Mathematical Techniques for Computer Science - Notes

1 Gaussian Elimination

Gaussian Elimination is a recursive algorithm - it has a base case and a general case:

Base Case There is only one equation and one unknown: $ax = b$. This can be solved as $x = \frac{b}{a}$.

General Case There are n equations and each contains n unknowns. We use the first equation to eliminate the first unknown in the other $n - 1$ equations. Apply the algorithm recursively to these $n - 1$ equations.

This should lead to a staircase pattern of zeros.

$$\begin{pmatrix} \bullet & * & * & * \\ 0 & \bullet & * & * \\ 0 & 0 & \bullet & * \\ 0 & 0 & 0 & \bullet \end{pmatrix}$$

The term for this is **echelon form**.

2 Gaussian Elimination: Special Cases

These are all to do with zeros appearing in the "wrong place".

Contradictory equation If, in the base case $ax = b$, $a = 0$ and $b \neq 0$, then the equation is contradictory since $0 = b$. In this case there is *no solution*.

Irrelevant equation This is like the last case but this time both sides are zero, i.e. the equation reduces to $0 = 0$. This means that the value of x can be **chosen freely**.

Can't use the first equation to eliminate the first unknown If the coefficient of the first unknown in the first equation is zero, then the first variable of the other equations cannot be eliminated.

The solution is to exchange the first equation with another equation where the first coefficient is not zero, and run the algorithm on this rearranged matrix. If the calculation is being done by a human, we would like the coefficient to be as close to 1 as possible.

Can't use any of the equations to eliminate the first unknown Similar to the previous case, this means that the first variable is not constrained at all and can be chosen freely. However, this creates a system where we have *two equations* for *one unknown*. We have to consider more general systems of linear equations.

General Gaussian elimination The General Case stays the same - we only need to reconsider the base case.

Base Case 1 There are multiple equations but only one unknown left. Solve each equation independantly and compare the answers: if all the same, then that is the solution. If they disagree, then the system has no solution.

Base Case 2 There are multiple (say m many) unknowns but only one equation left. In this case $m - 1$ unknowns can be chosen freely and the other one is computed from the equation.

Special cases in Echelon form Suppose after performing Gaussian elimination we end up with this matrix:

$$\begin{pmatrix} 0 & \bullet & * & * & * & * \\ 0 & 0 & 0 & \bullet & * & * \\ 0 & 0 & 0 & 0 & \bullet & * \\ 0 & 0 & 0 & 0 & 0 & ? \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Here the bullets represent non-zero numbers and the asterisks represent arbitrary numbers. If the question mark is non-zero, there is no solution (since we have contradictory equations). If it is zero, then we have infinitely many solutions, since some variables can be chosen freely. The ones that can be chosen freely are the ones where the staircase does not drop down one level (in this case x_1 and x_3). The value of certain other variables will depend on what is chosen for x_1 and x_3.

Fields There are many *number systems* (also known as **fields**) that can take the place of rational (or real) numbers. The requirements of a field are:

- Elements of the field can be added and multiplied.
- There is a "zero" and a "one", which we write as 0 and 1.

Therefore the following two equations must be satisfied:

$$x + 0 = x$$
$$x * 1 = x$$

$$x + y = y + x \qquad x * y = y * x \qquad x * (y + z) = x * y + x * z$$
$$x + (y + z) = (x + y) + z \qquad x * (y * z) = (x * y) * z$$

Finally, the following equations must be able to be solved:

$$a + x = 0$$
$$a * x = 1 \text{ assuming } a \neq 0$$

An example of a finite field A useful **finite field** is $GF(2)$. It has two elements, zero and one. Addition and multiplication is like usual, except that $1 + 1 = 0$.

3 Analytical Geometry in the Plane

Points: Given points P and Q with coordinates $\begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$ and $\begin{pmatrix} q_1 \\ q_2 \end{pmatrix}$, their distance d can be computed using pythagoras:

$$d = \sqrt{(q_1 - p_1)^2 + (q_2 - p_2)^2}$$

Vectors:

- Pair $\begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$ can be a movement of the plane: every point $P = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$ is shifted to $P' = \begin{pmatrix} p_1 + v_1 \\ p_2 + v_2 \end{pmatrix}$
- Uppercase letters are used for points and lowercase with arrows for vectors.
- A vector has length $|\vec{v}| = \sqrt{(v_1)^2 + (v_2)^2}$ which is the distance each point travels under the movement described by $\vec{v}$.
- A Vector of length 1 is a Unit Vector.
- $\vec{0} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ is the null vector.
- $\vec{v}/|\vec{v}|$ is the unit vector pointing in the same direction as $\vec{v}$.
- The vector $\vec{PQ}$ that moves point P into point Q has coordinates (q1-p1, q2-p2).

- All points X that can be reached from P by following some distance along the direction of $\vec{v}$ lie on the straight line $X = P + (s \cdot v)$.
- This is a parametric representation of a line where the parameter is s.
- If given two points P and Q in the plane then this defines a straight line $X = P + (s \cdot PQ)$.
- If given two lines $X = P + (s \cdot v)$ and $Y = Q + (t \cdot w)$ their point of intersection satisfies $p1 + sv1 = q1 + tw1$ and $p2 + sv2 = q2 + tw2$. This can be solved using Gaussian Elimination.

4 Geometry in 3 Dimensions

Planes The parametric representation of a plane has the form $X = P + s \cdot \vec{v} + t \cdot \vec{w}$ where P is a point in space and $\vec{v}$ and $\vec{w}$ are vectors (neither of which are null). $\vec{w}$ must not point in the same (or opposite) direction as $\vec{v}$, otherwise it is just a line.

Three points P, Q and R which are not all on the same line determine a plane $X = P + s \cdot \vec{PQ} + t \cdot \vec{PR}$.

Intersection Tasks

- **Test whether a point lies on a line or plane** For point Q: $X = P + (s \cdot v)$ therefore $P + (s \cdot v) = Q$.
- **Find the intersection point between lines/planes** Simply set the two equations as equal to each other.

Solve using Gaussian Elimination.

Two-point description of a line Two points P and Q determine a line

$$X = P + s \cdot \vec{PQ}$$

This can be rewritten as

$$\begin{aligned} X &= P + s \cdot (Q - P) \\ &= P + s \cdot Q - s \cdot P \\ &= (1 - s) \cdot P + s \cdot Q \end{aligned}$$

This can also be done with a plane using 3 points.

Vector spaces So we have a null vector, we can add two vectors, and we can multiply vectors with a scalar. Any structure that satisfies the laws of vector algebra and carries these two operations is called a **vector space**.

The idea of a vector space is more complex than just 3-dimensional movements. Scalars can come from any field $\mathbb{F}$, for example $GF(2)$. One then speaks of a "vector space over $\mathbb{F}$".

Subspaces If $\vec{v}$ is an element of some vector space then we can generate a **subspace** (a **sub-vector space**) by considering all vectors of the form $s \cdot \vec{v}$. Another subspace would be all expressions of the form $s \cdot \vec{v} + t \cdot \vec{w}$.

Another way of looking at parametric representations is that we pick a point and allow all movements from a subspace to act on this point. This leads to an **affine subspace**. In other words, lines and planes are affine subspaces of 2D/3D.

Bases If two generators point in the same direction then one of them is redundant and can be removed. A set of generators that includes a redundant generator is said to be **linearly dependent**. A set of generators that can not be made any smaller is a **basis** of the subspace. The number of elements of a basis is the **dimension** of the subspace.

If we start with some set of generators and we are not sure if any of them are redundant, we can write the vectors as rows into a matrix and run Gaussian elimination. The rows of the resulting echelon form will be a basis for the subspace. Any redundancy will show itself as rows consisting entirely of zeros.

Codes Subspaces in $GF(2)^n$ are used as linear **codes** in coding theory. This is coding to spot and correct errors in data, not programming or cryptography.

5 Vector Form

A line from a linear equation The linear equation

$$x_1 - 2x_2 = 3$$

has the solutions

$$\begin{array}{lcl} x_2 & : & \text{choose freely} \\ x_1 & = & 3 + 2x_2 \end{array}$$

This can be written in vector form as:

$$X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 3 + 2x_2 \\ x_2 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \end{pmatrix} + x_2 \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

and we see that all solutions lie on a line.

Intersection tasks ...become a lot easier when using vector form. For example, intersecting a line with a plane:

$$\begin{array}{rl} \text{line:} & X = \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} + s \cdot \begin{pmatrix} 1 \\ 0 \\ -3 \end{pmatrix} \\ \text{plane:} & x_1 - 2x_2 + 3x_3 = 5 \end{array}$$

To solve just substitute the line into the equation of the plane.

$$[2 + s] - 2[1] + 3[1 - 3s] = 5$$

It is much simpler to solve because a parametric representation *generates points* whilst an equation *tests points.*

Translating from parametric to equational

Lines If we are given the parametric representation of a line in 2D

$$X = P + s \cdot \vec{v} = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} + s \cdot \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$$

and we are looking for an equation

$$ax_1 + bx_2 = d$$

then we just need to set

$$\begin{array}{lcl} a & = & -v_2 \\ b & = & v_1 \\ d & = & ap_1 + bp_2 \end{array}$$

Planes If we are given the parametric representation of a plane in 3D

$$X = P + s \cdot \vec{v} + t \cdot \vec{w} = \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} + s \cdot \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} + t \cdot \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix}$$

and we are looking for an equation

$$ax_1 + bx_2 + cx_3 = d$$

then we just need to set

$$\begin{array}{lcl} a & = & v_2w_3 - v_3w_2 \\ b & = & v_3w_1 - v_1w_3 \\ c & = & v_1w_2 - v_2w_1 \\ d & = & ap_1 + bp_2 + cp \end{array}$$

6 The Inner Product

Geometric interpretations Given a linear equation

$$ax_1 + bx_2 + cx_3 = d$$

we assemble the coefficients in a vector

$$\vec{n} = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$$

This vector is orthogonal to the plane. This is called the **normal** to the plane.
The right-hand side d of the equation is negative if the origin is on the same side of the plane as the normal, and positive otherwise. The distance of the origin from the plane is given by

$$\text{distance} = \frac{d}{|\vec{n}|}$$

where $|\vec{n}| = \sqrt{a^2 + b^2 + c^2}$. Since the normal can easily be computed from equations of the form $ax_1 + bx_2 + cx_3 = d$, this is called the *normal form*.

Inner Product The expression $ax_1 + bx_2 + cx_3$ can be viewed as the **inner product** of two tuples $\vec{n} = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$ and $X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$. This is denoted by $\langle \vec{n}, X \rangle$. It is also known as the **dot product** $(\vec{n} \cdot X)$.
The following laws apply:

$$\begin{aligned} \langle \vec{v}, \vec{w} \rangle &= \langle \vec{w}, \vec{v} \rangle \\ \langle \vec{v} + \vec{w}, \vec{x} \rangle &= \langle \vec{v}, \vec{x} \rangle + \langle \vec{w}, \vec{x} \rangle \\ \langle s \cdot \vec{v}, \vec{w} \rangle &= s \times \langle \vec{v}, \vec{w} \rangle \end{aligned}$$

If you know the normal to a plane and a point P on it, the normal form can be written as

$$\langle \vec{n}, X \rangle = \langle \vec{n}, P \rangle$$

Geometric properties

Orthognality Two vectors $\vec{v}$ and $\vec{w}$ are perpendicular if $\langle \vec{v}, \vec{w} \rangle = 0$.

Angles $\langle \vec{v}, \vec{w} \rangle = |\vec{v}| \times |\vec{w}| \times cos(\alpha)$ where α is the angle between $\vec{v}$ and $\vec{w}$. $\langle \vec{v}, \vec{w} \rangle$ is positive if the angle is acute and negative if the angle is obtuse.

Length $|\vec{v}|^2 = \langle \vec{v}, \vec{v} \rangle$

Projection We can compute the **orthogonal projection** of $\vec{v}$ onto the line defined by $\vec{w}$ by computing

$$\frac{\langle \vec{v}, \vec{w} \rangle}{\langle \vec{w}, \vec{w} \rangle} \cdot \vec{w}$$

which is the same as

$$\left\langle \vec{v}, \frac{\vec{w}}{|\vec{w}|} \right\rangle \cdot \frac{\vec{w}}{|\vec{w}|}$$

Graphics-related tasks

Computing the distance from a plane If E is a plane $\langle \vec{n}, X \rangle = d$ and Q is a point then the distance Q to E (measured in the direction of the normal) is given by

$$\frac{d - \langle \vec{n}, Q \rangle}{|\vec{n}|} = \frac{\langle \vec{n}, P \rangle - \langle \vec{n}, Q \rangle}{|\vec{n}|}$$

If this returns 0 then Q is a point in the plane. If the result is negative then the normal is pointing towards the side that Q is on.

Nearest neighbour To find which point on E is closest to Q we move from Q to E in the direction of the normal.

$$Q' = Q + \frac{d - \langle \vec{n}, Q \rangle}{\langle \vec{n}, \vec{n} \rangle} \cdot \vec{n}$$

If the plane goes through the origin then $d = 0$ and the formula simplifies to $Q' = Q - \frac{\langle \vec{n}, Q \rangle}{\langle \vec{n}, \vec{n} \rangle} \cdot \vec{n}$.

Reflecting a point at a plane Similar to the previous task, but we go twice the distance.

$$Q' = Q + 2 \times \frac{d - \langle \vec{n}, Q \rangle}{\langle \vec{n}, \vec{n} \rangle} \cdot \vec{n}$$

Reflecting a line at a plane Pick two different points on the line and reflect them according to the previous formula. Then plug them into the parametric formula given in section 4.

Higher dimensions To represent a "normal form" for a line in 3D, we use two equations. The line of interest is the intersection of the two planes given by those equations. More generally, to represent an m-dimensional object in d-dimensional space, we can either use a parametric representation with m non-redundant variables, or an equational representation with $d - m$ equations. Translating from one representation to the other is done through our old friend guassian elimination.

Normal forms and finite fields We can represent subspaces in parametric form or equational form regardless of the underlying field.

One application of this is *error-correcting codes*. We use a parametric representation to generate code words from data vectors, then use the equational representation to check whether a word recieved is valid. In this case the parametric form is called the *generator matrix* and the equational form the *check matrix*.

In order to use the notion of "distance", a field needs the following properties:

$$\begin{array}{rcl} \langle \vec{v}, \vec{v} \rangle & \geq & 0 \\ \langle \vec{v}, \vec{v} \rangle = 0 & \implies & \vec{v} = \vec{0} \end{array}$$

Notice that the second property does not hold on GF(2).

$$\left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\rangle = 1 \times 1 + 1 \times 1 = 1 + 1 = 0$$

Therefore there is no notion of distance in GF(2).

7 Matrices

Uses of matrices A matrix is a rectangular arrangement of numbers. The **dimension** of a matrix gives the number of rows and columns. For example, the dimension of a matrix with 2 rows and 3 columns is 2×3. (This is not an equation - the dimension is not 6).

Any number ≥ 1 is allowed for the number of rows and columns in a matrix. A 1×1 matrix is just a number, a 1×3 matrix is just a vector, and a 3×1 matrix is just a vector written as a column. A matrix is **square** if the number of rows equals the number of columns.

A **stochastic matrix** is a square matrix where the values in each column add up to 1. These can describe the behaviour of a **Markov chain**, a system that changes state probabilistically. Matrices can also describe linear transformations (see Graphics module).

Notation Matrices are denoted by capital letters (A, B etc.), while entries in a matrix are denoted a_{ij}, where i is the row number and j is the column number. Unlike most programming languages, indexing starts at 1.

Vector space operations Matrices are compared *componentwise*. This means that two matrices are equal only if they agree in their dimensions and in each position. Scalar multiplication (multiplying a matrix by a number) is done in the same way as on vectors.

Laws for matrix operations

Matrix multiplication The result of multiplying an $m \times n$ matrix A with an $n \times p$ matrix B is an $m \times p$ matrix C whose entry c_{ik} in row i and column k is computed as

$$c_{ik} = \sum nj = 1 a_{ij} b_{jk} = a_{i1} \times b_{1k} + a_{i2} \times b_{2k} + ... + a_{in} \times b_{nk}$$

In words, to compute the entry of matrix C in row i and column k, compute the inner product of the ith row of A with the kth column of B. Clearly the width of the first matrix must equal the height of the second matrix if we want to multiply the two. It follows that multiplication of matrices is (usually) not commutative.

$$AB \neq BA$$

The Identity matrix Every dimension $n \times n$ has its own version of the **identity matrix**. The 3×3 matrix looks like this:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

The laws of matrix multiplication

$$\begin{aligned} (AB)C &= A(BC) \\ A(B+C) &= AB + AC \\ (A+B)C &= AC + BC \\ AE &= EA = A \\ A0 &= 0A = 0 \\ s \cdot (AB) &= (s \cdot A)B = A(s \cdot B) \end{aligned}$$

8 Invertibility of Matrices

For every matrix A there is almost always an inverse matrix A^{-1}. This matrix satisfies $A^{-1}A = E$ and $AA^{-1} = E$.
To compute the inverse of matrix A we just use Guassian elimination to solve the equation $AA^{-1} = E$. Some matrices cannot be inverted (for example the zero matrix).
For 2×2 matrices there is a simple formula for the inverse matrix.

$$\text{If } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ then } A^{-1} = \frac{1}{ad - bc} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

9 Sets

A set is a collection of things. These "things" can be people, colours, or PDF lecture notes. They are known as **elements** or **members**. There is usually a shared attribute involved.

Rules of Sets

- The elements of a set must be identifiable and distinguishable from each other. "Dust in my room" is not a set.
- There must be a clear criteria that distinguishes "things in the set" from "things not in the set".
- A member of a set is counted only once.
- The elements of a set are not ordered.
- A set is defined by which members it has and nothing else.

Notation $x \in A$ indicates that x is an element of A. Sets can also be written explicitly, e.g. {1, 2, 3, 4, 5} or {1, 4, 9, 16, 25, ...}.

New sets from old

Pairing The elements of the set $A \times B$ are pairs (x, y) where x is an element of A and y is an element of B. If both sets are equal ($A \times A$) we can call this A^2.

Finite sequences A^* is the set whose elements are finite sequences of elements of A. For example, if set A is an alphabet, then A^* contains the words you can make with the elements of A. Σ (capital sigma) is often used to denote alphabets. A^* also contains the *empty sequence*, often denoted by ϵ (epsilon).

Subsets If we have a set A then we can create a set B that consists of some elements from A. We can call this a **subset** of A. B is a subset of A only if all of the elements in B can be found in A.

Subset notation:

$$B = \{x \in A \mid x \text{ satisfies condition } c\}$$

"B is the set of all elements of A for which condition c is true."

To indicate that one set is a subset of another, we use the symbol $\subseteq$.

$$B \subseteq A$$

Whatever the set A is, we can always form two standard subsets:

$$\{x \in A \mid true\}$$
$$\{x \in A \mid false\}$$

The first is equal to A, and the second is the **empty set** ($\emptyset$ or $\{\}$).

Set definitions:

$$B \subseteq A \text{ iff (if and only if) } \forall x.\, x \in B \implies x \in A$$
$$A = B \text{ iff } A \subseteq B \text{ and } B \subseteq A$$

Operations on subsets Suppose B, B_1 and B_2 are subsets of a set A.

Union The union of B_1 and B_2 is the combination of all elements from both sets. If an element is in both sets, it still only appears in the union once.

$$B_1 \cup B_2 = \{x \in A \mid x \in B_1 \text{ or } x \in B_2\}$$

Intersection The intersection of B_1 and B_2 is the set of elements that are in both B_1 and B_2.

$$B_1 \cap B_2 = \{x \in A \mid x \in B_1 \text{ and } x \in B_2\}$$

Complement The complement of B is the set of elements that are in A but *not* in B.

$$\overline{B} = \{x \in A \mid x \notin B\}$$

Difference The difference of B_1 and B_2 is the set of elements that are in B_1 but not in B_2. (Note this is not the same as the *compliment* since that compares a set to the alphabet)

$$B_1 \backslash B_2 = B_1 \cup \overline{B_2} = \{x \in A \mid x \in B_1 \text{ but } x \notin B_2$$

Power sets The power set of A ($\mathscr{P}A$) is the set of all sets that are subsets of A.

10 Cardinalty: Countable and Uncountable sets

Counting the elements of a set The number of elements in a set is called the **Cardinality**. If set A has four elements we can write this as

$$|A| = 4 \quad \text{or} \quad \text{card}(A) = 4$$

Cardinality of infinite sets Since the sets $\mathbb{N}$ (natural numbers), $\mathbb{Z}$ (integers), $\mathbb{Q}$ (rational numbers) and $\mathbb{R}$ (real numbers) are infinite, therefore it appears that their cardinality is "infinity." However, this is not correct.

First consider the set of natural numbers $\mathbb{N}$. We call a set **countable** or **countably infinite** if it has the same cardinality as $\mathbb{N}$. We can prove that $\mathbb{Z}$ is countable by pairing each number in $\mathbb{Z}$ to a number in $\mathbb{N}$. For example:

$$(\mathbb{N}, \mathbb{Z}) = \{(0,0), (1,1), (2,-1), (3,2), (4,-2), ...\}$$

We can also prove that $\mathbb{N}^2$ is countable:

$$(\mathbb{N}, \mathbb{N}^2) = \{(0,(0,0)), (1,(1,0)), (2,(0,1)), (3,(2,0)), (4,(1,1)), (5,(0,2)), ...\}$$

If Σ is a finite alphabet, then the infinite set of words Σ^* is countable (imagine walking breadth-first through a tree and pairing $\mathbb{N}$ with the values in the tree). The set of valid Java programs is therefore also countable.

The set of real numbers is uncountable. Therefore there must exist non-computable real numbers.

Powersets again The powerset of $\mathbb{N}$ is uncountable. A powerset always has more elements than the set itself. Therefore, the sets in the sequence

$$\mathbb{N} \quad \mathscr{P}\mathbb{N} \quad \mathscr{P}\mathscr{P}\mathbb{N} \quad \mathscr{P}\mathscr{P}\mathscr{P}\mathbb{N}$$

have greater and greater cardinality. It's infinitely infinite!