Lecture 8: Finite fields

Rajat Mittal ⋆

IIT Kanpur

We have learnt about groups, rings, integral domains and fields till now. Fields have the maximum required properties and hence many nice theorems can be proved about them. For instance, in previous lectures we saw that the polynomials with coefficients from fields have unique factorization theorem.

One of the important sub case of fields is when they are finite. In this case the fields can be completely characterized up to isomorphism and have lot of applications in computer science. We will cover the characterization and an application in these lecture notes.

1 Characteristic of a field

We have seen how the characteristic of a ring was defined.

Exercise 1. What is the characteristic of a ring?

Since field is a special case of rings, the definition can be applied to fields too. The characteristic of a field F is the minimum $n \in \mathbb{N}$, s.t., $n1 = 0$. Here $n1$ denotes the addition of multiplicative identity n times,

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}.$$

In general, the characteristic might not exist for field (say $\mathbb{R}$). In that case we say that characteristic is zero. For the case of finite field though, the characteristic is always a positive number. Why?

Suppose n is a characteristic of a finite field. If n is composite, say $n = pq$, then $(p1)(q1) = 0$. But F does not have a zero divisor (it is a field) and hence either $p1 = 0$ or $q1 = 0$, establishing contradiction. So we get the theorem,

Theorem 1. *The characteristic of a finite field is always a prime.*

Note 1. $p1 = 0$ implies that $pf = 0$ for all $f \in F$, the proof is given as an exercise.

How does a field with characteristic p looks like? We can look at the additive structure. It turns out that it can be seen as a vector space over $\mathbb{Z}_p$.

Exercise 2. Review the definition of a vector space over a field.

Theorem 2. *A finite field F of characteristic p is a vector space over $\mathbb{Z}_p$. Hence, if there are r basis elements then $|F| = p^r$.*

Proof. Define nf to be $\underbrace{f + f + \cdots + f}_{n \text{ times}}$. From the previous discussion, the only relevant values of n are $\{0, 1, \cdots, p-1\}$.

Let us look at the set generated by $S = \{f_1, f_2, \cdots, f_k\}$. We call it the *span*,

$$span(S) = \{n_1 f_1 + n_2 f_2 + \cdots + n_k f_k : \ n_i \in \{0, 1, \cdots, p-1\} \ \forall i\}.$$

Exercise 3. Show that $span(S)$ is the smallest additive group containing S.

Clearly one set exist for which span is the entire field (the field itself).

⋆ Thanks to the book from Dummit and Foote and the book from Norman Biggs.

Exercise 4. Show that F is a vector space over $\mathbb{Z}_p$.

Say a basis $B = \{b_1, b_2, \cdots, b_r\}$ is the *minimal* set of elements such that $span(B) = F$. We have assumed that B has r elements. Then,

$$span(B) = \{n_1 b_1 + n_2 b_2 + \cdots + n_r b_r : \ n_i \in \{0, 1, \cdots, p-1\} \ \forall i\}.$$

We claim that no two elements of the above set are same. If they are then some element of B can be written as a linear combination of others, violating the minimalness of B. Hence $span(B)$ has no duplicates and it is equal to F. So the cardinality of F is p^r.

□

Note 2. The theorem shows that as an additive group, a field of size p^r, is isomorphic to $(\mathbb{Z}_p)^r$.

By the previous theorem we have proved that every finite field has characteristic some prime p and number of elements are p^r, some power of its characteristic. Hence the number of elements in a finite field can only be a prime power.

Does there exist a finite field for every prime power. Clearly for every p, $\mathbb{Z}_p$ is a field.

1.1 Finite fields of order p^r

To construct fields of cardinality p^r, we use the concept of field extension. Suppose g is an irreducible polynomial in $\mathbb{Z}_p$. Then we know that $\frac{\mathbb{Z}_p[x]}{(g)}$ is a field (from field extensions).

Exercise 5. Show that $\frac{\mathbb{Z}_3[x]}{x^2+1}$ is a field. What is its cardinality? What is the characteristic?

It is clear that in such a field $p1 = 0$. That shows that characteristic of the field is p. The different elements of this field are all the remainder polynomials modulo g. In other words, all the polynomials of degree $deg(g) - 1$ with coefficients from $\mathbb{Z}_p$. So the number of elements in this field are $p^{deg(g)}$.

This shows that to construct a finite field of size p^r, we need to find an irreducible polynomial of degree r. It is known that such an irreducible polynomial always exist. The proof of this statement will not be covered in this class.

So there always exist at least one field of size p^r. It can actually be shown that all such fields of size p^r are isomorphic and we call them $\mathbb{F}_{p^r}$. For $r = 1$, this field is $\mathbb{Z}_p$, we will also call it $\mathbb{F}_p$.

Exercise 6. What is the difference between vector space $\mathbb{Z}_3^2$ and field $\frac{\mathbb{Z}_3[x]}{x^2+1}$?

We won't prove that there exist a unique field of size p^r up to isomorphism. But we will provide a partial justification. We have seen that the additive group of any field of size p^r is isomorphic to $(\mathbb{Z}_p)^r$. In the next section we will show that their multiplicative group is also isomorphic to $\mathbb{Z}_{p^r-1}$ (it is cyclic). So for any two finite fields of same size, their additive groups and multiplicative groups are isomorphic.

Exercise 7. Why is this a partial and not full proof that two fields of the same size are isomorphic?

1.2 Primitive element

We need to show that the multiplicative group of any field is cyclic. That means, there exist an element $f \in F$, s.t., the order of f is $|F| - 1$ (why did we subtract 1?). Such an element generates the whole group $F - \{0\} = \{f^0, f^1, \cdots, f^{|F|-2}\}$.

Definition 1. *Primitive element: An element f of F which generates the multiplicative group of the field F is called the* primitive element *of F.*

To show that any field's multiplicative group is cyclic, we just need to show the existence of a primitive element.

Theorem 3. *For any finite field F, there always exist a primitive element of F.*

Proof. Lets call the multiplicative group $F^* = F - \{0\}$ and $|F^*| = n$. Since F^* has order n, for all elements x of F^*,

$$x^n - 1 = 0$$

So there are exactly n roots of the above equation (why exactly n?).

For any element x, the order d divides n, hence x is a solution of $p(d) = x^d - 1$ for some $d \mid n$. Notice that the polynomial $p(d)$ has at most d roots.

For the sake of contradiction, suppose there are no primitive elements. Then every element has order strictly less than n. We would like to show that there are not enough roots (n) for the polynomial $x^n - 1$.

So we would like to show,

$$\sum_{d<n, d|n} d < n \tag{1}$$

Note 3. There is a strict inequality $d < n$ in the summation index as well as the inequality.

Exercise 8. Show that this is not true for some n.

The reason why the above strategy does not work is that we are counting lot of elements multiple times. A solution of $p(d)$ will be a solution of $p(2d), p(3d), \cdots$. There is a decent chance that some of numbers $2d, 3d, \cdots$ might be divisors of n too.

So say $e(d)$ is the number of elements with order *exactly* d. Hence instead of Eq. 1, the contradiction will be shown by proving the equation,

$$\sum_{d<n, d|n} e(d) < n \tag{2}$$

This equation follows from the following two claims. The proof of first one is left as an exercise, other will be proved here.

Note 4. $\phi(d)$ is number of elements co-prime (gcd 1) to d.

Claim. For a number n, $\sum_{d|n} \phi(d) = n$.

Proof hint: For any number $k \leq n$, look at $gcd(k, n)$ and $\frac{k}{gcd(k,n)}$.

Claim. If there exist an element of order d then $\phi(d) = e(d)$.

Proof. Suppose the element with order d is x. Then the d roots for $x^d - 1$ are precisely $x^0, x^1, \cdots, x^{d-1}$ (these are d roots and there are at most d roots). The order of x^k is $\frac{d}{gcd(d,k)}$.

Exercise 9. Suppose the order of x in a group G is d. Show that for x^k, the order is $\frac{d}{gcd(d,k)}$.

Hence the elements with order d are precisely x^k, s.t., $gcd(d, k) = 1$. So $e(d) = \phi(d)$.

□

Using the claims,

$$n = \sum_{d|n} \phi(d) > \sum_{d|n} e(d).$$

The inequality follows because $e(d) \leq \phi(d)$ and we have assumed $e(n) = 0$. So the equation 2 follows from non-existence of primitive element and hence we get the contradiction.

Note 5. By definition of $e(d)$, $\sum_{d|n} e(d) = n$. Hence there should be equality in the above equation. That means there are exactly $\phi(d)$ elements of order d in a field n where $d \mid n$. Specifically, there are $\phi(n)$ primitive elements for a field F with size $n+1$.

□

Since $\mathbb{Z}_p$ is a field, by previous theorem, $\mathbb{F}_p = \mathbb{Z}_p$ is cyclic as a multiplicative group. This can be generalized to show that even $\mathbb{Z}_{p^k}^\times$ is cyclic.

Exercise 10. Show that $\mathbb{Z}_{p^k}^\times$ is NOT isomorphic to the multiplicative group of $\mathbb{F}_{p^k}$ for $k > 1$.

Theorem 4. *If $n = p^k$ for some power k of an odd prime p then $G = \mathbb{Z}_n^\times$ is cyclic.*

Note 6. This is not true for even prime, we have seen that $\mathbb{Z}_8^\times$ is not cyclic.

Exercise 11. Find out where did we use the fact that p is odd.

Proof. Assume that $t = p^{k-1}(p-1)$, the order of the group G.

We know that $\mathbb{F}_p$ is cyclic and hence have a generator g. We will use g to come up with a generator of G. First notice that,

$$(g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p \neq g^{p-1} \mod p^2.$$

So either $(g+p)^{p-1}$ or g^{p-1} is not $1 \mod p^2$. We can assume the latter case, otherwise replace g by $g+p$ in the argument below.

So $g^{p-1} = 1 + k_1 p$ where $p \nmid k_1$. So using binomial theorem,

$$g^{p(p-1)} = (1 + k_1 p)^p = 1 + k_2 p^2.$$

Where $p \nmid k_2$

Exercise 12. Continuing this process, show that,

$$g^{p^{e-1}(p-1)} = 1 + k_e p^e,$$

with $p \nmid k_e$.

From the previous exercise $g^t = 1 \mod p^k$ but $g^{t/p} \neq 1 \mod p^k$. The only possible order of g then is $p^{k-1}d$ where d is a divisor of $p-1$ (because the order has to divide t, Lagrange's theorem).

If the order is $p^{k-1}d$, then

$$g^{p^{k-1}d} = 1 \mod p^k = 1 \mod p.$$

But $g^p = g \mod p$ (why?). That implies $g^d = 1 \mod p$. Since $p-1$ is the order of g modulo p (g is the generator), implies $d = p-1$. Hence proved.

□

2 Application: The classical part of quantum algorithm for factorization

One of the most important achievements of quantum computing has been to solve factorization in polynomial time. There is no known *efficient* classical algorithm to factorize a number. The problem is easy to state, given a number n, find the factorization of n.

Note 7. An efficient algorithm for factorization runs in time polynomial in $\log n$, since the input size is $\log n$ (the number of bits needed to specify n).

The quantum algorithm works by reducing the problem classically to something known as the *hidden subgroup problem (HSP)*. Shor's factorization algorithm (1994) can be reduced to giving an efficient algorithm to solve HSP on a quantum computer.

The quantum algorithm for HSP is out of scope of this course. But we will present the classical reduction from factorization to HSP, a neat application of many things we learnt in this course.

2.1 Hidden subgroup problem (HSP)

In the hidden subgroup problem, we are given a group G and a function $f : G \to \mathbb{R}$ which *hides* a subgroup H. By hiding a subgroup means that the functions assign the same value to two elements from the same coset and different values to elements from a different coset. The subgroup H is not known and the task is to find this subgroup.

Note 8. For this case, we assume that a black-box is given which computes the value of a function on group elements. In practice, if we can compute the function efficiently then the algorithm for finding hidden subgroup is efficient too.

The interest in this problem is because many problems like order-finding, discrete logarithm can be thought of as HSP's over finite abelian groups. Their is a quantum algorithm for solving HSP over any finite abelian group. If we can solve HSP on non-abelian groups then it can be used to solve important problems like graph isomorphism and shortest vector problem in a lattice.

The problem of order-finding is that given an element g in a group G, find the order of g in G (smallest r, s.t., $g^r = 1$). Lets see how order-finding can be thought of as an example of HSP in $\mathbb{Z}$.

Suppose the order is r (the quantity we need to find). The set of multiples of r form a subgroup of $\mathbb{Z}$ known as $r\mathbb{Z}$. The cosets are the residue classes modulo r. Given an element $x \in \mathbb{Z}$, the function $a^x = a^{x \mod r}$ is constant on cosets and distinct on different cosets.

Exercise 13. Prove the above assertion.

This function can be computed efficiently (repeated squaring) and hence order-finding can be posed as a hidden subgroup problem.

Note 9. Above discussion shows that order-finding is an HSP over an abelian group ($\mathbb{Z}$, which is not finite). The quantum algorithm for finite abelian groups can be modified to handle this case too.

2.2 Factorization to order-finding

In this section we will reduce the factorization of n to order-finding in the group $\mathbb{Z}_n^\times$. Hence, complete the reduction from factorization to hidden subgroup problem.

We will first get rid of the trivial cases, it can be easily checked if the number is even or if $n = m^k$ (take the square root, cubic root etc. up to $\log n$). So it can be assumed that n is a number of type kk' where k and k' are co-prime and odd. We are interested in finding a non-trivial factor of n (not 1 or n). Once found one factor, we can repeat the procedure to find the complete factorization.

Look at the square roots of $1 \mod n$, i.e., b for which $b^2 = 1 \mod n$. Clearly there are two solutions $b = \pm 1 \mod n$. Suppose there exist a $b \neq \pm 1 \mod n$. Then $b^2 - 1$ is divisible by n and $b \pm 1$ is not. So the $gcd(b \pm 1, n)$ will give non-trivial factors of n.

The reduction from factorization to order-finding basically searches for such a b. It can be shown using Chinese remainder theorem that such a b always exists (exercise).

Exercise 14. In the if statement of the algorithm why didn't we check that $b = 1 \mod n$?

The only thing we need to show is that there are enough a's for which $b = a^{r/2} \neq \pm 1 \mod n$ is a square-root of $1 \mod n$.

Note 10. The quantum algorithm is a probabilistic algorithm, hence showing that there are enough "good" a's works.

Theorem 5. *Suppose n is a product of two co-prime numbers $k, k' > 1$. For a randomly chosen a, the probability that a has an even order r and $a^{r/2} \neq -1 \mod n$ is at least $1/4$.*

Check if n is even or of the form $n = m^k$;
Pick an a, s.t., $gcd(a, n) = 1$ (else we have already found a non-trivial factor of n) ;
for $i = 1, \cdots$ **do**
    Find the order of a and call it r (use the quantum algorithm for order-finding) ;
    if *r is odd or* $a^{r/2} = -1 \mod n$ **then**
        Pick another a co-prime to n ;
    else
        Found $b = a^{r/2} \neq \pm 1 \mod n$, square root of 1 ;
        Find the non-trivial factors from $gcd(b \pm 1, n)$;
        Break;
    end
end

Algorithm 1: Algorithm for factorization using order-finding

Proof. This proof is taken from the book Quantum computing and Quantum information by Nielsen and Chuang. We introduce a notation, $pow2(z)$, the highest power of 2 that divides any number z.

First we prove a lemma for a number $q = p^k$, which is a prime power. Say $m = \phi(q) = p^{k-1}(p-1)$ (exercise). By theorem 4, $\mathbb{Z}_q^\times$ is cyclic, say g is the generator (m is the least number, s.t., $g^m = 1 \mod q$).

Suppose $l = pow2(m)$ (m is even and hence $l \geq 1$).

Lemma 1. *Say, we choose a random element from $\mathbb{Z}_q^\times$. With probability $1/2$, the order r satisfies $pow2(r) = l$.*

Proof. We know that g^t has order $\frac{m}{gcd(m,t)}$. Then it can be easily seen that $pow2(r) = l$ iff t is odd. □

Now consider the prime factorization $n = p_1^{i_1} \cdots p_s^{i_s}$. By Chinese remainder theorem,

$$\mathbb{Z}_n^\times \cong \mathbb{Z}_{p_1^{i_1}}^\times \times \cdots \times \mathbb{Z}_{p_s^{i_s}}^\times.$$

So, to randomly chose a, we can pick random $a_1, \cdots, a_s$ from the respective $\mathbb{Z}_{p^i}^\times$'s. Say r_j are the orders of a_j modulo $p_j^{i_j}$.

Claim. Suppose the order r of a is odd or $a^{r/2} = -1 \mod n$. Then $pow2(r_j)$ is same for all j.

Proof. The order is odd iff all r_j's are odd. Otherwise, if $a^{r/2} = -1 \mod p_j^{i_j}$ then none of r_j divide $r/2$ (we use the fact that p_i's are not 2).

All the r_j's divide r but not $r/2$, so $pow2(r_j)$ is the same. □

From lemma 1, with half the probability, The order r_j of a_j will be such that $pow2(r_j) = l_j$ (where $l_j = pow2(p_j^{i_j - 1}(p_j - 1))$). Call the case when $pow2(r_j) = l_j$ as the "first" case and other the "second" case. We know that both cases happen with probability $1/2$.

Notice that l_j's only depend on n. If all l_j are equal, pick a_1's from first case and a_2 from the second case. If they are unequal, say $l_1 \neq l_2$, then pick the a_1, a_2 from the first case. So in either scenario, r_j's can't be all equal. Which implies r is even and $a^{\frac{r}{2}} \neq 1 \mod n$ (by claim). Since we have only fixed at most 2 cases out of s, the probability is at least $1/4$.

□

Hence the reduction from factorization to order finding is complete.

3 Assignment

Exercise 15. Biggs: Prove that the set of all elements of type $\underbrace{1+1+\cdots+1}_{n \text{ times}}$ form a subfield.

Exercise 16. If $p1 = 0$, prove that $pf = 0$ for all $f \in F$.

Exercise 17. Suppose in a field F, $p1 = 0$ for a prime p. Show that the characteristic of that field is p.

Exercise 18. Show that any field of size p is isomorphic to $\mathbb{Z}_p$.

Hint: 0 and 1 should exist in that field. Now construct the obvious isomorphism.

Exercise 19. Find a primitive element in field $\mathbb{F}_{23}$

Exercise 20. Write a program to find if a degree 2 polynomial is irreducible or not in $\mathbb{F}_p$ for a prime p.

Exercise 21. Construct the field $\mathbb{F}_{49}$.

Hint: Look at square roots modulo 7.

Exercise 22. Prove the claim 4.

Hint: Look at any number m less than n as $m = gcd(m, n).m'$.

Exercise 23. Discrete logarithm: Given an element a and a generator g in the group $G = \mathbb{Z}_m^\times$, the discrete log is the problem of finding least l, s.t., $g^l = a$. Show that it can be cast as an HSP.

Hint: Use the function $a^x g^y$ where $x, y \in \mathbb{Z}_{|G|}$.

Exercise 24. Show that for $n = kk'$ where k, k' are co-prime, there exist a square root of $1 \mod n$ which is not $\pm 1 \mod n$.

Exercise 25. If $n = p^k$, show that $\phi(n) = p^{k-1}(p-1)$.