(a) Principal Approaches to Writing Verified Software

(b) The Theorem Prover Agda

(c) Concept of a Type

(d) Rules and Judgements

(e) Dependent Judgements

(f) Dependent Types

(g) Examples of Dependent Types in Programming.
(i) **First a program is written.**
Then its correctness is verified.

- Most common approach, when formal methods are applied.
- **Main advantage:**
  Ordinary programming languages can be used.
- **Disadvantage:** all or most considerations of the programmers are lost.
- Requires advanced automated theorem proving technologies.
- **Dr. Kullmann** is an expert on the theorem proving techniques.

(ii) **Prove that a solution for the problem exists.**
Extract a program from it.

- Technology not yet far developed.
- **Dr. Berger** is an expert in this area of research.
(iii) **Programs written in a language which allows to state properties of the program.**

Example: “This program sorts a list”. Properties should be verified when compiling the program.

- **Advantages:**
  * Programmer is forced to think very clearly.
  * Programs will be very well documented.
  * The information about properties needed might guide the programmer.
    In some cases parts of the program can even be found automatically.

- **Disadvantages:**
  * Requires new programming languages.
  * Still essentially area of research. However advanced tools exist already.
  * Might be too difficult for ordinary programmers.

- **Effect:**
  * Proving and programming will be the same.
Principal Approaches to Writing Verified Software (Cont.)

(iv) **Mixtures** between (i), (iii).

- E.g. SPARK Ada.

In this lecture, we will follow the approach of (iii), based on dependent type theory.
There are several implementations of dependent type theory:

- NuPrl (Cornell, USA), the technically most advanced system.
- Coq (INRIA, France), as well technically very advanced.
- LEGO (Edinburgh), about to be replaced.
- The “Alf-family” (Gothenburg, Sweden) – has probably the clearest concepts.
  * Alf (developed by Lena Magnusson)
  * Half (= Haskell Alf), developed by Thierry Coquand, Dan Synek.
  * Agda developed by Catarina Coquand.
  * Alfa, a graphical user interface for Agda, developed by Thomas Hallgren.

In this module we will use Agda, but Alfa can be used to create Agda code.
• Half, Agda, Alf are written in Haskell.

• Half and Agda have an Emacs mode, which makes it quite convenient to develop proofs in it.

• In most theorem provers, one has to follow one or several goals, and derive proofs for them. This is close to the way, proofs are carried out by hand.
The Alf-family has a different approach of successive refinement:
- One starts writing the proof code similarly to writing functional programs.
- What cannot be done without machine assistance can be left open in the form of holes (goals).
- Now one can successively, assisted by the system, fill in those goals.
- Therefore proof/program development in the Alf family is very close to ordinary programming.
Installation of Agda

• Agda is installed in the Linux lab.
  – Follow the item “Getting started with Agda” on the module.
  – Please check whether the installation works.

• Agda is most easily installed under Linux or other versions of Unix.

• It has been reported that it can be installed under CYGWIN, a UNIX emulation under Windows.

• See information from the course home page.

• The source code for the examples given in this lecture will be available from the course home page.
Typed vs. untyped languages

- **Examples of typed languages:**
  Pascal, C, C++, Java, C#, Haskell, ML.

- **Examples of untyped languages:**
  Perl, Python, Visual Basic, Lisp.

- **Advantage of untyped languages:**
  Greater freedom in programming.

- **Advantage of typed languages:**
  Many errors are avoided, especially when using operations defined somewhere else.
  To find such errors in untyped languages can be very difficult.
• In order to guarantee **correctness of software**, we make use of a much more refined type system.
  
  – It will allow to specify any property of a program, which can be defined as a formula, as a type.
Types used in other Languages

- **Scalar types:**
  Booleans, integers, floating point numbers, characters, enumeration types.

- **Simple compound types:**
  Arrays, strings, record types, lists, sets.

- In **functional programming** additionally:
  Function types, inductive data types (= what can be defined using “data”).

- In **object-oriented programming** (not relevant here): interfaces (and classes).
•**Function types.**
  Int → Int is the type of functions mapping integers to integers.

• **Products** (essentially records).
  Int × Int is the type of pairs ⟨r, s⟩, where r, s are integers.
  – E.g. ⟨2, 3⟩ : Int × Int.
  – Haskell notation
    * for A × B is (A, B),
    * for ⟨a, b⟩ is (a, b).
    e.g. (2, 3) :: (Int, Int).

• **Inductive data types.** More about this later.

• **Dependent versions** of the above.
• The type theory will allow us to both write programs and prove their correctness.

• Correctness of programs is determined by their types.
  – Therefore we derive that a program \( p \) is of a type \( A \), written \( f : A \)
  
  – Example: for a sorting algorithm, we derive:

\[
\text{sort : NatList } \rightarrow \text{ SortedList}.
\]
• With all programs a type will be associated.

• Deriving the type of a program in Agda will look like programming.
Remark on the Syntax Used

- In type theory, one usually uses as in Pascal single colons `:` for "has type".
- In Haskell `:` is used in lists, and `::` is used for "has type".
- In order to be close to Haskell and Cayenne, it was decided to use in Agda as well `::` (although lists don’t play an important rôle there).
- In this lecture we will
  - usually use `:`,
  - except when referring to explicit Agda code (then `::`).
Remark on the Syntax Used (Cont.)

• Similarly for $\lambda$:
  
  - In type theory one uses $\lambda x . r$.
  - If one is more explicit about the type of $x$, one can write $\lambda (x : A). r$.
  
    \[ \lambda (x : A). r \]

  - In Agda one writes $\text{\textbackslash}(x :: A) \rightarrow r$.
    
    * $A$ can usually be inferred by Agda automatically.
  - We use usually $\lambda (x : A). t$ except when referring to Agda.
  - We often omit $A$, writing simply $\lambda x . t$.  

Critical Systems, CS_411, Lentterm 2003, Sec. B1
Rules

• In functional programming, one creates a file containing expressions, sometimes together with their types. E.g. one has defined before $f : A \rightarrow B$, $a : A$. Now one can introduce $f \, a : B$.

• The simple type theory of e.g. Haskell makes it easy to do this "by hand".

• Dependent type theory is more subtle, and it is helpful to explain concepts by using rules.
• Consider the formation of
  \[ f \, a : B \]
  using \( f : A \rightarrow B \) and \( a : A \).

• The steps taken before correspond to having a rule:
  If \( f : A \rightarrow B, \ a : A \), then \( f \, a : B \).
  We write briefly for it
  \[
  \frac{f : A \rightarrow B \quad a : A}{f \, a : B}
  \]
• So a rule is something like a **template**: 
  \( f, A, B, a \) in the previous example can be replaced by any expression.

• Rules might have **zero premises**, e.g.

  \[ 0 : \mathbb{N} \]

  (0 is a natural number).

  – In this case the **“fraction line” will be omitted.**
Example 1

- We can use the above rule to create longer derivations:

\[
\frac{f : A \to (B \to C) \quad a : A}{f\ a : B \to C \quad b : B} \quad \frac{f \ a\ b : C}{f\ a\ b : C}
\]

- We will abbreviate \( A \to (B \to C) \) by \( A \to B \to C \).

- The above uses 2 applications of the previous rule.
  - First one with premises \( f \) of type \( A \to B \to C \) and \( a \) of type \( A \):
    * \( f \) in the rule is \( f \),
    * \( A \) in the rule is \( A \),
    * \( B \) in the rule is \( B \to C \),
    * \( a \) in the rule is \( a \).
Example 1 (Cont.)

\[
f : A \rightarrow (B \rightarrow C) \quad a : A \quad b : B
\]

\[
\frac{f a : B \rightarrow C \quad b : B}{f a b : C}
\]

- Then one with premises \(fa\) of type \(B \rightarrow C\) and \(b\) of type \(B\).
  - \(f\) in the rule is \(fa\),
  - \(A\) in the rule is \(B\),
  - \(B\) in the rule is \(C\),
  - \(a\) in the rule is \(b\).

Critical Systems, CS.411, Lentterm 2003, Sec. B1
Example 2

- Derivation of \((\lambda(x : A).x)a : A\), provided \(a : A\). (We assume a derivation of \(\lambda(x : A).x : A \to A\)).

\[
\begin{align*}
\lambda(x : A).x : A \to A & \quad a : A \\
\hline
(\lambda(x : A).x)a : A 
\end{align*}
\]

- This uses 1 application of the previous rule.
  - \(f\) in the rule is \(\lambda(x : A).x\),
  - \(A\) in the rule is \(A\),
  - \(B\) in the rule is \(B\),
  - \(a\) in the rule is \(a\).
• In Agda, these rules are implicit.

• The rule

\[
\frac{f : A \to B \quad a : A}{f \ a : B}
\]

corresponds to the following:

• Assume we have introduced:
  
  – \( f :: A \to B, \ a :: A \).

  and want to solve the goal

  – \( \{! !\} :: B \).
  
  – Goal \( \{! !\} \) means: we don’t know yet what to fill in.
• Then we can fill this goal by typing in \( f \ a \):

• \( \{! \ f \ a \ ! \} :: B \)

• If we then choose menu “refine”, the system shows:

• \( f \ a :: B \).
Support given by the System

• However, one might not know what to fill in.

• One might guess it has something to do with $f$. So one inserts $f$ and uses menu “refine”.

• The system shows $f \{! !\} :: B$.

• We can ask for the type of the new goal $\{! !\}$, and get: $\{ ! ! \}$.

• Now we can solve this goal by filling in $a$ and using refine.

• See exampleSimpleDerivation.agda, exampleSimpleDerivation2.agda.
• In ordinary functional programming, it is easy to determine correctly formed types. In dependent type theory the type structure is richer and more complicated.

• Proof steps are required to conclude that something is a type.

• Therefore we have not only the judgement as in functional programming:

\[ a : A \]

but as well a typing judgement \( A \) is a type, written:

\[ A : \text{Type} \]
Judgements (Cont.)

- Before deriving $a : A$ we first have to show $A : \text{Type}$. 
Equality Judgements

• On a machine level, terms, which reduce to the same, will be identified:
  E.g. $s := (\lambda (x : A).x) \, r$ and $r$ will be identified.

• If one needs at some place $r$, one can insert $s$ instead of $r$ and vice versa.

• In Agda this is done automatically, the user doesn't see such equalities.
  – See exampleSimpleEquality.agda.

• When using rules, we need to be able to express that we can replace $r$ by $s$.

• Therefore we need a judgment, which states that $r$ and $s$ are equal.
  – $r$ and $s$ should have equal types, say $A$.
  – The judgement is written as $r = s : A$. 

Critical Systems, CS_411, Lentterm 2003, Sec. B1
Equality Judgements (Cont.)

- Similarly, we will have equality between types, written as

\[ A = B : \text{Type} \]

- This is something novel in dependent type theory.
  - In simple type theory, there is only one way of writing a
We have the following 4 types of judgements:

- \( A : \text{Type} \) "\( A \) is a type".
- \( a : A \) "\( a \) is of type \( A \)".
- \( A = B : \text{Type} \) "\( A \) and \( B \) are equal types".
- \( a = b : A \) "\( a \) and \( b \) are equal elements of type \( A \)".

**In Agda**, only \( A : \text{Type} \) and \( a : A \) are explicit.
(e) Dependent Judgements

• Consider the judgement in functional programming:

$$\lambda(x : A).x : A \rightarrow A$$

• It turns out that the most suitable rule for deriving \( \lambda \)-expression has as premise in the above case:
  If \( x : A \) then \( x : A \).

• This requires that we have judgements, which depend on variables.
• “If $x : A$ then $x : A$ is written as

\[ x : A \Rightarrow x : A \]

Here $x : A$ is called \textit{context}.

• In general this context can consist of several variables.
  – For instance, if $A : \text{Type}$, we can derive

\[ f : A \rightarrow A, a : A \Rightarrow f a : A \]
Example

• Assume we have an operation for concatenating strings:

\[
\text{concat} : (x : \text{String}, y : \text{String}) \rightarrow \text{String}
\]

• We want to define an operation double, which doubles a string:

  – double("Hello") = "HelloHello".
  – double: String \rightarrow String.
• We start by assuming $x : \text{String}$:
  $$x : \text{String} \Rightarrow x : \text{String}.$$ 

• The first argument of concat is a string, so we can apply concat to $x$:
  $$x : \text{String} \Rightarrow \text{concat } x : \text{String} \to \text{String}.$$ 
  
  – concat $x$ is the function, which takes a string $y$ and puts $x$ in front of it.

• The right hand side is a function, and can be applied to $x$:
  $$x : \text{String} \Rightarrow \text{concat } x 
  x : \text{String}.$$ 

• Now we can abstract from $x$:
  $$\text{double} := \lambda (x : \text{String}) \to \text{concat } x 
  x : \text{String} \to \text{String}.$$
Currying/Uncurrying

- We were using a **curried** version of `concat`:
  - `concat` has two arguments. If applied to one string, we obtain a function `concat x :: String -> String`. That function takes one argument `y` and returns the concatenation of `x` and `y`.
  - Called the **curried** version of `concat`.
• This is the same mechanism as in Haskell

• In Haskell, \((+) : \text{Int} \to \text{Int} \to \text{Int}\) can be applied to one argument:
  
  – \((+) 3\) is the function, which takes a number and returns that number incremented by 3.
  
  Therefore \((+\ 3\ 5\) (which is \(((+)\ 3)\ 5\) and is usually written \(3\ +\ 5\) returns 8.

  – \(\text{map ((+)}\ 3\ [1, 2, 3]\) returns the application of \((+)\ 3\) to \([1, 2, 3]\), namely \([4, 5, 6]\).
• The **uncurried** version `concat'` of `concat` takes as argument two strings.

• So we when applying `concat'` to two strings, we **first form** a pair of two arguments, and then apply the function to it.

• In dependent type theory it has type `(String × String) → String`, and is written like `concat ⟨x, y⟩`.

• In Haskell this would be written as `(String, String) → String`, and we would write `concat(x, y)` for the application.
  
  – Note that `(x, y)` is the **pair** consisting of `x` and `y`.
• The complete derivation of double reads as follows, given

- Note that the rules we are using haven’t been introduced.

\[
\begin{align*}
\text{concat : String} & \rightarrow \text{String} \\
x : \text{String} \Rightarrow x : \text{String} & \quad x : \text{String} \Rightarrow \text{concat} : \text{String} \\
& \quad x : \text{String} \Rightarrow \text{concat} \ x : \text{String} \rightarrow \text{String} \\
& \quad x : \text{String} \Rightarrow x : \text{String} \quad x : \text{String} \Rightarrow \text{concat} \ x : \text{String} \Rightarrow \text{concat} \ x \ x : \text{String} \\
& \quad \lambda(x : \text{String}) \Rightarrow \text{concat} \ x \ x : \text{String} \rightarrow \text{String}
\end{align*}
\]
Example (Cont.)

- In the previous derivation, we first expanded the context of a not needed \( x : \text{String} \):

\[
\text{concat} : \text{String} \rightarrow \text{String} \rightarrow \text{String} \\
\frac{}{x : \text{String}} \Rightarrow \text{concat} : \text{String} \rightarrow \text{String} \rightarrow \text{String}
\]

- This was so that when applying the rule

\[
\frac{}{x : \text{String}} \Rightarrow x : \text{String} \quad \frac{}{x : \text{String}} \Rightarrow \text{concat} : \text{String} \rightarrow \text{String} \rightarrow \text{String}
\]

we have in both premises the same context.
Example (Cont.)

• This is a bit pedantic, and often one omits this step and writes the top of the above derivation simply as:

\[
x : \text{String} \Rightarrow x : \text{String} \quad \text{concat} : \text{String} \to \text{String}
\]

\[
x : \text{String} \Rightarrow \text{concat} x : \text{String}
\]

• Further writing \( a : A \) is the same as \( \Rightarrow a : A \) (with empty context).
  – If we have no context, we usually omit the \( \Rightarrow \).
Contexts in Agda

• In Agda, we have no explicit contexts, since we don’t use rules. However, if we have the open judgement

\[ f \ (x :: B) :: A = \{! !\} \]

• Then we can make use of \( x :: B \) for refining the goal. This context can be shown with a menu.

• See exampleShowContext.agda.
Example: Derivation of double

(See `exampleDoubleString.agda`).

- We start with

\[
\text{double } (x :: \text{String}) :: \text{String} = \{! \! \}
\]

- We can insert into the goal `concat`:

\[
\text{double } (x :: \text{String}) :: \text{String} = \{! \text{concat} !\}
\]
Example: Derivation of double (Cont.)

- When using menu refine, we obtain:

\[
\text{double } (x :: \text{String}) \\
:: \text{String} \\
= \text{concat } \{! !\} \{! !\}
\]

- We check with Agda, that the two new goals require both type \text{String}.

- We can check the context of each of these goals and find

\[x :: \text{String}.\]
• We insert \( x \) into the first goal and refine:

\[
\begin{align*}
\text{double } (x :: \text{String}) \\
:: \text{String} \\
= \text{concat } x \{! \!\! \} 
\end{align*}
\]

• Doing the same with the second goal gives:

\[
\begin{align*}
\text{double } (x :: \text{String}) \\
:: \text{String} \\
= \text{concat } x \; x 
\end{align*}
\]

• We are done.
• Assume we want to assign a type to a sorting function \texttt{sort}.

• It will be
  
  \texttt{sort : NatList \rightarrow SortedList}.

• We assume some notion of \texttt{NatList} (list of natural numbers).

• What is \texttt{SortedList}?
  
  – An element of \texttt{SortedList} is a list which is sorted.
  – It is a pair \langle l, p \rangle \text{ s.t.}
    
    \begin{itemize}
    
    \item \( l \) is a \texttt{NatList}.
    \item \( p \) is a proof or verification that \( l \) is sorted
    
    \end{itemize}
Sorted Lists

- For the moment, ignore what is meant by “sorted” as a type.

- Only important: Sorted depends on \( l \).
  - Sorted(\( l \)) is a predicate expressed as a type.

- Elements of SortedList are pairs \( \langle l, p \rangle \) s.t.
  - \( l : \text{NatList} \).
  - \( p : \text{Sorted}(l) \).

- Sorted(\( l \)) is a dependent type.
• If \( l \) is sorted, then \( \text{Sorted}(l) \) will have an element.
  – It is possibile to write a program which computes an element of \( \text{Sorted}(l) \).

• If \( l \) is not sorted, \( \text{Sorted}(l) \) will be empty, it has no element.
  – Then it is not possibile to write a program which computes an element of \( \text{Sorted}(l) \).
The Dependent Product

- Then the pair \( \langle l, p \rangle \) will be an element of

\[
\text{SortedList} := (l : \text{NatList}) \times \text{Sorted}(l)
\]

- SortedList is the type of pairs \( \langle l, p \rangle \) s.t.
  
  - \( l : \text{NatList} \),
  - \( p : \text{Sorted}(l) \).

  called the dependent product

- \( \text{sort} : \text{NatList} \rightarrow ((l : \text{NatList}) \times \text{Sorted}(l)) \) expresses:
  
  - \( \text{sort} \) converts lists into sorted lists.
The Dependent Function Type

- From a sorting function we know more:
  - It takes a list and converts it into a sorted list with the same elements.

- Assume a type (or predicate) EqElements\((l, l')\) standing for:
  - \(l\) and \(l'\) have the same elements.
The Dependent Function Type (Cont.)

- A refined version of sort has type

\[(l : \text{NatList}) \rightarrow ((l' : \text{NatList}) \times \text{Sorted}(l') \times \text{EqElements}(l, l'))\]

- “sort(l) is a list, which is sorted and has the same elements.”

- “sort is a program, which takes a list and returns a sorted list with the same elements.”

- The type of sort is an instance of the dependent function type:
  - The result type depends on the arguments.
Dependent types are often **needed in programming**. Some examples:

- In Java, a relatively big library of "collection classes" is available.
  - Provides implementations of lists, sets, hash tables etc.
  - It would be nice to have "lists of type \( A \)".
  - However **this is a dependent type**, depending on a type \( A \).
  - Cannot be expressed in Java.
  - Instead, in Java only **lists of elements of type Object** are available.
  - Elements of other types have to be **upcasted** to Object.
    - Elements of the list have then to be **downcasted** to their original type.
  
* Type checking happens at run time rather than at compile time.*
• Assume a class StudentEntry.

• If we have a list listOfStudentEntries, and add to it an element of type StudentEntry, this element will first be converted (upcasted) to type Object.

• If we retrieve an element (e.g. the first element) of listOfStudentEntries, we obtain an element of Object.
  – If it was originally a StudentEntry, we can cast this element to StudentEntry.
  – However, whether we have an element of StudentEntry cannot be determined at compile time, only at run time.
Polymorphism

• What is needed is a weak form of dependent types, called
  – Types might depend on other types but not on elements.

• In C++, this form of dependency is available (called templates).
  – One writes for instance List<A> for lists of type A.

• In Java it might be available in the next release 1.5.

• In Haskell and ML it is available.
  – E.g. \( \lambda x.x :: \alpha \Rightarrow \alpha \rightarrow \alpha \),
    i.e. \( \lambda x.x \) is of type \( \alpha \rightarrow \alpha \) for every type \( \alpha \).
Examples of Dependent Types in Programming

- **Matrix multiplication** is an operation, which takes three natural numbers \(n, m, k\), an \(n \times m\)-matrix and an \(m \times k\)-matrix, and has as result an \(n \times k\)-matrix.

The type of this function is a **dependent type**: The types of \(n \times m\)-matrices, \(m \times k\)-matrices and \(n \times k\)-matrices depend on \(n, m, k\).

- Usually, this problem is solved by
  * taking matrices which are big enough and restricting to
    \(n \times m, m \times k\) and \(n \times k\) sub-matrices,
    - waste of memory
  * or by dynamically allocating arrays.
    - This means memory allocation has to be done at run-time.

  - In both solutions, checking that the dimensions are in accordance has to be done at **run-time**.
• Let $\mathbb{N}$ be the type of natural numbers (i.e. $0, 1, \ldots$; $\mathbb{N}$ will be introduced later).

• Let $\text{Mat}(n, m)$ be the type of $n \times m$-matrices. (Will be introduced later).

Then matrix multiplication has type

$$(n : \mathbb{N}) \rightarrow (m : \mathbb{N}) \rightarrow (k : \mathbb{N}) \rightarrow \text{Mat}(n, m) \rightarrow \text{Mat}(m, k) \rightarrow \text{Mat}(n, k)$$
Type of Matrix multiplication (Cont.)

- A shorter notation for this type is

\[
(n, m, k : \mathbb{N}) \\
\rightarrow \text{Mat}(n, m) \\
\rightarrow \text{Mat}(m, k) \\
\rightarrow \text{Mat}(n, k)
\]
Examples of Dependent Types in Programming (Cont.)

**Digital Components.**

- A digital component (e.g. a logic gate) with $n$ inputs and $m$ outputs can be considered as a function $\text{Bool}^n \rightarrow \text{Bool}^m$.

- In general such a component is a triple consisting of
  - $n$, the number of inputs,
  - $m$, the number of outputs,
  - a function $f : \text{Bool}^n \rightarrow \text{Bool}^m$.

- The type of $f$ depends on $n$ and $m$, an example of a dependent type.
Examples of Dependent Types in Programming (Cont.)

- **Predicates** are dependent types.
  - See the types of *sort* above.

- **Aarne Ranta** has used dependent types in *linguistics*:
  - In a sentence like “The man goes home”, the predicate (“goes”) depends on, whether the subject (“The man”) is singular or plural.
  - He constructed **grammars based on dependent types** for translating sentences between different languages.