The Ring of Additive Polynomials and Weights of Cyclic Codes

Cem Güneri

Faculty of Engineering and Natural Sciences
Sabancı University, Istanbul

Fq9 Dublin, July 13-17, 2009

Content

Content

Problem

Problem: Estimate the weights of codewords of cyclic codes!

Problem

Problem: Estimate the weights of codewords of cyclic codes!

Available bounds: BCH, Hartmann-Tzeng, van Lint-Wilson.

Problem

Problem: Estimate the weights of codewords of cyclic codes!

Available bounds: BCH, Hartmann-Tzeng, van Lint-Wilson.

Also, one can put divisibility constraints on the weights of cyclic codes (McEliece, Wilson).

Problem

Problem: Estimate the weights of codewords of cyclic codes!

Available bounds: BCH, Hartmann-Tzeng, van Lint-Wilson.

Also, one can put divisibility constraints on the weights of cyclic codes (McEliece, Wilson).

Goal: Write a general algebraic geometric bound for weights.

Setting

Consider $\mathbb{F}_q$ with $q = p^e$. Let $n = q^m - 1$ and $\mathbb{F}_{q^m}^* =< \alpha >$.

Setting

Consider $\mathbb{F}_q$ with $q = p^e$. Let $n = q^m - 1$ and $\mathbb{F}_{q^m}^* = < \alpha >$.

Let $C \subset \mathbb{F}_q[x]/ < x^n - 1 >$ be a cyclic code such that its dual has

$$\{\alpha^{i_1}, \ldots, \alpha^{i_s}\}$$

as *a defining zero set*, where $i_j > 0$ for all j.

Setting

Consider $\mathbb{F}_q$ with $q = p^e$. Let $n = q^m - 1$ and $\mathbb{F}_{q^m}^* =< \alpha >$.

Let $C \subset \mathbb{F}_q[x]/ < x^n - 1 >$ be a cyclic code such that its dual has

$$\{\alpha^{i_1}, \ldots, \alpha^{i_s}\}$$

as *a defining zero set*, where $i_j > 0$ for all j.

This means that

$$C^{\perp} =< g_1(x) \cdots g_s(x) >,$$

where $g_j(x) \in \mathbb{F}_q[x]$ is the minimal polynomial of α^{i_j} for all j.

Trace Representation of Cyclic Codes

Theorem. *For any codeword* $\mathbf{c} \in C$*, there exists* $c_1, \ldots c_s \in \mathbb{F}_{q^m}$ *such that for*

$$f_{\mathbf{c}}(x) := c_1 x^{i_1} + \cdots + c_s x^{i_s},$$

we have

$$\begin{aligned} \mathbf{c} &= \Big(\mathrm{Tr}(f_{\mathbf{c}}(\alpha)), \mathrm{Tr}(f_{\mathbf{c}}(\alpha^2)), \ldots, \mathrm{Tr}(f_{\mathbf{c}}(\alpha^{q^m-1}))\Big) \\ &= \Big(\mathrm{Tr}\big(f_{\mathbf{c}}(u)\big)\Big)_{u \in \mathbb{F}_{q^m}^*}. \end{aligned}$$

Here, Tr denotes the *trace function* from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$.

Problem Restated

So, for any $\mathbf{c} \in C$ there exists $f_{\mathbf{c}}(x) := c_1 x^{i_1} + \cdots + c_s x^{i_s}$ such that the weight of $\mathbf{c}$ is

Problem Restated

So, for any $\mathbf{c} \in C$ there exists $f_{\mathbf{c}}(x) := c_1 x^{i_1} + \cdots + c_s x^{i_s}$ such that the weight of $\mathbf{c}$ is

$$w(\mathbf{c}) \;=\; (q^m - 1) - |\{u \in \mathbb{F}_{q^m}^* : \mathrm{Tr}(f_{\mathbf{c}}(u)) = 0\}|$$

Problem Restated

So, for any $\mathbf{c} \in C$ there exists $f_{\mathbf{c}}(x) := c_1 x^{i_1} + \cdots + c_s x^{i_s}$ such that the weight of $\mathbf{c}$ is

$$\begin{aligned} w(\mathbf{c}) &= (q^m - 1) - |\{u \in \mathbb{F}_{q^m}^* : \mathrm{Tr}(f_{\mathbf{c}}(u)) = 0\}| \\ &= (q^m - 1) - \frac{|X_{\mathbf{c}}^{af}(\mathbb{F}_{q^m})| - q}{q} \quad \text{(Hilbert's Theorem 90)}, \end{aligned}$$

where $|X_{\mathbf{c}}^{af}(\mathbb{F}_{q^m})|$ denotes the number of affine $\mathbb{F}_{q^m}$-rational points on the curve $X_{\mathbf{c}}$ defined by

$$y^q - y = f_{\mathbf{c}}(x).$$

Problem Restated

So, for any $\mathbf{c} \in C$ there exists $f_{\mathbf{c}}(x) := c_1 x^{i_1} + \cdots + c_s x^{i_s}$ such that the weight of $\mathbf{c}$ is

$$\begin{aligned} w(\mathbf{c}) &= (q^m - 1) - |\{u \in \mathbb{F}_{q^m}^* : \mathrm{Tr}(f_{\mathbf{c}}(u)) = 0\}| \\ &= (q^m - 1) - \frac{|X_{\mathbf{c}}^{af}(\mathbb{F}_{q^m})| - q}{q} \quad \text{(Hilbert's Theorem 90)}, \end{aligned}$$

where $|X_{\mathbf{c}}^{af}(\mathbb{F}_{q^m})|$ denotes the number of affine $\mathbb{F}_{q^m}$-rational points on the curve $X_{\mathbf{c}}$ defined by

$$y^q - y = f_{\mathbf{c}}(x).$$

Problem: Bound the number of affine $\mathbb{F}_{q^m}$-rational points of each member in the family

$$\mathcal{F} = \left\{ y^q - y = c_1 x^{i_1} + \cdots + c_s x^{i_s} : \ c_1, \ldots, c_s \in \mathbb{F}_{q^m} \right\}.$$

Artin-Schreier Curves

Suppose $f(x) \in \mathbb{F}_{q^m}[x]$ is a polynomial such that $(\deg f, p) = 1$. Then, the equation

$$y^q - y = f(x)$$

defines an irreducible curve X (called *a degree q A-S curve*) over $\mathbb{F}_{q^m}$ whose genus is

$$g(X) = \frac{(q-1)(\deg f - 1)}{2}.$$

Artin-Schreier Curves

Suppose $f(x) \in \mathbb{F}_{q^m}[x]$ is a polynomial such that $(\deg f, p) = 1$. Then, the equation

$$y^q - y = f(x)$$

defines an irreducible curve X (called *a degree q A-S curve*) over $\mathbb{F}_{q^m}$ whose genus is

$$g(X) = \frac{(q-1)(\deg f - 1)}{2}.$$

So, if we assume that a basic zero set for the dual of a cyclic code is

$$\{\alpha^{i_1}, \ldots, \alpha^{i_s}\},$$

where $(i_j, p) = 1$ for all j,

Artin-Schreier Curves

Suppose $f(x) \in \mathbb{F}_{q^m}[x]$ is a polynomial such that $(\deg f, p) = 1$. Then, the equation

$$y^q - y = f(x)$$

defines an irreducible curve X (called *a degree q A-S curve*) over $\mathbb{F}_{q^m}$ whose genus is

$$g(X) = \frac{(q-1)(\deg f - 1)}{2}.$$

So, if we assume that a basic zero set for the dual of a cyclic code is

$$\{\alpha^{i_1}, \ldots, \alpha^{i_s}\},$$

where $(i_j, p) = 1$ for all j, then each nontrivial member in the family

$$\mathcal{F} = \left\{ y^q - y = c_1 x^{i_1} + \cdots + c_s x^{i_s} : \; c_1, \ldots, c_s \in \mathbb{F}_{q^m} \right\}$$

defines an irreducible curve whose genus can be found by the formula above.

Wolfmann's Bound

Theorem (Wolfmann). Let C be a q-ary cyclic code of length $n = q^m - 1$ such that the dual code has a basic zero set of the form $\{\alpha^{i_1}, \ldots, \alpha^{i_s}\}$, where $i_1 < \cdots < i_s$ and $(i_j, p) = 1$ for all j. Then, the nonzero weights w of C satisfy

$$\left| w - (q^m - q^{m-1}) \right| \leq (q-1)(i_s - 1)q^{\frac{m}{2}-1}.$$

Wolfmann's Bound

Theorem (Wolfmann). Let C be a q-ary cyclic code of length $n = q^m - 1$ such that the dual code has a basic zero set of the form $\{\alpha^{i_1}, \ldots, \alpha^{i_s}\}$, where $i_1 < \cdots < i_s$ and $(i_j, p) = 1$ for all j. Then, the nonzero weights w of C satisfy

$$\left|w - (q^m - q^{m-1})\right| \leq (q-1)(i_s - 1)q^{\frac{m}{2}-1}.$$

Proof. An arbitrary nonzero weight w in C satisfies

$$w = q^m - \frac{|X^{af}(\mathbb{F}_{q^m})|}{q},$$

where the curve X is defined by $y^q - y = c_1 x^{i_1} + \cdots + c_s x^{i_s}$. By Hasse-Weil bound, we have

$$|X^{af}(\mathbb{F}_{q^m}) - q^m| \leq 2g(X)q^{\frac{m}{2}}.$$

The result follows from the largest genus among such curves. □

Good for p-ary Codes

Let $q = p$ be prime. Say $i = rp^a$, where $(r, p) = 1$. Then "$\mathbb{F}_p$-conjugates" of α^i are

$$\alpha^{rp^a}, \alpha^{rp^{a+1}}, \ldots, \alpha^{rp^m} = \alpha^r, \ldots .$$

Good for p-ary Codes

Let $q = p$ be prime. Say $i = rp^a$, where $(r, p) = 1$. Then "$\mathbb{F}_p$-conjugates" of α^i are

$$\alpha^{rp^a}, \alpha^{rp^{a+1}}, \ldots, \alpha^{rp^m} = \alpha^r, \ldots.$$

i.e. the minimal exponent among the conjugates is necessarily relatively prime to p.

Good for p-ary Codes

Let $q = p$ be prime. Say $i = rp^a$, where $(r, p) = 1$. Then "$\mathbb{F}_p$-conjugates" of α^i are

$$\alpha^{rp^a}, \alpha^{rp^{a+1}}, \ldots, \alpha^{rp^m} = \alpha^r, \ldots.$$

i.e. the minimal exponent among the conjugates is necessarily relatively prime to p.

So for p-ary cyclic codes, one can choose the dual's defining set in a way that Wolfmann's bound is applicable.

Good for p-ary Codes

Let $q = p$ be prime. Say $i = rp^a$, where $(r, p) = 1$. Then "$\mathbb{F}_p$-conjugates" of α^i are

$$\alpha^{rp^a}, \alpha^{rp^{a+1}}, \ldots, \alpha^{rp^m} = \alpha^r, \ldots.$$

i.e. the minimal exponent among the conjugates is necessarily relatively prime to p.

So for p-ary cyclic codes, one can choose the dual's defining set in a way that Wolfmann's bound is applicable.

This is not necessarily the case if q is not prime.

Example

Let $q = 4$ and $n = 4^3 - 1 = 63$. Let α be a primitive element for $\mathbb{F}_{64}$.

Example

Let $q = 4$ and $n = 4^3 - 1 = 63$. Let α be a primitive element for $\mathbb{F}_{64}$. Consider the 4-ary cyclic code C of length n whose dual's defining zero set is $\{\alpha, \alpha^2\}$,

Example

Let $q = 4$ and $n = 4^3 - 1 = 63$. Let α be a primitive element for $\mathbb{F}_{64}$. Consider the 4-ary cyclic code C of length n whose dual's defining zero set is $\{\alpha, \alpha^2\}$,

$$\text{i.e.} \quad C^{\perp} = < g_{\alpha}(x) g_{\alpha^2}(x) > \subset \mathbb{F}_4[x] / < x^{63} - 1 > .$$

Example

Let $q = 4$ and $n = 4^3 - 1 = 63$. Let α be a primitive element for $\mathbb{F}_{64}$. Consider the 4-ary cyclic code C of length n whose dual's defining zero set is $\{\alpha, \alpha^2\}$,

$$\text{i.e.} \quad C^{\perp} =< g_{\alpha}(x) g_{\alpha^2}(x) > \subset \mathbb{F}_4[x]/ < x^{63} - 1 > .$$

Here is the related family of curves we have to study:

$$\mathcal{F} = \left\{ y^4 - y = \lambda x + \mu x^2 : \ \lambda, \mu \in \mathbb{F}_{64} \right\}$$

Example

Let $q = 4$ and $n = 4^3 - 1 = 63$. Let α be a primitive element for $\mathbb{F}_{64}$. Consider the 4-ary cyclic code C of length n whose dual's defining zero set is $\{\alpha, \alpha^2\}$,

$$\text{i.e.} \quad C^{\perp} = < g_{\alpha}(x) g_{\alpha^2}(x) > \subset \mathbb{F}_4[x] / < x^{63} - 1 > .$$

Here is the related family of curves we have to study:

$$\mathcal{F} = \left\{ y^4 - y = \lambda x + \mu x^2 : \ \lambda, \mu \in \mathbb{F}_{64} \right\}$$

If only one of the coefficients λ or μ is nonzero, the resulting curve is rational with 64 (affine) rational points over $\mathbb{F}_{64}$.

Example

Let $q = 4$ and $n = 4^3 - 1 = 63$. Let α be a primitive element for $\mathbb{F}_{64}$. Consider the 4-ary cyclic code C of length n whose dual's defining zero set is $\{\alpha, \alpha^2\}$,

$$\text{i.e.} \quad C^{\perp} = < g_{\alpha}(x) g_{\alpha^2}(x) > \subset \mathbb{F}_4[x]/ < x^{63} - 1 > .$$

Here is the related family of curves we have to study:

$$\mathcal{F} = \left\{ y^4 - y = \lambda x + \mu x^2 : \ \lambda, \mu \in \mathbb{F}_{64} \right\}$$

If only one of the coefficients λ or μ is nonzero, the resulting curve is rational with 64 (affine) rational points over $\mathbb{F}_{64}$.

However, for some combination (which can be explicitely determined) of nonzero λ, μ, the curve will be reducible.

$$y^4 + y + x^2 + x$$

$$y^4 + y + x^2 + x = y^4 + y^2 + x^2 + y^2 + y + x$$

$$
\begin{aligned}
y^4 + y + x^2 + x &= y^4 + y^2 + x^2 + y^2 + y + x \\
&= \left(y^2 + y + x\right)^2 + \left(y^2 + y + x\right)
\end{aligned}
$$

$$
\begin{aligned}
y^4 + y + x^2 + x &= y^4 + y^2 + x^2 + y^2 + y + x \\
&= \left(y^2 + y + x\right)^2 + \left(y^2 + y + x\right) \\
&= \left(y^2 + y + x\right)\left(y^2 + y + x + 1\right)
\end{aligned}
$$

$$
\begin{aligned}
y^4 + y + x^2 + x &= y^4 + y^2 + x^2 + y^2 + y + x \\
&= \left(y^2 + y + x\right)^2 + \left(y^2 + y + x\right) \\
&= \left(y^2 + y + x\right)\left(y^2 + y + x + 1\right)
\end{aligned}
$$

So, the curve defined by $y^4 + y = x^2 + x$ has 2 irreducible components both of which are rational curves.

$$\begin{aligned} y^4 + y + x^2 + x &= y^4 + y^2 + x^2 + y^2 + y + x \\ &= \left(y^2 + y + x\right)^2 + \left(y^2 + y + x\right) \\ &= \left(y^2 + y + x\right)\left(y^2 + y + x + 1\right) \end{aligned}$$

So, the curve defined by $y^4 + y = x^2 + x$ has 2 irreducible components both of which are rational curves.

So, there are 128 (affine) rational points over $\mathbb{F}_{64}$. One can show that the other reducible curves in $\mathcal{F}$ factor similarly.

Another Example

$$y^{16} + y + x^8 + x^2$$

Another Example

$$
\begin{aligned}
y^{16}+y+x^8+x^2 &= (y^8+y^4+y^2+y+x^4+x^2)^2 \\
&\quad +(y^8+y^4+y^2+y+x^4+x^2)
\end{aligned}
$$

Another Example

$$
\begin{aligned}
y^{16} + y + x^8 + x^2 &= (y^8 + y^4 + y^2 + y + x^4 + x^2)^2 \\
&\quad + (y^8 + y^4 + y^2 + y + x^4 + x^2) \\
&= (y^8 + y^4 + y^2 + y + x^4 + x^2) \\
&\quad (y^8 + y^4 + y^2 + y + x^4 + x^2 + \underbrace{1}_{\nu^2+\nu})
\end{aligned}
$$

Another Example

$$
\begin{aligned}
y^{16} + y + x^8 + x^2 &= (y^8 + y^4 + y^2 + y + x^4 + x^2)^2 \\
&\quad + (y^8 + y^4 + y^2 + y + x^4 + x^2) \\
&= (y^8 + y^4 + y^2 + y + x^4 + x^2) \\
&\quad (y^8 + y^4 + y^2 + y + x^4 + x^2 + \underbrace{1}_{\nu^2+\nu}) \\
&= (y^4 + y + x^2)(y^4 + y + x^2 + 1) \\
&\quad (y^4 + y + x^2 + \nu)(y^4 + y + x^2 + \nu + 1)
\end{aligned}
$$

Another Example

$$
\begin{aligned}
y^{16}+y+x^8+x^2 &= (y^8+y^4+y^2+y+x^4+x^2)^2 \\
&\quad +(y^8+y^4+y^2+y+x^4+x^2) \\
&= (y^8+y^4+y^2+y+x^4+x^2) \\
&\quad (y^8+y^4+y^2+y+x^4+x^2+\underbrace{1}_{\nu^2+\nu}) \\
&= (y^4+y+x^2)(y^4+y+x^2+1) \\
&\quad (y^4+y+x^2+\nu)(y^4+y+x^2+\nu+1)
\end{aligned}
$$

Here, ν is defined as: $\mathbb{F}_4 = \mathbb{F}_2(\nu)$ with $\nu^2+\nu+1=0$.

Theorem (G. - Özbudak). *Let* $q = p^e$, r *be relatively prime to* p, $a \in \mathbb{F}_q^*$ *and* $\lambda \in \mathbb{F}_{q^m}$. *Assume that* $0 \leq i < j$. *Then the reducible polynomial*

$$(*) \qquad F(x,y) := y^q - y - (\lambda x^{rp^i} - a^{p^{j-i}-1} \lambda^{p^{j-i}} x^{rp^j}) \ \in \mathbb{F}_{q^m}[x,y]$$

factors into irreducibles as follows:

Theorem (G. - Özbudak). *Let $q = p^e$, r be relatively prime to p, $a \in \mathbb{F}_q^*$ and $\lambda \in \mathbb{F}_{q^m}$. Assume that $0 \le i < j$. Then the reducible polynomial*

$$(*) \qquad F(x,y) := y^q - y - (\lambda x^{rp^i} - a^{p^{j-i}-1}\lambda^{p^{j-i}} x^{rp^j}) \in \mathbb{F}_{q^m}[x,y]$$

factors into irreducibles as follows:

i. *If $c = \gcd(e, j-i) = 1$, then*

$$F(x,y) = \prod_{\omega \in \mathbb{F}_p} H_\omega(x,y),$$

where

$$H_\omega(x,y) = \sum_{k=0}^{e-1} \left(a^{p^k - p^{-1}} y^{p^k}\right) + \sum_{\gamma=0}^{j-i-1} \left(a^{p^\gamma - p^{-1}} \lambda^{p^\gamma} x^{rp^{i+\gamma}}\right) - \omega a^{-p^{-1}}.$$

Theorem (G. - Özbudak). *Let $q = p^e$, r be relatively prime to p, $a \in \mathbb{F}_q^*$ and $\lambda \in \mathbb{F}_{q^m}$. Assume that $0 \leq i < j$. Then the reducible polynomial*

$$(*) \qquad F(x,y) := y^q - y - (\lambda x^{rp^i} - a^{p^{j-i}-1}\lambda^{p^{j-i}} x^{rp^j}) \ \in \mathbb{F}_{q^m}[x,y]$$

factors into irreducibles as follows:

i. *If $c = \gcd(e, j-i) = 1$, then*

$$F(x,y) = \prod_{\omega \in \mathbb{F}_p} H_\omega(x,y),$$

where

$$H_\omega(x,y) = \sum_{k=0}^{e-1} \left(a^{p^k - p^{-1}} y^{p^k} \right) + \sum_{\gamma=0}^{j-i-1} \left(a^{p^\gamma - p^{-1}} \lambda^{p^\gamma} x^{rp^{i+\gamma}} \right) - \omega a^{-p^{-1}}.$$

ii. *If $c = \gcd(e, j-i) > 1$, then each factor H_w above further factors as:*

$$H_\omega(x,y) = \prod_{\mathrm{Tr}_{\mathbb{F}_{p^c}/\mathbb{F}_p}(\beta)=0} (A_\omega(x,y) - \beta)\,,$$

where

$$A_\omega(x,y) = \sum_{k=0}^{e/c-1} \left(y^{p^{ck}} \right) + \sum_{\gamma=0}^{(j-i)/c-1} \left((a\lambda)^{p^{c\gamma}} x^{rp^{i+c\gamma}} \right) - v_\omega$$

and $\mathrm{Tr}_{\mathbb{F}_{p^c}/\mathbb{F}_p}(v_\omega) = \omega$.

Previous Examples

1. $c = \gcd(2, 1-0) = 1 \Rightarrow$ one step factorization!

$$\begin{aligned} y^4 + y + x^2 + x &= y^{2^2} + y + x^{1\cdot 2^1} + x^{1\cdot 2^0} \\ &= \left(y^2 + y + x\right)\left(y^2 + y + x + 1\right) \end{aligned}$$

Previous Examples

1. $c = \gcd(2, 1-0) = 1 \Rightarrow$ one step factorization!

$$\begin{aligned} y^4 + y + x^2 + x &= y^{2^2} + y + x^{1\cdot 2^1} + x^{1\cdot 2^0} \\ &= \left(y^2 + y + x\right)\left(y^2 + y + x + 1\right) \end{aligned}$$

2. $c = \gcd(4, 3-1) = 2 \Rightarrow$ two step factorization!

$$\begin{aligned} y^{16} + y + x^8 + x^2 &= y^{2^4} + y + x^{1\cdot 2^3} + x^{1\cdot 2^1} \\ &= (y^8 + y^4 + y^2 + y + x^4 + x^2) \\ &\quad\ (y^8 + y^4 + y^2 + y + x^4 + x^2 + 1) \end{aligned}$$

Previous Examples

1. $c = \gcd(2, 1-0) = 1 \Rightarrow$ one step factorization!

$$
\begin{aligned}
y^4 + y + x^2 + x &= y^{2^2} + y + x^{1\cdot 2^1} + x^{1\cdot 2^0} \\
&= \left(y^2 + y + x\right)\left(y^2 + y + x + 1\right)
\end{aligned}
$$

2. $c = \gcd(4, 3-1) = 2 \Rightarrow$ two step factorization!

$$
\begin{aligned}
y^{16} + y + x^8 + x^2 &= y^{2^4} + y + x^{1\cdot 2^3} + x^{1\cdot 2^1} \\
&= (y^8 + y^4 + y^2 + y + x^4 + x^2) \\
&\qquad (y^8 + y^4 + y^2 + y + x^4 + x^2 + 1) \\
&= (y^4 + y + x^2)(y^4 + y + x^2 + 1) \\
&\qquad (y^4 + y + x^2 + \nu)(y^4 + y + x^2 + \nu + 1)
\end{aligned}
$$

Remarks

1. If X denotes the reducible curve defined by

$$F(x,y) := y^q - y - (\lambda x^{rp^i} - a^{p^{j-i}-1}\lambda^{p^{j-i}} x^{rp^j}) \in \mathbb{F}_{q^m}[x,y],$$

then we have

$$\left| |X^{af}(\mathbb{F}_{p^{em}})| - p^{em+c} \right| \leq (p^e - p^c)(r-1)\sqrt{p^{em}}.$$

Remarks

1. If X denotes the reducible curve defined by

$$F(x,y) := y^q - y - \left(\lambda x^{rp^i} - a^{p^{j-i}-1}\lambda^{p^{j-i}} x^{rp^j}\right) \ \in \mathbb{F}_{q^m}[x,y],$$

then we have

$$\left| |X^{af}(\mathbb{F}_{p^{em}})| - p^{em+c} \right| \leq (p^e - p^c)(r-1)\sqrt{p^{em}}.$$

2. Full form of the previous result, together with the Hasse-Weil type bound, yields a minimum distance estimate for any cyclic code over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$. However, we cannot say the same thing for cyclic codes $\mathbb{F}_{p^3}, \mathbb{F}_{p^4}, \ldots$ Obtaining such explicit factorizations to estimate weights of all cyclic codes is hopeless!

The Ring $\mathcal{R}$

Let K be a perfect field of characteristic $p > 0$. A polynomial of the form

$$A(T) = a_n T^{p^n} + a_{n-1} T^{p^{n-1}} + \cdots + a_1 T^p + a_0 T \ \in K[T]$$

is called an *additive polynomial*.

The Ring $\mathcal{R}$

Let K be a perfect field of characteristic $p > 0$. A polynomial of the form

$$A(T) = a_n T^{p^n} + a_{n-1} T^{p^{n-1}} + \cdots + a_1 T^p + a_0 T \ \in K[T]$$

is called an *additive polynomial*.

The following identity is satisfied:

$$A(u+v) = A(u) + A(v)$$

The Ring $\mathcal{R}$

Let K be a perfect field of characteristic $p > 0$. A polynomial of the form

$$A(T) = a_n T^{p^n} + a_{n-1} T^{p^{n-1}} + \cdots + a_1 T^p + a_0 T \ \in K[T]$$

is called an *additive polynomial*.

The following identity is satisfied:

$$A(u + v) = A(u) + A(v)$$

The sum and composition of two additive polynomials in $K[T]$ are again additive polynomials in $K[T]$.

The Ring $\mathcal{R}$

Let K be a perfect field of characteristic $p > 0$. A polynomial of the form

$$A(T) = a_n T^{p^n} + a_{n-1} T^{p^{n-1}} + \cdots + a_1 T^p + a_0 T \ \in K[T]$$

is called an *additive polynomial*.

The following identity is satisfied:

$$A(u + v) = A(u) + A(v)$$

The sum and composition of two additive polynomials in $K[T]$ are again additive polynomials in $K[T]$.

The set $\mathcal{R}$ of additive polynomials in $K[T]$ together with addition and composition operations $(\mathcal{R}, +, \circ)$ forms a ring, called *the ring of additive polynomials (Ore ring)*.

Division

Let $A(T), B(T) \in \mathcal{R}$:

$$\begin{aligned} A(T) &= a_n T^{p^n} + a_{n-1} T^{p^{n-1}} + \cdots + a_1 T^p + a_0 T, \\ B(T) &= b_m T^{p^m} + b_{m-1} T^{p^{m-1}} + \cdots + b_1 T^p + b_0 T, \end{aligned}$$

Division

Let $A(T), B(T) \in \mathcal{R}$:

$$\begin{aligned} A(T) &= a_n T^{p^n} + a_{n-1} T^{p^{n-1}} + \cdots + a_1 T^p + a_0 T, \\ B(T) &= b_m T^{p^m} + b_{m-1} T^{p^{m-1}} + \cdots + b_1 T^p + b_0 T, \end{aligned}$$

We say that A is *left divisible* by B if there exists $C(T) \in \mathcal{R}$ such that $A = B \circ C$.

Division

Let $A(T), B(T) \in \mathcal{R}$:

$$\begin{aligned} A(T) &= a_n T^{p^n} + a_{n-1} T^{p^{n-1}} + \cdots + a_1 T^p + a_0 T, \\ B(T) &= b_m T^{p^m} + b_{m-1} T^{p^{m-1}} + \cdots + b_1 T^p + b_0 T, \end{aligned}$$

We say that A is *left divisible* by B if there exists $C(T) \in \mathcal{R}$ such that $A = B \circ C$.

Assuming $\deg A \geq \deg B$, we can write

$$A(T) = B(T) \circ \left((a_n/b_m)^{1/p^m} T^{p^{n-m}} + \cdots \right) + R(T),$$

where $R(T) \in \mathcal{R}$ is of degree less than $\deg B$, unless $R = 0$.

Division

Let $A(T), B(T) \in \mathcal{R}$:

$$\begin{aligned} A(T) &= a_n T^{p^n} + a_{n-1} T^{p^{n-1}} + \cdots + a_1 T^p + a_0 T, \\ B(T) &= b_m T^{p^m} + b_{m-1} T^{p^{m-1}} + \cdots + b_1 T^p + b_0 T, \end{aligned}$$

We say that A is *left divisible* by B if there exists $C(T) \in \mathcal{R}$ such that $A = B \circ C$.

Assuming $\deg A \geq \deg B$, we can write

$$A(T) = B(T) \circ \left((a_n/b_m)^{1/p^m} T^{p^{n-m}} + \cdots \right) + R(T),$$

where $R(T) \in \mathcal{R}$ is of degree less than $\deg B$, unless $R = 0$.

Hence, over a perfect field K, the ring $\mathcal{R}$ has Euclidean algorithm. In particular, two additive polynomials $A, B \in \mathcal{R}$ have a monic *left greatest common divisor* $\mathrm{lgcd}(A, B)$ in $\mathcal{R}$.

Theorem (G. - Özbudak). *Let* $A(T), B_1(T), \ldots, B_t(T) \in \mathcal{R}$ *be nonzero additive polynomials and assume that* A *is monic, separable and splits in* K*.*

Theorem (G. - Özbudak). *Let* $A(T), B_1(T), \ldots, B_t(T) \in \mathcal{R}$ *be nonzero additive polynomials and assume that* A *is monic, separable and splits in* K*. Let* $r_1, \ldots, r_t$ *be distinct positive integers with* $\gcd(p, r_i) = 1$*, for all* $1 \le i \le t$*.*

Theorem (G. - Özbudak). *Let* $A(T), B_1(T), \ldots, B_t(T) \in \mathcal{R}$ *be nonzero additive polynomials and assume that* A *is monic, separable and splits in* K*. Let* $r_1, \ldots, r_t$ *be distinct positive integers with* $\gcd(p, r_i) = 1$*, for all* $1 \leq i \leq t$*. Set*

$$L(T) := \mathrm{lgcd}(A(T), B_1(T), B_2(T), \ldots, B_t(T)),$$

and denote by W *the set of roots of* $L(T)$*. Then,*

Theorem (G. - Özbudak). *Let $A(T), B_1(T), \ldots, B_t(T) \in \mathcal{R}$ be nonzero additive polynomials and assume that A is monic, separable and splits in K. Let $r_1, \ldots, r_t$ be distinct positive integers with $\gcd(p, r_i) = 1$, for all $1 \leq i \leq t$. Set*

$$L(T) := \mathrm{lgcd}(A(T), B_1(T), B_2(T), \ldots, B_t(T)),$$

and denote by W the set of roots of $L(T)$. Then,

i.

$$A(y) - \sum_{i=1}^{t} B_i(x^{r_i}) \text{ is irreducible over } K(x) \text{ if and only if } L(T) = T.$$

Theorem (G. - Özbudak). *Let $A(T), B_1(T), \ldots, B_t(T) \in \mathcal{R}$ be nonzero additive polynomials and assume that A is monic, separable and splits in K. Let $r_1, \ldots, r_t$ be distinct positive integers with $\gcd(p, r_i) = 1$, for all $1 \leq i \leq t$. Set*

$$L(T) := \mathrm{lgcd}(A(T), B_1(T), B_2(T), \ldots, B_t(T)),$$

and denote by W the set of roots of $L(T)$. Then,

i.

$$A(y) - \sum_{i=1}^{t} B_i(x^{r_i}) \text{ is irreducible over } K(x) \text{ if and only if } L(T) = T.$$

ii. *If*

$$\begin{aligned} A(T) &= L(T) \circ \hat{A}(T) \\ B_i(T) &= L(T) \circ \hat{B}_i(T), \end{aligned}$$

then we have following factorization into irreducibles:

$$A(y) - \sum_{i=1}^{t} B_i(x^{r_i}) = \prod_{w \in W} \left(\hat{A}(y) - \sum_{i=1}^{t} \hat{B}_i(x^{r_i}) - w \right).$$

Corollary. *Let $K = \mathbb{F}_\ell$ be a finite field of characteristic p and consider the curve X defined by*

$$A(y) = \sum_{i=1}^{t} B_i(x^{r_i}).$$

If $\deg A = p^n$ *and* $\deg L = p^\mu$*, then*

$$\left| |X^{af}(\mathbb{F}_\ell)| - \ell p^\mu \right| \leq (p^n - p^\mu)(R-1)\sqrt{\ell}\ ,$$

where $R = \max\{r_1, \ldots, r_t\}$.

Corollary. *Let $K = \mathbb{F}_\ell$ be a finite field of characteristic p and consider the curve X defined by*

$$A(y) = \sum_{i=1}^{t} B_i(x^{r_i}).$$

If $\deg A = p^n$ *and* $\deg L = p^\mu$*, then*

$$\left| |X^{af}(\mathbb{F}_\ell)| - \ell p^\mu \right| \leq (p^n - p^\mu)(R-1)\sqrt{\ell}\ ,$$

where $R = \max\{r_1, \ldots, r_t\}$*.*

Conclusion. With this theorem, finding bounds for the weights of cyclic codes reduces to computing left greatest common divisor in the ring of additive polynomials over finite fields.