Formal Proofs

A *lemma* is a valid inference of the form $\phi_1, \ldots, \phi_k \models \psi$. Where the formulas $\phi_1, \ldots, \phi_k$ are known as premises or *axioms*, and ψ as the conclusion.

An important lemma is also called a *theorem* and a simple lemma is sometimes called a *proposition*.

If there are no premises, then we may write $\top \models \psi$, or just $\models \psi$, or even just ψ.

A lemma (theorem/proposition) must be a valid inference. The evidence that it is valid is called a *proof*.

The proofs we consider here are *formal proofs*, and they have a specific form:

The first k lines are the k premises of the lemma. The last line is the conclusion. Lines are numbered.

Proofs may contain flagpoles. A flagpole must be fully inside, around, above or below another flagpole.

In other words, a flagpole cannot partially overlap with another flagpole.

The formula in the flag is the *assumption*, the formula at the base of the flagpole is the *conclusion*.

The *context* of a line n are the lines above it ($k < n$), excluding those in a flag that has ended.

A formula β can be on a line, when $\alpha_1, \ldots, \alpha_i$ are in its context, and $\alpha_1, \ldots, \alpha_i \models \beta$.

A formula $\alpha \Rightarrow \beta$ can be on line n, when a flag with assumption α has a conclusion β on line $n-1$.

A formula $\forall_{x \in X}(\beta)$ can be on line n, when a flag with "**let** $x \in X$" concludes β on line $n-1$.

Using formulas from the context to derive another lines is called an *inference*.

A proof is *annotated* when it specifies which lines from the context were used to infer it.

The entailment that was used may be mentioned in the annotation.

There are various ways to construct a proof. You start with an incomplete proof with a gap.

Going forward: On the first open line, put a formula that can be inferred from context.

Going backward: On the last open line, put a formula such that, when combined with context, the next line can be inferred.

Doubling a gap: Put a line in the middle of the gap. You now have two (hopefully easier) gaps.

Closing a gap: Put a line in the gap which is both going forward and backward.

You may not know line numbers in advance (for lines after a gap). You can use temporary line numbers.

Don't forget to update the annotation when you change the line numbers to the final ones!

Each inference used in the proof must be known to be valid.

The simple inferences are covered in the course, and can be demonstrated with truth tables.

More complicated entailments can be proven separately in lemmas (or theorems or propositions).

Once an entailment is proven in a lemma, it can be reused forever in the future!