POSUDEK VEDOUCÍHO NA DIPLOMOVOU PRÁCI
JANA VACKA
POKRÝVACÍ MNOŽINY VE STEGANOGRAFII

Práce představuje základní myšlenky steganografie a některé metody vkládání. Má kompilační charakter, s výjimkou kapitoly 3.4 není příliš hluboká ani obtížná. Zejména v případě maticového vkládání se jedná o látku na úrovní základního kurzu samoopravných kódů. Přesto se v práci vyskytuje řada povrchností, nejasnosti a nepřesností, které nesvědčí o vysoké matematické kultuře a které uvádím níže.

Z obecného hlediska by práci prospělo konkrétnější a přesnější zhodnocení významu jednotlivých aspektů stegosystému. Opakovaně se např. konstatuje, že vyšší distorze zvyšuje riziko detekce, ale toto tvrzení zůstává na rovině prvoplánové samozřejmosti. Podobně by čtenář uvítal přesnější diskusi dilematu mezi relativní kapacitou a efektivitou.

Konkrétní výtky.

- Jak je v Definici 1.3.4 chápána absolutní hodnota rozdílu v případě prvků $\mathbb{Z}_p$?
- Na str. 9 oznámené značení Hammingovy vzdálenosti symbolem ϑ se v práci kromě dané podkapitoly nepoužívá.
- Veličiny měřící kvalitu stegosystému jsou popsány kostrbatě. Odkud pochází pravděpodobnostní rozdělení nosičů v Definici 1.3.3? Proč je míra změny v Definici 1.3.5 definována právě pro Hammingovu vzdálenost, když je sdělnost této volby v následujícím komentáři zpochybněna?
- Zarážející je základní definice kódu na str. 16, která hovoří bez vysvětlení o dimenzi *množiny*. Že se nejedná o pouhý překlep, dokládá až později následující definice kódu lineárního.
- Poznámka 1.6.18 na str. 20 je příliš slabá, v důkazu Tvrzení 1.6.20 na str. 21 a Tvrzení 2.4.1 na str. 31 je potřeba i opačná inkluze: každé $y \in C(s)$ je tvaru $x - c$ pro nějaké $c \in C$, tedy $C(s) = x + C$.
- Úvahy o projekci v sekci 2.1 jsou zmatené. Na str. 24 se diskutuje případ $p < q$, který byl na str. 23 vyloučen. Požadavek (2.1) by měl být asi součástí definice projekce. Nejasně je formulována informace o znaménkové reprezentaci prvků $\mathbb{Z}_q$. Rovnost na řádku -4, str. 24 totiž jistě platí bez dalšího. Naopak podobně formulovaný požadavek na str. 25 nahoře je pochybný: může být absolutní hodnota záporná? Podobně se zdá, že dvě následující podmínky jsou ekvivalentní a smysl požadavku je tedy nejasný. Celá pasáž o matematizaci nosiče, která měla umožnit snadnou manipulaci s jasně definovanými matematickými objekty, je ve výsledku asi spíše matoucí.
- Tvrzení 2.4.1 a Tvrzení 2.4.2 není nutné dokazovat odděleně, protože první z nich je speciálním případem druhého. Hodnota ${}_qR_a$ je podobně jako R_a průměrná vzdálenost od kódu v metrice d. Právě na tomto místě bylo možné pracovat s obecnou metrikou a dokázat tvrzení pro všechny metriky najednou. Tvrzení tedy nejsou pouze podobná, jak naznačuje poznámka na str. 33 nahoře.
- Popis ostranění dvojky na str. 53n je neúplný. Není řečeno, jak naložit se členem $3 \cdot 3^k$.
- Důkaz faktu, že čísel, která mají v trojkové soustavě zápis délky (nejvýše) n, je 3^n, působí středoškolsky.
- Definice 4.1.1 grafu je odbytá. Neorientovaný graf bez smyček bylo možné snadno získat definicí hrany jako neuspořádané dvojice $\{a, b\}$, $a \neq b$. Navíc se z definice zdá, že hrany mají být *všechny* dvojice.
- Definice 4.1.8 propásla příležitost použít definici distance.
- Co je $\mathbb{F}_{2d+1}$ na str. 69, řádek 12?

Po jazykové a gramatické stránce je práce pěkná, neobsahuje ani mnoho překlepů. V seznamu literatury se objevují položky bez udání zdroje ([9] a [10]). Nepodařilo se mi dohledat, odkud autor čerpá v kapitole 3.4.2, v uvedeném odkazu na [10] jsem konstrukci nenašel.

Přes uvedené nedostatky práci doporučuji k obhajobě.

Praha 10. května 2013 Štěpán Holub