Przestrzenie liniowe

Ostatnia aktualizacja: 30.10.2021 r.

Wykład ten poświęcony będzie pojęciu przestrzeni liniowej nad ciałem. Jest to fundamentalne pojęcie dla całego naszego wykładu i jedno z najważniejszych w całej matematyce. Mówić będziemy o strukturze określonej jednocześnie na dwóch typach obiektów: wektorach i skalarach. Struktura ta jest w swojej istocie „geometryczna", choć odnaleźć ją można w bardzo odległych z pozoru dziedzinach matematyki.

Definicja 1. ***Przestrzenią liniową nad ciałem*** $(K, +, \cdot, 0, 1)$ *nazywamy zbiór* V*, wraz z:*

- *odwzorowaniem:* $\oplus : V \times V \longrightarrow V$*, zwanym dodawaniem wektorów,*
- *odwzorowaniem:* $\otimes : K \times V \longrightarrow V$*, zwanym mnożeniem wektora przez skalar,*
- *wyróżnionym elementem* Θ *w* V *zwanym wektorem zerowym,*

przy czym spełnione są następujące aksjomaty przestrzeni liniowej:

$\forall_{\alpha,\beta,\gamma\in V}$	$\alpha \oplus (\beta \oplus \gamma) = (\alpha \oplus \beta) \oplus \gamma$	*łączność* $\oplus$
$\forall_{\alpha,\beta\in V}$	$\alpha \oplus \beta = \beta \oplus \alpha$	*przemienność* $\oplus$
$\forall_{\alpha\in V}$	$\alpha \oplus \Theta = \alpha$	Θ *jest elem. neutralnym* $\oplus$
$\forall_{\alpha\in V}\exists_{\gamma\in V}$	$\alpha \oplus \gamma = \Theta$	*istnienie wekt. przeciwnego*
$\forall_{\alpha\in V}$	$1 \otimes \alpha = \alpha$	*mnożenie wektora przez 1*
$\forall_{\alpha\in V}\forall_{a,b\in K}$	$(a \cdot b) \otimes \alpha = a \otimes (b \otimes \alpha)$	*zgodność* $\cdot$ *z mnożeniem* $\otimes$
$\forall_{\alpha\in V}, \forall_{a,b\in K}$	$(a + b) \otimes \alpha = (a \otimes \alpha) \oplus (b \otimes \alpha)$	*rozdzielność* $\otimes$ *względem* $+$
$\forall_{\alpha,\beta\in V}, \forall_{a\in K}$	$a \otimes (\alpha \oplus \beta) = (a \otimes \alpha) \oplus (a \otimes \beta)$	*rozdzielność* $\otimes$ *względem* $\oplus$

Jak widać, w definicji wystąpiło mnóstwo oznaczeń, zwłaszcza odnośnie działań. Gdy już przyzwyczaimy się do nowego pojęcia, wszystkie symbole dodawania $\oplus, +$ będą zamienione na $+$ oraz wszystkie symbole mnożenia $\cdot, \otimes$ będą pomijane. Jak się okaże jest to niezbędne do „higienicznej pracy" z przestrzeniami liniowymi i rzadko (wcale?) doprowadzi nas do błędu. Dziś skupimy się głównie na przykładach.

W przedstawionej wyżej definicji występują działania na różnych strukturach: dwa działania w ciele K, a także (nowe) działanie dodawania wektorów w V. Pojawia się również operacja, która wykracza poza dotychczasową definicję działania; określona na parach elementów, których współrzędne pochodzą z różnych zbiorów: mnożenie wektora przez skalar. Treść poszczególnych aksjomatów odzwierciedla własności wspominane na wykładzie o działaniach. Dodawanie w zbiorze wektorów spełnia cztery aksjomaty analogiczne[1] do tych, które dotyczą dodawania w ciele. Kolejne cztery aksjomaty dotyczą zgodności mnożenia wektora przez skalar z działaniami w K i w V.

Przykład 1. *Niech* K^n *oznacza zbiór wszystkich ciągów* n*-elementowych o wyrazach z ciała* K*, to znaczy:*

$$K^n = \{(x_1, x_2, \ldots, x_n) \,|\, x_i \in K, i = 1, 2, \ldots, n\}.$$

Wyraz x_i *w ciągu* $(x_1, x_2, \ldots, x_n)$ *nazywamy* i***-tą współrzędną*** *tego wektora.*
Działania w K^n *określone są w sposób naturalny wzorami:*

- $(x_1, x_2, \ldots, x_n) \oplus (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$,
- $a \otimes (x_1, x_2, \ldots, x_n) = (a \cdot x_1, a \cdot x_2, \ldots, a \cdot x_n)$.

Wówczas K^n *jest przestrzenią liniową z wektorem zerowym* $(0, 0, \ldots, 0)$.

Czy widzicie Państwo, że dodawanie wektorów, to inne dodawanie niż dodawanie wewnątrz współrzędnej odpowiedniego wektora sumy, które jest dodawaniem w ciele? Podobnie – mnożenie wektora przez skalar to co innego niż mnożenie elementów na konkretnej współrzędnej, które jest mnożeniem w ciele K.

Przykłady działań w przestrzeni K^n:

- dla $K = \mathbb{Z}_3$ i $n = 4$ mamy np. $(1, 2, 1, 2) + (0, 2, 2, 1) = (1, 1, 0, 0), \quad 2 \cdot (2, 2, 1, 1) = (1, 1, 0, 0)$,
- dla $K = \mathbb{C}$ i $n = 2$ mamy np. $(1, i) + i(i, 0) = (1, i) + (-1, 0) = (0, i)$.

[1] Mówimy, że zbiór wektorów V z operacją $\oplus$ oraz elementem neutralnym Θ jest grupą przemienną (abelową).

Przykład 2. *Niech $M_{m\times n}(K)$ oznacza zbiór wszystkich macierzy $m \times n$ o wyrazach z ciała K.*

- *Sumą macierzy $[a_{ij}]$ oraz $[b_{ij}]$ nazywamy macierz $[c_{ij}]$, gdzie $c_{ij} = a_{ij} + b_{ij}$:*

$$\begin{bmatrix} & \vdots & \\ \cdots & a_{ij} & \cdots \\ & \vdots & \end{bmatrix} + \begin{bmatrix} & \vdots & \\ \cdots & b_{ij} & \cdots \\ & \vdots & \end{bmatrix} = \begin{bmatrix} & \vdots & \\ \cdots & a_{ij} + b_{ij} & \cdots \\ & \vdots & \end{bmatrix}.$$

- *Iloczynem macierzy $[d_{ij}]$ przez skalar $c \in K$ nazywamy macierz $[c \cdot d_{ij}]$:*

$$c \cdot \begin{bmatrix} & \vdots & \\ \cdots & d_{ij} & \cdots \\ & \vdots & \end{bmatrix} = \begin{bmatrix} & \vdots & \\ \cdots & c \cdot d_{ij} & \cdots \\ & \vdots & \end{bmatrix}.$$

Wektorem zerowym w przestrzeni liniowej $M_{m\times n}(K)$ jest ***macierz zerowa*** *rozmiarów $m \times n$.*

Przykładowo, w przestrzeni liniowej $M_{2\times 3}(\mathbb{Z}_5)$ (ponownie $\oplus$ i $\otimes$ zastępujemy jako $+$ oraz $\cdot$):

$$\begin{bmatrix} 1 & 3 & 2 \\ 0 & 0 & 2 \end{bmatrix} + 2 \cdot \begin{bmatrix} 4 & 4 & 0 \\ 0 & 4 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 3 & 2 \\ 0 & 0 & 2 \end{bmatrix} + \begin{bmatrix} 3 & 3 & 0 \\ 0 & 3 & 4 \end{bmatrix} = \begin{bmatrix} 4 & 1 & 2 \\ 0 & 3 & 1 \end{bmatrix}.$$

Przykład 3. *Oznaczmy przez K^∞ zbiór wszystkich ciągów o wyrazach z ciała K, to znaczy:*

$$K^\infty = \{(x_i) \,|\, x_i \in K, i = 1, 2, \ldots\}.$$

Ciągi $x = (x_i)$ oraz $y = (y_i)$ dodajemy i mnożymy przez skalary według zasady:

$$(x \oplus y)_i = x_i + y_i, \quad (a \otimes x)_i = a \cdot x_i.$$

Wektorem zerowym w przestrzeni liniowej K^∞ jest ciąg, którego wszystkie wyrazy są zerem w ciele K.

Przykładowo, z równości:

$$\frac{1}{n} + (-1)\frac{1}{n+1} = \frac{1}{n(n+1)},$$

zachodzącej dla każdej dodatniej liczby całkowitej n mamy równość w $\mathbb{Q}^\infty$ postaci

$$\left(\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \ldots\right) - \left(\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\right) = \left(\frac{1}{2}, \frac{1}{6}, \frac{1}{12}, \ldots\right).$$

Przykład 4. *Niech $K[x]$ będzie zbiorem wszystkich wielomianów zmiennej x o współczynnikach w ciele K, czyli $K[x] = \{a_0 + a_1x + \ldots + a_nx^n \,|\, n = \mathbb{N} \cup \{0\}, a_0, a_1, \ldots, a_n \in K\}$. Dodawanie i mnożenie przez skalar pochodzą od omawianych tydzień wcześniej operacji na wielomianach. Wektorem zerowym w przestrzeni liniowej $K[x]$ jest wielomian zerowy.*

Przykład 5. *Niech $F(X, K)$ będzie zbiorem wszystkich funkcji z danego niepustego zbioru X do ciała K. Dla $f, g \in F(X, K)$ i dla $a \in K$ funkcje $f + g$ oraz af określone są warunkami:*

$$(f + g)(x) = f(x) + g(x), \quad (af)(x) = af(x).$$

Wektor zerowy przestrzeni liniowej $F(X, K)$ to funkcja stale równa 0.

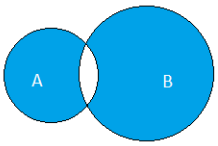
Przykład 6. *Jeśli K jest ciałem i L jest podciałem ciała K, to K ma strukturę przestrzeni liniowej nad ciałem L. Elementy ciała K można traktować jako wektory, zaś L jako skalary. Przykłady:*

- *przestrzeń $\mathbb{C}$ nad ciałem $\mathbb{R}$,*
- *przestrzeń $\mathbb{Q}(\sqrt{2})$ nad ciałem $\mathbb{Q}$,*
- *przestrzeń $\mathbb{R}$ nad ciałem $\mathbb{Q}$ (bardzo skomplikowana!),*
- *ciało o p^n elementach jest p. liniową nad ciałem $\mathbb{Z}_p$, gdzie p – liczba pierwsza.*

Podajmy jeszcze dwa przykłady o wielkim znaczeniu w kombinatoryce.

Przykład 7. *Niech X będzie zbiorem niepustym, zaś $P(X)$ – zbiorem podzbiorów zbioru X. Na zbiorze $P(X)$ określamy strukturę przestrzeni liniowej nad ciałem $\mathbb{Z}_2$.*

Operacja $\triangle$ dodawania wektorów określona jest w sposób następujący dla dowolnych $A, B \in P(X)$ jako ich tzw. różnica symetryczna $A \triangle B = A \cup B \setminus (A \cap B)$.



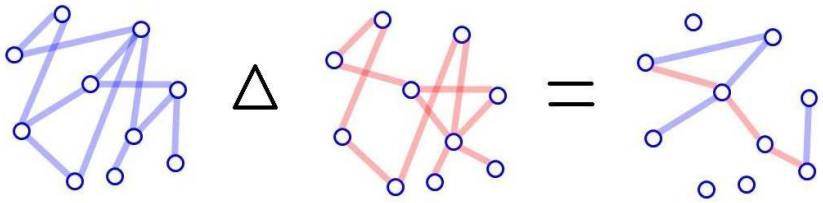
Rysunek 1. *Różnica symetryczna dwóch podzbiorów płaszczyzny.*

Co więcej, dla każdego $A \in P(X)$ definiujemy mnożenie wektora A przez skalar (jeden z dwóch w $\mathbb{Z}_2$):

- $0 \otimes A = \emptyset$ *– zbiór pusty*
- $1 \otimes A = A$.

Przykład 8. *Niech X będzie skończonym zbiorem niepustym, E zaś niech będzie podzbiorem zbioru par nieuporządkowanych zbioru X. Parę $G = (X, E)$ nazwiemy **grafem niezorientowanym** o zbiorze wierzchołków X i zbiorze krawędzi E. Jeśli $\{a, b\} \in E$ to mówimy, że między wierzchołkami a, b grafu G jest krawędź.*

*Określamy przestrzeń liniową $P(E)$ nad ciałem $\mathbb{Z}_2$, zwaną **przestrzenią krawędziową** grafu G, jak w poprzednim przykładzie.*



Rysunek 2. *Różnica symetryczna dwóch podzbiorów krawędzi grafu*

Sprawdzenie, że powyższe dwa przykłady opisują przestrzeń liniową wymaga odrobiny wysiłku, ale jest rutynowym ćwiczeniem. Na razie przestrzeń ta może wydawać się bardzo dziwna, ale poznamy jeszcze pewne jej ciekawe zastosowania. Na marginesie pytanie: jaki jest element przeciwny do danego zbioru krawędzi grafu?

Podobnie jak w przypadku ciał, podstawowym narzędziem do uzyskiwania kolejnych przykładów przestrzeni liniowych jest pojęcie podprzestrzeni liniowej. Będzie ono dla nas na tym wykładzie znacznie ważniejsze niż pojęcie podciała. Zobaczymy też całkiem niedługo w jaki sposób tego typu „podstruktury" wykorzystuje się w matematyce do uzyskiwania rozmaitych konstrukcji i rezultatów.

Definicja 2. *Niepusty podzbiór $W \subset V$ nazywamy **podprzestrzenią przestrzeni liniowej** V jeśli dla każdych $\alpha, \beta \in W$ oraz każdego $a \in K$ zachodzi:*

- $\alpha + \beta \in W$,
- $a \cdot \alpha \in W$.

*W każdej przestrzeni liniowej V podzbiór $\{0\}$, złożony tylko z wektora zerowego, jest jej podprzestrzenią. Nazywamy ją **podprzestrzenią zerową**. Mówimy, że przestrzeń liniowa V jest **przestrzenią zerową**, jeśli składa się tylko z wektora zerowego.*

UWAGA: Podprzestrzeń przestrzeni liniowej jest przestrzenią liniową (z działaniami pochodzącymi z V, w tym z odziedziczonym wektorem zerowym). **Wektor zerowy należy do każdej podprzestrzeni!**

Zobaczmy kilka przykładów.

Przykład 9. *W każdej przestrzeni liniowej V podzbiór $\{0\}$, złożony tylko z wektora zerowego, jest jej podprzestrzenią. Nazywamy ją* ***podprzestrzenią zerową****.*

Przejdźmy do kluczowego przykładu podprzestrzeni, który już poznaliśmy:

Przykład 10. *Rozpatrzmy jednorodny układ równań liniowych o współczynnikach w ciele K:*

$$U: \begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = 0 \\ a_{31}x_1 + a_{32}x_2 + \ldots + a_{3n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = 0. \end{cases}$$

Zbiór wszystkich rozwiązań układu U jest podprzestrzenią przestrzeni liniowej K^n.

Warto przypomnieć w tym miejscu obserwację poczynioną w materiałach uzupełniających pierwszy wykład. Mówi ona, że do zbioru rozwiązań **dowolnego** układu równań jednorodnych, który ma rozwiązania $(1,2,3,4,5)$ oraz $(2,0,0,1,0)$ należące do przestrzeni liniowej $\mathbb{R}^5$ należą też:

(a) każdy element $\lambda_1 \cdot (1,2,3,4,5) = (\lambda_1 \cdot 1, \lambda_1 \cdot 2, \lambda_1 \cdot 3, \lambda_1 \cdot 4, \lambda_1 \cdot 5)$,

(b) każdy element $\lambda_2 \cdot (2,0,0,1,0) = (\lambda_2 \cdot 2, \lambda_2 \cdot 0, \lambda_2 \cdot 0, \lambda_2 \cdot 1, \lambda_2 \cdot 0)$,

(c) każda kombinacja $\lambda_1 \cdot (1,2,3,4,5) + \lambda_2 \cdot (2,0,0,1,0)$ tych wektorów, czyli

$$(\lambda_1 \cdot 1 + \lambda_2 \cdot 2, \lambda_1 \cdot 2 + \lambda_2 \cdot 0, \lambda_1 \cdot 3 + \lambda_2 \cdot 0, \lambda_1 \cdot 4 + \lambda_2 \cdot 1, \lambda_1 \cdot 5 + \lambda_2 \cdot 0).$$

Przykład 11. *Dla każdej liczby naturalnej m niech $K_m[x]$ oznacza zbiór wszystkich wielomianów stopnia co najwyżej m w $K[x]$. Jest to podprzestrzeń $K[x]$.*

Przykład 12. *W przestrzeni ciągów $\mathbb{R}^\infty$ wskazać można bardzo wiele podprzestrzeni, np.:*

- *ciągi mające skończenie wiele niezerowych wyrazów,*
- *ciągi ograniczone,*
- *ciągi zbieżne,*
- *ciągi $(x_i)_{i=1}^\infty$ spełniające $\sum_{i=1}^{\infty} x_i^2 < \infty$.*
- *ciągi $(x_i)_{i=1}^\infty$ spełniające określone rekurencje liniowe, np. $x_{n+2} = x_{n+1} + x_n$.*

Przykład 13. *Przykłady podprzestrzeni w przestrzeni funkcji $F(K,K)$:*

- *funkcje parzyste, spełniające równanie $f(x) = f(-x)$, dla $x \in K$,*
- *funkcje nieparzyste, spełniające równanie $f(x) = -f(-x)$, dla $x \in K$,*
- *nad $\mathbb{R}$ (i nie tylko): funkcje ograniczone, monotoniczne itd.*
- *funkcje będące rozwiązaniami równania Cauchy'ego[2], tzn. dla każdych $x, y \in K$:*

$$f(x+y) = f(x) + f(y),$$

[2]To słynne równanie funkcyjne rozważane dla funkcji rzeczywistych badane było przez wielkich matematyków, jak Cauchy, Darboux, d' Alembert i inni. Przy niewielu dodatkowych założeniach można pokazać, że jego rozwiązaniami są jedynie funkcje postaci $f(x) = ax$, dla $a \in \mathbb{R}$. Do tych „drobnych" dodatkowych założeń należą: ciągłość (Cauchy, 1821), ciągłość w punkcie (Darboux, 1875), monotoniczność lub ograniczoność na dowolnym przedziale (Darboux, 1880). W 1905 roku Georg Hamel pokazał, używając aksjomatu wyboru, że bez przyjęcia tego typu założeń o regularności wskazać można znacznie bardziej skomplikowane i egzotyczne funkcje spełniające równanie Cauchy'ego. Wspomnijmy o tym jeszcze raz – przestrzeń liniowa $\mathbb{R}$ nad $\mathbb{Q}$ jest niezwykle skomplikowana. Na czym to polega powiemy po kolejnym wykładzie.

Powiemy teraz o bardzo ważnym typie konstrukcji związanych z podprzestrzeniami. Chodzi o sytuację, gdy mamy przestrzeń liniową i szukamy takiej jej podprzestrzeni, która zawierałaby z góry określone przez nas wektory – wybranej przy tym możliwie oszczędnie. Taką dokładnie sytuację opisaliśmy wyżej, znajdując najmniejszą możliwą podprzestrzeń zawierającą pewne dwa rozwiązania układu równań jednorodnych nad $\mathbb{R}$. Co to znaczy „oszczędnie"? Ano chcemy, by każda inna podprzestrzeń, która zawiera wybrane wektory, zawierała i całą „oszczędnie wybraną" podprzestrzeń.

Definicja 3. *Niech V będzie przestrzenią liniową nad ciałem K.* ***Kombinacją liniową*** *układu wektorów $\alpha_1, \ldots, \alpha_k$ o współczynnikach $a_1, \ldots, a_k \in K$ nazywamy wektor:*

$$\beta = a_1\alpha_1 + \ldots + a_k\alpha_k = \sum_{i=1}^{k} a_i\alpha_i.$$

Przykłady.

- W przestrzeni $V = \mathbb{R}^4$ kombinacją liniową wektorów $(2, 1, -3, 4), (0, 2, 5, 1), (7, 4, 3, 2)$ ze współczynnikami $2, -1, 1$ jest wektor

$$2(2, 1, -3, 4) - 1(0, 2, 5, 1) + 1(7, 4, 5, 2) = (11, 4, -8, 9).$$

- W przestrzeni funkcji $F(\mathbb{R}, \mathbb{R})$ kombinacją liniową wektorów $\sin(x)$ oraz $\cos(x)$ o współczynnikach $\frac{1}{\sqrt{2}}$ oraz $-\frac{1}{\sqrt{2}}$ jest funkcja

$$\frac{1}{\sqrt{2}}\sin(x) - \frac{1}{\sqrt{2}}\cos(x) = \sin(x - \frac{\pi}{4}).$$

- Wektor $(0, 3, 1) \in \mathbb{R}^3$ nie jest kombinacją liniową wektorów $(0, 1, 1), (-1, 0, 1)$, bo założenie, że

$$(0, 3, 1) = a(0, 1, 1) + b(-1, 0, 1)$$

prowadzi do układu równań $0 = -b$, $3 = a$, $1 = a + b$, który nie ma rozwiązań.

Uwaga 1. *Niech $\alpha_1, \ldots, \alpha_k$ będą wektorami przestrzeni liniowej V nad K. Jeśli wektory β, γ są kombinacjami liniowymi wektorów $\alpha_1, \ldots, \alpha_k$, to wektory $\beta + \gamma$ oraz $a\beta$, dla każdego $a \in K$, również są kombinacjami liniowymi wektorów $\alpha_1, \ldots, \alpha_k$.*

Definicja 4. *Niech V będzie przestrzenią liniową nad ciałem K i niech $\alpha_1, \ldots, \alpha_k \in V$. Wówczas przez $\mathrm{lin}(\alpha_1, \ldots, \alpha_k)$ oznaczamy zbiór wszystkich kombinacji liniowych wektorów $\alpha_1, \ldots, \alpha_k$.*

Przykład. Zbiór rozwiązań jednorodnego układu równań liniowych o współczynnikach rzeczywistych postaci:

$$\begin{cases} x_1 + x_2 + x_3 + x_4 &= 0 \\ x_1 - x_2 - x_3 - x_4 &= 0 \end{cases}$$

to podprzestrzeń przestrzeni $\mathbb{R}^4$ złożona z czwórek postaci:

$$(0, -s - t, s, t), \text{gdzie } s, t \in \mathbb{R},$$

czyli podprzestrzeń postaci:

$$\mathrm{lin}((0, -1, 1, 0), (0, -1, 0, 1)),$$

bo dla dowolnych $s, t \in \mathbb{R}$ mamy:

$$(0, -s - t, s, t) = (0, -s, s, 0) + (0, -t, 0, t) = s(0, -1, 1, 0) + t(0, -1, 0, 1).$$

Uwaga 2. *Zbiór $\mathrm{lin}(\alpha_1, \ldots, \alpha_k)$ jest podprzestrzenią przestrzeni V. Podprzestrzeń ta jest najmniejszą podprzestrzenią V (względem inkluzji) zawierającą wektory $\alpha_1, \ldots, \alpha_k$.*

Dowód. Z poprzedniej uwagi wynika, że $\mathrm{lin}(\alpha_1, \ldots, \alpha_k)$ jest podprzestrzenią w V. Niech W będzie dowolną podprzestrzenią zawierającą wektory $\alpha_1, \ldots, \alpha_k$. Z definicji podprzestrzeni W zawiera każdą kombinację liniową wektorów $\alpha_1, \ldots, \alpha_k$, czyli każdy wektor z $\mathrm{lin}(\alpha_1, \ldots, \alpha_k)$. Stąd $\mathrm{lin}(\alpha_1, \ldots, \alpha_k) \subseteq W$. □

Definicja 5. *Niech $\alpha_1, \ldots, \alpha_k$ będzie układem wektorów w V. Wówczas podprzestrzeń liniową $\mathrm{lin}(\alpha_1, \ldots, \alpha_k)$ nazywamy* ***przestrzenią rozpiętą na układzie*** *$\alpha_1, \ldots, \alpha_k$. Mówimy, że układ $\alpha_1, \ldots, \alpha_k$* ***rozpina przestrzeń*** *V, jeśli $V = \mathrm{lin}(\alpha_1, \ldots, \alpha_k)$, to znaczy każdy wektor z V jest kombinacją liniową wektorów $\alpha_1, \ldots, \alpha_k$.*

Przy badaniu przestrzeni rozpiętych na układach wektorów w K^n (czyli do rozwiązywania wielu fascynujących zadań o podprzestrzeniach przestrzeni K^n) użyteczna jest następująca prosta obserwacja.

Definicja 6. *Niech $A \in M_{m\times n}(K)$ będzie macierzą o wyrazach a_{ij}, dla $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$. Wówczas:*

- *przez podprzestrzeń wierszową $W(A)$ rozumieć będziemy podprzestrzeń K^n rozpiętą przez wektory:*

$$(a_{11}, a_{12}, \ldots, a_{1n}), (a_{21}, a_{22}, \ldots, a_{2n}), \ldots, (a_{m1}, a_{m2}, \ldots, a_{mn}).$$

- *przez podprzestrzeń kolumnową $K(A)$ rozumieć będziemy podprzestrzeń K^m rozpiętą przez wektory:*

$$(a_{11}, a_{21}, \ldots, a_{m1}), (a_{12}.a_{22}, \ldots, a_{m2}), \ldots, (a_{1n}, a_{2n}, \ldots, a_{mn}).$$

Uwaga 3. *Niech $A, A' \in M_{m\times n}(K)$ oraz niech*

- $\alpha_1, \ldots, \alpha_m$ – *wiersze macierzy A,*
- $\alpha'_1, \ldots, \alpha'_m$ – *wiersze macierzy A'.*

Jeśli założymy, że A' może być otrzymana z A za pomocą ciągu operacji elementarnych na wierszach, to wynika stąd, że

$$\lin(\alpha_1, \ldots, \alpha_m) = \lin(\alpha'_1, \ldots, \alpha'_m).$$

Dowód. Wystarczy pokazać tezę w przypadku, gdy A' powstaje z A przez wykonanie pojedynczej operacji elementarnej na wierszach. Wykażemy tezę jedynie w najtrudniejszym przypadku. Pokazujemy mianowicie, że dla dowolnych $1 \leqslant i, j \leqslant m$ oraz dowolnego $a \in K$ mamy:

$$\lin(\alpha_1, \ldots, \alpha_i, \ldots, \alpha_j, \ldots, \alpha_m) = \lin(\alpha_1, \ldots, \alpha_i, \ldots, a \cdot \alpha_i + \alpha_j, \ldots, \alpha_m).$$

Weźmy $\beta \in \lin(\alpha_1, \ldots, \alpha_i, \ldots, \alpha_j, \ldots, \alpha_m)$. Istnieją $b_1, b_2, \ldots, b_m \in K$, że:

$$\begin{aligned}\beta &= b_1\alpha_1 + b_2\alpha_2 + \ldots + b_i\alpha_i + \ldots + b_j\alpha_j + \ldots + b_m\alpha_m = \\ &= b_1\alpha_1 + b_2\alpha_2 + \ldots + (b_i - a \cdot b_j)\alpha_i + \ldots + b_j(a\alpha_i + \alpha_j) + \ldots + b_m\alpha_m.\end{aligned}$$

Zatem $\beta \in \lin(\alpha_1, \ldots, \alpha_i, \ldots, a \cdot \alpha_i + \alpha_j, \ldots, \alpha_m)$.

Weźmy teraz $\gamma \in \lin(\alpha_1, \ldots, \alpha_i, \ldots, a \cdot \alpha_i + \alpha_j, \ldots, \alpha_m)$. Istnieją $c_1, c_2, \ldots, c_m \in K$, że:

$$\begin{aligned}\gamma &= c_1\alpha_1 + c_2\alpha_2 + \ldots + c_i\alpha_i + \ldots + c_j(a \cdot \alpha_i + \alpha_j) + \ldots + c_m\alpha_m = \\ &= c_1\alpha_1 + c_2\alpha_2 + \ldots + (c_i + a \cdot c_j)\alpha_i + \ldots + c_j\alpha_j + \ldots + c_m\alpha_m.\end{aligned}$$

Zatem $\gamma \in \lin(\alpha_1, \ldots, \alpha_i, \ldots, \alpha_j, \ldots, \alpha_m)$. □

Wykład zakończymy uwagą dotyczącą układów rozpinanych przez nieskończenie wiele elementów. Bez narzędzi analitycznych nie jest możliwe rozważanie sum nieskończonych. Mimo to przyjąć można następującą definicję.

Definicja 7. *Niech $X = \{\alpha_t\}_{t\in T}$ będzie dowolnym układem wektorów przestrzeni V. Wówczas przez $\lin(X)$ oznaczamy zbiór wszystkich kombinacji liniowych* ***skończonych podukładów*** *układu X. To znaczy:*

$$\beta \in \lin(X) \iff \beta = \sum_{i=1}^{k} a_i\alpha_{t_i}, \text{ dla pewnych } a_1, \ldots, a_k \in K, \alpha_{t_1}, \ldots, \alpha_{t_k} \in X.$$

Jeśli $V = \lin(X)$ to mówimy, że układ X rozpina V i przestrzeń V jest rozpięta na X. Dla układu pustego $X = \emptyset$ przyjmujemy $\lin(X) = \{0\}$.

Przykłady:

- $V = \lin(V)$,
- $K[x] = \lin(1, x, x^2, x^3, \ldots)$,
- problem: „wypisać"' najmniejszy taki zbiór X, by $\mathbb{R} = \lin(X)$, gdzie $\mathbb{R}$ – przestrzeń nad $\mathbb{Q}$.

Pojęcie przestrzeni liniowej to pierwszy krok w kierunku uzyskania nowej geometrycznej perspektywy na rozmaite obiekty matematyczne. Na kolejnym wykładzie zastanowimy się nad fundamentalnym problemem: ile elementów z przestrzeni liniowej rozpiętej przez n wektorów musimy znać, aby przestrzeń ta była wyznaczona jednoznacznie oraz jakie własności mają takie „minimalne układy rozpinające".

Uzupełnienie. Kombinacje liniowe i układy równań

Jedną z przestrzeni liniowych poznanych na wykładzie jest przestrzeń macierzy o m wierszach i n kolumnach o wyrazach z ciała K. Nietrudno zauważyć, że dodawanie macierzy lub mnożenie ich przez skalar są w zasadzie identyczne z operacjami wprowadzonymi w przestrzeni $K^{m\cdot n}$. Aby to unaocznić weźmy na przykład sumę macierzy w $M_{2\times 3}(\mathbb{Q})$ oraz sumę wektorów w $\mathbb{Q}^6$ postaci:

$$\begin{bmatrix}1&2&3\\4&5&6\end{bmatrix}+\begin{bmatrix}6&5&4\\3&2&1\end{bmatrix}=\begin{bmatrix}7&7&7\\7&7&7\end{bmatrix},\quad (1,2,3,4,5,6)+(6,5,4,3,2,1)=(7,7,7,7,7,7).$$

Wkrótce poznamy język, który pozwoli nam powiedzieć, że z punktu widzenia „struktury" przestrzeni liniowych przestrzenie $M_{2\times 3}(\mathbb{Q})$ oraz $\mathbb{Q}^6$ w zasadzie niczym się nie różnią – są **izomorficzne**. Dlaczego więc rozróżniamy te dwie przestrzenie? Macierze okazały się wygodnym narzędziem do badania układów równań. Jak niedługo zobaczymy, są one również wygodnym narzędziem do badania przekształceń pomiędzy przestrzeniami liniowymi. Jest jeden przypadek, gdy utożsamienie wektorów z macierzami wykonać można bez żadnych dodatkowych umów: gdy rozważamy macierze o jednym wierszu lub jednej kolumnie. Zajmiemy się teraz drugą sytuacją.

Zapiszmy równań liniowych nad $\mathbb{R}$ za pomocą operacji w $M_{3\times 1}(\mathbb{R})$:

$$\begin{cases}x\quad -z&=0\\2x+y&=0\\3x+y+z&=0\end{cases}\quad\Rightarrow\quad x\cdot\begin{bmatrix}1\\2\\3\end{bmatrix}+y\cdot\begin{bmatrix}0\\1\\1\end{bmatrix}+z\cdot\begin{bmatrix}-1\\0\\1\end{bmatrix}=\begin{bmatrix}0\\0\\0\end{bmatrix}.$$

Widzimy zatem, że rozwiązanie układu równań sprowadza się do sprawdzenia, czy pewna macierz rozmiaru 3×1 jest kombinacją liniową pewnych trzech macierzy ze współczynnikami x,y,z. Jest jednak jasne, że w istocie jest to zagadnienie równoważne z przedstawieniem wektora $(0,0,0)\in\mathbb{R}^3$ jako kombinacji liniowej wektorów $(1,2,3),(0,1,1),(-1,0,1)$. Często mówimy nawet, że wektory te zapisane zostały w równaniu wyżej w notacji kolumnowej. A zatem w dalszym ciągu często dokonywać będziemy utożsamienia elementów K^n oraz przestrzeni macierzy $M_{1\times n}(K)$ oraz $M_{n\times 1}(K)$ mówiąc przy tym, że wektor $v\in K^n$ zapisujemy w formie kolumnowej v^T lub wierszowej v.

Rozwiązywanie układów równań przez poszukiwanie kombinacji liniowych nie przyspieszy samego procesu rozwiązywania (dalej stosować będziemy metodę Gaussa), ale pozwoli nam zadać kilka istotnych pytań. Wróćmy do układu wyżej i zapytajmy: czy jeśli zamienimy wektor $(0,0,0)$ na dowolny inny, układ pozostanie niesprzeczny? A zatem: czy dowolny wektor $(a,b,c)\in\mathbb{R}^3$ jest kombinacją liniową wektorów $(1,2,3),(0,1,1),(-1,0,1)$? Zupełnie wprost: czy dla każdych a,b,c istnieją x,y,z takie, że

$$x\cdot\begin{bmatrix}1\\2\\3\end{bmatrix}+y\cdot\begin{bmatrix}0\\1\\1\end{bmatrix}+z\cdot\begin{bmatrix}-1\\0\\1\end{bmatrix}=\begin{bmatrix}a\\b\\c\end{bmatrix}?$$

Skąd mamy wiedzieć coś takiego i jak wyznaczyć x,y,z? Okazuje się, że nie jest to trudne. W języku kombinacji liniowych nasze pytanie brzmi: czy dowolny wektor z $\mathbb{R}^3$ jest kombinacją liniową wektorów $(1,2,3),(0,1,1),(-1,0,1)$? W skrócie, pytamy o prawdziwość równości:

$$\operatorname{lin}((1,2,3),(0,1,1),(-1,0,1))=\mathbb{R}^3.$$

Czy to może być prawda? Nietrudno się przekonać, że tak jest: twierdzenie wykazane na wykładzie mówi, że wpisując powyższe trzy wektory w wiersze możemy wykonywać operacje wierszowe i przekonać się, że ciągiem operacji elementarnych na wierszach macierz

$$\begin{bmatrix}1&2&3\\0&1&1\\-1&0&1\end{bmatrix}$$

sprowadzić można do macierzy:

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

Jest natomiast jasne, że $\operatorname{lin}((1,0,0),(0,1,0),(0,0,1))=\mathbb{R}^3$, bo dla każdego $(a,b,c)\in\mathbb{R}^3$ mamy $(a,b,c)=a(1,0,0)+b(0,1,0)+c(0,0,1)$.

A zatem odpowiedzieliśmy na pytanie o rozwiązywalność dowolnego układu niejednorodnego o pewnej konkretnej macierzy współczynników. A jak wygląda rozwiązanie dla konkretnych a, b, c? Zobaczmy nasz układ w jeszcze innej postaci:

$$x \cdot \begin{bmatrix}1\\2\\3\end{bmatrix} + y \cdot \begin{bmatrix}0\\1\\1\end{bmatrix} + z \cdot \begin{bmatrix}-1\\0\\1\end{bmatrix} = a \begin{bmatrix}1\\0\\0\end{bmatrix} + b \begin{bmatrix}0\\1\\0\end{bmatrix} + c \begin{bmatrix}0\\0\\1\end{bmatrix}$$

Przypomnijmy, że jeśli zaczniemy wykonywać jednocześnie te same operacje na wierszach następujących macierzy:

$$\begin{bmatrix}1 & 0 & -1\\2 & 1 & 0\\3 & 1 & 1\end{bmatrix}, \quad \begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix},$$

wówczas kombinacje liniowe ich kolumn ze współczynnikami x, y, z oraz a, b, c będą nadal równe! Zobaczmy to. Wykonajmy dwie operacje na obydwu macierzach:

$$\begin{bmatrix}1 & 0 & -1\\2 & 1 & 0\\3 & 1 & 1\end{bmatrix} \longrightarrow \begin{bmatrix}1 & 0 & -1\\0 & 1 & 2\\3 & 1 & 1\end{bmatrix} \longrightarrow \begin{bmatrix}1 & 0 & -1\\0 & 1 & 2\\0 & 1 & 4\end{bmatrix}, \quad \begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix} \longrightarrow \begin{bmatrix}1 & 0 & 0\\-2 & 1 & 0\\0 & 0 & 1\end{bmatrix} \longrightarrow \begin{bmatrix}1 & 0 & 0\\-2 & 1 & 0\\-3 & 0 & 1\end{bmatrix}$$

Mamy:

$$x \cdot \begin{bmatrix}1\\0\\0\end{bmatrix} + y \cdot \begin{bmatrix}0\\2\\1\end{bmatrix} + z \cdot \begin{bmatrix}-1\\2\\4\end{bmatrix} = a \begin{bmatrix}1\\-2\\-3\end{bmatrix} + b \begin{bmatrix}0\\1\\0\end{bmatrix} + c \begin{bmatrix}0\\0\\1\end{bmatrix}$$

Czy Czytelnik widzi, że kontynuując proces schodkowania macierzy wyjściowego układu równań dojdziemy w końcu do postaci pozwalającej wyznaczyć x, y, z za pomocą a, b, c? Kontynuujmy eliminację, tym razem zapisując już macierze obok siebie:

$$\begin{bmatrix}1 & 0 & -1 & 1 & 0 & 0\\0 & 1 & 2 & -2 & 1 & 0\\0 & 1 & 4 & -3 & 0 & 1\end{bmatrix} \longrightarrow \left[\begin{array}{ccc|ccc}1 & 0 & -1 & 1 & 0 & 0\\0 & 1 & 2 & -2 & 1 & 0\\0 & 0 & 6 & -1 & -1 & 1\end{array}\right]$$

$$\longrightarrow \left[\begin{array}{ccc|ccc}1 & 0 & -1 & 1 & 0 & 0\\0 & 1 & 2 & -2 & 1 & 0\\0 & 0 & 1 & -\frac{1}{6} & -\frac{1}{6} & \frac{1}{6}\end{array}\right]$$

$$\longrightarrow \left[\begin{array}{ccc|ccc}1 & 0 & 0 & \frac{5}{6} & -\frac{1}{6} & \frac{1}{6}\\0 & 1 & 0 & -\frac{10}{6} & \frac{4}{6} & \frac{2}{6}\\0 & 0 & 1 & -\frac{1}{6} & -\frac{1}{6} & \frac{1}{6}\end{array}\right]$$

A zatem mamy:

$$x \cdot \begin{bmatrix}1\\0\\0\end{bmatrix} + y \cdot \begin{bmatrix}0\\1\\0\end{bmatrix} + z \cdot \begin{bmatrix}0\\0\\1\end{bmatrix} = a \begin{bmatrix}\frac{5}{6}\\-\frac{5}{3}\\-\frac{1}{6}\end{bmatrix} + b \begin{bmatrix}-\frac{1}{6}\\\frac{2}{3}\\-\frac{1}{6}\end{bmatrix} + c \begin{bmatrix}\frac{1}{6}\\\frac{1}{3}\\\frac{1}{6}\end{bmatrix}$$

Po uproszczeniu:

$$\begin{bmatrix}x\\y\\z\end{bmatrix} = \begin{bmatrix}\frac{5}{6}a - \frac{1}{6}b + \frac{1}{6}c\\-\frac{5}{3}a + \frac{2}{3}b + \frac{1}{3}c\\-\frac{1}{6}a - \frac{1}{6}b + \frac{1}{6}c\end{bmatrix}.$$

Wracając do wyjściowego problemu widzimy, że rozwiązaniem układu:

$$\begin{cases} x \quad - z & = a\\ 2x + y & = b\\ 3x + y + z & = c \end{cases}$$

jest trójka:

$$\left(\frac{5}{6}a - \frac{1}{6}b + \frac{1}{6}c, \quad -\frac{5}{3}a + \frac{2}{3}b + \frac{1}{3}c, \quad -\frac{1}{6}a - \frac{1}{6}b + \frac{1}{6}c\right).$$

Jeśli Czytelnik dotrwał do tego momentu, to gratuluję: odwróciliśmy właśnie wspólnie pierwszą macierz. Nie wiemy na razie co to znaczy, ale sam termin „odwrócenia" powinien rodzić jasne skojarzenia. Rozpisaliśmy ustalony wektor jako kombinację liniową trzech zadanych z góry wektorów. Nie zawsze będzie to jednak możliwe. Proszę zauważyć, że gdyby zamiast wektorów $(1, 2, 3), (0, 1, 1), (-1, 0, 1)$ szukać kombinacji liniowych wektorów: $(1, 2, 3), (2, 4, 6), (-1, 0, 1)$, to nie każdy wektor $\mathbb{R}^3$ byłby ich kombinacją liniową. Inaczej mówiąc $\operatorname{lin}((1, 2, 3), (2, 4, 6), (-1, 0, 1)) \neq \mathbb{R}^3$. Sprawom tym przyjrzymy się już na następnym wykładzie.

Dodatek. Kody samokorekcyjne.

Nie sposób opisać wszystkich zastosowań przestrzeni liniowych. W naszym wykładzie zajmować się będziemy w dużej mierze przestrzenią współrzędnych K^n, jej podprzestrzeniami, rozmaitymi opisami tych podprzestrzeni itd. Warto przekonać się od razu, że te podstawowe i bardzo elementarne przestrzenie mają ważne zastosowania. Opowieść przedstawiona poniżej mówi o przykładach tzw. kodów liniowych.

W 1948 roku Claude Shannon, amerykański inżynier i matematyk, wydał artykuł „A Mathematical Theory of Communitacion", który uważany jest za początek tzw. teorii informacji i teorii kodowania. Podstawowym celem jest efektywne i wiarygodne przesyłanie komunikatów w niekooperacyjnym (być może wrogim) środowisku. Aby być **efektywne** – komunikaty nie mogą wymagać nadawania przez zbyt długi czas lub zbyt duży koszt. Aby transmisja była **wiarygodna** potrzebne jest by otrzymywany sygnał przypominał ten wyemitowany, przynajmniej w ramach pewnej z góry określonej tolerancji. Wysiłki matematyków poszły w dwóch kierunkach. Shannon, ojciec teorii informacji, studiował osiągalne ograniczenia komunikacyjne głównie metodami analitycznymi i probabilistycznymi. Jego kolega – Richard Hamming, pracował nad poprawianiem kodów pierwszych komputerów i stosował głównie metody algebraiczne.

Informacja nadana ze źródła trafia do „przewodu", „przestrzeni" „kanału", którym podróżuje do odbiorcy. Nasz model komunikacji oparty jest o założenie, że informacja poddana jest zgodnie z naszą wolą pewnej strukturze u źródła oraz pewnej metodzie odczytu u odbiorcy, ale nie mamy żadnej kontroli nad przestrzenią pomiędzy nadawcą, a odbiorcą. W ten sposób wiadomość ulec może zniekształceniu. Prostym przykładem jest rozmowa w bardzo głośnej kawiarni, pisanie książki, która ma być odczytana lata później. Jest też wiele sposobów radzenia sobie z możliwymi zaburzeniami przekazu. Osobę, której nie dosłyszałem mogę poprosić o powtórzenie, a w przypadku znalezienia zniszczonego manuskryptu mogę próbować poszukiwać innej jego kopii. Tu jednak zaburzone są: efektywność (*Ile razy mam powtarzać*?!) i wiarygodność (*może nie ma innego manuskryptu, a może obydwa są fałszywe*?).

Zakłady Bell Telephone Laboratories w latach 50-tych XX wieku

Shannon i Hamming, a także wielu innych ojców teorii komunikacji, pracowali dla Bell Telephone Laboratories. Byli szczególnie zainteresowani radzeniem sobie z błędami, które powstają gdy wiadomość podróżuje kablem telefonicznym i zostanie zniekształcona przez uderzenie pioruna lub przez nałożenie się na siebie dwóch rozmów. Komunikacja w przestrzeni kosmicznej zaburzana jest przez atmosferę ziemską i aktywność słoneczną. Podczas misji Galileo, gdy padła jedna z anten sondy, naukowcy przeprogramowali komputer pokładowy sondy tak, by w sposób bardziej intensywny przetwarzał kod wysyłany na Ziemię i w ten sposób byli w stanie odzyskać część pierwotnej efektywności przekazu wiadomości. Dyski twarde naszych komputerów wyposażone są w CRC, czyli *Cyclic Redundancy Check*, z uwagi na konieczność wykrywania zaburzeń w przechowywaniu danych wystawionych na działanie promieni gamma czy interferencji magnetycznej. Gdy Phillips wprowadził technologię płyt CD reklamował ją jako niewrażliwą na wiele typów zniszczenia – nawet z porysowanej (nieznacznie) płyty jesteśmy (byliśmy?) w stanie odczytywać informacje. Jest to zasługa teorii kodowania. Można podać wiele więcej przykładów.

Informację można zapisać na wiele sposobów. Używamy w tym celu najczęściej słów zbudowanych z liter określonego alfabetu. W informatyce najczęściej są to bity, a więc ciągi zer i jedynek. **Kodowanie wiadomości polega na dodaniu do niej pewnego dodatkowego zestawu bitów** służącego do jej odczytania w sytuacji, gdy wiemy, że wystąpić może błąd. Można tego dokonywać na wiele sposobów.

Załóżmy, że chcecie Państwo przesłać Komuś wiadomość złożoną z trzech liter ze zbioru $\{0,1\}$ postaci $v = abc$. Między emiterem a odbiornikiem wiadomość może ulec zniekształceniu i dojdzie do Kogoś niewłaściwe słowo. Czy ów Ktoś zdoła wykryć taki błąd i odczytać poprawną wiadomość, jeśli wiemy na przykład, że błąd zwykle nie dotyczy więcej niż jednej litery?

Do opisu rozwiązania zastosujemy algebrę liniową. W tym celu zakłada się, że zakodowana wiadomość, którą przesyłamy, jest podprzestrzenią przestrzeni liniowej. Kodem liniowym długości n nad ciałem F nazywamy podprzestrzeń przestrzeni F^n. Zakodowane słowa to wektory.

Najpierw naiwne rozwiązanie problemu. Dla każdego 0 w planowanej wiadomości, wysyłamy dwa zera. Podobnie dla jedynek. A zatem jeśli oryginalna wiadomość miała na przykład postać [010], to zakodujemy ją jako [00 : 11 : 00]. A zatem nasz kod to element przestrzeni $(\mathbb{Z}_2)^6$. Czy możemy traktować go jako podprzestrzeń? Zauważmy, że $\mathrm{lin}((0,0,1,1,0,0))$ to po prostu $\{(0,0,0,0,0,0),(0,0,1,1,0,0)\}$, a więc niezerowe elementy tej podprzestrzeni tworzą zakodowaną wiadomość. Odbiorca jest w stanie stwierdzić czy jest ona poprawna, a więc czy wiadomość przyszła z jednym błędem (nie rozważamy tutaj dla uproszczenia innych sytuacji). Dla przykładu: jeśli wiadomość jest postaci [00 : 11 : 10] odbiorca wie, że jest błąd w trzecim segmencie wiadomości. Może zatem wydedukować, że oryginalna wiadomość miała postaci [010] lub [011]. Naiwne podejście ma dwie wady: po pierwsze przesyłamy dwa razy więcej danych, niż potrzeba, a po drugie – odbiorca nie ma dość informacji, by poprawić błąd, który wykrył.

Naiwne rozwiązanie problemu niemożności naprawienia (pojedynczego) błędu w transmisji jest proste: wysyłać trzy razy więcej danych. A więc na przykład oryginalną wiadomość postaci [010] przesłać możemy jako [000 : 111 : 000]. Jeśli odbiorca otrzyma, powiedzmy, wiadomość postaci [000 : 111 : 010] to wie już nie tylko, że błąd wystąpił w trzecim segmencie ale też, że w oryginalnej wiadomości ten segment miał postać 000. Widzimy jednak, że nie jest to efektywne przesyłanie danych. Oto inna propozycja, pochodząca od Hamminga.

Jeśli chcemy wysłać wiadomość postaci $[c_1 : c_2 : c_3]$, gdzie $c_1, c_2, c_3 \in \{0,1\}$, to wysyłamy ciąg złożony z pięciu znaków postaci: $[c_1 : c_2 : c_3 : c_1 + c_2 : c_2 + c_3]$, przy czym operacje dodawania wykonujemy nad ciałem $\mathbb{Z}_2$, czyli $c_1 + c_2$ jest równe 0 lub 1 w zależności od składników c_1, c_2. Okazuje się, że w tym kodowaniu jesteśmy w stanie wykryć nawet dwa błędy, a jeśli jest tylko jeden – to możemy go naprawić. Zobaczmy przykłady.

Wysyłamy [100], a wiec po zakodowaniu dostajemy słowo [10010]. Załóżmy, że wystąpi dokładnie jeden błąd przy transmisji i otrzymamy jedną z wiadomości: [00010], [01010], [10110], [10000], [10011]. Czy Czytelnik widzi, że w każdym wypadku możemy nie tylko wykryć błąd, ale i go naprawić? W pierwszym przypadku [00010] nie spełnia na czwartej współrzędnej warunku $c_1 + c_2 = 1$, ale spełnia na piątej warunek $c_2 + c_3 = 0$. A zatem skoro jest dokładnie jeden błąd, to c_2, c_3 są przesłane dobrze, a błędny jest przekaz c_1. Oczywiście umiemy też wykryć wiadomość poprawnie odebraną.

Czy wykrywanie pojedynczego błędu w ogóle może kogoś interesować? Nie tylko może, ale jest powszechne. Nie ma dwóch numerów kont, które różniłyby się tylko jedną lub dwiema cyframi. Jeśli wysyłając przelew pomylimy się o jedną lub dwie cyfry w numerze konta, to przelew zostanie odrzucony. Kod Hamminga stosuje się dla wiadomości dowolnej długości. Do zakodowania słowa długości n potrzeba $2n - 1$ znaków (oczywiście chodzi o słowo zerojedynkowe).

Być może Czytelnik nie dostrzega jeszcze żadnej wielkiej „matematyki" w tej opowieści, ale zapewniam, że dzieje się tak tylko dlatego, że niemal zmuszam się do unikania wprowadzania jakiejkolwiek terminologii, a dzieje się tu bardzo dużo. Mówiąc o kodach wspomnielibyśmy zaraz o odległości Hamminga, problemie pakowania sfer, macierzach generujących, wielomianach kodujących słowa itd. Zainteresowanych odsyłam do bardzo ciekawych notatek J. Halla z teorii kodowania (polecam zwłaszcza wstępny rozdział – kolejne mogą być za trudne na razie – tylko na razie) dostępnych pod adresem:

https://users.math.msu.edu/users/jhall/classes/CODENOTES/CODING-NOTES.HTML

Kto by chciał poczytać (w języku polskim) więcej o kodach, szyfrach i ogólnie o teorii informacji, czy też przekonać się wszechstronnym występowaniu kodowania, np. w numerach PESEL, ISBN, IBAN, polecam tekst dr. Grzegorza Szkibiela „Wstęp do teorii informacji i kodowania", dostępny online.