Teaching mathematics with structured derivations

Ralph-Johan Back

Åbo Akademi, Dept of Information Technologies

May 25, 2008

Mathematical proofs

- Proofs are of central importance for understanding mathematics
- A theorem with a proof is evident, without a proof it is magic,
- But writing proofs is seen as difficult in (Finnish) high school math, and is usually avoided

  $\Rightarrow$

- students entering university (e.g. CS studies) have a weak understanding of mathematics
- The proofs that are given are intuitive and informal
- More formal and rigorous proofs and derivations are given in certain subareas, like equation solving and simplifying algebraic expressions.

Logic and proofs

- A mathematical proof is a logical argumentation
- But logical notation is not used much in high schools, and logical inference rules are seldom given explicitly
- When logic is given as a course, it is taught as a separate (mathematical) topic, not as a tool for solving mathematical problems.
- We need to teach how to use logic in practice, how logic helps in organizing proofs and making them more rigorous:

logical mathematics rather than *mathematical logic*

Logic in high school mathematics

- Logic is abundant in high school math, but not usually recognized
- Example: Solve the equation

$$(x-1)(x^2+1)=0$$

Calculational style derivation

$$
\begin{array}{ll}
\bullet & (x-1)(x^2+1)=0 \\
\equiv & \{\text{zero product rule: } ab=0 \equiv a=0 \vee b=0\} \\
 & x-1=0 \vee x^2+1=0
\end{array}
$$

Calculational style derivation

- $(x-1)(x^2+1) = 0$

$\equiv$ {zero product rule: $ab = 0 \equiv a = 0 \vee b = 0$}

$x - 1 = 0 \vee x^2 + 1 = 0$

$\equiv$ {add 1 to both sides in left disjunct}

$x = 1 \vee x^2 + 1 = 0$

Calculational style derivation

- $(x-1)(x^2+1)=0$

$\equiv$ {zero product rule: $ab=0 \equiv a=0 \vee b=0$}

$x-1=0 \vee x^2+1=0$

$\equiv$ {add 1 to both sides in left disjunct}

$x=1 \vee x^2+1=0$

$\equiv$ {add -1 to both sides in right disjunct}

$x=1 \vee x^2=-1$

Calculational style derivation

$$
\begin{array}{ll}
\bullet & (x-1)(x^2+1)=0 \\
\equiv & \{\text{zero product rule: } ab=0 \equiv a=0 \vee b=0\} \\
 & x-1=0 \vee x^2+1=0 \\
\equiv & \{\text{add 1 to both sides in left disjunct}\} \\
 & x=1 \vee x^2+1=0 \\
\equiv & \{\text{add } -1 \text{ to both sides in right disjunct}\} \\
 & x=1 \vee x^2=-1 \\
\equiv & \{\text{a square is never negative}\} \\
 & x=1 \vee F
\end{array}
$$

Calculational style derivation

- $(x-1)(x^2+1) = 0$

$\equiv$ {zero product rule: $ab = 0 \equiv a = 0 \vee b = 0$}

$x - 1 = 0 \vee x^2 + 1 = 0$

$\equiv$ {add 1 to both sides in left disjoint}

$x = 1 \vee x^2 + 1 = 0$

$\equiv$ {add -1 to both sides in right disjunct}

$x = 1 \vee x^2 = -1$

$\equiv$ {a square is never negative}

$x = 1 \vee F$

$\equiv$ {disjunction rule}

$x = 1$

Calculational style proofs

- Derivation above is written in the calculational style that was proposed by Edsger Dijkstra and his colleagues (Wim Feijen, Carel Scholten och Nettie van Gasteren).
- A central goal of their approach was that proofs and derivations should be more like computations, required logical properties are calculated using logical inference rules in the same way as one calculates with arithmetic and algebraic rules when solving equations and simplifying expressions.
- Dijkstra's calculational style has become rather standard within formal methods research community.
- David Gries and Fred Schneider have studied and propagated for the use of calculational style proofs in mathematics teaching, in particular for teaching logic and discrete mathematics in introductory university courses.

Structured derivations

- *Structured derivations* is an extension of this calculational style of reasoning. Structured derivations were developed by Ralph-Johan Back and Joakim von Wright, as part of their research on programming methods and programming logic.

- The method was originally presented in a book (Back & von Wright: Refinement Calculus: A Systematic Introduction, Springer Verlag 1998) and in some journal and conference publications

- Dijkstra's calculational style is based on a variant of first order predicate calculus and on a Hilbert like proof system, whereas Back and von Wright base structured derivations on *higher order logic* and on *Gentzen like* proof systems.

- Structured derivations can thus be seen as a synthesis of classical Gentzen-like proof systems and Dijkstra's calculational style proofs.

Structured derivations in teaching

- The use of structured derivations in proofs in our book felt very intuitive and made the proofs really simple to understand. This lead us to start looking at the use of structured derivations also in ordinary mathematics teaching
  - in high school (age group 15 - 19, upper secondary school) and
  - in introductory courses at university
- A central goal is to increase the use of formal logical argumentation in mathematics teaching. This is achieved in two different ways
  - Structured derivations are written with a fixed proof format
  - Logical notation and logical inference rules are used systematically in proofs to calculate the required properties

The power of tradition

- The notation that is used in mathematics teaching today is very traditional. It has grown out from centuries of mathematics research, and has not been much influenced by the last 150 years of research in mathematical logic.
- This has lead to a situation where the same logical concept is described in different ways and with different notation in separate branches of mathematics.
- Simple and basic inference rules are not stated explicitly, the students have to grasp the logical way of thinking through a number of examples.
- This means that today's mathematics is presented in a way that is unnecessarily complex and unsystematic.
- Opportunities to use logic in high school mathematics, to simplify and systematize argumentation, seems almost limitless.

Learning and reasoning laboratory

Much of the research carried on structured derivations has been carried out within the *Learning and Reasoning laboratory*, a joint research laboratory for the IT departments of Åbo Akademi University och University of Turku.

We have a web-based resource center,

IMPEd http://crest.cs.abo.fi/imped/

with more information on structured derivations and other methods in teaching that we are developing

The research has been supported by the Academy of Finland, TEKES and by the Technology Industry's 100 year foundation.

Proof chains

A common way of proving a statement is by using a chain of equalities,

$$t_0 = t_1 = \ldots = t_n$$

The chain says that

$$t_0 = t_1 \text{ and } t_1 = t_2 \text{ and } \ldots t_{n-1} = t_n$$

The chain allows us to conclude that

$$t_0 = t_n$$

because equality is transitive.

Proof chains in structured derivations

$$
\begin{array}{ll}
\bullet & t_0 \\
= & \{\text{motivation why } t_0 = t_1\} \\
 & t_1 \\
= & \{\text{motivation why } t_1 = t_2\} \\
 & t_2 \\
\vdots & \\
 & t_{n-1} \\
= & \{\text{motivation why } t_{n-1} = t_n\} \\
 & t_n
\end{array}
$$

The format

- ✦ Each equality is justified with an argument for why this specific equality is valid
- ✦ We write each term and each justification on a line of their own, to make place for longer terms and more detailed justifications
- ✦ We can use two or more lines for a term or a justification, if needed
- ✦ The proof layout has two columns: the first for the relation symbols, the second for terms and justifications
- ✦ The purpose of the fixed layout is to make proofs easier to read, write and understand.

Example: Proof chain

We prove that the conjugation rule $(a-b)(a+b) = a^2 - b^2$ holds.

$$
\begin{array}{ll}
\bullet & (a-b)(a+b) \\
= & \{\text{by the rules for multiplying polynomials}\} \\
 & a^2 + ab - ba - b^2 \\
= & \{\text{middle terms cancel each other}\} \\
 & a^2 - b^2
\end{array}
$$

Traditional format

$$
\begin{aligned}
(a-b)(a+b) &= a^2+ab-ba-b^2 && \text{(by the rules for multiplying polynomials)}\\
&= a^2-b^2 && \text{(middle terms cancel each other)}
\end{aligned}
$$

- ✦ This format requires that both terms and justifications fit on the same line
- ✦ The justifications then easily become brief and cryptic, and it is easy to leave them out in the proof.

Justifications

- ✦ The main idea of a proof is lost if we omit justifications:
  - to convince the reader that each individual proof step is correct, and that
  - the proof steps together establish the required conclusion
- ✦ If we leave out the justifications in the proofs, then the reader has to figure out these himself.
- ✦ This makes the proof more difficult to read; it should be up to the one who is writing the proof to make the proofs as easy to understand as possible
- ✦ It is also important from an educational point of view that justifications are written out explicitly in proofs. The teacher can then check that the student has understood the underlying theory, and has been able to apply it in an appropriate way.
- ✦ A structured derivation forces the student to write a justification for each step, because a missing justification sticks out (as an empty pair of curly brackets).

Relations used in proof chains

- Vi can use different kinds of relations in proof chains.
- The most common relations are
  - $\equiv$ (equivalence),
  - $\Rightarrow$ (implication),
  - $\Leftarrow$ (reverse implication) ,
  - $=$ (equality), och
  - ordering relations, like $\leq, <, \geq, \ldots$

Properties of relations

- We usually choose relations that are transitive
- But we can also use non-transitive relations between terms
- We can mix different relations in the same proof chain

Task and assumptions

The proof chain only shows the proof itself, while the task that is solved is left implicit. The assumptions that one is allowed to make in the proof are also not stated explicitly.

We often want to be more explicit about these issues. We can then use the following more general format for structured derivations.

•	task
-	assumption$_1$
⋮	
-	assumption$_m$
$\Vdash$	{justification for why the chain is a solution of the task}
	t_0
$=$	{justification for $t_0 = t_1$}
	t_1
$=$	{justification for $t_1 = t_2$}
	t_2
⋮	
	t_{n-1}
$=$	{justification for $t_{n-1} = t_n$}
	t_n
$\square$	

The format

- ✦ The derivation starts with a description of the task at hand and of the assumptions that we can make when solving the task.
- ✦ The task is marked with the symbol "•", while each assumption is marked with the symbol "-".
- ✦ The proof/derivation is marked with the symbol $\Vdash$ (pronounced "is proved by").
- ✦ We can end the proof with the traditional symbol $\Box$ ("quad erat demonstrandum").
- ✦ A justification on the same line as the proof symbol explains why the following proof solves the task at hand.
- ✦ The derivation layout has two columns, one for the special symbols " $\bullet$ ", "$\Vdash$" , "$\Box$" and the relation symbols (here "$=$ "), while the second column has terms and justifications.

How detailed should the proof be

- The proof format with explicitly stated task and assumption can be unnecessarily formal if the task to be solved is evident from the proof. This is often the case when we use proof chains with transitive relations.

- On the other hand, it is often useful to write down the task and the assumptions explicitly, before starting to work on the proof.

- In may also be important in some case to explicitly indicate why the proof chain solves the task, in particular when we use a non-transitive relation, or the proof abstracts from the original task.

Example: Tasks and assumptions

We show that if a, b and c are non-negative real numbers, then

$$(1+a)(1+b)(1+c) \geq 1+a+b+c$$

- Show that $(1+a)(1+b)(1+c) \geq 1+a+b+c$

\- when $a, b, c \geq 0$

$\Vdash$ {combining $=$ and $\geq$ gives $\geq$}

$(1+a)(1+b)(1+c)$

$=$ {multiply two last parenthesis}

$(1+a)(1+b+c+bc)$

$=$ {multiply remaining parenthesis}

$1+b+c+bc+a+ab+ac+abc$

$\geq$ {subtract the non-negative expression $ab+ac+bc+abc$}

$1+a+b+c$

$\square$

Comments

- We use two different relations in the proof, $=$ and $\geq$
- The justification for the proof states that combining $=$ and $\geq$ gives $\geq$.
- The proposition is proved under the assumption that $a, b, c \geq 0$.

Subderivations

- A simple proof chain is sufficient as long as each justification is relatively simple and can be summarized on a few lines
- A more complex justification requires a proof of its own.
- We show next how to extend structured derivations with proof chains for justifications

Example: Ordering

Show that $m^2 - n^2 \geq 3$, when m and n are positive integers and $m > n$.

We use two common arithmetic rules in this derivation

$$\begin{array}{rl} \text{addition is monotonic} & : \; a + b \leq a + b', \text{ when } b \leq b' \\ \text{multiplication is monoton} & : \; ab \leq ab', \text{ when } a \geq 0 \text{ and } b \leq b' \end{array}$$

- Prove that $m^2 - n^2 \geq 3$

\- when m, n are positive integers and

\- $m > n$

$\Vdash$ $m^2 - n^2$

$=$ {conjugation rule}

$(m - n)(m + n)$

$\geq$ {multiplication is monotonic, $m - n \geq 1$ and $m + n \geq 3$}

$(m - n) \cdot 3$

$\geq$ {multiplication is monotonic, $m - n \geq 1$ by assumption, and $3 \geq 0$}

$1 \cdot 3$

$=$ {arithmetic}

3

$\square$

Discussion

- The second step in the proof is somewhat complicated
- We use the rule that multiplication is monotonic. This rule is used to establish that $m - n \geq 1$ and that $m + n \geq 3$.
- We justify this conclusion with the following observations:
  - $m > n$ by assumption, so $m - n > 0$, hence $m - n \geq 1$,
  - $n > 0$ by assumption, so $n \geq 1$, and
  - $m > n \geq 1$ by assumption, so $m \geq 2$, hence $m + n \geq 3$.

Justifications as subderivations

- $m > n$

  $\Rightarrow$ {arithmetic}

  $m - n > 0$

  $\Rightarrow$ {arithmetic}

  $m - n \geq 1$

- $m > n$ and $n > 0$

  $\Rightarrow$ {arithmetic}

  $m \geq n + 1$ and $n \geq 1$

  $\Rightarrow$ {arithmetic}

  $m \geq 2$ och $n \geq 1$

  $\Rightarrow$ {arithmetic}

  $m + n \geq 3$

Subderivations

- We can also write these proofs directly in the main proof, as justifications for a specific proof step.
- A proof for a proof step is called a *subproof* or *subderivation*.
- Consider a step in the proof chain,

$$
\begin{array}{ll}
 & t \\
R & \{\text{justification}\} \\
 & t'
\end{array}
$$

In stead of a simple justification, we can prove that $t\,R\,t'$ is true in a subderivation. The proof step then looks as follows:

t

R {justification that the relation holds when H_1, ..., H_m hold}

- H_1

$\Vdash \ldots$

⋮

- H_m

$\Vdash \ldots$

$\ldots$ t'

The format

- Here $H_1, \ldots, H_m$ are subtasks, which are proved in the same way as the main task at hand.
- The justification explains why the relation $t\,R\,t'$ holds if the subtasks $H_1, \ldots, H_m$ can be shown to hold.
- A subderivation can sometimes be quite long, so we indicate the end of the subderivation by marking the second term in the relation (here t') with "...".
- This is intended to make it easier to see where the subderivation ends and the main derivation continues.

Example: Subderivations

We rewrite the previous derivation using subderivations:

- Show that $m^2 - n^2 \geq 3$

\- when m, n are positive integers, and

\- $m > n$

$\Vdash$ $m^2 - n^2$

$=$ {conjugate rule}

$(m - n)(m + n)$

$\geq$ {multiplication is monotonic, $m - n \geq 1$ and $m + n \geq 3$}

- $m > n$

  $\Rightarrow$ {arithmetic}

  $m - n > 0$

  $\Rightarrow$ {arithmetic}

  $m - n \geq 1$

- $m > n$ och $n > 0$

  $\Rightarrow$ {arithmetic}

$$
\begin{array}{ll}
 & m \geq n+1 \text{ och } n \geq 1 \\
\Rightarrow & \{\text{arithmetic}\} \\
 & m \geq 2 \text{ och } n \geq 1 \\
\Rightarrow & \{\text{arithmetic}\} \\
 & m+n \geq 3
\end{array}
$$

$$
\begin{array}{ll}
\ldots & (m-n)\cdot 3 \\
\geq & \{(m-n) \geq 1 \text{ by assumption, and } 3 \geq 0\} \\
 & 1 \cdot 3 \\
= & \{\text{arithmetic}\} \\
 & 3
\end{array}
$$

$\square$

Example: Subderivations on paper

- ✦ A subderivation can sometimes be easier to write in a separate box on the same page
- ✦ Makes it easier to add, delete and change subderivations when working with paper and pen

•	Prove that $m^2 - n^2 \geq 3$
-	when m, n are positive integers and
-	$m > n$
$\Vdash$	$m^2 - n^2$
$=$	{conjugation rule}
	$(m - n)(m + n)$
$\geq$	{multiplication is monotonic, $m-n \geq 1$, $m+n \geq 3$}
$\ldots$	$(m - n) \cdot 3$
$\geq$	{multiplication is monotonic, $m - n \geq 1$ by assumption, and $3 \geq 0$}
	$1 \cdot 3$
$=$	{arithmetic}
	3

•	$m > n$
$\Rightarrow$	{arithmetic}
	$m - n > 0$
$\Rightarrow$	{arithmetic}
	$m - n \geq 1$

•	$m > n$ and $n > 0$
$\Rightarrow$	{arithmetic}
	$m \geq n + 1 \wedge n \geq 1$
$\Rightarrow$	{arithmetic}
	$m \geq 2$ och $n \geq 1$
$\Rightarrow$	{arithmetic}
	$m + n \geq 3$

Example: Simplifying subexpressions

Another use of a subderivation is to simplify a subexpression in a larger expression. A subderivation avoids having to copy the whole expression with minor modifications through the whole derivation.

$\bullet$ Simplify $x(x-1)(x+1)+x-x^3$:

$\Vdash$ $x(x-1)(x+1)+x-x^3$

$=$ {simplify $x(x-1)(x+1)$}

$\bullet$ $x(x-1)(x+1)$

$=$ {conjugate rule}

$x(x^2-1)$

$=$ {multiply}

x^3-x

$\ldots$ $x^3-x+x-x^3$

$=$ {simplify}

0

$\square$

Discussion

- ✦ We focus in this derivation on the subexpression $x(x-1)(x+1)$ and simplify it in a subderivation
- ✦ We then replace the original subexpression with the simplified subexpression in the whole expressions.

Computer support

- ✦ A text editor that can fold and unfold text is very useful here (an “outlining editor”). We can the selectively show and hide subderivations.
- ✦ Hiding subderivations gives us an overview of the whole proof. A specific proof step can be studied in more detail by showing (unfolding) that step.
- ✦ This is more difficult to achieve when working with pen and paper. One strategy is to write the subderivation on a separate place on the paper (like we did above)
- ✦ The ellipsis (...) indicates that there is (or should be) a subderivation for the proof step.
- ✦ Example: previous example, when folding subderivations:

- Prove that $m^2 - n^2 \geq 3$

\- when m, n are positive integers and

\- $m > n$

$\Vdash$ $m^2 - n^2$

$=$ {conjugation rule}

$(m - n)(m + n)$

$\geq$ {multiplication is monotonic, $m - n \geq 1$ and $m + n \geq 3$}

$\ldots$ $(m - n) \cdot 3$

$\geq$ {multiplication is monotonic, $m - n \geq 1$ by assumption, and $3 \geq 0$}

$1 \cdot 3$

$=$ {arithmetic}

3

$\square$

Derivations with logic

Using logical notation and proof rules of logic explicitly is a central idea in structured derivations

We compute with logical expressions in the same way as we compute with arithmetic and algebraic expressions.

Logical operations

T : *truth*, the true proosition

F : *falsity,* the false proposition

$\neg p$: *negation*, proposition p is not true

$p \wedge q$: *conjunction*, both p and q are true propositions

$p \vee q$: *disjunction*, p is true or q is true (or both propositions are true)

$p \Rightarrow q$: *implication*, if p then also q is true

$p \equiv q$: *equivalence*, p is true if and only if q is true

$(\forall x \cdot p(x))$: *universal quantification*, proposition p is true for every value of x

$(\exists x \cdot p(x))$: *existential quantification*, proposition p is true for some value of x

Example: Definedness of rational expression

✦ Problem

Determine the values of x for which the expression $\frac{x-1}{x^2-2}$ is well-defined.

$\bullet \quad \frac{x-1}{x^2-1}$ is well-defined

$\equiv \quad$ {definedness of rational expressions}

$x^2 - 1 \neq 0$

$\bullet \quad \frac{x-1}{x^2-1}$ is well-defined

$\equiv \quad$ {definedness of rational expressions}

$x^2 - 1 \neq 0$

$\equiv \quad$ {switch to logic notation}

$\neg(x^2 - 1 = 0)$

$\bullet \quad \frac{x-1}{x^2-1}$ is well-defined

$\equiv \quad$ {definedness of rational expressions}

$x^2 - 1 \neq 0$

$\equiv \quad$ {switch to logic notation}

$\neg(x^2 - 1 = 0)$

$\equiv \quad$ {solve equation in brackets}

$\bullet \quad x^2 - 1 = 0$
$\equiv \quad$ {factorization rule}
$(x+1)(x-1) = 0$

• $\frac{x-1}{x^2-1}$ is well-defined

$\equiv$ {definedness of rational expressions}

$x^2 - 1 \neq 0$

$\equiv$ {switch to logic notation}

$\neg(x^2 - 1 = 0)$

$\equiv$ {solve equation in brackets}

- • $x^2 - 1 = 0$

  $\equiv$ {factorization rule}

  $(x+1)(x-1) = 0$

  $\equiv$ {rule for zero product}

  $x = -1 \vee x = 1$

•　$\frac{x-1}{x^2-1}$ is well-defined

≡　{definedness of rational expressions}

$x^2 - 1 \neq 0$

≡　{switch to logic notation}

$\neg(x^2 - 1 = 0)$

≡　{solve equation in brackets}

- •　$x^2 - 1 = 0$
- ≡　{factorization rule}
- 　$(x + 1)(x - 1) = 0$
- ≡　{rule for zero product}
- 　$x = -1 \lor x = 1$

…　$\neg(x = -1 \lor x = 1)$

- $\frac{x-1}{x^2-1}$ is well-defined

$\equiv$ {definedness of rational expressions}

$x^2 - 1 \neq 0$

$\equiv$ {switch to logic notation}

$\neg(x^2 - 1 = 0)$

$\equiv$ {solve equation in brackets}

- $x^2 - 1 = 0$

  $\equiv$ {factorization rule}

  $(x+1)(x-1) = 0$

  $\equiv$ {rule for zero product}

  $x = -1 \vee x = 1$

$\ldots$ $\neg(x = -1 \vee x = 1)$

$\equiv$ {de Morgans laws}

$\neg(x = -1) \wedge \neg(x = 1)$

$\equiv \quad$ {change notation}

$x \neq -1 \wedge x \neq 1$

Hiding subderivation

$$
\begin{array}{ll}
\bullet & \frac{x-1}{x^2-1} \text{ is well-defined} \\
\Leftrightarrow & \{\text{definedness of rational expressions}\} \\
& x^2 - 1 \neq 0 \\
\Leftrightarrow & \{\text{switch to logic notation}\} \\
& \neg(x^2 - 1 = 0) \\
\Leftrightarrow & \{\text{solve equation in brackets}\} \\
\ldots & \neg(x = -1 \vee x = 1) \\
\Leftrightarrow & \{\text{de Morgans laws}\} \\
& \neg(x = -1) \wedge \neg(x = 1) \\
\Leftrightarrow & \{\text{change notation}\} \\
& x \neq -1 \wedge x \neq 1
\end{array}
$$

Example: Equation with absolute values

- ✦ Problem

  Solve the equation $|x-1|+|2x-y|=0$

- ✦ Solution illustrates use of assumptions in subderivations

Solution

$$
\begin{array}{ll}
\bullet & |x-1| + |2x-y| = 0 \\
\equiv & \{\text{property of absolute values}\} \\
 & x-1=0 \wedge 2x-y=0
\end{array}
$$

Solution

$$
\begin{array}{ll}
\bullet & |x-1| + |2x-y| = 0 \\
\equiv & \{\text{property of absolute values}\} \\
 & x-1=0 \wedge 2x-y=0 \\
\equiv & \{\text{add 1 to both sides of left equation}\} \\
 & x=1 \wedge 2x-y=0
\end{array}
$$

Solution

- $|x-1| + |2x-y| = 0$

$\equiv$ {property of absolute values}

$x - 1 = 0 \wedge 2x - y = 0$

$\equiv$ {add 1 to both sides of left equation}

$x = 1 \wedge 2x - y = 0$

$\equiv$ {simplify right conjunct}

- $[x = 1]$ <——- may assume left conjunct when simplifying right conjunct
  $2x - y = 0$

Solution

- $|x - 1| + |2x - y| = 0$

$\equiv$ {property of absolute values}

$x - 1 = 0 \wedge 2x - y = 0$

$\equiv$ {add 1 to both sides of left equation}

$x = 1 \wedge 2x - y = 0$

$\equiv$ {simplify right conjunct}

- $[x = 1]$ <——- may assume left conjunct when simplifying right conjunct

  $2x - y = 0$

  $\equiv$ {substitute using assumption}

  $2 - y = 0$

Solution

$$\bullet \quad |x-1| + |2x-y| = 0$$

$\equiv$ {property of absolute values}

$$x - 1 = 0 \wedge 2x - y = 0$$

$\equiv$ {add 1 to both sides of left equation}

$$x = 1 \wedge 2x - y = 0$$

$\equiv$ {simplify right conjunct}

- $[x = 1]$ <——- may assume left conjunct when simplifying right conjunct

  $2x - y = 0$

  $\equiv$ {substitute using assumption}

  $2 - y = 0$

  $\equiv$ {solve}

  $y = 2$

Solution

$\bullet \quad |x-1| + |2x-y| = 0$

$\equiv \quad$ {property of absolute values}

$\quad x-1=0 \wedge 2x-y=0$

$\equiv \quad$ {add 1 to both sides of left equation}

$\quad x=1 \wedge 2x-y=0$

$\equiv \quad$ {simplify right conjunct}

$\quad \bullet \quad [x=1]$ <—— may assume left conjunct when simplifying right conjunct

$\quad\quad 2x-y=0$

$\quad \equiv \quad$ {substitute using assumption}

$\quad\quad 2-y=0$

$\quad \equiv \quad$ {solve}

$\quad\quad y=2$

$\ldots \quad x=1 \wedge y=2$

Example: Natural language in proofs

We use structured derivations also for arguing about natural language propositions.

Show that $k^2 + k$ is an even number for every integer k.

- Show that $k^2 + k$ is an even number

\- when k is an integer

$\Vdash$ $k^2 + k$ is an even number

$\equiv$ {factorization}

$k(k+1)$ is an even number

$\equiv$ {a product is even if one of its factors is even}

k is an even number $\vee$ $k+1$ is an even number

$\equiv$ {one of two successive integers is even}

T

$\Box$

Discussion

- We use here natural language to express the proposition: "$k^2 + k$ is an even number". This saves us from the task of formally defining what it means to be an even number, and allows us to reason just in terms of properties of even numbers.

- Our task is to prove that the proposition "$k^2 + k$ is an even number" is true. We express this as

  $$k^2 + k \text{ is an even number } \equiv T$$

  where T stands for "truth", i.e, we say that "$k^2 + k$ is an even number" is equivalent to T. We have to write propositions as relational terms $t\,R\,t'$ in proof chains.

- $p \Rightarrow T$ is always true, so it is in fact sufficient to show that $T \Rightarrow p$, this already implies that p is true. The general rule is that

  $$(p \equiv T) \equiv (T \Rightarrow p)$$

Example: a slightly more difficult problem

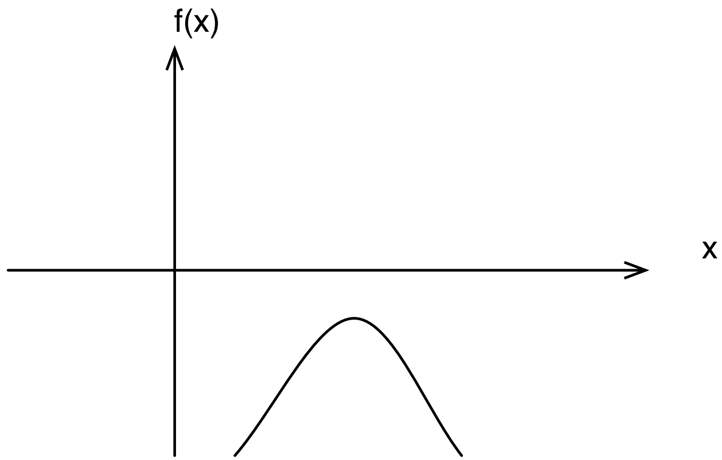
This derivation illustrates

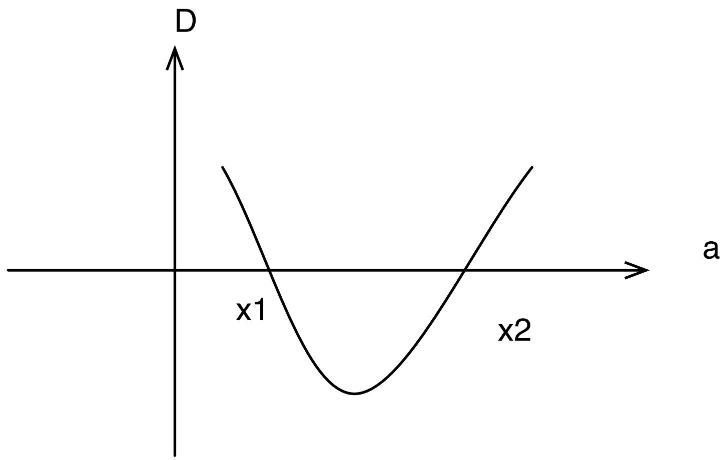
- use of logical notation,
- manipulation of logical expressions,
- use of figures in the derivation, and
- the need for subderivations.

The problem

Determine the values of a for which the function $f(x) = -x^2 + ax + a - 3$ is always negative.

We use the following two figures in the proof:





- Determine the values of a for which the function $f(x) = -x^2 + ax + a - 3$ is always negative.

$\Vdash$ $(\forall x \cdot -x^2 + ax + a - 3 < 0)$

$\equiv$ {the function is a parabola that opens downwards (the coefficients of the quadratic term is negative); such a function is always negative if it does not intersect the x-axis (figure on the left)}

$(\forall x \cdot -x^2 + ax + a - 3 \neq 0)$

$\equiv$ {this is true if the discriminant D for the function is negative}

$D < 0$

$\equiv$ {compute D}

	$\bullet$	Compute D:
	$\Vdash$	D
	$=$	{the discriminant for the equation $Ax^2 + Bx + C = 0$ is $B^2 - 4AC$}
		$a^2 - 4(-1)(a-3)$
	$=$	{simplify}
		$a^2 + 4a - 12$

$\ldots \quad a^2 + 4a - 12 < 0$

$\equiv \quad$ {the function $a^2 + 4a - 12$ opens upwards, because the coefficient for the square term is positive; such a function is negative between the intersection points with the x - axis (figure on the right)}

- Compute intersection points with x - axis for function $a^2 + 4a - 12$:

$\Vdash$ $a^2 + 4a - 12 = 0$

$\equiv$ {square root formula}

$a = \frac{-4 \pm \sqrt{4^2 - 4 \cdot 1 \cdot (-12)}}{2 \cdot 1}$

$\equiv$ {simplify}

$a = 2 \vee a = -6$

$\ldots$ $-6 < a < 2$

$\square$

Discussion

We have proved that

$$(\forall x \cdot -x^2 + ax + a - 3 < 0) \equiv -6 < a < 2$$

In other words, the function is always negative if and only if $-6 < a < 2$.

We use logical propositions and notation freely in structure derivations, and use logical inference rules as justifications. Here we need universal quantification to express the problem , $(\forall x \cdot -x^2 + ax + a - 3 < 0)$.

The main derivation and one of the subderivations uses equivalence between terms, the other subderivation uses equality between terms.

Observation

- We have to show equivalence between the two propositions.
- If we only show implication to the right,

$$(\forall x \cdot -x^2 + ax + a - 3 < 0) \Rightarrow -6 < a < 2$$

  then the constraint on a can be too weak, i.e., so that it also allows values for a that do not satisfy the original condition.
- If we only show

$$(\forall x \cdot -x^2 + ax + a - 3 < 0) \Leftarrow -6 < a < 2$$

  then we could miss some values for a that satisfy the original condition.
- By proving equivalence, we show that the original condition is satisfied exactly by the values of a that satisfy the derived constraint.

Additional material

We can use additional material, like figures, tables and so on, in structured derivations. This additional material is provided outside the proof, but we can refer to it inside the proof.

In the same way, we can discuss the background theory needed for the proof before the derivation itself. In this proof, we used general properties about parabolas.

General problems

A more common form of a problem is where we describe a situation and then are asked to prove some property or derive some quantify in this context.

The context is described in a structured derivation with the assumptions.

Example: Geometry

We have a triangle with a right angle. The hypotenuse is 15 cm, while the perimeter is 36 cm. Determine the length of the catheter.

Pythagoras theorem gives us that $a^2 + b^2 = c^2$ where a and b are the catheter and c is the hypotenuse.

The perimeter is given by $a + b + c$.

- Determine the catheter in the triangle :

[1] The triangle has a right angle, has catheter a and b and hypotenuse c.

[2] $c = 15cm$

[3] the perimeter is $36cm$

$\Vdash$ $[1] \wedge [3]$

$\Rightarrow$ {Pythagoras theorem, definition of perimeter}

$a^2 + b^2 = c^2 \wedge a + b + c = 36$

$\equiv$ {assumption [2]}

$a^2 + b^2 = 15^2 \wedge a + b + 15 = 36$

$\equiv$ {solve b from the right equation}

$a^2 + b^2 = 15^2 \wedge b = 21 - a$

$\equiv$ {substitute values for b in left equation, $15^2 = 225$}

$a^2 + (21 - a)^2 = 225 \wedge b = 21 - a$

$\equiv$ {compute $(21-a)^2$}

$$a^2+441-42a+a^2=225 \wedge b=21-a$$

$\equiv$ {simplify the equation}

$$2a^2-42a+216=0 \wedge b=21-a$$

$\equiv$ {solve the second degree equation}

- $$2a^2-42a+216=0$$

  $\equiv$ {square root formula}

  $$a=\frac{-(-42)\pm\sqrt{42^2-4\cdot 2\cdot 216}}{2\cdot 2}$$

  $\equiv$ {simplify}

  $$a=\frac{42\pm\sqrt{1764-1728}}{4}$$

  $\equiv$ {simplify}

  $$a=\frac{42\pm 6}{4}$$

$\equiv$ {simplify}

$a = 9 \vee a = 12$

$\ldots$ $(a = 9 \vee a = 12) \wedge b = 21 - a$

$\equiv$ {distribution rule: $(p \vee q) \wedge r = (p \wedge r) \vee (q \wedge r)$}

$(a = 9 \wedge b = 21 - a) \vee (a = 12 \wedge b = 21 - a)$

$\equiv$ {substitute a in expression for b}

$(a = 9 \wedge b = 21 - 9) \vee (a = 12 \wedge b = 21 - 12)$

$\equiv$ {simplify}

$(a = 9 \wedge b = 12) \vee (a = 12 \wedge b = 9)$

Discussion

- The result shows that the catheter are 9 cm and 12 cm.
- We have numbered the assumptions, so that it is easier to refer to them in the proof.
- The proof starts from a conjunction of propositions that we know to be true (because they are assumed to be true). We then prove that the assumptions imply the result $(a = 9 \wedge b = 12) \vee (a = 12 \wedge b = 9)$.
- Because the assumptions were assumed to be true, the result must also be true, i.e., we have solved the problem.

Example: Problem in mechanics

The travel time for the fastest train connection between Helsinki and Lappeenranta has been shortened by 37% since 1960. Determine how many percentage the average travel speed then has increased. You may assume that the track length has not changed.

We start by reformulating the problem, in order to introduce the notation that we are going to use in the proof.

The problem is then as follows: The travel time t' for the fastest train connection between Helsinki and Lappeenranta has been shortened by 37% compared to the original travel time t since 1960. Determine how many percentage p the average travel speed V' then has increased from the original speed V. You may assume that the track length s has not changed.

- Determine increase in speed p:

\- $t' = 0.63 \cdot t$

$\Vdash$ {transitivity, approximation}

p

$=$ {definition of speed increase}

$$\frac{V' - V}{V}$$

$=$ {physics: speed v is defined as $v = \dfrac{s}{t}$ where s is the distance and t is time}

$$\frac{\frac{s}{t'} - \frac{s}{t}}{\frac{s}{t}}$$

$=$ {simplify}

$$\frac{\frac{s}{t'}}{\frac{s}{t}} - 1$$

$$
\begin{array}{ll}
= & \{\text{simplify fraction}\} \\
& \dfrac{s \cdot t}{s \cdot t'} - 1 \\
= & \{\text{simplify, use assumption}\} \\
& \dfrac{1}{0.63} - 1 \\
\approx & \{\text{compute approximate value}\} \\
& 0.59 \\
= & \{\text{change to percentage, } x\% = \frac{x}{100}\} \\
& 59\%
\end{array}
$$

The answer is that the speed has increased with 59%.

Reduction proofs

A proof chain is useful when the chain consists of two or more steps. A proof step for a single chain feels slightly clumsy.

We can then use an alternative proof format, where we prove the conjecture directly using subderivations. This is the traditional proof format for Gentzen like proofs.

Reduction proofs are not strictly necessary, we can restrict ourselves to proof chains only, but they are sometimes quite convenient and make proofs cleaner and less verbose.

Reduction proof

- *task*

$\Vdash$ *{motivation}*

  - *derivation*$_1$

  $\vdots$

  - *derivation*$_n$

✦ We solve the original task by reducing it to a collection of subderivations.

✦ The subderivations are indented one step to the right.

✦ The motivation explains why the subderivations together solve the original task.

Two different proof approaches

We have two different proof approaches:

- proof chain, and
- reduction proof

These can be freely combined, so that subderivations in a reduction proof can be solved using proof chains or additional reduction proofs.

Example: Case analysis

We want to prove that $|x+1| > 1$ is true both when $x > 0$ and when $x < -2$.

In a case proof, we first identify a number of cases. Then we prove the original conjecture for each case separately. It is important that the cases together exhaust all possibilities.

- Show that $|x+1| > 1$

[1] when $x > 0 \vee x < -2$

$\Vdash$ {case rule, it is sufficient to consider only alternatives $x > 0$ and $x < -2$ by [1]}

- Show that $|x+1| > 1$

- when $x > 0$

$\Vdash$ $|x+1|$

$=$ {definition of absolute value, assumption $x > 0$}

$x+1$

$>$ {assumption}

$0+1$

$=$ {arithmetic}

1

- Show that $|x+1| > 1$

- when r $x < -2$

$$
\begin{array}{ll}
\Vdash & |x+1| \\
= & \{\text{definition of absolute value, assumption } x < -2\} \\
 & -(x+1) \\
= & \{\text{simplify}\} \\
 & -x-1 \\
> & \{\text{assumption } x < -2\text{, so } -x > 2\} \\
 & 2-1 \\
= & \{\text{arithmetic}\} \\
 & 1
\end{array}
$$

$\square$

Example: Inductions proof

We prove that

$$(\forall n \in \mathbb{N} \bullet 0 + 1 + \ldots + n = \frac{n(n+1)}{2})$$

using induction on the natural numbers.

- Show that $(\forall n \in \mathbb{N} \bullet 0 + 1 + \ldots + n = \frac{n(n+1)}{2})$

$\Vdash$ {induction proof}

- Basis step: $0 + 1 + \ldots + n = \frac{n(n+1)}{2}$

\- when $n = 0$

$\Vdash$ $0 + 1 + \ldots + n = \frac{n(n+1)}{2}$

$\equiv$ {assumption $n = 0$, definition of sum }

$0 = \frac{0(0+1)}{2})$

$\equiv$ {multiplication with 0}

T

- Induction step: $0 + 1 + \ldots + n' = \frac{n'(n'+1)}{2})$

\- when $n' = n + 1$ and

\- $0 + 1 + \ldots + n = \frac{n(n+1)}{2}$

$\Vdash$ $0 + 1 + \ldots + n'$

$=$ {assumption }

$$
\begin{array}{ll}
 & 0 + 1 + \ldots + n + (n+1) \\
= & \{\text{induction assumption}\} \\
 & \frac{n(n+1)}{2} + (n+1) \\
= & \{\text{write with common denominator}\} \\
 & \frac{n^2+n+2n+2}{2} \\
= & \{\text{simplify}\} \\
 & \frac{n^2+3n+2}{2} \\
= & \{\text{factorize}\} \\
 & \frac{(n+1)(n+2)}{2} \\
= & \{\text{assumption } n' = n+1\} \\
 & \frac{n'(n'+1)}{2}
\end{array}
$$

Example: Epsilon-delta method

- Show that $f(x)$ is uniformly continuous

\- when $f(x) = 2x$

$\Vdash$ $f(x)$ is uniformly continuous

$\equiv$ {definition of uniform continuity}

$(\forall \epsilon > 0 \cdot \exists \delta \cdot (\forall x, y \cdot y < x \wedge x - y < \delta \Rightarrow |f(x) - f(y)| < \epsilon))$

$\equiv$ {Generalization rule, choose an arbitrary ϵ}

- Show that $(\exists\delta \cdot (\forall x, y \cdot y < x \wedge x - y < \delta \Rightarrow |f(x) - f(y)| < \epsilon))$

\- when $\epsilon > 0$

$\Vdash$ {Provide witness δ for existential quantification}

  - Show that $(\forall x, y \cdot y < x \wedge x - y < \delta \Rightarrow |f(x) - f(y)| < \epsilon)$

  \- when $\delta(\epsilon) =?$

  $\Vdash$ {Generalization, choose arbitrary x and y}

    - Show that $|f(x) - f(y)| < \epsilon$

    \- when $y < x$ and $x - y < \delta$

    $\Vdash$ $|f(x) - f(y)| < \epsilon$

    $\equiv$ {definition of $f(x)$}

    $|2x - 2y| < \epsilon$

    $\equiv$ {assumption}

$\ldots \quad T$

Structured derivations in general

We have introduced structured derivations by a sequence of examples.

The purpose was to show different ways in which structured derivations can be used in high school mathematics.

Next we describe structured derivations from a more general perspective:

- how to write structured derivations (syntax),
- what do structured derivations stand for (semantics), and
- how do you construct structured derivations in practice (pragmatics).

Syntax for structured derivations

- ✦ We define both syntax and layout at the same time
- ✦ This makes the syntax two dimensional, a k o tiling syntax.
- ✦ Syntax leaves basic components of the derivation undefined: what is a
  - conjecture
  - assumption
  - motivation
  - term
  - relation
- ✦ This allows the proof format to be used for (almost) any mathematical area of discourse, by using notation that feels familiar in this area
- ✦ We emphasize the use of logic in expressing conjectures, assumptions and terms

Syntax definition

derivation =
task *lemmas* *proof*

task =	
•	*conjecture*
-	*assumption*$_1$
⋮	
-	*assumption*$_n$

$n \geq 0$

lemmas =	
-	*derivation*$_1$
⋮	
-	*derivation*$_m$

$m \geq 0$

proof =	*proof* =	*proof* =
proof chain	*reduction proof*	

reduction proof =	
$\Vdash$	*{motivation}*
	derivation$_1$
$\vdots$	
	derivation$_n$

$n \geq 0$

proof chain =	
$\Vdash$	*{motivation}*
	term$_0$
rel$_1$	*subproof*$_1$
	term$_1$
$\vdots$	
	term$_{n-1}$
rel$_n$	*subproof*
	term$_n$

$n \geq 1$

subproof =
{motivation}
derivation$_1$
$\vdots$
derivation$_n$

$n \geq 0$

Comments

- ✦ The special symbols are written in the first column, while the tasks, lemmas and proofs are written in the second column. The symbol "$\square$" can also be written on the last line of the proof.

- ✦ We can use a more specific identification of tasks, assumptions and lemmas. In stead of $\bullet$, we can give the task a name, like *"Theorem 3"*, *"Assignment 7a"*, *"Problem 14"*, in stead of "- ", we can give the lemmas more specific identification, like "[1], [2], [3]" or "Lemma 1", "Lemma 2", .. . In stead of "-", we can write [1], [2], .. or [a], [b] to identify the assumptions.

- ✦ The proof symbol $\Vdash$ implies that the assumptions in the task may be used in the proof as well as in subproofs of the main proof. If we want to restrict the assumptions to just be used in the main proof, then we should use the symbol $\Vdash_0$ for the proof.

Summary

- ✦ A structured derivation starts with a description of the task at hand.
- ✦ The task has a goal and a collection of assumptions that we may use when solving the task.
- ✦ The goal can be of the form "Prove that . . . ", or "Determine the value of . . . ".
- ✦ Every assumption is written on a line of its own, and is usually given a unique identification (a number or a name), so that we can refer to it in the proof.
- ✦ The task may be followed by a collection of lemmas. Each lemma is a derivation in itself, with task, sublemmas and proof. The lemmas may be used in the main proof. The proof of the lemma is indented one step to the right
- ✦ The syntax allows empty proofs. This is so that incomplete proofs can be seen as syntactically correct.
- ✦ A derivation is *complete,* if there are no empty proofs. This does not mean that the proof is correct, it just means that all proofs that are needed have been given.
- ✦ A non-empty proof is either a proof chain or a reduction proof.

- ✦ A reduction proof lists the subtasks that need to be solved in order for the original goal to be achieved.
- ✦ A proof chain starts with a term, which is then stepwise transformed to new terms, with the relations between the terms explicitly indicated, and with a justification for each step.
- ✦ A relational step can be justified with a subproof.

Level of precision in the proof

The level of precision can be chosen freely in a structured derivation, and will in general depend on the circumstances.

When one is teaching a new mathematical concept or a new application of a familiar concept, one should show each step in detail, with detailed motivations and explicit assumptions.

When theory is already familiar, and one is only looking for a solution to the given task, then the proof can proceed in much larger steps, and with shorter, more intuitive motivations.

Motivations

- ✦ A motivation should clearly explain why the proof step is justified.
- ✦ A very detailed motivation will give
  - the name of the inference rule used,
  - the substitution that has been used in the rule,
  - and check that the rule can indeed be applied in the situation at hand
- ✦ In practice, this is usually too detailed, and it is sufficient to just give the name of the inference rule, or even just the kind of inference rule that is used ("simplification", "logic", etc.)

Abbreviations

We use certain abbreviations quite frequently, in order to make the derivations as simple and concise as possible.

$$
\begin{array}{ll}
\bullet & \textit{conjecture} \\
\Vdash & \{\textit{motivation}\} \\
 & \textit{term}_0 \\
\textit{rel}_1 & \{\textit{motivation}_1\} \\
 & \textit{term}_1 \\
\vdots & \\
 & \textit{term}_{n-1} \\
\textit{rel}_n & \{\textit{motivation}\} \\
 & \textit{term}_n
\end{array}
$$

can be abbreviated to

$$
\begin{array}{ll}
\bullet & \textit{term}_0 \\
\textit{rel}_1 & \{\textit{motivation}_1\} \\
 & \textit{term}_1 \\
\vdots & \\
 & \textit{term}_{n-1} \\
\textit{rel}_n & \{\textit{motivation}\} \\
 & \textit{term}_n
\end{array}
$$

•	*conjecture*		•	[*assumption*$_1$]
-	*assumption*$_1$		⋮	
⋮				[*assumption*$_m$]
-	*assumption*$_m$			*term*$_0$
$\Vdash$	{*motivation*}		*rel*$_1$	{*motivation*$_1$}
	term$_0$	can be abbreviated to		*term*$_1$
rel$_1$	{*motivation*$_1$}		⋮	
	term$_1$			*term*$_{n-1}$
⋮			*rel*$_n$	{*motivation*$_n$}
	term$_{n-1}$			*term*$_n$
rel$_n$	{*motivation*$_n$}			
	term$_n$			

Solving a mathematical problem

✦ Solving a mathematical problem may entail also other things than just giving a structured derivation. One often also needs to record other kind of information

- reformulating the problem, in order to introduce notation
- drawing figures that help with the argumentation
- constructing tables that can be used in the proof
- recalling relevant mathematical notation and results
- discussion about the proof, the central ideas and possible alternative solutions

Constructing a structured derivation

- ✦ A structured derivation is constructed step by step, often through a process and trial and error. .
- ✦ We should not expect to construct the right solution directly, we have to try our way, somethings backtracking on what we have already written.
- ✦ The analogue to writing a structured derivation is writing a piece of program code that solves a specific programming problem. The code is written, tested, rewritten and rewritten again, until we are satisfied with that it is a solution to the given problem.

Structured derivations and programming languages

- The structured derivation notation is similar to a programming language notation,
  - it has an exact syntax
  - it is modular, hierarchical and allows for arbitrarily deep nesting of constructs
  - the syntax can be checked by a computer (provided we have decided on the syntax of the basic constructs)
  - the correctness of a derivation can also be checked by a computer (but may require quite an advanced automatic or semi-automatic theorem prover)
- We need to look at a proof as a *product* that we are constructing, rather than as a *process* that we are carrying out.

Manipulating a proof

We can start by giving the proof in rough details, just recording the main assumptions and writing down the main proof steps. We can then make the proof more precise, by, e.g.,

- ✦ adding new assumptions needed in the proof
- ✦ adding new lemmas
- ✦ prove that an assumption follows from other assumptions (thus turning it into a lemma)
- ✦ prove a motivation with a subproof
- ✦ add a new step in a proof chain, in order to show some reasoning in more detail, or remove an existing proof step
- ✦ change a subproof into a lemma, so that it can be used also in other parts of the proof, or vice verse, change a lemma to a subderivation, if it turns out that the lemma is only needed in one place