Códigos e curvas algébricas

Gregory Duran Cunha

Instituto de Matemática e Estatística
Universidade Federal de Goiás

Resumo

Códigos algébricos geométricos são códigos lineares construídos via curvas algébricas definidas sobre um corpo finito $\mathbb{F}_q$. Tal construção foi originalmente introduzida por Goppa [2] e assim estes códigos ficaram também conhecidos por códigos de Goppa. Estes códigos são construídos a partir de certas funções racionais, cujos polos se concentram em um dado divisor $\mathbb{F}_q$ -racional F , por avaliando elas em algum conjunto de pontos $\mathbb{F}_q$ -racionais disjunto de $\text{Supp}(F)$. O dual destes códigos pode ser obtido utilizando os resíduos de formas diferenciais. Neste trabalho, consideramos uma família de curvas planas não singulares $\mathcal{X}$ tal que existem três retas distintas que cortam em $\mathcal{X}$ os divisores $nP_1 + P_2$, $nP_2 + P_3$, e $nP_3 + P_1$. Fazendo um estudo sobre semigrupos de Weierstrass e lacunas puras em $\mathcal{X}$, construímos códigos de Goppa com uma boa cota para a distância mínima em relação à cota de Goppa.

Referências

- [1] H. STICHTENOTH, *Algebraic function fields and codes*, Springer-Verlag, Berlin, 1993.
- [2] V.D. GOPPA, *Codes associated with divisors*, Problemy Peredachi Informatsii. 13 (1977), 33–39.
- [3] C. CARVALHO; F. TORRES, *On Goppa codes and Weierstrass gaps at several points*, Des. Codes and Cryptogr.. 35 (2) (2005), 211–225.
- [4] M. HOMMA; S. J. KIM, *Goppa codes with Weierstrass pairs*, J. Pure Appl. Algebra. 162 (2-3) (2001), 273–290.