Oponentský posudek diplomové práce

Kateřina Teplá: Kerdock codes and around

Diplomová práce se zabývá Kerdockovými samoopravnými kódy, jejich konstrukcí a vlastnostmi a jejich aplikacemi v kombinatorice a kryptografii. V aplikacích se jedná o konstrukci kombinatorických designů, a tzv. "bent" a "resilient" funkcí.

Většina práce se zdá být kompilační, ovšem šíře diskutovaného tématu a různorodost použitých zdrojů rozhodně stojí za povšimnutí. Kerdockovy kódy jsou zajímavými a složitými objekty, jejichž ucelené představení v návaznosti na další obory je velice záslužné a vyžaduje dosti úsilí. Čtenářský dojem z tohoto slibně pojatého projektu ovšem kazí několik nedůsledností (dle mého názoru celkem zbytečně, ale bohužel nezanedbatelně).

Nejvíce matoucí mi připadá absence jakékoliv zmínky ohledně vztahu dvou netriviálních a hodně odlišných konstrukcí Kerdockových kódů v první kapitole. V dalším textu jsou volně používány vlastnosti těchto kódů, které jsou zřejmé jenom z jedné z těchto konstrukcí. Navíc obě konstrukce obsahují určité volby: V prvním případě musíme zvolit Kerdockovu množinu, v druhém případě pak základní primitivní polynom $h(x)$. Z textu není jasné, jakým způsobem se např. změna Kerdockovy množiny promítne do změny $h(x)$, nebo dokonce jestli polynom $h(x)$ vůbec odpovídajícím způsobem změnit lze.

Dále se v práci ve více důkazech vyskytuje zajímavý fenomén, kdy je argument k určitému ne zcela zřejmému kroku odbyt nebo takřka vypuštěn, a to v kontrastu k okolnímu textu, kde je vše velice dobře vysvětleno. Jedná se konkrétně o:

1. Theorem 1.2.15 na str. 17 a vysvětlení, proč $c(x)(x-1)h(x) = 0$,
2. poslední odstavec důkazu Theoremu 2.1.8 na str. 25,
3. důkaz Lemmatu 3.3.1, části (iii) na str. 43,
4. chybějící diskuzi počtu výskytů slov typu (iv) a (v) v důkazu Theoremu 3.3.3,
5. chybějící diskuzi, jak se od sebe navzájem odliší typy slov ve dvojicích zmíněných v prvním odstavci na str. 50,
6. nepříliš vysvětlený fakt, proč i nad $\mathbb{Z}_4$ platí rovnost $(\mathcal{C}^T)^\perp = (\mathcal{C}^\perp)^{0@T}$ na str. 51,
7. implikaci (i) $\Rightarrow$ (ii) v důkazu Theoremu 4.1.9 na str. 59.

Práci vytkl bych ještě několik nepřesností:

1. Ekvivalence
$$Q \text{ nesingulární} \iff \beta \text{ nesingulární.}$$
na str. 22 pro kvadratické formy v charakteristice 2 nemůže platit, viz např. $Q = id$ pro $V = F$.

2. Ekvivalence mezi Q a $Q + f$ na str. 23 je též špatně, např. rozdíl Q^+ a Q^- ze str. 25 je pro $F = \mathbb{F}_2$ lineární forma. Naštěstí argument na str. 36 je možné dokončit i bez použití tohoto chybného faktu.

3. V důkazu Theoremu 3.2.2 se ve skutečnosti dvěma způsoby počítají páry $(\mathbf{v}, \mathbf{c})$ takové, že $\mathbf{v}$ pokrývá $\mathbf{u}$ a má váhu $t + j$ a $\mathbf{c}$ patří do C a pokrývá $\mathbf{v}$ (viz první odst. na str. 40).

Na závěr bych zmínil místy poněkud matoucí použití členů (práce je napsána v anglickém jazyce).

I přes uvedené nedostatky je předložená práce velice zajímavá a prokazuje dobré porozumění tématu.

Práci **doporučuji uznat jako diplomovou** a hodnocení příkládám na zvláštním listě.

V Praze dne 13. 9. 2012 RNDr. Jan Šťovíček, Ph.D.