Background required

1 Linear Algebra

The reader should be familiar with the following notions from linear algebra: vector spaces over a field, linear independence, span, basis of a vector space, the lattice of subspaces, linear maps between vector spaces, linear forms, ranks of matrices, determinants, quotient spaces, eigenvalues and eigenspaces.

The following basic theorems will often be directly useful to us.

Theorem 0.1. *Let U_1, U_2 be two finite dimensional subspaces of a vector space V. Then*

$$\dim U_1 + \dim U_2 = \dim(U_1 \cap U_2) + \dim(U_1 + U_2).$$

Theorem 0.2 (Rank-Nullity Theorem)**.** *Let L be a linear map from a vector space V to a vector space W. Then*

$$\dim \ker(L) + \dim \operatorname{im}(L) = \dim V.$$

Theorem 0.3. *Let U be a subspace of an n dimensional vector space V, and let V/U be the quotient space with respect to U. Then* $\dim V/U = n - \dim U$.

Theorem 0.4. *Let A be a square matrix of order n. Then the eigenvalues of A are the solutions of the degree n polynomial equation* $\det(A - \lambda I) = 0$*, where I is the identity matrix.*

Corollary 0.5. *The sum of all eigenvalues of A is equal to the trace of A, that is, the sum of the diagonal entries of A, and the product of all eigenvalues is equal to the determinant of A.*

Theorem 0.6. *Let A be a real symmetric matrix of order n. Then A has n eigenvalues, $\lambda_1 \geq \cdots \geq \lambda_n$, counted with multiplicity. Moreover, there exists an orthonormal basis of $\mathbb{R}^n$, $x_1, \ldots, x_n$, such that x_i is an eigenvector of M with eigenvalue equal to λ_i.*

2 Finite Fields

The reader should be familiar with the notions of groups, rings, ideals, fields, quotient rings, isomorphism of rings/fields and field extensions.

The simplest example of a finite field is $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, that is, the integers modulo p, for a prime number p. The main thing to check is that every element has an inverse, which follows from Euclid's theorem: for any integers a, b with $\mathrm{GCD}(a, b) = 1$, there exist

integers x and y such that $ax + by = 1$. Let F be an arbitrary field which is finite. By the repeated addition of 1, we see that there exists a smallest integer m such that $1 + \cdots + 1$ (m times) is equal to 0 in F. This smallest integer must necessarily be a prime p, since there are no zero divisors in F, and this prime number is known as the characteristic of the finite field F. The set $\{0, s_1, \ldots, s_{p-1}\} \subseteq F$ where s_i is the i-fold sum of 1, is a subfield of F, which is known as the *prime subfield*, and it is isomorphic to $\mathbb{F}_p$.

Theorem 0.7. *For every finite field F, there exists a prime number p and a positive integer n such that $|F| = p^n$.*

Proof. Let p be the characteristic of F, and let n be the dimension of F when seen as a vector space over its prime subfield. The number of elements in an n-dimensional vector space over $\mathbb{F}_p$ is equal to p^n. □

Therefore, every finite field must have order equal to a prime power. In fact, we have the following converse.

Theorem 0.8. *For every prime power q, there exists a unique field of order q (up to isomorphism).*

Proof. Let $q = p^n$ where p is a prime. Any finite field of characteristic p is algebraic over the subfield $\mathbb{F}_p$, since it is finite, and hence contained in the algebraic closure F of $\mathbb{F}_p$. The unique field of order q is then just the set of zeros of the polynomial $x^q - x$ in F. □

This finite field of order $q = p^n$ is denoted by $\mathbb{F}_q$.[1] The proof above is not really constructive. The most concrete way to construct the finite field $\mathbb{F}_q$, and to do computations in it, is to take an irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree n (they always exist), to get the field $\mathbb{F}_q$ as $\mathbb{F}_p[x]/(f(x))$.

We now enumerate some basic properties of $\mathbb{F}_q$ that will be useful to us.

(a) For every $\alpha \in \mathbb{F}_q$ we have $\alpha^q = \alpha$. Moreover, the elements of the prime subfield are precisely the zeros of the polynomial $x^p - x \in \mathbb{F}_q[x]$.

(b) $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$ if and only if m divides n. Moreover, for every divisor m of n, there exists a unique copy of $\mathbb{F}_{p^m}$ in the subfield lattice of $\mathbb{F}_{p^n}$, given by the elements satisfying $\alpha^{p^m} = \alpha$ in $\mathbb{F}_{p^n}$.

(c) The additive group of $\mathbb{F}_q$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^n$. The multiplicative group $\mathbb{F}_q^*$ of $\mathbb{F}_q$, is generated by a single element of order $q - 1$, and therefore it's isomorphic to $\mathbb{Z}/(q-1)\mathbb{Z}$. Any generator of this group is called a primitive element of $\mathbb{F}_q$.

(d) The map $x \mapsto x^p$ is an automorphism of the field $\mathbb{F}_q$. The full automorphism group of $\mathbb{F}_q$ is a cyclic group of order n consisting of the maps $x \mapsto x^{p^i}$, for $i = 1, \ldots, n$.

(e) For q odd, there are precisely $(q-1)/2$ squares (quadratic residues) in $\mathbb{F}_q^*$ and $(q-1)/2$ non-squares. Multiplying $\mathbb{F}_q^*$ by a square fixes these two sets while multiplying by a non-square permutes the two of them. For q even, every element of $\mathbb{F}_q$ is a square since $x \mapsto x^2$ is a field automorphism.

[1] In finite geometry literature it is sometimes denoted by GF(q), where GF stands for *Galois Field*.

Lemma 0.9. *For all $i \in \mathbb{N}$, the sum*

$$\sum_{a \in \mathbb{F}_q} a^i$$

is -1 if i is a multiple of $q-1$ and 0 otherwise.

Proof. Let S be the sum and α be the generator of the group $\mathbb{F}_q^*$. Then

$$S = \sum_{a \in \mathbb{F}_q} a^i = \sum_{a \in \mathbb{F}_q} (\alpha a)^i = \alpha^i \sum_{a \in \mathbb{F}_q} a^i = \alpha^i S.$$

Now, α^i is equal to 1 if and only if i is a multiple of $q-1$, and hence for all $i \notin (q-1)\mathbb{N}$, we must have $S = 0$ for the equality above to hold. When $i \in (q-1)\mathbb{N}$, then since $a^{q-1} = 1$ for all $a \neq 0$, S is the $(q-1)$-fold sum of the identity 1, and hence it's equal to -1. □

Definition 0.10. Let $\mathbb{F}_{q^n}$ be a field extension of $\mathbb{F}_q$. Then the *trace* function, with respect to this extension, is defined as

$$\mathrm{Tr}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{n-1}}.$$

The *norm* function with respect to this extension is defined as

$$\mathrm{Norm}(x) = x x^q \cdots x^{q^{n-1}} = x^{(q^n-1)/(q-1)}.$$

If $\mathbb{F}_q$ is the prime subfield, then these maps are known as *absolute trace* and *absolute norm*, respectively.

Lemma 0.11. Tr *is an additive surjective function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ with $|\mathrm{Tr}^{-1}(a)| = q^{n-1}$ for all $a \in \mathrm{F}_q$.*

Lemma 0.12. Norm *is a multiplicative function from $\mathbb{F}_{q^n}^*$ to $\mathbb{F}_q^*$, with $|\mathrm{Norm}^{-1}(a)| = (q^n-1)/(q-1)$ for all $a \in \mathbb{F}_q^*$.*