Wykład 10.

10.1 Podstawy algebraiczne

Będziemy korzystać z następujących twierdzeń:

Twierdzenie 10.1 *Dla dowolnej liczby pierwszej k i dowolnej liczby n istnieje nierozkładalny nad ciałem Z_k wielomian stopnia n.*

Twierdzenie 10.2 *Jeżeli $p(x)$ jest wielomianem stopnia n, nierozkładalnym nad ciałem F, to zbiór $F^{n-1}[x]$ z dodawaniem wielomianów i mnożeniem wielomianów modulo $p(x)$ jest ciałem (mającym $\mid F\mid^n$ elementów).*

Dowód. Aby pomnożyć modulo $p(x)$ dwa wielomiany, mnożymy je w zwykły sposób, a następnie dzielimy je przez $p(x)$. Wynikiem mnożenia modulo $p(x)$ jest reszta z dzielenia zwykłego iloczynu przez $p(x)$.

W standardowy sposób sprawdzamy, że $F^{n-1}[x]$ z dodawaniem i mnożeniem modulo $p(x)$ pierścieniem. Aby dowieść, że ta struktura jest ciałem, wystarczy pokazać istnienie elemetów odwrotnych.

Niech $q(x) \in F^{n-1}[x]$. Największym wspólnym dzielnikiem wielomianów $p(x)$ i $q(x)$ jest 1, gdyż w przeciwnym razie wielomian $p(x)$ byłby rozkładalny. Wobec tego, $a(x) \cdot q(x) + b(x) \cdot p(x) = 1$ dla pewnych wielomianów $a(x)$ i $b(x)$. Wynika to z analizy algorytmu Euklidesa. W ten sposób otrzymujemy także, że wielomiany $a(x)$ i $b(x)$ są stopnia mniejszego od stopnia wielomianu $p(x)$. Oczywiście, iloczyn modulo $p(x)$ wielomianów $a(x)$ i $q(x)$ jest równy 1, a więc w rozważanym pierścieniu $a(x)$ jest elementem odwrotnym do $q(x)$.

Można także dowieść twierdzenie odwrotne. □

Twierdzenie 10.3 *W dowolnym ciele skończonym F istnieje element g taki, że zbiór $F \setminus \{0\}$ (czyli grupa multiplikatywna ciała F) jest równy $\{g^i : i < \mid F\mid\}$ (tj. grupa multiplikatywna F jest cykliczna, czyli generowana przez pojedyńczy element).*

Wielomian $p(x) = x^3 + x + 1$ jest nierozkładalny nad Z_2. Dla przykładu przeanalizujemy ciało $Z_2^2[x]$ z dodawaniem i mnożeniem $\cdot_p$ modulo $p(x)$. Oczywiście,

$$Z_2^2[x] = \{0, 1, x, x^2, 1 + x, 1 + x^2, x + x^2, 1 + x + x^2\}.$$

Zauważmy, ze

$$(1 + x^2) \cdot (1 + x + x^2) = 1 + x + x^3 + x^4 = (1 + x) \cdot (1 + x + x^3) + (x + x^2).$$

Wobec tego,

$$(1 + x^2) \cdot_p (1 + x + x^2) = x + x^2.$$

Ponieważ grupa multiplikatywna rozważanego ciała ma 7 elementów, więc każdy element tej grupy różny od 1 generują ją. Obliczmy kolejne potęgi (modulo $p(x)$) wielomianu x. Mamy $x^0 = 1$, $x^1 = x$, $x^2 = x^2$, $x^3 = (1 + x + x^3) + 1 + x = 1 + x$ $x^4 = (1 + x) \cdot_p x = x + x^2$, $x^5 = (x + x^2) \cdot_p x = 1 + x + x^2$, $x^6 = (1 + x + x^2) \cdot_p x = 1 + x^2$ oraz $x^7 = (1 + x^2) \cdot_p x = 1$.

10.2 Znowu o kodzie Hamminga

Niech m będzie dodatnią liczbą naturalną. Weźmy ciało $F = Z_2^{m-1}[x]$ z mnożeniem modulo $p(x)$ dla nierozkładalnego wielomianu $p(x)$ stopnia m oraz generator β grupy multiplikatywnej tego ciała. Rozważmy

$$K = \{w \in Z_2^{2^m-2}[x] : w(\beta) = 0\}.$$

Zbiór K jest oczywiście kodem liniowym. Ponieważ β jest generatorem grupy multiplikatywnej F o $2^m - 1$ elementach, więc $\beta^{2^m-1} = 1$ (z definicji generatora, $\beta^{2^m-1} = \beta^i$ dla pewnego i, gdyby $0 < i < 2^m - 1$, to β nie mógłby generować całej grupy multiplikatywnej, a więc $i = 0$). Wobec tego, jeżeli β jest pierwiastkiem wielomianu $w(x)$, to jest także pierwiastkiem cyklicznego przesunięcia wielomianu $w(x)$, czyli wielomianu $C(w(x)) = x \cdot w(x) - a \cdot (x^{2^m-1} - 1)$. Oznacza to, że kod K jest cykliczny.

Dla każdego $j < 2^m - 1$ przedstawmy β^j jako wielomian należący do $Z_2^{2^m-1}[x]$. Niech

$$\beta^j = \sum_{i=0}^{m-1} a_{i,j} \cdot x^i.$$

Utwórzmy macierz

$$H = \begin{bmatrix} a_{0,0} & a_{0,1} & \ldots & a_{0,2^m-1} \\ \vdots & \vdots & & \vdots \\ a_{m-1,0} & a_{m-1,1} & \ldots & a_{m-1,2^m-1} \end{bmatrix}.$$

Przyjmijmy, że $w(x) = \sum_{j=0}^{2^m-2} w_j \cdot x^j$. Wtedy

$$w(\beta) = \sum_{j=0}^{2^m-2} w_j \cdot \beta^j = \sum_{j=0}^{2^m-2} w_j \cdot (\sum_{i=0}^{m-1} a_{i,j} \cdot x^i) = \sum_{i=0}^{m-1} (\sum_{j=0}^{2^m-2} w_j \cdot a_{i,j}) \cdot x^i.$$

Tak więc współczynnikami $w(\beta)$ (a więc wielomianu z ciała $Z_2^{m-1}[x]$) są iloczyny skalarne wierszy macierzy H i współczynników wielomianu $w(x)$. Stąd wynika, że

$$K = \{w \in Z_2^{2^m-1} : H \cdot w = \vec{0}\}$$

(gdyż $w(\beta) = 0$ wtedy i tylko wtedy, gdy wszystkie współczynniki wielomianu $w(\beta)$ są zerami; zauważmy, że $w(\beta)$ jest zarówno wartością wielomianu w dla argumentu β, jak i pewnym wielomianem stopnia $\leqslant m - 1$).

Kolumny macierzy H są współczynnikami wielomianów postaci β^j. Ponieważ wśród elementów tej postaci nie ma zera, więc macierz H nie ma kolumny zerowej. Ponadto, każde dwie kolumny macierzy H są różne, gdyż każde dwa elementy postaci β^i dla $i \leqslant 2^m - 1$ są różne. Tak więc kod K jest cykliczną wersją kodu Hamminga.

Z rachunków przeprowadzonych w poprzednim rozdziale wynika, że dla $m = 3$ i dla wielomianu $p(x) = 1 + x + x^3$ można wziąć $\beta = x$. Wtedy macierz H przyjmuje postać

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Gdyby wykonać cykliczne przesunięcie wierszy macierzy H w lewo o 1 element, to okazałoby się, że kod dualny do K jest generowany przez wielomian $g(x) = 1 + x^2 + x^3 + x^4$. Ponieważ

$$x^7 - 1 = (1 + x^2 + x^3 + x^4) \cdot (1 + x^2 + x^3) = (1 + x) \cdot (1 + x + x^3) \cdot (1 + x^2 + x^3),$$

więc kod K jest generowany przez wielomian

$$x^3 \cdot (1 + (\frac{1}{x})^2 + (\frac{1}{x})^3) = 1 + x + x^3.$$

W ogólnym przypadku, generatorem kodu K jest unormowany wielomian $g(x)$ najmniejszego stopnia taki, że $g(\beta) = 0$. Wielomian ten można scharakteryzować jako nierozkładalny dzielnik $g(x) \in Z_2^{2^m-2}[x]$ wielomianu $x^{2^m-1} - 1$ taki, że $g(\beta) = 0$. Aby obliczyć $g(x)$, możemy rozłóżyć $x^{2^m-1} - 1$ na iloczyn wielomianów nierozkładalnych i wybrać odpowiedni czynnik z tego iloczynu. W rozważanym przykładzie, jeżeli weźmiemy wielomian $1+x^2+x^3$, podstawimy $\beta = x$ zamiast x i wykonamy obliczenia modulo $p(x)$, to otrzymamy $x + x^2 \neq 0$. Analogiczne obliczenia dla wielomianu $1+x+x^3 = p(x)$ dadzą wynik równy 0. Tak więc wielomian $1+x+x^3$ jest generatorem kodu K.

Aby obliczyć $g(x)$ w ogólnym przypadku, możemy też znaleźć przedstawienie tego wielomianu w postaci iloczynu wielomianów o współczynnikach z F. Wiadomo bowiem, że jeżeli $b \in F$ jest pierwiastkiem wielomianu g (nad Z_2), to także b^2 jest pierwiastkiem tego wielomianu. Aby znaleźć $g(x)$, szukamy więc najmniejszej liczby k takiej, że $\beta^{2^k} = \beta$. Oczywiście, wielomian

$$g'(x) = \prod_{i=0}^{k-1} (x - \beta^{2^i})$$

dzieli wielomian $g(x)$ (w pierścieniu $F[x]$). Dowodzi się, że $g'(x) \in Z_2[x]$. Stąd oczywiście wynika, że $g(x) = g'(x)$.

W rozważanym przykładzie mamy $x^1 = x$, $x^2 = x^2$, $x^4 = x + x^2$ oraz $x^8 = x$. Wobec tego, $k = 3$ oraz

$$g(y) = (y - x) \cdot (y - x^2) \cdot (y - x - x^2)$$

(piszemy $g(y)$, ponieważ rozważamy wielomiany o współczynnikach, które są wielomianami zmiennej x). Mamy więc

$$\begin{aligned} g(y) &= (y^2 - (x + x^2) \cdot y - x^3) \cdot (y - x - x^2) \\ &= (y^3 - (x + x^2) \cdot y^2 + (x + 1) \cdot y) - (y^2 - (x + x^2) \cdot y + (x + 1)) \cdot (x + x^2) \\ &= y^3 + y + 1. \end{aligned}$$

10.3 Przykłady kodów korygujących dwa błędy

Niech $\varphi(n)$ oznacza liczbę tych dodatnich liczb $< n$, które są względnie pierwsze z n.

Przypuśćmy, że $X = \{a_1, a_2, \ldots, a_{\varphi(n)}\}$ jest zbiorem wszystkich dodatnich liczb $< n$, które są względnie pierwsze z n. Niech q będzie liczbą względnie pierwszą z n. Rozważamy funkcję $f : X \to N$ zdefiniowana wzorem $f(x) = x \cdot q \bmod n$. Jeżeli x i q są względnie pierwsze z n, to względnie pierwsze z n są także $x \cdot q$ oraz $f(x)$. Dodatkowo, $f(x) < n$. Wobec tego,

$f : X \to X$. Funkcja f jest też różnowartościowa. Gdyby bowiem $f(a_i) = f(a_j)$ dla $a_i \geqslant a_j$, to $q \cdot (a_i - a_j)$ dzieliłoby się przez n. Ponieważ q jest względnie pierwsze z n, więc wtedy n dzieliłoby $a_i - a_j < n$. Jest to możliwe tylko, gdy $a_i = a_j$. Wobec tego, liczby $b = a_1 \cdot \ldots \cdot a_{\varphi(n)}$ oraz $q^{\varphi(n)} \cdot b = (q \cdot a_1) \cdot \ldots \cdot (q \cdot a_{\varphi(n)})$ przystają do siebie modulo n. Oznacza to, że n dzieli $b \cdot (q^{\varphi(n)} - 1)$. Ale b jest względnie pierwsze z n. Tak więc n dzieli $q^{\varphi(n)} - 1$.

W szczególności, jeżeli n jest liczbą nieparzystą, to n dzieli $2^{\varphi(n)} - 1$.

Weźmy dowolną liczbę nieparzystą n. Przyjmijmy, że $n \cdot m = 2^{\varphi(n)} - 1$. Niech F będzie ciałem $Z_2^{\varphi(n)-1}[x]$ z mnożeniem modulo $p(x)$. Multiplikatywna grupa ciała F ma generator b. Niech $\beta = b^m$. Zauważmy, że $\beta^n = (b^m)^n = b^{2^{\varphi(n)}-1} = 1$ oraz, że $\beta^i \neq 1$ dla i takich, że $0 < i < n$. Przyjmijmy, że

$$K = \{w(x) \in Z_2^{n-1}[x] : w(\beta) = w(\beta^3) = 0\}.$$

Zbiór K jest kodem cyklicznym (dowodzimy to tak, jak analogiczny fakt w poprzednim rozdziale).

Udowodnimy, że tak zdefiniowany kod K koryguje (przynajmniej) dwa błędy.

Przypuśćmy, że $S_2(0) \subseteq Z_2^{n-1}[x]$ jest zbiorem wielomianów o najwyżej dwóch niezerowych współczynnikach. Zdefiniujemy funkcję $s : Z_2^{n-1}[x] \to F^2$ przyjmując, że $s(w) = (w(\beta), w(\beta^3))$ (wielomianowi w przyporządkowujemy parę wartości wielomianu w obliczonych w ciele F dla argumentów β i β^3).

Funkcja s na zbiorze $S_2(0)$ jest różnowartościowa. Najpierw zauważmy, że z tego wynika, że kod K koryguje dwa błędy. Przypuśćmy, że $u \in S_2(w) \cap S_2(v)$ dla pewnych $w, v \in K$. Wtedy z definicji kodu K otrzymujemy, że $s(u) = s(u - w)$ oraz $s(u) = s(u - v)$. Oczywiście, $u - w, u - v \in S_2(0)$. Ponieważ $s(u - w) = s(u - v)$ oraz s jest różnowartościowa na $S_2(0)$, więc $u - w = u - v$, a także $w = v$. Tym samym kod K koryguje dwa błędy.

W zbiorze $S_2(0)$ są trzy rodzaje wielomianów: wielomian zerowy, wielomiany $e_i(x) = x^i$ dla $i < n$ oraz wielomiany $e_{i,j}(x) = x^i + x^j$ dla $i < j < n$. Funkcja s wielomianowi 0 przyporządkowuje parę złożoną z dwóch zer. Pierwsza współrzędna pary $s(e_i)$ jest równa β^i i jest różna od 0. Pierwsza współrzędna pary $s(e_{i,j})$ jest równa $\beta^i + \beta^j$, i gdyby była równa 0, to $\beta^i(\beta^{j-i} - 1) = 0$ oraz $\beta^{j-i} - 1 = 0$. Ten ostatni fakt jest sprzeczny z wyborem β. Wobec tego, funkcja s przyjmuje parę złożoną z dwóch 0 tylko dla wielomianu 0.

Jeżeli $s(e_i) = (c, d)$, to $c^3 = d$. Zauważmy, że pary $s(e_{i,j})$ nie mają tej własności. Jeżeli $a = \beta^i$ oraz $b = \beta^j$, to $s(e_{i,j}) = (a + b, a^3 + b^3)$ oraz zachodzi wzór

$$(a + b)^3 - a^3 - b^3 = a \cdot b \cdot (a + b), \tag{13}$$

w którym prawa strona jest różna od 0 (pamiętajmy, że liczymy w ciele, w którym $x + x = 0$ dla dowolnego x). Wobec tego, $s(e_{i,j}) \neq s(e_k)$ dla wszystkich dopuszczalnych i, j, k. Jest też oczywiste, że pary $s(e_i)$ oraz $s(e_j)$ dla $i \neq j$ różnią się pierwszą współrzędną.

Przyjmujemy dalej, że $a = \beta^i$ oraz $b = \beta^j$. Tak więc $s(e_{i,j}) = (a + b, a^3 + b^3)$ oraz $a + b \neq 0$. Zauważmy, że gdyby $a + b = c + d \neq 0$ oraz $a^3 + b^3 = c^3 + d^3$, to także $a \cdot b = c \cdot d$. Wynika to z wzoru (13). Rozważmy równanie $x^2 - (a + b) \cdot x + a \cdot b = 0$. Jest oczywiste, że a i b są rozwiązaniami tego równania i równanie to ma najwyżej dwa różne rozwiązania. Gdyby $s(e_{i,j}) = s(e_{k,l})$ dla różnych wielomianów $e_{i,j}$ i $e_{k,l}$, to zbiór $\{\beta^i, \beta^j, \beta^k, \beta^l\}$ miałby przynajmniej trzy elementy i elementy te spełniałyby podane równanie. Ponieważ nie jest to możliwe, więc równość $s(e_{i,j}) = s(e_{k,l})$ implikuje, że $e_{i,j} = e_{k,l}$. W ten sposób zakończyliśmy dowód, że s jest róznowartościowa na zbiorze $S_2(0)$.

Przyjmijmy, że $n = 9$. Mamy więc $\varphi(n) = 6$. W ciele $Z_2^5[x]$ z mnożeniem modulo $p(x)$ istnieje element β taki, że $\beta^9 = 1$ i $\beta^i \neq 1$ dla i takich, że $0 < i < 9$. Wielomian $1 + x + x^6$ jest nierozkładalny i może być wielomianem $p(x)$. Niech $\beta = x + x^2$. Mamy

$$\begin{aligned}
\beta^2 &= x^2 + x^4, \\
\beta^3 &= x^3 + x^4 + x^5 + x^6 = 1 + x + x^3 + x^4 + x^5, \\
\beta^4 &= x^2 + x^3 + x^4, \\
\beta^5 &= 1 + x + x^3, \\
\beta^6 &= x + x^3 + x^4 + x^5, \\
\beta^7 &= x + x^3 + x^4, \\
\beta^8 &= 1 + x + x^2 + x^3 + x^4, \\
\beta^9 &= 1.
\end{aligned}$$

Jeżeli β jest pierwiastkiem wielomianu $w \in Z_2[x]$, to pierwiastkami tego wielomianu są także β^2, β^4, β^8, β^7 i β^5. Wobec tego, β jest pierwiastkiem wielomianu $w(y)$ wtedy i tylko wtedy, gdy $w(y)$ jest podzielny przez wielomian

$$\begin{aligned}
g_1(y) &= (y - \beta) \cdot (y - \beta^2) \cdot (y - \beta^4) \cdot (y - \beta^5) \cdot (y - \beta^7) \cdot (y - \beta^8) \\
&= (y^2 + (x + x^4) \cdot y + \beta^3) \cdot (y^2 + (1 + x) \cdot y + \beta^3) \cdot (y^2 + (1 + x^4) \cdot y + \beta^3) \\
&= y^6 + y^3 + 1
\end{aligned}$$

Jeżeli β^3 jest pierwiastkiem wielomianu $w \in Z_2[x]$, to pierwiastkami tego wielomianu jest także β^6. Wobec tego, β jest pierwiastkiem wielomianu $w(y)$ wtedy i tylko wtedy, gdy $w(y)$ jest podzielny przez wielomian

$$g_2(y) = (y - \beta^3) \cdot (y - \beta^6) = y^2 + y + 1$$

W końcu otrzymujemy, że $w(y) \in K$ wtedy i tylko wtedy, gdy $w(y)$ jest podzielny przez wielomian

$$g_1(y) \cdot g_2(y) = 1 + y + y^2 + y^3 + y^4 + y^5 + y^6 + y^7 + y^8 = \frac{y^9 - 1}{y - 1}.$$

Tak więc K jest kodem powtórzeniowym długości 9.