Posudek vedoucího diplomové práce

Název: CRC-kódy
Autor: Filip Lorenc

Tématem práce Filipa Lorence je matematický popis polynomiálních kódů a jejich využití v protokolech CAN a CAN FD. Hlavní řešený problém práce představuje schopnost této třídy kódů, které jsou při kódování pomocí dělení se zbytkem v technické praxi označovány jako CRC-kódy (Cyclic redundany check), odhalit a případně opravit chybu.

Text vedle úvodu a závěru sestává ze čtyř kapitol. Zatímco první kapitola je věnována uvedení základních vlastností polynomiálních kódů, už druhá část se zabývá schopností této třídy kódů odhalit chybu v závislosti na generujícím polynomu. Kromě standardní otázky vzdálenosti kódů je diskutována schopnost kódu odhalit shluky chyb. Samotnými CRC-kódy, které lze interpretovat jako kódování polynomiálních kódů pomocí matic ve standardním tvaru, se zabývá třetí kapitola, jejímž hlavním výsledkem je porovnání efektivity implementací těchto tohoto kódování. Rozsáhlá čtvrtá část práce se zabývá dvěma variantami protokolu CAN, který je na CRC-kódování založen. Vedle popisu protokolů je diskutován problém jeho zranitelnosti, způsobený přidáváním synchronizačních bitů. Na závěr je provedena analýza generujících polynomů, které jsou v protokolech CAN fakticky využívány.

Ačkoli je kódování pomocí polynomiálních kódů v praxi široce využívané, drtivá většina literatury matematický pohled (ke své škodě) zcela pomíjí a věnuje se ryze technickým implementačním otázkám, v nichž zaniká i elementární a velmi užitečný fakt, že obvyklý kódovací algoritmus tvoří lineární zobrazení dané generující maticí ve standardním tvaru. To pro studenta znamenalo, že i část věnovaná matematickému popis CRC-kódů soustředěná v prvních třech kapitolách a původně zamýšlená jako kompilační, je z podstatné části výsledkem studentovy samostatné práce. Vedle řady detailů a příkladů týkajících se odhalení chyb nebo shluků chyb v prvních dvou kapitolách je do značné míry původní celá třetí kapitola textu. Rovněž v aplikační části je podstatná část popis zranitelnosti protokolů CAN originální a ač nenabízí efektivní řešení, jak spolehlivost protokolu CAN zlepšit, zdá se být velmi zajímavým (byť negativním) výsledkem.

Práce je podle mého mínění napsána pečlivě a přesně a přesto velmi čtivě. Ačkoli matematický popis řešených otázek vystačí jen s lineární algebrou a základy polynomiální algebry, je korektní a poměrně elegantní. Všechny (drobné) nedostatky, kterých jsem si v pracovních verzích práce všiml, autor opravil a k předložené práci tak nemám žádné matematické ani jazykové námitky.

Práce Filipa Lorence *CRC-kódy* bez pochyby úspěšně naplnila zadání a doporučuji ji uznat jako diplomovou.

Jan Žemlička
Katedra algebry
14.6.2021