IV.2 (a) Definition of the URM

A model of computation consists of a set of partial computable functions together with methods, which describe how to compute those functions.

- One aims at models of computation which are complete.
  - Here a model of computation is complete, if it contains all computable functions.
  - Since “intuitively computable” is not a mathematical notion, completeness is not a mathematical notion and cannot be proved mathematically.
IV.2 (a) Definition of the URM

Turing Completeness

▶ Sometimes by "complete" it is meant that the model contains all functions computable by a Turing machine – then one obtains a mathematical definition.
▶ We use Turing complete for this mathematical definition.
  ▶ So a model is Turing complete if it contains all functions computable by a Turing machine.

Models of Computation

▶ Aim: an as simple model of computation as possible: constructs used minimised, while still being able to represent all intuitively computable functions.
  ▶ Makes it easier to show for other models of computation, that the first model can be interpreted in it.
  ▶ In mathematics one always aims at giving as simple and short definitions as possible, and to avoid unnecessary additions.
▶ Models of computation are mainly used for showing that something is non-computable rather than for showing that something is computable in this model.

Models of Computations Discussed

In this module we will discuss 2 models of computation:
▶ The URM.
  ▶ Minimalised version of a machine language of a computer.
  ▶ Model which represents what can be carried out on a computer with a von Neumann architecture.
▶ The Turing machine.
  ▶ Abstraction of computation on a piece of paper.

There are other models of computation.

For instance the set of functions computable by a Java program forms a Turing complete model of computation.

The URM

▶ The URM (the unlimited register machine) is one model of computation.
  ▶ Particularly easy.
  ▶ It defines a virtual machine, i.e. a description how a computer would execute its program.
  ▶ The URM is not intended for actual implementation (although it can easily be implemented).
  ▶ It is not intended to be a realistic model of a computer.
  ▶ It is intended as a mathematical model, which is then investigated mathematically.
  ▶ Not many programs are actually written in it – one shows that in principal there is a way of writing a certain program in this language.
IV.2 (a) Definition of the URM

The URM

- Rather difficult to write actual programs for the URM.
- Low level programming language (only goto)
- URM idealised machine – no bounds on the amount of memory or execution time
  - however all values will be finite.
- Many variants of URM – this URM will be particularly easy.

Description of the URM

- The URM consists of
  - infinitely many registers \( R_i \)
    - can store arbitrarily big natural number;
  - a URM program consisting of a finite sequence of instructions \( I_0, I_1, I_2, \ldots I_n \);
  - and a program counter PC.
    - stores a natural number.
    - If PC contains a number \( 0 \leq i \leq n \), it points to instruction \( I_i \).
    - If content of PC is outside this range, the program stops.

Remark

- Note that the URM program is part of the URM.
- One could distinguish between
  - The architecture of a URM consisting of registers, the program counter and a memory for a URM program,
  - and the URM program itself.
- For historic reasons by a URM we mean the URM architecture together with a URM program.
IV.2 (a) Definition of the URM

The URM

\[ R_0 \ R_1 \ R_2 \ R_3 \ R_4 \ R_5 \ R_6 \ R_7 \ R_8 \ R_9 \ \cdots \]

\[ I_0 \ I_1 \ I_2 \ I_3 \ I_4 \ I_5 \ I_6 \ I_7 \ I_8 \ I_9 \]

**Program has terminated**

**Execute Instruction**

**URM Instructions**

- 3 kinds of **URM instructions**.
  - The **successor instruction**
    \[ \text{succ}(k) \]
    where \( k \in \mathbb{N} \).
  - Execution:
    - Add 1 to register \( R_k \).
    - Increment PC by 1.
    - \( \rightarrow \) execute next instruction or terminate.
  - A more readable notation is
    \[ R_k := R_k + 1 \]
  - The **predecessor instruction**
    \[ \text{pred}(k) \]
    where \( k \in \mathbb{N} \).
  - Execution:
    - If \( R_k \) contains value > 0, decrease the content by 1.
    - If \( R_k \) contains value 0, leave it as it is.
    - In all cases increment PC by 1.
  - A more readable notation is
    \[ R_k := R_k - 1 \]
IV.2 (a) Definition of the URM

**URM Instructions**

- **The conditional jump instruction**

  \[ \text{ifzero}(k, q) \]

  where \( k, q \in \mathbb{N} \). Execution:

  - If \( R_k \) contains 0, PC is set to \( q \)
    → next instruction is \( I_q \), if \( I_q \) exists.
    If no instruction \( I_q \) exists, the program stops.
  - If \( R_k \) does not contain 0, the PC incremented by 1.
    → Program continues executing the next instruction, or terminates, if there is no next instruction.
  - A more readable notation is

  \[
  \text{if } R_k = 0 \text{ then goto } q
  \]

**Finiteness**

- A URM program refers only to **finitely many registers**, namely those referenced explicitly in one of the instructions.

**Example of a URM Program**

- The following is an example of a URM-program:

  \[ I_0 = \text{ifzero}(0, 3) \]
  \[ I_1 = \text{pred}(0) \]
  \[ I_2 = \text{ifzero}(1, 0) \]
Example

\[ I_0 = \text{ifzero}(0, 3) \quad I_1 = \text{pred}(0) \quad I_2 = \text{ifzero}(1, 0) \]

If we run this program with initial values \( R_0 = 2, \ R_1 = 0 \), we obtain the following trace of a run of this program:

<table>
<thead>
<tr>
<th>Instruction</th>
<th>( R_0 )</th>
<th>( R_1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( I_0 )</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>( I_1 )</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>( I_2 )</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>( I_0 )</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>( I_1 )</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>( I_2 )</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( I_0 )</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( I_3 )</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

URM Stops

Operation of the Example

\[ I_0 = \text{ifzero}(0, 3) \quad I_1 = \text{pred}(0) \quad I_2 = \text{ifzero}(1, 0) \]

- Assume \( R_1 \) is initially zero.
- Then \( R_1 \) will never be changed by the program, so it will remain 0 forever.
- So in instruction 2 the URM will always jump to instr. 0.
- Then the program will as long as \( R_0 \neq 0 \) decrease \( R_0 \) by 1.
- The result is that \( R_0 \) is set to 0.
- This corresponds to the instruction from a higher level language \( R_0 := 0 \).

URM-Computable Functions

- For every URM-program we define the function defined by it.
- In fact there are many functions which are defined by the same U-program:
  - A unary function \( U^{(1)} \), which stores its argument in \( R_0 \), sets all other registers to 0, then starts to run the U.
    - If the U stops, the result is read off from \( R_0 \).
    - Otherwise the result is undefined.
  - A binary function \( U^{(2)} \), which stores its two arguments in \( R_0 \) and \( R_1 \), then operates as \( U^{(1)} \).
  - And so on. In general we obtain a \( k \)-ary partial function \( U^{(k)} \) for every \( k \geq 1 \).

Partial Functions

- The functions \( U^{(1)}, U^{(2)}, \ldots \) will be partial, since not for all inputs we obtain an output.
- A partial function \( f : A \leadsto B \) is a function mapping some elements of \( A \) to elements of \( B \).
- We write
  - \( f(a) \downarrow \) for "\( f(a) \) is defined" (\( f(a) \) returns an element of \( B \)).
  - \( f(a) \uparrow \) for "\( f(a) \) is undefined".
  - \( f(a) \rightleftharpoons t \) ("\( f(a) \) is partially equal to term \( t \)") for "\( f(a) \) and \( t \) are both undefined or both defined and return the same value".
  - \( f(a) = t \) for "both \( f(a) \) and \( t \) are defined and return the same value".
  - \( \bot \) for the term which is always undefined (pronounced "bottom").
Partial Functions

- So in case \( f(a) \simeq g(a') \) we only demand that if one of \( f(a) \) or \( g(a') \) are defined then both are defined and return the same result.
- If we write \( f(a) = g(a') \) we demand that both \( f(a) \) and \( g(a') \) are defined and return the same value.
- \( f(a) \simeq \perp \) means the same as \( f(a) \uparrow \).

Domain Theory

- There is a theory called “domain theory” in which there is an ordering on the definedness of objects.
- For instance if \( f, g : \mathbb{N} \to \mathbb{N} \) only differ by \( f(0) \downarrow, g(0) \uparrow \), then we can consider \( g \) to be more defined than \( f \).
- \( \perp \) is the completely undefined element, therefore it is called \textbf{bottom} for being the least element in this order.

Definition \( U^{(k)} \)

- Let \( U = I_0, \ldots, I_{n-1} \) be a URM program, \( k \in \mathbb{N}, k \geq 1 \).
- We define a function \( U^{(k)} : \mathbb{N}^k \to \mathbb{N} \) by determining how it is computed:
  - Assume we want to compute \( U^{(k)}(a_0, \ldots, a_{k-1}) \).
  - **Initialisation:**
    - PC set to 0.
    - \( a_0, \ldots, a_{k-1} \) stored in registers \( R_0, \ldots, R_{k-1} \), respectively.
    - All other registers set to 0.
      (Sufficient to do this for registers referenced in the program).

URM-Computable Functions

- **Iteration:**
  As long as the PC points to an instruction, execute it. Continue with the next instruction as given by the PC.
- **Output:**
  - If PC value \( > n \), the program stops.
  - The function returns the value in \( R_0 \).
  - So if \( R_0 \) contains \( b \) then
    \[ U^{(k)}(a_0, \ldots, a_{k-1}) \simeq b \, . \]
  - If the program never stops,
    \[ U^{(k)}(a_0, \ldots, a_{k-1}) \uparrow \, . \]
IV.2 (a) Definition of the URM

URM-Computable Functions

- \( f : \mathbb{N}^k \rightarrow \mathbb{N} \) is **URM-computable**, if \( f = U^{(k)} \) for some \( k \in \mathbb{N} \) and some URM program \( U \).

---

Example

Consider the example of a URM-program treated before:

\[
\begin{align*}
I_0 &= \text{ifzero}(0,3) \\
I_1 &= \text{pred}(0) \\
I_2 &= \text{ifzero}(1,0)
\end{align*}
\]

- We have seen that if \( R_1 \) is initially zero, then the program reduces \( R_0 \) to 0 and then stops.

---

Example

\[
\begin{align*}
I_0 &= \text{ifzero}(0,3) \\
I_1 &= \text{pred}(0) \\
I_2 &= \text{ifzero}(1,0)
\end{align*}
\]

- A computation of \( U^{(1)}(k) \) is as follows:
  - We set \( R_0 \) to \( k \), all other registers to 0.
  - Then the URM program is executed, starting with instruction \( I_0 \).
  - This program terminates, with \( R_0 \) containing 0.
  - The value returned is the content of \( R_0 \), i.e. 0.
  - Therefore \( U^{(1)}(k) \simeq 0 \).

- In order to compute \( U^{(2)}(k, l) \) we have to do the same, but set initially \( R_0 \) to \( k \), \( R_1 \) to \( l \).
  - For \( l = 0 \) we obtain the same run of the URM program as before.
    - Therefore \( U^{(2)}(k, 0) \simeq 0 \).
  - What is \( U^{(2)}(k, l) \) for \( l > 0 \)?
IV.2 (a) Definition of the URM

Partial Computable Functions

- For a **partial** function $f$ to be computable we need only:
  - If $f(a) \downarrow$, then after finite amount of time we can determine this property, and the value of $f(a)$.
  - If $f(a) \uparrow$, we will wait infinitely long for an answer, so we never determine that $f(a) \uparrow$.
  - **Turing halting problem** is the question: “Is $f(a) \downarrow$?”. Turing halting problem is **undecidable**.
  - If we want to have always an answer, we need to refer to **total computable functions**.

Example of URM-Comp. Function

The following function is computable:

$$f : \mathbb{N}^2 \rightarrow \mathbb{N}, \quad f(x, y) \equiv x + y$$

We derive a URM-program for it in several steps.

**Step 1:**
Initially $R_0$ contains $x$, $R_1$ contains $y$, and the other registers contain 0. Program should then terminate with $R_0$ containing $f(x, y)$, i.e. $x + y$.

A higher level program is as follows:

$$R_0 := R_0 + R_1$$

**Step 2:**
Only successor and predecessor available, replace the program by the following:

```
while (R_1 \neq 0) do {
    R_0 := R_0 + 1
    R_1 := R_1 - 1
}
```

- This increases $R_0$ by 1 as many times as the value contained in $R_1$.
- This means that the content of $R_1$ is added to $R_0$.
- Note that at the end of the run, $R_1$ contains 0. But this is no problem since the at the end we only read off the result from $R_0$, and ignore $R_1$. 

In order to describe the total computable functions, we need to introduce the partial computable functions first.

- There is no program language s.t.
  - it is decidable whether a string is a program,
  - and the program language describes all total computable functions.
- This is essentially a consequence of the undecidability of the Turing Halting Problem.
IV.2 (a) Definition of the URM

Example of URM-Comp. Function

while \((R_1 \neq 0)\) do \{\(R_0 := R_0 + 1\)  \\
\(R_1 := R_1 - 1\)\}

**Step 3:**
Replace the while-loop by a goto:

**LabelBegin:** if \(R_1 = 0\) then goto **LabelEnd**;
\(R_0 := R_0 + 1\);
\(R_1 := R_1 - 1\);
goto **LabelBegin**;

**LabelEnd:**

**Step 4:**
Replace last goto by a conditional goto, depending on \(R_2 = 0\).
\(R_2\) is initially 0 and never modified, therefore this jump will always be carried out.

**LabelBegin:** if \(R_1 = 0\) then goto **LabelEnd**;
\(R_0 := R_0 + 1\);
\(R_1 := R_1 - 1\);
if \(R_2 = 0\) then goto **LabelBegin**;

**LabelEnd:**

**Step 5:**
Resolve labels:

0: if \(R_1 = 0\) then goto 4;
1: \(R_0 := R_0 + 1\);
2: \(R_1 := R_1 - 1\);
3: if \(R_2 = 0\) then goto 0;
4:

**Step 6:**
Translate the program into a URM program \(I_0, I_1, I_2, I_3\):

\(I_0 = \text{ifzero}(1, 4)\)
\(I_1 = \text{succ}(0)\)
\(I_2 = \text{pred}(1)\)
\(I_3 = \text{ifzero}(2, 0)\)
IV.2 (b) Higher level programming concepts for URMs

In this Subsection we will introduce some higher level program constructs for URMs, and how to translate them back into the original URM language.

These constructs will be still be rather low level in terms of the theory of programming languages, but high enough in order to allow easily to introduce the programs needed in this module.

Convention Concerning Jump Addresses

- When inserting URM programs $U$ as part of new URM programs, jump addresses will be adapted accordingly.
- E.g., in
  
  $\text{succ}(0)$
  
  $U$
  
  $\text{pred}(0)$

  we add 1 to the jump addresses in the original version of $U$.

- Furthermore, we assume that, if $U$ terminates, it terminates with the PC containing the number of the first instruction following $U$.
  - Means that if we then insert $U$, and a run of $U$ terminates, the next instruction to be executed is the one following $U$.

More Readable Statements

- We use the more readable statements
  
  $R_k := R_k + 1$ for $\text{succ}(k)$,
  
  $R_k := R_k - 1$ for $\text{pred}(k)$,
  
  if $R_k = 0$ then goto $q$ for $\text{ifzero}(k, q)$.
IV.2 (b) Higher level programming concepts for URMs

Labelled URM programs

- We introduce labelled URM programs.
- It will be easier to translate them back into original URM programs.
- The label End denotes the first instruction following a program.
- So instead of
  
  $I_0 = \text{if } R_0 = 0 \text{ then goto } 3$
  $I_1 = \text{ } R_0 := R_0 - 1$
  $I_2 = \text{if } R_1 = 0 \text{ then goto } 0$

  we write

  \[ \text{LabelBegin: } I_0 = \text{if } R_0 = 0 \text{ then goto } \text{End} \]
  \[ I_1 = \text{ } R_0 := R_0 - 1 \]
  \[ I_2 = \text{if } R_1 = 0 \text{ then goto } \text{LabelBegin} \]

  \[ \text{End: } \]

Omitting $I_k =$

- We omit now “$I_k =$”.
- Furthermore, labels don’t have to start with Label, so we can write Begin instead of LabelBegin.
- We obtain the following program:

  \[ \text{Begin: } \text{if } R_0 = 0 \text{ then goto } \text{End} \]
  \[ R_0 := R_0 - 1 \]
  \[ \text{if } R_1 = 0 \text{ then goto } \text{Begin} \]

  \[ \text{End: } \]

  Since End : is always the first instruction following the program, we will omit the last line End :

Replacing Registers by Variables

We write variable names instead of registers.
So if $x, y$ denote $R_0, R_1$, respectively, we write instead of

\[ \text{Begin: } \text{if } R_0 = 0 \text{ then goto } \text{End} \]
\[ R_0 := R_0 - 1 \]
\[ \text{if } R_1 = 0 \text{ then goto } \text{Begin} \]

the following

\[ \text{Begin: } \text{if } x = 0 \text{ then goto } \text{End} \]
\[ x := x - 1 \]
\[ \text{if } y = 0 \text{ then goto } \text{Begin} \]

Goto

- goto mylabel;
  stands for the (labelled) URM statement
  \[ \text{if } \text{aux0} = 0 \text{ then goto mylabel; } \]
- Here aux0 is a register (which we can keep fixed), which is initially zero and never modified in the URM program, so it contains always 0.
IV.2 (b) Higher level programming concepts for URMs

Goto

So

LabelLoop : if x = 0 then goto End;
  x := x − 1
  goto LabelLoop;

stands for

LabelLoop : if x = 0 then goto End;
  x := x − 1
  if aux0 = 0 then goto LabelLoop;

for a new register aux0.

CS 236
Sect. IV.2 (b)
46a/ 117

Repeat Loop

A repeat loop has the form:

repeat{
  ⟨Instructions⟩
until ⟨condition⟩;

A repeat loop is executed by running the body again and again, until at the end of running it until ⟨condition⟩ is true.

So the loop is executed at least one, and then executed iteratively as long as ⟨condition⟩ is false.

So it is equivalent to

⟨Instructions⟩
while ¬⟨condition⟩ do {
  ⟨Instructions⟩

CS 236
Sect. IV.2 (b)
47/ 117

Repeat Loop

So a repeat loop

repeat{
  ⟨Instructions⟩
until x = 0;

can be replaced by the following URM program:

⟨Instructions⟩;
while (x ≠ 0) do {
  ⟨Instructions⟩;

Note that this results in doubling of ⟨Instructions⟩.

One can avoid this.

But the length of the resulting program is not a problem as long as we are not dealing with complexity theory.
x := 0

stands for the following program:
while (x ≠ 0) do {x := x − 1;};

y := x;

y := x;
stands for the following
(assuming x, y denote different registers, aux is new):

aux := 0
while (x ≠ 0) do {
x := x − 1;
aux := aux + 1;}; −−x = 0; aux = x ∼
y := 0;
y := y + 1;
while (aux ≠ 0) do {
aux := aux − 1;
x := x + 1;
y := y + 1;}; −−x = x ∼; y = x ∼; aux = 0;

Aliasing Problem

Note that if for x, y denoting the same register we would define
y := x as the same program as when they are different (using a while
loop) we obtain the following program (comments explain the effects
in this case):

aux := 0
while (x ≠ 0) do {
x := x − 1;
aux := aux + 1;}; −−x = 0; aux = x ∼
x := 0;
x := x + 1;
while (aux ≠ 0) do {
aux := aux − 1;
x := x + 1;
x := x + 1;}; −−x = x ∼; aux = 0;
IV.2 (b) Higher level programming concepts for URMs

Aliasing Problem

- Instead of assigning x to y (which means doing nothing), x is doubled in this program.
- The above is an occurrence of the aliasing problem.
- The aliasing problem occurs if we have procedure with parameters which modifies its arguments, and if this program doesn’t do what it is intended to do in case two of its arguments are instantiated by the same variable.
- Frequent reason for programming errors, which are difficult to detect.

\[ y := x; \]

- Note that the URM program \( y := x; \) preserved the value of \( x \).
  - So after executing the URM program, \( x \) contains the value as it had before starting the execution.
- Similarly, in the URM programs introduced on the next slides

\[
\begin{align*}
  x & := y + z \\
  x & := y - z
\end{align*}
\]

the values of \( y \) and \( z \) will preserved.

\[ x := y + z; \]

Assume \( x, y, z \) denote different registers.
\( x := y + z; \) stands for the following program (aux is an additional variable):

\[
\begin{align*}
x & := y; \quad \leadsto x = y \sim; y = y \sim \\
aux & := z; \\
\text{while} \ (aux \neq 0) \ \text{do} \{ \\
  aux & := aux + 1; \\
x & := x + 1; \}; \\
y & := y \sim + z \sim; \\
y & := y \sim; z = z \sim; aux = 0;
\end{align*}
\]

Assume \( x, y, z \) denote different registers.
Remember, that \( a \sim b := \max\{0, a - b\} \).
\( x := y - z; \)
is computed as follows (aux is an additional variable):

\[
\begin{align*}
x & := y; \\
aux & := z; \\
\text{while} \ (aux \neq 0) \ \text{do} \{ \\
  aux & := aux + 1; \\
x & := x + 1; \}; \\
y & := y \sim + z \sim; \\
y & := y \sim; z = z \sim; aux = 0;
\end{align*}
\]
Checking for Inequality

- We have \((x - y) + (y - x) \neq 0 \iff x \neq y\)

- Proof:
  - If \(x > y\), then 
    \[
    \begin{align*}
    x - y &> 0, \\
    y - x &= 0, \\
    (x - y) + (y - x) &> 0
    \end{align*}
    \]
  - If \(y > x\), then 
    \[
    \begin{align*}
    y - x &> 0, \\
    x - y &= 0, \\
    (x - y) + (y - x) &> 0
    \end{align*}
    \]

- So a while loop
  \[
  \text{while } (x \neq y) \text{ do } \{ \ldots \}
  \]
  can be replaced by
  \[
  \text{while } ((x - y) + (y - x) \neq 0) \text{ do } \{ \ldots \}
  \]

which can be replaced by

\[
\begin{align*}
\text{aux} &:= (x - y) + (y - x) \\
\text{while aux } \neq 0 \text{ do } \\
\{ \ldots \} \\
\text{aux} &:= (x - y) + (y - x) \\
\}
\]

If we unfold this further, we obtain the following:
Assume \( x, y \) denote different registers.

while \((x \neq y)\) do {
    \langle Statements \rangle;

stands for (\( \text{aux, aux_i} \) denote new registers):

\[
\begin{align*}
\text{aux}_0 &:= x - y; \\
\text{aux}_1 &:= y - x; \\
\text{aux} &:= \text{aux}_0 + \text{aux}_1; \\
\text{while} (\text{aux} \neq 0) &\text{ do }
\langle \text{Statements} \rangle \\
\text{aux}_0 &:= x - y; \\
\text{aux}_1 &:= y - x; \\
\text{aux} &:= \text{aux}_0 + \text{aux}_1; \}
\end{align*}
\]

We introduce some constructions for introducing URM-computable functions.

We will later introduce the set of partial recursive functions as the least set of functions closed under these constructions.

- Then by the fact that the URM-computable functions are closed under these operations it follows that all partial recursive functions are URM-computable.

We introduce first names for all functions constructed this way.

**Definition 2.1**

(a) Define the zero function \( \text{zero} : \mathbb{N} \rightarrow \mathbb{N}, \text{zero}(x) = 0 \).

(b) Define the successor function \( \text{succ} : \mathbb{N} \rightarrow \mathbb{N}, \text{succ}(x) = x + 1 \).

(c) Define for \( 0 \leq i < n \) the projection function \( \text{proj}^i : \mathbb{N}^n \rightarrow \mathbb{N}, \text{proj}^i(x_0, \ldots, x_{n-1}) = x_i \).

**Remark**

- Note that all total functions are as well partial, so we have for instance as well zero : \( \mathbb{N} \sim \mathbb{N} \).
- \( \text{proj}^0 : \mathbb{N} \rightarrow \mathbb{N} \) is the identity function: \( \text{proj}^0(x) = x \).
IV.2 (c) URM computable functions

Notations for Partial Functions

Definition (Cont)

(d) Assume

\[ g : (B_0 \times \cdots \times B_{k-1}) \rightarrow C, \]
\[ h_i : A_0 \times \cdots \times A_{n-1} \rightarrow B_i. \quad i = 0, \ldots, k-1 \]

Define

\[ f := g \circ (h_0, \ldots, h_{k-1}) : A_0 \times \cdots \times A_{n-1} \rightarrow C : \]
\[ f(\bar{a}) :\simeq g(h_0(\bar{a}), \ldots, h_{k-1}(\bar{a})) \]

In case of \( k = 1 \) we write \( g \circ h \) instead of \( g \circ (h) \).

Furthermore as usual

\[ g_1 \circ g_2 \circ \cdots \circ g_n := g_1 \circ (g_2 \circ (\cdots \circ (g_{n-1} \circ g_n))) \]

Definition (Cont)

(e) Assume

\[ g : N^k \rightarrow N, \]
\[ h : N^{k+2} \rightarrow N. \]

Then we can define a function \( f : N^{k+1} \rightarrow N \) defined by primitive recursion from \( g \) and \( h \) as follows:

\[ f(\bar{n}, 0) :\simeq g(\bar{n}) \]
\[ f(\bar{n}, m+1) :\simeq h(\bar{n}, m, f(\bar{n}, m)) \]

We write \( \text{primrec}(g, h) \) for the function \( f \) just defined.

So \( \text{primrec}(g, h) : N^{k+1} \rightarrow N \).

In the special case \( k = 0 \), it doesn’t make sense to use \( g() \).

Instead replace in this case \( g \) by some natural number.

So the case \( k = 0 \) reads as follows:

Assume \( a \in \mathbb{N} \), \( h : \mathbb{N}^2 \rightarrow \mathbb{N} \).

Define

\[ f : \mathbb{N} \rightarrow \mathbb{N} \]

by primitive recursion from \( a \) and \( h \) as follows:

\[ f(0) :\simeq a \]
\[ f(m+1) :\simeq h(m, f(m)) \]

We write \( \text{primrec}(a, h) \) for \( f \), so \( \text{primrec}(a, h) : \mathbb{N} \rightarrow \mathbb{N} \).
In Haskell we can define \texttt{primrec} as a higher-order function as follows:

\begin{verbatim}
data Nat = Z | S Nat
  deriving Show
\end{verbatim}

\begin{itemize}
  
  \item \texttt{primrec0} is the operator for primitive recursion
  
  \item defining a 1-ary function \texttt{primrec0 \ f \ a :: Nat \rightarrow Nat}
  
  \item from \texttt{f: Nat \rightarrow Nat \rightarrow Nat} and \texttt{a: Nat}

\end{itemize}

\begin{verbatim}
primrec0 :: Nat -> (Nat -> Nat) -> Nat -> Nat
primrec0 a g Z = a
primrec0 a g (S n) = g n (primrec0 a g n)
\end{verbatim}

\begin{itemize}
  
  \item \texttt{primrec1} is the operator for primitive recursion
  
  \item defining a 2-ary function \texttt{primrec1 \ f \ g :: Nat \rightarrow Nat \rightarrow Nat}
  
  \item from \texttt{f: Nat \rightarrow Nat \rightarrow Nat \rightarrow Nat} and \texttt{g: Nat \rightarrow Nat}

\end{itemize}

\begin{verbatim}
primrec1 :: Nat -> (Nat -> Nat) -> Nat -> Nat
primrec1 g h n Z = g n
primrec1 g h n (S m) = h n m (primrec1 g h n m)
\end{verbatim}

\begin{itemize}
  
  \item Addition can be defined using primitive recursion:

  Let \texttt{add \ :: \ N^2 \rightarrow N}, \texttt{add(x, y) := x + y}. We have

  \begin{align*}
  \text{add}(x, 0) & = x + 0 = x \\
  \text{add}(x, y + 1) & = x + (y + 1) = (x + y) + 1 = \text{add}(x, y) + 1
  \end{align*}


  Therefore

  \begin{align*}
  \text{add}(x, 0) & = g(x) \\
  \text{add}(x, y + 1) & = h(x, y, \text{add}(x, y))
  \end{align*}


  \begin{itemize}
    
    \item where

    \begin{align*}
    g : \mathbb{N} \rightarrow \mathbb{N} \\
    g(x) & := x \\
    h : \mathbb{N}^3 \rightarrow \mathbb{N} \\
    h(x, y, z) & := z + 1
    \end{align*}

    \end{itemize}

  So \texttt{add = primrec}(g, h).

  \end{itemize}
IV.2 (c) URM computable functions

Examples for Primitive Recursion

Multiplication can be defined using primitive recursion:
Let \( \text{mult} : \mathbb{N}^2 \to \mathbb{N} \), \( \text{mult}(x, y) := x \cdot y \). We have

\[
\begin{align*}
\text{mult}(x, 0) &= x \cdot 0 = 0 \\
\text{mult}(x, y + 1) &= x \cdot (y + 1) = x \cdot y + x = \text{mult}(x, y) + x
\end{align*}
\]

Therefore

\[
\begin{align*}
\text{mult}(x, 0) &= g(x) \\
\text{mult}(x, y + 1) &= h(x, y, \text{mult}(x, y))
\end{align*}
\]

where

\[
\begin{align*}
g : \mathbb{N} &\to \mathbb{N} \quad g(x) := 0 \\
h : \mathbb{N}^3 &\to \mathbb{N} \\
&h(x, y, z) := z + x
\end{align*}
\]

So \( \text{mult} = \text{primrec}(g, h) \).

Let \( \text{pred} : \mathbb{N} \to \mathbb{N} \), \( \text{pred}(n) := n - 1 = \begin{cases}  n - 1 & \text{if } n > 0, \\  0 & \text{otherwise}. \end{cases} \) 

\( \text{pred} \) can be defined using primitive recursion:

\[
\begin{align*}
\text{pred}(0) &= 0 \\
\text{pred}(x + 1) &= x
\end{align*}
\]

Therefore

\[
\begin{align*}
\text{pred}(0) &= 0 \\
\text{pred}(x + 1) &= h(x, \text{pred}(x))
\end{align*}
\]

where

\[
\begin{align*}
h : \mathbb{N}^2 &\to \mathbb{N} \\
h(x, y) &= x
\end{align*}
\]

So \( \text{pred} = \text{primrec}(0, h) \).

In Haskell we can define add from \text{primrec} as follows

\[
\text{add} :: \text{Nat} \to \text{Nat} \to \text{Nat} \\
\text{add} = \text{primrec1} (\lambda n \to n) (\lambda n \ m \ k \to \text{S} \ k)
\]
Examples for Primitive Recursion

- $x - y$ can be defined using primitive recursion:
  Let $f(x, y) := x - y$. We have
  
  $f(x, 0) = x - 0 = x$
  $f(x, y + 1) = x - (y + 1) = (x - y) - 1$
  $= \text{pred}(x - y) = \text{pred}(f(x, y))$

  Therefore
  
  $f(x, 0) = g(x)$
  $f(x, y + 1) = h(x, y, f(x, y))$

  where
  
  $g : \mathbb{N} \to \mathbb{N}$, $g(x) := x$, $h : \mathbb{N}^3 \to \mathbb{N}$, $h(x, y, z) := \text{pred}(z)$.

  So $f = \text{primrec}(g, h)$.

Proof of Remark

- Therefore we have
  
  $f(\overline{n}, m) \uparrow \rightarrow f(\overline{n}, m + 1) \uparrow$.

- By induction it follows that $f(\overline{n}, m) \uparrow$ implies
  
  $\forall k \geq m. f(\overline{n}, k) \uparrow$.

Remark

- If $f = \text{primrec}(g, h)$, then
  
  $f(\overline{n}, m) \uparrow \rightarrow \forall k \geq m. f(\overline{n}, k) \uparrow$

Proof:

- We have
  
  $f(\overline{n}, m + 1) \simeq h(\overline{n}, m, f(\overline{n}, m))$

- All functions are strict.
- So if $f(\overline{n}, m) \uparrow$, then
  
  $f(\overline{n}, m + 1) \simeq h(\overline{n}, m, f(\overline{n}, m)) \uparrow$

  therefore
  
  $f(\overline{n}, m + 1) \uparrow$

Example

- Let
  
  $h : \mathbb{N}^2 \sim \mathbb{N}$, $h(n, m) \simeq \begin{cases} m - 1 & \text{if } m > 0, \\ \bot & \text{otherwise.} \end{cases}$

- Let
  
  $f : \mathbb{N} \sim \mathbb{N}$, $f := \text{primrec}(1, h)$, i.e. $f(0) \simeq 1$, $f(n + 1) \simeq h(n, f(n))$.

- Then
  
  $f(0) \simeq 1$
  $f(1) \simeq h(0, f(0)) \simeq h(0, 1) \simeq 0$
  $f(2) \simeq h(1, f(1)) \simeq h(1, 0) \uparrow$
  $\forall m \geq 2. f(m) \uparrow$
IV.2 (c) URM computable functions

Primitive-Recursive Functions

- The functions, which can be defined from zero, succ, proj\_k by using composition (\(\circ\)) and primitive recursion (primrec) are called the **primitive recursive functions**.
- The primitive-recursive functions will be studied more in detail in Sect. 5.
  - There we will see that they are powerful, but **not Turing-complete**.

**Notations for Partial Functions**

**Definition (Cont)**

- Let \(g : \mathbb{N}^{n+1} \rightarrow \mathbb{N}\). We define \(\mu y.(g(\vec{x}, y) \simeq 0)\)
  - the least \(y \in \mathbb{N}\) s.t. \(g(\vec{x}, y) \simeq 0\) and for \(0 \leq y' < y\) there exists a \(z' \neq 0\) s.t. \(g(\vec{x}, y') \simeq z'\) if such \(y\) exists,
  - \(\perp\) otherwise

**Examples**

- Assume
  
  \[
  \begin{align*}
  g(\vec{x}, 0) &\simeq 1 \\
  g(\vec{x}, 1) &\uparrow \\
  g(\vec{x}, 2) &\simeq 0
  \end{align*}
  \]
  
  Then
  
  \[\mu y.(g(\vec{x}, y) \simeq 0)\uparrow\]

- Assume instead
  
  \[
  \begin{align*}
  g(\vec{x}, 0) &\simeq 1 \\
  g(\vec{x}, 1) &\simeq 5 \\
  g(\vec{x}, 2) &\simeq 0
  \end{align*}
  \]
  
  Then
  
  \[\mu y.(g(\vec{x}, y) \simeq 0) \simeq 2\]
Computation of \( \mu(g) \)

\[ \mu(g)(\vec{x}) \approx \mu y. (g(\vec{x}, y) \simeq 0). \]

- If \( g \) is intuitively computable, we see that \( h := \mu(g) \) is intuitively computable as follows:
  - In order to compute \( h(\vec{x}) \) we first compute \( g(\vec{x}, 0) \).
    - If this computation never terminates \( g(\vec{x}, 0) \uparrow \) and \( \mu y. (g(\vec{x}, y) \simeq 0) \uparrow \) as well.
    - If it terminates, and we have \( g(\vec{x}, 0) \simeq 0 \), we obtain \( \mu y. (g(\vec{x}, y) \simeq 0) \simeq 0 \).
  - Otherwise, repeat the above with testing of \( g(\vec{x}, 1) \simeq 0 \).
    - If successful repeat it with 2, 3, etc.

- If we defined \( \mu(g)(\vec{x}) \) to be the least \( y \) s.t.
  \[ g(\vec{x}, y) \simeq 0 \]
  independently of whether \( g(\vec{x}, y') \downarrow \) for all \( y' < y \), then we would obtain a non computable function.

Examples for \( \mu \)

- Let \( f : \mathbb{N}^2 \rightarrow \mathbb{N} \), \( f(x, y) := x - y \). Then
  \[ \mu y. (f(x, y) \simeq 0) \simeq x \]
  so \( \mu(f)(x) \simeq x \).

- Let \( f : \mathbb{N} \rightarrow \mathbb{N} \)
  \( f(0) \uparrow \),
  \( f(n) := 0 \) for \( n > 0 \).
  Then
  \[ \mu y. (f(y) \simeq 0) \uparrow \]
Examples for $\mu$

- Let $f : \mathbb{N} \rightarrow \mathbb{N}$,
  \[ f(n) := \begin{cases} 1 & \text{if there exist primes } p, q < 2n + 4, \\ 0 & \text{otherwise} \end{cases} \]
  \[ \mu y.(f(y) \simeq 0) \text{ is the first } n \text{ s.t. there don’t exist primes } p, q \text{ s.t. } 2n + 4 = p + q. \]

Goldbach’s conjecture says that every even number $\geq 4$ is the sum of two primes.

This is equivalent to $\mu y.(\neg \exists p, q \text{ s.t. } 2n + 4 = p + q)$.

It is one of the most important open problems in mathematics to show (or refute) Goldbach’s conjecture.

If we could decide whether a partial computing function is defined (which we can’t), we could decide Goldbach’s conjecture.

Partial Recursive Functions

- The functions, which can define in the same way as the primitive-recursive functions
  - i.e. being defined from zero, succ, proj$^k$ by using composition ($\circ$) and primitive recursion (primrec)
  - but by additionally closing them under $\mu$, are called the partial recursive functions.

- The partial recursive functions will be studied more in detail in Sect. 6.
  - There we will see that the partial recursive functions form a Turing complete model of computation.

Lemma and Definition 2.2

Assume $f : \mathbb{N}^k \rightarrow \mathbb{N}$ is URM-computable.
Assume $x_0, \ldots, x_{k-1}, y, z_0, \ldots, z_l$ are different variables.
Then one can define a URM program, which computes $f(x_0, \ldots, x_{k-1})$ and stores the result in $y$ in the following sense:
- If $f(x_0, \ldots, x_{k-1}) \downarrow$, the program terminates at the first instruction following this program, and stores the result in $y$.
- If $f(x_0, \ldots, x_{k-1}) \uparrow$, the program never terminates.

The program can be defined so that it doesn’t change $x_0, \ldots, x_{k-1}, z_0, \ldots, z_l$.
For $U$ we say it is a URM program which computes $y \simeq f(x_0, \ldots, x_{k-1})$ and preserves $z_0, \ldots, z_l$. 

IV.2 (c) URM computable functions

Intuition behind Lem. 2.2

Lemma 2.2 means that if \( f \) is URM-computable then we can define a URM-program in such a way that

- it takes the arguments from registers we have chosen,
- and stores the result in a register we have chosen,
- and does this in such a way that the content of the input registers and of some other registers we have chosen are not modified.
- This is possible as long as the input registers and the output register are all different.

Idea of the proof

First copy the arguments in some other registers, so that the arguments are preserved.

Then compute the function on those auxiliary registers and make sure that the computation doesn’t affect the registers to be preserved.

Then move the result into the register chosen as output register, and set variables \( x_0, \ldots, x_{k-1}, z_0, \ldots, z_l \) back to their original (stored) values.

Omit Proof.

Proof

Let \( U \) be a URM program s.t. \( U^{(k)} = f \).
Let \( u_0, \ldots, u_{k-1} \) be registers different from the above.
By renumbering of registers and of jump addresses, we obtain a program \( U' \), which computes the result of \( f(u_0, \ldots, u_{k-1}) \) in \( u_0 \)
leaves the registers mentioned in the lemma unchanged, and which, if it terminates, terminates in the first instruction following \( U' \).
The following is a program as intended:

\[
\begin{align*}
  u_0 & := x_0; \\
  \vdots \\
  u_{k-1} & := x_{k-1}; \\
  U' & \\
  y & := u_0;
\end{align*}
\]

Lemma 2.3

1. \( \text{zero}, \text{succ} \) and \( \text{proj}_i^n \) are URM-computable.
2. If \( f : \mathbb{N}^n \rightarrow \mathbb{N}, g_i : \mathbb{N}^k \rightarrow \mathbb{N} \) are URM-computable, so is \( f \circ (g_0, \ldots, g_{n-1}) \).
3. If \( g : \mathbb{N}^n \rightarrow \mathbb{N}, \) and \( h : \mathbb{N}^{n+2} \rightarrow \mathbb{N} \) are URM-computable, so is the function \( f := \text{primrec}(g, h) \) defined by primitive recursion from \( g \) and \( h \).
4. If \( g : \mathbb{N}^{n+1} \rightarrow \mathbb{N} \) is URM-computable, so is \( \mu(g) \).
Remark

- The Lemma is very powerful:
  - It shows that many functions are URM-computable.
  - This shows that for instance the exponential function is URM computable.
    - This follows since addition, multiplication and exponentiation can be defined by primitive recursion from the basic functions.
  - Writing a URM program directly which computes the exponential function would be very difficult.

Omit Proof.

Proof of Lemma 2.3 (a)

Let $x_i$ denote register $R_i$.

Proof of (a)

- $\text{zero}$ is computed by the following program:
  $$x_0 := 0.$$
- $\text{succ}$ is computed by the following program:
  $$x_0 := x_0 + 1.$$
- $\text{proj}^n_k$ is computed by the following program:
  $$x_0 := x_k.$$
  - Especially, if $k = 0$ then $\text{proj}^n_0$ is the empty program (i.e. the program with no instructions this is since we defined $x_0 := x_0$ to be the empty program.)

Proof of Lemma 2.3 (b)

Assume $f : \mathbb{N}^n \simeq \mathbb{N}$, $g_i : \mathbb{N}^k \simeq \mathbb{N}$ are URM-computable.
Show $f \circ (g_0, \ldots, g_{n-1})$ is computable.

A plan for the program is as follows:

- Input is stored in registers $x_0, \ldots, x_{k-1}$.
  - Let $\bar{x} := x_0, \ldots, x_{k-1}$.
- First we compute $g_i(\bar{x})$ for $i = 0, \ldots, n-1$, store result in registers $y_i$.
  - By Lemma 2.2 we can do this in such a way that $x_0, \ldots, x_{k-1}$ and the previously computed values $g_i(\bar{x})$, which are stored in $y_j$ for $j < i$ are not destroyed.
- Then compute $f(y_0, \ldots, y_{n-1})$, and store result in $x_0$.
- Then $x_0$ contains $f(g_0(\bar{x}), \ldots, g_{n-1}(\bar{x})))$.

Proof of Lemma 2.3 (b)

- Let therefore $U_i$ be a URM program $(i = 0, \ldots, n - 1)$, which computes $y_i \simeq g_i(\bar{x})$ and preserves $y_j$ for $j \neq i$.
- Let $V$ be a URM program, which computes $x_0 \simeq f(y_0, \ldots, y_{n-1})$. 
Let $U'$ be defined as follows:

$U_0$

... 

$U_{n-1}$

$V$

We show $U'^{(k)}(\overline{x}) \simeq (f \circ (g_0(\overline{x}), \ldots, g_{n-1}(\overline{x})))$. 

Omit rest of proof.

### Proof of Lemma 2.3 (b)

$U'$ is the program

$U_0$

... 

$U_{n-1}$

$V$

- **Case 1:** For one $i$ $g_i(\overline{x})$↑.
  
  The program will loop in program $U_i$ for the first such $i$.

  $U'^{(k)}(\overline{x}) \uparrow, f \circ (g_0, \ldots, g_{n-1})(\overline{x}) \uparrow$.

- **Case 2:** For all $i$ $g_i(\overline{x})$ ↓.
  
  The program executes $U_i$, sets $y_i \simeq g_i(x_0, \ldots, x_{k-1})$ and reaches beginning of $V$.

In all cases

$U'^{(k)}(\overline{x}) \simeq (f \circ (g_0, \ldots, g_{n-1}))(\overline{x})$. 

Assume
\[ g : \mathbb{N}^n \rightarrow \mathbb{N}, \quad h : \mathbb{N}^{n+2} \rightarrow \mathbb{N} \]
are URM-computable.

Let
\[ f := \text{primrec}(g, h). \]

Show \( f \) is URM-computable.

Defining equations for \( f \) are as follows
(let \( \vec{n} := n_0, \ldots, n_{n-1} \)):

\[
\begin{align*}
  f(\vec{n}, 0) &\simeq g(\vec{n}), \\
  f(\vec{n}, k+1) &\simeq h(\vec{n}, k, f(\vec{n}, k)).
\end{align*}
\]

Plan for the program:

\begin{itemize}
  \item Let \( \vec{x} := x_0, \ldots, x_{n-1} \).
  \item Let \( y, z, u \) be new registers.
  \item Compute \( f(\vec{x}, y) \) for \( y = 0, 1, 2, \ldots, x_n \), and store result in \( z \).
    \begin{itemize}
      \item Initially we have \( y = 0 \) (holds for all registers except of \( x_0, \ldots, x_n \) initially).
      \item We compute \( z \simeq g(\vec{x}) \) (\( \simeq f(\vec{x}, 0) \)).
      \item Then \( y = 0, z \simeq f(\vec{x}, 0) \).
    \end{itemize}
\end{itemize}

Computation of \( f(\vec{n}, l) \) for \( l > 0 \) is as follows:

\begin{itemize}
  \item Compute \( f(\vec{n}, 0) \) as \( g(\vec{n}) \).
  \item Compute \( f(\vec{n}, 1) \) as \( h(\vec{n}, 0, f(\vec{n}, 0)) \), using the previous result.
  \item Compute \( f(\vec{n}, 2) \) as \( h(\vec{n}, 1, f(\vec{n}, 1)) \), using the previous result.
  \item \ldots
  \item Compute \( f(\vec{n}, l) \) as \( h(\vec{n}, l-1, f(\vec{n}, l-1)) \), using the previous result.
\end{itemize}

\begin{itemize}
  \item In step from \( y \) to \( y+1 \):
    \begin{itemize}
      \item Assume that we have \( z \simeq f(\vec{x}, y) \).
      \item We want that after increasing \( y \) by 1 the \textbf{loop invariant} \( z \simeq f(\vec{x}, y) \) still holds.
      \item Obtained as follows
        \begin{itemize}
          \item Compute \( u \simeq h(\vec{x}, y, z) \) (\( \simeq h(\vec{x}, y, f(\vec{x}, y)) \simeq f(\vec{x}, y + 1) \)).
          \item Execute \( z := u \) (\( \simeq f(\vec{x}, y + 1) \)).
          \item Execute \( y := y + 1 \).
          \item At the end, \( z \simeq f(\vec{x}, y) \) for the new value of \( y \).
        \end{itemize}
    \end{itemize}
  \item Repeat this until \( y = x_n \).
  \item Once \( y \) has reached \( x_n \), \( z \) contains \( f(\vec{x}, y) \simeq f(\vec{x}, x_n) \).
  \item Execute \( x_0 := z \).
\end{itemize}
Proof of Lemma 2.3 (c)

Let
- U be a URM program, which computes \( z \simeq g(\vec{x}) \) and preserves \( y \) (by definition 2.2, it doesn’t modify the arguments \( \vec{x} \) of \( g \));
- V be a program, which computes \( u \simeq h(\vec{x}, y, z) \). (by definition 2.2, it doesn’t change \( \vec{x}, y, z \).)

Let \( U' \) be as follows:

\[
U \quad \text{--- Compute } z \simeq g(\vec{x})(\simeq f(\vec{x}, 0))
\]

\[
\text{while } (x_n \neq y) \text{ do }
V \quad \text{--- Compute } u \simeq h(\vec{x}, y, z)
\]

\[
z := u;
y := y + 1;
\]

\[
x_0 := z;
\]

Correctness of this program:
- When \( U \) has terminated, we have \( y = 0 \) and \( z \simeq g(\vec{x}) \simeq f(\vec{x}, y) \).
- After each iteration of the while loop, we have \( y := y' + 1 \) and \( z \simeq h(\vec{x}, y', z') \).
  \((y', z') \) are the previous values of \( y, z \), respectively.\)
- Therefore we have \( z \simeq f(\vec{x}, y) \).
- The loop terminates, when \( y \) has reached \( x_n \).
  Then \( z \) contains \( f(\vec{x}, y) \).
  This is stored in \( x_0 \).

- If \( U \) loops for ever, or in one of the iterations \( V \) loops for ever, then:
  - \( U' \) loops, \( U'^{(n+1)}(\vec{x}, x_n) \uparrow \).
  - \( f(\vec{x}, k) \uparrow \) for some \( k < x_n \).
  - subsequently \( f(\vec{x}, l) \uparrow \) for all \( l > k \).
  - Especially, \( f(\vec{x}, x_n) \uparrow \).
  - Therefore \( f(\vec{x}, x_n) \simeq U'^{(n+1)}(\vec{x}, x_n) \).
Proof of Lemma 2.3 (d)

Assume 
\[ g : \mathbb{N}^{n+1} \rightarrow \mathbb{N} \]

is URM-computable.
Show 
\[ \mu(g) \]
is URM-computable as well.
Note \( \mu(g)(x_0, \ldots, x_{k-1}) \) is the minimal \( z \) s.t. 
\[ g(x_0, \ldots, x_{k-1}, z) \approx 0 \]

Let \( \vec{x} := x_0, \ldots, x_{k-1} \) and let \( y, z \) be registers different from \( \vec{x} \).

Let \( U \) compute 
\[ z \approx g(x_0, \ldots, x_{k-1}, y) \]
(and preserve the arguments \( x_0, \ldots, x_{k-1}, y \))
Let \( V \) be as follows:

\[
\text{repeat}\{ \\
\quad U \\
\quad y := y + 1; \\
\text{until } (z = 0); \\
\quad y := y - 1; \\
\quad x_0 := y;
\}
\]

Omit rest of proof.
Finally $y$ is decreased by one.

Then $y$ is the least $y$ s.t.

$$g(x_0, \ldots, x_{k-1}, y) \simeq 0.$$ 

$x_0$ is then set to that value.