Posudek oponenta k bakalářské práci
Lineární rekurentní posloupnosti nad konečnými tělesy
Michala Szabadose

Předložená práce se zabývá posloupnostmi prvků konečného tělesa T, které lze zadat pomocí rekurentního vztahu tvaru $s_{n+k} = a_0 s_n + \cdots + a_{k-1} s_{n+k-1}$, kde $a_0, \ldots, a_{k-1} \in T$, a jejich aplikací pro konstrukci pseudonáhodného generátoru. Takto zadané posloupnosti se nazývají lineární rekurentní posloupnosti řádu k. Hlavní částí je třetí kapitola, ve které je odvozen tvar explicitního vyjádření lineární rekurentní posloupnosti (Věta 3.8). Dále je ukázáno, že lineární rekurentní posloupnost musí být periodická a je vysvětleno, jak minimální délka periody souvisí s minimálním polynomem rekurence (Věta 3.25) a doprovodnou maticí minimální rekurence posloupnosti (Věta 3.21). Z této teorie je pak vidět existence lineárních rekurentních posloupností s maximální možnou minimální periodou velikosti $|T|^k - 1$. Ve čtvrté kapitole se pak studují zejména tyto posloupnosti především z hlediska možnosti použít je jako generátor pseudonáhodných čísel. Jako kritéria náhodnosti jsou zde zkoumány varianty distribučního, sériového, korelačního a decimačního testu v rámci celé periody. Obtížnější tvrzení týkající se menších částí periody nejsou uvedena. V závěru čtvrté kapitoly je vyřešeno několik cvičení z knihy Lidla a Niederreitera. Práci uzavírá implementace pseudo-náhodného generátoru pomocí posloupnosti s periodou $2^{64} - 1$ nad F_2.

Práce je sepsána velmi srozumitelně a pečlivě. Většinu uvedených důkazů autor vymyslel sám. Určité problémy způsobuje nutnost připustit i rekurence řádu 0 (nulovou posloupnost). Tvrzení 3.17 pro $k = 0$ pak říká, že nulová posloupnost má periodu nula. Dále je zde několik drobností: V poznámce u Definice 3.22 měl být polynom $x^{q^k-1} - 1$ a na straně 28 dole nejspíš mělo být, že nenulový k-vektor se vyskytuje v periodě jednou.

Předloženou práci proto doporučuji k obhajobě s hodnocením *výborně*.

V Praze, 7. 9. 2010