Wykład 7.

7.1 Kody dualne do cyklicznych

Przypuśćmy, że mamy dany cykliczny kod $K \subseteq F^n[x]$. Będziemy szukać kodu $K^\perp$ dualnego do K.

Zauważmy, że jeżeli $p(x) = a_0 + a_1 \cdot x + \ldots + a_n \cdot x^n$, to wielomian

$$p_n^R(x) = a_n + a_{n-1} \cdot x + \ldots + a_0 \cdot x^n$$

spełnia równość

$$p_n^R(x) = x^n \cdot p(\frac{1}{x}).$$

Dodatkowo, jeżeli wektor $\vec{w} = (a_0, \ldots, a_n)$, to symbolem $\vec{w}^R$ oznaczamy wektor $(a_n, \ldots, a_0)$.

Iloczyn skalarny wektorów $(a_0, \ldots, a_n)$ i $(b_0, \ldots, b_n)$ można obliczyć stosując następujący, zawiły algorytm:

1. najpierw odwracamy wektor $(b_0, \ldots, b_n)$,
2. tworzymy wielomiany o współczynnikach $(a_0, \ldots, a_n)$ i $(b_n, \ldots, b_0)$, a więc wielomiany $p(x) = a_0 + a_1 \cdot x + \ldots + a_n \cdot x^n$ oraz $q(x) = b_n + b_{n-1} \cdot x + \ldots + b_0 \cdot x^n$
3. znajdujemy iloczyn wielomianów p i q, a właściwie współczynnik tego iloczynu przy potędze x^n. Współczynnik ten jest równy iloczynowi skalarnemu $\sum_{i=0}^n a_i \cdot b_i$.

Poprawność tego sposobu liczenia iloczynu skalarnego wynika bezpośrednio z definicji iloczynu wielomianów.

Twierdzenie 7.1 *Przypuśćmy, że mamy dany cykliczny kod $K \subseteq F^n[x]$ i jego generator g stopnia k. Niech h będzie wielomianem takim, że $g(x) \cdot h(x) = x^{n+1} - 1$. Przestrzeń $K^\perp$ dualna (ortogonalna) do K jest kodem cyklicznym generowanym przez wielomian*

$$\pm h_{n+1-k}^R(x) = \pm x^{n+1-k} \cdot h(\frac{1}{x}).$$

Dowód. Przestrzeń K jest generowana przez wektory współczynników wielomianów $g(x)$, $x \cdot g(x)$, $\ldots$, $x^{n-k} \cdot g(x)$. Najpierw udowodnimy, że do przestrzeni $K^\perp$ należą odwrócone wektory współczynników wielomianów $h(x)$, $x \cdot h(x)$, $\ldots$, $x^{k-1} \cdot h(x)$.

Dla ustalonego $i < k$ niech $\vec{w}$ będzie wektorem współczynników wielomianu $x^i \cdot h(x)$. Będziemy dowodzić, że wektor $\vec{w}^R$ należą do $K^\perp$. Aby to dowieść, wystarczy dla dowolnego $j \leqslant n - k$ obliczyć iloczyn skalarny wektora $\vec{u}$ współczynników wielomianu $x^j \cdot g(x)$ oraz wektora $\vec{w}^R$ i sprawdzić, że iloczyn ten jest równy 0.

Interesujące nas iloczyn skalarny obliczamy w wyżej podany sposób. Tak więc, najpierw odwracamy wektor $\vec{w}^R$. Otrzymujemy w ten sposób wektor $\vec{w}$. Teraz tworzymy wielomiany o współczynnikach $\vec{u}$ i $\vec{w}$. Otrzymujemy więc wielomiany $x^j \cdot g(x)$ i $x^i \cdot h(x)$. Po wymnożeniu tych wielomianów otrzymujemy wielomian $x^{j+i} \cdot g(x) \cdot h(x) = x^{j+i} \cdot (x^{n+1} - 1)$. Współczynnik przy potędze x^n tego wielomianu jest współczynnikiem przy potędze x^{n-i-j} wielomianu $x^{n+1} - 1$.

Zauważmy, że $0 \leqslant i < k$ i $0 \leqslant j \leqslant n-k$. Tak więc $0 \leqslant i+j < n$ i ostatecznie $0 < n-i-j \leqslant n$. Jest oczywiste, że współczynnik wielomianu $x^{n+1}-1$ przy potędze x^{n-i-j} takiej, że $0 < n-i-j \leqslant n$ jest równy 0.

Jeżeli $p(x) = x^i \cdot h(x)$, to

$$p_n^R(x) = x^n \cdot p(\frac{1}{x}) = x^n \cdot \frac{1}{x^i} \cdot h(\frac{1}{x}) = x^{n-i} \cdot h(\frac{1}{x}) = x^{k-1-i} \cdot x^{n+1-k} \cdot h(\frac{1}{x}) = x^{k-1-i} \cdot h_{n+1-k}^R(x).$$

Wobec tego udowodniliśmy, że dla $i < k$ wielomiany $x^i \cdot h_{n+1-k}^R(x)$ należą do $K^\perp$. Kod $K^\perp$ jest przestrzenią wymiaru $(n+1)-(n+1-k) = k$. Jest też oczywiste, że wektor współczynników wielomianu $x^i \cdot h_{n+1-k}^R(x)$ zaczyna się i zerami. Implikuje to, że wielomiany $x^i \cdot h_{n+1-k}^R(x)$ dla $i < k$ tworzą bazę przestrzeni $K^\perp$. Zarówno wyraz wolny wielomianu h, jak i współczynnik przy potędze x^{n+1-k} wielomianu h_{n+1-k}^R jest równy 1 lub -1. Tak więc, wielomian $\pm h_{n+1-k}^R(x)$ (z odpowiednio dobranym znakiem) generuje kod $K^\perp$.

Podstawmy we wzorze $g(x) \cdot h(x) = x^{n+1} - 1$ odwrotność x zamiast x. W ten sposób otrzymujemy, że

$$g(\frac{1}{x}) \cdot h(\frac{1}{x}) = \frac{1}{x^{n+1}} - 1 = \frac{1 - x^{n+1}}{x^{n+1}}.$$

Mnożąc obie strony otrzymanego wzoru przez $-x^{n+1}$ dostajemy

$$x^{n+1} - 1 = -x^{n+1} \cdot g(\frac{1}{x}) \cdot h(\frac{1}{x}) = -x^k \cdot g(\frac{1}{x}) \cdot x^{n+1-k} \cdot h(\frac{1}{x}) = -g_k^R(x) \cdot h_{n+1-k}^R(x).$$

Tak więc, wielomian $h_{n+1-k}^R(x)$ jest dzielnikiem $x^{n+1} - 1$, a to implikuje, że kod $K^\perp$ jest cykliczny. □

7.2 Kod Golay'a

Zauważmy, że w pierścieniu $Z_2[x]$

$$x^{23} - 1 = (x-1) \cdot (x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1) \cdot (x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1).$$

Niech

$$w(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1.$$

Wielomian $w_{11}^R(x)$ jest równy $x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$. Wobec tego,

$$x^{23} - 1 = (x-1) \cdot w(x) \cdot w_{11}^R(x).$$

Kodem Golay'a nazywamy kod cykliczny zawarty w przestrzeni $Z_2^{22}[x] = Z_2^{23}$ generowany przez wielomian w.

Lemat 7.2 *Istnieje ciało F i element $p \in F$ takie, że $1+1=0$, $w(p)=0$, $p^{23}=1$ oraz $p^i \neq 1$ dla wszystkich i spełniających nierówność $0 < i < 23$.* □

Niech F i p będą ciałem i elementem o własnościach podanych w powyższym lemacie. Zauważmy, że Z_2 jest podciałem ciała F, a więc Z_2 jest zawarte w F i działania na elementach Z_2 wykonywane w ciałach Z_2 i F dają te same rezultaty. Ponadto, w ciele F spełniona jest równość $x + x = 0$.

Lemat 7.3 *Jeżeli $u \in Z_2[x]$, $a \in F$ i $u(a) = 0$, to $u(a^2) = 0$.*

Dowód. Zauważmy, że

$$0 = u^2(a) = (\sum_{i=1}^{m} a_i \cdot a^i)^2 = \sum_{i=1}^{m} a_i^2 \cdot a^{2\cdot i} + 2 \cdot \sum_{i<j} a_i \cdot a_j \cdot a^{i+j} = \sum_{i=1}^{m} a_i^2 \cdot a^{2\cdot i} = \sum_{i=1}^{m} a_i \cdot (a^2)^i = w(a^2). \ \Box$$

Wniosek 7.4 *Elementy p, p^2, p^4, p^8, p^{16}, p^9, p^{18}, p^{13}, p^3, p^6 i p^{12} są pierwiastkami wielomianu w.* $\Box$

Wniosek 7.5 *W pierścieniu $F[x]$ wielomian $w(x)$ jest równy iloczynowi*

$$(x-p)\cdot(x-p^2)\cdot(x-p^3)\cdot(x-p^4)\cdot(x-p^6)\cdot(x-p^8)\cdot(x-p^9)\cdot(x-p^{12})\cdot(x-p^{13})\cdot(x-p^{16})\cdot(x-p^{18}). \ \Box$$

Wniosek 7.6 *Elementy p^5, p^7, p^{10}, p^{11}, p^{14}, p^{15}, p^{17}, p^{19}, p^{20}, p^{21} i p^{22} nie są pierwiastkami wielomianu $(x-1)\cdot w(x)$, a więc są pierwiastkami wielomianu $w_{11}^R(x)$. W pierścieniu $F[x]$ wielomian $w_{11}^R(x)$ jest równy iloczynowi*

$$(x-p^5)\cdot(x-p^7)\cdot(x-p^{10})\cdot(x-p^{11})\cdot(x-p^{14})\cdot(x-p^{15})\cdot(x-p^{17})\cdot(x-p^{19})\cdot(x-p^{20})\cdot(x-p^{21})\cdot(x-p^{22}). \ \Box$$

Lemat 7.7 *Jeżeli wielomian*

$$u(x) = a_1 \cdot x^{m_1} + a_2 \cdot x^{m_2} + a_3 \cdot x^{m_3} + a_4 \cdot x^{m_4}$$

stopnia $\leqslant 22$ z parami różnymi wykładnikami m_1, m_2, m_3 i m_4 jest podzielny przez wielomian $w(x)$, to $a_1 = a_2 = a_3 = a_4 = 0$.

Dowód. Oczywiście, $w(p) = w(p^2) = w(p^3) = w(p^4) = 0$. Stąd wynika, że także $u(p) = u(p^2) = u(p^3) = u(p^4) = 0$. Równości te oznaczają, że liczby a_1, a_2, a_3 i a_4 są rozwiązaniami następującego układu równań liniowych:

$$\begin{array}{c} p^{m_1} \cdot z_1 + p^{m_2} \cdot z_2 + p^{m_3} \cdot z_3 + p^{m_4} \cdot z_4 = 0 \\ (p^{m_1})^2 \cdot z_1 + (p^{m_2})^2 \cdot z_2 + (p^{m_3})^2 \cdot z_3 + (p^{m_4})^2 \cdot z_4 = 0 \\ (p^{m_1})^3 \cdot z_1 + (p^{m_2})^3 \cdot z_2 + (p^{m_3})^3 \cdot z_3 + (p^{m_4})^3 \cdot z_4 = 0 \\ (p^{m_1})^4 \cdot z_1 + (p^{m_2})^4 \cdot z_2 + (p^{m_3})^4 \cdot z_3 + (p^{m_4})^4 \cdot z_4 = 0. \end{array}$$

Wyznacznik główny tego układu równań jest wyznacznikiem Vandermonde'a

$$\begin{bmatrix} p^{m_1} & p^{m_2} & p^{m_3} & p^{m_4} \\ (p^{m_1})^2 & (p^{m_2})^2 & (p^{m_3})^2 & (p^{m_4})^2 \\ (p^{m_1})^3 & (p^{m_2})^3 & (p^{m_3})^3 & (p^{m_4})^3 \\ (p^{m_1})^4 & (p^{m_2})^4 & (p^{m_3})^4 & (p^{m_4})^4 \end{bmatrix}$$

i – zgodnie ze znanym wzorem – jest równy

$$\prod_{1 \leqslant i < j \leqslant 4} (p^{m_i} - p^{m_j}),$$

a więc jest różny od 0. Implikuje to, że tylko układ czterech zer jest rozwiązaniem rozważanego układu równań. Tak więc $a_1 = a_2 = a_3 = a_4 = 0$. $\Box$

Twierdzenie 7.8 *Jeżeli wielomian $u(x)$ należy do kodu Golay'a i ma parzystą liczbę niezerowych współczynników, to liczba niezerowych współczynników u dzieli się przez 4.*

Dowód. Niech

$$v(x) = x^{23} \cdot u(\frac{1}{x}).$$

Oczywiście

$$v(p^{22}) = (p^{22})^{23} \cdot u(\frac{p^{23}}{p^{22}}) = u(p) = 0.$$

Z lematu 7.3 i wniosku 7.6 wynika, że wielomian $w_{11}^R(x)$ dzieli $v(x)$ w pierścieniu $F[x]$. Ponieważ $u(1) = 0$, więc $x - 1$ dzieli $u(x)$ i tym bardziej wielomian $x^{23} - 1 = (x-1) \cdot w(x) \cdot w_{11}^R(x)$ dzieli w pierścieniu $F[x]$ iloczyn $u(x) \cdot v(x)$. Nietrudno zauważyć (analizując algorytm dzielenia wielomianów), że współczynniki ilorazu i reszty z dzielenia wielomianów należą do najmniejszego ciała, do którego należą współczynniki dzielonych wielomianów. Stąd wynika, że wielomian $x^{23} - 1$ dzieli także w pierścieniu $Z_2[x]$ iloczyn $u(x) \cdot v(x)$.

Przyjmijmy, że

$$u(x) = \sum_{i=0}^{22} a_i \cdot x^i$$

oraz, że tym przedstawieniu jest r współczynników różnych od 0, czyli równych 1. Wtedy, dla odpowiedniego wielomianu q

$$\begin{aligned}
&u(x) \cdot v(x) = \\
&(\sum_{i=0}^{22} a_i \cdot x^i) \cdot x^{23} \cdot (\sum_{i=0}^{22} a_i \cdot x^{-i}) = \\
&\sum_{i,j=0}^{22} a_i \cdot a_j \cdot x^{23+i-j} = \\
&\sum_{i=0}^{22} a_i^2 \cdot x^{23} + \sum_{i<j}^{22} a_i \cdot a_j \cdot x^{23+i-j} + \sum_{i>j}^{22} a_i \cdot a_j \cdot x^{23+i-j} = \\
&(\sum_{i=1}^{r} 1) \cdot x^{23} + \sum_{i<j}^{22} a_i \cdot a_j \cdot x^{23+i-j} + (\sum_{i>j}^{22} a_i \cdot a_j \cdot x^{i-j}) \cdot x^{23} = \\
&\sum_{i=1}^{r} 1 + \sum_{i<j}^{22} a_i \cdot a_j \cdot x^{23+i-j} + \sum_{i>j}^{22} a_i \cdot a_j \cdot x^{i-j} + (\sum_{i=1}^{r} 1 + \sum_{i>j}^{22} a_i \cdot a_j \cdot x^{i-j}) \cdot (x^{23} - 1) = \\
&\sum_{i=1}^{r} 1 + \sum_{i<j}^{22} a_i \cdot a_j \cdot x^{23+i-j} + \sum_{i<j}^{22} a_i \cdot a_j \cdot x^{j-i} + q(x) \cdot (x^{23} - 1) = \\
&\sum_{i=1}^{r} 1 + \sum_{k=1}^{22} (\sum_{i=0}^{22-k} a_i \cdot a_{i+k}) \cdot x^{23-k} + \sum_{k=1}^{22} (\sum_{i=0}^{22-k} a_i \cdot a_{i+k}) \cdot x^k + q(x) \cdot (x^{23} - 1) = \\
&\sum_{i=1}^{r} 1 + \sum_{k=1}^{22} (\sum_{i=0}^{22-k} a_i \cdot a_{i+k} + \sum_{i=0}^{k-1} a_{i+23-k} \cdot a_i) \cdot x^k + q(x) \cdot (x^{23} - 1) = \\
&\sum_{i=1}^{r} 1 + \sum_{k=1}^{22} (\sum_{i=0}^{22-k} a_i \cdot a_{i+k} + \sum_{i=23-k}^{22} a_i \cdot a_{i+k-23}) \cdot x^k + q(x) \cdot (x^{23} - 1).
\end{aligned}$$

Niech

$$c_k = \sum_{i=0}^{22-k} a_i \cdot a_{i+k} + \sum_{i=23-k}^{22} a_i \cdot a_{i+k-23}. \tag{9}$$

Tak więc

$$u(x) \cdot v(x) = \sum_{i=1}^{r} 1 + \sum_{k=1}^{22} c_k \cdot x^k + q(x) \cdot (x^{23} - 1). \tag{10}$$

Co więcej, równość ta jest prawdziwa bezwzględu na to, jak jest wykonywane dodawanie i mnożenie współczynników, a więc zarówno w pierścieniu $Z_2[x]$, jak i w pierścieniu $Z[x]$ wielomianów o współczynnikach całkowitych.

Zauważmy, że $c_k = c_{23-k}$ dla $k = 1, \ldots, 22$. Aby się o tym przekonać wystarczy podstawić $23 - k$ zamiast k we wzorze na c_k i porównać otrzymany wzór z wzorem na c_k.

Podstawmy $x = 1$ we wzorze (10) i wykonajmy obliczenia w pierścieniu liczb całkowitych korzystając z powyższej uwagi. Wtedy

$$r^2 = u(1) \cdot v(1) = r + 2 \cdot \sum_{k=1}^{11} C_k, \tag{11}$$

gdzie C_k jest wartością prawej strony wzoru (9) obliczonej przy założeniu, że $+$ i $\cdot$ oznaczają działania w zbiorze liczb całkowitych.

Pokażemy, że liczby C_k są parzyste. Niech C'_k bedzie wartością prawej strony wzoru (9) obliczonej przy założeniu, że $+$ i $\cdot$ oznaczają działania w w ciele Z_2. Ze związków między działaniami w Z i w Z_2 wynika, że C'_k jest resztą z dzielenia C_k przez 2. Tak więc C_k jest liczbą parzystą wtedy i tylko wtedy, gdy $C'_k = 0$. W pierścieniu $Z_2[x]$ wzór (10) przyjmuje postać

$$u(x) \cdot v(x) = \sum_{i=1}^{r} 1 + \sum_{k=1}^{22} C'_k \cdot x^k + q(x) \cdot (x^{23} - 1).$$

Wzór ten oznacza, że wielomian

$$\sum_{i=1}^{r} 1 + \sum_{k=1}^{22} C'_k \cdot x^k$$

jest resztą z dzielenia w pierścieniu $Z_2[x]$ wielomianu $u(x) \cdot v(x)$ przez $x^{23} - 1$. Wiemy też, że ta reszta jest wielomianem zerowym. Stąd wynika, że $C'_k = 0$, a także że liczby C_k są parzyste.

Z wzoru (11) otrzymujemy teraz, że $r(r-1)$ jest liczbą podzielną przez 4. Ponieważ r jest liczbą parzystą, więc r musi być podzielne przez 4. $\square$