## Posudek vedoucího bakalářské práce

**Název:** Zobecněná integrální vlastnost
**Autor:** Jana Hrúzová

### Shrnutí obsahu práce

Práce Jany Hrúzové se zabývá takzvanou dělící vlastnosti dané množiny slov, která představuje jeden z teoretických nástrojů útoků na blokové šifry, a jeho souvislost s Reed-Mullerovými kódy.

Text je rozdělen do tří věcných částí. První kapitola je věnována standardnímu popisu Reed-Mullerových kódů pomocí booleovských funkcí a booleovských polynomů. Jádro práce tvoří druhá kapitola zavádějící centrální pojem dělící vlastnosti stupně k a související teorii. Závěrečná část prezentuje možnou aplikaci dělící vlastnosti v situaci šíření množiny parit prostřednictvím permutací.

### Celkové hodnocení práce

**Téma práce.** Téma práce je primárně kompilační. Od studentky vyžadovalo porozumění odbornému článku, jeho zpracování a doplnění o detaily některých důkazů a příklady. Zadání bylo podle mého mínění studentkou naplněno.

**Vlastní příspěvek.** Studentčin vlastní příspěvek spočívá především v detailnější argumentaci v důkazech tvrzení a konstrukci několika ilustračních příkladů.

**Matematická úroveň.** Matematická úroveň práce je podle mého mínění dobrá. Výběr tvrzení z původního textu i jejich uspořádání jsou dobře motivované a formulace jsou korektní .

**Práce se zdroji.** Text se sice primárně opírá o jediný článek a strukturou argumentace se mu příliš nevzdaluje, formulačně závislý na něm ovšem není.

**Formální úprava.** Formální náležitosti práce podle mého mínění nezasluhují podstatnější výtky. Text je poměrně čtivý a množství jazykových nepřesností je přiměřené jeho rozsahu.

### Připomínky a otázky

1. Argument závěr důkazu Lemmatu 3 je příliš stručný, z definice okamžitě plyne rovnost
$$\sum_{u\leq v} x^v y^{v+u} = \sum_{u\leq v} \prod_{i=1}^{n} x_i^{v_i} y_i^{v_i+u_i}$$
a nikoli požadovaná rovnost $\sum_{u\leq v} x^v y^{v+u} = \prod_{i=1}^{n} \sum_{u_i\leq v_i} x_i^{v_i} y_i^{v_i+u_i}$.

### Závěr

Práce Jany Hrúzové „Zobecněná integrální vlastnost" podle mého názoru splnila zadání a doporučuji ji uznat jako bakalářskou.

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

Jan Žemlička
Katedra algebry
22.6.2020