

## POSUDEK OPONENTA BAKALÁŘSKÉ PRÁCE

**Název:** Dekódování RS-kódů

**Autor:** Dalibor Procházka

### SHRNUTÍ OBSAHU PRÁCE

Práce se zabývá Reedovými-Solomonovými kódy a hlavně pak algoritmy pro jejich dekódování za přítomnosti chyb při přenosu dat. RS kódy tvoří známou a v praxi používanou třídu samoopravných kódů, které mají v jistém smyslu optimální parametry (jsou to tzv. maximum distance separable kódy). Práce podrobně popisuje tři dekódovací algoritmy: původní z článku Reeda a Solomona, dnes běžně používaný efektivní algoritmus založený na rozšířeném Eukleidově algoritmu pro polynomy a alternativní algoritmus z článku S. Gaa z roku 2003. Popisy jsou na konci vždy doplněny diskuzí časové složitosti a konkrétním příkladem dekódování přijatého slova.

### CELKOVÉ HODNOCENÍ PRÁCE

**Téma práce.** Téma práce považuji za přiměřené a vhodné pro bakalářskou práci. Použité metody vycházejí ze základních kurzů lineární a abstraktní algebry, ale vedou k zajímavým aplikacím a úvahám.

**Vlastní příspěvek.** Hlavním příspěvkem je podrobné a ucelené zpracování tématu dekódování Reedových-Solomonových kódů z několika zdrojů, přičemž byly doplněny detaily v důkazech, přidány příklady a podrobněji rozebrána časová složitost.

**Matematická úroveň.** Text je z matematického hlediska korektní, přehledný a dobře čitelný.

**Práce se zdroji.** Použité zdroje jsou řádně citovány.

**Formální úprava.** Formální úprava práce je dobrá, počet překlepů je přiměřený délce textu.

### KONKRÉTNÍ PŘIPOMÍNKY

Nakonec uvádím několik drobných připomínek ke konkrétním místům v textu práce:

- str. 3, kap. 1.1: Na pátém řádku kapitolky by místo „a subspace of a linear vector space“ spíš mělo být „a subspace of  $\mathbb{F}_q^n$ “. Má to být podprostor tohoto zcela konkrétního vektorového prostoru. Dále omezení  $n \leq q$  má co do činění ne s obecnými lineárními kódy, ale až se (zobecněnými) RS kódy, které v tu chvíli ještě nebyly zavedeny.
- str. 6, algoritmus 1: V kroku 8 by se mělo spíš vracet  $(r_{i-1}, u_{i-1}, v_{i-1})$ , protože v tu chvíli  $r_i = 0$ .
- odstavec na konci str. 13/začátku str. 14: K čemu nám je omezení  $l \geq N$ ? Indexy menší než  $l$  se podle všeho v odstavci nikde nepoužívají. Také by bylo dobré lépe vysvětlit, proč posloupnosti mají opravdu periodu  $2^N - 1$  (což sice z argumentů nakonec vyplývá, ale podle mě netriviálně).
- str. 25, důkaz lematu 4.2: Na začátku důkazu by bylo dobré upřesnit, že pro vstupy  $r_0, r_1$  a  $g_0, g_1$  dává rozšířený Eukleidův algoritmus stejné výsledky jen do určitého kroku.
- str. 26, sedmý řádek odspodu: místo  $0 + f(a_i)$  má být ve vzorci  $b_i - c_i + f(a_i)$ .

## ZÁVĚR

Práci doporučuji uznat jako bakalářskou práci.

*Návrh klasifikace vedoucí sdělí předsedovi zkušební (sub)komise.*

doc. RNDr. Jan Šťovíček, Ph.D.

Katedra algebry MFF UK

14. 6. 2023