Posudek oponenta k diplomové práci
Ideal lattices in cryptography
Sáry Vyhnalové

Předložená práce se zabývá ideálovými mřížemi, tedy celočíselnými mřížemi, které kanonicky reprezentují ideál okruhu $\mathbb{Z}[x]/(q)$, kde q je monický celočíselný polynom. Řada konstrukcí mřížové kryptografie není pro praktické využití dostatečně efektivní a využití ideálových mříží představuje možnost jistého zefektivnění. Nevýhodou naopak je, že teoretické výsledky, od kterých se odvozuje bezpečnost konstrukce, zpravidla nejsou pro ideálové mříže dokázány. Jsou známy i případy, kdy optimalizace pomocí ideálových mříží představovala zásadní problém pro bezpečnost kryptosystému. Schopnost rozhodnout, zda je daná celočíselná mříž ideálová, se proto jeví jako přirozený problém mřížové kryptografie. Tomuto problému je také věnovaná podstatná část této práce.

Po zavedení značení a připomenutí základních pojmů v kapitolách 1 a 2 je ve třetí kapitole popsán algoritmus, který řeší výše popsaný problém pro úplné celočíselné mříže (sekce 3.1). Algoritmus, případně myšlenky, na kterých je založen, je aplikován na příkladech (sekce 3.2). Důležitý problém, kdy je celočíselná mříž (metricky) izomorfní ideálové mříži, je pro speciální případ diskutován v sekci 3.3. Čtvrtá kapitola řeší problém detekce NTRU mříží a jejich zobecnění. Pátá kapitola stručně demonstruje možnost kryptografického využití mříží.

Práce vychází zejména z článku J. Ding, R. Lindner: *Identifying ideal lattices* z roku 2007. Autorka doplňuje různé detily do důkazů, formuluje a dokazuje několik vlastních tvrzení (Proposition 20 a Lemma 21). Za asi největší vlastní přínos práce považuji Theorem 29, kde autorka zobecňuje Theorem 3 z článku Dinga a Lindnera. Rovněž většinu čtvrté kapitoly lze považovat za vlastní práci autorky.

Po formální stránce je práce psána velmi pečlivě a s minimem překlepů. Za jediný vážnější problém považuji využití CRT v Algoritmu 1 (viz konkrétní připomínky níže).

Po obsahové stránce práce působí poměrně elementárně - nevyužívá žádný komplikovanější aparát (což osobně nepovažuji za problém). Potenciál tématu ale nebyl zcela vyčerpán: Chybí odhad složitosti algoritmu, lze si představit verzi Algoritmu 1, která by pracovala i s mřížemi, které nejsou úplné (diskuse v sekci 2.2.6 se týká pouze situace, kdy je polynom q ireducibilní). Pátá kapitola mohla jít více do hloubky, například ukázat algoritmy, které netriviálním způsobem využívají ideálové mříže.

Celkově si myslím, že práce splnila zadání a doporučuji ji uznat jako práci diplomovou.

V Praze, 7. 9. 2021

Pavel Příhoda

Konkrétní připomínky k práci:

- str. 14, předposlední řádek důkazu: v součtu by měl být sčítanec ar_0
- str. 16 uprostřed: matice označená jako T by měla být transponovaná
- str. 17, Proposition 20: Mělo by být vysvětleno, co je d (podobně i v dalších tvrzeních).
- str. 18, ř.-7: finally $\rightarrow$ finitely
- str. 20, Algoritmus 1: Pro využití CRT na řádku 8 bychom podle Theorem 3 potřebovali z a d/z nesoudělná, což asi obecně platit nemusí. Ani z důkazu Theorem 23 mi není jasné, jak tento problém vyřešit.
- str. 22, kongruence (3.3), (3.4) a kongruence nad (3.3): tyto platí modulo d/z
- str. 27, ř. 12: rovnost $u_3 = u_4$ má být $u_3 = -u_4$, v matici níže na diagonále pak prvek $-u_3$ místo u_3
- str. 30, Proposition 28: V popisu množiny v části (b) by měla být podmínka $c \neq 0$.
- str. 30, Proposition 28, důkaz: Pro důkaz inkluze $\subseteq$ bychom potřebovali ověřit uzavřenost pravé strany dokazované inkluze na grupové operace.
- str. 31, ř. -5: $\cos(\alpha) = \cos(\pi - \alpha) \rightarrow -\cos(\alpha) = \cos(\pi - \alpha)$
- str. 33, ř. 4: Znamínka v matici uprostřed.
- str. 37, Proposition 32: Přidal bych předpoklad $n > 1$ (argument v důkazu neprojde pro $n = 1$ a $\lambda = \mu$).