# Posudek oponenta na diplomovou práci Dáši Krasnayové
# Constructions of APN permutations

Předložená práce pojednává o APN (almost perfect nonlinear) funkcích, které jsou zároveň permutacemi. Funkce $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ (kde $\mathbb{F}_{2^n}$ označuje konečné těleso s $2^n$ prvky) je APN, pokud rovnice $f(x+a) - f(x) = b$ má nejvýše dvě řešení pro všechna $a \in \mathbb{F}_{2^n}^*$ a všechna $b \in \mathbb{F}_{2^n}$. APN funkce mají důležité aplikace v kryptografii, neboť poskytují nejvyšší možnou ochranu proti diferenciální kryptoanalýze. Pro konstrukci některých typů blokových šifer, zejména typu SPN (substitution-permutation network), je důležité, aby APN funkce byla invertibilní, to znamená aby to byla permutace tělesa $\mathbb{F}_{2^n}$. Vlastnost APN je zachována při transformaci funkce pomocí CCZ ekvivalence (Theorem 1.9, strana 11 předložené práce), zatímco vlastnost, zda je funkce permutací, obecně není zachována při transformaci funkce pomocí CCZ ekvivalence. Pro liché hodnoty $n$ je známo mnoho příkladů APN permutací tělesa $\mathbb{F}_{2^n}$. Pro sudé hodnoty $n$ je známo, že neexistují APN permutace těles $\mathbb{F}_{2^2}$ a $\mathbb{F}_{2^4}$ a příklad APN permutace tělesa $\mathbb{F}_{2^6}$ je uveden v článku [3]. Existence APN permutací těles $\mathbb{F}_{2^n}$ pro sudé $n > 6$ je významný otevřený problém, kterému se věnuje předložená práce.

Práce je zahájena kapitolami 1 a 2, které shrnují výsledky známé z literatury. V hlavní části práce jsou studovány funkce velmi speciálního typu, uvedeného na začátku kapitoly 3 (první rovnice na straně 15). V kapitole 3 jsou vyvozeny podmínky, za kterých mají funkce tohoto typu vlastnost APN. V kapitole 4 jsou vyvozeny podmínky, za kterých jsou funkce tohoto typu CCZ ekvivalentní určitým speciálním permutacím tělesa $\mathbb{F}_{2^n}$. Pokud by výsledky kapitol 3 a 4 byly kompatibilní, celkově by umožňovaly konstruovat APN permutace. Bohužel v krátkém závěru práce (Conclusion) je konstatováno, že výsledky kapitol 3 a 4 jsou natolik vzájemně odlišné, že je nelze snadno propojit a dospět ke kýženému cíli. Možné propojení výsledků kapitol 3 a 4 pro obecné $n$ zůstává otevřeným problémem. Pro $n = 6$ a $n = 10$ výsledky kapitol 3 a 4 byly použity pro hledání APN permutací pomocí počítače. Pro $n = 6$ bylo nalezeno 84 APN permutací typu studovaného v kapitolách 3 a 4, zatímco pro $n = 10$ nebyly nalezeny žádné APN permutace tohoto typu.

APN permutace typu studovaného v předložené práci byly studovány již dříve a předběžné výsledky byly uvedeny v přednášce

P. Lisoněk, APN permutations and double simplex codes, Workshop Mathematics of Communications: Sequences, Codes and Designs. Banff International Research Station for Mathematical Innovation and Discovery, January 28, 2015.
Videozáznam této přednášky je dostupný on-line na adrese

http://www.birs.ca/events/2015/5-day-workshops/15w5139/videos/watch/201501281028-Lisonek.html

V této přednášce jsem vysvětlil, že trojčlenný tvar polynomů studovaný v článku [3] lze přirozeným způsobem rozšířit na určitý čtyřčlenný tvar tak, že pro zjišťování CCZ ekvivalence s permutacemi toto neznamená ztížení problému. Mnou navržený ctyřčlenný tvar je převzat a použit v předložené práci. Bylo by vhodné, aby v případných dalších publikacích autorka tento zdroj citovala. V mé přednášce je dále uvedeno, že pro $n = 6$ všechny APN permutace daného typu jsou navzájem CCZ ekvivalentní. Autorka uvádí seznam 84 APN permutací v příloze A (strana 36), avšak možný vzájemný vztah těchto funkcí není v práci nijak zmíněn. Navrhuji, aby autorka nezávisle ověřila, že všechny funkce uvedené v příloze A jsou skutečně navzájem CCZ ekvivalentní.

V práci jsem zpozoroval několik drobných chyb, které považuji spíše za překlepy. Za jediný závažnější problém považuji způsob, jakým autorka diskutuje řešení polynomiálních rovnic. Například na straně 16 čteme "This means that (3.4) should have no solutions" kde (3.4) je polynom uvedený výše na téže straně, a podobně formulovaná tvrzení se vyskytují na mnoha místech předložené práce. Nelze říci, že polynomiální rovnice nemá řešení. Taková rovnice má vždy řešení, a to buďto v tělese koeficientů rovnice, anebo v nějakém algebraickém rozšíření tohoto tělesa. Proto je naopak důležité zdůraznit, ve kterém tělese se řešení hledají nebo tam neexistují. Například uvedená polynomiální rovnice (3.4) má koeficienty v tělese $\mathbb{F}_{q^2}$, ale neexistence řešení se dokazuje pouze v podtělese $\mathbb{F}_q$ (což však není uvedeno).

Předloženou práci považuji za velmi kvalitní, protože se zabývá velmi náročnou tématikou, používá technicky náročné postupy a dospívá k novým výsledkům. Výsledky v kapitolách 3 a 4 se jeví být originálním příspěvkem autorky. Doporučuji práci uznat jako diplomovou a hodnotit ji známkou výborně.

Burnaby, 31. srpna 2016

RNDr. Petr Lisoněk, Ph.D.
Professor
Department of Mathematics
Simon Fraser University
Burnaby, BC
V5A 1S6
Canada