Ivo Machek: Kvazigrupy, jednosměrné funkce a hašování

POSUDEK VEDOUCÍHO DIPLOMOVÉ PRÁCE

Předloženou diplomovou práci považuji za velmi kvalitní. V obecné rovině je zaměřena na důkaz toho, že existují beztvaré kvazigrupy ve smyslu Gligoroského a Markovského, pro které lze najít efektivní způsob řešení kvazigrupových rovnic.

Ve speciální části se jednak dokazuje, že kvazigrupy uvažovaného typu bychom dostali při návrzích hašovacích funkcí typu *Edon*, pokud bychom vynechali rotační krok návrhu, jednak se dalším pokračováním v daném směru úvah nalezne algoritmus, který sice neznamená teoretické prolomení hašovací funkce *Edon-R-II*, ale přesto ho lze považovat za útok, jenž poukazuje na její slabiny.

Práce je po formální stránce napsaná v zásadě korektně; místy je ovšem formulačně nepříliš obratná. Jazykových prohřešků není zcela zanedbatelně (namátkou, chybějící čárka ve *vždy poznáme k jaké kvazigrupě*, strana 31, *získané ztohoto vztahu*, strana 64, *standart*, strana 75) celkově však nejde o takový počet nedopatření, které by rušilo při čtení.

Doporučuji, aby práce byla uznána jako diplomová a hodnocena známkou velmi dobře.

V Praze 18. května 2009

Aleš Drápal