Lecture - 11

Validity using truth tables: Let A and B be two statement formulas. We say that "B *logically follows from* A" or "B *is a valid conclusion (consequence)* of the premise A" iff $A \to B$ is a tautology, i.e., $A \implies B$.

The above can be extended for a set of premises as follows; we say that from a set of premises $\{H_1, H_2, \cdots, H_m\}$ a conclusion C follows logically iff

$$H_1 \wedge H_2 \wedge \cdots \wedge H_m \implies C \tag{1}$$

Let $P_1, P_2, \cdots, P_n$ be all the atomic variables appearing in the premises $H_1, H_2, \cdots, H_m$ and tge conclusion C. By looking at truth table one can immediately tell whether (1) holds or not.

We look for the rows in which all the premises $H_1, H_2, \cdots, H_m$ have the truth value T. If, for every such row, C also has the truth value T, then (1) holds.

Alternatively, we may look for rows in which the truth value of C is F. If, in every such row, at leat one of the truth values of $H_1, H_2, \cdots, H_m$ is F, then (1) holds.

Rule **P**: A premise may be introduced at any point in the derivation.
Rule **T**: A formula S may be introduced in a derivation if S is tautologically implied by any one or more of the preceding formulas in the derivation.

Rule **CP**: If we can derive S from R and a set of premises, then we can derive $R \to S$ from the set of premises alone.

Rule **CP** follows also from the equivalence $(P \wedge R) \to S \iff P \to (R \to S)$.

Let P be the conjunction of the set of premises and let R be any formula. Then the above equivalence says that if we include R as an additional premise and if S is derived from $P \wedge R$, then $R \to S$ can be derived from the premise P alone.

Example: Prove that $R \to S$ can be derived from the premise $P \to (Q \to S), \neg R \vee P$, and Q.

$\{1\}$	(1)	$\neg R \vee P$	**P**
$\{2\}$	(2)	R	**P** (assumed premise)
$\{1,2\}$	(3)	P	**T**, (1), (2), and I_{10}
$\{4\}$	(4)	$P \to (Q \to S)$	**P**
$\{1,2,4\}$	(5)	$Q \to S$	**T**, (3), (4), and I_{11}
$\{6\}$	(6)	$Q \to R$	**P**
$\{1,2,4,6\}$	(7)	S	**T**, (5), (6), and I_{11}
$\{1,4,6\}$	(8)	$R \to S$	**CP**

Consistency of premises and Indirect Method of proofs. We say that a set of formulas $H_1, H_2, \cdots, H_m$ is consistent if their conjunction has the truth value T for some assignment of the truth values to the atomic variables appearing in $H_1, H_2, \cdots, H_m$.

If, for every assignment of the truth values to the atomic variables, at least one of the formulas $H_1, H_2, \cdots, H_m$ is false, so that their conjunction is identically false, then the formulas $H_1, H_2, \cdots, H_m$ are called inconsistent.

Equivalently, a set of formulas $H_1, H_2, \cdots, H_m$ is inconsistent if their conjunction implies a contradiction, i.e.,

$$H_1 \wedge H_2 \wedge \cdots \wedge H_m \implies R \wedge \neg R,$$

where R is any formula.

Note here that, $R \wedge \neg R$ is a contradiction, and it is necessary and sufficient for the implication that $H_1 \wedge H_2 \wedge \cdots \wedge H_m$ be a contradiction.
We have introduced the notion of consistency, because it is used in a procedure called proof by contradiction or indirect method of proof.

In order to show that a conclusion C follows logically from the premises $H_1, H_2, \cdots, H_m$, we shall assume that C is false, and consider $\neg C$ as an additional premise. If the new set of premises is inconsistent, so that they imply a contradiction, then the assumption that $\neg C$ is true does not hold simultaneously with $H_1 \wedge H_2 \wedge \cdots \wedge H_m$ being true. Therefore, C is true whenever $H_1 \wedge H_2 \wedge \cdots \wedge H_m$ is true, and hence the conclusion C follows logically from the premises $H_1, H_2, \cdots, H_m$.

Example 1: Prove that $\neg(P \wedge Q)$ follows from $\neg P \wedge \neg Q$.

We introduce $\neg\neg(P \wedge Q)$ as an additional premises and prove that this additional premise leads to a contradiction.

$\{1\}$	(1)	$\neg\neg(P \wedge Q)$	Rule **P**(assumed)
$\{1\}$	(2)	$P \wedge Q$	Rule **T**, (1), and E_1
$\{1\}$	(3)	P	Rule **T**, (2), and I_1
$\{4\}$	(4)	$\neg P \wedge \neg Q$	Rule **P**
$\{4\}$	(5)	$\neg P$	Rule **T**, (4), and I_1
$\{1, 4\}$	(6)	$P \wedge \neg P$	Rule **T**, (3), (5), and I_9

Example 1: Show that the following premises are inconsistent.

(1) If Jack misses many classes through illness, then he fails high school.
(2) If Jack fails high school, then he is uneducated.
(3) If Jack reads a lot of book, then he is not uneducated.
(4) Jack misses many classes through illness and reads a lot of book.

E : Jack misses many classes.
S : Jack fails high school.
A : Jack reads a lot of book.

H : Jack is uneducated.

The given premises are

$$E \to S, S \to H, A \to \neg H, E \wedge A.$$

$\{1\}$	(1)	$E \to S$	Rule **P**
$\{2\}$	(2)	$S \to H$	Rule **P**
$\{1,2\}$	(3)	$E \to H$	Rule **T**, (1), (2) and I_{13}
$\{4\}$	(4)	$A \to \neg H$	Rule **P**
$\{4\}$	(5)	$H \to \neg A$	Rule **T**, (4), and E_{18}
$\{1,2,4\}$	(6)	$E \to \neg A$	Rule **T**, (3), (5), and I_{13}
$\{1,2,4\}$	(7)	$\neg E \vee \neg A$	Rule **T**, (6), and E_{16}
$\{1,2,4\}$	(8)	$\neg(E \wedge A)$	Rule **T**, (7), and E_8
$\{9\}$	(9)	$E \wedge A$	Rule **P**
$\{1,2,4,9\}$	(10)	$(E \wedge A) \wedge \neg(E \wedge A)$	Rule **T**, (8), (9), and I_9

The method of proof by contradiction is sometimes convenient. However, it can be eliminated and replaced by a conditional proof **CP**. Observe that

$$P \to (Q \wedge \neg Q) \implies P.$$

In the proof by contradiction we show that

$$H_1, H_2, \cdots, H_m \implies C$$

by showing that

$$H_1, H_2, \cdots, H_m, \neg C \implies R \wedge \neg R.$$

Now the above can be converted to the following by using **CP**

$$H_1, H_2, \cdots, H_m \implies \neg C \to (R \wedge \neg R).$$

Now the first and last implications with E_1, together yield

$$H_1, H_2, \cdots, H_m \implies C.$$

Automatic Theorem Proving: We now see the rules of inference theory for statement calculus and describe a process of derivation which can be conducted mechanically. The formulation given earlier could not be used for this purpose because the construction of derivation depends heavily upon the skill, experience, and inenuity of the person to make the righr decision at every step.

- Rule **P** permits the introduction of a premise at any point in the derivation, but does not suggest either the premise or the step at which it should be introduced.
- Rule **T** allows us to introduce any formula which follows from the previous steps. However, there is no choice of such formula, nor is there any guidance for the use of any particular equivalence.
- Similarly, rule **CP** does not tell anything about the stages at which an antecedent is to be introduced as an assumed premise, nor does it indicate the stage at which it is again incorporated into the conditional.

At every step, such decisions are taken from a large number of alternatives, with the ultimate aim of reaching the conclusion. Thus, such a process is far from mechanical.

We shall now give a set of rules and a process which allow to construct each step derivation in a specified manner without recourse to any ingenuity and finally arrive at a last step which clearly tells whether a given conclusion follows from the premises or not. Therefore, this process is not only mechanical, but is also a full decision process of validity.

We now described our system which consists of certain rules, an axiom schema, and rules of well formed sequents and formulas;

(1) **Variables:** The capital letters $A, B, C, \cdots, P, Q, R, \cdots$ are used as statement variables. They are also used as statement formulas; however, in such cases the context will clearly indicate this usage.
(2) **Connectives:** The connectives $\neg, \wedge, \vee, \rightarrow$, and $\leftrightarrow$ appear in the formula with the order of the precedence as given, namely., $\neg$ has the highest precedence, followed by $\wedge$, and so on. The concept of well-formed formula remains same as discussed earlier with an additional assumption of precedence and associativity of the connectives need in order to reduce the number of parentheses appearing in the formula.
(3) **Strings of formula:** A string of formulas is defined as follows;
   (a) Any formula is a string of formulas.
   (b) If α and β are strings of formula, then α, β and β, α are strings of formulas.
   (c) Only those strings which are obtained by the steps above are strings of formulas, with the exception of the empty string which is also a string of formulas.
   Here the order in which the formulas appear in a string does not matter; $A, B, C; B, C, A; C, B$ are the same.
(4) **Sequents:** If α and β are strings of formulas, then $\alpha \xrightarrow{s} \beta$ is called a sequent in which α is denoted the antecedent and β the consequent of the sequent.

   A sequent $\alpha \xrightarrow{s} \beta$ is true iff either at least one of the formulas of antecedent is false or at least one of the formulas of the consequent is true.

   Thus, $A, B, C \xrightarrow{s} D, E, F$ is true iff $A \wedge B \wedge C \rightarrow D \vee E \vee F$ is true. In this sense the symbol $\xrightarrow{s}$ is generalization of the connective $\rightarrow$ to strings of formulas.

   Similarly, we use the symbol $\overset{s}{\Rightarrow}$ applied to the string of formulas, as a generalization of the symbol $\implies$. Thus, $A \implies B$ means $A \rightarrow B$ is a tautology and $\alpha \overset{s}{\Rightarrow} \beta$ means $\alpha \xrightarrow{s} \beta$ is true.
(5) **Axiom Schema:** If α and β are strings of formulas such that every formula in both α and β are variables only, then the sequent $\alpha \xrightarrow{s} \beta$ is an axiom iff α and β have at least one variable in common. e.g., $A, B, C \xrightarrow{s} P, B, R$, where A, B, C, P, and R are variables, is an axiom.
(6) **Theorem:** The following sequents are theorem of our system.
   (a) Every axiom is a theorem.
   (b) If a sequent α is a theorem and a sequent β results from α through the use of one of the 10 rules of the systems which are given below, then β is a theorem.
   (c) Sequents obtained by the above two are the only theorems.

(7) **Rules:** The following rules are used to combine formulas within stringgs by introducing connectives. Correspondin to each of the connectives there are two rules, one for the introduction of the connective in the antecedent and the other for its introduction in the consequent. In the description of these rules, $\alpha, \beta, \gamma, \cdots$ are strings of formulas while X and Y are formulas to which the connectives are applied.

Antecedent Rules

Rule $\neg\Longrightarrow$: If $\alpha, \beta \overset{s}{\Rightarrow} X, \gamma,$ then $\alpha, \neg X \overset{s}{\Rightarrow} \gamma.$

Rule $\wedge\Longrightarrow$: If $X, Y, \alpha, \beta \overset{s}{\Rightarrow} \gamma,$ then $\alpha, X \wedge Y, \beta \overset{s}{\Rightarrow} \gamma.$

Rule $\vee\Longrightarrow$: If $X, \alpha, \beta \overset{s}{\Rightarrow} \gamma,$ and $Y, \alpha, \beta \overset{s}{\Rightarrow} X, \gamma,$ then $\alpha, X \vee Y, \beta \overset{s}{\Rightarrow} \gamma.$

Rule $\rightarrow\Longrightarrow$: If $Y, \alpha, \beta \overset{s}{\Rightarrow} \gamma,$ and $\alpha, \beta \overset{s}{\Rightarrow} X, \gamma,$ then $\alpha, X \rightarrow Y, \beta \overset{s}{\Rightarrow} \gamma.$

Rule $\leftrightarrow\Longrightarrow$: If $X, Y, \alpha, \beta \overset{s}{\Rightarrow} X, \gamma,$ and $\alpha, \beta \overset{s}{\Rightarrow} X, Y, \gamma$ then $\alpha, X \leftrightarrow Y, \beta \overset{s}{\Rightarrow} \gamma.$

Consequent Rules

Rule $\Longrightarrow\neg$: If $X, \alpha, \overset{s}{\Rightarrow} \beta, \gamma,$ then $\alpha \overset{s}{\Rightarrow} \beta, \neg X, \gamma.$

Rule $\Longrightarrow\wedge$: If $\alpha \overset{s}{\Rightarrow} X, \beta, \gamma,$ and $\alpha \overset{s}{\Rightarrow} Y, \beta, \gamma,$ then $\alpha \overset{s}{\Rightarrow} \beta, X \wedge Y, \gamma.$

Rule $\Longrightarrow\vee$: If $\alpha, \beta \overset{s}{\Rightarrow} X, Y, \beta, \gamma,$ then $\alpha \overset{s}{\Rightarrow} \beta, X \vee Y, \gamma.$

Rule $\Longrightarrow\rightarrow$: If $X, \alpha, \beta \overset{s}{\Rightarrow} Y, \beta, \gamma,$ then $\alpha \overset{s}{\Rightarrow} \beta, X \rightarrow Y, \gamma.$

Rule $\Longrightarrow\leftrightarrow$: If $X, \alpha, \overset{s}{\Rightarrow} Y, \beta, \gamma,$ and $Y, \alpha \overset{s}{\Rightarrow} X, \beta, \gamma$ then $\alpha \overset{s}{\Rightarrow} \beta, X \leftrightarrow Y, \gamma.$

The order in which the formulas and strings of formulas appear in a string in any of the rules is not important.

The system which have described above is equivalent to the one described in the previous class except that the procedure and techniques of derivation are different. However, this difference does not affect the validity of an argument.

We now see how this procedure can be used in practice.

In the method which was introduced in the previous class, we showed that a conclusion C follows from the premises $H_1, H_2, \cdots, H_m$ by a derivation whose last step was C, and $H_1, H_2, \cdots, H_m$ were introduced at various stages by using the rule **P**. This method essentially means showing

(2) $$H_1, H_2, \cdots, H_m \implies C.$$

Another way of stating (2) is

(3) $$H_1 \rightarrow (H_2 \rightarrow (H_3 \cdots (H_m \rightarrow C) \cdots))$$

is a tautology (because??)

This new formulation is premise-free, so that in order to show that C follows from $H_1, H_2, \cdots, H_m$, we establish that

$$(4) \qquad \overset{s}{\to} H_1 \to (H_2 \to (H_3 \cdots (H_m \to C) \cdots))$$

is a theorem. We must show that

$$(5) \qquad \overset{s}{\Rightarrow} H_1 \to (H_2 \to (H_3 \cdots (H_m \to C) \cdots)).$$

Our procedure involves showing (4) to be a theorem. For this purpose, we first assume (5) and then show that this is or is not justified. This task is done by working backword from (5), using tje rules and showing that (5) holds if some simpler sequent is a theorem. We continue going backward until we arive at the simplest possible sequents, i.e., those which do not have any connectives. If these sequents are axioms, then we have justified our assumption in (5). If at least one of the simplest sequents is not an axiom, then the assumption in (5) is not justified and C does not follow from $H_1, H_2, \cdots, H_m$.

We now demonstrate the above process by means of some examples.

Example 1: Show that $P \vee Q$ follows from P.

We need to show that

$$\begin{array}{lll} (1) & \overset{s}{\Rightarrow} & P \to (P \vee Q) \\ (1) & \text{if } (2) & P \overset{s}{\Rightarrow} (P \vee Q) \ (\Longrightarrow\to) \\ (2) & \text{if } (3) & P \overset{s}{\Rightarrow} P, Q \ (\Longrightarrow \vee) \end{array}$$

We first eliminate the connective $\to$ in (1). Using the rule $\Longrightarrow\to$ we have "if $P \overset{s}{\Rightarrow} P \vee Q$ then $\overset{s}{\Rightarrow} P \to (P \vee Q)$". Here, we have named $P \overset{s}{\Rightarrow} P \vee Q$ by (2). Each line of derivation thus introduces the name as well as gives a rule. Note also that "(1) if (2)" means "(2) then (1)." The chain of arguments is then given by (1) holds if (2), and (2) holds if (3). Finally, (3) is a theorem, because it is an axiom. The actual derivation is simply a reversal of these steps in which (3) is an axiom that leads to $\overset{P}{\Rightarrow}\to (P \vee Q)$ as shown

$$\begin{array}{ll} (a) & P \overset{s}{\Rightarrow} P, Q, \ \text{Axiom} \\ (b) & P \overset{s}{\Rightarrow} P \vee Q, \ \text{Rule } (\Longrightarrow \vee), \text{(a)} \\ (c) & \overset{s}{\Rightarrow} P \to (P \vee Q), \ \text{Rule } (\Longrightarrow\to), \text{(b)} \end{array}$$

Example 2: Show that $\overset{s}{\Rightarrow} (\neg Q \wedge (P \vee Q)) \to \neg P$.

$$
\begin{array}{ll}
(1) & \overset{s}{\Rightarrow} (\neg Q \wedge (P \to Q)) \to \neg P \\
(1) & \text{if } (2)\ \neg Q \wedge (P \to Q) \overset{s}{\Rightarrow} \neg P\ (\Longrightarrow\!\to) \\
(2) & \text{if } (3)\ \neg Q, P \to Q \overset{s}{\Rightarrow} \neg P\ (\wedge \Longrightarrow) \\
(3) & \text{if } (4)\ P \to Q \overset{s}{\Rightarrow} \neg P, Q,\ (\neg\Longrightarrow) \\
(4) & \text{if } (5) Q \overset{s}{\Rightarrow} \neg P, Q,\ \text{and } (6) \overset{s}{\Rightarrow} P, \neg P, Q\ (\to\Longrightarrow) \\
(5) & \text{if } (7)\ P, Q \overset{s}{\Rightarrow} Q\ (\Longrightarrow \neg) \\
(6) & \text{if } (8)\ P \overset{s}{\Rightarrow} P, Q\ (\Longrightarrow \neg)
\end{array}
$$

Now (7) and (8) are axioms, hence the theorem (1) follows. We omit the derivation, which is easily obtained by starting with the axiom (7) and (8) and retracing the steps.

Example 3: Does P follows from $P \vee Q$?

We investigate whether $\overset{s}{\to} (P \vee Q) \to P$ is a theorem. Assume (1) $\overset{s}{\Rightarrow} (P \vee Q) \to P$.

$$
\begin{array}{ll}
(1) & \text{if } (2)\ P \vee Q \overset{s}{\Rightarrow} P\ (\Longrightarrow\!\to) \\
(2) & \text{if } (3)\ P \overset{s}{\Rightarrow} P \text{ and } (4)\ Q \overset{s}{\Rightarrow} P\ (\vee \Longrightarrow)
\end{array}
$$

Note that (3) is an axiom, but (4) is not. Hence P does not follow from $P \vee Q$.

Example 4: Show that $S \vee R$ is tautologically implied by $(P \vee Q) \wedge (P \to R) \wedge (Q \to S)$.

$$
\begin{array}{ll}
(1) & \overset{s}{\Rightarrow} ((P \vee Q) \wedge (P \to R) \wedge (Q \to S)) \to (S \vee R) \\
(1) & \text{if } (2)\ (P \vee Q) \wedge (P \to R) \wedge (Q \to S) \overset{s}{\Rightarrow} (S \vee R)\ (\Longrightarrow\!\to) \\
(2) & \text{if } (3)\ (P \vee Q) \wedge (P \to R) \wedge (Q \to S) \overset{s}{\Rightarrow} S, R\ (\Longrightarrow \vee) \\
(3) & \text{if } (4)\ (P \vee Q), (P \to R), (Q \to S) \overset{s}{\Rightarrow} S, R\ (\vee\Longrightarrow \text{ twice}) \\
(4) & \text{if } (5)\ P, P \to R, Q \to S \overset{s}{\Rightarrow} S, R,\ \text{and } (6)\ Q, P \to R, Q \to S \overset{s}{\Rightarrow} S, R\ (\vee \Longrightarrow) \\
(5) & \text{if } (7)\ P, R, Q \to S \overset{s}{\Rightarrow} S, R \text{ and } (8)\ P, Q \to S \overset{s}{\Rightarrow} P, S, R\ (\to\Longrightarrow) \\
(7) & \text{if } (9)\ P, R, S \overset{s}{\Rightarrow} S, R \text{ and } (10)\ P, R \overset{s}{\Rightarrow} S, R, Q\ (\to\Longrightarrow) \\
(8) & \text{if } (11)\ P, S \overset{s}{\Rightarrow} P, S, R \text{ and } (12)\ P \overset{s}{\Rightarrow} P, S, R, Q\ (\to\Longrightarrow) \\
(6) & \text{if } (13)\ Q, R, Q \to S \overset{s}{\Rightarrow} S, R \text{ and } (14)\ Q, Q \to S \overset{s}{\Rightarrow} S, R, P\ (\to\Longrightarrow) \\
(13) & \text{if } (15)\ Q, R, S \overset{s}{\Rightarrow} S, R \text{ and } (16)\ Q, R \overset{s}{\Rightarrow} S, R, Q\ (\to\Longrightarrow) \\
(14) & \text{if } (17)\ Q, S \overset{s}{\Rightarrow} S, R, P \text{ and } (18)\ Q \overset{s}{\Rightarrow} S, R, P, Q\ (\to\Longrightarrow)
\end{array}
$$

Now, (9) to (12) and (15) to (18) are all axioms; therefore the result follows.