# Proof Examples

Peter Cappello
cappello@cs.ucsb.edu

## Introduction

A mathematical proof, no less than a poem, musical composition, or computer program, can be a thing of beauty. Composing a mathematical proof is similar, in some respects, to the human artifacts mentioned above: The first version is not the final version. There are stylistic considerations, as one seeks precision, clarity, and elegance. Achieving these attributes entails iteratively refining the proof, as one would an essay, poem, musical composition, or computer program.

Incremental improvements are at best inconvenient when the proof is rendered with a pencil and paper, enough so that, to seek excellence, one must venture into a machine-readable medium. Latex currently is the easiest and most popular tool for this purpose. Its use eliminates the inhibition and inconvenience associated with erasing and rewriting, and enables rapid production of multiple lines of mathematics that differ symbolically only in small ways. These seemingly minor mechanical advantages are key to the accumulation of improvements needed to turn a first draft into an elegant proof of publication quality.

In producing the proofs below, I hope to help you 1) learn by example what I like to see in the form of a proof, and 2) explore personally issues of mathematical style. If you think any of the proofs are incorrect or could be simpler, clearer, or improved in any other way, please email me.

On a separate page, the latex used to produce these proofs is provided as evidence that latex is a labor-saving device, even for mathematical work as ephemeral as homework.

## Style

I encourage a mathematical style that I think is appropriate for a student taking a *first* course where mathematical proofs are the coin of the realm: As you mature mathematically, some elements can be abbreviated or omitted. For now, err on the side of giving an explanations where none is needed. Similarly, strive for a form that is clear to another first-year student. Indeed, asking another student to read your proof is a good source of feedback.

One source of thoughts about mathematical writing style is a document by Goss [4]. Another is by Gillman [3]. There also is a guide to the use of the

Americam Mathematical Society (AMS) Latex package [2] and an AMS author-related FAQ [1].

Below, I produce a few style notes, certainly not a comprehensive list. Also, some of these notes run against the grain of convention. Please use your own judgment.

1. It generally is considered bad form to mix mathematical symbols with English words (e.g., $\forall n \in N, n^2$ is greater than 0.) I disagree. Please use mathematical symbols as much as possible; this results in fewer characters, enabling the eye to see more content at once. I also disagree, and for the same reasons, with the rule that numbers less than 10 should be written in English. In my opinion, this is like saying, for the number 7, "Why use a single universally understood symbol, when we can use a sequence of five letters that only English speakers understand?"

2. It often is helpful to give a concrete example before giving a fully general proof.

3. A proof should be free of debris that obscures the forest for the trees. Omit purely *routine* symbol manipulation (i.e., not requiring a trick). What constitutes a "trick" however depends on your audience: Whether or not a proof is well written depends on the intended audience.

4. A diagram or picture may convey properties better than a 1000 words. Fig. 1 is a fine proof of the Pythagorean theorem.
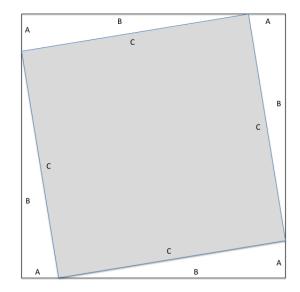


Figure 1: Proof of Pythagorean theorem.

# Mathematical Induction

The following proofs are of exercises in Rosen [5], §5.1: Mathematical Induction.

**Exercise 62**

Show that $n$ lines separate the plane into $(n^2 + n + 2)/2$ regions, if no 2 of these lines are parallel and no 3 pass through a common point.

Let $r_n$ denote the number of regions in the partition of the plane by $n$ lines, where no 2 of these lines are parallel and no 3 pass through a common point.

**Theorem.** $\forall n \in \mathbf{N} \; r_n = (n^2 + n + 2)/2$.

*Proof.* By induction on $n$, the number of lines.
**Basis:** $n = 0$: If the plane is partitioned by 0 lines, there is $1 = (0^2 + 0 + 2)/2$ region.
**Induction hypothesis:** $r_n = (n^2 + n + 2)/2$.
**Induction:** Let there be $n + 1$ lines in the plane, where no lines are parallel and no 3 lines intersect at the same point. Remove any line. By the inductive hypothesis, the remaining $n$ lines partition the plane into $(n^2 + n + 2)/2$ regions. Fig. 2(A) illustrates a plane partitioned into 11 regions by 4 lines. In part (B), adding a $5^{th}$ (red) line increases the number of regions by 5.
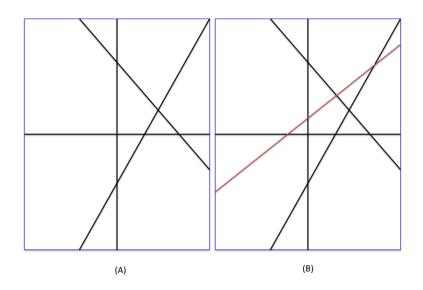


(A)  (B)

Figure 2: (A) A plane partitioned into 11 regions by 4 lines.
(B) A plane partitioned into $11 + 5$ regions by adding a $5^{th}$ (red) line.

In general, when line $n + 1$ is placed so that it is not parallel to any of the other $n$ lines and it intersects each line $l$ at a point where no other lines

intersect line $l$, then $n$ such intersections are formed. Order these intersection points from left to right (or bottom to top, if they are vertical). The region to the left of (or below) the $1^{st}$ intersection point, is divided into 2 regions by line $n + 1$. Similarly, when this line enters the region to the right (or top) of an intersection point, it subdivides this region into 2 regions. Since there are $n$ intersection points, this increases the number of regions by $n$, totalling $n + 1$ additional regions:

$$
\begin{align}
r_{n+1} &= r_n + n + 1 \tag{1} \\
&= \frac{n^2 + n + 2}{2} + n + 1 \tag{2} \\
&= \frac{(n+1)^2 + (n+1) + 2}{2} \tag{3}
\end{align}
$$

Above, the inductive hypothesis is used to go from Eqn. (1) to (2).

$\square$

# Structural Induction

The following proofs are of exercises in Rosen [5], §5.3: Recursive Definitions & Structural Induction.

**Exercise 44**

The set of *full binary trees* is defined recursively:

**Basis step:** The tree consisting of a single vertex is a full binary tree.

**Recursive step:** If $T_1$ and $T_2$ are disjoint full binary trees, there is a full binary tree, denoted by $T_1 \cdot T_2$, consisting of a root $r$ together with edges connecting $r$ to each of the roots of the left subtree $T_1$ and the right subtree $T_2$.

Use structural induction to show that $l(T)$, the number of leaves of a full binary tree $T$, is 1 more than $i(T)$, the number of internal vertices of $T$.

**Theorem.** *If $T$ is a full binary tree, $l(T) = i(T) + 1$.*

*Proof.* By structural induction.
**Basis:** The full binary tree consisting of a single vertex, denoted $\bullet$, clearly has 1 leaf and 0 internal vertices: $l(\bullet) = i(\bullet) + 1$.
**Recursive step:** Assume for full binary trees $T_1$ and $T_2$ that

$$
\begin{align}
l(T_1) &= i(T_1) + 1 \tag{4} \\
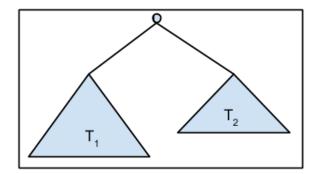l(T_2) &= i(T_2) + 1. \tag{5}
\end{align}
$$

Figure 3: An illustration of full binary tree of $T_1 \cdot T_2$.

For full binary tree $T_1 \cdot T_2$ (see Fig. 3),

$$
\begin{aligned}
i(T_1 \cdot T_2) &= i(T_1) + i(T_2) + 1 & (6)\\
l(T_1 \cdot T_2) &= l(T_1) + l(T_2) & (7)\\
&= (i(T_1) + 1) + (i(T_2) + 1) & (8)\\
&= i(T_1 \cdot T_2) + 1. & (9)
\end{aligned}
$$

Eqns. (6) and (7) follow from the construction of $T_1 \cdot T_2$; (8) follows from the induction hypotheses; (9) follows from (6). $\qquad\square$

# Equivalence Relations

The following proofs are of exercises in Rosen [5], §9.5: Equivalence Relations.

### Exercise 54

Suppose that $R_1$ and $R_2$ are equivalence relations on a set $A$, and that $P_1$ and $P_2$ are their respective partitions. Show that $R_1 \subseteq R_2 \Leftrightarrow P_1$ refines $P_2$.

*Proof.*

$$
\begin{aligned}
R_1 \subseteq R_2 \quad &\Leftrightarrow \quad \forall a \forall b \, (aR_1 b \Rightarrow aR_2 b) & (10)\\
&\Leftrightarrow \quad \forall a([a]_{R_1} \subseteq [a]_{R_2}) & (11)\\
&\Leftrightarrow \quad P_1 \text{ refines } P_2. & (12)
\end{aligned}
$$

The left side of eqn. (10) is equivalent to the right side, by the definition of subset. The right side of (10) is equivalent to (11) by the definition of equivalence class. Eqn. (11) is equivalent to (12) by the definition of partitions $P_1$ and $P_2$ in terms of their corresponding relations, and the definition of refinement. $\qquad\square$

# Permutations & Combinations

The following proofs are of exercises in Rosen [5], §6.3: Permutations & Combinations.

### Exercise 54

How many ways are there for a horse race with 4 horses to finish, if ties are possible? (*Note:* Any number of the 4 horses may tie.)

The following general solution was contributed by Benjamin Chang.

Let $H$ be a set of horses. Define binary relation, $T$ on $H$, where $(horse_1, horse_2) \in T$ when $horse_1$ ties $horse_2$. Since $T$ is an equivalence relation, it partitions the set of horses. A particular finish of a horse race corresponds to a particular ordered partition of $H$.

Let $\mathcal{P}_n$ denote the number of ordered partitions of a set of $n$ elements. For example, there are 3 ordered partitions of $\{1, 2\}$:

1. $(\{1\}, \{2\})$

2. $(\{2\}, \{1\})$

3. $(\{1, 2\})$.

In general,

1. $\mathcal{P}_0 = 1$

2. $\mathcal{P}_n = \sum_{k=1}^{n} \binom{n}{k} \mathcal{P}_{n-k}$.

The recursive case partitions the set of ordered partitions of a set with $n$ elements into $n$ subsets according to the number of elements in the *first* subset of the ordered partition.

For each $k \in \{1, 2, \cdots, n\}$, there are $\binom{n}{k}$ ways to select the $k$-set comprising the first part of the partition and $\mathcal{P}_{n-k}$ ways to complete the ordered partition of a set with $n$ elements.

$$
\begin{aligned}
\mathcal{P}_1 &= \binom{1}{1} \mathcal{P}_0 = 1 \\
\mathcal{P}_2 &= \binom{2}{1} \mathcal{P}_1 + \binom{2}{2} \mathcal{P}_0 = 3 \\
\mathcal{P}_3 &= \binom{3}{1} \mathcal{P}_2 + \binom{3}{2} \mathcal{P}_1 + \binom{3}{3} \mathcal{P}_0 = 13 \\
\mathcal{P}_4 &= \binom{4}{1} \mathcal{P}_3 + \binom{4}{2} \mathcal{P}_2 + \binom{4}{3} \mathcal{P}_1 + \binom{4}{4} \mathcal{P}_0 = 75.
\end{aligned}
$$

# Binomial Coefficients & Identities

The following proofs are of exercises in Rosen [5], §6.4: Binomial Coefficients & Identities.

### Exercise 32

Prove the Binomial Theorem using mathematical induction.

*Proof.* **Basis:** $n = 0$: $1 = (x + y)^0 = \begin{pmatrix} 0 \\ 0 \end{pmatrix} x^0 y^0$.

**Induction hypothesis:** $(x + y)^n = \sum_{j=0}^{n} \begin{pmatrix} n \\ j \end{pmatrix} x^{n-j} y^j$.

**Induction:**

$$
\begin{aligned}
(x+y)^{n+1} &= (x+y)(x+y)^n \\
&= (x+y) \left[ \begin{pmatrix} n \\ 0 \end{pmatrix} x^n y^0 + \begin{pmatrix} n \\ 1 \end{pmatrix} x^{n-1} y^1 + \cdots + \begin{pmatrix} n \\ j \end{pmatrix} x^{n-j} y^j + \cdots + \begin{pmatrix} n \\ n \end{pmatrix} x^0 y^n \right] \\
&= \begin{pmatrix} n \\ 0 \end{pmatrix} x^{n+1} y^0 \quad + \quad \begin{pmatrix} n \\ 1 \end{pmatrix} x^n y^1 + \cdots + \begin{pmatrix} n \\ j \end{pmatrix} x^{n+1-j} y^j \quad + \cdots + \quad \begin{pmatrix} n \\ n \end{pmatrix} x^1 y^n \\
&\quad + \qquad\qquad \begin{pmatrix} n \\ 0 \end{pmatrix} x^n y^1 + \cdots + \begin{pmatrix} n \\ j-1 \end{pmatrix} x^{n-(j-1)} y^j + \cdots + \begin{pmatrix} n \\ n-1 \end{pmatrix} x^1 y^n \quad + \quad \begin{pmatrix} n \\ n \end{pmatrix} x^0 y^{n+1} \\
&= \begin{pmatrix} n+1 \\ 0 \end{pmatrix} x^{n+1} y^0 + \begin{pmatrix} n+1 \\ 1 \end{pmatrix} x^n y^1 + \cdots + \begin{pmatrix} n+1 \\ j \end{pmatrix} x^{n+1-j} y^j + \cdots + \begin{pmatrix} n+1 \\ n \end{pmatrix} x^1 y^n + \begin{pmatrix} n+1 \\ n+1 \end{pmatrix} x^0 y^{n+1}
\end{aligned}
$$

The $2^{nd}$ equation uses the induction hypothesis. The sum that is broken over 2 lines is just $x(x+y)^n$ on one line plus $y(x+y)^n$ on the following line. The last line makes use of the fact that $\begin{pmatrix} n+1 \\ 0 \end{pmatrix} = \begin{pmatrix} n \\ 0 \end{pmatrix}$ and $\begin{pmatrix} n+1 \\ n+1 \end{pmatrix} = \begin{pmatrix} n \\ n \end{pmatrix}$, and uses Pascal's identity to form the coefficient of each term as the sum of like terms in the preceding equation. □

# Applications of Recurrence Relations

The following proofs are of exercises in Rosen [5], §8.1: Applications of Recurrence Relations.

Let $\{a_n\}$ be a sequence of real numbers. The **backward differences** of this sequence are defined recursively as follows. The $1^{st}$ **difference** $\nabla a_n$ is

$$\nabla a_n = a_n - a_{n-1}.$$

The $(\mathbf{k+1})^{\mathbf{st}}$ difference $\nabla^{k+1} a_n$ is

$$\nabla^{k+1} a_n = \nabla^k a_n - \nabla^k a_{n-1}.$$

### Exercise 50

Prove that $a_{n-k}$ is expressible in terms of $a_n, \nabla a_n, \nabla^2 a_n, \ldots, \nabla^k a_n$.

*Proof.* Proof by induction on $k$.

**Basis:** $k = 1$: $a_{n-1} = a_n - \nabla a_n$.

**Induction hypothesis:** $a_{n-k}$ is expressible in terms of $a_n, \nabla a_n, \nabla^2 a_n, \ldots, \nabla^k a_n$.

**Induction:** We show that $a_{n-(k+1)}$ is a function of $a_n, \nabla a_n, \nabla^2 a_n, \ldots, \nabla^{k+1} a_n$.

$$
\begin{align}
a_{n-(k+1)} &= a_{(n-1)-k} \tag{13} \\
&= f(a_{n-1}, \nabla a_{n-1}, \nabla^2 a_{n-1}, \ldots, \nabla^k a_{n-1}) \tag{14} \\
&= f(a_n - \nabla a_n, \nabla a_n - \nabla^2 a_n, \ldots, \nabla^k a_n - \nabla^{k+1} a_n). \tag{15}
\end{align}
$$

Eqn. 14 follows from 13 by the induction hypothesis; eqn. 15 follows from 14 by definition of backward differences. $\qquad\square$

# References

[1] Author-related frequently asked questions. url = http://www.ams.org/publications/authors/faq/author-faq.

[2] Using the amsthm package. Version 2.20, url = ftp://ftp.ams.org/ams/doc/amscls/amsthdoc.pdf.

[3] Leonard Gillman. *Writing Mathematics Well*. The Mathematical Association of America, 1987.

[4] David Goss. Some hints on mathematical style. url = https://people.math.osu.edu/goss.3/hint.pdf.

[5] Kenneth H. Rosen. *Discrete Mathematics and Its Applications*. McGraw-Hill, 7th edition, 2007.