Posudek oponenta na diplomovou práci

Jana Kučerová:

Řešení soustav diferenčních rovnic
pro sčítání a booleovské operace

Grupovým párem se rozumí dvojice grupových operací $+, \circ$ na téže dané množině. Diferenční rovnicí se pak rozumí rovnice

$$(x \circ a) + (y \circ b) = (x + y) \circ c$$

kde a,b,c jsou prvky dané množiny. Předložená práce je podstatným zobecněním práce autorů S. Paula a B. Preneela, v níž je nalezen algoritmus, pracující v polynomiálním čase, pro řešení soustav diferenčních rovnic v grupovém páru tvořeném množinou mohutnosti 2^n, s operacemi sčítání modulo 2^n a xor. Zobecnění se vztahuje na tzv. husté abelovské grupové páry, v předložené práci zavedené a studované.

Práce má velmi pěknou úroveň, obsahuje originální výsledky a je sepsána přehledným a srozumitelným způsobem.
Práce zcela vyhovuje podmínkám pro diplomovou práci a navrhuji ji hodnotit známkou výborně.

V Praze dne 13.8.2008

Prof. RNDr. Jaroslav Ježek, DrSc.