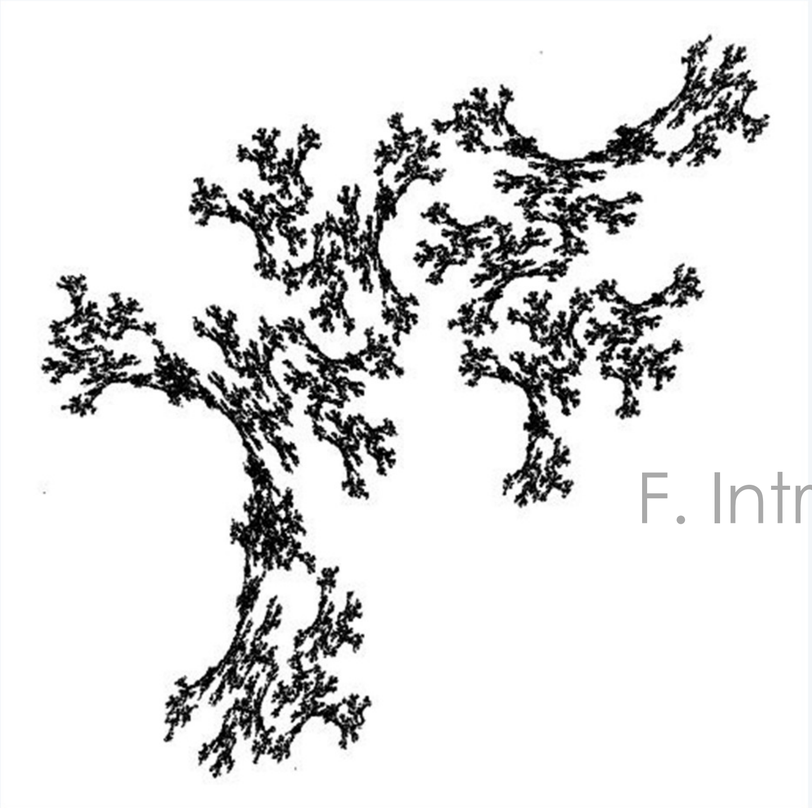
INTRODUCTION TO
DISCRETE STRUCTURES

4.1 Introduction to Proofs

1.1–1.2



INTRODUCTION TO DISCRETE STRUCTURES

F. Introduction to Proofs

- Types of proofs
- Rules of inference
- Lemma’s, theorems and corollaries
- Direct proofs
- Proof by contraposition
- Proof by contradiction

Proof Types

- Proof by evidence
- Proof by picture
- Geometric proof
- Proof by experiment
- Direct Proofs
- Proof by Contraposition
- Proof by contradiction
- Inductive Proofs

4.1 Introduction to Proofs

- Rules of inference
- Lemma’s, theorems and corollaries
- Direct proofs
- Proof by contraposition
- Proof by contradiction

Rules of inference

TABLE 1 Rules of Inference.

Rule of Inference	*Tautology*	*Name*
p $p \rightarrow q$ $\therefore q$	$(p \wedge (p \rightarrow q)) \rightarrow q$	Modus ponens
$\neg q$ $p \rightarrow q$ $\therefore \neg p$	$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$	Modus tollens
$p \rightarrow q$ $q \rightarrow r$ $\therefore p \rightarrow r$	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$	Hypothetical syllogism
$p \vee q$ $\neg p$ $\therefore q$	$((p \vee q) \wedge \neg p) \rightarrow q$	Disjunctive syllogism
p $\therefore p \vee q$	$p \rightarrow (p \vee q)$	Addition
$p \wedge q$ $\therefore p$	$(p \wedge q) \rightarrow p$	Simplification
p q $\therefore p \wedge q$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$	$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$	Resolution

INTRODUCTION TO
DISCRETE STRUCTURES

4.1 Introduction to Proofs

- Rules of inference
- Lemma’s, theorems and corollaries
- Direct proofs
- Proof by contraposition
- Proof by contradiction

Proof

Definition. A mathematical proof of a proposition is a chain of logical deductions leading to the proposition from a base set of axioms.

A broader definition of a proof is that "any statement that can be established to be true" (by example, by picture, by god, by a jury)

We are focusing on mathematical proofs

Lemma

Lemma. is a simple statement that can be shown to be true in just a few steps (like helper functions). Lemma's are used to simplify the steps in the proof.

Simple Lemma. If n^2 is even, then n is even.

An advanced Lemma.

LEMMA 3.1. *Let $A = I - L - U$ be a Q-matrix with the usual splitting. Suppose that T is the Gauss-Seidel iteration matrix defined by $T = (I - L)^{-1}U$ or the Jacobi iteration matrix defined by $T_J = L + U$. Then $\rho(T) = 1$.*

Proof. Let $e = (1, 1, \ldots, 1)^T$. Then $e^T A = 0$, since A is a Q-matrix. This implies $e^T(I - L) = e^T U$ and therefore

$$e^T = e^T\left[U(I - L)^{-1}\right].$$

This implies $\rho([U(I - L)^{-1}]^T) = 1$ by Theorem 2.2, and hence $\rho(U(I - L)^{-1}) = 1$. Since $\operatorname{spectrum}(U(I - L)^{-1}) = \operatorname{spectrum}((I - L)^{-1}U)$, we have $\rho((I - L)^{-1}U) = 1$. Thus $\rho(T) = 1$.

Theorem

Theorem is a major statement that can be shown to be true. Lemma's may be used in proving the theorem.

Example.

THEOREM 2.2. *Let A be a nonnegative matrix. Then:*

(a) *If* $\alpha x \leqslant Ax$ *for some nonnegative vector* x, $x \neq 0$, *then* $\alpha \leqslant \rho(A)$.

(b) *If* $Ax \leqslant \beta x$ *for some positive vector* x, *then* $\rho(A) \leqslant \beta$. *Moreover, if A is irreducible and if*

$$0 \neq \alpha x \leqslant Ax \leqslant \beta x$$

for some nonnegative vector x, *then* $\alpha \leqslant \rho(A) \leqslant \beta$ *and* x *is a positive vector.*

Corollary

Corollary is a result that can be established directly from a theorem that has been proved

An Example.

COROLLARY 4.6. *Let* $A = I - L - U$, $T_J, \tilde{T}_J$ *be as defined in Theorem* 4.5. *Replace* "$T_J, \tilde{T}_J$ *are irreducible matrices*" *by the condition* "$0 < a_{i\,i+1}a_{i+1\,i} < 1$." *Then the conclusion of Theorem* 4.5 *holds.*

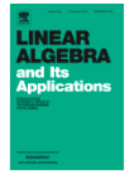
The proof follows from Lemma 3.8.

Proofs in Journals

ELSEVIER

Linear Algebra and its Applications

Volumes 154–156, August–October 1991, Pages 123-143



Modified iterative methods for consistent linear systems

Dedicated to Gene Golub, Richard Varga, and David Young

Ananda D. Gunawardena, S.K. Jain, Larry Snyder

⊞ **Show more**

https://doi.org/10.1016/0024-3795(91)90376-8

Get rights and content

Abstract

In order to solve a linear system *Ax=b*, certain elementary row operations are performed on *A* before applying the Gauss-Seidel or Jacobi iterative methods. It

Workshop

Many theorems assert that a property holds for <u>all elements in a domain</u>, such as the integers or the real numbers

Prove or disprove. If $x > y$, where x and y are positive integers, then $x^2 > y^2$

Prove or disprove. For all real numbers x and y, if $x > y$, then $x^2 > y^2$

INTRODUCTION TO
DISCRETE STRUCTURES

4.1 Introduction to Proofs

- Rules of inference
- Lemma's, theorems and corollaries
- Direct proofs
- Proof by contraposition
- Proof by contradiction

Definition

A **direct proof** of a conditional statement $p \rightarrow q$ is constructed when the first step is the assumption that p is true;

subsequent steps are constructed using **rules of inference**

Example.

- If n and m are perfect squares, then nm is also a perfect square

- There exist an integer n such that $n^2 + n + 41$ is not prime

workshop

Prove that If $0 \leq x \leq 2$, then $-x^3 + 4x + 1 > 0$

A buggy Proof

Bogus Claim: $1/8 > 1/4$.

Bogus proof.

$$
\begin{aligned}
3 &> 2 \\
3\log_{10}(1/2) &> 2\log_{10}(1/2) \\
\log_{10}(1/2)^3 &> \log_{10}(1/2)^2 \\
(1/2)^3 &> (1/2)^2,
\end{aligned}
$$

A valid proof?

If a and b are two equal real numbers, then $a = 0$

Facts about even and odd integers used in Proofs

Even integer

- An integer n is even, if it can be written as $n = 2k$, for some integer k

Odd Integer

- An integer n is odd, if it can be written as $n = 2k + 1$, for some integer k

workshop

Exercise 1. The sum of any two even integers is also even

Exercise 2. The square of an odd integer is also odd

Exercise 3. The sum of any two odd integers is even

Exercise 4. The sum of an even integer and odd integer is odd

Exercise 5. The square of a non-zero even integer can be divided by 4

Definitions

A real number r is rational if r can be expressed as $r = p/q$, where p and q are integers and $q \neq 0$

Direct Proofs.

The sum of two rational numbers is also rational.

The product of two rational numbers is also rational.

Question. Is the sqrt of a rational number, rational?

INTRODUCTION TO
DISCRETE STRUCTURES

4.1 Introduction to Proofs

- Rules of inference
- Lemma's, theorems and corollaries
- Direct proofs
- Proof by contraposition
- Proof by contradiction

Proof by Contraposition

Use. $p \Rightarrow q$ is equivalent to $\neg q \Rightarrow \neg p$

Why. $p \Rightarrow q$ might be harder to prove, and so prove $\neg q \Rightarrow \neg p$

Example. Suppose n is an integer. Prove that if $3n + 2$ is odd, then n is also odd.

workshop

if n is an integer and n^2 is odd, then n is odd.

INTRODUCTION TO
DISCRETE STRUCTURES

4.1 Introduction to Proofs

- Rules of inference
- Lemma’s, theorems and corollaries
- Direct proofs
- Proof by contraposition
- Proof by contradiction

The concept

Suppose we want to prove p

Assume that p is false. Then obtain a contradiction.

That is, a false assumption leads to a falsehood (F ➔ F) and hence the statement must be true.

Challenging proof

Show that is p is irrational, then sqrt(p) is also irrational

INTRODUCTION TO
DISCRETE STRUCTURES

4.1 Introduction to Proofs

- Rules of inference
- Lemma's, theorems and corollaries
- Direct proofs
- Proof by contraposition
- Proof by contradiction

INTRODUCTION TO
DISCRETE STRUCTURES

4.1 Introduction to Proofs

1.1–1.2