Mathematical Techniques for Computer Science - Notes

Harvey Hyatt

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:

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

All the usual rules of arithmetic must be valid:

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

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

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