Abstract Algebra, Lecture 15

Finite Fields

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

Linköping, fall 2019

Lecture notes availabe at course homepage
`http://courses.mai.liu.se/GU/TATA55/`

Summary

1. Existence of finite fields
   - Size is a prime power
   - The Frobenius endomorphism
   - Separability
   - Proof of existence and uniqueness
   - Galois field
2. Properties of finite fields
   - The multiplicative group is cyclic
   - Inclusion relations
3. Applications of finite fields
   - Calculating the number of irreducible polynomials of a given degree
   - Recurrence equations
     - Recognizing a recurrent sequence

Summary

1. **Existence of finite fields**
   - Size is a prime power
   - The Frobenius endomorphism
   - Separability
   - Proof of existence and uniqueness
   - Galois field
2. **Properties of finite fields**
   - The multiplicative group is cyclic
   - Inclusion relations
3. **Applications of finite fields**
   - Calculating the number of irreducible polynomials of a given degree
   - Recurrence equations
     - Recognizing a recurrent sequence

Summary

1. **Existence of finite fields**
    - Size is a prime power
    - The Frobenius endomorphism
    - Separability
    - Proof of existence and uniqueness
    - Galois field
2. **Properties of finite fields**
    - The multiplicative group is cyclic
    - Inclusion relations
3. **Applications of finite fields**
    - Calculating the number of irreducible polynomials of a given degree
    - Recurrence equations
        - Recognizing a recurrent sequence

Theorem

If F is a finite field, then $\mathtt{char}(F) = p$, where p is a prime number, and F has p^n elements.

Proof.

1. A field has characteristic zero (and then contains $\mathbb{Q}$ as a prime subfield) or characteristic p, with p prime, and then contains $\mathbb{Z}_p$ as its prime subfield
2. For a finite field F, the latter case must hold
3. Thus F is a vector space of finite dimension, n, over $\mathbb{Z}_p$
4. Thus F has p^n elements

□

Theorem

If $f(x) \in \mathbb{Z}_p[x]$ is irreducible, and of degree n, then

$$\frac{\mathbb{Z}_p[x]}{(f(x))}$$

is a finite field with p^n elements.

Theorem

For any prime p, and positive integer n, there is some irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree n.

Corollary

For any prime power $q = p^n$, there is a finite field with q elements.

The proof of the above theorem is somewhat tricky — so we will prove the existence of finie fields of size $q = p^n$ in another way.

Lemma

If F is a field with $\mathrm{char}(F) = p$, then

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \tag{1}$$

for all $a, b \in F$ and $n \in \mathbb{Z}_+$.

Proof

1. $n = 1$: By the binomial thm,

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \cdots + \binom{p}{p-1} a b^{p-1} + b^p$$

   where all terms except the first and the last are $\equiv 0 \mod p$

2. Suppose the identity holds for a fixed n; then it also holds for $n+1$, since

$$(a+b)^{p^{n+1}} = ((a+b)^p)^{p^n} = (a^p + b^p)^{p^n} = a^{p^{n+1}} + b^{p^{n+1}}$$

□

Frobenius endomorphism

Theorem

Let F be a field with characteristic p. Then

$$\varphi : F \to F$$
$$\varphi(v) = v^p$$

is an injective field homomorphism. If F is finite, then φ is an isomorphism.

Proof.

We have shown that $\varphi(u+v) = \varphi(u) + \varphi(v)$. Furthermore $\varphi(uv) = (uv)^p = u^p v^p = \varphi(u)\varphi(v)$, $\varphi(0) = 0^p = 0$, $\varphi(1) = 1^p = 1$. If $varphi(u) = u^p = 0$ then $u = 0$, so φ is injective. An injective map from a finite set to itself is also surjective. □

Fixed field of the Frobenius endomorphism

Theorem

Let F be a field of characteristic p which is an algebraic extension of its prime field $\mathbb{Z}_p$. Then $\mathbb{Z}_p$ is exactly the fixed field of φ, i.e., the set

$$\{\, u \in F \,|\, \varphi(u) = u \,\}$$

Proof.

Every element a of the prime field satisfies $a^p = a$, hence is a zero of $x^p - x$. This polynomial can have no more than p zeroes in F. But a zero of this polynomial is precisely a fixed point of φ. □

Definition

The polynomial $f(x) \in F[x]$, F a field, is *separable* if it has $\deg(f)$ distinct zeroes in its splitting field (no multiple zeroes).
An algebraic extension $F \leq L$ is separable if every element in L is the zero of a separable polynomial in $F[x]$.

Example

$x^3 - 2 \in \mathbb{Q}[x]$ is separable, as is $x^2 + x + 1 \in \mathbb{Z}_2[2]$, as we have seen.
Their splitting fields form separable extensions over the base fields.

Example

The polynomial $\mathbb{Z}_2(t)[x] \ni x^2 + t$ is irreducible, but splits as $(x + s)^2$ in its splitting field; here $s^2 = t$. Thus, the polynomial in question is not separable!

Theorem

Let F be a field and $f(x) \in F[x]$. Then $f(x)$ is separable iff $\gcd(f(x), f'(x)) = 1$.

Proof

- Assume $f(x)$ separable (and monic, for simplicity)
- Then $f(x) = (x - r_1) \cdots (x - r_n)$ in its splitting field
- Then $f'(x) = \sum_{j=1}^{n} \prod_{\ell \neq j} (x - r_\ell)$
- The zeroes of f are $r_1, \ldots, r_n$, but $f'(r_j) = \prod_{\ell \neq j} (r_j - r_\ell) \neq 0$
- No common zeroes (in the splitting field), so no common factor

Proof (cont)

- Now assume $f(x)$ not separable
- Then $f(x) = (x-r)^s g(x)$
- So $f'(x) = s(x-r)^{s-1}g(x) + (x-r)^s g'(x)$
- Can you spot the common factor?

□

Example

- Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. Then $f'(x) = 3x^2$, and $\gcd(f(x), f'(x)) = 1$. Hence $f(x)$ is separable.
- If $g(x) = x^2 + t \in \mathbb{Z}_2(t)[x]$ then $g'(x) = 2x = 0$, so $\gcd(g(x), g'(x)) = g(x)$. Hence $f(x)$ is not separable.
- Let $h(x) = x^2 + 1 \in \mathbb{Z}_2[x]$. Then $h'(x) = 0$, so $\gcd(h(x), h'(x)) = h(x)$ and $h(x)$ is not separable. Indeed, $h(x) = (x+1)^2$.
- Let $f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$. Then $f'(x) = 3x^2 + 1$ and $\gcd(f(x), f'(x) = 1$. So $f(x)$ is separable. Indeed, in $F[y] = \frac{\mathbb{Z}_2[x]}{(x^3+x+1)}[y]$, we have that

$$y^3 + y + 1 = (y + \overline{x}) * (y + \overline{x}^2) * (y + \overline{x}^2 + \overline{x})$$

We come to our main result:

Theorem

For any prime power $q = p^n$ there is a finite field F with q elements. Any field with q elements is isomorphic to the splitting field of

$$\phi_q(x) = x^q - x \in \mathbb{Z}_p[x].$$

Proof (of existence)

- Let F be the splitting field of $\phi(x) \in \mathbb{Z}_p[x]$
- The derivative is $\phi'(x) = qx^{q-1} - 1 = -1 \in \mathbb{Z}_p[x]$, because of charateristic p. It is thus is relatively prime to $\phi(x)$.
- So $\phi(x)$ is a separable polynomial, and splits into q distinct linear factors in F.
- Claim: the zeroes of $\phi(x)$ in F form a subfield of F. Proved on next slide
- Since the zeroes of ϕ form a subfield of F, the smallest field with all the zeroes, it is F
- $\phi(x)$ has q distinct zeroes, so F has q elements

Proof (of the claim)

- Clearly $\phi(0) = \phi(1) = 0$
- If $\phi(u) = u^q - u = 0$ and $\phi(v) = v^q - v = 0$, then

  $$\phi(u+v) = (u+v)^q - (u+v) = u^q + v^q - (u+v) = u^q - u + v^q - v = 0,$$

  where we used the lemma from earlier
- $\phi(-u) = (-u)^q - (-u) = -u^q + u = 0$ in odd characteristic, and in characteristic 2 we have that $-u = u$, so still OK.
- $\phi(1/u) = u^{-q} - u^{-1} = 1/u^q - 1/u = 1/u - 1/u = 0$.

Proof (of uniqueness up to iso)

- Suppose E another field with q elements
- Pick $u \in E$
- If $u = 0$ then $f(u) = 0$
- If $u \neq 0$ then $u \in E^*$, the multiplicative group of E
- E^* has $q - 1$ elems, so by Lagrange, $u^{q-1} = 1$
- So $u^q = u$, and $\phi(u) = 0$.
- E has q elemens, and $\phi(x)$ splits in E, so it is a splitting field of $\phi(x)$
- Splitting fields of $\phi(x)$ are isomorphic

Definition

Let $q = p^n$, with p prime. The unique (up to iso) finite field with q elements is denoted $GF(q)$ and refered to as the *Galois field* of order q.

Example

- Let's construct $GF(2^3)$ as the splitting field of $\phi(x) = x^8 + x \in \mathbb{Z}_2[x]$
- We first factor

$$x^8 + x = x(x+1)(x^3+x+1)(x^3+x^2+1)$$

- We make a Kronecker extension to get at least one zero:

$$F = \frac{\mathbb{Z}_2[x]}{(x^3+x+1)}$$

- In $F[x]$, everything splits:

$$\begin{aligned} x^8 + x = x(x+1)(x+\overline{x})(x+\overline{x}^2)(x+\overline{x}^2+\overline{x})\cdot \\ \cdot (x+\overline{x}+1)(x+\overline{x}^2+1)(x+\overline{x}^2+\overline{x}+1) \end{aligned}$$

- So F is already the splitting field

Example ($GF(8)$ cont)

- So $F \simeq GF(8)$
- The 8 elements are

$$0, 1, \overline{x}, \overline{x}+1, \overline{x}^2, \overline{x}^2+1, \overline{x}^2+\overline{x}, \overline{x}^2+\overline{x}+1.$$

- Relation: $\overline{x}^3 = \overline{x}+1$.
- If we instead put

$$K = \frac{\mathbb{Z}_2[y]}{(y^3+y^2+1)}$$

  things still work
- K is the splitting field of $\phi(x)$, $K \simeq GF(8)$.
- The 8 elements are

$$0, 1, \overline{y}, \overline{y}+1, \overline{y}^2, \overline{y}^2+1, \overline{y}^2+\overline{y}, \overline{y}^2+\overline{y}+1.$$

- Relation: $\overline{y}^3 = \overline{y}^2+1$.
- The map $\overline{x} \mapsto \overline{y}+1$ is an isomorphism between F and K

Theorem

Let F be a field (not necessarily finite), and let G be a finite subgroup of the multiplicative group F^*. Then G is cyclic.

Proof

- Put $n = |G|$
- G is abelian, so $G \simeq C_{q_1} \times \cdots \times C_{q_r}$, with q_i prime powers
- Put $m = \mathrm{lcm}(q_1, \ldots, q_r)$
- Exists $g \in G$ with $o(g) = m$
- If $h \in G$, with $r = o(h)$, then $r|m$, and $h^r = 1$
- Hence h is a zero of $x^r - 1$
- But $x^r - 1$ divides $x^m - 1$, so h is a zero of that poly, as well

Proof (cont)

- Lagrange: $x^m - 1$ has at most m zeroes in F
- We have found n zeroes, so $n \leq m$
- But m is maximal order of element in G, and $n = |G|$, so $m \leq n$
- Thus $m = n$
- Thus G is cyclic

Corollary

If F is a finite field of characteristic p, then $F^* = \langle u \rangle$ for some $u \in F^*$. Furthermore, $F = \mathbb{Z}_p(u)$.

Recall:

Theorem

If $G = |g|$ is a cyclic group of order $n < \infty$, then g^k is another generator iff $\gcd(k, n) = 1$. Thus there are precisely $\varphi(n)$ generators of G.

Example

$\varphi(2^3 - 1) = 2^3 - 1 - 1 = 6$, so $GF(8)^*$ is a cyclic group of order 7, and every element except the identity generates it. For instance, if we present it as

$$GF(8) = \frac{\mathbb{Z}_2[x]}{(x^3 + x + 1)}$$

then the element $\overline{x}$ generates $GF(8)^*$:

$$\overline{x}^0 = 1, \overline{x}^1 = \overline{x}, \overline{x}^2 = \overline{x}^2, \overline{x}^3 = \overline{x} + 1,$$

$$\overline{x}^4 = \overline{x}^2 + \overline{x}, \overline{x}^5 = \overline{x}^2 + \overline{x} + 1, \overline{x}^6 = \overline{x}^2 + 1, \overline{x}^7 = 1$$

In a somewhat backwards fashion, we are able to prove the existence of irreducible polynomials of arbitrary degree:

Theorem

Let p be a prime and n a positive integer. Then there is some irreducible polynomial in $\mathbb{Z}_p[x]$ of degree n.

Proof.

- $E = GF(p^n)$ exist
- It has $\mathbb{Z}_p$ as prime subfield
- $E^* = \langle u \rangle$ for some $u \in E^*$
- The element u thus satisfies $\mathbb{Z}_p(u) = E$
- It has a minimal polynomial $f(x) \in \mathbb{Z}_p[x]$
- That polynomial is irreducible, and has degree n.

□

Example

We calculate the minimal polynomial of the elements $GF(8) \simeq \frac{\mathbb{Z}_2[x]}{(x^3+x+1)}$.

0	x
1	$x+1$
$\overline{x}$	x^3+x+1
$\overline{x}+1$	x^3+x^2+1
$\overline{x}^2$	x^3+x+1
$\overline{x}^2+1$	x^3+x^2+1
$\overline{x}^2+\overline{x}$	x^3+x+1
$\overline{x}^2+\overline{x}+1$	x^3+x^2+1

Theorem

Every subfield of $GF(p^n)$ has size p^m with $m|n$; conversely, if $m|n$ then there is a unique isomorphic copy of $GF(p^m)$ inside $GF(p^n)$.

Proof.

If $\mathbb{Z}_p \leq E \leq GF(p^n)$ then $n = [GF(p^n) : \mathbb{Z}_p] = [GF(p^n) : E][E : \mathbb{Z}_p]$, so $m = [E : \mathbb{Z}_p]$ is a divisor of n, and $|E| = p^m$.
If $n = mk$ then $p^m - 1 | p^n - 1$, and $(x^{p^m-1} - 1)|(x^{p^n-1} - 1)$; thus $(x^{p^m} - x)|(x^{p^n} - x)$.
So every zero of $x^{p^m} - x$ is a zero of $x^{p^m} - x$, thus $GF(p^n)$ contains the splitting field of $x^{p^m} - x$ as a subfield (the subfield consisting of precisely those zeroes). □

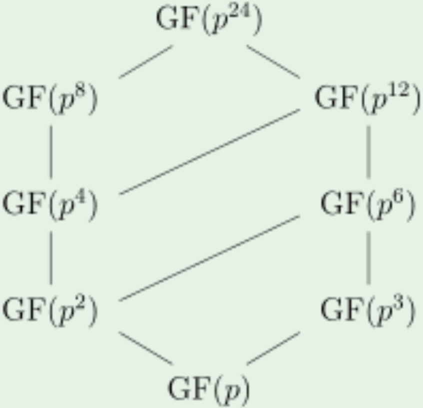
Example

The non-zero elements of $GF(16)$ have the following orders and minimal polynomials. The ones with order 3 and minimal polynomial x^2+x+1 form (together with zero) a subfield isomorphic to $GF(4)$.

15	x^4+x+1
15	x^4+x+1
5	$x^4+x^3+x^2+x+1$
15	x^4+x+1
3	x^2+x+1
5	$x^4+x^3+x^2+x+1$
15	x^4+x^3+1
15	x^4+x+1
5	$x^4+x^3+x^2+x+1$
3	x^2+x+1
15	x^4+x^3+1
5	$x^4+x^3+x^2+x+1$
15	x^4+x^3+1
15	x^4+x^3+1
1	$x+1$

Example

The subfields of $GF(p^n)$ form a poset order-isomorphic to the divisor lattic of n. For instance, the subfields of $GF(p^{24})$ are as follows.



Theorem

Let F be a subfield of $GF(p^n)$. Then $|F| = p^m$ with $m|n$.

1. *F is the splitting field of $x^{p^m} - x$*
2. *F is the fixed field of φ^m, where φ is the Frobenius endomorphism.*

Example

Let $GF(2^4) = \mathbb{Z}_2(c)$ where c has minimal polynomial x^4+x+1. Then φ^2 acts as

$$\begin{pmatrix} 0 & 0 \\ c & c+1 \\ c^2 & c^2+1 \\ c^3 & c^3+c^2+c+1 \\ c+1 & c \\ c^2+c & c^2+c \\ c^3+c^2 & c^3+c \\ c^3+c+1 & c^3+c^2+1 \\ c^2+1 & c^2 \\ c^3+c & c^3+c^2 \\ c^2+c+1 & c^2+c+1 \\ c^3+c^2+c & c^3+1 \\ c^3+c^2+c+1 & c^3 \\ c^3+c^2+1 & c^3+c+1 \\ c^3+1 & c^3+c^2+c \\ 1 & 1 \end{pmatrix}$$

Theorem

Fix a prime p and consider all finite fields $GF(p^n)$ with n a positive integer.

1. *All such fields contain $GF(p)$*
2. *Given two such fields, there is a unique smallest field in the collection that contains both*
3. *The union of all fields in the collection is the algebraic closure of each and every field therein*

Theorem

Let p be a prime, n a positive integer, $q = p^n$. The factorization of $x^q - x \in \mathbb{Z}_p[x]$ into irreducible factors contain each monic irreducible polynomial $h(x) \in \mathbb{Z}_p[x]$ whose degree divides n, each such polynomial occuring exactly once.

Example

$x^{2^4} - x = x \cdot (x+1) \cdot (x^2+x+1) \cdot (x^4+x+1) \cdot (x^4+x^3+1) \cdot (x^4+x^3+x^2+x+1)$ and the factorization lists all irreducible polynomials in $\mathbb{Z}_2[x]$ of degree 1,2, or 4.

Proof

- $GF(q)$ is the splitting field of $\phi(x)$ and consists precisely of its zeroes.
- Let $u \in GF(q)$ and let $h(x)$ be its minimal polynomial. Then $h(x)$ is irreducible, and $d = \deg(h(x)) = [\mathbb{Z}_p(u) : \mathbb{Z}_p]$, so it is a divisor of $n = [GF(q) : \mathbb{Z}_p]$.
- There will be d zeroes in total of $h(x)$, and $h(x) = (x - u)(x - u_2) \cdots (x - u_d)$.
- This accounts for all zeroes, since different irreducible polynomials have no zeroes in common (each irreducible polynomial is the minimal polynomial of each of its zeroes)

Theorem

Let p be prime, and let $c(d,p)$ denote the number of irreducible monic polynomials of degree d in $\mathbb{Z}_p[x]$. Then for any positive integer n, it holds that

$$p^n = \sum_{d|n} d c_{d,p} \tag{2}$$

Proof.

Consider

$$x^{p^n} - x = \prod_{d|n} \prod_{\substack{\deg(h(x))=d \\ h(x) \text{ irr}}} h(x)$$

and take degrees of the LHS and the RHS. □

Theorem (Möbius inversion)

Let $\mu(n)$ be zero unless n is a square-free integer, in which case it is $(-1)^r$ where r is the number of primes in its factorization. Let f be defined on the positive integers, and define F via f as

$$F(n) = \sum_{d|n} f(d).$$

Then one can recover f as

$$f(n) = \sum_{d|n} F(d)\mu(n/d) = \sum_{d|n} F(n/d)\mu(d).$$

Proof.

Induction gives a short and uninspired proof. □

Theorem

Let $c_{n,p}$ denote the number of degree n monic irreducible polynomials in $\mathbb{Z}_p[x]$. Then

$$c_{n,p} = \frac{1}{n} \sum_{d|n} \mu(n/d) p^d.$$

Proof.

Put $f(n) = nc_{n,p}$. Then

$$F(n) = p^n = \sum_{d|n} f(n)$$

so by Möbius inversion

$$f(n) = \sum_{d|n} \mu(n/d) F(n) = \sum_{d|n} \mu(n/d) p^d,$$

whence

$$c_{n,p} = \frac{1}{n} \sum_{d|n} \mu(n/d) p^d.$$

□

Example

The number of irreducible polynomials of degree n in $\mathbb{Z}_2[x]$ is

$$
\begin{aligned}
c_{1,2} &= \frac{1}{1}(\mu(1)2^1) = 2\\
c_{2,2} &= \frac{1}{2}(\mu(2)2^1 + \mu(1)2^2) = 1\\
c_{3,2} &= \frac{1}{3}(\mu(3)2^1 + \mu(1)2^3) = 2\\
c_{4,2} &= \frac{1}{4}(\mu(4)2^1 + \mu(2)2^2 + \mu(1)2^4) = 3\\
c_{5,2} &= 6\\
c_{6,2} &= 9
\end{aligned}
$$

and so on.

Example

The number of irreducible monic polynomials of degree n in $\mathbb{Z}_3[x]$ is

$$\begin{aligned} c_{1,3} &= \frac{1}{1}(\mu(1)3^1) = 3 \\ c_{2,3} &= \frac{1}{2}(\mu(2)3^1 + \mu(1)3^2) = 6 \\ c_{3,3} &= \frac{1}{3}(\mu(3)3^1 + \mu(1)3^3) = 24 \end{aligned}$$

and so on.

Corollary

There are irreducible polynomials of degree n in $\mathbb{Z}_p[x]$.

Proof.

We have that

$$c_{n,p} = \mu(1)p^n + \sum_{\substack{d|n \\ d<n}} \mu(n/d)p^d,$$

and the latter sum is in magnitude $\leq$

$$\sum_{d=0}^{n-1} p^d = \frac{p^n - 1}{p - 1} < p^n,$$

so $c_{n,p} > 0$. □

In fact, the same methods show

Theorem

Let $c_{n,q}$ denote the number of degree n monic irreducible polynomials in $GF(q)[x]$. Then

$$c_{n,q} = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d.$$

This integer is always positive, so there are irreducible monic polynomials of degree n in $GF(q)[x]$.

Definition

A *linear homogeneous reccurence equation with constant coefficients* of degree m over a field F is of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}, \qquad n \geq k$$

with $c_j \in F$. A solution is a sequence $(a_n)_{n \in \mathbb{N}}$ in F.
It is uniquely determined once additional *initial conditions*

$$\begin{aligned} a_0 &= b_0 \\ a_1 &= b_1 \\ &\vdots \\ a_{k-1} &= b_{k-1} \end{aligned}$$

are assigned.

Theorem

- *Any F-linear combination of solutions to the LHRE (without initial conditions) is again a solution*
- *If u is a root (in some extension field, if necessary) of the characteristic equation*

  $$u^k = c_1 u^{k-1} + c_2 u^{k-2} + \cdots + c_k$$

  then

  $$a_n = u^n, \qquad n \geq 0$$

  is a solution
- *If u has multiplicity r then*

  $$a_n = n^s u^n$$

  is also a solution, for $s < r$.

Example

Consider the Fibonacci reccurence

$$a_n = a_{n-1} + a_{n-2}$$

over $\mathbb{Q}$. The characteristic equation is

$$x^2 - x - 1 = 0,$$

with roots

$$\sigma_1 = -\frac{1}{2}\sqrt{5} + \frac{1}{2}, \quad \sigma_2 = \frac{1}{2}\sqrt{5} + \frac{1}{2}$$

Note that the roots lie in the extension $\mathbb{Q}(\sqrt{5})$. The general solution is

$$a_n = v_1\sigma_1^n + v_2\sigma_2^n,$$

where v_1, v_2 can be determined by the initial conditions.

Example (cont)

For instance, if $a_0 = a_1 = 1$, (and $a_2 = 2$, $a_3 = 3$, $a_4 = 5$,and so on) then

$$\begin{aligned} 1 &= v_1 \sigma_1^0 + v_2 \sigma_2^0 = v_1 + v_2 \\ 1 &= v_1 \sigma_1^1 + v_2 \sigma_2^1 = v_1 \sigma_1 + v_2 \sigma_2 \end{aligned}$$

and $v_1, v_2 \in \mathbb{Q}(\sqrt{5})$, yet each $a_n \in \mathbb{Q}$, (in fact, in $\mathbb{Z}$).

Example

Now consider the same reccurence

$$a_n = a_{n-1} + a_{n-2}$$

but over $\mathbb{Z}_2$. Now $\sigma_1, \sigma_2 \in E$, where

$$E = \frac{\mathbb{Z}_2[x]}{x^2 + x + 1} \simeq GF(4).$$

In fact, $\sigma_1 = \overline{x}$ and $\sigma_2 = \overline{x} + 1$. The general solution is

$$a_n = v_1 \overline{x}^n + v_2 (\overline{x} + 1)^n$$

Example (cont)

We tabulate

n	a_n	$\overline{x}^n$	$(\overline{x}+1)^n$
0	1	1	1
1	1	$\overline{x}$	$\overline{x}+1$
2	0	$\overline{x}+1$	$\overline{x}$
3	1	1	1
4	1	$\overline{x}$	$\overline{x}+1$
5	0	$\overline{x}+1$	$\overline{x}$
6	1	1	1

Interestingly, the solutions are periodic!

Example (Cont)

To solve the recurrence with the initial conditions $a_0 = a_1 = 1$, we must solve

$$\begin{aligned} 1 &= v_1 + v_2 \\ 1 &= v_1 \overline{x} + v_2(\overline{x} + 1) \end{aligned}$$

which gives $v_1 = v_2 = 1$ and $a_n = \overline{x}^n + (\overline{x} + 1)^n$.
Of course, taking periodicity into account, we have that

$$a_n = \begin{cases} 1 & n \equiv 0 \mod 3 \\ 1 & n \equiv 1 \mod 3 \\ 0 & n \equiv 2 \mod 3 \end{cases}$$

Theorem

Any solution to the degree k LHRE over $GF(q)$ is periodic, with period length $\leq q^k$.

Proof.

The value of a_n depends only on the vector

$$(a_{n-1}, a_{n-2}, \dots, a_{n-k}) \in GF(q)^k$$

We can form a digraph where the vertices are such "states", and where there are directed edges

$$(a_{n-1}, a_{n-2}, \dots, a_{n-k}) \longrightarrow (a_n, a_{n-2}, \dots, a_{n-k+1})$$

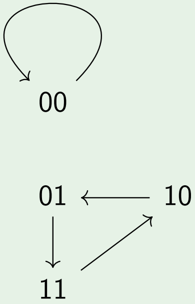
Starting at

$$(a_{k-1}, a_{k-2}, \dots, a_0)$$

in this digraph, we'll eventually enter a directed cycle. □

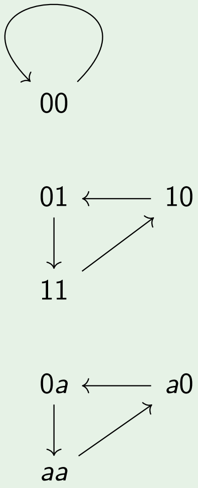
Example

The Fibonacci reccurence over $GF(2)$ is described by



Example

Over $GF(4)$ the Fibonacci reccurence (we put $a = \overline{x}$ and $b = \overline{x} + 1$) is described by a digraph with 16 vertices. Here is a portion of it:



Generating function

Definition

Let R be a domain and $a = (a_j)_{j=0}^{\infty}$ a sequence of elements in R. The *generating function* of the sequence is the formal power series

$$G(a) = \sum_{j=0}^{\infty} a_j t^j \in R[[t]]$$

Example

The generating function of the constant sequence $1, 1, 1, \ldots$ is

$$1 + t + t^2 + t^3 + \cdots = \frac{1}{1-t}.$$

The utility of generating functions comes from the following properties:

Lemma

- *$G(a+b) = G(a) + G(b)$*
- *If $c \in R$ then $G(ca) = cG(a)$*
- *Denote by S the shift $S(a)_i = a_{i-1}$, $S(a)_0 = 0$. Then $G(S(a)) = tG(a)$*

Proof.

The first two properties are obvious, and

$$t \sum_{j=0}^{\infty} a_j t^j = \sum_{j=0}^{\infty} a_j t^{j+1} = 0 + \sum_{\ell=1}^{\infty} a_{\ell-1} t^{\ell}$$

□

Theorem

Suppose that the sequence $(s_n)_{n=0}^{\infty}$ *in* $F = GF(q)$ *satisfies*

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \dots a_0 s_n$$

a linear recurrence relation over F *of degree* k*. Call*

$$g(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \dots - a_0 \in F[x]$$

the characteristic polynomial of the sequence, and denote by

$$g^*(x) = 1 - a_{k-1}x - a_{k-2}x^2 - \dots - a_0 x^k \in F[x]$$

its reciprocal polynomial. Suppose that all zeroes of $g(x)$*, in some extension* $\tilde{F}$ *of* F*, are simple. Then*

1. $$s_n = \sum_{j=1}^{k} \beta_j \alpha_j^n$$

   where the α*'s are the zeroes of* $f(x)$ *in* $\tilde{F}$*, and the* β*'s are uniquely determined elements of* $\tilde{F}$*.*
2. *The generating function of the sequence is a rational function*

   $$G(x) = \frac{f(x)}{g^*(x)}$$

   with $f(x)$ *of degree* $< k$*.*

Example

Let (a_j) be the sequence over $\mathbb{Z}_2$ given by $a_0 = a_1 = 1$, $a_n = a_{n-1} + a_{n-2}$. Let $f(t) = G(a)$. Then

$$a = (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, \dots)$$

as we have seen before, and

$$f(t) = 1 + t + 0t^2 + t^3 + t^4 + \cdots \in \mathbb{Z}_2[[t]]$$

Since

$$1 + t^3 + t^6 + t^9 + \cdots = \frac{1}{1+t^3}$$

we get that

$$f(t) = \frac{1+t}{1+t^3} = \frac{1}{1+t+t^2}.$$

Example (cont.)

We could have arrived at this as follows: from

$$a_n = a_{n-1} + a_{n-2}, \qquad a_0 = a_1 = 1$$

we sum and get

$$\sum_{n=2}^{\infty} a_n t^n = \sum_{n=2}^{\infty} a_{n-1} t^n + \sum_{n=2}^{\infty} a_{n-2} t^n$$

hence

$$f(t) - a_1 t - a_0 = tf(t) - a_0 t + t^2 f(t)$$

so

$$f(t) = \frac{a_1 t + a_0 - a_0 t}{t^2 - t - 1} = \frac{1}{1 + t + t^2}$$

Example (cont.)

We now factor the denominator as

$$t^2 + t + 1 = (t + \alpha)(t + \alpha + 1)$$

in the extension $GF(4) = \mathbb{Z}_2(\alpha)$ with $\alpha^2 = \alpha + 1$. Then we can do partial fraction decomposition as

$$\frac{1}{t^2 + t + 1} = \frac{1}{(t + \alpha)(t + \alpha + 1)} = \frac{A}{t + \alpha} + \frac{B}{t + \alpha + 1}$$

so

$$A(t + \alpha + 1) + B(t + \alpha) = 1,$$

hence setting $t = \alpha$ we get $A * 1 = 1$, and setting $t = \alpha + 1$ we have $B * 1 = 1$.

Example (cont.)

Since $\alpha^2 = \alpha + 1$ we have that $1 = \alpha(\alpha+1)$ so

$$\sum_{n=0}^{\infty} a_n t^n = \frac{1}{t+\alpha} + \frac{1}{t+\alpha+1} = \frac{\alpha^{-1}}{1+\alpha^{-1}t} + \frac{(1+\alpha)^{-1}}{1+(1+\alpha)^{-1}t} =$$

$$\frac{\alpha+1}{1+(\alpha+1)t} + \frac{\alpha}{1+\alpha t} =$$

$$\sum_{n=0}^{\infty} (\alpha+1)^{n+1} t^n + \sum_{n=0}^{\infty} (\alpha)^{n+1} t^n = \sum_{n=0}^{\infty} (\alpha^{n+1} + (\alpha+1)^{n+1}) t^n$$

Example (cont.)

We tabulate

n	α^{n+1}	$(\alpha+1)^{n+1}$	$\alpha^n + (\alpha+1)^{n+1}$
0	α	$\alpha+1$	1
1	$\alpha+1$	α	1
2	1	1	0
3	α	$\alpha+1$	1
4	$\alpha+1$	α	1
5	1	1	0

We once again see that the sequence $(a)_n$ is periodic with period 3.

Example

Suppose that we are given the start of a sequence in $GF(q)$, and are told that the sequence is reccurent, of relatively low degree. Can we find the reccurence relation that the sequence satisfies, even if the part we are given is shorter than the period length?
Express $F = GF(25)$ as $\mathbb{Z}_5(a)$, with a having minimal polynomial

$$x^2 + 4x + 2 = 0$$

over $\mathbb{Z}_5$. Consider the sequence with generating function

$$G(x) = a + 2 + (4a + 4)\,x + 2x^2 + 4x^3 + 3ax^4 + (3a + 3)\,x^5 + 3x^6 + 4x^7 + (2a + 2)\,x^8 + (4a + 1)\,x^9 + O(x^{10})$$

We want to express $G(x) = f(x)/g(x)$, i.e., $G(x) * g(x) = f(x)$

Example

Let us first check if any linear $g(x)$ works. For instance, what about $1+x$? Well,

$$(1+x)*(a+2+(4a+4)\,x+2x^2+4x^3+3ax^4+(3a+3)\,x^5+3x^6+4x^7+(2a+2)\,x^8+(4a+1)\,x^9+O(x^{10}))=$$
$$a+2+x+(4a+1)\,x^2+x^3+(3a+4)\,x^4+(a+3)\,x^5+(3a+1)\,x^6+2x^7+(2a+1)\,x^8+(a+3)\,x^9+O(x^{10})$$

so no dice. No other first degree denominators work, either. However, testing quadratic monic irreducible polynomials, we find

$$(1+x+(a+3)\,x^2) \quad *$$
$$(a+2+(4a+4)\,x+2x^2+4x^3+3ax^4+(3a+3)\,x^5+3x^6+4x^7+(2a+2)\,x^8+(4a+1)\,x^9+O(x^{10}))=$$
$$a+2+x+O(x^{10})$$

so we belive that

$$G(x)=\frac{t+a+2}{(a+3)\,t^2+t+1}.$$

One can use so-called Padé approximants to get the denominator an the numerator directly:

Theorem

Let $f(x) \in F[[x]]$ be a formal power series. For positive integers m, n, there is a unique rational function $R(x) = a(x)/b(x)$ with $\deg(a) = m$, $\deg(b) = n$, $b(0) = 1$, called the Padé approximant of order $[m/n]$, such that

$$f(x) \equiv R(x) \mod (x^{m+n}).$$

The Padé approximant can be determined by performing the Euclidean algorithm (see for instance the Wikipedia page) or by solving for the coefficients in the Ansatz

$$\frac{a_m x^m + \cdots + a_0}{b_n x^n + \cdots + b_1 x + 1} = c_0 + c_1 x + \ldots c_{n+m} x^{n+m} \mod (x^{n+m+1})$$

For [2/2] PA we have

$$\frac{a_2x^2 + a_1x + a_0}{b_2x^2 + b_1x + 1} \approx c_0 + c_1x + c_2x^2 + c_3x^3 + c_4x^4$$

so

$$\begin{aligned} a_2x^2 + a_1x + a_0 &\approx (c_0 + c_1x + c_2x^2 + c_3x^3 + c_4x^4)(b_2x^2 + b_1x + 1) \\ &\approx c_0 + (c_0b_1 + c_1)x + (c_0b_2 + c_1b_1 + c_2)x^2 + \\ &\quad (c_1b_2 + c_2b_1 + c_3)x^3 + (c_2b_2 + c_3b_1 + c_4)x^4 \end{aligned}$$

hence

$$\begin{aligned} a_0 &= c_0 \\ a_1 &= c_0b_1 + c_1 \\ a_2 &= c_0b_2 + c_1b_1 + c_2 \\ 0 &= c_1b_2 + c_2b_1 + c_3 \end{aligned}$$

et cetera are the equations to determine the a_i's and the b_j's.

Example

In our example, the Padé approximant of order $[1/2]$ is

$$\frac{t+a+2}{(a+3)\,t^2+t+1}.$$

Note that we only need a tiny part of $G(x)$ to find this; however, a longer initial sequence gives us more confidence that we have found the true rational function.

Example

Since the denominator is $(a+3)\,t^2 + t + 1$, the sequence should satisfy

$$s_{n+2} = -s_{n+1} - (a+3)s_n.$$

The sequence starts

$$a+2,\ 4a+4,\ 2$$

and

$$\begin{aligned}-(4a+4) - (a+3)(a+2) = -4a - 4 - a^2 - 2a - 3a - 6 = \\ -a^2 + a = 4a + 2 + a = 2.\end{aligned}$$