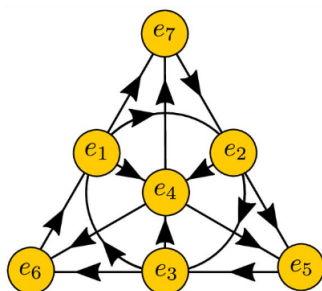


Domácí úlohy 1.

do 20.4. 12:20

Úkoly odevzdávejte na prosemináři nebo je pošlete na email `david.stanovsky@matfyz.cuni.cz` v jednom souboru ve formátu `Prijmeni_cislosady.PDF` (čitelný sken v jednom souboru, na bílém pozadí bez tmavých okrajů). Uveďte také svoji přezdívku, pod kterou řešíte kahooty a pod kterou uvidíte výsledky na webu.

- (5 bodů) Najděte nekonečně mnoho kořenů polynomu $x^2 + 1$ v oboru kvaternionů.
- (5 bodů) Řešte lineární rovnici $(e_1 + e_3)x = e_7$ v oboru oktonionů. Pro počítání s imaginárními jednotkami využijte následující ohodnocenou Fanovu rovinu:



- (5 bodů) Realizujte grupu permutací tří prvků pomocí rotací v \mathbb{R}^3 (přesněji: najděte v $SO(3)$ grupu isomorfní S_3).
- (5 bodů) Uvažujte Hammingův $(4, 7)$ -kód daný generující maticí

$$G^T = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

(tj. kódovací zobrazení je $\mathbb{Z}_2^4 \rightarrow \mathbb{Z}_2^7$, $v \mapsto Gv$). Dostali jste zprávu

00100010011101001110110110111101100010100010011001100111

Předpokládejte, že v každé sedmici je nejvýše jedna chyba. Najděte původní zprávu.

Návod: Použijte ten trik s hledáním sloupce v kontrolní matici H : je-li přijatá zpráva $u + e_i$, tak $H(u + e_i) = He_i = i$ -tý sloupec matice H .

- (5 bodů) Uvažujte Reed-Solomonův (k, n) -kód nad tělesem \mathbb{F}_q daný generující maticí

$$G^T = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & b & b^2 & \dots & b^{n-1} \\ 1 & b^2 & b^4 & \dots & b^{2(n-1)} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & b^{k-1} & b^{2(k-1)} & \dots & b^{(k-1)(n-1)} \end{pmatrix},$$

1

přičemž b je prvek řádu n v grupě \mathbb{F}_q^* , to jest $b^n = 1$ a $b^m \neq 1$ pro $0 < m < n$. Dokažte, že kontrolní matice je

$$H = \begin{pmatrix} 1 & b & b^2 & \dots & b^{n-1} \\ 1 & b^2 & b^4 & \dots & b^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & b^{n-k} & b^{2(n-k)} & \dots & b^{(n-k)(n-1)} \end{pmatrix}.$$

Návod: má platit $HG = 0$ (proč?). Na výpočet prvků součinu použijte součet geometrické řady, ten funguje v jakémkoliv tělese, i konečném. Dejte pozor, jestli opravdu sčítáte geometrickou řadu a ne samé jedničky.

6. (5 bodů) Zkusíme si dekodovat QR-kód. Aby to bylo trochu jednodušší, použijeme menší těleso a kratší kód, ale princip je stejný.

Uvažujte těleso $\mathbb{F}_{16} = \mathbb{Z}_2[\alpha]/(\alpha^4 + \alpha + 1)$. Jeho prvek $a\alpha^3 + b\alpha^2 + c\alpha + d$ budeme reprezentovat jako čtvercovou mřížku 2×2

$$\begin{array}{|c|c|} \hline a & b \\ \hline c & d \\ \hline \end{array},$$

graficky budeme značit $0 = \text{bílá}$, $1 = \text{černá}$. Posloupnost n prvků tělesa \mathbb{F}_{16} budeme reprezentovat jako obdélníkovou mřížku $2 \times 2n$.

Uvažujte Reed-Solomonův $(3, 5; 3)$ -kód nad tělesem \mathbb{F}_{16} daný prvkem $b = \alpha^3$ řádu 5, generující matici najdete v předchozí úloze. Přečetli jste kód



Předpokládejte, že nastala právě jedna chyba (tj. porušen je právě jeden čtverec, může to být i více políček v tom čtverci). Dekódujte zprávu.

Návod: Na Reed-Solomonův kód se můžete dívat jako na dosazování hodnot $1, b, b^2, b^3, b^4$ do polynomu stupně ≤ 2 . Tím, že nastala právě jedna chyba, můžete použít stejný trik s kontrolní maticí, jako v případě Hammingova kódu. Na výpočty matic G, H klidně použijte nějaký software, i když s trochou trpělivosti to jde i ručně.