Jméno:

Samoopravné kódy

Domácí úkol 8

Termín odevzdání: 20. dubna 2020 do půlnoci

Problém 1. Na přednášce jsme si definovali BCH kódy pomocí parametrů q, m, δ, ale nerozebírali jsme, jak se BCH kód změní v závislosti na tom, kterou primitivní $(q^m - 1)$-ní odmocninu z jedné zvolíme jako α. Ve skutečnosti změna α vede na ekvivalentní kód; v tomto úkolu si ukážeme speciální případ tohoto jevu, který už vede na obecný důkaz.

Buď $p = 9283$; to je prvočíslo (to mi můžete věřit nebo si to zkontrolovat na počítači). Buď δ nějaké číslo z množiny $\{1, 2, \ldots, 1000\}$. Uvažme kód $\mathrm{BCH}_{p,1,\delta}$. Prvek $\alpha = 2$ je generátor grupy $\mathbb{F}_p^\star$ (to mi zase můžete věřit).

1. Buď $\beta = 2^5$ (počítáno v $\mathbb{F}_p$). Dokažte, že β je také generátor grupy $\mathbb{F}_p^\star$. Chci aspoň krátký argument, který je o podrobnější než „známe to z Algebry I“.

2. Označme $\mathcal{C}$ BCH kód sestávající z polynomů f stupně $\leq p - 1$ nad $\mathbb{F}_p$ takových, že $f(\alpha), f(\alpha^2), \ldots, f(\alpha^{\delta-1}) = 0$.

   Označme $\mathcal{D}$ BCH kód sestávající z polynomů f stupně $\leq p - 1$ nad $\mathbb{F}_p$ takových, že $f(\beta), f(\beta^2), \ldots, f(\beta^{\delta-1}) = 0$.

   Dokažte, že kódy $\mathcal{C}$ a $\mathcal{D}$ jsou ekvivalentní.

Prosím, neřešte úlohu metodou hrubé síly na počítači; tím se nic moc nenaučíte. Ta konkrétní čísla jsou tam proto, abyste si mohli snáze představit, co se děje. Pokud chcete použít Sage nebo Mathematicu na experimenty, tak to je samozřejmě OK, ale nakonec byste měli najít krátké abstraktní řešení.

Při rešení úloh je možné se poradit s dalšími lidmi (nejlépe s Vašimi spolužáky a spolužačkami), ale svá řešení *pište samostatně* a před termínem odevzdání úloh sepsaná řešení nikomu *neukazujte*.