21-238, Math Studies Algebra 2, Department of Mathematical Sciences, Carnegie Mellon University
Spring 2012: Monday, Wednesday, Friday, 10:30 am, Doherty Hall 1211.
Luc Tartar, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

25- Wednesday March 21, 2012.

Remark 25.1: There are particular linear codes which show a richer algebraic structure, for which it is useful to write an element of F^n as $a = (a_0, \ldots, a_{n-1})$ and consider it as the polynomial $a(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} \in F[x]$, and one then refers to elements of C as *code polynomials.*

It is also useful to denote $F[x]_n$ the vector space of polynomials of degree $\leq n-1$, and to consider it as the ring $F[x]/(x^n-1)$, quotient of $F[x]$ by the (principal) ideal (x^n-1) generated by x^n-1; one then writes $A \star B$ for the product *modulo* x^n-1 of two polynomials $A, B \in F[x]_n$.

Definition 25.2: A linear code $C \subset F^n$ is called a *cyclic code* if $\sigma(a) \in C$ for all $a \in C$, where the *cyclic shift* σ: $F^n \mapsto F^n$ is defined by $\sigma(a_0, \ldots, a_{n-1}) = (a_{n-1}, a_0, \ldots, a_{n-2})$ for all $a = (a_0, \ldots, a_{n-1}) \in F$.

Lemma 25.3: If C is a linear code over F, then it is a cyclic code if and only if $x \star a(x) \in C$ for all $a(x) \in C$.

A subspace C of $F[x]_n$ is a cyclic code if and only if C is an ideal of the ring $F[x]_n$. If C is a non-zero ideal of the ring $F[x]_n$, then there exists a unique *monic* polynomial g of least degree in C, called the *generator polynomial* of C because $C = (g)$; g divides x^n-1 in $F[x]$,[1] and the monic polynomial h such that $x^n - 1 = g\,h$ is called the *check polynomial* of C (see Lemma 25.6); g divides every $a \in C$ in $F[x]$.
Proof: The characterization of cyclic codes follows from the observation that $b = \sigma(a)$ corresponds to $b(x) = x \star a(x)$.

If g_1 and g_2 are two monic polynomials in C of least degree m $(\leq n-1)$, then $a = g_1 - g_2 \in C$ has degree $< m$ or is 0, so that $a = 0$ by minimality of m. Writing $x^n - 1 = g\,q + r$ with $degree(r) < m$ or $r = 0$, so that $r(x) = -g(x) \star q(x)$ in $F[x]_n$, one deduces that $r \in C$, and $r = 0$ by minimality of m. For $a \in C$, one has $a = g\,q + r$ with $degree(r) < m$ or $r = 0$, and since $degree(g\,q) \leq n-1$ because $degree(a) \leq n-1$ and $m \leq n-1$, one has $a = g \star q + r$ in $F[x]_n$, so that $r \in C$, and $r = 0$ by minimality of m.

Remark 25.4: For a given finite field F, one then finds all the non-trivial cyclic codes of length n over F (i.e. $C \neq F^n$ and $C \neq \{0\}$) by using the factors g of x^n-1 in $F[x]$ with $1 \leq degree(g) \leq n-1$.

The choice $g = x - 1$ corresponds to $a \in C$ if and only if $a(1) = 0$: it means that $a_0 + \ldots + a_{n-1} = 0$, i.e. the parity-check matrix $H = [\,1, \ldots, 1\,]$.

The choice $g = 1 + x + \ldots + x^{n-1}$ corresponds to $a \in C$ if and only if $a = \lambda\,g$ for a scalar $\lambda \in F$: it means that $a_0 = \ldots = a_{n-1}$, i.e. C is the repetition code.

Remark 25.5: If $C \subset F[x]_n$ is a cyclic code with generator polynomial $g(x) = g_0 + \ldots + g_r x^r$ with $g_r = 1$ (and $1 \leq r \leq n-1$), then C has dimension $n-r$ and a generator matrix of C is the $(n-r) \times n$ matrix

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & \cdots & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & \cdots & \cdots & g_{r-1} & g_r & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & g_0 & \cdots & \cdots & \cdots & \cdots & g_r \end{bmatrix},$$

and a message word $u = (u_0, \ldots, u_{k-1})$ with $k = n - r$ corresponds to the message polynomial $u(x) = u_0 + \ldots + u_{k-1}x^{k-1}$, and is encoded as $u(x)g(x)$.

Lemma 25.6: If $C \subset F[x]_n$ is a cyclic code with check polynomial $h(x) = h_0 + \ldots + h_k x^k$ with $h_k = 1$ (and $1 \leq k \leq n-1$), then $a(x) \in F[x]_n$ belongs to C if and only if $a \star h = 0$.
Proof: If $c = u\,g$, then $c\,h = u\,g\,h = u\,(x^n-1) = 0 \pmod{x^n-1}$, i.e. $c \star h = 0$. Conversely, $a \star h = 0$ means $a\,h = v\,(x^n-1)$ in $F[x]$ for a polynomial $v \in F[x]$, and since $x^n - 1 = g\,h$ one deduces that $a = v\,g$, because $F[x]$ is an integral domain; then, $degree(v) \leq k-1$ because $degree(a) \leq n-1$ and $degree(h) = k$, and $F[x]$ is an integral domain.

[1] If C is the ideal generated by $P \in F[x]_n$, then P has minimal degree in C if and only if P divides x^n-1.

Lemma 25.7: If C is a cyclic $[n,k]$-code with check polynomial $h(x) = h_0 + \ldots + h_k x^k$ with $h_k = 1$, then a parity-check matrix for C is the $(n-k) \times n$ matrix

$$H = \begin{bmatrix} h_k & h_{k-1} & \ldots & \ldots & \ldots & h_0 & 0 & 0 & \ldots & 0 \\ 0 & h_k & \ldots & \ldots & \ldots & h_1 & h_0 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & \ldots & 0 & h_k & \ldots & \ldots & \ldots & \ldots & h_0 \end{bmatrix}.$$

The dual code $C^\perp$ is cyclic and generated by the polynomial $\overline{h}(x) = h_k + \ldots + h_0 x^k$.
Proof: If $a(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} \in C$, then $a \star h = 0$; since the product $a\,h$ in $F[x]$ has degree $\leq n+k-1$, the coefficient of x^i in $a \star h$ coincides with the coefficient of x^i in $a\,h$ for $i = k, \ldots, n-1$, hence $a_{i-k}h_k + a_{i-k+1}h_{k-1} + \ldots + a_i h_0 = 0$ for $i = k, \ldots, n-1$; this is exactly saying that $H\,\begin{bmatrix} a_0 & \ldots & a_{n-1} \end{bmatrix}^T = 0$, hence the rows of H belong to $C^\perp$, but since the $n-k$ rows of H are linearly independent, one deduces that H is a parity-check matrix for C, and a generator matrix for $C^\perp$. Lemma 25.6 implies then that $C^\perp$ is a cyclic code with generating polynomial $\overline{h}$.

Remark 25.8: The syndrome decoding procedure can be shown to give $S(a) = rem_g(x^{n-k}a)$, the remainder in the division by g of $x^{n-k}a(x)$, if one uses a canonical parity-check matrix H for C. However, one may simplify the definition and consider instead $S(a) = rem_g(a)$.

Remark 25.9: The binary Hamming code $Ham(r,2)$ is equivalent to a cyclic code,[2] and other cyclic codes are the two *Golay codes*,[3] and the *Reed–Solomon codes*,[4,5] which are all examples from a larger family of parametrized error-correcting codes invented by HOCQUENGHEM in 1959,[6] and independently in 1960 by BOSE and RAY-CHAUDHURI,[7,8] which are now called *BCH codes*.

If similar codes were discovered around 1960 by a French (HOCQUENGHEM), two Indians (BOSE and RAY-CHAUDHURI), working in United States, and two Americans (REED and SOLOMON), working at MIT (Massachusetts Institute of Technology) Lincoln Laboratory,[9] it is the sign that the advance in technology had made problems of coding natural, and that many around the world were thinking about that question with a similar knowledge in algebra, hence found similar solutions. GOLAY had worked much earlier at Bell

[2] If F is the field with 2^r elements, and $\xi \in F^*$ generates the multiplicative group F^*, then its minimal monic polynomial $g \in \mathbb{Z}_2[x]$ is irreducible of degree r, and g generates a cyclic code equivalent to the binary Hamming code $Ham(r,2)$.

[3] Marcel Jules Édouard GOLAY, Swiss-born mathematician and engineer, 1902–1989. He worked at Bell Telephone Laboratories, and then at the US Army Signal Corps. The Golay cell, a type of infrared detector, and the Golay codes are named after him.

[4] Irving Stoy REED, American mathematician and engineer, born in 1923. He worked at USC (University of Southern California) Los Angeles, CA. The Reed–Solomon codes are partly named after him.

[5] Gustave SOLOMON, American mathematician and engineer, 1930–1996. The Reed–Solomon codes are partly named after him.

[6] Alexis HOCQUENGHEM, French mathematician, 1908–1990. He worked at CNAM (Conservatoire National des Arts et Métiers), Paris, France. The BCH codes are partially named after him, although he introduced them a year before R. C. BOSE and D. K. RAY-CHAUDHURI.

[7] Raj Chandra BOSE, Indian-born mathematician, 1901–1987. He worked in Calcutta, India, at UNC (University of North Carolina) Chapel Hill, NC, and at Colorado State University, Fort Collins, CO. The BCH codes are partially named after him, although they were introduced by HOCQUENGHEM a year before he introduced them with RAY-CHAUDHURI.

[8] Dwijendra Kumar RAY-CHAUDHURI, Indian-born mathematician, born in 1933. He worked at OSU (Ohio State University) Columbus, OH. The BCH codes are partially named after him, although they were introduced by HOCQUENGHEM a year before he introduced them with R. C. BOSE.

[9] Abraham LINCOLN, American politician, 1809–1865. He was the 16th President of the United States, serving from March 1861 until his assassination.

Telephone Laboratories,[10] on the question of efficient transmission of (telephonic) information along noisy channels of communication, but he was no longer working there when he published the Golay codes in a very short article in 1949, while HAMMING published on his codes in 1950, while he was working at Bell Telephone Laboratories. Actually, the combinatorial aspect of the perfect ternary Golay code had been discovered by VIRTAKALLIO,[11] for finding a good betting system for soccer-pools, and he published the 729 codewords in 1947 (in the soccer-pool magazine Veikkaaja).

Example 25.10: Over F_2 ($\simeq \mathbb{Z}_2$), one has $x^{23}-1 = (x-1)\,g(x)\,\overline{g}(x)$, with $g(x) = x^{11}+x^9+x^7+x^6+x^5+x+1$ and $\overline{g}(x) = x^{11}+x^{10}+x^6+x^5+x^4+x^2+1$.[12] The *binary Golay code* G_{23} is a cyclic $[23,12]$-code over F_2 with generating polynomial g (and using $\overline{g}$ gives an equivalent code). It can be shown to have minimum distance 7, and it is perfect since $2^{12}\big[\binom{23}{0}+\binom{23}{1}+\binom{23}{2}+\binom{23}{3}\big] = 2^{12}\big(1+23+23\cdot 11+23\cdot 77\big) = 2^{12}2048 = 2^{23}$.

The $[23,12,7]$ binary Golay code can be made into a $[24,12,8]$ *extended* binary Golay code by adding a parity bit.

Example 25.11: Over F_3 ($\simeq \mathbb{Z}_3$), one has $x^{11}-1 = (x-1)\,g(x)\,\overline{g}(x)$, with $g(x) = x^5+x^4-x^3+x^2-1$ and $\overline{g}(x) = x^5-x^3+x^2-x-1$.[13] The *ternary Golay code* G_{11} is a cyclic $[11,6]$-code over F_3 with generating polynomial g (and using $\overline{g}$ gives an equivalent code). It can be shown to have minimum distance 5, and it is perfect since $3^6\big[\binom{11}{0}+2\binom{11}{1}+2^2\binom{11}{2}\big] = 3^6\big(1+2\cdot 11+4\cdot 55\big) = 3^6 243 = 3^{11}$.

The $[11,5,5]$ ternary Golay code can be made into a $[12,5,6]$ *extended* ternary Golay code by adding a parity bit.

Remark 25.12: It can be shown that every non-trivial *single-error correcting perfect* code is equivalent to a binary Hamming code, and that every non-trivial *multiple-error correcting perfect* code is equivalent to either the binary $[23,12,7]$ Golay code G_{23} or to the ternary $[11,6,5]$ Golay code G_{11}.

[10] Alexander Graham BELL, Scottish-born inventor, 1847–1922. His most prestigious invention is the telephone. His Bell Telephone Company went through a few changes before becoming AT&T (American Telephone & Telegraph Company).

[11] Juhani VIRTAKALLIO, Finnish soccer-pool enthusiast.

[12] The multiplicative group $F^*_{2^{22}}$ of the field $F_{2^{22}}$ is a cyclic group with a number of elements which is a multiple of 23 (since $2^{22} = 1 \pmod{23}$ by Fermat's theorem), so that there exists a primitive 23rd root of unity ξ, which has an irreducible monic polynomial $g \in F_2[x]$. Since z and z^2 have the same minimal polynomial (because the Frobenius map is $z \mapsto z^2$) g has roots $\xi, \xi^2, \xi^4, \xi^8, \xi^{16}, \xi^{32} = \xi^9, \xi^{18}, \xi^{36} = \xi^{13}, \xi^{26} = \xi^3, \xi^6, \xi^{12}$. The polynomial $\overline{g}$ is $x^{11} g\big(\frac{1}{x}\big)$.

[13] The multiplicative group $F^*_{3^{10}}$ of the field $F_{3^{10}}$ is a cyclic group with a number of elements which is a multiple of 11 (since $3^{10} = 1 \pmod{11}$ by Fermat's theorem), so that there exists a primitive 11th root of unity ξ, which has an irreducible monic polynomial $g \in F_3[x]$. Since z and z^3 have the same minimal polynomial (because the Frobenius map is $z \mapsto z^3$) g has roots $\xi, \xi^3, \xi^9, \xi^{27} = \xi^5, \xi^{15} = \xi^4$. The polynomial $\overline{g}$ is $-x^5 g\big(\frac{1}{x}\big)$.