# Wykład 2.

## 2.1 Ciała

Zbiór $F$ jest ciałem, jeżeli są w nim określone dwa działania: dodawanie $+$ i mnożenie $\cdot$ mające najprostsze własności dodawania i mnożenia liczb rzeczywistych. Przyjmujemy więc, że działania te są łączne i przemienne, a także mają elementy neutralne oznaczane zwykle symbolami 0 i 1. Mnożenie jest rozdzielne względem dodawania. Ponadto, dla każdego elementu ciała istnieje element przeciwny (czyli taki, który w sumie z tym elementem daje 0), a dla każdego elementu różnego od 0 istnieje element odwrotny (czyli taki, który po pomnożeniu przez ten element daje 1). Zakładamy też, że 0 jest różne od 1.

Rozważmy zbiór liczb $\{0, 1, \ldots, n-1\}$ z dodawaniem i mnożeniem modulo $n$. Taką strukturę algebraiczną oznaczamy symbolem $Z_n$. Dowodzi się, że w tej strukturze są spełnione wszystkie własności podane w definicji ciała z wyjątkiem (najwyżej) istnienia elementów odwrotnych. Struktury o tych własnościach nazywamy pierścieniami.

**Lemat 2.1** *$Z_n$ jest ciałem wtedy i tylko wtedy, gdy $n$ jest liczbą pierwszą.*

**Dowód.** Przypuśćmy najpierw, że $Z_n$ jest ciałem dla pewnej złożonej liczby $n$. Niech $n = a \cdot b$ dla pewnych liczb $a$ i $b$ takich, że $1 < a, b < n$. Wyliczmy iloczyn liczb $a$ i $b$ w ciele $Z_n$. W tym ciele $a \cdot b = 0$. Ponieważ $a$ jest różne od 0, więc możemy wziąć $c$ będące w $Z_n$ elementem odwrotnym do $a$. Dla tego $c$ mamy $b = 1 \cdot b = c \cdot a \cdot b = c \cdot 0 = 0$. Przeczy to nierówności $1 < b < n$.

Załóżmy teraz, że $n$ jest liczbą pierwszą. Niech $a$ będzie dowolną liczbą spełniającą nierówności $0 < a < n$. Będziemy rozważać funkcję $f : \{0, \ldots, n-1\} \to \{0, \ldots, n-1\}$ zdefiniowaną wzorem $f(x) = a \cdot x$ (modulo $n$). Funkcja $f$ jest różnowartościowa. Gdyby bowiem $f(x) = f(y)$ dla pewnych $x$ i $y$ takich, że $0 \leqslant x < y < n$, to liczba $n$ dzieliłaby $a(y-x)$ i tym samym dzieliłaby albo $a$, albo $y-x$. Nie jest to jednak możliwe. Liczba $a$ nie jest podzielna przez $n$ ponieważ spełnia podaną nierówność. Liczba $n$ nie dzieli też liczby $y - x$, gdyż $0 \leqslant y - x \leqslant y < n$.

Różnowartościowość $f$ implikuje, że jest to funkcja typu „na”. Wobec tego $f(x) = a \cdot x = 1$ dla pewnego $x$. Ten $x$ jest elementem odwrotnym do $a$ w pierścieniu $Z_n$. □

## 2.2 Przestrzenie liniowe

Przestrzenią liniową nad ciałem $F$ nazywamy zbiór $V$, w którym jest określona operacja dodawania, i którego elementy można mnożyć przez elementy ciała $F$. Operacja dodawania elementów przestrzeni liniowej jest łączna i przemienna, ma element neutralny i dla każdego elementu istnieje element przeciwny. Mnożenie jest rozdzielne względem dodawania, a więc $(a + b)x = ax + bx$ oraz $a(x + y) = ax + ay$ dla wszystkich $a, b \in F$ oraz $x, y \in V$, a także jest łączne w następującym sensie: $(ab)x = a(bx)$ dla wszystkich $a, b \in F$ i $x \in V$.

Niech $F$ będzie ciałem. W zbiorze $F^n$ określamy dodawanie i mnożenie w następujący sposób:

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

oraz

$$a(x_1, \dots, x_n) = (ax_1, \dots, ax_n)$$

dla wszystkich $a, x_1, \dots, x_n, y_1, \dots, y_n \in F$. Zbiór $F^n$ z tym działaniami jest przestrzenią liniową nad ciałem $F$. Można wykazać, że są to jedyne (z dokładnością do izomorfizmu), interesujące nas przestrzenie liniowe nad $F$ (pozostałe przestrzenie liniowe nad $F$ nie mają ważnej dla nas własności).

Podprzestrzenią przestrzeni liniowej $V$ (nad ciałem $F$) nazywamy dowolny, niepusty podzbiór $V$ zamknięty ze względu na dodawanie i mnożenie przez elementy z ciała $F$.

## 2.3 Kody liniowe

Niech $F$ będzie ciałem skończonym (np. ciałem $Z_2$). Zbiór $K \subseteq F^n$ nazywamy kodem liniowym, jeżeli $K$ jest podprzestrzenią liniową przestrzeni $F^n$ (nad ciałem $F$).

Nietrudno zauważyć, że jeżeli $F$ jest jednym z ciał $Z_m$, to zbiór $K \subseteq F^n$ jest kodem liniowym wtedy i tylko wtedy, gdy jest zamknięty ze względu na dodawanie.

**Lemat 2.2** *Dla dowolnych $x, y \in F^n$ zachodzi wzór*

$$d(x, y) = d(x - y, 0).$$

**Wniosek 2.3** *Jeżeli $K \subseteq F^n$ jest kodem liniowym, to*

$$\min\{d(x, y) : x, y \in K \wedge x \neq y\} = \min\{d(x, 0) : x \in K \wedge x \neq 0\}.$$

## 2.4 Definiowanie podprzestrzeni liniowych

Ustalmy ciało $F$ i przestrzeń liniową $F^n$. Niech $\vec{v}_1, \dots, \vec{v}_m$ będą wektorami z $F^n$.

Zbiór

$$\{\sum_{i=1}^{m} a_i \cdot \vec{v}_i : a_1, \dots, a_m \in F\}$$

jest podprzestrzenia liniową przestrzeni $F^n$. Nazywamy ją podprzestrzenią generowaną przez wektory $\vec{v}_1, \dots, \vec{v}_m$.

Iloczynem skalarny $\vec{x} \cdot \vec{y}$ wektorów $\vec{x} = (x_1, \dots, x_n)$ i $\vec{y} = (y_1, \dots, y_n)$ definiujemy wzorem

$$\vec{x} \cdot \vec{y} = \sum_{i=1}^{n} x_i \cdot y_i.$$

Podprzestrzenią liniową jest także zbiór rozwiązań jednorodnego układu równań liniowych, a więc np.

$$\{\vec{x} \in F^n : \vec{v}_i \cdot \vec{x} = 0 \text{ dla } i = 1, \dots, m\}.$$

Zbiór ten zdefiniujemy jeszcze wykorzystując mnożenie macierzy.

Niech $\vec{v}_i = (v_{i,1}, \dots, v_{i,n})$ oraz niech

$$H = \begin{bmatrix} v_{1,1} & v_{1,2} & \dots & v_{1,n} \\ & & \vdots & \\ v_{m,1} & v_{m,2} & \dots & v_{m,n} \end{bmatrix}. \tag{2}$$

Wtedy zbiór rozwiązań podanego układu można zdefiniować jako

$$\{\vec{x} \in F^n : H\vec{x}^T = \vec{0}^T\},$$

przy czym występujący w tym zbiorze warunek $H\vec{x}^T = \vec{0}^T$ oznacza, że iloczyn macierzy $H$ i jednokolumnowej macierzy $\vec{x}^T$ o wyrazach będących współrzędnymi wektora $\vec{x}$ jest równy jednokolumnowej macierzy wypełnionej zerami. Zgodnie z definicją, iloczyn $H\vec{x}^T$ jest określony, jeżeli długość wiersza macierzy $H$ jest równa długości wektora $\vec{x}$, iloczyn ten jest jednokolumnową macierzą o tylu wyrazach, ile wierszy ma macierz $H$, a $i$-ty wyraz tego iloczynu jest iloczynem skalarnym $i$-tego wiersza macierzy $H$ i wektora $\vec{x}$.

Pokazuje się, że każda podprzestrzeń $F^n$ może zostać zdefiniowana jako podprzestrzeń generowana przez pewien (skończony) układ wektorów, a także jako zbiór rozwiązań pewnego jednorodnego układu równań liniowych.

## 2.5 Kod Hamminga

W tym rozdziale będziemy zajmować się liniowymi kodami binarnymi, a więc podprzestrzeniami liniowymi przestrzeni $(Z_2)^n$ (nad ciałem $Z_2$).

**Lemat 2.4** *Niech*

$$K = \{\vec{x} \in (Z_2)^n : H\vec{x}^T = \vec{0}^T\}.$$

*Kod $K$ pozwala na korygowanie 1 błędu wtedy i tylko wtedy, gdy macierz $H$ nie ma dwóch identycznych kolumn i nie zawiera kolumny zerowej.*

**Dowód.** Niech $\vec{e}_i \in (Z_2)^n$ będzie wektorem, którego $i$-ta współrzędna jest równa 1, a pozostałe są równe 0. Podobnie, $i$-ta i $j$-ta współrzędna $\vec{e}_{i,j} \in (Z_2)^n$ jest równa 1, a pozostałe są zerami.

Zauważmy, że $H\vec{e}_i^T$ jest $i$-tą kolumną macierzy $H$. Wobec tego, $i$-ta kolumna macierzy $H$ jest zerowa wtedy i tylko wtedy, gdy $\vec{e}_i \in K$.

Zauważmy także, że $H\vec{e}_{i,j}^T$ jest kolumną powstającą przez zsumowanie $i$-tej i $j$-tej kolumny macierzy $H$. Implikuje to, że kolumny $i$-ta i $j$-ta macierzy $H$ są identyczne wtedy i tylko wtedy, gdy $\vec{e}_{i,j} \in K$ (gdyż w $Z_2$ mamy $x + x = 0$ dla wszystkich $x$).

Powyższe spostrzeżenia pozwalają wykazać, że macierz $H$ ma podane w tezie własności wtedy i tylko wtedy, żaden z wektorów $\vec{e}_i$ oraz $\vec{e}_{i,j}$ nie należy do $K$. Ten ostatni warunek jest równoważny stwierdzeniu, że minimalna odległość wektora zerowego od pozostałych elementów $K$ wynosi przynajmniej 3. To z kolei oznacza, że kod $K$ pozwala korygować 1 błąd. $\Box$

Niech $n$ będzie ustaloną liczbą naturalną. Weźmy przedstawienia dwójkowe długości $n$ liczb od 1 do $2^n - 1$ i potraktujmy je jako kolumny pewnej macierzy. Aby dokładnie określić taką macierz musimy podać kolejność, w jakiej umieścimy w niej poszczególne przedstawienia. W ciągu liczb $1, \ldots, 2^n - 1$ zamieniamy stosowne wyrazy tak, aby na początku ciągu znalazły się potęgi dwójki $2^{n-1}, 2^{n-2}, \ldots, 2^0$. Przyjmijmy, że kolumny macierzy $H$ są przedstawieniami kolejnych wyrazów utworzonego w ten sposób ciągu. Macierz ta ma więc $n$ wierszy i $2^n - 1$ kolumn. Kod $K$ zdefiniowany wzorem

$$K = \{\vec{x} \in (Z_2)^{2^n-1} : H\vec{x}^T = \vec{0}^T\}$$

nazywamy kodem Hamminga. Jest oczywiste, że kod ten pozwala korygować 1 błąd.

Przyjmijmy, że wyrazy macierzy $H$ oznaczamy tak, jak we wzorze (2). Zauważmy, że wtedy równania definiujące kod Hamminga mają postać

$$x_i + \sum_{j=n+1}^{2^n-1} v_{i,j} \cdot x_j = 0$$

dla $i = 1, \ldots, n$. Ponieważ współczynniki tych równań są z ciała $Z_2$, więc możemy równania zapisać równoważnie jako

$$x_i = \sum_{j=n+1}^{2^n-1} v_{i,j} \cdot x_j \tag{3}$$

dla $i = 1, \ldots, n$.

Kod $K : \mathcal{A}^n \to \mathcal{A}^k$ pozwalający korygować $\leqslant e$ błędów nazywamy doskonałym, jeżeli

$$\bigcup_{a \in K(\mathcal{A}^n)} S_e(a) = \mathcal{A}^k.$$

**Twierdzenie 2.5** *Kod Hamminga jest doskonałym kodem pozwalający korygować $\leqslant 1$ błąd.*

**Dowód.** Wektory z przestrzeni $(Z_2)^{2^n-1}$ będziemy przedstawiać w postaci konkatenacji $(\vec{a}, \vec{y})$ dwóch ciągów $\vec{a}$ i $\vec{y}$, z których pierwszy ma długość $n$. Niech $(\vec{a}, \vec{y})$ będzie dowolnym wektorem z tej przestrzeni. Udowodnimy, że ten wektor jest odległy o $\leqslant 1$ od pewnego słowa (wektora) kodowego.

Zdefiniujmy ciąg $\vec{b} = (b_1, \ldots, b_n)$ zgodnie z wzorem (3). Tak więc

$$b_i = \sum_{j=n+1}^{2^n-1} v_{i,j} \cdot y_{j-n}.$$

Oczywiście, wektor $(\vec{b}, \vec{y})$ jest słowem kodowym (należy do $K$). Jeżeli odległość $\vec{a}$ i $\vec{b}$ (w przestrzeni $(Z_2)^n$) jest $\leqslant 1$, to także odległość $(\vec{a}, \vec{y})$ i $(\vec{b}, \vec{y})$ (w przestrzeni $(Z_2)^{2^n-1}$) jest $\leqslant 1$. Załóżmy więc, że odległość $\vec{a}$ i $\vec{b}$ wynosi przynajmniej 2.

Stąd i z definicji macierzy $H$ wynika, że jej kolumna $(v_{1,n+k}, \ldots, v_{n,n+k})$ o numerze postaci $n + k$ spełnia dla $i = 1, \ldots, n$ równoważność

$$a_i \neq b_i \Leftrightarrow v_{i,n+k} = 1. \tag{4}$$

Weźmy ciąg $\vec{e} = (e_1, \ldots, e_{2^n-n-1})$ o wszystkich wyrazach z wyjątkiem $k$-tego równych zero i zdefiniujmy

$$c_i = \sum_{j=n+1}^{2^n-1} v_{i,j} \cdot e_{j-n}.$$

Zauważmy, że $c_i = v_{i,n+k}$ dla $i = 1, \ldots, n$. Stąd i z równoważności (4) otrzymujemy, że $\vec{a} = \vec{b} + \vec{c}$. Wiemy również, że $(\vec{c}, \vec{e})$ jest słowem kodowym.

Aby zakończyć dowód wystarczy zauważyć, że $(\vec{a}, \vec{y} + \vec{e}) = (\vec{b} + \vec{c}, \vec{y} + \vec{e})$ jest słowem kodowym odległym od wektora $(\vec{a}, \vec{y})$ o 1. □