Wykład 6.

Zastosowanie: Kody Hammonda

S: skończony zbiór, alfabet,
$\#$
ϕ $S^n = \{$słowa długości n, nad $S\}$
$\overset{\in}{w} = a_1 a_2 \dots a_n$, $a_i \in S$

Problem: przesłać słowo w do odbiorcy, po zakodowaniu

Nadawca Odbiorca

$S^n \ni w \mapsto \bar{w} \rightsquigarrow \bar{w}'$

kod w
słowa

ale: mogą wystąpić błędy: $\bar{w}' \neq \bar{w}$

np. może być tak, że $P(>1$ błąd w $\bar{w}') \approx 0$

ale $P(1$ błąd$)$: istotne.

Sposób 1. $w = abcd \longrightarrow \bar{w} = aaabbbcccddd \longrightarrow \bar{w}'$

jeśli tylko ≤ 1 błąd,
to odczytujemy w z $\bar{w}'$!

Kosztowne:
4 bity $\overset{}{\underset{\text{kodowanie}}{\rightsquigarrow}}$ 12 bitów.

Sposób 2. Kody liniowe:

$S = F =$ ciało skończone, np. $F = F_2 = \{0,1\}$.

AlI 2/6

$C < F^7$ o bazie

$$b_1 = \begin{pmatrix}1\\0\\0\\0\\1\\1\\1\end{pmatrix} \quad b_2 = \begin{pmatrix}0\\1\\0\\0\\1\\1\\0\end{pmatrix} \quad b_3 = \begin{pmatrix}0\\0\\1\\0\\1\\0\\1\end{pmatrix} \quad b_4 = \begin{pmatrix}0\\0\\0\\1\\0\\1\\1\end{pmatrix}$$

$\dim C = 4$. $\quad A = (b_1, b_2, b_3, b_4) \in M_{7\times 4}(F_2)$

$f := f_A : F^4 \longrightarrow F^7$, $\operatorname{Im} f = C$ $(\Rightarrow f: 1\text{-}1)$

$g : F^7 \xrightarrow[\text{na}]{} F^l$ liniowe t. że $C = \operatorname{Ker} g$.

$l = ?$ $\quad 7 = \underbrace{\dim \operatorname{Ker} g}_{= 4} + \underbrace{\dim \operatorname{Im} g}_{= l} \Rightarrow \underline{\underline{l = 3}}$

Jak znaleźć g?

$F^7 \supseteq \underset{\text{baza}}{\mathcal{B}} = \{b_1, b_2, b_3, b_4, E_5, E_6, E_7\}$

określamy g na wektorach bazy $\mathcal{B}$:

- $g(b_1) = g(b_2) = g(b_3) = g(b_4) = 0$ $(\Rightarrow C \subseteq \operatorname{Ker} g)$
- $g(E_5) = E_1$, $g(E_6) = E_2$, $g(E_7) = E_3$ $(\Rightarrow \operatorname{Im} g = F^3)$

$\Rightarrow C = \operatorname{Ker} g$

Niech B: macierz g w bazach standardowych. Al I/6

Jak znaleźć B?

w F^7:

$$E_1 = b_1 + E_5 + E_6 + E_7 \qquad g(E_1) = \begin{pmatrix}1\\1\\1\end{pmatrix}$$

$$E_2 = b_2 + E_5 + E_6$$

$$E_3 = b_3 + E_5 + E_7$$

$$E_4 = b_4 + E_6 + E_7$$

$$\Rightarrow g(E_2) = \begin{pmatrix}1\\1\\0\end{pmatrix} \quad g(E_4) = \begin{pmatrix}0\\1\\1\end{pmatrix} \quad g(E_3) = \begin{pmatrix}1\\0\\1\end{pmatrix}$$

$$B = \begin{array}{c} \begin{array}{ccccccc} B_1 & B_2 & B_3 & B_4 & B_5 & B_6 & B_7 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

: wszystkie kolumny różne.

kodowanie: $F^4 \ni w \rightsquigarrow \overline{w} = f_A(w) \in C$,

f_A

$\boxed{\text{liniowe}}$

$$w = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix}$$

$$\overline{w} = Aw = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_1 + a_2 + a_3 \\ a_1 + a_2 + a_4 \\ a_1 + a_3 + a_4 \end{bmatrix}$$

w łatwo odczytać z $\overline{w}$ (jako początek),

dla $w_1, w_2 \in F^n$ $\quad d(w_1, w_2) = \left|\{i \in \{1, \ldots, n\} : w_1(i) \neq w_2(i)\}\right|$

odległość Hamminga

metryka

<u>Uwaga</u> $w_1 \neq w_2 \in F^4 \Rightarrow d(f_A(w_1), f_A(w_2)) \geq 3$

<u>D-d</u>

Wystarczy pokazać, że dla $0 \neq v \in C < F^7$

$$d(0,v) \geq 3$$

[bo: $d(f_A(w_1), f_A(w_2)) = d(\underbrace{f_A(w_1) - f_A(w_1)}_{=0}, \underbrace{f_A(w_2) - f_A(w_1)}_{\in C,\ \neq 0 \text{ bo } w_1 \neq w_2})$]

Zał. nie wprost, że dla $0 \neq v \in C < F^7$

$$1 \leq d(0,v) \leq 2.$$

tzn: 1 lub 2 jedynki w $v \in F^7$.

$v \in \mathrm{Ker}\, g$, tzn: $Bv = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ $\quad v = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_7 \end{bmatrix} \in C$

$$Bv = c_1 B_1 + c_2 B_2 + \dots + c_7 B_7 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

- Dokładnie jedno $c_i = 1$? wtedy $Bv = B_i$ <u>niemożliwe</u>, bo $B_i \neq 0$.
- Dokładnie dwa $c_i, c_j = 1$? wtedy

$$Bv = B_i + B_j \neq 0, \text{ bo } B_i \neq B_j, \text{ sprzeczność.}$$

To druta

Nadawca   Odbiorca

$F^4 \ni W \xrightarrow[\text{kodowanie}]{} \bar{w} = f_A(w) \rightsquigarrow \bar{w}' \in F^7$ t.że

f_A $d(\underset{C}{\bar{w}}, \bar{w}') \leq 1$

- dla każdego $u \in F^7$ istnieje co najwyżej jedno $u' \in C$ t.że $d(u,u') \leq 1$.

<u>d-d</u>: Jeśli $u', u'' \in C$, $d(u,u') \leq 1$ i $d(u,u'') \leq 1$,

to $d(u',u'') \leq d(u,u') + d(u,u'') \leq 2$

$\Longrightarrow \quad u' = u''$

(uwaga)

Odczytanie $\bar{w}$ z $\bar{w}'$:

- obliczamy $g(\bar{w}') = B\bar{w}'$. Jeśli $g(\bar{w}') = 0$, to $\bar{w}' \in C$ i $\bar{w}' = \bar{w}$ koniec.

Jeśli $g(\bar{w}') \neq 0$, to $\bar{w}' = \bar{w} + E_i$ dla pewnego $1 \leq i \leq 7$ (i: miejsce błędu)

Jak znaleźć i?

$$g(\bar{w}') = g(\bar{w} + E_i) = \underset{0}{\underbrace{g(\bar{w})}} + g(E_i) = g(E_i) : i\text{-ta kolumna } B.$$

znajdujemy i.

- zmieniamy w $\overline{w}'$ i-ty bit i dostajemy $\overline{w}$.
- Odczytujemy w z $\overline{w}$.

Uogólnienie.

Niech $l \geqslant 2$, $n = 2^l - 1$, B: macierz $l \times n$,
kolumny: wszystkie wektory z $F^l \setminus \{0\}$

$g : F^n \longrightarrow F^l$

liniowe o macierzy B, g jest "na".

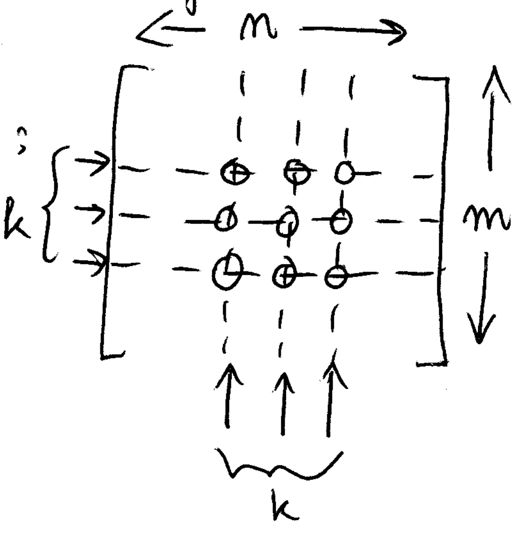
$C := \ker g < F^n$, $\dim C = n - l$.

$f : F^{n-l} \xrightarrow[\text{liniowe}]{1-1} F^n$, $\operatorname{Im} f = C$

↑
kodowanie.

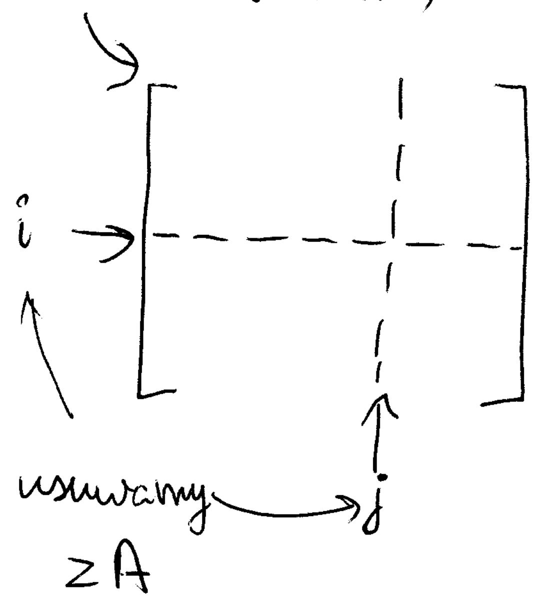
Uogólniony ciąg Hammonda
długości $n = 2^l - 1$, $l \geqslant 2$
(wszystko działa jak poprzednio)

Z powrotem do czystej matematyki.

- $A = [a_{ij}]_{m \times n}$; 

$\det \begin{bmatrix} \circ & \circ & \circ \\ \circ & \circ & \circ \\ \circ & \circ & \circ \end{bmatrix}$: minor stopnia k macierzy A.

$A = [a_{ij}]_{n\times n}$, $1 \le i,j \le n$



$\longrightarrow A'$: macierz $(n-1)\times(n-1)$

$A_{ij} = (-1)^{i+j} \det A'$: dopełnienie algebraiczne wyrazu a_{ij} macierzy A.

Przykład $A = \begin{bmatrix} 1 & 2 & 3 \\ 5 & 7 & 8 \\ 2 & 7 & 3 \end{bmatrix}$ $A_{22} = (-1)^{2+2} \det \begin{bmatrix} 1 & 3 \\ 2 & 3 \end{bmatrix}$

TW. 6.1 (rozwinięcie Laplace'a)

$\det A = a_{i1} A_{i1} + a_{i2} A_{i2} + \ldots + a_{in} A_{in}$: rozwinięcie względem i-tego wiersza

$\det A = a_{1j} A_{1j} + a_{2j} A_{2j} + \ldots + a_{nj} A_{nj}$ $\leftarrow$ względem j-tej kolumny.

D-d. Ustalmy i. Określamy

$G: M_{n\times n}(\mathbb{R}) \longrightarrow \mathbb{R}$ $\quad G(A) = \sum_{j=1}^{n} a_{ij} A_{ij}$

- spełnia D1–D4 z definicji det $\Rightarrow G(A) = \det(A)$.

- kolumny: przez transpozycję macierzy.

Przykład

$$\det \begin{array}{c} \begin{bmatrix} 0 & 2 & 2 & 1 \\ 0 & 0 & 1 & 2 \\ 1 & 2 & 1 & 0 \\ 0 & 0 & 3 & 5 \end{bmatrix} \\ j=1 \end{array} = \underbrace{1\cdot(-1)^{1+3}}_{1}\cdot \det \begin{array}{c} j=1 \\ \begin{bmatrix} 2 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 3 & 5 \end{bmatrix} \end{array} =$$

$$= 2\cdot(-1)^{1+1}\cdot\det\begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix} = 2\cdot(5-6) = -2$$

Tw. 6.2

Jeśli $A=[a_{ij}]_{n\times n}$ jest odwracalna, to

$$A^{-1} = \frac{1}{\det(A)}\left[a'_{ij}\right]_{n\times n}, \text{ gdzie } a'_{ij} = A_{ji};$$

dopełnienie algebraiczne wyrazu a_{ji} macierzy A

D-d.

Niech $A' = [a'_{ij}]_{n\times n}$, $C=[c_{ij}]=AA'$.

$$c_{ij} = \sum_{t=1}^{n} a_{it}a'_{tj} = \sum_{t=1}^{n} a_{it}A_{jt}$$

z tw. 6.1: $c_{ij} = \det(\bar{A})$, gdzie $\bar{A}$ powstaje z A przez zastąpienie j-tego wiersza przez wiersz i-ty.

dlatego: $c_{ij} = \begin{cases} 0, & \text{gdy } i\neq j \\ \det(A), & \text{gdy } i=j \end{cases} \Rightarrow C = \det(A)\cdot I$

$$\Downarrow$$

$$A\cdot\left(\frac{1}{\det A}A'\right) = I$$

Metoda "bezwyznacznikowa" znajdowania A^{-1}:

$$\begin{bmatrix} & & \\ & A & \\ & & \end{bmatrix}_{n\times n}\begin{bmatrix} & & \\ & I & \\ & & \end{bmatrix}_{n\times n} \xrightarrow{\text{operacje elementarne}} \begin{bmatrix} & & \\ & I & \\ & & \end{bmatrix}\begin{bmatrix} & & \\ & A' & \\ & & \end{bmatrix}$$

na wierszach macierzy $n\times 2n$

do wiersza dodajemy skalarną krotność innego wiersza

$A^{-1}=A'$.

<u>Przykład</u>. Znaleźć A^{-1} dla $A=\begin{bmatrix}1&2&1\\0&1&0\\0&1&1\end{bmatrix}$;

$$\begin{bmatrix}1&2&1\\0&1&0\\0&1&1\end{bmatrix}\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}\begin{array}{l}-2\cdot[2]\\ \\ \\ \end{array} \longrightarrow \begin{bmatrix}1&0&1\\0&1&0\\0&1&1\end{bmatrix}\begin{bmatrix}1&-2&0\\0&1&0\\0&0&1\end{bmatrix}\begin{array}{l} \\ \\ -[2]\end{array} \longrightarrow$$

$$\begin{bmatrix}1&0&1\\0&1&0\\0&0&1\end{bmatrix}\begin{bmatrix}1&-2&0\\0&1&0\\0&-1&1\end{bmatrix}\begin{array}{l}-[3]\\ \\ \\ \end{array} \longrightarrow \begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}\underbrace{\begin{bmatrix}1&-1&-1\\0&1&0\\0&-1&1\end{bmatrix}}_{A^{-1}}.$$

Zmiana współrzędnych wektora przy zmianie bazy.

$\mathcal{B}=\{b_1,\dots,b_n\}$, $\mathcal{C}=\{c_1,\dots,c_n\}\subseteq V$ bazy (ponumerowane)

Problem: dany $v\in V$ i $[v]_{\mathcal{B}}$. Znaleźć $[v]_{\mathcal{C}}$.

Fakt 6.3 $[v]_{\mathcal{C}} = m_{\mathcal{BC}}(id_V)[v]_{\mathcal{B}}$.

D-d $id_V : V \longrightarrow V$ liniowe.

$$[v]_{\mathcal{C}} = [id(v)]_{\mathcal{C}} = m_{\mathcal{BC}}(id_V)[v]_{\mathcal{B}}$$ z definicji $m_{\mathcal{BC}}(id_V)$.

Def. 6.4.
$m_{\mathcal{BC}}(id_V)$: macierz przejścia od współrzędnych w bazie $\mathcal{B}$ do współrzędnych w bazie $\mathcal{C}$.

[nie mylić z macierzą przejścia od bazy $\mathcal{B}$ do bazy $\mathcal{C}$]

Przykład

$$\begin{cases} b_1 = a_{11}c_1 + a_{21}c_2 + \dots + a_{n1}c_n & \leftarrow \text{1. kolumna} \\ b_2 = a_{12}c_1 + a_{22}c_2 + \dots + a_{n2}c_n & \\ \vdots \qquad\qquad \vdots & \begin{pmatrix}\text{dla pewnych} \\ a_{ij} \in \mathbb{R}\end{pmatrix} \\ b_n = a_{1n}c_1 + a_{2n}c_2 + \dots + a_{nn}c_n & \leftarrow n\text{-ta kolumna} \end{cases}$$

Wtedy $m_{\mathcal{BC}}[id_V] = [a_{ij}]_{n \times n}$. $m_{\mathcal{BC}}[id_V]^T$: macierz przejścia od bazy $\mathcal{C}$ do bazy $\mathcal{B}$

Uwaga 6.5.
$m_{\mathcal{BC}}(id)$ jest odwracalna i $m_{\mathcal{BC}}(id)^{-1} = m_{\mathcal{CB}}(id)$

D-d $m_{\mathcal{BC}}(id_V)\, m_{\mathcal{CB}}(id_V) = m_{\mathcal{CC}}(id_V \circ id_V) = m_{\mathcal{CC}}(id) = I$.

Przykład

1. $V = \mathbb{R}^3$, $\mathcal{E} = \{E_1, E_2, E_3\}$ baza standardowa

$$\mathcal{B} = \{u, v, w\}$$

$$u = \frac{1}{\sqrt{3}}\begin{bmatrix}1\\1\\1\end{bmatrix}, \quad v = \frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\-1\end{bmatrix}, \quad w = \frac{1}{\sqrt{6}}\begin{bmatrix}-2\\1\\1\end{bmatrix}$$

$$u = \frac{1}{\sqrt{3}}E_1 + \frac{1}{\sqrt{3}}E_2 + \frac{1}{\sqrt{3}}E_3$$

$$v = \frac{1}{\sqrt{2}}E_2 - \frac{1}{\sqrt{3}}E_3$$

$$w = -\frac{2}{\sqrt{6}}E_1 + \frac{1}{\sqrt{6}}E_2 + \frac{1}{\sqrt{6}}E_3$$

$$m_{\mathcal{B}\mathcal{E}}(id) = \begin{bmatrix}\frac{1}{\sqrt{3}} & 0 & -\frac{2}{\sqrt{6}}\\ \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}}\\ \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{3}} & \frac{1}{\sqrt{6}}\end{bmatrix}$$

macierz ortogonalna (kolumny to wektory ortogonalne długości 1) [później]

$$m_{\mathcal{E}\mathcal{B}}(id) = m_{\mathcal{B}\mathcal{E}}(id)^{-1} \Leftarrow$$

$$= \underline{\underline{m_{\mathcal{B}\mathcal{E}}(id)^T}}$$

[Wektory u, v, w: długości 1, parami $\perp$

2. Niech $u, v, w \in \mathbb{R}^3 =: V$ jak wyżej.

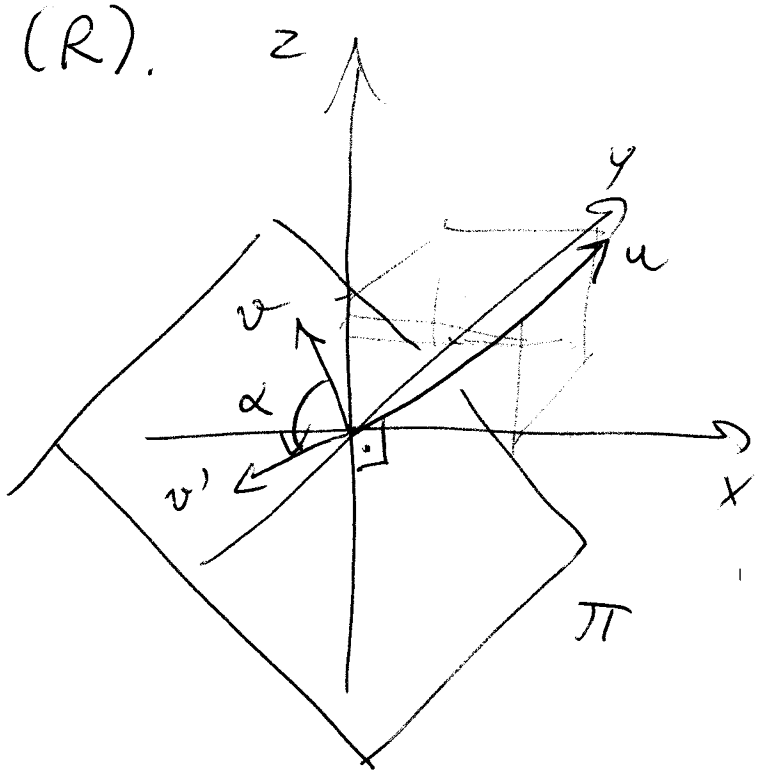
Niech $v' = \frac{1}{\sqrt{6}}\begin{bmatrix}-1\\2\\1\end{bmatrix}$ i $\Pi = \mathrm{Lin}\{v, w\}$, $L = \mathrm{Lin}\{u\}$

$$\Pi \perp L$$

$v' \in \Pi$, bo $v' \perp u$.

Niech $R: \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ obrót wokół prostej L taki, że $R(v) = v'$.

Problem: znaleźć $m_{\mathcal{E}}(R)$.



1. $m_{\mathcal{B}}(R)$:

$R(u) = u$

$R(v) = v' =$

$= \frac{\sqrt{3}}{2} v + \frac{1}{2} w$

$\Downarrow$

$[v']_{\mathcal{B}} = \begin{bmatrix} 0 \\ \frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{bmatrix}$ ⟵ alternatywnie:

$= m_{\mathcal{E}\mathcal{B}}(id)[v']_{\cancel{\mathcal{B}}\mathcal{E}} = \begin{bmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ -\frac{2}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} \end{bmatrix} \begin{bmatrix} -\frac{1}{\sqrt{6}} \\ \frac{2}{\sqrt{6}} \\ -\frac{1}{\sqrt{6}} \end{bmatrix}$

$\frac{\sqrt{3}}{2} = \cos\alpha, \ \frac{1}{2} = \sin\alpha,$

$\alpha = \frac{\pi}{6} = 30°,$

$\cancel{m_{\mathcal{B}}(R)}\ m_{\mathcal{B}}(R) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ 0 & \frac{1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix}$ Jak znaleźć $m_{\mathcal{E}}(R)$?

Uwaga 6.6. $F: \underset{\mathcal{B}}{V} \longrightarrow \underset{\mathcal{C}}{V}$ liniowe, $\mathcal{B}, \mathcal{C}$ bazy

$m_{\mathcal{C}\mathcal{C}}(F) = m_{\mathcal{B}\mathcal{C}}(id)\, m_{\mathcal{B}\mathcal{B}}(F)\, m_{\mathcal{C}\mathcal{B}}(id)$

<u>D-d</u> $F = id_V \circ F \circ id_V$.

13

AlT/6

Dlatego:

$$m_{\mathcal{B}\mathcal{E}}(id)^T$$

$$m_{\mathcal{E}}(R) = m_{\mathcal{B}\mathcal{E}}(id)\; m_{\mathcal{B}}(R)\; \cancel{m_{\mathcal{B}\mathcal{E}}(}\; m_{\mathcal{E}\mathcal{B}}(id)$$

$$= \begin{bmatrix} \frac{1}{\sqrt{3}} & 0 & -\frac{2}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{3}} & \frac{1}{\sqrt{6}} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ 0 & \frac{1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix} \begin{bmatrix} \; & \; & \; \\ \; & \; & \; \\ \; & \; & \; \end{bmatrix}^T$$