Lecture 8.

Proofs (continuation). Sect. 1.5, 1.~~6~~4, 1.7

$T \wedge P \Leftrightarrow P$; $F \vee P \Leftrightarrow P$.

1. Quiz 3.

2. Selected problems from HW 4.

Sect. 1.4

Pr. 4 ~~(a)~~

Elem. P_1 - Plum is guilty

P_2 Crime in kitchen

— " at midnight

P_3, P_4 Weapon - candlestick

P_5 Crime in library

(i) $\sim P_1 \Rightarrow P_2$

(ii) $P_3 \Rightarrow P_1$

(iii) $P_1 \Leftrightarrow \sim P_4$

(iv) $(P_4 \wedge \sim P_5) \vee (\sim P_4 \wedge P_5)$ - alternative disjunction

(v) $\sim P_1$ - Scarlet is guilty — " —

(a) $\cancel{P_4} P_5 \underset{}{\Rightarrow} \sim P_2 \underset{(i)}{\Rightarrow} P_1 \; ; \underset{(viii)}{\Rightarrow} \sim P_4$

(b) $\cancel{\sim P_5 \underset{(iv)}{\Rightarrow} \sim P_4 \underset{(iii)}{\Rightarrow} P_1 \wedge P_4}$ $\sim P_5 \underset{(iv)}{\Rightarrow} P_4 \underset{(iii)}{\not\Rightarrow} \sim P_1$

$\underset{(i)}{\Rightarrow} P_2$

(c) $\sim P_3 \wedge \sim P_4 \underset{(iii)}{\not\Rightarrow} P_1 \wedge P_5$

(d) $P_3 \underset{(ii)}{\Rightarrow} P_1$

	Criminal	Place	Time	Weapon
a	Plum	Library	?	Revolver
b	~~Plum~~ Scarlet	~~Library~~ Kitchen	?	~~[illegible]~~ Candelstick
c	Plum	Library	$\sim$ 12pm	Revolver
d	Plum	Conservat.	12pm	Revolver

n as **proof by exhaustion** consists of an examination
tement to be proved may have any form P. For exam-
er x in the closed interval $[0, 5]$ has a certain property,
$x = 0$, $0 < x < 5$, and $x = 5$. The exhaustive method
e above, and in the proof of Theorem 1.1.1, where we
ns of truth values for two propositions. Naturally, the
appealing only when the number of cases is small, or
can be systematically handled. Care must be taken to
have been considered.

mber. Prove that $-|x| \le x \le |x|$.

value of x is defined by cases ($|x| = x$ if $x \ge 0$;
f will proceed by cases.)

hen $|x| = x$. Since $x \ge 0$, we have $-x \le x$. Hence,
h is $-|x| \le x \le |x|$ in this case.
hen $|x| = -x$. Since $x < 0$, $x \le -x$. Hence, we have
$(-x) \le x \le -x$, which is $-|x| \le x \le |x|$.

$-|x| \le x \le |x|$. ■

es of truly exhausting proofs involving great numbers of
pel and Wolfgang Haken of the University of Illinois
ur-Color Theorem. The original version of their proof of
ecture contains 1,879 cases and took $3\frac{1}{2}$ years to develop.*
s by exhaustion with cases so similar in reasoning that
ngle case and alert the reader with the phrase "without
ngle case and alert the reader with the phrase "without
case represents the essence of arguments for the other

ne integers m and n, one of which is even and the other
$4k + 1$ for some integer k.

egers. Without loss of generality, we may assume that m
ase where m is odd and n is even is similar.) Then there
h that $m = 2s$ and $n = 2t + 1$. Therefore, $m^2 + n^2$
$^2 + 4t + 1 = 4(s^2 + t^2 + t) + 1$. Since $s^2 + t^2 + t$ is an
rm $4k + 1$ for some integer k. ■

ves coloring regions or countries on a map in such a way that no two
color. It states that four colors are sufficient, no matter how intertwined
at the proof depended so heavily on the computer for checking cases
of proof. Verifying the 1,879 cases required more than 10 billion cal
d whether there might have been at least one error in a process so
d out by one human being in a lifetime. Haken and Appel's proof has
r-Color Theorem is accepted; but the debate about the role of comput

Exercises 1.4

1.5: contrapos, bicond. 2 ways

1. Analyze the logical form of each of the following statements and construct just the outline of a proof. Since the statements may contain terms with which you are not familiar, you should not (and perhaps could not) provide any details of the proof.
   - ☆ **(a)** Outline a direct proof that if $(G, *)$ is a cyclic group, then $(G, *)$ is abelian.
   - **(b)** Outline a direct proof that if **B** is a nonsingular matrix, then the determinant of **B** is not zero.
   - **(c)** Suppose A, B, and C are sets. Outline a direct proof that if A is a subset of B and B is a subset of C, then A is a subset of C.
   - **(d)** Outline a direct proof that if the maximum value of the differentiable function f on the closed interval $[a, b]$ occurs at x_0, then either $x_0 = a$ or $x_0 = b$ or $f'(x_0) = 0$.
   - **(e)** Outline a direct proof that if **A** is a diagonal matrix, then **A** is invertible whenever all its diagonal entries are nonzero.
2. A theorem of linear algebra states that if **A** and **B** are invertible matrices, then the product **AB** is invertible. As in Exercise 1, outline
   - **(a)** a direct proof of the theorem.
   - **(b)** a direct proof of the converse of the theorem.
3. Verify that $[(\sim B \Rightarrow M) \wedge \sim L \wedge (\sim M \vee L)] \Rightarrow B$ is a tautology. See the example on page 30.
4. These facts have been established at a crime scene.
   - **(i)** If Professor Plum is not guilty, then the crime took place in the kitchen.
   - **(ii)** If the crime took place at midnight, Professor Plum is guilty.
   - **(iii)** Miss Scarlet is innocent if and only if the weapon was not the candlestick.
   - **(iv)** Either the weapon was the candlestick or the crime took place in the library.
   - **(v)** Either Miss Scarlet or Professor Plum is guilty.

   Use the above and the additional fact(s) below to solve the case. Explain your answer.
   - ☆ **(a)** The crime lab determines that the crime took place in the library.
   - **(b)** The crime lab determines that the crime did not take place in the library.
   - **(c)** The crime lab determines that the crime was committed at noon with the revolver.
   - **(d)** The crime took place at midnight in the conservatory. (Give a complete answer.)
5. Let x and y be integers. Prove that
   - **(a)** if x and y are even, then $x + y$ is even.
   - **(b)** if x is even, then xy is even.
   - **(c)** if x and y are even, then xy is divisible by 4.
   - **(d)** if x and y are even, then $3x - 5y$ is even.
   - **(e)** if x and y are odd, then $x + y$ is even.

5i) $x = 2m,\ y = 2n+1 \Rightarrow xy = 4mn + 2m =$

$= 2(2mn+m) = 2p \Rightarrow xy$ - even.

7i) $\mathbb{Z}$ - integer numbers

$a>0 \wedge b>0 \wedge (ab=1) \Rightarrow a \le 1 \wedge b \le 1 \Rightarrow$

$0<a\le 1 \wedge 0<b\le 1 \Rightarrow a=b=1.$

7b) $ab \mid c \Leftrightarrow c = abq \Rightarrow a \mid c$

$a \mid b \Leftrightarrow b = aq$ for some $q \in \mathbb{Z}$

8a) $\forall\, n \in \mathbb{N} \Rightarrow n^2+n+3$ odd

2 cases n - odd $\vee$ n - even

$$\left.\begin{aligned} n=2k+1 &\Rightarrow n^2+n = (\text{odd})+(\text{odd}) = \text{even} \\ n=2k &\Rightarrow n^2+n = (\text{even})+(\text{even}) = \text{even} \end{aligned}\right\} \Rightarrow$$

n^2+n+3 - odd as a sum of even and odd

9a) $\dfrac{x+y}{2} \ge \sqrt{xy} \Leftrightarrow \dfrac{(x+y)^2}{4} \ge xy$

~~$\wedge\, x>y \wedge$~~   since $x>0, y>0$

$x>0,\ y>0$ ~~Theorem: $a \ge b$~~

Theorem. $(a>0 \wedge b>0) \Rightarrow (a \ge b \Leftrightarrow a^2 \ge b^2)$

$$\frac{x^2+y^2+2xy}{4} \geq 2x \Leftrightarrow (x-y)^2 \geq 0.$$

9d) $x^3+2x^2<0 \Rightarrow 2x+5<11$

$x^2(x+2)<0 \Leftrightarrow x\neq 0 \wedge x+2<0 \Leftrightarrow x<-2$

$\Rightarrow 2x+5<1$

1.5, 3g) $8 \nmid x^2-1 \Rightarrow x$ - even.

$P \Rightarrow Q$

Contraposition: $\sim Q \Rightarrow \sim P$.

Let $\sim Q$ is True: x is odd: $x=2k+1$

$\Rightarrow x^2-1 = 4k^2+4k = 4k(k+1)$

(k - even $\vee$ $k+1$ - odd) $\Rightarrow$

$\underline{P}_1$: ~~$k(k+1)$~~ $2 \mid k(k+1)$

$(P_1 \wedge \sim Q) \Rightarrow 8 \mid x^2-1$. Contradiction.

4d. xy - even $\Rightarrow x$ - even $\vee$ y - even

$P \Rightarrow Q$. $\sim Q \Rightarrow \sim P$

$\sim Q$: $x=2k+1 \wedge y=2k+1 \Rightarrow xy$ - odd $(\sim \underline{P})$.

4 c) $x^3+x>0 \Rightarrow x>0$. $P \Rightarrow Q$

$\mathbb{R}$ $\sim Q: x \le 0$

$\sim Q \Rightarrow x^3 \le 0 \Rightarrow x^3+x \le 0$ contradiction

~~$\sim Q$~~

Extra Problems.

1. a_i - # of handshakes of i-th person.

$a = a_1 + \dots + a_N$.

If B - the number of all handshakes

then $a = 2B$.

(2 persons at each hand shake!).

$a = a_{even} + a_{odd}$

a_{even} sum of h.s. for people with even h.s.

a_{odd} - —— " —— " —— odd h.s.

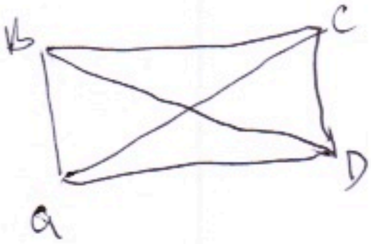
---

a-even, a_{even}-even $\Rightarrow a_{odd}$ is even.

a_{odd} - ~~by~~ sum of odd numbers $\Rightarrow$ the number of these numbers (people) is $\boxed{\text{even}}$

☒

2. Theorem. At a rectangular $ABCD$ diagonal $AC = BD$.



$P \Rightarrow Q$

$P = P_1 \wedge P_2$ ~~P_1 - Parallelogram~~

P_1 - $\square ABCD$ - parallelogram

P_2 $\angle BAD = \angle ADC$ - right.

Kea idea: Consider right triangles ABD and ACD.

Proof. 1) Intermediate proposition

$R \Rightarrow S$

Corresponding legs at right triangles are eques

R

$\Rightarrow$ triangles are congruent. S

2) $P_1 \Rightarrow R_1$ - (opposite sides are equal)

Specialization of R_1: $AB = CD$,

R_2 - AD is joint.

3) $R \equiv R_1 \wedge R_2 = T \Rightarrow S$.

4) $S \Rightarrow$ hypotenuses are equal ($AC = BD$). $\square$

We'll try to understand how to prove Theorems

- analyse specific methematical proofs (1)
- analyse logical tools (2)
- solve problems on proofs (3)

Properties of Convolution can be ~~a~~ usefull

~~In paper~~

Proposition 1.1. Next connectives are equivalent to Convolution $P \Rightarrow Q$

(i) $\sim Q \Rightarrow \sim P$; (contraposition)

(ii) $(P \wedge \sim Q) \Rightarrow \sim P$;

(iii) $(P \wedge \sim Q) \Rightarrow Q$;

(iv) $(P \wedge \sim Q) \Rightarrow F$

Contradiction (any identical False), i.e. F

- How to prove these equivalencies?

- How to use them?

Examples.

__Theorem.__ $\sqrt{2}$ is an irrational.

Formalization of the statement.

There are no such natural m, n that $2m^2 = n^2$. Q

$2 = \frac{n^2}{m^2}$.

Proof. Let ~~such~~ suppose m, n exist and (m,n) have ~~then~~. no joint divisor $\neq 1$.

$(2m^2 = n^2) \Rightarrow 2 \mid n^2 \Rightarrow 2 \mid n \Rightarrow 4 \mid n^2 \Rightarrow 2 \mid m^2$

$\sim Q$ $\Rightarrow 2 \mid m \Rightarrow$ 2 is an joint divisor for m and n.

__Contradiction.__

Theorem. There are infinitely many different prime numbers. Q

Proof. ~~Known~~ $\sim Q$ Let the set of prime numbers is

$p_1, p_2, p_3, \dots, p_k$ are all prime numbers

Let us consider

$$n = p_1 \cdots p_k + 1.$$

R_1 - $n > p_j$ for all $j \Rightarrow R_2$ - n is not prime

R_3 $p_j \nmid n$ for all j since $p_j \mid (n-1)$,

and $n, n-1$ can't ~~be prim~~
have join factors $\neq 1$.

$\Rightarrow \nexists R_2$ Contradiction

Division with a remainder.

$a, b \in \mathbb{Z}$

$b = aq + r$, $0 \le r < |a|$.

q - quotien, r - remainder

Simple problems.

1. For $b \in \mathbb{N}$, $a = 6$, the remainder in the division on 6 is equal 5.

What will be the remainder in the division a on 3?

2

2. Which remainders are possible in the division $b = n^2$ on 5.

[Hint]. It's enough to consider $n = 0, 1, 2, 3, 4$

$n = 5k + r$, $n^2 = (5k+r)^2$.

Answer: 0, 1, 4.