[x^r h(x)]$$

Przykład 3.11

Przykład wyznaczenia ciągu kodowego systematycznego



Robert Borowiec

Kodowanie i kryptografia
Wykład V, strona 23/62

Przykład 3.11

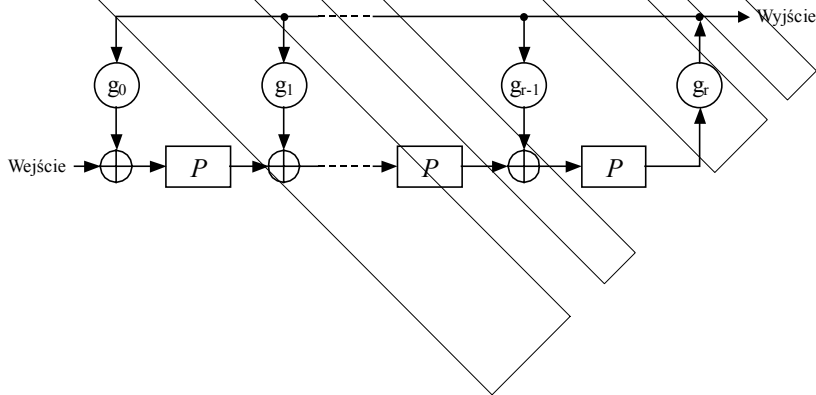
$$\begin{array}{l}
 \begin{array}{c}
 x^9 + x^5 + x^2 + 1 \\
 h(x) \quad \boxed{1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1}
 \end{array} \\
 \begin{array}{c}
 x^5 h(x) \quad \boxed{1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0} \\
 x^{14} + x^{10} + x^7 + x^5
 \end{array} \\
 \begin{array}{c}
 c(x) \quad \boxed{1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1} \\
 x^{14} + x^{10} + x^7 + x^5 + x + 1 \\
 \underbrace{\hspace{10em}}_{x^5 h(x)} \quad \underbrace{\hspace{10em}}_{R_{g(x)}[x^5 h(x)]}
 \end{array}
 \end{array}$$

Robert Borowiec

Kodowanie i kryptografia
Wykład V, strona 24/62

Dzielenie wielomianów

Układ od dzielenia dowolnego wielomianu przez wielomian $g(x) = g_r x^r + g_{r-1} x^{r-1} + \dots + g_1 x + g_0$



Robert Borowiec

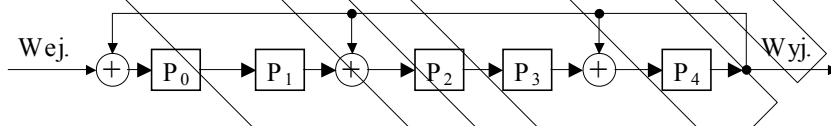
Kodowanie i kryptografia
Wykład V, strona 25/62

Przykład dzielenia wielomianów

Układ od dzielenia wielomianu $h(x)$ przez wielomian $g(x)$

$$h(x) = x^9 + x^5 + x^2 + 1$$

$$g(x) = x^5 + x^4 + x^2 + 1$$



Zasadnicze dzielenie w tym wypadku odbywa się po 5 taktach (po dojściu bitu informacji do pętli sprzężenia), gdyż wcześniej informacja jest wpisywana do rejestrów. W istocie sam proces dzielenia odbywa się na wielomianie:

$$x^5 \cdot h(x) = x^{14} + x^{10} + x^7 + x^5$$

Robert Borowiec

Kodowanie i kryptografia
Wykład V, strona 26/62

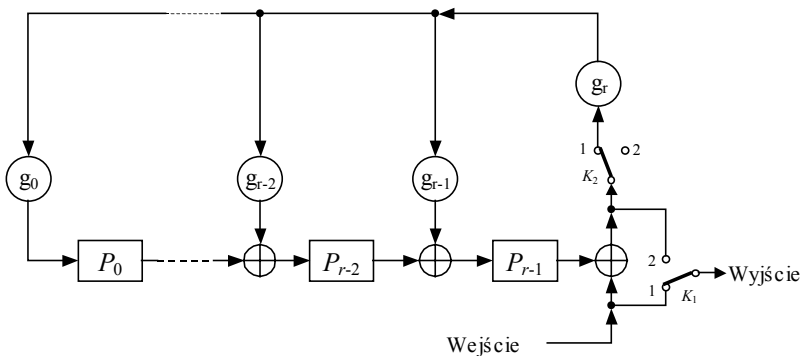
Przykład dzielenia wielomianów

Takt	Wejście	Zawartość rejestru					Wyjście	Wielomian
		P_0	P_1	P_2	P_3	P_4		
1	1	0	0	0	0	0	0	x^{14}
2	0	1	0	0	0	0	0	x^{13}
3	0	0	1	0	0	0	0	x^{12}
4	0	0	0	1	0	0	0	x^{11}
5	1	0	0	0	1	0	0	x^{10}
6	0	1	0	0	0	1	1	x^9
7	0	1	1	1	0	1	1	x^8
8	1	1	1	0	1	1	1	x^7
9	0	0	1	0	0	0	0	x^6
10	1	0	0	1	0	0	0	x^5
11	0	1	0	0	1	0	0	x^4
12	0	0	1	0	0	1	1	x^3
13	0	1	0	0	0	1	1	x^2
14	0	1	1	1	0	1	1	x^1
15	0	1	1	0	1	1	1	x^0
Reszta		1	1	0	0	0		
Wielomian		x^0	x^1	x^2	x^3	x^4		

Robert Borowiec

Kodowanie i kryptografia
Wykład V, strona 27/62

Schemat ogólny kodera cyklicznego



Robert Borowiec

Kodowanie i kryptografia
Wykład V, strona 28/62

Schemat kodera systematycznego (15,10)

<http://www.ee.uwa.edu.au/~roberto/teach/itc314/java/CRC/crc.html>

lub z dyskiety [Koder cykliczny\Koder cykliczny.htm](#)

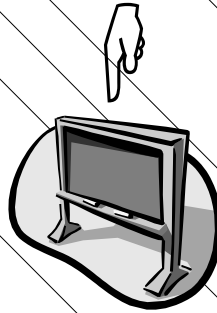
Dekodowanie kodów cyklicznych

- Metody detekcji błędów
 - wyznaczenie syndromu $S(y)$ za pomocą macierzy H^T
 - wyznaczenie reszty z dzielenia

$$r(x) = R_{g(x)}[y(x)]$$

- dla $r \neq 0 \Rightarrow$ wektor y nie jest wektorem kodowym -
nastąpił błąd transmisji!
- Wybrane metody korekcji błędów w kodach cyklicznych
 - tablica dekodowania
 - polowanie na błędy

Metoda polowania na błędy Wprowadzenie



Robert Borowiec

Kodowanie i kryptografia
Wykład V, strona 31/62

Metoda polowania na błędy

- Wyznaczamy resztę z dzielenia

$$r(x) = R_{g(x)}[y(x)] \Rightarrow \mathbf{r}$$

- Obliczamy wagę Hamminga wektora \mathbf{r}

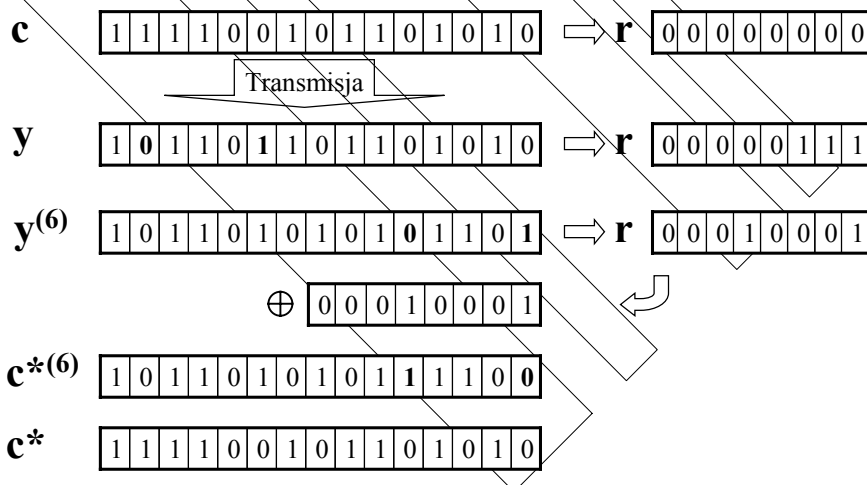
- jeżeli $w_H(\mathbf{r}) > t$, to ilość błędów jest większa niż zdolność korekcyjna lub błędy nie leżą w obszarze bitów parzystości
- jeżeli $w_H(\mathbf{r}) \leq t$, to błąd można skorygować-błędy leżą w obszarze bitów parzystości, a ich ilość jest mniejsza od zdolności korekcyjnej kodu

Robert Borowiec

Kodowanie i kryptografia
Wykład V, strona 32/62

Metoda polowania na błędy

na przykładzie kodu BCH(15, 7, 2)



Robert Borowiec

Kodowanie i kryptografia
Wykład V, strona 33/62

Przykład cd..

- Parametry kodu BCH (15, 7, 2), to $n=15, k=7, t=2$
- Wielomian generujący kod BCH (15, 7, 2)
$$g(x) = x^8 + x^7 + x^6 + x^4 + 1.$$
- Dekoder z sieci lub z dyskietki

Robert Borowiec

Kodowanie i kryptografia
Wykład V, strona 34/62

Przegląd kodów cyklicznych

- Kody BCH
 - Binarne kody BCH
 - Niebinarne kody BCH
 - Wielowartościowe kody BCH
 - Kody BCH generowane przez elementy niepierwotne rozszerzonego ciała Galois'a
- Kody HAMMINGA
- Kody REEDA-SOLOMONA
- Kody FIRE'A

Robert Borowiec

Kodowanie i kryptografia
Wykład V, strona 35/62

KODY CYKLICZNE

- Wielomian generujący kod cykliczny (n, k) o długości $n = p^m - 1$ można przedstawić w postaci iloczynu pewnych wielomianów pierwszych stopnia nie większego niż m

$$g(x) = \mu_1(x) \cdot \mu_2(x) \cdot \dots$$

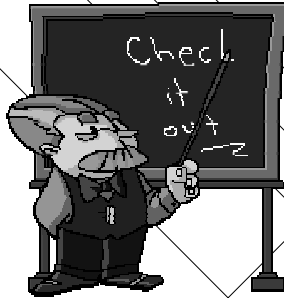
Robert Borowiec



Kodowanie i kryptografia
Wykład V, strona 36/62

Przykład 3.4

Związek między ciałem Galoisa, a
pierwiastkami wielomianu
generującego



Robert Borowiec

Kodowanie i kryptografia
Wykład V, strona 37/62

Przykład 3.4 cd..

Reprezentacja ciała $CG(2^3)$ generowanego przez
wielomian pierwotny $p(x) = x^3 + x + 1$

Element ciała	Reprezentacja potęgowa	Reprezentacja wielomianowa	Reprezentacja binarna
a_1	α	x	010
a_2	α^2	x^2	100
a_3	α^3	$x + 1$	011
a_4	α^4	$x^2 + x$	110
a_5	α^5	$x^2 + x + 1$	111
a_6	α^6	$x^2 + 1$	101
a_7	$\alpha^7 = \alpha^0 = 1$	1	001
a_8	nie istnieje	0	000

Robert Borowiec

Kodowanie i kryptografia
Wykład V, strona 38/62

Definicja kodu BCH

Niech $\{c(x)\}$ stanowi zbiór wielomianów stopnia nie większego niż $n - 1$ o współczynnikach z ciała podstawowego $CG(p)$ oraz niech m, m_0 i d będą liczbami naturalnymi, takimi że:

$$0 \leq m_0 \leq p^m - 1, \quad d \leq p^m - 1$$

Jeśli wielomian $c(x) \in \{c(x)\}$ ma jako kolejne pierwiastki $d - 1$ elementów ciała $CG(p^m)$: $\alpha^{m_0}, \alpha^{m_0+1}, \dots, \alpha^{m_0+d-2}$, to zbiór $\{c(x)\}$ jest zbiorem wielomianów kodowych p -narnego kodu BCH, którego odległość minimalna

$$d_{\min} = d$$

Konstruowanie wielomianu generującego kodu BCH

Wielomian generujący kod BCH jest najmniejszą wspólną wielokrotnością (NWW) wielomianów minimalnych tych elementów ciała $CG(p^m)$, które stanowią jego pierwiastki. Jeśli więc przez $\psi_i(x)$ oznaczmy wielomian minimalny i -tego elementu α_i ciała $CG(p^m)$, to

$$g(x) = \text{NWW}[\psi_{m_0}(x), \psi_{m_0+1}(x), \dots, \psi_{m_0+d-2}(x)]$$

Dla przypomnienia elementy α_i ciała $CG(p^m)$ powstają poprzez podniesienie do potęgi i -tej elementu pierwotnego α , tak więc $\alpha_i = \alpha^i$.

Wielomiany minimalne-przypomnienie

Wielomiany minimalne elementów α^i ciała wyznacza się z zależności

$$\psi_i(x) = \begin{cases} x-1 & \text{dla } i=0, \\ p(x) & \text{dla } i=1, \\ \prod_{j=0}^{\lambda_i-1} (x - (\alpha^i)^{p^j}) & \text{dla } i > 1. \end{cases}$$

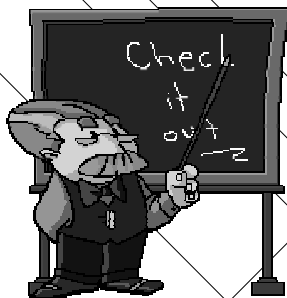
$p(x)$ wielomian pierwotny generujący ciało $CG(p^m)$,

α element pierwotny ciała $CG(p^m)$,

λ_i rząd i -tego elementu ciała $CG(p^m)$.

Przykład 3.6

Wielomiany minimalne
ciała $CG(2^3)$



Przykład 3.6

Wielomiany minimalne ciała $CG(2^3)$

Element ciała	Wielomian minimalny
α^0	$x + 1$
$\alpha^1, \alpha^2, \alpha^4$	$x^3 + x + 1$
$\alpha^3, \alpha^5, \alpha^6$	$x^3 + x^2 + 1$

Binarne kody BCH

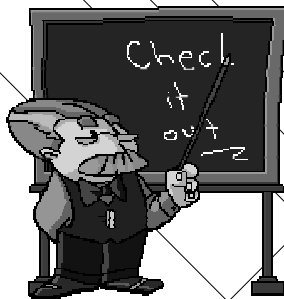
konstrukcja kodu (n, k, t)

1. Symbole są określone w ciele pierwotnym $CG(2)$.
2. Liczba bitów $n=(2^m-1)$ określa ciało rozszerzone $CG(2^m)$, z którego będą pochodziły wielomiany minimalne.
3. Wybieramy m_0 .
4. Jeśli $m_0=1$, to d jest nieparzyste i wynosi $d=d_{min}=2 \cdot t+1$, gdy $m_0=0$, to d jest parzyste.
5. Pamiętamy, że $0 \leq m_0 \leq p^m - 1$, $d \leq p^m - 1$
6. Wyznaczamy wielomian $g(x)$ i odczytujemy jego stopień r
7. Wyznaczamy długość ciągów informacyjnych $k=(n-r)$



Przykład 3.7

Wielomian generujący kod
BCH (15, 7, 2)



Robert Borowiec

Kodowanie i kryptografia
Wykład V, strona 45/62

Przykład 3.7

Tablica 9. Wielomiany minimalne elementów ciała $CG(2^4)$

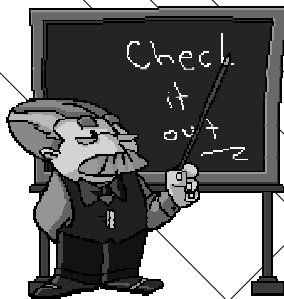
Pierwiastki sprzężone	Wielomian minimalny
0	x
α^0	$x+1$
$\alpha^1, \alpha^2, \alpha^4, \alpha^8$	x^4+x+1
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$	$x^4+x^3+x^2+x+1$
α^5, α^{10}	x^2+x+1
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	x^4+x^3+1

Robert Borowiec

Kodowanie i kryptografia
Wykład V, strona 46/62

Przykład 3.8

Wielomian generujący kod BCH (15, 5, 3)



Robert Borowiec

Kodowanie i kryptografia
Wykład V, strona 47/62

Kody Hamminga

Kod cykliczny nazywamy kodem Hamminga, jeżeli jego wielomian generujący jest wielomianem pierwotnym ciała $CG(p^m)$

$$g(x) = p(x)$$

Cykliczny kod Hamminga generowany przez wielomian stopnia m ma następujące parametry

$$n = 2^m - 1$$

$$d = d_{\min} = 3$$

$$k = 2^m - m - 1$$

$$t = 1$$

Robert Borowiec



Kodowanie i kryptografia
Wykład V, strona 48/62

Niebinarne kody BCH

W przypadku niebinarnych kodów BCH symbole pochodzą z ciała $CG(p)$, przy czym $p > 2$. Współczynniki wielomianu generującego kod są również niebinarne i są elementami ciała $CG(p)$. Długość bloku wynosi

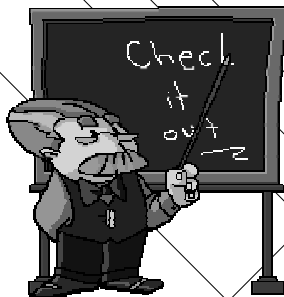
$$n = p^m - 1 \text{ [symboli]}$$

Wielomian generujący kod jest określony nad ciałem $CG(p)$ i ma pierwiastki w ciele rozszerzonym $CG(p^m)$.

W istocie sposób tworzenia jest taki sam jak kodu binarnego BCH. Należy jednak zwrócić uwagę, że operacje na współczynnikach odbywają się modulo p , a nie modulo 2.

Przykład 3.9

Niebinarny kod BCH (8, 2, 2)



Przykład 3.9

Reprezentacja ciała $\mathbb{CG}(3^2)$ generowanego przez wielomian

$$p(x) = x^2 + x + 2$$

Element ciała	Reprezentacja potęgowa	Reprezentacja wielomianowa	Reprez. tetrarna	Wielomiany minimalne
a_1	α	x	10	$\psi_1(x) = x^2 + x + 2 = p(x)$
a_2	α^2	$2x + 1$	21	$\psi_2(x) = (x - \alpha^2)(x - \alpha^6) = x^2 + 1$
a_3	α^3	$2x + 2$	22	$\psi_3(x) = \psi_1(x)$
a_4	α^4	2	02	$\psi_4(x) = x - \alpha^4 = x + 1$
a_5	α^5	$2x$	20	$\psi_5(x) = (x - \alpha^5)(x - \alpha^7) = x^2 + 2x + 2$
a_6	α^6	$x + 2$	12	$\psi_6(x) = \psi_2(x)$
a_7	α^7	$x + 1$	11	$\psi_7(x) = \psi_1(x)$
a_8	$\alpha^8 = \alpha^0 = 1$	1	01	$\psi_8(x) = \psi_0(x) = x - 1 = x + 2.$
a_9	nie istnieje		00	

Robert Borowiec

Kodowanie i kryptografia
Wykład V, strona 51/62

Przykład 3.9

Macierz kontrolna i generująca BCH (8,2,2,)

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 1 & 1 & 2 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 & 0 & 2 & 2 & 1 \end{bmatrix} = [\mathbf{I}_2 \mathbf{P}_{2,6}]$$

$$\mathbf{H} = [\mathbf{P}_{2,6}^T \mathbf{I}_6] = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 1 & 0 & 0 \\ 2 & 2 & 0 & 0 & 0 & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Robert Borowiec

Kodowanie i kryptografia
Wykład V, strona 52/62

Przykład 3.9

Macierz kontrolna i generująca BCH (8, 2, 2)

Ciagi informacyjne	Ciagi kodowe BCH (8, 2, 2)
0 0	0 0 0 0 0 0 0 0
1 0	1 0 1 1 2 0 2 2
0 1	0 1 1 2 0 2 2 1
2 0	2 0 2 2 1 0 1 1
0 2	0 2 2 1 0 1 1 2
2 1	2 1 0 1 1 2 0 2
2 2	2 2 1 0 1 1 2 0
1 2	1 2 0 2 2 1 0 1
1 1	1 1 2 0 2 2 1 0



Wielowartościowe kody BCH definicja

Niech $\{c(x)\}$ stanowi zbiór wielomianów stopnia nie większego niż $n - 1$ o współczynnikach z ciała oraz niech: m , d i m_0 będą pewnymi liczbami naturalnymi, takimi że:

$$0 \leq m_0 \leq q^m - 1$$

$$q = p^c$$

$$d \leq q^m - 1$$

c - liczba naturalna;

Jeśli dowolny wielomian $c(x) \in \{c(x)\}$ ma jako pierwiastki kolejne $d - 1$ elementów ciała: $\alpha^{m_0}, \alpha^{m_0+1}, \dots, \alpha^{m_0+d-2}$, to zbiór $\{c(x)\}$ jest zbiorem wielomianów kodowych q -narnego kodu BCH o długości $n = q^m - 1$.



Wielowartościowe kody BCH definicja

Przedstawiona definicja wielowartościowego kodu BCH różni się od podanej definicji p -narnego kodu BCH tylko różnym sposobem zdefiniowania elementu pierwotnego α , który jest bądź elementem pierwotnym ciała $CG(p^m)$, bądź ciała $CG(q^m)$. Wspólną definicję p -narnych i q -narnych kodów BCH można więc przedstawić w postaci układu $d - 1$ równań liniowych

$$\sum_{i=0}^{n-1} c_i \alpha^{li} = 0, \quad m_0 \leq l \leq m_0 + d - 2$$

Przykład 3.10

Wielomiany minimalne elementów ciała $CG(16)$

Pierwiastki sprzężone	Wielomiany minimalne			
0	x			
α^0	x	+		1
α^1, α^4	x^2	+	x	2
α^2, α^8	x^2	+	x	3
α^3, α^{12}	x^2	+	$3x$	1
α^5	x	+		2
α^6, α^9	x^2	+	$2x$	1
α^7, α^{13}	x^2	+	$2x$	2
α^{10}	x	+		3
α^{11}, α^{14}	x^2	+	$3x$	3



Realizacja kodów wielowartościowych

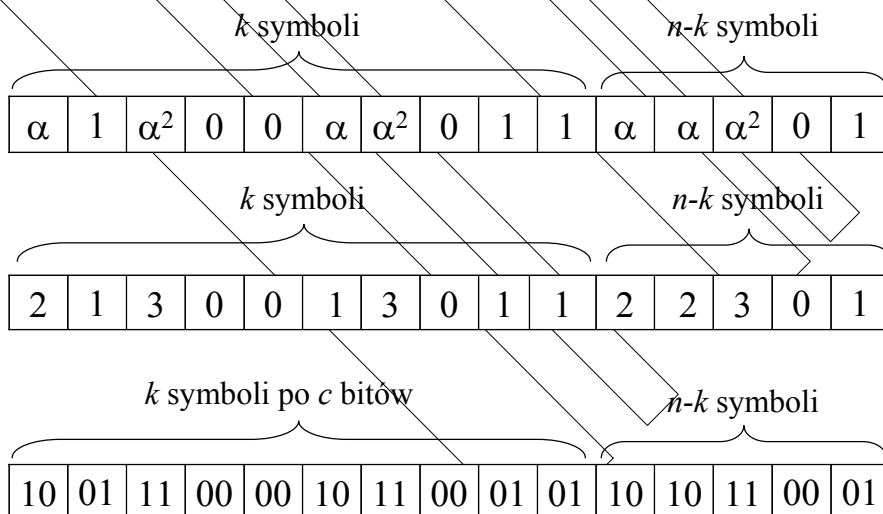
Elementy ciała rozszerzonego mają postać potęg elementu pierwotnego i w tej postaci nie nadają się do transmisji przez kanał telekomunikacyjny. Aby to zapewnić należy przyjąć odwzorowanie zbioru elementów ciała $CG(q)$ na q -elementowy zbiór liczb całkowitych dodatnich:

$$\sigma : \{0, 1, \alpha, \alpha^2, \dots, \alpha^{q-2}\} \rightarrow \{0, 1, 2, 3, \dots, q-1\}$$

$$\sigma(\alpha^x) = \begin{cases} x+1 & \text{dla } \alpha^x \neq 0 \\ 0 & \text{dla } \alpha^x = 0 \end{cases}$$



Wielowartościowe kody BCH ..



Kody BCH generowane przez elementy niepierwotne rozszerzonego ciała Galois

Kody te, zwane *kodami BCH generowanymi przez niepierwotne elementy rozszerzonego ciała Galois*, są zdefiniowane równaniami:

$$\sum_{i=0}^{\lambda_j-1} c_i \alpha_j^{li}, \quad m_0 \leq l \leq m_0 + d - 2,$$

przy czym:

$\alpha_j = \alpha^j$ - niepierwotny element ciała rozszerzonego,
 λ_j - rząd elementu .

Kody Reeda-Solomona cd..

Kody Reeda-Solomona stanowią szczególny przypadek niebinarnych kodów BCH. Definicję kodu Reeda-Solomona (RS), generowanego przez element α^j ciała $CG(q)$ możemy sprowadzić do równań o postaci

$$\sum_{i=0}^{n-1} c_i \alpha_j^{li} = 0, \quad m_0 \leq l \leq m_0 + d_{\min} - 2$$

przy czym d_{\min} jest odległością minimalną kodu, a n - długością ciągów kodowych.

Wartość n określa zależność:

$$n = \frac{q-1}{\text{NWP}(q-1, j)}$$

Kody Reeda-Solomona cd..

Kod RS przystosowany do korekcji t błędów ma następujące parametry:

Długość bloku: $n = 2^m - 1 [\text{syboli}] = m(2^m - 1) [\text{bitów}]$

Długość wiadomości: $k [\text{syboli}] = mk [\text{bitów}]$

Liczba symboli kontrolnych: $r [\text{syboli}] = n - k [\text{syboli}]$

Minimalna odległość $d [\text{syboli}] = 2t + 1$

Kody Fire'a

Kod Fire'a jest to kod cykliczny generowany przez wielomian o postaci:

$$g(x) = (x^c + 1)p(x)$$

przy czym $p(x)$ jest wielomianem pierwotnym stopnia m , a c - liczbą naturalną nie podzielną przez rząd λ pierwiastków rozkładu wielomianu $p(x)$ w ciele $CG(2^m)$.

Kody Fire'a

Parametry kodu Fire'a:

-długość ciągu kodowego $n = NWW(\lambda, c)$

-ilość pozycji informacyjnych $k = n - m - c$

Kod Fire'a jest typowym kodem zabezpieczającym przed błędami seryjnymi o następujących właściwościach detekcyjno-korekcyjnych:

- wykrywa wszystkie pojedyncze serie błędów o długości nie większej niż $m + c$
- wykrywa dwie serie błędów o długościach l_1 i l_2 , spełniających warunki:
 $l_1 \leq l_2, l_1 \leq m, l_1 + l_2 \leq c + 1$; koryguje krótszą z tych serii.