Posudek oponenta na bakalářskou práci Michala Maršálka nazvanou APN functions with non-classical Walsh spectra

Motiv práce je dobře popsán. Student svými výsledky a výpočty přispěl k hledání nových APN funkcí, byť výsledek je negativní. Mezi kvalitou výsledků a formálním zpracováním je značný nesoulad. Nebudu v tomto posudku popisovat přínos práce. Ten je nezpochybnitelný a jistě bude obsažen v posudku vedoucího. Soustředím se na nedostatky, které jsou podle mého soudu dosti závažné, vezmeme-lí v úvahu poslání bakalářské práce.

strana 3. Theorem 1 má chybný důkaz. Jde o přehlédnutí, ale nepříjemné. Funkce $l_a(x)$ je definována špatně.

strana 3. V důkazu Theorem 1 se píše: "Uniqueness: Let $p, q \in \mathbb{F}_{2^n}[x]$ of degree at most $2^n - 1$," místo (například) "To prove uniqueness consider polynomials $p, q \in \mathbb{F}_{2^n}[x]$ of degree at most $2^n - 1$,". Úsečných formulací je v práci spoustu a místy je to výrazně na úkor srozumitelnosti.

strana 4. Funkce popisované v poznámce by bylo vhodné označit jako afinní.

strana 5. U definice Walsh-Hadamardovy transformace chybí diskuse, v jakém smyslu nezávisí na volbě skalárního součinu. Text v poznámce je nedostačující.

strana 5. Důkaz Lemmatu 5 je podivný. Zápis je chybný (obrat $b \in |\{$) a argumentace ve větě obsahující tento obrat je možná teprve po té, co je uvedena úvaha ve větě, která následuje.

strana 6. Nechápu, proč autor uvedl na straně 6 poznámku, že pro $u \in \mathbb{F}_{2^n}$ obvykle pod u^{-i} myslíme u^{2^n-1-i}. Proč obvykle?

strana 6. Theorem 9 je uveden bez důkazu i odkazu.

strana 7. Má být bivariate, ne bivariete.

strana 8. Důkaz Lemma 10 působí mimochodně. Začíná odkazem na Proposition 6, která má zaručovat, že nějaká nejasně definovaná množina řešení je vektorový prostor. Proposition 6 nijak o vektorovém prostoru nehovoří. V důkazu se píše o $\mathbb{F}_{2^n}$, ale n definováno není. Z kontextu se zdá, že nejde o pouhou záměnu n a m. Pak je tam věta začínající slovy "Each pair", která se nezdá dávat smysl.

Tvůrčí část od strany 10 dále je napsána tak, že se směr a smysl úvah autora dá sledovat. Nicméně formální úroveň je i zde velmi kolísavá. Některá místa vzbuzují značné rozpaky.

Například, když na straně 10 student volí hodnoty g_x a g_y a pak napíše "Different more complicated choices of g_x, g_y might lead to more or less equivalent results as simpler choices." Proč si to student myslí se ale čtenář nedozví.

Na straně 13 se používá cyklotomická rozkladová třída (cyclotomic coset). Jsou to orbity permutace $x \mapsto 2x$ v $\mathbb{F}_{2^n}$. To je něco jiného než definice uvedená na straně 6 dole.

Lemma 19 je uvedeno bez důkazu a komentáře.

Student použil v tvrzení 15 obratu "In order for the construction to work". Nebylo mi jasné, zda to work znamená dostat APN nebo APN s neklasickým spektrem.

Je patrné, že student do bakalářské práce vložil spoustu úsilí. Věřím, že tématice do hloubky rozumí. Kdyby práce obsahovalo polovinu výsledku a byla

napsána pečlivě, mohla by být hodnocena stupněm výborně. Nicméně v situaci tak, jak je, a s ohledem na instrukce garanta oboru, jež stanoví, že při hodnocení práce se klade důraz na schopnost prezentovat rigorózním a korektním způsobem matematický text, že každá práce by měla mít aspoň jednu část, na níž student tuto schopnost prokáže, a že při posuzování matematického textu se berou v úvahu: korektní a matematicky přesné definice používaných pojmů; jednoznačné, jasně definované a včas zavedené značení; přesně a správně stanovené předpoklady jednotlivých tvrzení; úplné a matematicky správné důkazy tvrzení a vět, nemá oponent jinou možnost, aby, byť s lítostí, navrhl hodnocení práce stupněm *dobře*.

Navrhuji, aby práce byla přijata jako práce bakalářská.

Aleš Drápal

V Praze 12. června 2019