

Meeting: 998, Houston, Texas, SS 17A, Special Session on Coding Theory and Cryptography

998-94-214

Horacio Tapia-Recillas* (htr@xanum.uam.mx), Av. Sn Rafael Atlixco #186, Col. Vicentina, Iztapalapa, 09340, Mexico, D.F., 09340 Mexico, D.F., D.F., Mexico. *Repeated-root p -cyclic codes.*

J. van Lint discussed the question of binary cyclic codes with repeated-roots. If n is an odd integer, g_1, g_2 are coprime polynomials over \mathbb{F}_2 divisors of $x^n - 1$ let C_1, C_2 be the cyclic codes of length n generated by g_1 and g_1g_2 respectively. Then, up to a permutation, he proved that the Gray map image $\Phi(C_2 + 2C_1)$ is the cyclic code of length $2n$ generated by $g_1^2g_2$. Let p be a prime, $n > 0$ an integer such that $(p, n) = 1$ and C_j the \mathbb{F}_p -cyclic code of length n generated by $g_1g_2 \cdots g_j$, for $j = 1, 2, \dots, p$, where $g_i \in \mathbb{F}_p[x]$ are coprime divisors of $x^n - 1$. Let $D = (C_p \oplus_p \cdots \oplus_p C_2) + pC_1 \subseteq \mathbb{Z}_{p^2}^n$ and let Φ be the (generalized) Gray map on $\mathbb{Z}_{p^2}^n$. In this talk it will be shown that the image $\Phi(D)$ is, up to a permutation, a \mathbb{F}_p -cyclic code of length pn generated by $g_1^p g_2^{p-1} \cdots g_{p-1}^2 g_p$. An example will be presented.

¹Supported by Red de Criptología (CONACYT-UAM). (Received March 02, 2004)