POSUDEK VEDOUCÍHO/OPONENTA BAKALÁŘSKÉ PRÁCE

Název: Metody odhalování denních klíčů u Enigmy
Autor: Dominika Kubániová

Shrnutí obsahu práce

Práce pojednává o metodách odhalování denních klíčů u Enigmy po 15.9.1938. Tehdy došlo ke změně protokolu, která vyžadovala vytvoření zcela nových metod.Práce se zabývá metodami vytvořenými v Polsku – Rejewského bombou a Zygalského plachtami. A dále Turingovou bombou, která by zásadní pro odhalování denních klíčů po další změně protokolu v květnu 1940. Turingova bomba byl první „programovatelný" počítač.

Jádro práce spočívá v matematické formulaci a odůvodnění uvedených metod.

Celkové hodnocení práce

Téma práce. Téma je pro bakalářskou práci vhodné a bylo autorkou výborně naplněné.

Vlastní příspěvek. K tématu práce sice existuje mnoho zdrojů, ale jejich úroveň je velmi různá. Až na originální Turingovu „Prof's Book" a pár stručných poznámek v některých Rejewského pracích jde výhradně o druhotné popularizační práce postrádající jakékoliv matematické zdůvodnění. Vlastní přínos autorky spočívá ve formulaci a důkazech matematických tvrzení potvrzujících funkčnost uvedených metod.

Matematická úroveň. Jaká je matematická úroveň práce? Práce obsahuje rigorózně a korektně zformulovaná matematická tvrzení. Protože jde o aplikované téma, práce obsahuje i popisné části týkající se konstrukce Enigmy a protokolů pro její používání.

Práce se zdroji. Zdroje jsou správně citovány a práce neobsahuje žádné doslova zkopírované nebo otrocky přeložené pasáže. Práce se zdroji byla hodně náročná, autorka musela vyhledat a přečíst řadu článků a vytřídit z nich ty nepodstatné.

Formální úprava. Formální zpracování práce je na vysoké úrovni.

Připomínky a otázky

1. Část 4.4.1 lze formulovat více matematicky – po přidánímkabelu propojujícího vstup s výstupem Turingova bomba vlastně počítá orbitu v nějaké permutační grupě. Můžete tuto grupu definovat pomocí generátorů
2. Které otázky týkající se metod odhalování denních klíčů podle Vás ještě zůstávají ještě nezodpovězené?

Závěr

Práci považuji za výbornou a doporučuji ji uznat jako bakalářskou práci. Po jistém dopracování jsou matematické části práce publikovatelné.

Doc. RNDr. Jiří Tůma, DrSc
Katedra algebry MFF UK
5.9.2018