REU 2017 Day 6 V. Reiner

Primitive polynomials

1. Review $\mathbb{F}_{p^k}$ and
2. define primitive
3. REU Problem 6(a)
4. Motivation from cyclic codes & REU Prob. 6(b)

1. Recall $\mathbb{F}_{p^k}$ = splitting field over $\mathbb{F}_p$ of $x^{p^k}-x$
$= \{\text{roots of } x^{p^k}-x\}$
$\cong \mathbb{F}_p[x]/(f(x))$ where $f(x) \in \mathbb{F}_p[x]$ is any irreducible polynomial of degree k

and recall THM: $\mathbb{F}_{p^k}^\times := \mathbb{F}_{p^k} - \{0\}$
$= \{1, \pi, \pi^2, \dots, \pi^{p^k-2}\} = \langle \pi \rangle$ for some π with $\pi^{p^k-1}=1$
$\cong \mathbb{Z}/(p^k-1)\mathbb{Z}$ as multiplicative group

DEF'N: $f(x) \in \mathbb{F}_p[x]$ (monic and) irreducible of degree k is called primitive if
$\bar{x} \in \mathbb{F}_p[x]/(f(x))$ ($\cong \mathbb{F}_{p^k}$) has multiplicative order p^k-1 (i.e. $\bar{x}$ can play the role of π, $\mathbb{F}_{p^k}^\times = \langle \bar{x} \rangle$)

Equivalently: $f(x) \nmid x^d-1$ for any proper divisor d of p^k-1.

REMARK: Most irreducibles are primitive, but testing primitivity is a bit of a pain!

EXAMPLES:

① $\mathbb{F}_{2^4} = \mathbb{F}_{16}$ splits $x^{16}-x = x(x^{15}-1)$

$= x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$

3 irreducibles $f(x) \in \mathbb{F}_2[x]$ of degree 4

(x^4+x+1): primitive; (x^4+x^3+1): primitive; $(x^4+x^3+x^2+x+1)$: not primitive; divides x^5-1

$\{0, 1, \pi, \pi^2, \pi^3, \ldots, \pi^{13}, \pi^{14}\}$ $\quad \| \quad \pi^{15}$

Frobenius map $\mathbb{F}_{p^k} \xrightarrow{F} \mathbb{F}_{p^k}$, $\alpha \mapsto \alpha^p$

roots: 0 ($0 \xrightarrow{F} 0$); 1 ($1 \xrightarrow{F} 1$); π^5 ($\pi^5 \xrightarrow{F} \pi^{10} \xrightarrow{F} \pi^5$); π, π^2, π^4, π^8; $\pi^7, \pi^{14}, \pi^{13}, \pi^{11}$; $\pi^3, \pi^6, \pi^{12}, \pi^9$

---

② $\mathbb{F}_{3^2} = \mathbb{F}_9$ splits $x^9 - x = x(x^8-1)$

$= x(x-1)(x-2)(x^2+x+2)(x^2+2x+2)(x^2+1)$

3 irreducibles $f(x) \in \mathbb{F}_3[x]$ of degree 2

(x^2+x+2): primitive; (x^2+2x+2): primitive; (x^2+1): not primitive; divides x^4-1

$\{0, 1, \pi, \pi^2, \pi^3, \pi^4, \pi^5, \pi^6, \pi^7\}$ $\quad \| \quad \pi^8$

roots: 0 ($0 \xrightarrow{F} 0$); 1 ($1 \xrightarrow{F} 1$); $\pi^4 = 2$ ($2 \xrightarrow{F} 2$); $\pi^9 = \pi$ ($\pi \xrightarrow{F} \pi^3 \xrightarrow{F} \pi$); π^5 ($\pi^5 \xrightarrow{F} \pi^7 \xrightarrow{F} \pi^5$); π^2 ($\pi^2 \xrightarrow{F} \pi^6 \xrightarrow{F} \pi^2$)

---

2. REU Problem (6a): Prove the following...

CONJECTURE: For $f(x) \in \mathbb{F}_p[x]$ irreducible of degree k,

$f(x)$ is primitive $\iff$ $\dfrac{x^{p^k-1}}{f(x)} = a_0 + a_1 x^1 + a_2 x^2 + \ldots + a_{p^k-2} x^{p^k-2}$ with $a_i \in \{0, 1, \ldots, p-1\}$ ($\iff$ if p)

has exactly $\frac{p-1}{2} \cdot p^{k-1}$ descents in the sequence $(a_0, a_1, \ldots, a_{p^k-2})$

positions i where $a_i > a_{i+1}$ (using $0 < 1 < \ldots < p-1$)

RMK: ($\Rightarrow$) will be more important than ($\Leftarrow$) for the motivation

EXAMPLES:

① For $\mathbb{F}_{2^4}$, have $p=2$, $k=4$

Want $\frac{p-1}{2}\cdot p^{k-1} = \frac{2-1}{2}\cdot 2^{4-1} = \frac{1}{2}\cdot 2^3 = 4$ descents

$f(x)$	x^4+x+1	x^4+x^3+1	$x^4+x^3+x^2+x+1$
$\frac{x^{p^k-1}-1}{f(x)} = \frac{x^{15}-1}{f(x)}$	$1+x^3+x^4+x^6+x^8+x^9+x^{10}+x^{11}$	$1+x+x^2+x^3+x^5+x^7+x^8+x^{11}$	$1+x+x^5+x^6+x^{10}+x^{11}$
$(a_0,a_1,\dots,a_{14})$	100110101111000	111101011001000	110001100011000
	4 descents (= breaks between 1 and 0 strings)	4 descents	only 3 descents
	primitive ✓	primitive ✓	not primitive ✗

② For $\mathbb{F}_{3^2}$, have $p=3$, $k=2$

Want $\frac{p-1}{2}\cdot p^{k-1} = \frac{3-1}{2}\cdot 3 = 3$ descents

$f(x)$	x^2+x+2	x^2+2x+2	x^2+1
$\frac{x^{p^k-1}-1}{f(x)} = \frac{x^8-1}{f(x)}$	$1+x+2x^2+2x^4+2x^5+x^6$	$1+2x+2x^2+2x^4+x^5+x^6$	$2+x^2+2x^4+x^6$
$(a_0,a_1,\dots,a_7)$	11202210	12202110	20102010
	3 descents	3 descents	4 descents
	primitive ✓	primitive ✓	not primitive ✗

(Healthy, maybe useful?)

~~REU EXERCISE~~ A necklace of length k is a circular equivalence class $(b_0,b_1,\dots,b_{k-1}) \equiv (b_{k-1},b_0,b_1,\dots,b_{k-2}) \equiv \cdots$, and is primitive if the class has size k.

Prove that these two maps both give bijections

$$\left\{\begin{array}{c}\text{primitive necklaces } (b_0,b_1,\dots,b_k) \text{ with} \\ b_i \in \{0,1,\dots,p-1\}\end{array}\right\} \longrightarrow \left\{\begin{array}{c}\text{monic irreducible degree } k \\ f(x) \in \mathbb{F}_p[x]\end{array}\right\}$$

e.g. $p=2$

$k=2$ $(^0_1)$ | x^2+x+1

$k=3$ $\{^0_0{}^0_1{}^1_1\}$ versus x^3+x+1 x^3+x^2+1

$k=4$ $a^{0}_{0}{}^{0}_{0}{}^{1}_{0}{}^{1}_{1}$ | x^4+x+1 x^4+x^3+1 $x^4+x^3+x^2+x+1$

I didn't assign this one after all!

(a) $(b_0,b_1,\dots,b_k) \longmapsto \prod_{i=0}^{k-1}(x-F^i(\gamma))$ where $\gamma := \pi^{b_0+b_1q+b_2q^2+\cdots+b_{k-1}q^{k-1}}$ and π is a fixed generator of $\mathbb{F}_{p^k}^\times$

(b) Same map, except $\gamma := b_0\beta + b_1F(\beta) + b_2F^2(\beta) + \cdots + b_{k-1}F^{k-1}(\beta)$ where $\mathbb{F}_{p^k}$ has $\mathbb{F}_p$-basis $\{F^i(\beta)\}_{i=0,\dots,k-1}$ (guaranteed by Normal Basis Thm.)

(8.5) REU EXERCISE 13:

(a) Show $f(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_{k-1} x^{k-1} + x^k \in \mathbb{F}_p[x]$

irreducible will be primitive

$\Leftrightarrow$ the associated LFSR (linear feedback shift register) map

$$\mathbb{F}_p^k \xrightarrow{T} \mathbb{F}_p^k$$

$$\begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{k-1} \end{bmatrix} \longmapsto \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{k-1} \\ x_k \end{bmatrix} \quad \text{where } x_k := -c_0 x_{k-1} - c_1 x_{k-2} - \dots - c_{k-1} x_0$$

has maximum possible period, namely $p^k - 1$. [illegible] starting with any [illegible].

(b) In fact, show that in this case, starting with any $\underline{x} \in \mathbb{F}_p^k - \{\underline{0}\}$, the vectors $\{\underline{x}, T\underline{x}, T^2\underline{x}, \dots, T^{p^k-2}\underline{x}\}$ exhaust all of $\mathbb{F}_p^k - \{\underline{0}\}$.

3. Motivation from cyclic codes

In error-correcting codes, people only transmit codewords from a subset $C \subsetneq \mathbb{F}_p^n$, so that one can detect/correct errors.

Often C is an $\mathbb{F}_p$-(linear) subspace and its perp space $C^\perp := \{ x \in \mathbb{F}_p^n : x \cdot y = 0 \ \forall y \in C \}$ is called the dual linear code

EXAMPLE: $C = \mathbb{F}_p \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} = \left\{ \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}, \dots, \begin{bmatrix} p-1 \\ \vdots \\ p-1 \end{bmatrix} \right\}$ = repetition code of length n over $\mathbb{F}_p$

$$C^\perp = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}^\perp = \left\{ \bar{x} \in \mathbb{F}_p^n : \sum_{i=0}^{n} x_i = 0 \right\} = \text{parity check code}$$

Call C a cyclic code if its codewords are closed under cycling positions

$$\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} \mapsto \begin{bmatrix} a_{n-1} \\ a_0 \\ a_1 \\ \vdots \\ a_{n-2} \end{bmatrix}$$

If we identify $\mathbb{F}_p[x]/(x^n-1) \cong \mathbb{F}_p^n$, then cycling positions = mult. by x, x^2, x^3, ...

$$a_0 + a_1 x + \dots + a_{n-1} x^{n-1} \longleftrightarrow \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}$$

Hence cyclic (linear) codes $C \subset \mathbb{F}_p^n$ correspond to ideals in $\mathbb{F}_p[x]/(x^n-1)$, which are always principal ideals $(g(x))$ with $g(x) \mid x^n-1$ (because $\mathbb{F}_p[x]$ is a P.I.D.)

(called a generator for C)

[redacted]: In this case, $C^\perp$ is also cyclic, generated by $g^\perp(x) = \frac{x^n-1}{g(x)}$

EXAMPLES: (2) The Hamming codes of length $n = p^k - 1$ over $\mathbb{F}_p$ are cyclic, generated by any primitive $f(x) \in \mathbb{F}_p[x]$ of degree k.

The dual Hamming codes are their duals, generated by $\frac{x^{p^k-1}-1}{f(x)}$.

(1) Repetition code $C \subset \mathbb{F}_p^n$ is cyclic, generator $1 + x + x^2 + \dots + x^{n-1}$

Parity check is its dual $C^\perp \subset \mathbb{F}_p^n$, generator $x-1 = \frac{x^n-1}{1+x+\dots+x^{n-1}}$

(5) Back in May (2017), Jim Propp asked

"Are there many cyclic codes $\mathcal{C} \subset \mathbb{F}_p^n$ for which the polynomial $X_{\mathcal{C}}^{maj}(q) := \sum_{\underline{a}=(a_0,a_1,\ldots,a_{n-1}) \in \mathcal{C}} q^{maj(\underline{a})}$ (where $maj(\underline{a}) := \sum_{i=0,\ldots,n-1 : a_i > a_{i+1}} i$ — major index)

has $X_{\mathcal{C}}^{maj}(q)\Big|_{q=f_n^d}$ counts codewords fixed by c^d ?" ($c :=$ cyclic shift)

(He had checked it worked for several codes $\mathcal{C} \subset \mathbb{F}_2^7$)

What about for $X_{\mathcal{C}}^{inv}(q) := \sum_{\underline{a} \in \mathcal{C}} q^{inv(\underline{a})}$ where $inv(\underline{a}) := \sum_{0 \le i < j \le n-1 : a_i > a_j} 1$?"

~~PROOF (not hard)~~

~~CONJECTURE~~

(Some context: MacMahon showed $\sum_{\underline{a} \text{ having } k \text{ 0's and } n-k \text{ 1's}} q^{maj(\underline{a})} = \sum_{\text{same } \underline{a}} q^{inv(\underline{a})} = \begin{bmatrix} n \\ k \end{bmatrix}_q$

so this fits with our $\begin{bmatrix} n \\ k \end{bmatrix}_{q=f_n^d}$ interpretation in PROBLEM 2)

CONJECTURE: Dual Hamming codes have the above property for $X_{\mathcal{C}}^{maj}(q)$ when $p=2$ or 3

⇑ + REU PROBLEM 6(a)

PROP (not hard): ~~Dual~~ Dual Hamming codes have the above property $\Leftrightarrow$ $f(x) \in \mathbb{F}_p[x]$ primitive, always has of degree k

$\frac{x^{p^k-1}-1}{f(x)} = \sum_{i=0}^{p^k-2} a_i x^i$ with # of descents in $(a_0, \ldots, a_{p^k-2})$ relatively prime to p^k-1

note $\frac{p-1}{2} \cdot p^{k-1}$ is rel. prime to p^k-1 if $p=2,3$

$= \begin{cases} 2^{k-2} & \text{if } p=2 \\ 3^{k-1} & \text{if } p=3 \end{cases}$

REU PROBLEM 6(b): Prove...

~~CONJ~~: Dual Hamming codes have the above property also for $X_{\mathcal{C}}^{inv}(q)$ when $p=2$.