POSUDEK BAKALÁŘSKÉ PRÁCE "IRREDUCIBLE POLYNOMIALS MODULO p"

MICHAL FEROV

V práci je navrhnut probabilistický algoritmus pro konstrukci nerozložitelného polynomu stupně n nad q-prvkovým tělesem $\mathbb{F}_q$, s očekávanou složitostí $O(n^3 \log(n) \log(q) + n^3 \log(n) \log(\omega(n)) + n^3\omega(n))$, kde q je prvočíslo a $\omega(n)$ značí počet prvočísel, které dělí n. Značná část práce je věnována důkazu, že popsaný algoritmus má danou očekávánou složitost. Nejprve uvedu připomínky k jednotlivým částem práce.

První kapitola je motivací k řešenému problému a přehledem základních pojmů. Domnívám se, že by mělo být lépe voleno co v úvodu zmínit. Není nutné uvádět v části 1.2 definici a elementární vlastnosti těles. Stačilo by začít Větou 1.2 a následujícími lemmaty. Naopak by mohly být zmíněny vlastnosti konečných těles využité například v části 1.3. Konkrétní připomínky k první kapitole jsou tyto:

- Strana 7, řádky 1,2,11, atd : Častější než *Euclidian* je *Euclidean*;
- Strana 7, řádek 18 : *In fact, any polynomial somehow defines an extension.* Není mi zcela jasný smysl této věty;
- Definice 1.3 : Rozklad polynomu na lineární činitele v uvedém tvaru je v pořádku jen pro monické polynomy;
- Důkaz Lemmatu 1.3 : *The order of* $\mathbb{F}^*$ *is* q - daný řád je $q-1$;
- Důkaz Věty 1.5 : Místo m má být všude n. Ve třetím řádku je F místo f;
- Lemma 1.7 : Místo *following the conditions* má být *the following conditions*;

Ve druhé kapitole je odhadnut počet nerozložitelných polynomů stupně n nad konečným tělesem $\mathbb{F}_q$ a odtud jsou odvozeny odhady pravděpodobnosti, že náhodně vybraný polynom stupně n je nerozložitelný. Detailní připomínky k této kapitole jsou následující:

- Důkaz Věty 2.2, řádek 1 : Před $\mu(d)H(\frac{n}{d})$ chybí $\sum_{d|n}$;
- Strana 13, řádek 7 : Místo *all monic polynomials whose degree divides n* by mělo být *all monic irreducible polynomials whose degrees divide n*;
- Strana 13, řádek 10 : Místo

$$N_q(n) = \sum_{d|n} dN_q(d)$$

  má být

$$q^n = \sum_{d|n} dN_q(d)$$

  ;
- Strana 13, řádek -3 : $H(n) = q^n.H(n) = \sum_{d|n} h(d)$ ... - Příklad proč nezačínat novou větu v matematickém modu;
- Lemma 2.5 : Je nutné předpokládat, že $1 < n$. Pro $n = 1$ nerovnost neplatí;

- Strana 15, řádek -1 : Výraz

$$\frac{1}{n}\left(1-\frac{1}{q^{\frac{n}{2}+}}+\frac{1}{q^n}\right)$$

není správně;
- Strana 16, řádek -3 : *If we use* $\frac{1}{2n}$ *as the probability* → lépe by bylo například: *If we estimate the probability by its lower bound* $\frac{1}{2n}$;
- Strana 16, řádek -2 : Místo k má být i;

Ve třetí, poslední, kapitole je sestrojen algoritmus, který hledá nerozložitelný polynomu stupně n nad q-prvkovým tělesem $\mathbb{F}_q$ a je odhadnuta jeho složitost. V kapitole je opět řada nepřesností. Uvedu jen některé z nich.

- Úvod části 3.1 : Co je to n_i, h_i?;
- Důkaz Lemmatu 3.1, řádek 2 : the second → The second;
- Strana 19, řádek -11 : Following algorithm → The following algorithm;
- Strana 19, řádek -10 : $\deg(a) \leq \deg(f) = n \rightarrow \deg(\alpha) \leq \deg(f) = n$;
- Strana 19, řádek -9 : Místo $i \in \{1, \ldots, r\}$ má být $i \in \{1, \ldots, k\}$;
- Atd...;

Obsahově je práce vynikající, po formální stránce je však odbytá. Práci navrhuji uznat jako práci bakalářskou. Vzhledem k množství drobných nepřesností navrhuji hodnotit ji známkou velmi dobře.

V Praze dne 26.8.2008, Pavel Růžička