# Posudek oponenta na diplomovou práci Jiřího Pavlů nazvanou Search of APN permutations among known APN functions

Práci považuji za vynikající co do výsledků. Rovněž i rozhled studenta a jeho formulační schopnosti jsou na vysoké úrovni. Po formální stránce však práce vykazuje množství nedopatření. Angličtina je přijatelná, byť ne vynikající. Problém je příliš velké množství přehlédnutí v důkazech i definicích. Po seznámení se s prací jsem autorovi poslal seznam chyb, který se stal základem pro Errata, jež vložil do Studijního informačního systému. S jednou výjimkou, která se týkala reprodukce důkazu převzatého z literatury, šlo ve všech případech o chyby zápisu, nikoliv o věcné neporozumění.

Prvých dvacet stran je dobrým úvodem do problematiky. Bylo by lépe některé začáteční pasáže nahradit odkazem na literaturu a místo toho dokázat některá fakta (například ekvivalenci dvou definic APN funkce).

Dalších pět stránek informuje o výsledcích Dillona. Jejich vylepšení je vlastní cíl práce. Hlavní výsledky práce jsou tedy v kapitole 3. Ta má rozsah osmi stran a vedle popisu algoritmu je tam i jeden teoretický výsledek. Dosažené výsledky jsou dobře vyloženy na začátku kapitoly tři, proto je nebudu zde reprodukovat.

Celkově to působí velmi povedeně. Jádrem výsledku je pozorování, že pokud se soustředíme na po složkách zarovnané funkce (componentwise plateaued functions), tak je možné test CZZ ekvivalence omezit na nezprohýbanou část $NB_f$.

Práci doporučuji uznat jako práci diplomovou. Bude-li přihlédnuto k opravám přiloženým k práci, lze vzhledem ke kvalitě výsledků práci podle mého soudu hodnotit stále ještě stupněm *výborně*.

Aleš Drápal

V Praze 28. srpna 2018