Rings in Coding Theory

Steven T. Dougherty

July 3, 2013

Cyclic Codes

Cyclic Codes were first studied by Prange in 1957.

Prange, E. Cyclic error-correcting codes in two symbols. Technical Note TN-57-103, Air Force Cambridge Research Labs., Bedfrod, Mass.

Cyclic Codes

Cyclic codes are an extremely important class of codes – initially because of an efficient decoding algorithm.

A code C is cyclic if
$(a_0, a_1, \ldots, a_{n-1}) \in C \implies (a_{n-1}, a_0, a_1, a_2, \ldots, a_{n-2}) \in C$.

Cyclic Codes

Cyclic codes are an extremely important class of codes – initially because of an efficient decoding algorithm.

A code C is cyclic if
$(a_0, a_1, \ldots, a_{n-1}) \in C \implies (a_{n-1}, a_0, a_1, a_2, \ldots, a_{n-2}) \in C$.

Let $\pi((a_0, a_1, \ldots, a_{n-1})) = (a_{n-1}, a_0, a_1, a_2, \ldots, a_{n-2})$. So a cyclic code C has $\pi(C) = C$.

Cyclic Codes

There is a natural connection from vectors in a cyclic code to polynomials:

$$(a_0, a_1, \ldots, a_{n-1}) \leftrightarrow a_0 + a_1 x + a_2 x^2 \ldots a_{n-1} x^{n-1}$$

Cyclic Codes

There is a natural connection from vectors in a cyclic code to polynomials:

$$(a_0, a_1, \ldots, a_{n-1}) \leftrightarrow a_0 + a_1 x + a_2 x^2 \ldots a_{n-1} x^{n-1}$$

Notice that $\pi((a_0, a_1, \ldots, a_{n-1}))$ corresponds to $x(a_0 + a_1 x + a_2 x^2 \ldots a_{n-1} x^{n-1}) \pmod{x^n - 1}$.

Cyclic Codes

If C is linear over F and invariant under π then a cyclic code corresponds to an ideal in $F[x]/\langle x^n - 1\rangle$.

Cyclic Codes

If C is linear over F and invariant under π then a cyclic code corresponds to an ideal in $F[x]/\langle x^n - 1\rangle$.

Cyclic codes are classified by finding all ideals in $F[x]/\langle x^n - 1\rangle$.

Cyclic Codes

If C is linear over F and invariant under π then a cyclic code corresponds to an ideal in $F[x]/\langle x^n - 1\rangle$.

Cyclic codes are classified by finding all ideals in $F[x]/\langle x^n - 1\rangle$.

Easily done when the length of the code is relatively prime to the characteristic of the field, that is we factor $x^n - 1$ uniquely in $F[x]$.

Cyclic Codes

Theorem

Let C be a non-zero cyclic code in $F[x]/\langle x^n - 1\rangle$, then

- *There exists a unique monic polynomial $g(x)$ of smallest degree in C;*

Cyclic Codes

Theorem

Let C be a non-zero cyclic code in $F[x]/\langle x^n - 1\rangle$, then

- *There exists a unique monic polynomial $g(x)$ of smallest degree in C;*
- $C = \langle g(x)\rangle$;

Cyclic Codes

Theorem

Let C be a non-zero cyclic code in $F[x]/\langle x^n - 1\rangle$, then

- *There exists a unique monic polynomial $g(x)$ of smallest degree in C;*
- $C = \langle g(x)\rangle$;
- *$g(x)$ is a factor of $x^n - 1$.*

Cyclic Codes

To find all cyclic codes of a given length one must simply identify all factors of $x^n - 1$.

Cyclic Codes

To find all cyclic codes of a given length one must simply identify all factors of $x^n - 1$.

A degree r generator polynomial generates a code with dimension $n - r$.

Cyclic Codes

Let $x^n - 1 = p_1(x)p_2(x)\dots p_s(x)$ over F. Then there are 2^s cyclic codes of that length n.

Cyclic Codes

Let $g(x) = a_0 + a_1 + \cdots + a_r$.

$$\begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_r & 0 & 0 & \dots & 0 \\ 0 & a_0 & a_1 & a_2 & \dots & a_r & 0 & \dots & 0 \\ 0 & 0 & a_0 & a_1 & a_2 & \dots & a_r & \dots & 0 \\ \vdots & & & & & & & & \\ 0 & 0 & \dots & 0 & a_0 & a_1 & a_2 & \dots & a_r \end{pmatrix}$$

Cyclic Codes

If $g(x)$ is the generator polynomial, let $h(x) = \frac{x^n - 1}{g(x)}$.

Cyclic Codes

If $g(x)$ is the generator polynomial, let $h(x) = \frac{x^n - 1}{g(x)}$.

Then $c(x) \in C$ if and only if $c(x)h(x) = 0$.

Cyclic Codes

Let $h(x) = b_0 + b_1 x + \cdots + b_k x^k$.

Cyclic Codes

Let $h(x) = b_0 + b_1 x + \cdots + b_k x^k$. $C^\perp$ is generated by

$\overline{h}(x) = b_k + b_{k-1} x + \cdots + h_0 x^k$.

Cyclic Codes

Let $h(x) = b_0 + b_1 x + \cdots + b_k x^k$. $C^\perp$ is generated by

$\overline{h}(x) = b_k + b_{k-1} x + \cdots + h_0 x^k$.

$$\begin{pmatrix} b_k & b_{k-1} & b_{k-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_k & b_{k-1} & b_{k-2} & \dots & b_r & 0 & \dots & 0 \\ 0 & 0 & b_k & b_{k-1} & b_{k-2} & \dots & b_r & \dots & 0 \\ \vdots & & & & & & & & \\ 0 & 0 & \dots & 0 & b_k & b_{k-1} & b_{k-2} & \dots & b_r \end{pmatrix}$$

Golay Code

As an example, if C is the $[23, 12, 7]$ perfect Golay code:

$$g(x) = 1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11}$$

Golay Code

As an example, if C is the $[23, 12, 7]$ perfect Golay code:

$$g(x) = 1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11}$$

If C is the $[11, 6, 5]$ ternary Golay code:

$$g(x) = 2 + x^2 + 2x^3 + x^4 + x^5$$

Constacyclic Codes

A code C is constacyclic if $(a_0, a_1, \ldots, a_{n-1}) \in C \implies (\lambda_{n-1}, a_0, a_1, a_2, \ldots, a_{n-2}) \in C$ for some $\lambda \in F$.

Constacyclic Codes

A code C is constacyclic if $(a_0, a_1, \ldots, a_{n-1}) \in C \implies (\lambda_{n-1}, a_0, a_1, a_2, \ldots, a_{n-2}) \in C$ for some $\lambda \in F$.

If $\lambda = -1$ the codes are said to be negacyclic.

Constacyclic Codes

A code C is constacyclic if $(a_0, a_1, \ldots, a_{n-1}) \in C \implies (\lambda_{n-1}, a_0, a_1, a_2, \ldots, a_{n-2}) \in C$ for some $\lambda \in F$.

If $\lambda = -1$ the codes are said to be negacyclic.

Under the same reasoning, constacyclic codes corresponds to ideals in $F[x]/\langle x^n - \lambda\rangle$.

Cyclic Codes over $\mathbb{Z}_4$

Let n be odd.

Let $\mu : \mathbb{Z}_4[x] \to \mathbb{Z}_2[x]$ that reads the coefficients modulo 2.

Cyclic Codes over $\mathbb{Z}_4$

Let n be odd.

Let $\mu : \mathbb{Z}_4[x] \to \mathbb{Z}_2[x]$ that reads the coefficients modulo 2.

A polynomial f in $\mathbb{Z}_4[x]$ is basic irreducible if $\mu(f)$ is irreducible in $\mathbb{Z}_2[x]$; f is primary if $\langle f \rangle$ is a primary ideal.

Cyclic Codes over $\mathbb{Z}_4$

Lemma

If f is a basic irreducible polynomial, then f is primary.

Cyclic Codes over $\mathbb{Z}_4$

Lemma

If f is a basic irreducible polynomial, then f is primary.

Lemma

If $x^n - 1 = f_1 f_2 \dots f_r$, where the f_i are basic irreducible and pairwise coprime, then this factorization is unique.

Cyclic Codes over $\mathbb{Z}_4$

Lemma

If f is a basic irreducible polynomial, then f is primary.

Lemma

If $x^n - 1 = f_1 f_2 \ldots f_r$, where the f_i are basic irreducible and pairwise coprime, then this factorization is unique.

Lemma

Let $x^n - 1 = f_1 f_2 \ldots f_r$ be a product of basic irreducible and pairwise coprime polynomials for odd n and let $\widehat{f_i}$ denote the product of all f_j except f_i. Then any ideal in the ring $\mathbb{Z}_4[x]/\langle x^n - 1\rangle$ is a sum of some $\langle \widehat{f_i} \rangle$ and $\langle 2\widehat{f_i} \rangle$.

Cyclic Codes over $\mathbb{Z}_4$

Theorem

The number of $\mathbb{Z}_4$ cyclic codes of length n is 3^r, where r is the number of basic irreducible polynomial factors in $x^n - 1$.

Cyclic Codes over $\mathbb{Z}_4$

Theorem

Let C be a $\mathbb{Z}_4$ cyclic code of odd length n. Then there are unique, monic polynomials f, g, h such that $C = \langle fh, 2fg \rangle$ where $fgh = x^n - 1$ and $|C| = 4^{deg(g)} 2^{deg(h)}$.

Cyclic Codes over $\mathbb{Z}_4$

Theorem

Let $C = \langle fh, 2fg \rangle$ be a quatenray cyclic code of odd length, with $fgh = x^n - 1$. Then $C^{\perp} = \langle \overline{g}\overline{h}, 2\overline{g}\overline{h} \rangle$.

Cyclic Codes over $\mathbb{Z}_4$ of even length

Let n be an odd integer and $N = 2^k n$ will denote the length of a cyclic code over $\mathbb{Z}_4$.

Cyclic Codes over $\mathbb{Z}_4$ of even length

Let n be an odd integer and $N = 2^k n$ will denote the length of a cyclic code over $\mathbb{Z}_4$.

Define the ring $\mathcal{R} = \mathbb{Z}_4[u]/\langle u^{2^k} - 1\rangle$.

Cyclic Codes over $\mathbb{Z}_4$ of even length

Let n be an odd integer and $N = 2^k n$ will denote the length of a cyclic code over $\mathbb{Z}_4$.

Define the ring $\mathcal{R} = \mathbb{Z}_4[u]/\langle u^{2^k} - 1\rangle$.

We have a module isomorphism $\Psi : \mathcal{R}^n \to (\mathbb{Z}_4)^{2^k n}$ defined by

$$\begin{aligned}
& \Psi(a_{0,0} + a_{0,1}u + a_{0,2}u^2 + \cdots + a_{0,2^k-1}u^{2^k-1}, \ldots, \\
& a_{n-1,0} + a_{n-1,1}u + a_{n-1,2}u^2 + \cdots + a_{n-1,2^k-1}u^{2^k-1}) \\
= \quad & (a_{0,0}, a_{1,0}, a_{2,0}, a_{3,0}, \ldots, a_{n-1,0}, a_{0,1}, a_{1,1}, a_{2,1} \\
& \ldots, a_{0,2^k-1}, a_{1,2^k-1}, \ldots, a_{n-1,2^k-1}).
\end{aligned}$$

Cyclic Codes over $\mathbb{Z}_4$ of even length

We have that

$$\begin{aligned} & \Psi\left(u\left(\sum_{j=0}^{2^k-1} a_{n-1,j}u^j\right), \sum_{j=0}^{2^k-1} a_{0,j}u^j, \sum_{j=0}^{2^k-1} a_{1,j}u^j, \ldots, \sum_{j=0}^{2^k-1} a_{n-2,j}u^j\right) \\ = \quad & (a_{n-1,2^k-1}, a_{0,0}, a_{1,0}, \ldots, a_{n-2,2^k-1}). \end{aligned}$$

This gives that a cyclic shift in $(\mathbb{Z}_4)^{2^k n}$ corresponds to a constacyclic shift in $\mathcal{R}^n$ by u.

Cyclic Codes over $\mathbb{Z}_4$ of even length

Theorem

Cyclic codes over $\mathbb{Z}_4$ of length $N = 2^k n$ correspond to constacyclic codes over $\mathcal{R}$ modulo $X^n - u$ via the map Ψ.

Generalizations

S.T. Dougherty, Young Ho Park, On Modular Cyclic Codes , Finite Fields and their Applications Volume 13, Number 1, 31-57, 2007.

Generalizations

Cyclic codes of length N over a ring R are identified with the ideals of $R[X]/\langle X^N - 1\rangle$ by identifying the vectors with the polynomials of degree less than N.

Generalizations

Every cyclic code C over $\mathbb{F}_q$ is generated by a nonzero monic polynomial of the minimal degree in C, which must be a divisor of $X^N - 1$ by the minimality of degree.

Generalizations

Since $\mathbb{F}_q[X]$ is a UFD, cyclic codes over $\mathbb{F}_q$ are completely determined by the factorization of $X^N - 1$ whether or not N is prime to the characteristic of the field, even though when they are not relatively prime we are in the repeated root case.

Generalizations

For cyclic codes over $\mathbb{Z}_{p^e}$ if the length N is prime to p, $X^N - 1$ factors uniquely over $\mathbb{Z}_{p^e}$ by Hensel's Lemma.

Generalizations

All cyclic codes over $\mathbb{Z}_{p^e}$ of length prime to p have the form

$$\langle f_0, pf_1, p^2 f_2, \ldots, p^{e-1} f_{e-1} \rangle,$$

where $f_{e-1} \mid f_{e-2} \mid \cdots \mid f_0 \mid X^N - 1$.

Generalizations

All cyclic codes over $\mathbb{Z}_{p^e}$ of length prime to p have the form

$$\langle f_0, pf_1, p^2 f_2, \ldots, p^{e-1} f_{e-1} \rangle,$$

where $f_{e-1} \mid f_{e-2} \mid \cdots \mid f_0 \mid X^N - 1$.

These ideals are principal:

$$\langle f_0, pf_1, p^2 f_2, \ldots, p^{e-1} f_{e-1} \rangle = \langle f_0 + pf_1 + p^2 f_2 + \cdots + p^{e-1} f_{e-1} \rangle.$$

Generalizations

Therefore, cyclic codes of length N prime to p are again easily determined by the unique factorization of $X^N - 1$. The reason that the case when the characteristic of the ring divides the length N is more difficult is that in this case we do not have a unique factorization of $X^N - 1$.

Generalizations

Let C be a (linear) cyclic code of length N over the ring $\mathbb{Z}_M$, where M and N are arbitrary positive integers.

Generalizations

We use the Chinese Remainder Theorem to decompose the code C, i.e. an ideal of $\mathbb{Z}_M[X]/\langle X^N - 1\rangle$, into a direct sum of ideals over $\mathbb{Z}_{p_i^{e_i}}$ according to the prime factorization of $M = p_1^{e_1} p_2^{e_2} \dots p_r^{e^r}$.

Generalizations

Therefore, it is enough to study cyclic codes over the rings $\mathbb{Z}_{p^e}$ for a prime p.

Generalizations

Fix a prime p and write $N = p^k n$, p not dividing n.

Generalizations

Define an isomorphism between $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$ and a direct sum, $\oplus_{i\in I}\S_{p^e}(m_i, u)$, of certain local rings. This shows that any cyclic code over $\mathbb{Z}_{p^e}$ can be described by a direct sum of ideals within this decomposition.

Generalizations

The inverse isomorphism can also be given, so that the corresponding ideal in $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$ can be computed explicitly.

Generalizations

$R = \mathbb{Z}_{p^e}$ and write

$$R_N = \mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle,$$

so that $R_N = R^N$ after the identification.

Generalizations

By introducing an auxiliary variable u, we break the equation $X^N - 1 = 0$ into two equations $X^n - u = 0$ and $u^{p^k} - 1 = 0$. Taking the equation $u^{p^k} - 1 = 0$ into account, we first introduce the ring

$$\mathcal{R} = \mathbb{Z}_{p^e}[u]/\langle u^{p^k} - 1\rangle.$$

Generalizations

There is a natural R-module isomorphism $\Psi : \mathcal{R}^n \to R^N$ defined by

$$\Psi(a^0, a^1, \ldots, a^{n-1}) = (a_0^0, a_0^1, \ldots, a_0^{n-1}, a_1^0, a_1^1, \ldots, a_1^{n-1}, \ldots, a_{p^k-1}^0, a_{p^k-1}^1, \ldots, a_{p^k-1}^{n-1})$$

where $a^i = a_0^i + a_1^i u + \cdots + a_{p^k-1}^i u^{p^k-1} \in \mathcal{R}$ for $0 \leq i \leq n-1$.

Generalizations

u is a unit in $\mathcal{R}$ and

$$\begin{aligned}
\Psi(ua^{n-1}, a^0, \dots, a^{n-2}) &= \Psi(a^{n-1}_{p^k-1} + a^{n-1}_0 u + \dots \\
&+ a^{n-1}_{p^k-2} u^{p^k-1}, a^0, \dots, a^{n-2}) \\
&= (a^{n-1}_{p^k-1}, a^0_0, \dots, a^{n-2}_0, a^{n-1}_0, a^0_1, \\
&\dots \quad , a^{n-2}_1, \dots, a^{n-1}_{p^k-2}, a^0_{p^k-1}, \dots, a^{n-2}_{p^k-1}).
\end{aligned}$$

Generalizations

The constacyclic shift by u in $\mathcal{R}^n$ corresponds to a cyclic shift in R^N.

Generalizations

We identify $\mathcal{R}^n$ with $\mathcal{R}[X]/\langle X^n - u\rangle$, which takes the equation $X^n - u = 0$ into account.

Generalizations

View Ψ as a map from $\mathcal{R}[X]/\langle X^n - u\rangle$ to R_N, we have that

$$\Psi\left(\sum_{i=0}^{n-1}\Big(\sum_{j=0}^{p^k-1} a_j^i u^j\Big)X^i\right) = \sum_{i=0}^{n-1}\sum_{j=0}^{p^k-1} a_j^i X^{i+jn}.$$

Generalizations

Ψ is an R-module isomorphism, we

$$\Psi(u^j X^i) = X^{i+jn}$$

for $0 \leq i \leq n-1$ and $0 \leq j \leq p^k - 1$.

Generalizations

Let $0 \leq i_1, i_2 \leq n-1$ and $0 \leq j_1, j_2 \leq p^k - 1$. Write $i_1 + i_2 = \delta_1 n + i$, and $j_1 + j_2 = \delta_2 p^k + j$ such that $0 \leq i \leq n-1$ and $0 \leq j \leq p^k - 1$. Clearly $\delta_i = 0$ or 1.

Generalizations

Since $u^{p^k} = 1$, $X^n = u$ in $\mathcal{R}[X]/\langle X^n - u\rangle$ and $X^{p^k n} = 1$ in $R[X]/\langle X^N - 1\rangle$ we have that

$$\begin{aligned}\Psi(u^{j_1}X^{i_1}u^{j_2}X^{i_2}) &= \Psi(u^{j_1+j_2}X^{i_1+i_2}) = \Psi(u^{j+\delta_1}X^{i}) = X^{i+(j+\delta_1)n} \\ &= X^{i+\delta_1 n}X^{jn} = X^{i_1+i_2}X^{(j_1+j_2)n} = \Psi(u^{j_1}X^{i_1})\Psi(u^{j_2}X^{i_2}).\end{aligned}$$

Generalizations

By the R-linearity property of Ψ, it follows that Ψ is a ring homomorphism.

Lemma

Ψ is an R-algebra isomorphism between $\mathcal{R}[X]/\langle X^n - u\rangle$ and $R[X]/\langle X^N - 1\rangle$. Furthermore, the cyclic codes over R of length N correspond to constacyclic codes of length n over $\mathcal{R}$ via the map Ψ.

Generalizations

The ring $\mathcal{R}$ is a finite local ring, and hence the regular polynomial $X^n - u$ has a unique factorization in $\mathcal{R}[X]$

$$X^n - u = g_1 g_2 \dots g_l$$

into monic, irreducible and pairwise relatively prime polynomials $g_i \in \mathcal{R}[X]$, and by the Chinese Remainder Theorem

$$\mathcal{R}[X]/\langle X^n - u\rangle \simeq \mathcal{R}[X]/\langle g_1\rangle \oplus \cdots \oplus \mathcal{R}[X]/\langle g_l\rangle.$$

This isomorphism will give us a decomposition of R_N via the map Ψ.

Generalizations

Cyclic codes can also be studied over the infinite *p*-adic integers. A. R. Calderbank and N. J. A. Sloane, Modular and p-Adic Cyclic Codes, Designs, Codes and Cryptography, 6 (1995), pp. 21-35.

Skew Cyclic Codes

Let F be a field and θ an automorphism of the field.

Skew Cyclic Codes

Let F be a field and θ an automorphism of the field.

A θ-cyclic code is a linear code C with the property that

$$(a_0, a_1, \ldots, a_{n-1}) \in C \implies (\theta(a_{n-1}), \theta(a_0), \theta(a_1), \ldots, \theta(a_{n-2})) \in C.$$

Skew Cyclic Codes

$$F[X,\theta] = \{a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} \mid a_i \in F\}$$

Skew Cyclic Codes

$$F[X, \theta] = \{a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} \mid a_i \in F\}$$

Addition is the usual addition and $Xa = \theta(a)X$, then extend by associativity and distributivity.

Skew Cyclic Codes

Let $\psi : F[X, \theta] \to F[X, \theta]/\langle X^n - 1 \rangle$.

Skew Cyclic Codes

Let $\psi : F[X,\theta] \to F[X,\theta]/\langle X^n - 1\rangle$.

Theorem

Let F be a finite field, θ an automorphism of F and n an integer divisible by the order of θ. The ring $F[X,\theta]/\langle X^n - 1\rangle$ is a principal left ideal domain in which left ideals are generated by $\psi(G)$ where G is a ring divisor of $X^n - 1$ in $F[X,\theta]$.

Skew Cyclic Codes

Theorem

Let F be a finite field, θ an automorphism of F and n an integer divisible by the order of θ. Let C be a linear code of length n. The code C is a θ-cyclic code if and only if the skew polynomial representation of C is a left idea in $F[X, \theta]/\langle X^n - 1\rangle$.