Proofs about Frobenius

Sizes of finite fields

Theorem: Let k be a finite field. Let t be the smallest positive integer such that

$$\underbrace{1 + \ldots + 1}_{t} = 0$$

Then t is a prime number, and the number of elements in k is a power of t.

Proof: Define a map $f : \mathbf{Z} \to k$ by

$$f(\ell) = \underbrace{1 + \ldots + 1}_{\ell} \in k$$

This map respects addition and multiplication, in the sense that $f(\ell + m) = f(\ell) + f(n)$ and $f(\ell \cdot m) = f(\ell) \cdot f(m)$. This can be proven by induction, or heuristically by drawing pictures with braces. Let

$$I = \{\ell \in \mathbf{Z} : f(\ell) = 0\}$$

It is pretty easy to check that I is closed under addition, and under multiplication by integers, and thus must be of the form

$$I = t \cdot \mathbf{Z}$$

for some integer t, the least positive element in I. Therefore, we get a map

$$f : \mathbf{Z}/t \to k$$

that preserves addition and multiplication. If the latter f were not injective, then for some $1 \leq i < j \leq t$ we'd have $f(i) = f(j)$, but then $f(j - i) = 0$ and $0 < j - i < t$, contradiction.

The integer t is prime, since if $t = ab$ with $1 < a \leq b < t$, then

$$f(a) \cdot f(b) = 0$$

so since k is a field one or the other of the factors is 0. But this contradicts the minimality of t. So t is prime.

Thus, the copy $f(\mathbf{Z}/t)$ of the **field** $\mathbf{F}_t = \mathbf{Z}/t$ sits inside k. We choose to view k as a vectorspace with scalars $\mathbf{F}_t$. It is finite, so must have finite dimension, and a *basis* $e_1, \ldots, e_n$ over $\mathbf{F}_t$. The set of linear combinations of these basis elements is exactly the whole (field) vector space k, and there are t^n choices of coefficients, so k has t^n elements. ///

Corollary: There are no finite fields with number of elements other than powers of primes. ///

Definition: Given a finite field k, the uniquely determined prime integer p such that (a copy of) $\mathbf{Z}/p$ sits insides k, and such that k is a vector space over $\mathbf{Z}/p$, is the **characteristic** of k.

Field extensions

Let k be a field. A field K containing k is an **extension field** of k, and k is a **subfield** of K.

Theorem: Let k be a field, $P(x)$ an irreducible polynomial of degree $d > 0$ in $k[x]$. Then $k[x]/P$ is a *field*. Any element $\beta \in k[x]/P$ can be *uniquely* expressed as

$$\beta = R(\alpha)$$

where R is a polynomial with coefficients in k and of degree strictly less than the degree of $P. < d$. //

Remark: The **degree** of the extension K of k, written $[K : k]$, is the degree of the polynomial P.

Remark: Thinking of α as 'existing' and being a root of the equation $P(x) = 0$, we have **adjoined** a root of $P(x) = 0$ to k. Write

$$k(\alpha) = k[x]/P$$

Corollary: For $k = \mathbf{F}_q$, for irreducible polynomial P of degree n, $K = k[x]/P(x)$ has q^n elements.

Proof: Every element of K has a unique expression as $Q(\alpha)$ for polynomial Q of degree $< n$. There are q choices for each coefficient, so q^n choices altogether. ///

Frobenius automorphism

Let $k = \mathbf{F}_q = GF(q)$ where $q = p^n$ is a power of a prime p. Fix $N > 1$ and $K = \mathbf{F}_{q^N} = GF(q^N)$. The **Frobenius automorphism** of K **over** k is

$$\Phi(\alpha) = \alpha^q$$

Proposition: The Frobenius Φ of $K = \mathbf{F}_{q^N}$ over $k = \mathbf{F}_q$ is a bijection of K to K. In particular,

$$\Phi^N = \underbrace{\Phi \circ \Phi \circ \ldots \circ \Phi}_{N}$$

is the identity map on K (which maps every element of K to itself).

Proof: Since the Frobenius just takes q^{th} powers and K is closed under multiplication, Φ maps K to K. A cute way to prove that $\Phi : K \to K$ is a bijection is to prove Φ^N is the identity map on K. Certainly $\Phi(0) = 0$. The set $K^\times = K - \{0\}$ has $q^N - 1$ elements, so (Lagrange's theorem, or computation) $\beta^{q^N-1} = 1$ for $\beta \in K^\times$.

///

Proposition: $\alpha \in K$ is in k if and only if $\Phi(\alpha) = \alpha$.

Proof: The multiplicative group $k^\times$ of nonzero elements in k has $q - 1$ elements, so by Lagrange's theorem the *order* of any element α in k is a divisor d of $q - 1$, so $\alpha^{q-1} = 1$ and $\alpha^q = \alpha$.

On the other hand, suppose $\alpha \in K$ and $\Phi(\alpha) = \alpha$. Then α is a solution $x^q - x = 0$ lying inside K. By unique factorization, an equation of degree q has at most q roots. We already found q roots of this equation, namely the elements of the smaller field k sitting inside K. So there simply can't be any other roots of that equation other than the elements of k.

///

Proposition: The Frobenius Φ of K over k has the property that, for any α, β in K,

$$\begin{aligned} \Phi(\alpha + \beta) &= \Phi(\alpha) + \Phi(\beta) \\ \Phi(\alpha \cdot \beta) &= \Phi(\alpha) \cdot \Phi(\beta) \end{aligned}$$

Thus, Φ preserves addition and multiplication. Φ is bijective, so is a **field isomorphism**.

Proof: The assertion about preserving multiplication is simply the assertion that the q^{th} power of a product is the product of the q^{th} powers.

The fact Φ preserves addition uses the fact that the exponent is q, a power of a prime number p. We claim that for α, β in K

$$(\alpha + \beta)^p = \alpha^p + \beta^p$$

Expanding by the binomial theorem, the left-hand side is

$$\alpha^p + \binom{p}{1}\alpha^{p-1}b + \ldots + \binom{p}{p-1}\alpha^1 b^{p-1} + \beta^p$$

All the middle binomial coefficients are integers divisible by p, so are 0 in K. Repeatedly invoking this,

$$(\alpha + \beta)^{p^2} = (\alpha^p + \beta^p)^p = a^{p^2} + b^{p^2}$$

$$(\alpha+\beta)^{p^3} = (\alpha^p+\beta^p)^{p^2} = (a^{p^2}+b^{p^2})^p = \alpha^{p^3}+\beta^{p^3}$$

That is, by induction,

$$(\alpha + \beta)^{p^{nN}} = \alpha^{p^{nN}} + \beta^{p^{nN}}$$

That is, the Frobenius map preserves addition.

///

Proposition: Let $P(x)$ be a polynomial with coefficients in $k = \mathbf{F}_q$. Let $\alpha \in K$ be a root of $P(x) = 0$. Then $\Phi(\alpha) = \alpha^q$, $\Phi^2(\alpha) = \Phi(\Phi(\alpha)) = \alpha^{q^2}$, ... are also roots of the equation.

Proof: Let

$$P(x) = c_n x^n + c_{n-1}x^{n-1} + \ldots + c_2x^2 + c_1x + c_0$$

with all c_i's in k. Apply Frobenius to both sides of

$$0 = c_n\alpha^n + c_{n-1}\alpha^{n-1} + \ldots + c_2\alpha^2 + c_1\alpha + c_0$$

to obtain

$$0 = \Phi(c_n)\Phi(\alpha)^n + \ldots + \Phi(c_1)\Phi(\alpha) + \Phi(c_0)$$

since Φ preserves addition and multiplication. The c_i are in k, so Φ doesn't change them. Thus, in fact

$$0 = c_n\Phi(\alpha)^n + \ldots + c_1\Phi(\alpha) + c_0$$

That is,

$$0 = P(\Phi(\alpha))$$

So $\Phi(\alpha)$ is a root of $P(x) = 0$. By repeating this, we obtain the assertion of the proposition.

///

Proposition: Let

$$A = \{\alpha_1, \ldots, \alpha_t\}$$

distinct elements of K, with the **Frobenius-stable** property, namely, that for any α in A, $\Phi(\alpha)$ is again in A. Then the polynomial

$$(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_t)$$

(when multiplied out) has coefficients in k.

Proof: For a polynomial

$$P(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_2 x^2 + c_1 x + c_0$$

with coefficients in K, define $\Phi(P)$ by letting Φ act on the coefficients

$$\Phi(P)(x) = \Phi(c_n) x^n + \ldots + \Phi(c_1) x + \Phi(c_0)$$

Since Φ preserves addition and multiplication in K, it preserves addition and multiplication of polynomials

$$\begin{array}{rcl} \Phi(P+Q) & = & \Phi(P) + \Phi(Q) \\ \Phi(P \cdot Q) & = & \Phi(P) \cdot \Phi(Q) \end{array}$$

Applying Φ to the product

$$(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_t)$$

mixes around the factors, since Φ just permutes A. The order in which the factors are multiplied doesn't matter, so

$$\Phi((x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_t))$$

$$= (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_t)$$

Thus, the multiplied-out version

$$(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_t)$$

$$= c_n x^n + c_{n-1}x^{n-1} + \ldots + c_2 x^2 + c_1 x + c_0$$

has the property that

$$c_n x^n + c_{n-1}x^{n-1} + \ldots + c_2 x^2 + c_1 x + c_0$$

$$= \Phi(c_n)x^n + \ldots + \Phi(c_1)x + \Phi(c_0)$$

Equality for polynomials means that corresponding coefficients are equal, so $\Phi(c_i) = c_i$, hence $c_i \in k$, for all indices i. ///

Proposition: Let α be an element of $K = k[x]/Q$. There is exactly one monic irreducible polynomial P in $k[x]$ such that α is a root of $P(x) = 0$, namely

$$P(x) =$$

$$(x - \alpha)(x - \Phi(\alpha))(x - \Phi^2(\alpha)) \ldots (x - \Phi^{d-1}(\alpha))$$

where d is the smallest positive integer so that $\Phi^d(\alpha) = \alpha$.

Proof: Consider successive images $\Phi^i(\alpha)$ of α under Frobenius. Since the field is finite, at some point $\Phi^i(\alpha) = \Phi^j(\alpha)$ for some $0 \leq i < j$. Since Φ is a bijection of K to K, it has an inverse map Φ^{-1}. Applying the inverse i times to $\Phi^i(\alpha) = \Phi^j(\alpha)$,

$$\alpha = \Phi^0(\alpha) = \Phi^{j-i}(\alpha)$$

So $i = 0$. Thus, for the smallest j so that $\Phi^j(\alpha)$ is already $\Phi^j(\alpha) = \Phi^i(\alpha)$ for $1 \leq i < j$, in fact

$$\Phi^j(\alpha) = \alpha$$

Let
$$\alpha,\ \Phi(\alpha),\ \ldots,\ \Phi^{d-1}(\alpha)$$
be the distinct images of α under Frobenius.
Let
$$P(x) =$$
$$(x-\alpha)(x-\Phi(\alpha))(x-\Phi^2(\alpha))\ldots(x-\Phi^{d-1}(\alpha))$$
Application of Φ permutes the factors on the right. When multiplied out, P is unchanged by application of Φ, so has coefficients in k.

If β is a root in K of a polynomial with coefficients in k, then $\Phi(\beta)$ is also a root. So *any* polynomial with coefficients in k of which α is a zero must have factors $x - \Phi^i(\alpha)$ as well, for $1 \leq i < d$. By unique factorization, this is the *unique* such polynomial.

P must be irreducible in $k[x]$, because if it factored in $k[x]$ as $P = P_1 P_2$ then (by unique factorization) α would be a root of either $P_1(x) = 0$ or $P_2(x) = 0$, and all the d distinct elements $\Phi^i(\alpha)$ would be roots of the same equation. Since the number of roots is at most the degree, there cannot be any proper factorization, so P is irreducible. ///

Corollary: Let β be the image of x in $K = \mathbf{F}_q[x]/Q$, and let n be the degree of Q. Then

$$Q(x) =$$

$$(x - \beta)(x - \Phi(\beta))(x - \Phi^2(\beta)) \ldots (x - \Phi^{n-1}(\beta))$$

Also $\Phi^n(\beta) = \beta$, and n is the smallest positive integer such that this is so. ///

Let e denote the identity map of $K = \mathbf{F}_q[x]/Q$ to itself, and

$$G = \{e, \Phi, \Phi^2, \ldots, \Phi^{n-1}\}$$

where Q is of degree n. This is a set of maps of K to itself, and these maps when restricted to $\mathbf{F}_q$ are the identity map on $\mathbf{F}_q$. Since each Φ^i is the identity on $\mathbf{F}_q$ and maps K bijectively to itself, we say that G is a set of **automorphisms** of K over $\mathbf{F}_q$.

Proposition: This set G of automorphisms of K over $\mathbf{F}_q$ is a *group*, with identity e. (The **Galois group** of K over $\mathbf{F}_q$.)

Proof: (Exercise using the defintion of **group**.

Definition: The **stabilizer subgroup** G_α of α in G is

$$G_\alpha = \{g \in G : g(\alpha) = \alpha\}$$

Proposition: For α in K the stabilizer subgroup G_α of α is a subgroup of G.

///

Proposition: Given α in $K = \mathbf{F}_q[x]/Q$, the number of distinct images $\Phi^i(\alpha)$ of α under repeated applications of the Frobenius map is a divisor of the degree n of Q.

Proof: Actually, the collection of images $\Phi^i(\alpha)$ is in bijection with the cosets G/G_α where G_α is the stabilizer subgroup of α in the automorphism G. Indeed, if $g \in G$ and $h \in G_\alpha$, then

$$(gh)(\alpha) = g(h(\alpha)) = g(\alpha)$$

This proves that $gG_\alpha \to g(\alpha)$ is well-defined. And if $g(\alpha) = g'(\alpha)$, then $\alpha = g^{-1}g'(\alpha)$, so $g^{-1}g'$ is in the stabilizer subgroup G_α. So no two distinct cosets gG_α and $g'G_\alpha$ of G_α send α to the same thing. ///

Corollary: For α in the field $K = k[x]/Q$, the degree of the unique monic irreducible polynomial P with coefficients in k so that $P(\alpha) = 0$ is a divisor of the degree n of Q.

Proof: From above,

$$P(x)$$

$$= (x - \alpha)(x - \Phi(\alpha))(x - \Phi^2(\alpha)) \ldots (x - \Phi^{d-1}(\alpha))$$

where α, $\Phi(\alpha)$, $\Phi^2(\alpha)$, ..., $\Phi^{d-1}(\alpha)$ are the distinct images of α and d is the degree of P. From Lagrange's theorem, all cosets of G_α have the same cardinality.

$$\mathrm{card}\,(G) = d \cdot \mathrm{card}\,(G_\alpha)$$

In the special case of the image β of x in K, the stabilizer subgroup is just $\{e\}$, so

$$\mathrm{card}\,(G) = n \cdot 1$$

so $\mathrm{card}\,(G) = n$, and $d|n$. ///

Counting irreducibles

Proposition: Let P be an irreducible monic polynomial of degree d with d dividing the degree n of an irreducible Q. Then $P(x) = 0$ has d distinct roots in $K = k[x]/Q$, and $P(x)$ factors into distinct linear factors in K.

Proof: The quotient ring $L = k[x]/P$ is a field. Let α be the image of x. We know $P(\alpha) = 0$, and

$$P(x) =$$

$$(x - \alpha)(x - \Phi(\alpha))(x - \Phi^2(\alpha)) \ldots (x - \Phi^{d-1}(\alpha))$$

By Lagrange, $\alpha^{q^d-1} = 1$. By unique factorization, $P(x)$ divides $x^{q^d-1} - 1$.

On the other hand, the existence of a primitive root g in K means that $g^{q^n-1} = 1$ but no smaller positive exponent works. Thus, g^1, g^2, g^3, $\ldots$, g^{q^n-1} are distinct. For any t

$$(g^t)^{q^n-1} = (g^{q^n-1})^t = 1^t = 1$$

so these q^n-1 elements are roots of $x^{q^n-1}-1 = 0$. On the other hand, this equation is of degree q^n-1, so has at most q^n-1 roots. We conclude that

$$x^{q^n-1}-1 = (x-g^1)(x-g^2)(x-g^3)\ldots(x-g^{q^n-1})$$

For d dividing n,

$$q^n - 1 = (q^d - 1)(q^{(n-d)} + q^{(n-2d)} + \ldots + q^d + 1)$$

Thus, q^d-1 divides q^n-1, and $x^{q^d-1}-1$ divides $x^{q^n-1} - 1$. As $P(x)$ divides $x^{q^d-1} - 1$, $P(x)$ divides $x^{q^n-1}-1$. Thus, $P(x) = 0$ has d roots in K, since $x^{q^n-1} - 1$ factors into *linear* factors in $K[x]$. ///

Proof: (of theorem) We count elements of K by grouping them in d-tuples of roots of elements of irreducible monic polynomials with coefficients in $k = \mathbf{F}_q$, where d runs over positive divisors of n including 1 and n. Let N_d be the number of irreducible monic polynomials of degree d with coefficients in $k = \mathbf{F}_q$. Then this grouping and counting argument gives

$$q^n = \sum_{d|n} d \cdot N_d$$

Let μ be the Möbius function

$$\mu(n) = \begin{cases} (-1)^t & (t \text{ primes divide } n) \\ & (\text{and } n \text{ square-free}) \\ & \\ 0 & (n \text{ not squarefree}) \end{cases}$$

By **Möbius inversion** (*inclusion-exclusion!*) we obtain the formula

$$n \cdot N_n = \sum_{d|n} \mu(d)\, q^{n/d}$$

which gives the assertion of the theorem.

///