THINGS TO KNOW BEFORE GOING INTO DISCRETE MATHEMATICS

1 The distributive law

The distributive law is this:

$$a(b + c) = ab + ac$$

This can be generalized to any number of terms between parenthesis; for instance:

$$a(b + c + d) = ab + ac + ad$$

$$(a + b)(c + d) = ac + ad + bc + bd$$

and one of the familiar consequences is this:

$$(a + b)(a - b) = a^2 - ab + ba - b^2 = a^2 - b^2$$

The distributive law is very useful in making certain calculations easy. Consider for instance the multiplication table:

	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	12	14	16	18	20
3	3	6	9	12	15	18	21	24	27	30
4	4	8	12	16	20	24	28	32	36	40
5	5	10	15	20	25	30	35	40	45	50
6	6	12	18	24	30	36	42	48	54	60
7	7	14	21	28	35	42	49	56	63	70
8	8	16	24	32	40	48	56	64	72	80
9	9	18	27	36	45	54	63	72	81	90
10	10	20	30	40	50	60	70	80	90	100

and let's say we want to add all the 100 entries in that table. One way is to explicitly add them up. However, using the distributive law, we can observe that

$$(1 + 2 + 3 + \ldots + 10)(1 + 2 + 3 + \ldots + 10)$$

covers every product in the above table. As described in the section on arithmetic series, this is $[10(10 + 1)/2]^2$.

2 Intervals

Consider the sequence

$$2, 5, 8, 11, \ldots, 35$$

How many elements are in that sequence? We will explore two ways to find out the answer to this question in general.

Counting steps

One way is to count the number of steps. Going from one number to the next is one step. In the example above, the step size is $s = 3$ (observe that the step size can also be negative if the sequence is decreasing). The number of steps can be obtained by

$$\frac{last - first}{s} = \frac{\max - \min}{|s|}$$

where $|s|$ is called the absolute value of s:

$$|s| = \begin{cases} s & s \geq 0 \\ -s & s < 0 \end{cases}$$

Therefore, we have $(35-2)/3 = 11$ steps. The number of elements is **always** one plus the number of steps. So we have 12 elements.

In general, if our sequence looks like:

$$a, a+s, a+2s, \ldots, a+(n-1)s = b$$

then we have $n-1$ steps and $n = (b-a)/s + 1$ elements. A special case is when $s = 1$, then the number of elements is $n = b - a + 1$ (a typical mistake here is to say $n = b - a$).

Mapping

Given the sequence

$$a, a+s, a+2s, \ldots, b$$

find a function $f(x)$ that maps the sequence to consecutive numbers starting with 1. For instance,

$$y = f(x) = \frac{x-a}{s} + 1$$

We can verify $f(a) = 1, f(a+s) = 2, f(a+2s) = 3, \ldots$. Therefore, the number of elements must be $f(b)$.

In general, a sequence like the above has: the first element a, the last element b, the step size s, and the number of elements n. Given any three, one should be able to determine the fourth.

3 Arithmetic series

Let's say we are interested in the sum:

$$2 + 5 + 8 + 11 + \ldots + 35$$

and in general:

$$a + (a+s) + (a+2s) + \ldots + b$$

We will explore three methods for finding this sum.

Gauss

Consider the sum, and the same sum in reverse:

$$\begin{array}{ccccc} a & a+s & a+2s & \ldots & b \\ b & b-s & b-2s & \ldots & a \end{array}$$

Adding the two rows one column at a time we get $(a+b)n$, where n is the number of elements, which we now know is $(b-a)/s+1$. Now that's twice the sum we need, so we must divide by 2, we get:

$$\frac{(a+b)[(b-a)/s+1]}{2}$$

A special case is when $a = s = 1$, we get $1+2+3+\ldots+b = b(b+1)/2$, which also counts the number of pairs we can make using $b+1$ things.

Mapping

We saw before that we can map the sequence to $1, 2, 3, \ldots$ using the function:

$$y = f(x) = \frac{x-a}{s} + 1$$

Therefore, $x = sy+(a-s)$ and each element y of $1, 2, 3, \ldots$, maps to one element x of $a, a+s, a+2s, \ldots$. Since we know $1+2+3+\ldots+n = n(n+1)/2$, the sum $a+(a+s)+(a+2s)+\ldots+b = sn(n+1)/2+n(a-s)$, where n is the number of elements.

Rewriting

We can rewrite the sum as:

$$\underbrace{a+a+\ldots+a}_{n \text{ times}}+s+2s+\ldots+(n-1)s$$

where n is the number of elements. Using the distributive law, this is:

$$\underbrace{a+a+\ldots+a}_{n \text{ times}}+s[1+2+\ldots+(n-1)]$$

which is equal to $na+sn(n-1)/2$.

4 Powers

We will consider integer powers for now. We define x^a, where a is an integer, the product $\underbrace{x \cdot x \cdot \ldots \cdot x}_{a \text{ times}}$. Using this definition, we can easily observe that

$$x^a x^b = x^{a+b}$$

$$(x^a)^b = x^{ab}, \text{ note this is different from } x^{a^b}$$
$$x^a x^0 = x^{a+0} = x^a \Rightarrow x^0 = 1 \text{ (the empty product is 1)}$$
$$x^a x^{-b} = x^{a+(-b)} = x^{a-b} = \frac{x^a}{x^b} \Rightarrow x^{-b} = \frac{1}{x^b}$$
$$x^a x^{-a} = x^0 = 1 \Rightarrow x^{-a} = \frac{1}{x^a} \text{ is the } \textbf{inverse} \text{ of } x^a$$

From the above, we can also conclude properties of fractional powers; for instance $x = x^1 = (x^{0.5})^2$, so $x^{0.5} = \sqrt{x}$.

5 Geometric series

Consider the following sum when $x \neq 1$

$$S = x^0 + x^1 + x^2 + \ldots + x^n$$

We can evaluate this sum using a *shifting* trick and the property that powers add up.

First, consider $xS = x(x^0 + x^1 + x^2 + \ldots + x^n)$. By the distributive law this is $x \cdot x^0 + x \cdot x^1 + x \cdot x^2 + \ldots + x \cdot x^n$. Second, add up the powers, we get

$$xS = x^1 + x^2 + x^3 + \ldots + x^{n+1}$$

Finally, observe that xS is a *shifted* version of S, and

$$xS = S - x^0 + x^{n+1}$$

Solving for S when $x \neq 1$ (because we can't divide by 0) gives:

$$S = \frac{x^{n+1} - 1}{x - 1}$$

A familiar result is to consider the limit when n goes to infinity and $|x| < 1$, then x^{n+1} goes to 0, and we get

$$x^0 + x^1 + x^2 + x^3 + \ldots = \frac{-1}{x-1} = -\frac{1}{x-1} = \frac{1}{1-x}$$

A typical scenario is when $x = 1/a$, where $|a| > 1$, we get $1/(1-1/a) = a/(a-1)$.

6 Sum and product notations

Assume a and b are two integers.

$$\sum_{i=a}^{b} f(i) = f(a) + f(a+1) + f(a+2) + \ldots + f(b)$$

If $b < a$, the above is assumed to be 0 (empty sum is always 0)

$$\prod_{i=a}^{b} f(i) = f(a) \cdot f(a+1) \cdot f(a+2) \cdot \ldots \cdot f(b)$$

If $b < a$, the above is assumed to be 1 (empty product is always 1).

So an arithmetic series with n numbers can be expressed as:

$$\sum_{i=0}^{n-1} (a + is) = a + (a+s) + \ldots + [a + (n-1)s]$$

We can often play with the bounds; for instance, the same sum above can be written as:

$$\sum_{i=1}^{n} [a + (i-1)s]$$

Observe also that the sum can be manipulated as follows:

$$\sum_{i=0}^{n-1} (a + is) = \sum_{i=0}^{n-1} a + \sum_{i=0}^{n-1} is = na + s\sum_{i=0}^{n-1} i = na + sn(n-1)/2$$

Similarly, a geometric series with n numbers can be expressed as:

$$\sum_{i=0}^{n-1} x^i = 1 + x + x^2 + \ldots + x^{n-1}$$

7 Quadratic equation

To solution of $ax^2 + bx + c = 0$ is given by

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

A simplified version of this is when we are given $x^2 - Sx + P = 0$ and we can easily find two integers a and b such that $a + b = S$ and $ab = P$. Then the solution is given by $x = \{a, b\}$.

proof: $(x-a)(x-b) = x^2 - ax - bx + ab = x^2 - (a+b)x + ab = x^2 - Sx + P = 0$. It is obvious that only $x = a$ and $x = b$ make this product 0 (one of the factors must be 0).

8 Falling powers and factorials

We define the a^{th} falling power of x, where $a \geq 0$ is an integer, as:

$$x^{\underline{a}} = \underbrace{x(x-1)(x-2)\ldots(x-a+1)}_{a \text{ terms}}$$

(verify that $[(x-a+1)-x]/(-1)+1=a$ is the number of terms as seen in the section on intervals). Since $x^{\underline{0}}$ is an empty product, it's 1. Observe also that $x^{\underline{a}}=0$ if $a \geq x+1$ and x is a non-negative integer (because at some point we hit 0). Falling powers preserve some properties of calculus in the discrete setting. For instance, let $f(x)=x^{\underline{a}}$, and let's find $\Delta f(x)=f(x+1)-f(x)$.

$$\Delta f(x)=f(x+1)-f(x)=(x+1)^{\underline{a}}-x^{\underline{a}}$$

$$=\underbrace{(x+1)x(x-1)\ldots(x-a+2)}_{a \text{ terms}}-\underbrace{x(x-1)(x-2)\ldots(x-a+2)(x-a+1)}_{a \text{ terms}}$$

$$=\underbrace{x(x-1)\ldots(x-a+2)}_{a-1 \text{ terms}}[(x+1)-(x-a+1)]$$

$$=ax^{\underline{a-1}}$$

Compare this to the case when $f(x)=x^a$ and $\frac{d}{dx}f(x)=ax^{a-1}$ in the continuous setting.

Falling powers can also be expressed in terms of factorials when x is a non-negative integer. The factorial of x is given by $x! = x(x-1)(x-2)\ldots 2\cdot 1$, which can also be written as

$$\prod_{i=1}^{x} i$$

This means 0!=1 (empty product). From this definition of factorials, we conclude that (when $x \geq a$)

$$x^{\underline{a}}=\frac{x!}{(x-a)!}$$

This is how we typically represent the number of permutations.

9 Floors and ceilings

The floor of x, denoted $\lfloor x \rfloor$ is the largest integer that is less or equal to x. Similarly, the ceiling of x, denoted by $\lceil x \rceil$, is the smallest integer that is greater or equal to x.

Therefore, when x is an integer, $\lfloor x \rfloor = \lceil x \rceil = x$; otherwise, $\lfloor x \rfloor$ rounds down to the nearest integer, and $\lceil x \rceil$ rounds up to the nearest integer. It is not hard to see that:

$$\lfloor x \rfloor \leq x \leq \lceil x \rceil$$

$$\lfloor x \rfloor > x-1$$

$$\lceil x \rceil < x+1$$

Here's a nice challenge: can you replace $\lfloor x \rfloor$ by an expression that only uses $\lceil\ \rceil$, and vice-versa?

10 Logarithms and exponentials

If $b^x = a$, then $\log_b a = x$, where $b > 1$ is the base of the logarithm, and $a \geq 0$. For instance, $2^4 = 16$, then $\log_2 16 = 4$. From the definition of logarithm, $\log_b b = 1$, $\log 1 = 0$ for any base, and $b^{\log_b a} = a$.

As an application of this concept, assume we start with some number n, and then divide it by b repeatedly, until we reach a number ≤ 1,

$$n, \frac{n}{b}, \frac{n}{b^2}, \frac{n}{b^3}, \ldots, \frac{n}{b^{\lceil \log_b n \rceil}}$$

then the number of terms is $1 + \lceil \log_b n \rceil$. Use your knowledge about geometric series to find that the sum of these terms is $n[b - (1/b)^{\lceil \log_b n \rceil}]/(b-1)$.

The natural logarithm is

$$\ln a = \int_1^a \frac{1}{x} dx$$

The base of the natural logarithm is $e = 2.71828\ldots$, which satisfies

$$\ln e = \int_1^e \frac{1}{x} dx = 1$$

The base of the natural logarithm, e, can also be found in:

$$e^x = \lim_{n \to \infty} (1 + \frac{x}{n})^n$$

and

$$e^x = \frac{x^0}{0!} + \frac{x^1}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} \cdots$$

It is also known that

$$e^x \geq x + 1$$

for all x (with equality when $x = 0$), which means $x \geq \ln(x+1)$ when $x + 1 \geq 0$.

The logarithm is useful in transforming products into sums:

$$\log(ab) = \log a + \log b$$

$$\log(a/b) = \log a - \log b$$

$$\log(a^b) = b \log a$$

11 Sets

A set is a collection of elements (not ordered in any particular way). In set notation, we list the elements between two braces separated by commas, e.g.

$$S = \{a, b, c\}$$

When the set is finite, we denote by $|S|$ the *cardinality* of the set S, which is the number of elements in it (don't confuse this notation with the absolute value when applied to numbers). For the above example, $|S| = 3$. The empty set is denoted by ϕ, $|\phi| = 0$.

$$\phi = \{\ \}$$

Sets can be infinite, for instance:

$$\mathbb{N} = \{1, 2, 3, \ldots\} \text{ (the set of natural numbers, the positive integers)}$$

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} \text{ (the set of all integers)}$$

The symbol $\in$ means that an element belongs to a set; for instance, $1 \in \mathbb{N}$, but $0 \notin \mathbb{N}$. The symbol $\subset$ means that a set is a subset of another, i.e. every element of the first is an element of the second; for instance, $\mathbb{N} \subset \mathbb{Z}$, but $\mathbb{Z} \not\subset \mathbb{N}$. A set is always a subset of itself. The empty set is a subset of every set.

Sometimes it is useful to describe set implicitly. For instance, the set of all even integers can be expressed in the following way:

$$\mathbb{E} = \{x = 2k \mid k \in \mathbb{Z}\}$$

which means that E contains every integer that can be expressed as two times a number k, where k is in $\mathbb{Z}$. So $\mathbb{E} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$. Here's another example:

$$\mathbb{Q} = \{x = \frac{a}{b} \mid a \in \mathbb{Z} \text{ and } b \in \mathbb{N}\} \text{ (the set of rational numbers)}$$

which represents the set of all numbers that can be written as a ratio of two integers. The set $\mathbb{R}$ is the set of all real numbers, $\mathbb{Q} \subset \mathbb{R}$.

The intersection of two sets, denoted by $\cap$, and the union of two sets, denoted by $\cup$, are defined as follows:

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

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

The product of two sets is:

$$A \times B = \{(x, y) \mid x \in A \text{ and } y \in B\}$$

For instance, if $S = \{a, b, c\}$ and $T = \{1, 2\}$, then

$$S \times T = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$$

While $A \cap B = B \cap A$ and $A \cup B = B \cup A$, in general $A \times B \neq B \times A$. If A and B are finite, then $|A \times B| = |B \times A| = |A| \times |B|$. The sizes of the intersection and union can be tricky, in general:

$$|A \cup B| = |A| + |B| - |A \cap B|$$