Course Notes for Math 162: Mathematical Statistics
Approximation Methods in Statistics

Adam Merberg and Steven J. Miller

August 18, 2006

Abstract

We introduce some of the approximation methods commonly used in mathematical statistics. We first consider Taylor series expansion. We then look at Stirling's Formula, which provides an approximation for $n!$. As an application we show how to apply these techniques to estimate the solution to the Birthday Problem. In the appendices we review the Intermediate and Mean Value Theorems, factorials, the Gamma function and proofs by induction.

Contents

1 Introduction

Often when studying statistics, we find that we must work with expressions which are too unwieldy to consider exactly. For example, we often need to look at factorials, which are often contributed by binomial coefficients. Sometimes we have the good fortune of being able to cancel one factorial with another. Often, however, we will have no way to simplify exactly an expression involving a factorial. In order to draw meaningful conclusions, we must therefore rely on approximations, which will typically be valid for large sample sizes.

Stirling's Formula provides an approximation for $n!$. Before introducing Stirling's Formula, we will look at Taylor series, an approximation method used in justifying Stirling's Formula and elsewhere.

2 Taylor Series

A Taylor series is a power series that allows us to approximate a function that has certain properties. The theoretical basis for Taylor series is given by the following theorem. The theorem and its proof are as given in [Rud]; by $f^{(i)}(t)$ we mean the i^{th} derivative of $f(t)$. A key ingredient in our proof is the Mean Value Theorem, which is proved in Appendix A.

Theorem 2.1 (Taylor's Theorem)**.** *Let f be a real-valued function on $[a,b]$ and let n be a positive integer. Suppose that the following conditions hold:*

1. *$f^{(n-1)}(t)$ is continuous on $[a,b]$*
2. *$f^{(n)}(t)$ exists for every $t \in (a,b)$.*

Let α and β be distinct points of $[a,b]$, and define

$$P_{n-1}(t) \;=\; \sum_{i=0}^{n-1} \frac{f^{(i)}(\alpha)}{i!}(t-\alpha)^i. \tag{2.1}$$

Then for some x between α and β,

$$f(\beta) \;=\; P_{n-1}(\beta) + \frac{f^{(n)}(x)}{n!}(\beta-\alpha)^n. \tag{2.2}$$

Given appropriate bounds on the higher derivatives, we can approximate a function as a polynomial, which is often much simpler than considering the function exactly. The function $P_{n-1}(t)$ is called the Taylor series of order (or degree) $n-1$. It is the best approximation to $f(t)$ among polynomials of degree $n-1$, and the error between our function $f(t)$ and our Taylor series approximation $P_{n-1}(t)$ is bounded by the n^{th} derivative. Not surprisingly, the larger n is, the better the approximation. This is because we are using more and more information. If $n-1=0$ then we are approximating $f(\beta)$ with $f(\alpha)$. This means that, if all we know at time α is the value $f(\alpha)$, our best guess is that the function is always this value (for we do not know if it is increasing or decreasing).

If now we know $f'(\alpha)$, we know how rapidly the function f is changing at α (if we think of f as representing distance, then $f'(\alpha)$ is the speed at α). Our best guess is now that the speed is constant, always equal to $f'(\alpha)$. If this were true, then the value of f at β would be $f(\alpha)+f'(\alpha)(\beta-\alpha)$ (where we start plus the distance traveled, which under the assumption of constant speed is just speed times elapsed time). This is the first order Taylor series approximation. The next piece of information, $f''(\alpha)$, tells us how fast the speed is changing at time α. This allows us weaken our assumption of constant speed, and obtain a better approximation.

Proof. For $a<t<b$, we define

$$g(t) \;=\; f(t) - P_{n-1}(t) - M(t-\alpha)^n, \tag{2.3}$$

where M is chosen so that $g(\beta)=0$. It is easily seen from (2.1) that the values of $P_{n-1}^{(i)}(\alpha)$ coincide with the values of $f^{(i)}(\alpha)$ for any choice of i with $0\le i\le n-1$. Then for any such i, we have

$$g^{(i)}(\alpha) \;=\; f^{(i)}(t) - P_{n-1}^{(i)}(t) - M\frac{n!}{(n-i)!}(\alpha-\alpha)^{n-i} \;=\; 0 \tag{2.4}$$

From the Mean Value Theorem, since $g(\beta)=g(\alpha)=0$, we must have $g'(x_1)=0$ for some x_1 between α and β. We can now apply the mean value theorem to $g'(t)$. We have $g'(x_1)=g'(\alpha)=0$, so $g''(x_2)=0$ for some x_2 between x_1 and α. We can continue this process for a total of n steps to see that $g^{(n)}(x_n)=0$ for some x_n between α and x_{n-1}. We let $x=x_n$ and note that x is also between α and β.

By differentiating n times the equation (2.3), we have

$$g^{(n)}(t) \;=\; f^{(n)}(t) - P_{n-1}^{(n)}(t) - Mn!(t-\alpha)^0. \tag{2.5}$$

Since $P_{n-1}(t)$ is a polynomial of degree $n-1$, this becomes

$$g^{(n)}(t) \;=\; f^{(n)}(t) - Mn!. \tag{2.6}$$

Since $g^{(n)}(\alpha)=0$,

$$f^{(n)}(t) \;=\; Mn!. \tag{2.7}$$

We then have

$$P_{n-1}(\beta) + \frac{f^{(n)}(x)}{n!}(\beta-\alpha)^n \;=\; P_{n-1}(\beta) + \frac{Mn!}{n!}(\beta-\alpha)^n \;=\; f(\beta)-g(\beta) \;=\; f(\beta). \tag{2.8}$$

The x we have chosen therefore satisfies the statement of the theorem. □

Taylor's Theorem allows us to approximate $f(\beta)$ as $P_{n-1}(\beta)$ and gives us to approximate the error by finding the maximum value of $\frac{f^{(n)}(x)}{n!}(\beta-\alpha)^n$ for x on the interval $[a,b]$. If we have a good upper bound on the derivatives of f, we can get a good polynomial approximation for $f(\beta)$.

Example 2.2. Let us consider

$$f(x) \;=\; \log(1-x). \tag{2.9}$$

We will compute the Taylor series about $x=0$.

By direct computation, we have $f(0)=0$. We now compute the first derivative:

$$f'(x) \;=\; -\frac{1}{1-x}. \tag{2.10}$$

Hence, $f'(0) = -1$.

We will now show that

$$f^{(n)}(x) \;=\; -\frac{(n-1)!}{(1-x)^n} \tag{2.11}$$

for $n \geq 1$. We have just shown the case $n = 1$, and we will proceed by induction (see Appendix C). Assuming the statement for $n-1$, we compute $f^{(n)}(x)$ as the derivative of $f^{(n-1)}(x)$. We have

$$f^{(n)}(x) \;=\; \frac{d}{dx}\left(-\frac{(n-2)!}{(1-x)^{n-1}}\right) \;=\; -\frac{-(n-1)\cdot(n-2)!}{(1-x)^n}\cdot(-1) \;=\; -\frac{(n-1)!}{(1-x)^n}. \tag{2.12}$$

The statement in 2.11 now follows by induction for $n \geq 1$. From this, we see that $f^{(n)}(0) = -(n-1)!$. The Taylor series for $f(x)$ about 0 is therefore given by

$$f(x) \;=\; -\left(\frac{0!}{1!}\cdot x + \frac{1!}{2!}\cdot x^2 + \frac{2!}{3!}\cdot x^3 + \cdots\right) \;=\; -\left(x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots\right) \;=\; -\sum_{n=1}^{\infty}\frac{x^n}{n}. \tag{2.13}$$

Remark 2.3. *Note the expansion for* $\log(1-x)$ *above converges for* $0 \leq x < 1$. *Further, one can see that this expansion is a negative number for* $x > 0$. *This makes sense, as for* $x \in (0,1)$, $1 - x \in (0,1)$. *When we calculate* $\log(1-x)$ *we are taking the logarithm of a positive number less than* 1*; this has to be negative (the logarithm of* 1 *is zero, the logarithm of numbers greater than* 1 *are positive and those less than* 1 *are negative). It is very important to be able to quickly spot-check a formula to look for simple omission. For complicated formulas, try to concentrate on the main parts or features, and see if they make sense.*

Remark 2.4. *One can also derive the Taylor series expansion by integration. From the geometric series formula, we know*

$$-\frac{1}{1-y} \;=\; -\sum_{n=0}^{\infty} y^n \tag{2.14}$$

for $0 \leq y < 1$. *If we integrate both sides from* 0 *to* $x < 1$, *provided we can interchange the integration and summation, we have*

$$\begin{aligned}
\int_0^x -\frac{1}{1-y}\,dy &= \int_0^x -\sum_{n=1}^{\infty} y^n\,dy \\
\ln(1-y)\Big|_0^x &= -\sum_{n=0}^{\infty}\int_0^x y^n\,dy \\
\ln(1-x) &= -\sum_{n=0}^{\infty}\frac{x^{n+1}}{n+1} \;=\; -\sum_{n=1}^{\infty}\frac{x^n}{n};
\end{aligned} \tag{2.15}$$

the interchange of integration and summation can be justified by Fubini's Theorem.

Example 2.5. One of the most important Taylor series is that of $f(x) = e^x$ about $x = 0$. As $f^{(n)}(x) = e^x$ for all n, we have

$$e^x \;=\; \sum_{n=0}^{\infty}\frac{f^{(n)}(0)x^n}{n!} \;=\; \sum_{n=0}^{\infty}\frac{x^n}{n!}. \tag{2.16}$$

Exercise 2.6. *Calculate the Taylor series of* $\cos\theta$ *and* $\sin\theta$ *around* $\theta = 0$. *Consider what we get by formally plugging in* $i\theta$ *in the Taylor series expansion of* e^x: $\sum_{n=0}^{\infty}(i\theta)^n/n!$. *Often the Taylor series expansion is used as the definition of* e^x; *because of the rapid decay of* $n!$ *(see §3), this infinite sum converges for all complex valued* x. *Thus we may define* e^x *by* $\sum_{n=0}^{\infty} x^n/n!$ *for all* x, *real or complex. Show that*

$$e^{i\theta} \;=\; \cos\theta + i\sin\theta. \tag{2.17}$$

One can use this to derive all trigonometric formulas[1]. *For example,* $\sin^2\theta + \cos^2\theta = 1$ *follows from* $e^{i\theta}\cdot e^{-i\theta} = 1$. *Taking real and imaginary parts of* $e^{i\theta}\cdot e^{i\phi} = e^{i(\theta+\phi)}$ *gives the angle addition formulas for sine and cosine. To see this we substitute the Taylor series expansions, and find*

$$(\cos\theta + i\sin\theta)\cdot(\cos\phi + i\sin\phi) \;=\; \cos(\theta+\phi) + i\sin(\theta+\phi); \tag{2.18}$$

complete the proof by multiplying out the two factors on the left hand side, and comparing the real and imaginary parts.

[1]We need one additional, important fact: $e^x \cdot e^y = e^{x+y}$ holds for all x and y, even those that are complex valued. This is not at all clear, as we have defined e^x and e^y as infinite sums! One must do some book-keeping to show that, interpreting all three quantities as infinite sums, we do indeed get $e^x \cdot e^y = e^{x+y}$. While it is likely that this relation is true (if it wasn't, this would be horrible notation!), we must *prove* this.

Exercise 2.7. *Calculate the Taylor series of* e^{-t^2} *about* $t = 0$ *two different ways. First use the standard technique of finding derivatives and evaluating them at zero, and then check your work by substituting* $-t^2$ *in for* x *in the Taylor series expansion of* e^x. *This second technique is a very useful way to find the Taylor series of* $f(g(t))$ *if we know the Taylor series of* $f(x)$.

Example 2.8. Consider

$$f(x) \;=\; \frac{1-\sqrt{1-4x}}{2}. \tag{2.19}$$

We will compute the Taylor series expansion of $f(x)$ about $x = 0$. For the constant term, we have $f(0) = 0$. We now find the first derivative:

$$f'(x) = (1-4x)^{-1/2}. \tag{2.20}$$

Hence $f'(0) = 1$.

We introduce some useful notation:

$$(2n)!! \;=\; 2n(2n-2)(2n-4)\cdots 4\cdot 2, \quad (2n+1)!! \;=\; (2n+1)(2n-1)(2n-3)\cdots 3\cdots 1. \tag{2.21}$$

Thus the double factorial means take every other until you reach 2 (if even) or 1 (if odd).

For $n > 1$, we will now show that

$$f^{(n)}(x) = 2^{n-1}\cdot(2n-3)!! \;\cdot\; (1-4x)^{-\frac{2n-1}{2}}. \tag{2.22}$$

Note that by the definition of the double factorial, $(2n-3)!! = (2n-3)\cdot(2n-5)\cdots 3\cdot 1$. For $n = 2$, this is $f''(x) = 2(1-4x)^{-3/2}$, which is true by direct computation of the derivative in (2.20). We now assume the statement for $n-1$. Then

$$f^{(n)}(x) \;=\; \frac{d}{dx}f^{(n-1)}(x) \;=\; \frac{d}{dx}\left(2^{n-2}\cdot(2n-5)!(1-4x)^{-\frac{2n-3}{2}}\right) \;=\; 2^{n-1}\cdot(2n-5)!\left(-\frac{2n-3}{2}(1-4x)^{-\frac{2n-5}{2}}\cdot(-4)\right). \tag{2.23}$$

Simplification yields (2.22), so the claim follows by induction.

Evaluating (2.22) at $x = 0$, we see that

$$f^{(n)}(0) \;=\; 2^{n-1}\cdot(2n-3)!!. \tag{2.24}$$

Therefore, $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots$ where

$$a_n \;=\; \begin{cases} 0 & n = 0 \\ 1 & n = 1 \\ \frac{2^{n-1}\cdot(2n-3)!!}{n!} & n \geq 2. \end{cases} \tag{2.25}$$

Exercise 2.9. *With reference to Example 2.8, show that*

$$\lim_{n\to\infty}\frac{a_{n+1}}{a_n} \;=\; 4. \tag{2.26}$$

Exercise 2.10. *Compute the Taylor polynomial of degree 2 of* $\log(1+x)$ *about* $x = 0$.

Exercise 2.11. *Consider the function* $f(x)$ *given by*

$$f(x) \;=\; \begin{cases} e^{-1/x^2} & x \neq 0 \\ 0 & x = 0. \end{cases} \tag{2.27}$$

Show that the Taylor series for $f(x)$ *about* $x = 0$ *is* 0 *even though* $f(x)$ *is not the zero function. Why is this the case?* Hint: *you must go back to the definition of the derivative to take the derivative at* $x = 0$.

3 Stirling's Formula

Stirling's Formula allows us to approximate the factorial in terms of elementary functions.

Theorem 3.1 (Stirling's Theorem)**.** *For large* n,

$$n! \;\approx\; n^n e^{-n}\sqrt{2\pi n}. \tag{3.28}$$

Remark 3.2. *Before proving Stirling's formula, we show it is a reasonable approximation. It is often easier to analyze a product by converting it to a sum; this is readily accomplished by taking logarithms; in fact, we shall see this trick again when we study the Birthday Problem in §4. We have*

$$\log n! \;=\; \sum_{k=1}^{n} \log k \;\approx\; \int_1^n \log t dt \;=\; (t \log t - t)|_1^n. \tag{3.29}$$

Thus $\log n! \approx n \log n - n$, *or* $n! \approx n^n e^{-n}$.

For a more precise statement of the theorem and a proof that relies on some more advanced results of analysis, we refer the reader to [Rud]. We include the simpler proof of [Wei] here.

Proof. To prove the theorem, we will use the identity

$$n! \;=\; \Gamma(n+1) \;=\; \int_0^\infty e^{-x} x^n \, dx. \tag{3.30}$$

A review of the Gamma function, including a proof of this identity, can be found in Appendix B.

In order to get an approximation, we would like to find where the integrand is largest. Because of the exponential factor in the integrand, we will take the logarithm before differentiating[2]:

$$\frac{d}{dx} \log(e^{-x} x^n) \;=\; \frac{d}{dx}(-x + n \log x) \;=\; \frac{n}{x} - 1. \tag{3.31}$$

The maximum value of the integrand is therefore seen to occur only for $x = n$. The exponential factor shrinks much more quickly than the growth of x^n, so we assume that $x = n + \alpha$ with $|\alpha|$ much smaller then n. We then have,

$$\log x \;=\; \log(n+\alpha) \;=\; \log n + \log\left(1 + \frac{\alpha}{n}\right). \tag{3.32}$$

We now expand the second term using the Taylor polynomial computed in Example 2.2[3] to find

$$\log(n+\alpha) \;=\; \log n + \frac{\alpha}{n} - \frac{1}{2}\frac{\alpha^2}{n^2} + \cdots. \tag{3.33}$$

Therefore

$$\log(x^n e^{-x}) \;=\; n \log x - x \;\approx\; n\left(\log n + \frac{\alpha}{n} - \frac{1}{2}\frac{\alpha^2}{n^2}\right) - (n+\alpha) \;=\; n \log n - n - \frac{\alpha^2}{2n^2}. \tag{3.34}$$

It follows that

$$x^n e^{-x} \;\approx\; \exp\left(n \log n - n - \frac{\alpha^2}{2n^2}\right) \;=\; n^n e^{-n} \cdot \exp\left(-\frac{\alpha^2}{2n^2}\right). \tag{3.35}$$

Then returning to the integral expression for $n!$ of (3.30), we have

$$n! \;=\; \int_0^\infty e^{-x} x^n \, dx \;\approx\; \int_{-n}^\infty n^n e^{-n} \cdot \exp\left(-\frac{\alpha^2}{2n^2}\right) d\alpha \;\approx\; n^n e^{-n} \cdot \int_{-\infty}^\infty \exp\left(-\frac{\alpha^2}{2n^2}\right) d\alpha. \tag{3.36}$$

In the last step, we rely on the fact that the integrand is very small for $\alpha < -n$. The integral is the the same as the one we would obtain in integrating a normal density with mean 0 and variance $\sqrt{n}$. Its value is $\sqrt{2\pi n}$. We thus have

$$n! \;\approx\; n^n e^{-n} \sqrt{2\pi n}, \tag{3.37}$$

which is the statement of the theorem. □

4 The Birthday Problem

There are several variants of the Birthday Problem; we state a few here. Assume each day of the year is equally likely to be someone's birthday, and no one is ever born on February 29[th] (just to make our lives easier!). How many people must there be in a room before there is at least a 50% chance that two share a birthday? How many other people must there be before at least one of them shares *your* birthday? Note the two questions have very different answers, because in the

[2] Maximizing a positive function $f(x)$ is equivalent to maximizing $\log f(x)$. There are many useful versions of this principle: in calculus it is often easier to minimize the square of the distance rather than the distance (as this avoids the square-root function).

[3] In the example, we computed the Taylor series for $\log(1-x)$, but we can write $\log(1+\alpha) = \log(1-(-\alpha))$ to apply our result.

first we do not specify beforehand *which* is the shared day, while in the second we do. How many people must be in the room before at least two share a birthday?

One can, of course, solve these questions by brute force. For the standard formulation, we are looking for an n such that

$$\left(1-\frac{0}{365}\right)\cdot\left(1-\frac{1}{365}\right)\cdots\left(1-\frac{n-1}{365}\right) \ \approx\ \frac{1}{2}. \tag{4.38}$$

To solve this with a calculator is possible, especially if we simplify it by using factorials:

$$\frac{365!}{(365-n)!}. \tag{4.39}$$

Such large factorials quickly overflow standard calculators (though we would be fine if we used Mathematica or Matlab); things are even worse if we are on a planet such as Mars or Jupiter with a longer year. We discuss how one can very easily approximate the correct answer.

The probability that n people all have distinct birthdays is

$$p(n) \ =\ \left(1-\frac{0}{365}\right)\cdots\left(1-\frac{n-1}{365}\right) \ =\ \prod_{k=0}^{n-1}\left(1-\frac{k}{365}\right). \tag{4.40}$$

We want to find n so that $p(n)=\frac{1}{2}$. A common technique to analyze products is to take logarithms, as logarithms convert products to sums. Thus we want to solve

$$\log\frac{1}{2} \ =\ \sum_{k=0}^{n-1}\log\left(1-\frac{k}{365}\right). \tag{4.41}$$

We use $\log\frac{1}{2}\approx -.7$, the Taylor series expansion $\log(1-x)=x+O(x^2)$ for x small (see Example 2.2), and $\sum_{k=0}^{n-1}k\approx n^2/2$ (which can be proved by induction; see Appendix C for a review of proofs by induction) to find

$$-.7 \ \approx\ -\sum_{k=0}^{n-1}\frac{k}{365} \ \approx\ -\frac{n^2/2}{365}. \tag{4.42}$$

Thus $n^2\approx 511$ or $n\approx 22.6$, which agrees very well with the exact answer. Similar arguments also provide a terrific (and easy!) approximation to the number of people needed before there is a 50% probability that one of them shares your birthday (about 253 are needed).

A The Intermediate and Mean Value Theorems (IVT, MVT)

These notes are a modified version of the presentation in [MT-B].

Theorem A.1 (Intermediate Value Theorem (IVT))**.** *Let f be a continuous function on $[a,b]$. For all C between $f(a)$ and $f(b)$ there exists a $c\in[a,b]$ such that $f(c)=C$. In other words, all intermediate values of a continuous function are obtained.*

Sketch of the proof. We proceed by **Divide and Conquer**. Without loss of generality, assume $f(a)<C<f(b)$. Let x_1 be the midpoint of $[a,b]$. If $f(x_1)=C$ we are done. If $f(x_1)<C$, we look at the interval $[x_1,b]$. If $f(x_1)>C$ we look at the interval $[a,x_1]$.

In either case, we have a new interval, call it $[a_1,b_1]$, such that $f(a_1)<C<f(b_1)$ and the interval has half the size of $[a,b]$. We continue in this manner, repeatedly taking the midpoint and looking at the appropriate half-interval.

If any of the midpoints satisfy $f(x_n)=C$, we are done. If no midpoint works, we divide infinitely often and obtain a sequence of points x_n in intervals $[a_n,b_n]$. This is where rigorous mathematical analysis is required (see [Rud] for details) to show x_n converges to an $x\in(a,b)$.

For each n we have $f(a_n)<C<f(b_n)$, and $\lim_{n\to\infty}|b_n-a_n|=0$. As f is continuous, this implies $\lim_{n\to\infty}f(a_n)=\lim_{n\to\infty}f(b_n)=f(x)=C$. □

Theorem A.2 (The Mean Value Theorem (MVT))**.** *Let $f(x)$ be differentiable on $[a,b]$. Then there exists a $c\in(a,b)$ such that*

$$f(b)-f(a)=f'(c)\cdot(b-a). \tag{A.43}$$

We give an interpretation of the Mean Value Theorem. Let $f(x)$ represent the distance from the starting point at time x. The average speed from a to b is the distance traveled, $f(b) - f(a)$, divided by the elapsed time, $b - a$. As $f'(x)$ represents the speed at time x, the Mean Value Theorem says that there is some intermediate time at which we are traveling at the average speed.

To prove the Mean Value Theorem, it suffices to consider the special case when $f(a) = f(b) = 0$; this case is known as Rolle's Theorem:

Theorem A.3 (Rolle's Theorem)**.** *Let f be differentiable on $[a, b]$, and assume $f(a) = f(b) = 0$. Then there exists a $c \in (a, b)$ such that $f'(c) = 0$.*

Exercise A.4. *Show the Mean Value Theorem follows from Rolle's Theorem.* Hint: *Consider*

$$h(x) \;=\; f(x) - \frac{f(b) - f(a)}{b - a}(x - a) - f(a). \tag{A.44}$$

Note $h(a) = f(a) - f(a) = 0$ and $h(b) = f(b) - (f(b) - f(a)) - f(a) = 0$. The conditions of Rolle's Theorem are satisfied for $h(x)$, and

$$h'(c) \;=\; f'(c) - \frac{f(b) - f(a)}{b - a}. \tag{A.45}$$

Proof of Rolle's Theorem. Without loss of generality, assume $f'(a)$ and $f'(b)$ are non-zero. If either were zero we would be done. Multiplying $f(x)$ by -1 if needed, we may assume $f'(a) > 0$. *For convenience, we assume $f'(x)$ is continuous.* This assumption simplifies the proof, but is not necessary. In all applications in these notes this assumption will be met.

Case 1: $f'(b) < 0$**:** As $f'(a) > 0$ and $f'(b) < 0$, the Intermediate Value Theorem applied to $f'(x)$ asserts that all intermediate values are attained. As $f'(b) < 0 < f'(a)$, this implies the existence of a $c \in (a, b)$ such that $f'(c) = 0$.

Case 2: $f'(b) > 0$**:** $f(a) = f(b) = 0$, and the function f is increasing at a and b. If x is real close to a then $f(x) > 0$ if $x > a$. This follows from the fact that

$$f'(a) \;=\; \lim_{x \to a} \frac{f(x) - f(a)}{x - a}. \tag{A.46}$$

As $f'(a) > 0$, the limit is positive. As the denominator is positive for $x > a$, the numerator must be positive. Thus $f(x)$ must be greater than $f(a)$ for such x. Similarly $f'(b) > 0$ implies $f(x) < f(b) = 0$ for x slightly less than b.

Therefore the function $f(x)$ is positive for x slightly greater than a and negative for x slightly less than b. If the first derivative were always positive then $f(x)$ could never be negative as it starts at 0 at a. This can be seen by again using the limit definition of the first derivative to show that if $f'(x) > 0$ then the function is increasing near x. Thus the first derivative cannot always be positive. Either there must be some point $y \in (a, b)$ such that $f'(y) = 0$ (and we are then done) or $f'(y) < 0$. By the Intermediate Value Theorem, as 0 is between $f'(a)$ (which is positive) and $f'(y)$ (which is negative), there is some $c \in (a, y) \subset [a, b]$ such that $f'(c) = 0$. □

B Factorials and the Gamma Function

The Gamma function is defined by the equation

$$\Gamma(x) \;=\; \int_0^\infty x^{n-1} e^{-x}\, dx. \tag{B.47}$$

The Gamma function is useful to us because of the following theorem.

Theorem B.1. *Let n be a nonnegative integer. Then*

$$n! \;=\; \Gamma(n + 1). \tag{B.48}$$

Proof. We prove the theorem by induction. For $n = 0$, the theorem says

$$0! \;=\; \Gamma(1) \;=\; \int_0^\infty e^{-x}\, dx. \tag{B.49}$$

Both the leftmost and rightmost expressions evaluate to 1, so the base case is proven.

We now assume the statement to be true for 0 to $n - 1$. We must show $\Gamma(n + 1) = n!$. By definition,

$$\Gamma(n + 1) \;=\; \int_0^\infty x^n e^{-x}\; dx. \tag{B.50}$$

Integrating by parts gives us

$$\begin{aligned}\Gamma(n+1) &= \int_0^\infty x^n e^{-x}\,dx \\ &= \left[-e^{-x}x^n\right]_0^\infty + \int_0^\infty n x^{n-1} e^{-x}\,dx \\ &= 0 + n\int_0^\infty x^{n-1}e^{-x}\,dx \\ &= n\Gamma(n) \\ &= n\cdot(n-1)! \\ &= n!. \end{aligned} \tag{B.51}$$

The theorem follows by induction (see Appendix C for a review of induction). □

C Proofs by Induction

These notes are a modified version of the presentation in [MT-B].

Assume for each positive integer n we have a statement $P(n)$ which we desire to show is true. $P(n)$ is true for all positive integers n if the following two statements hold:

- **Basis Step:** $P(1)$ is true;
- **Inductive Step**: whenever $P(n)$ is true, $P(n+1)$ is true.

This technique is called **Proof by Induction**, and is a very useful method for proving results; we shall see many instances of this in this appendix. The reason the method works follows from basic logic. We assume the following two sentences are true:

$$\begin{gathered} P(1) \text{ is true} \\ \forall n \geq 1, P(n) \text{ is true implies } P(n+1) \text{ is true.} \end{gathered} \tag{C.52}$$

Set $n = 1$ in the second statement. As $P(1)$ is true, and $P(1)$ implies $P(2)$, $P(2)$ must be true. Now set $n = 2$ in the second statement. As $P(2)$ is true, and $P(2)$ implies $P(3)$, $P(3)$ must be true. And so on, completing the proof. Verifying the first statement the **basis step** and the second the **inductive step**. In verifying the inductive step, note we assume $P(n)$ is true; this is called the **inductive assumption**. Sometimes instead of starting at $n = 1$ we start at $n = 0$, although in general we could start at any n_0 and then prove for all $n \geq n_0$, $P(n)$ is true.

We give three of the more standard examples of proofs by induction, and one false example; the first example is the most typical. When you have mastered proofs by induction, the following is a fun problem involving the Fibonacci numbers.

Exercise C.1 (Zeckendorf's Theorem)**.** *Consider the set of distinct Fibonacci numbers: $\{1, 2, 3, 5, 8, 13, \dots\}$. Show every positive integer can be written uniquely as a sum of distinct Fibonacci numbers where we do not allow two consecutive Fibonacci numbers to occur in the decomposition. Equivalently, for any n there are choices of $\epsilon_i(n) \in \{0, 1\}$ such that*

$$n \;=\; \sum_{i=2}^{\ell(n)} \epsilon_i(n) F_i, \quad \epsilon_i(n)\epsilon_{i+1}(n) = 0 \text{ for } i \in \{2, \dots, \ell(n)-1\}. \tag{C.53}$$

Does a similar result hold for all recurrence relations? If not, can you find another recurrence relation where such a result holds?

C.1 Sums of Integers

Let $P(n)$ be the statement

$$\sum_{k=1}^{n} k \;=\; \frac{n(n+1)}{2}. \tag{C.54}$$

Basis Step: $P(1)$ is true, as both sides equal 1.

Inductive Step: Assuming $P(n)$ is true, we must show $P(n+1)$ is true. By the inductive assumption, $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$. Thus

$$\begin{aligned}\sum_{k=1}^{n+1} k &= (n+1) + \sum_{k=1}^{n} k \\ &= (n+1) + \frac{n(n+1)}{2} \\ &= \frac{(n+1)(n+1+1)}{2}.\end{aligned} \tag{C.55}$$

Thus, given $P(n)$ is true, then $P(n+1)$ is true.

Exercise C.2. *Prove*

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}. \tag{C.56}$$

Find a similar formula for the sum of k^3.

Exercise C.3. *Show the sum of the first n odd numbers is n^2, i.e.,*

$$\sum_{k=1}^{n} (2k-1) = n^2. \tag{C.57}$$

Remark C.4. *We define the empty sum to be 0, and the empty product to be 1. For example, $\sum_{n \in \mathbb{N}, n<0} 1 = 0$.*

See [Mil] for an alternate derivation of sums of powers that does not use induction.

C.2 Divisibility

Let $P(n)$ be the statement 133 divides $11^{n+1} + 12^{2n-1}$.

Basis Step: A straightforward calculation shows $P(1)$ is true: $11^{1+1} + 12^{2-1} = 121 + 12 = 133$.
Inductive Step: Assume $P(n)$ is true, i.e., 133 divides $11^{n+1} + 12^{2n-1}$. We must show $P(n+1)$ is true, or that 133 divides $11^{(n+1)+1} + 12^{2(n+1)-1}$. But

$$\begin{aligned}11^{(n+1)+1} + 12^{2(n+1)-1} &= 11^{n+1+1} + 12^{2n-1+2} \\ &= 11 \cdot 11^{n+1} + 12^2 \cdot 12^{2n-1} \\ &= 11 \cdot 11^{n+1} + (133+11)12^{2n-1} \\ &= 11\left(11^{n+1} + 12^{2n-1}\right) + 133 \cdot 12^{2n-1}.\end{aligned} \tag{C.58}$$

By the inductive assumption 133 divides $11^{n+1} + 12^{2n-1}$; therefore, 133 divides $11^{(n+1)+1} + 12^{2(n+1)-1}$, completing the proof.

Exercise C.5. *Prove 4 divides $1 + 3^{2n+1}$.*

C.3 The Binomial Theorem

We prove the Binomial Theorem. First, recall that

Definition C.6 (Binomial Coefficients)**.** *Let n and k be integers with $0 \le k \le n$. We set*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}. \tag{C.59}$$

Note that $0! = 1$ and $\binom{n}{k}$ is the number of ways to choose k objects from n (with order not counting).

Lemma C.7. *We have*

$$\binom{n}{k} = \binom{n}{n-k}, \qquad \binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}. \tag{C.60}$$

Exercise C.8. *Prove Lemma C.7.*

Theorem C.9 (The Binomial Theorem)**.** *For all positive integers n we have*

$$(x+y)^n \;=\; \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k. \tag{C.61}$$

Proof. We proceed by induction.
Basis Step: For $n=1$ we have

$$\sum_{k=0}^{1}\binom{1}{k}x^{1-k}y^k \;=\; \binom{1}{0}x+\binom{1}{1}y \;=\; (x+y)^1. \tag{C.62}$$

Inductive Step: Suppose

$$(x+y)^n \;=\; \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k. \tag{C.63}$$

Then using Lemma C.7 we find that

$$\begin{aligned}(x+y)^{n+1} &= (x+y)(x+y)^n\\ &= (x+y)\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k\\ &= \sum_{k=0}^{n}\binom{n}{k}x^{n+1-k}y^k+\binom{n}{k}x^{n-k}y^{k+1}\\ &= x^{n+1}+\sum_{k=1}^{n}\left\{\binom{n}{k}+\binom{n}{k-1}\right\}x^{n+1-k}y^k+y^{n+1}\\ &= \sum_{k=0}^{n+1}\binom{n+1}{k}x^{n+1-k}y^k. \end{aligned}\tag{C.64}$$

This establishes the induction step, and hence the theorem. □

C.4 False Proofs by Induction

Consider the following: let $P(n)$ be the statement that in any group of n people, everyone has the same name. We give a (false!) proof by induction that $P(n)$ is true for all n!

Basis Step: Clearly, in any group with just 1 person, every person in the group has the same name.

Inductive Step: Assume $P(n)$ is true, namely, in any group of n people, everyone has the same name. We now prove $P(n+1)$. Consider a group of $n+1$ people:

$$\{1,2,3,\dots,n-1,n,n+1\}. \tag{C.65}$$

The first n people form a group of n people; by the inductive assumption, they all have the same name. So, the name of 1 is the same as the name of 2 is the same as the name of 3 $\dots$ is the same as the name of n.

Similarly, the last n people form a group of n people; by the inductive assumption they all have the same name. So, the name of 2 is the same as the name of 3 $\dots$ is the same as the name of n is the same as the name of $n+1$. Combining yields everyone has the same name! Where is the error?

If $n=4$, we would have the set $\{1,2,3,4,5\}$, and the two sets of 4 people would be $\{1,2,3,4\}$ and $\{2,3,4,5\}$. We see that persons 2, 3 and 4 are in both sets, providing the necessary link.

What about smaller n? What if $n=1$? Then our set would be $\{1,2\}$, and the two sets of 1 person would be $\{1\}$ and $\{2\}$; there is no overlap! The error was that we assumed n was "large" in our proof of $P(n)\Rightarrow P(n+1)$.

Exercise C.10. *Show the above proof that $P(n)$ implies $P(n+1)$* is *correct for $n\geq 2$, but fails for $n=1$.*

Exercise C.11. *Similar to the above, give a false proof that any sum of k integer squares is an integer square, i.e., $x_1^2+\cdots+x_n^2=x^2$. In particular, this would prove all positive integers are squares as $m=1^2+\cdots+1^2$.*

Remark C.12. *There is no such thing as* Proof By Example*. While it is often useful to check a special case and build intuition on how to tackle the general case, checking a few examples is not a proof. For example, because $\frac{16}{64}=\frac{1}{4}$ and $\frac{19}{95}=\frac{1}{5}$, one might think that in dividing two digit numbers if two numbers on a diagonal are the same one just cancels them. If that were true, then $\frac{12}{24}$ should be $\frac{1}{4}$. Of course this is* not *how one divides two digit numbers!*

References

[MM] I. Miller and M. Miller, *John E. Freund's Mathematical Statistics with Applications*, seventh edition, Prentice Hall, 2004.

[Mil] S. J. Miller, *Differentiating identities*, Class Notes from Math 162: Statistics, Brown University, Spring 2005.

[MT-B] S. J. Miller and R. Takloo-Bighash, *An Invitation to Modern Number Theory*, Princeton University Press, Princeton, NJ, 2006.

[Rud] W. Rudin, *Principles of Mathematical Analysis*, third edition, International Series in Pure and Applied Mathematics, McGraw-Hill Inc., New York, 1976.

[Wei] Weisstein, Eric W. "Stirling's Approximation." From *MathWorld*–A Wolfram Web Resource. http://mathworld.wolfram.com/StirlingsApproximation.html.