A Formalization of Multi-tape Turing Machines

Andrea Asperti\textsuperscript{a}, Wilmer Ricciotti\textsuperscript{b,1}

\textsuperscript{a}Department of Computer Science and Engineering, University of Bologna, Mura Anteo Zamboni 7, 40127 Bologna, Italy

\textsuperscript{b}IRIT, University of Toulouse, 118 Route de Narbonne, 31062 Toulouse Cedex 9, France

Abstract

We discuss the formalization, in the Matita Theorem Prover, of basic results on multi-tapes Turing machines, up to the existence of a (certified) Universal Machine, and propose it as a natural benchmark for comparing different interactive provers and assessing the state of the art in the mechanization of formal reasoning. The work is meant to be a preliminary step towards the creation of a formal repository in Complexity Theory, and is a small piece in our long-term Reverse Complexity program, aiming to a comfortable, machine independent axiomatization of the field.

1. Introduction

In spite of the remarkable achievements recently obtained in the automatic checking of complex results in many different domains, spanning from pure mathematics \cite{13, 23, 7, 21} to software verification \cite{28, 27, 36, 1}, passing through the metatheory and semantics of programming languages \cite{15, 33}, the learning curve of interactive provers is still extremely steep and the mechanization of formal reasoning remains a very complex task.

Even comparing proof assistants in terms of their concrete usability \cite{34, 6} looks difficult, due to the different domains of applications (for instance, alpha equivalence and binding mechanisms are important issues for the metatheory of functional languages and type systems \cite{33}, but are almost negligible for proving properties on compilers or other software tools \cite{2}) and the different criteria that can be used in the comparison (in \cite{14}, it is particularly stressed the importance of having human readable proofs, while \cite{2} shifts the emphasis on the connection between the proof of a specification and the corresponding implementation, and the possibility of extracting or automatically checking it).

\textsuperscript{1}Wilmer Ricciotti is supported by the project \textsc{Ajitprop} of the Fondation Airbus.
Creating several benchmarks in different domains seems to be the best approach for promoting the actual development of the field and for comparing theorem provers on their ability to express/synthesize proofs and to support the user in the process of formalization.

Somewhat surprisingly, very little work has been done so far in major fields of theoretical computer science, such as computability theory and, especially, complexity theory. Two notable exceptions are the articles by Norrish [29] and, very recently, by Xu, Zhang and Urban [35]. Norrish’s work contains basic results in computability theory relying on $\lambda$-calculus and recursive functions as computational models. A major drawback of this approach is that computational constructs like $\beta$-reduction or recursive function call are not finitistic and hence are not suitable for a foundational investigation of complexity. In spite of the many attempts of providing machines independent characterizations of Complexity Theory, its actual foundation still relies on Turing machines.

Turing machines are the actual focus of Xu, Zhang and Urban’s work [35], that testifies the new, recent interest of the interactive theorem prover community on these topics. Their contribution appeared after the first version of this article was submitted, and our development was completely independent and uninfluenced by their work. We shall postpone the comparison with [35] to the conclusions.

As a matter of fact, the subject of Turing machines provides an excellent test bench for proof assistants, for several reasons

1. it is a well established subject, not deserving auxiliary specifications; even undergraduate students can directly tackle it, possibly as an experimental part of traditional theoretical courses;
2. it does not require sophisticated mathematics; it can be easily formalized in first order logic, but it can also take advantage of more sophisticated logical frameworks, like systems with dependent types (for instance, we found both natural and convenient to use them to formalize multi-tape machine by means of vectors of a specified length);
3. it provides simple but effective examples of executable specifications, allowing to test the computational capabilities of the system and/or its code-extraction facilities;
4. it allows to address interesting termination problems, that is one of the most complex issue in the mechanization of formal reasoning.

In this paper, we present a down-to-earth formalization for the Matita Interactive Theorem Prover [9, 10] of the theory of multi-tape Turing machines, up to the existence of a universal machine and the proof of its correctness. The code is available at http://www.cs.unibo.it/~asperti/turing.tar.

In our development, we have been inspired by several traditional articles and textbooks, comprising e.g. [20, 26, 18, 32, 30]; all of them are excellent works, and provide a rigorous mathematical exposition of the theory of Turing machines, and nevertheless none of them gives a sufficiently accurate description (especially of the universal machine) to be directly translated in formal terms.
Although we do not claim any particular originality in our approach, there are several points in the development where the choice of the data structures used for the formal encoding, or the means used for expressing the semantics of Turing machines have not been entirely straightforward. In particular, for obvious reasons, we tried to be as compositional as possible in the semantic specification, allowing us to discover unexpected compositional properties in a domain that is usually reputed to be (quite) non-compositional.

The current work is a major revisitation of the work presented at WoLLIC [8]; in particular, we switched from mono to multi-tape Machines, forcing us to completely rewrite the universal machine. While [8] was essentially a preliminary report on an ongoing effort, this paper describes a much more mature and stabilized version of the formalization. Relevant differences between the two works are emphasized at suitable places along the paper, and an overall comparison is given in the conclusions.

The structure of the paper is the following: Section 2 contains a short description of the main libraries of Matita used in the development; Section 3 gives the formal definition of multi-tape Turing machines and their semantics; Section 4 provides means for composing machines (sequential composition, conditionals and iteration); Section 5 contains the definition of basic, atomic machines and a few examples of slightly more complex machines derived from them by compositional mechanisms; Section 6 introduces the notion of Normal Turing machine and its standard representation as a list of tuples; Section 7 gives an outline of the universal machine; Sections 8 and 10 are respectively devoted to the three main routines of the universal machine, namely finding the right tuple to apply, and use it to update the state and execute the suitable action on the simulated tape; in Section 11 we summarize the main results which have been proved about the universal machine. In the conclusion we provide overall information about the size of the contribution and the resources required for its development as well as more motivations for pursuing formalization in computability and complexity theory: in particular we shall briefly outline our long term Reverse Complexity program, aiming to a trusted and machine independent axiomatization of the field, suitable for mechanization.

2. Preliminaries

Our formalization of Turing machines relies on two main libraries of Matita, that we shall rapidly discuss in this section: finite sets; and vectors. A theory of finite sets is essential not only to formalize data structures like the tape alphabet or the machine states, but also to transform a (executable!) transition function into a finite graph (that is, up to trivial encodings, the representation exploited by the universal machine). Vectors can be conveniently used to develop the theory of multi-tape machines in a fully parametric way.

2.1. Implicit Parameters

Before addressing Matita code, it is worth to spend a few words about the syntax for implicit parameters. Matita is a type-theory based interactive prover,
and proof checking is reduced to type-checking, via the well known Curry-Howard (Types as Propositions) analogy. Types are often redundant and can be automatically guessed by a suitable type inference algorithm [12]. The user may ask the system to automatically synthesize a given argument by replacing it by a question mark. Each question mark stands for a different parameter; a sequence of \( n \) questions marks stands for \( n \) implicit parameters (question marks do not need to be spaced). Instead of question marks, the user can also use ellipses (\(...)\), standing for an arbitrary number of implicit arguments: in this case we also delegate to the system the charge to figure out the correct number of arguments. Both question marks and ellipses could be made completely transparent by adding suitable notational extensions (a mechanism supported by Matita); however, the fact that a term expecting a given number of arguments is actually receiving in input only a subset of them can be sometimes quite confusing, and we prefer to explicitly leave a bit of notation to recall an omitted, implicit information.

2.2. Finite Sets

As customary in type-theoretic formalizations of abstract algebra, libraries are usually organized into a hierarchy of structures based on nested dependent record types. In Matita, at the bottom of this hierarchy there is the \texttt{DeqSet} structure, that deals with types equipped with a decidable equality (essentially analogous to the \texttt{eqType} in [22]):

```agda
record DeqSet : Type :=
{ carr : Type;
  eqb : carr \rightarrow\rightarrow carr \rightarrow bool;
  eqb_true : \forall x,y. (eqb x y = true) \leftrightarrow (x = y)}. 
```

We recall that, in Matita, each definition of a record \texttt{foo} implicitly defines an associated constructor \texttt{mk_foo} that takes a list of arguments corresponding to the record fields, and returns a new record. The names given by the user to the record fields are associated to projection functions, extracting from the record the corresponding field value.

The \(\rightarrow\rightarrow\) symbol declares \texttt{carr} as a coercion from a \texttt{DeqSet} to its carrier type.

Suppose we build a record \texttt{DeqNat:DeqSet} having the natural numbers \texttt{nat} as carrier. Then, for instance, the expression \(0:\texttt{DeqNat}\) is well typed, and it is understood by the system as \(0:\texttt{carr DeqNat}\). We use the infix notation \(\texttt{==}\) for the decidable equality \texttt{eqb} of the set (different from the primitive logical equality of the system, denoted with \(\texttt{==}\)).

Inductive data structures can usually be turned into a \texttt{DeqSet} by defining \(\texttt{==}\) as a structural equality test. This is for instance the case for booleans and natural numbers (and many others), for which we have two corresponding \texttt{DeqSets} named \texttt{DeqBool} and \texttt{DeqNat}. We use the mechanism of unification hints [11] to suggest to Matita that, for example, if it meets a natural number, and if required by unification, it may lift it up to an element of a \texttt{DeqSet} using a suitable decidable equality hinted to by the user. For instance, the expression \(0 \texttt{== 1}\) is well typed: the comparison would require two elements of type \texttt{carr ?X} for some
unknown DeqSet ?X, while it receives two elements of type nat. The purpose of the hint is to suggest a possible solution for the equation carr ?X = Nat\(^2\), namely, in this case, ?X = DeqNat.

A finite set is a record consisting of a DeqSet A, a list of elements of type A enumerating all the elements of the set, and the proofs that the enumeration does not contain repetitions and is complete (**memb** is the membership operation on lists, defined in the obvious way; the question mark is an example of an implicit parameter automatically filled in by the system).

```plaintext
record FinSet :=
{ FinSetcarr:> DeqSet;
  enum: list FinSetcarr;
  enum_unique: uniqueb FinSetcarr enum = true;
  enum_complete : @x:FinSetcarr. memb ? x enum = true}.
```

The library provides many operations for building new FinSets by composing existing ones: for example, if A and B have type FinSet, then option A, A \(\otimes\) B, A \(\otimes\) B are finite sets too. In all these cases, unification hints are used to suggest the intended finite set structure associated with them, that makes their use quite transparent to the user.

Among all constructions, the most interesting one for the purpose of this paper is the arrow type A \(\rightarrow\) B. We may define the graph of \(f:A \rightarrow B\), as the set (sigma type) of all pairs \(a, b\) such that \(f(a) = b\).

```plaintext
definition graph_of :=\(\lambda\)A,B.\(\lambda\)f:A \(\rightarrow\) B. \(\sum\)p:A \(\times\) B. f (\fst p) = \snd p.
```

In case the equality is decidable, we may effectively enumerate all elements of the graph by simply filtering from pairs in A \(\times\) B those satisfying the test \(\lambda\)p.f (\fst p) == \snd p):

```plaintext
definition graph_enum :=\(\lambda\)A,B:FinSet.\(\lambda\)f:A \(\rightarrow\) B. filter ? (\(\lambda\)p.f (\fst p) == \snd p) (enum (FinProd A B)).
```

The proofs that this enumeration does not contain repetitions and is complete are straightforward.

2.3. Vectors

A vector of length n of elements of type A is simply defined in Matita as a record composed by a list of elements of type A, plus a proof that the list has the expected length. Vectors are a paradigmatic example of dependent type, that is of a type whose definition depends on a term.

```plaintext
record Vector (A:Type) (n:nat): Type :=
{ vec:>list A;
  len: length ? vec = n }.  
```

\(^2\)The solution to this type of unification problems would require narrowing, that is a complex and expensive operation transcending the (pseudo)-first order capabilities of the unification algorithms typically (and wittingly) implemented in proof assistants.
Given a list \( l \) we may trivially turn it into a vector of length \(|l|\); we just need to prove that \(|l| = |l|\) that follows from the reflexivity of equality.

**definition** Vector_of_list := \( \lambda A, l.\text{mk\_Vector } A (|l|) l \text{ (refl ??)} \).

Most functions operating on lists can be naturally extended to vectors; interesting cases are \text{vec\_append}, concatenating vectors, and \text{vec\_map}, mapping a function \( f \) on all elements of the input vector and returning a vector of the same dimension of the input one.

Since a vector is automatically coerced, if needed, to the list of its elements, we may simply use typical functions over lists (such as \text{nth}) to extract/filter specific components.

The function \( \text{change\_vec } A n v a i \) replaces the content of the vector \( v \) at position \( i \) with the value \( a \).

The most frequent operation on vectors for the purposes of our work is their comparison. In this case, we have essentially two possible approaches: we may proceed component-wise, using the following lemma

**lemma** eq_vec: \( \forall A,n. \forall v1,v2: \text{Vector } A n. \forall d.
(\forall i. i < n \rightarrow \text{nth } i A v1 d = \text{nth } i A v2 d) \rightarrow v1 = v2. \)

or alternatively we may manipulate vectors exploiting the commutation or idempotence of \( \text{change\_vec} \) and its interplay with other operations.

3. The notion of Turing machine

Turing machines were defined by Alan M. Turing in [31]. To computer scientists, they are a very familiar notion, so we shall address straight away their formal definition. We formalized both mono and multi-tape machines; in many cases, simple multi tape (sub-)machines work on a single tape at a time, and it is convenient to define them as “injections” of mono tapes machines.

3.1. The tape

A first interesting issue is the definition of the tape. The natural idea is to formalize it as a zipper, that is a pair of lists \( l \) and \( r \), respectively representing the portions of the tape at the left and the right of the tape head; by convention, we may assume the head is reading the first symbol on the right. Of course, the machine must be aware this list can be empty, that means that the transition function should accept an \text{optional} tape symbol as input. Unfortunately, in this way, the machine is only able to properly react to a right overflow; the

---

3It is worth to recall that the choice about the number of tapes, while irrelevant for computability issues, it is not from the point of view of complexity. Hartmanis and Stearns [24] have shown that any k-tape machine can be simulated by a one-tape machine with at most a quadratic slow-down, and Hennie [25] proved that in some cases this is the best we can expect; Hennie and Stearns provided an efficient simulation of multi-tape machines on a two-tape machine with just a logarithmic slow-down [19].
problem arises when the left tape is empty and the head is moved to the left: a new "blank" symbol should be added to the right tape. A common solution in textbooks is to reserve a special blank character \( \square \) of the tape alphabet for this purpose: the annoying consequence is that tape equality should be defined only up to a suitable equivalence relation ignoring blanks. To make an example, suppose we move the head to the left and then back to the right: we expect the tape to end up in the same situation we started with. However, if the tape was in the configuration \([\square],r\) we would end up in \([\square],r\). As anybody with some experience in interactive proving knows very well, reasoning up to equivalence relations is \textit{extremely} annoying, that prompts us to look for a different representation of the tape.

The main source of our problem was the asymmetric management of the left and right tape, with the arbitrary assumption that the head symbol was part of the right tape. If we try to have a more symmetric representation we must clearly separate the head symbol from the left and right tape, leading to a configuration of the kind \((l,c,r)\) (mid-tape); if we have no \(c\), this may happen for three different reasons: we are on the left end of a non-empty tape (left overflow), we are on the right end of a non-empty tape (right overflow), or the tape is completely empty. This definition of the tape may seem conspicuous at first glance, but it resulted to be quite convenient in practice.

\begin{verbatim}
inductive tape (sig:FinSet) : Type :=
| niltape : tape sig
| leftof : sig -> list sig -> tape sig
| rightof : sig -> list sig -> tape sig
| midtape : list sig -> sig -> list sig -> tape sig.
\end{verbatim}

For instance, suppose to be in a configuration with an empty left tape, that is \((\text{midtape} \[] a \) \): moving to the left will result in \((\text{leftof} a \) \); further moves to the left are forbidden, and moving back to the right restores the original situation.

Given a tape, we may easily define the optional current symbol

\begin{verbatim}
definition current :=\(\lambda \text{sig.} \lambda \text{t:tape sig.match t with}
[ \text{midtape } _ c _ \Rightarrow \text{Some ? c | _ } \Rightarrow \text{None ? } ].\)
\end{verbatim}

as well as the left and right portions of the tape:

\begin{verbatim}
definition left :=\(\lambda \text{sig.} \lambda \text{t:tape sig.match t with}
[ \text{niltape } \Rightarrow [] | \text{leftof } _ _ \Rightarrow [] | \text{rightof } s l \Rightarrow s::l | \text{midtape } _ _ _ \Rightarrow l ].\)
definition right :=\(\lambda \text{sig.} \lambda \text{t:tape sig.match t with}
[ \text{niltape } \Rightarrow [] | \text{leftof } s r \Rightarrow s::r | \text{rightof } _ _ \Rightarrow [] | \text{midtape } _ _ r \Rightarrow r ].\)
\end{verbatim}

Note that if \((current \ t) = \text{None}\) then either \((left \ t)\) or \((right \ t)\) is empty.

### 3.2. Multi-tape Machines

We shall consider machines with three possible moves for the head: \(L\) (left) \(R\) (right) and \(N\) (None).
The notion of Turing machine is parametric over a tape alphabet $\text{sig}$ and the number $\text{tapes\_no}$ of additional working tapes (i.e. we assume the machine always has at least one tape). Formally, it is a record composed of a finite set of $\text{states}$, a transition function $\text{trans}$, a $\text{start}$ state, and a set of halting states identified by a boolean function. To encode the alphabet and the states, we exploit the $\text{FinSet}$ library of Matita, described in Section 2.

$$
\text{record mTM (sig:FinSet) (tapes\_no:nat) : Type :=}
\{
\; \text{states} : \text{FinSet};
\; \text{trans} : \text{states} \times (\text{Vector (option sig) (S tapes\_no)}) \to 
\; \text{states} \times (\text{Vector ((option sig) \times move) (S tapes\_no)});
\; \text{start} : \text{states};
\; \text{halt} : \text{states} \to \text{bool} \}.
$$

The transition function takes in input a pair $\langle q, \vec{a} \rangle$ where $q$ is the current internal state and $\vec{a}$ is a vector of optional symbols under the tape heads; it returns a pair $\langle q', \vec{p} \rangle$ where $q'$ is a new internal state and $\vec{p}$ is a vector of actions. Each action is a pair $\langle b, m \rangle$ composed of a new optional character $b$ and a move $m$. The new character is optional since we want to give the possibility to leave the tape untouched, that is particularly convenient when we are in an overflow position on some tape.4

Executing an action $p = \langle b, m \rangle$ on a tape simply consists in writing $b$ and moving the tape according to $m$:

$$
\text{definition tape\_move\_mono :=}\lambda \text{sig}, \text{t}, \text{mv}.
\; \text{tape\_move\_mono sig (tape\_write sig t (f\text{\_st} mv)) (f\text{\_snd} mv)}.
$$

Writing a symbol is straightforward:

$$
\text{definition tape\_write :=}\lambda \text{sig}. \lambda \text{t}: \text{tape sig}. \lambda \text{s:option sig}. 
\; \text{match s with [ None \Rightarrow t \mid \text{Some} \; s0 \Rightarrow \text{midtape ? (left ? t) s0 (right ? t)\]}}.
$$

The move operation is slightly more complex; we start by splitting it in simpler operations, according to the move

$$
\text{definition tape\_move :=}\lambda \text{sig}. \lambda \text{t: tape sig}. \lambda \text{m:move}.
\; \text{match m with [ R \Rightarrow \text{tape\_move\_right \? t \mid L \Rightarrow \text{tape\_move\_left \? t \mid N \Rightarrow t} \]}}.
$$

Then, $\text{tape\_move\_right}$ is defined in the following way ($\text{tape\_move\_left}$ is analogous); note in particular that trying to move right when we are in an empty tape or in a right overflow situation has no effect.

4The type of actions has changed w.r.t.8; the point is that in mono-tape machines overflow situations are essentially pathological, while in multi-tape machines it is extremely convenient to exploit the border of the tapes as natural delimiters of data types stored on dedicated working tapes.
Finally, moving a vector of tapes w.r.t. a vector of actions simply consists in mapping the corresponding mono-tape operation:

```
definition tape_move_multi := λsig,n,ts,actions.  
pmap_vec ...(tape_move_mono sig) n ts actions.
```

3.3. Configurations and computations

A configuration relative to a given set of states and an alphabet \( \text{sig} \) is a record composed of a current internal state \( \text{cstate} \) and a vector \( \text{ctapes} \) of tapes.

```
record mconfig (sig,states:FinSet) (n:nat): Type :=  
{ cstate : states;  
ctapes : Vector (tape sig) (S n) }.
```

To perform a transition step between two configurations we must first of all extract from the input configuration \( c \) the current state and the vector of characters under the tape heads; then, we apply the transition function to get a new state \( \text{news} \) and an action, and finally build a new configuration composed by \( \text{news} \) and the tapes resulting by executing the given action. This is summarized by the following code:

```
definition step := λsig,λn:ℕ,mM sig n.λc:mconfig sig (states ?? M) n.  
let (news,actions) := trans sig n M (cstate ... c,current_chars ... (ctapes ... c)) in  
mk_mconfig ... news (tape_move_multi sig ? (ctapes ... c) actions).
```

where \( \text{current_chars} \) returns the symbols currently under the tape heads:

```
definition current_chars := λsig,λn,Atapes. vec_map ?? (current sig) (S n) tapes.
```

A computation is an iteration of the step function until a final internal state is met. In Matita, we may only define total functions, hence we provide an upper bound to the number of iterations, and return an optional configuration
depending on the fact that the halting condition has been reached or not. To this purpose, we use the following generic iterator \( \text{loop} \) (inspired by [17]):

\[
\text{let rec loop (A:Type) n (f:A \rightarrow A) p a on n :=}
\]

\[
\begin{cases}
\quad \text{if } p a \text{ then } \text{Some } a \text{ else loop } A \text{ n } f \text{ p } (f a) .
\end{cases}
\]

The transformation between configurations relative to Turing machine \( M \) is:

\[
\text{definition loopM := } \lambda \text{sig,n.}\text{\lambda}M:\text{mTM sig n.}\lambda i,cin.\text{loop } i (\text{step sig n M}) (\lambda c.\text{halt sig n M (cstate ... c)}) cin.
\]

### 3.4. Semantics

The usual notion of computation for Turing machines is defined in relation with given input and output functions, providing the initial tape encoding and the final read-back function. As we know from Kleene’s normal form, the output function is particularly important: the point is that our notion of Turing machine is monotonically increasing w.r.t. tape consumption, with the consequence that the transformation relation between configurations is decidable. However, input and output functions are extremely annoying when composing machines and we would like to get rid of them as far as possible.

Our solution is to define the semantics of a Turing machine by means of a relation between the input tape and the final tape (possibly embedding the input and output functions): in particular, we say that a machine \( M \) realizes a relation \( R \) between tapes (\( M \models R \)), if for all \( t_1 \) there exists a computation leading from \( \langle q_0, t_1 \rangle \), to \( \langle q_f, t_2 \rangle \) and \( t_1 \models t_2 \), where \( q_0 \) is the initial state, \( q_f \) is some halting state of \( M \), and \( t_2 \) is the tape resulting from the computation.

It is natural to wonder why we use relations on tapes, and not on configurations. The point is that different machines may easily share tapes, but they can hardly share their internal states. Working with configurations would force us to an input/output recoding between different machines that is precisely what we meant to avoid.

The previous notion of realizability implies termination. It is useful to define a weaker notion (weak realizability, denoted \( M \models R \)), asking that \( t_1 \models t_2 \) provided there is a computation between \( t_1 \) and \( t_2 \). It is easy to prove that

\footnote{For us, it was gratifying to discover that the small library of lemmas relative to the loop iterator that we develop for the mono-tape case, did not require any extension or modification after switching to the multi-tape case.}
termination together with weak realizability imply realizability (we shall use the notation $M \downarrow t$ to express the fact that $M$ terminates on input tapes $t$).

```
definition WRealize := \lambda sig,n.\lambda M:mTM sig n.\lambda R:relation (Vector (tape sig) ?). D@. D@. D@. D@. D@. sig n M i (initc sig n M t) = Some ? outc Ñ R t (ctapes ??? outc).
definition Terminate := \lambda sig,n.\lambda M:mTM sig n.\lambda t. D@. D@. D@. D@. D@. sig n M i (initc sig n M t) = Some ? outc.

lemma WRealize_to Realize : \forall sig,n.\forall M:mTM sig n.\forall R. (\forall t.M \downarrow t) Æ M \models \lambda t. R Æ M \models \lambda t. R.
```

### 3.5. A canonical relation

For every machine $M$ we may define a canonical relation, that is the smallest relation weakly realized by $M$.

```
definition R_mTM := \lambda sig,n.\lambda M:mTM sig n.\lambda q.\lambda t1,t2. D@. D@. D@. D@. D@. sig n M i (mk_mconfig ... q t1) = Some ? outc Æ t2 = (ctapes ... outc).

lemma Wrealize_R_mTM : \forall sig,n.\forall M:mTM sig n. M \models \lambda t. R_mTM sig n M (start sig n M).

lemma R_mTM_to_R: \forall sig,n.\forall M:mTM sig n.\forall R. \forall t1,t2. M \models \lambda t. R Æ M \models \lambda t. R_mTM ?? M (start sig n M) t1 t2 Æ R t1 t2.
```

### 3.6. The Nop Machine

As a first, simple example, we define a Turing machine performing no operation (we shall also use it in the sequel to force, by sequential composition, the existence of a unique final state).

The machine has a single state that is both initial and final: we define the states as $\text{initN} 1$, that is the interval of natural numbers less than 1. This is actually a sigma type containing a natural number $m$ and an (irrelevant) proof that $m$ is smaller than $n$.

```
definition nop_states := initN 1.
definition start_nop : initN 1 := mk_Sig ?? 0 (le_n ... 1).
```

The transition function is irrelevant, since it will never be executed: we define it as a map returning a vector of dummy actions.

```
definition null_action := \lambda sig.An. Vector_of_list (make_list (option sig \times move) ((None ?,N)) (S n)).
definition nop := Aalpha:FinSet.\lambda n.mk_mTM alpha n nop_states (\lambda p. let \langle q,a \rangle := p in \langle q,\text{null_action} sig n \rangle) start_nop (\lambda _.true).
```
The semantic relation \( R_{\text{nop}} \) characterizing the machine is just the identity; the proof that the machine realizes \( R_{\text{nop}} \) is entirely straightforward.

\[
\text{definition } R_{\text{nop}} := \lambda \alpha, n. \lambda t_1, t_2: \text{Vector} (\text{tape} \alpha) (S \ n). t_2 = t_1.
\]

\[
\text{lemma } \text{sem}_{\text{nop}}: \forall \alpha, n. \text{nop} \alpha n \models R_{\text{nop}} \alpha n.
\]

4. Composing Machines

Turing machines are usually reputed to suffer for a lack of compositionality. Our semantic approach, however, allows us to compose them in relatively easy ways. This will give us the opportunity to reason at a higher level of abstraction, rapidly forgetting their low level architecture.

4.1. Sequential composition

The sequential composition \( M_1 \cdot M_2 \) of two Turing machines \( M_1 \) and \( M_2 \) is a new machine having as states the disjoint union of the states of \( M_1 \) and \( M_2 \). The initial state is the (injection of the) initial state of \( M_1 \), and similarly the halting condition is inherited from \( M_2 \); the transition function is essentially the disjoint sum of the transition functions of \( M_1 \) and \( M_2 \), plus a transition leading from the final states of \( M_1 \) to the (old) initial state of \( M_2 \) (here it is useful to have the possibility of not moving the tape).

\[
\text{definition } \text{seq}_{\text{trans}} := \lambda \text{sig, n. } \lambda M_1, M_2 : \text{mTM sig n.}
\]

\[\lambda \text{p. let } (s, a) := \text{p in}
\]

\[
\text{match } s \text{ with } \begin{cases} \text{inl s1} \Rightarrow & \text{if halt sig n M1 s1 then } \text{inr ... (start sig n M2), null_action sig n} \\ \text{else let } (\text{news1, m}) := \text{trans sig n M1 s1, a} \text{ in } \text{inl ... news1, m} \\ \text{inr s2} \Rightarrow & \text{let } (\text{news2, m}) := \text{trans sig n M2 s2, a} \text{ in } \text{inr ... news2, m} \end{cases} \]

\[
\text{definition } \text{seq} := \lambda \text{sig, n. } \lambda M_1, M_2 : \text{mTM sig n.}
\]

\[
\text{mk_mTM sig n} \left( (\text{states sig n M1}) \oplus (\text{states sig n M2}) \right) \left( \text{seq}_{\text{trans} \text{ sig n M1 M2}} \right) \left( \text{inl ... (start sig n M1)} \right) \left( \text{As.match s with } \begin{cases} \text{inl _ } \Rightarrow \text{false} & | \text{inr s2 } \Rightarrow \text{halt sig n M2 s2} \end{cases} \right).
\]

If \( M_1 \models R_1 \) and \( M_2 \models R_2 \) then

\[
M_1 \cdot M_2 \models R_1 \circ R_2
\]

that is a very elegant way to express the semantics of sequential composition. The proof of this fact, however, is not as straightforward as one could expect. The point is that \( M_1 \) works with its own internal states, and we should “lift” its computation to the states of the sequential machine. To have an idea of the kind of results we need, here is one of the key lemmas:
lemma loop_lift : ∀A,B,k,lift,f,g,h,hlift,c,c1.
   (∀x.hlift (lift x) = h x) →
   (∀x.h x = false → lift (f x) = g (lift x)) →
   loop A k f h c = Some ? c1 →
   loop B k g hlift (lift c) = Some ? (lift ...c1).

It says that the result of iterating a function $g$ starting from a lifted configuration $lift c$ is the same (up to lifting) as iterating a function $f$ from $c$ provided that

1. a base configuration is halting if and only if its lifted counterpart is halting;
2. $f$ and $g$ commute w.r.t. lifting on every non-halting configuration.

4.2. If then else

The next machine we define is an if-then-else composition of three machines $M_1, M_2$ and $M_3$ respectively implementing a boolean test, and the two conditional branches. We found convenient to store the result of the boolean test in an internal state of the first machine instead than on a tape: in particular we expect to end up in a distinguished final state $q_{acc}$ if the test is successful, and in a different state otherwise. This special state $q_{acc}$ must be explicitly mentioned when composing the machines. The definition of the if-then-else machine is then straightforward: the states of the new machine are the disjoint union of the states of the three composing machines; the initial state is the initial state of $M_1$; the final states are the final states of $M_2$ and $M_3$; the transition function is the union of the transition functions of the composing machines, where we add new transitions leading from $q_{acc}$ to the initial state of $M_2$ and from all other final states of $M_1$ to the initial state of $M_2$.

definition if_trans :=
   λsig,n. λM1,M2,M3 : mTM sig n.
   λq:states sig n M1.
   λp.
   let x s,a y :=p
   in
   match s
   with
   [ inl s1
     ⇒
     if halt sig n M1 s1 then
     if s1=⇒q then
       (inr ... (inl ... (start sig n M2)), null_action ??)
     else (inr ... (inr ... (start sig n M3)), null_action ??)
     else let x news1,m y :=trans sig n M1 x s1,a y
       in
       x inl ...
       news1,m y
     | inr s'
     ⇒
     match s' with
     [ inl s2 ⇒
       let ⟨news2,m⟩ :=trans sig n M2 ⟨s2,a⟩ in ⟨inr ... (inl ... news2),m⟩
     | inr s3 ⇒
       let ⟨news3,m⟩ :=trans sig n M3 ⟨s3,a⟩ in ⟨inr ... (inr ... news3),m⟩
     ]].

definition ifTM :=
   λsig,n. λcondM,thenM,elseM : mTM sig n.
   λqacc: states sig n condM.
   mk_mTM sig n
   ((states sig n condM) ⊔ (states sig n thenM) ⊔ (states sig n elseM))
   (if_trans sig n condM thenM elseM qacc)
   (inl ... (start sig n condM))
   (As.match s with
       [ inl _ ⇒ false
       | inr s' ⇒ match s' with
         [ inl s2 ⇒ halt sig n thenM s2
         | inr s3 ⇒ halt sig n elseM s3 ]]).
Our realizability semantics is defined on tapes, and not configurations. In order to observe the accepting state we need to define a suitable variant that we call conditional realizability, denoted by $M \models [q : R_1, R_2]$. The idea is that $M$ realizes $R_1$ if it terminates the computation on $q$, and $R_2$ otherwise.

$$\text{definition accRealize} := \lambda \text{sig}, n. \lambda M: \text{mTM sig n}. \lambda \text{acc: states sig n M. Rtrue, Rfalse.}$$

$$\forall t. \exists ! \text{outc.}$$

$$\text{let x, a, y := p in}$$

$$\text{if s == q then \langle start ?? M, null_action ?? \rangle}$$

$$\text{else \langle trans ?? M p. \rangle}$$

The semantics of the if-then-else machine can be now elegantly expressed in the following way:

$$\text{definition while_trans} := \lambda \text{sig, n. AM: mTM sig n. Aq: states sig n M. Ap.}$$

$$\text{let \langle s, a \rangle := p in}$$

$$\text{if s == q then \langle start ?? M, null_action ?? \rangle}$$

$$\text{else \langle trans ?? M p. \rangle}$$

$$\text{definition whileTM} := \lambda \text{sig, n. AM: mTM sig n. Aqacc: states ?? M.}$$

$$\text{mk_mTM sig n}$$

$$\text{(states ?? M)}$$

$$\text{(while_trans sig n qacc)}$$

$$\text{(start sig n M)}$$

$$\text{(\lambda s. halt sig n M s \land \neg s==qacc).}$$

4.3. While

The last machine we are interested in, implements a while-loop over a body machine $M$. Its definition is really simple, since we have just to add to $M$ a single transition leading from a distinguished final state $q$ back to the initial state.
More interesting is the way we can express the semantics of the while machine: provided that $M = [q : R_1, R_2]$, the while machine (relative to $q$) weakly realizes $R_1 \circ R_2$:

\[ \text{theorem sem_while: } \forall \text{sig}, n, M, \text{acc}, R_{\text{true}}, R_{\text{false}}. \]
\[ \text{halt } \text{sig} \ n \ M \ \text{acc} \ = \ \text{true} \rightarrow \]
\[ M \models [\text{acc}: R_{\text{true}}, R_{\text{false}}] \rightarrow \]
\[ \text{whileTM } \text{sig} \ n \ M \ \text{acc} \ ||_u (\text{star ? R}_{\text{true}}) \circ R_{\text{false}}. \]

In this case, the use of weak realizability is essential, since we are not guaranteed to exit the while loop, and the computation can actually diverge. Interestingly, we can reduce the termination of the while machine to the well foundedness of $R_{\text{true}}$:

\[ \text{theorem terminate_while: } \forall \text{sig}, n, M, \text{acc}, R_{\text{true}}, R_{\text{false}}, t. \]
\[ \text{halt } \text{sig} \ n \ M \ \text{acc} \ = \ \text{true} \rightarrow \]
\[ M \models [\text{acc}: R_{\text{true}}, R_{\text{false}}] \rightarrow \]
\[ \text{WF ? (inv ... R}_{\text{true}}) \ t \rightarrow \text{whileTM } \text{sig} \ n \ M \ \text{acc} \downarrow t. \]

5. Basic Machines

An important lesson learned in [8] was to avoid modelling relatively complex operations by directly writing a corresponding Turing machine. While writing the code is usually not very complex, proving its correctness can easily become a nightmare, due to the complexity of specifying and reasoning about internal states of the machines and all intermediate configurations. A much better approach consists in specifying a small set of basic machines, and define all other machines by means of the compositional constructs of the previous section. In this way, we may immediately forget about Turing machines’ internals, since the behavior of the whole program only depends on the behavior of its components.

We can divide the basic machines in two sets: machines acting on a single tape, and machines acting in parallel over two tapes.

The set of machines acting on a single table is essentially a subset of the machines\(^6\) already considered in [8]:

- **write c** write the character $c$ on the tape at the current head position
- **move D** move the head one step towards direction $D$
- **test_char f** perform a boolean test $f$ on the current character ending in state $tc_{\text{true}}$ or $tc_{\text{false}}$ according to the result of the test

\(^6\)Most of them are actually families of machines, indexed over suitable input arguments.
The specification of these machines is straightforward. We typically generalized them to the multi-tape case by means of a generic “injection” operation allowing to operate on a specified tape.

Typical basic machines working in parallel on two tapes are the following:

\textbf{par\_move\_step}\ i\ j\ D \ make\ a\ parallel\ D\ move\ on\ tapes\ i\ and\ j

\textbf{compare\_step}\ i\ j \ compare\ head\-characters\ on\ tapes\ i\ and\ j,\ ending\ up\ in\ state\ \text{comp}\_1\ if\ they\ are\ equal,\ and\ \text{comp}\_2\ otherwise.

\textbf{copy\_char\_N}\ i\ j \ copy\ head\-character\ on\ tape\ i\ to\ tape\ j\ without\ advancing\ the\ tapes.

It is interesting to observe that the swap operation, that played an important role when working on mono-tape machines, is absolutely useless in the multi-tape case.

5.1. Composing machines

Let us see an example of how we can use the previous bricks to build more complex functions. In Turing machines, moving the head to a specific position on the tape is a very frequent operation. In particular, our universal machine needs to return to one end of a given tape on several different occasions. We are now going to show how to write a machine \texttt{move\_to\_end} that moves the head towards a given direction until the end of the tape is met.

A step of the machine essentially consists of a move operation, but guarded by a conditional test; then we shall simply wrap a while machine around this step.

\begin{verbatim}
definition mte\_step := \lambda \alpha,D.
  ifTM ? (test\_null \alpha) (single\_finalTM ? (move \alpha D)) (nop ?) tc\_true.
\end{verbatim}

If the test succeeds we expect to end up in the single final state of the “then” machine, that is the following \texttt{mte\_acc} state:

\begin{verbatim}
definition mte\_acc := \forall \alpha,D.states ? (mte\_step \alpha D) :=
  \lambda \alpha,D.(inr ... (inl ... (inr ... start\_nop))).
\end{verbatim}

In this case, the input tape \(t_1\) must be a midtape and we expect to end up with a tape \(t_2\) resulting from \(t_1\) by performing the given move. This is expressed by the following relation:

\begin{verbatim}
definition R_mte\_step\_true := \lambda \alpha,D,t1,t2.
  3ls,c,rs. t1 = midtape \alpha ls c rs \wedge t2 = tape\_move ? t1 D.
\end{verbatim}

Conversely, if the test fails it means that we are in overflow, and we do nothing:

\begin{verbatim}
definition R_mte\_step\_false := \lambda \alpha,t1,t2:tape \alpha.
  current ? t1 = None \wedge t1 = t2.
\end{verbatim}

The semantics of the \texttt{mte\_step} machine is hence expressed as follows:
lemma sem_mte_step :
  ∀α,β,δ.mte_step α δ →
  [ mte_acc ... : R_mte_step_true α δ, R_mte_step_false α δ ].

Here is the full move_to_end program:

definition move_to_end := λσ,δ.whileTM δ (mte_step σ δ) (mte_acc ...).

definition R_move_to_end_l := λσ,int,outt.
  (current ? int = None ? ∧
  ∀ls,c,rs.int = midtape σ ls c rs →
  outt = mk_tape ? [ ] (None ?) (reverse ? ls@@c::rs)).

definition R_move_to_end_r := λσ,int,outt.
  (current ? int = None ? →
  ∀ls,c,rs.int = midtape σ ls c rs →
  outt = mk_tape ? (reverse ? rs@@c::ls) (None ?) [ ]).

lemma sem_move_to_end_l : ∀σ. move_to_end σ L → R_move_to_end_l σ.
lemma sem_move_to_end_r : ∀σ. move_to_end σ R → R_move_to_end_r σ.

We do not give semantics for the useless non-terminating machine obtained by
instantiating move_to_end to the N direction.

6. Normal Turing machines

A normal Turing machine is a mono-tape machine where:

1. the tape alphabet is \{0,1\};
2. the finite states are supposed to be an initial interval of the natural num-
bers.

By convention, we assume the starting state is 0.

record normalTM : Type :=
{ no_states : nat;
  pos_no_states : (0 < no_states);
  ntrans : (initN no_states)×Option bool → (initN no_states)×(Option bool)×Move;
  nhalt : initN no_states → bool }.

We may easily define a coercion transforming a normal TM into a traditional
Machine.

A normal configuration nconfig n is a configuration for a normal machine
with n states, that is a record composed of an element in initN n (representing
the state) and a single boolean tape.

definition nconfig := λn. config FinBool (initN n).
6.1. Tuples

By the results on FinSets of Section 2 we know that every function \( f \) between two finite sets \( A \) and \( B \) can be described by means of a finite graph of pairs \( \langle a, f(a) \rangle \). Hence, the transition function of a normal Turing machine can be described by a finite set of tuples \( \langle \langle i, c \rangle, \langle j, d, m \rangle \rangle \) of the following type:

\[
(\text{init} \mathbb{N} n \times \text{option bool}) \times (\text{init} \mathbb{N} n \times (\text{option bool}) \times \text{move})
\]

Unfortunately, this description is not directly suitable for a Universal Machine, since such a machine must work with a fixed set of states, while the size on \( n \) is unknown. Hence, we must pass from natural numbers to a representation for them on a finitary, e.g. binary, alphabet. In general, we shall associate to a pair \( \langle \langle i, c \rangle, \langle j, d, m \rangle \rangle \) a tuple with the following syntactical structure

\[
| w_i x w_j y z
\]

where

1. "|" is a special character used as a separator;
2. \( w_i \) and \( w_j \) are lists of booleans representing the states \( i \) and \( j \);
3. \( x \) represents the symbol \( c \): it is a special character \texttt{null} if \( c = \text{None} \) and is the boolean \( b \) if \( c = \text{Some} b \); the character \( y \) represents \( d \) in the same way;
4. similarly, for moves we map \( N \) into \texttt{null}, and \( L \) and \( R \) on the two booleans false and true.

This encoding of tuples is much simpler than the one described in [8]. In fact, working with a multi-tape machine, the set of tuples will be stored on a dedicated tape, that allows to spare a few delimiters; moreover, having multiple heads, we may avoid the annoying use of markers to remember tape positions during comparison and copying operations on strings (performed over different tapes).

\begin{verbatim}
definition mk_tuple := λqin,cin,qout,cout,mv.
  bar :: qin @ cin :: qout @ [cout; mv].
\end{verbatim}

We codified a state \( i \) in a machine with \( n \) states as a list of \( n \) bits where the bit at position \( i \) is set to 1 and the other bits are all 0. We also add an initial bit set to 1 if the state is final and to 0 otherwise. For instance, if you have four states and states 2 and 4 are final, they would be encoded as follows:

\[
1 = 01000, 2 = 10100, 3 = 00010, 4 = 10001
\]

The function computing such a representation is called \texttt{bits_of_state} (we omit the obvious definition). As a matter of fact, the actual encoding of states is not very important, but it is convenient to assume that (a) all states (and hence all tuples for a given machine) have a fixed, uniform length, and (b) it is easy to extract from the state the fact that it is final or not.

In the same way, the two functions \texttt{low_char} and \texttt{low_mv} compute the low level representation of characters and moves of the normal machine.
It is simple to prove that such encoding functions (as well as \texttt{bits_of_state}) are injective (and hence invertible).

Combining all these functions together, it is easy to write a function \texttt{tuple_encoding} mapping a machine tuple into a list of characters. More precisely, the function \texttt{tuple_encoding} takes as arguments a number \texttt{n} of tapes, a halting test function \texttt{h:Nat_to n→bool} relative to some normal machine \texttt{M}, a tuple \texttt{t} for the same machine and returns the encoding for \texttt{t}.

6.2. Input configurations

An input configuration is a string corresponding to some input \(\langle q, a \rangle\) for the transition function of the normal machine, preceded by the symbol “\(\mid\)” (\texttt{\textbar}).

If \texttt{\textbar}::qin@cin::cout@mv\] is a tuple, then \texttt{\textbar}::qin@cin\] is an input configuration, and similarly \texttt{\textbar}::cout@cout\] is the (next) input configuration.

In the universal machine, input configurations will be stored on a dedicated tape. The following predicate captures the relevant syntactical characteristics of input configurations:

\[
definition \text{is\_config} : := \lambda n, \text{cfg}. D qin, \text{cin}. \text{only\_bits} qin ^ \text{cin} \not= \text{bar} ^ |qin| = S n ^ \text{cfg} = \text{bar::qin@cin}.
\]

An important property of tuples is that, if they derive from a transition function, they are deterministic: for any input configuration there is only one corresponding output configuration.

\[
\text{lemma \ deterministic: } \forall M: \text{normalTM}.\forall t1,t2,c,\text{out1, out2}.\ 1 = \text{graph\_enum ?? (ntrans M)} \rightarrow \text{mem} ? t1 \rightarrow \text{mem} ? t2 \rightarrow \text{is\_config (no\_states M) c} \rightarrow \text{tuple\_encoding ? (nhalt M) t1} = (c@out1) \rightarrow \text{tuple\_encoding ? (nhalt M) t2} = (c@out2) \rightarrow \text{out1} = \text{out2}.
\]

6.3. The table of tuples

The list of all tuples, concatenated together, provides the low level description of the normal Turing machine to be interpreted by the Universal Machine: we call it a \textit{table}.

\[
definition \text{table\_TM} : := \lambda n, h. \text{flatten ? (tuples\_list n h l)}.
\]
The main lemma relating a table to the list of its tuples \( l \) is the following one, stating that for any input configuration \( c \), if \( c \) is matched inside the table, then it is followed by a string \( \text{out} \) such that \( c@\text{out} \) is the encoding of some tuple \( t \) in \( l \).

\[
\text{lemma table_to_list: } \forall n, l, h, c. \ \text{is_config n c} \rightarrow
\forall l, l_r. \ \text{table_TM n l h} = l_l@c@l_r \rightarrow
\exists \text{out}, l_r, t. \ l_r = \text{out}@l_r \land \text{tuple_encoding n h t} = (c@\text{out}) \land \text{mem t} \land l.
\]

7. The Universal Machine

In this section we define a multi-tape Universal Machine (UM) for normal Turing machines. Let \( M \) be the normal machine to be simulated; the universal machine will work with three tapes, with the following functions:

- the object tape (obj) is used to simulate the tape of \( M \);
- the configuration (cfg) tape contains the encoding of the current state of \( M \), concatenated with a copy of the head symbol (that is, at each step of \( M \), the input for its transition function);
- the program (prg) tape contains the table of tuples relative to \( M \).

Each step of the normal machine \( M \) is simulated by the following sequence of operations:

\[
definition \text{unistep :=}
\begin{align*}
&\text{match_m \ cfg \ prg \ UniS 2} : (\ast \text{ find a matching tuple } \ast) \\
&\text{restart_tape \ cfg} : (\ast \text{ move to the beginning of the cfg tape } \ast) \\
&\text{mmove \ cfg \ ? \ 2 \ R} : (\ast \text{ skip initial bar on cfg } \ast) \\
&\text{copy \ prg \ cfg \ UniS 2} : (\ast \text{ copy the tuple output to cfg } \ast) \\
&\text{exec_move} : (\ast \text{ update the obj tape } \ast)
\end{align*}
\]

where \text{mmove} is the (non-primitive) multi-tape version of \text{move}. The behaviour of the other functions is summarized in Figure 1, where we also also emphasize the expected positions of the tape heads after each operation (that is a quite delicate semantical issue). An execution of \text{unistep} is shown in Figure 2.

The body of the universal machine \text{uni_body} consists of checking the termination condition (i.e. examining the first bit of the current state, to see if it is a final state) and, if the condition is not met, executing \text{uni_step}.

The universal machine is simply a while over \text{uni_body}:

\[
\text{definition \ uni_body :=}
\begin{align*}
&\text{ifTM ?? (mtestR \ ? \ cfg \ 2 \ stop)} \\
&\text{ (single_finalTM ?? \ uni_step)} \\
&\text{ (nop \ ...) (mtestR\_acc \ ? \ cfg \ 2 \ stop)}.
\end{align*}
\]

\[
\text{definition \ universalTM :=whileTM \ ? \ uni_body \ us\_acc.}
\]
Figure 1: Machines used in unistep.
Figure 2: Sample execution of unistep.

8. Matching

The matching operation involves repeatedly comparing the current configuration to the input configuration of each tuple on the prg tape: when the two are different, we will move to the next tuple and loop; otherwise we will stop, keeping the head of the prg tape at the beginning of the output configuration of the matching tuple.

Matching is the most complex operation used in the universal machine, since it is obtained by iterating, in a while loop, the string comparison machine, which is made of a while loop itself. In our mono-tape formalization, its implementation was further complicated by the need to consider various kinds of delimiters, and to set marks needed to move back and forth between the two strings under consideration.

8.1. String comparison

In a multi-tape setting we can compare two characters in a single step, without any need to store the first character in the internal state (let alone use the more complicated comparison technique adopted in [8] for technical reasons). A further difference, accounting for more simplification, is that the
new machine does not use delimiters to decide whether the comparison has been completed successfully, but terminates when one of the two tapes is over. This machine is obtained by means of a simple while iterating the `compare_step` basic machine.

**definition**

```plaintext
definition compare := λi,j,sig,n. 
whileTM ...(compare_step i j sig n) compl.
```

More precisely, the compare machine running on tapes `i` and `j` will succeed if one of the two is a prefix of the other one. Since we plan to use the machine to compare an initial configuration in `prg` with the content of `cfg`, success corresponds to the case where the portion of those two tapes standing on the right of the head is found to be equal, until the end of tape `cfg` is reached.

Failure happens when at some point, the \(k\)-th characters on the right of the two tapes considered are different, in which case the heads are left on the two differing characters. These two outcomes are described by the semantics of `compare`:

**definition**

```plaintext
definition R_compare := 
λi,j,sig,n.λint,outt: Vector (tape sig) (S n). 
... 
\(\forall i \leq j \leq S n. \lambda n.\eta i = \eta j \Rightarrow \eta n = \eta n\).
```

The semantics of `compare` as we formalized it also includes two more possible outcomes (here denoted by ellipses): a symmetric success case (due to the fact that the machine operates in the same way on the two tapes) and a base case stating the outcome of the machine when the termination condition is immediately verified and no iterations of `compare_step` are executed.

8.2. match_step

The `match_step` starts by performing a compare over the tapes `cfg` and `prg`, then it checks whether the halting condition is met: we want to stop if the head of `cfg` or `prg` has stopped over an uninitialized portion of the tape. In the former case, the compare operation was successful; in the latter case, we have finished examining a table without finding a matching tuple. Checking whether
the table has ended may seem useless, since it is supposed to represent a total
transition function, but it will allow us to prove the termination of \texttt{match\_step}
for all inputs (including ill-formed ones).

If the termination condition is not met, in order to prepare for a new iteration
of \texttt{match\_step} we will move back to the start of tape \texttt{cfg}, and to the next tuple
on tape \texttt{prg}. Since both the configuration on \texttt{cfg} and all the tuples in the tape
start with a “|” character, we obtain the same result with a simpler machine
by moving to the next character in \texttt{prg}, instead of moving to the next tuple:
subsequent iterations will fail immediately until the next tuple, starting with
“|”, is found.

\begin{verbatim}
definition match_step := \lambda src,dst,sig,n.
    compare src dst sig n ·
        (ifTM ?? (partest sig n (match_test src dst sig ?))
            (single_finalTM ??
                (rewind src dst sig n · mmove dst ?? R))
            (nop ...
                partest1).
\end{verbatim}

Notice that the termination condition \texttt{match\_test} will check whether either
the source or the destination tape have ended.

The \texttt{match\_m} machine is obtained by simply iterating \texttt{match\_step} until the
termination condition is met.

\begin{verbatim}
definition match_m := \lambda src,dst,sig,n.
    whileTM ...
        (match_step src dst sig n)
        (inr ?? (inr ?? (inl ...
            (inr ?? start_nop))))).
\end{verbatim}

After a successful execution of \texttt{match\_m}, the \texttt{prg} head will be at the beginning
of the output of the matching tuple, and the \texttt{cfg} head will be at the right end
of its tape in overflow position.

9. State update

We decompose the execution of an action in two simpler operations, which
can be executed sequentially: in the first half, we will copy the output portion
of the tuple selected by the \texttt{match\_m} machine into the \texttt{cfg} tape, which will then
contain the new current state and the new character to be written to the tape;
the second half is concerned with updating the \texttt{obj} tape and obtaining the next
input configuration.

The update of the state is performed, after returning the head on the \texttt{cfg}
tape to the first character on the left (\texttt{restart\_tape}), by the \texttt{copy} machine.

\begin{verbatim}
definition copy := \lambda src,dst,sig,n.
    whileTM ...
        (copy_step src dst sig n) copy1.
\end{verbatim}

Similarly to the compare operation, copying is done one character at a time
and stops when the end of the tape is reached on either the source or the
destination. This is obtained by iterating the conditional machine \texttt{copy\_step} in
a while cycle. In our case, it is the destination (\texttt{cfg}) that is going to end first:
thus at the end of the execution, the cfg head will be at the right end of its tape
in overflow position, and the prg head will have moved to the last character of
the selected tuple (representing the direction towards which the obj head should
move).

10. Tape update

Finally, the exec move updates the tape of the simulated machine.

\[
\text{definition exec \_move :=}
\]
\[
\text{cfg \_to \_obj \cdot tape \_move \_obj \cdot restart \_tape prg 2 \cdot obj \_to \_cfg.}
\]

The cfg \_to \_obj machine reads the new character to be written from the cfg
tape (where it has just been written by \text{copy}) and writes it to the obj tape at
the current position. However, if the character is not a bit, but the special value
null, the prg tape will be left untouched.

tape move obj moves the obj head to the left (if the current character under
the prg head is a 0 bit), to the right (if that character is a 1 bit), or does not
move it at all (if that character is a null).

The restart tape has the usual semantics, and is used in this case to return
the prg head to its initial position, where it is expected to be at the next iteration
of unistep.

The last machine obj to cfg updates cfg putting the new character read
from obj, obtaining the next input configuration. If the obj head is in an overflow
position, the special character null will be written to cfg instead. After this
operation, the cfg head is also returned to its initial position.

The previous machines are relatively trivial; the interesting point, in this
case, is to relate their low-level operational behaviour to the intended meaning,
that is to mimic the execution of a move of the simulated machine.

11. Main Results

Given a configuration \( c \) for a normal machine \( M \), the following function builds
the corresponding “low level” representation, i.e. the three tapes \([\text{obj;cfg;prg}]\)
manipulated by the Universal Machine:

\[
\text{definition low \_tapes: VM: normalTM.\forall c:nconfig (no \_states M).Vector ? 3 :=}
\]
\[
\text{\lambda VM: normalTM.\forall c:nconfig (no \_states M).Vector \_of \_list ?}
\]
\[
\text{[tape \_map ?? bit (ctape ?? c)}
\]
\[
\text{;midtape ? [ ] bar}
\]
\[
\text{;midtape ? [ ] bar (tail ? (table \_TM ? (graph \_enum ?? (ntrans M)) (nhalt M)))]
\].
\]

The first tape is simply an embedding of the tape \( c\text{tape ?? c} \) in the alphabet
of the Universal Machine: every bit \( b \) is transformed in the character \( \text{bit b} \); the
tape map function is the obvious extension of the map functions to tapes:
The second tape contains the current input configuration for the transition function discussed in Section 6.2.

Finally, the third tape is just the table of tuples for the normal machine \( M \).

The semantics of the \texttt{unistep} machine can be expressed very elegantly in terms of \texttt{low_tapes}:

\begin{verbatim}
definition tape_map :\forall A,B:FinSet. \lambda f:A \rightarrow B.\lambda t.
    mk_tape B (map ?? f (left ? t))
    (option_map ?? f (current ? t)) (map ?? f (right ? t)).
\end{verbatim}

Every relation over tapes can be reflected into a corresponding relation on their low-level representations:

\begin{verbatim}
definition R_unistep_high :=\forall M:normalTM.\lambda t1,t2.
    \forall c:nconfig (no_states M).
    t1 = low_tapes M c \rightarrow t2 = low_tapes M (step ? M c).
\end{verbatim}

Starting from the above semantics of the \texttt{unistep} machine, it is then easy (20 lines) to prove that, for any normal machine \( M \), the Universal Machine weakly realizes the low level version of the canonical relation for \( M \):

\begin{verbatim}
theorem sem_universal: \forall M:normalTM. \forall q.
    universalTM \models \text{low}_R M q (R(TM FinBool M q)).
\end{verbatim}

As a corollary of the latter result we obtain that, for any relation weakly realized by \( M \), the universal machine weakly realizes its low level counterpart.

\begin{verbatim}
M \models R \rightarrow universalTM \models \text{low}_R M (start ? M) R.
\end{verbatim}

Termination is stated by the following result, whose proof (once we may rely the totality of the \texttt{unistep} function, is entirely straightforward (ten lines of code):

\begin{verbatim}
theorem terminate_UTM: \forall M:normalTM. \forall t.
    universalTM \models \text{low}_R (mk_config ?? (start ? M) t).
\end{verbatim}

12. Discussion

We provided in this paper a formalization of the basic Theory of Turing machines, up to the definition of a universal machine and the proof of its correctness.

The work is a deep revisitation of [8]; in particular, we generalized the investigation from mono-tape machines to the multi-tape case. In spite of the fact that the meta-theory of multi-tapes machines is technically more complex, its formalization, taking advantage of the vector library of Matita, takes about the same space of the mono-tape case.
On the other side, the formalization of the universal machine is sensibly simplified. In Table 3 we compare the size, in lines, of the main files in the case of the mono-tape version described in [8] with respect to the multi-tape version described in this article. Note that the complex management of marks for copying/comparing strings in the mono-tape case has no counterpart in the multi-tape case. We should also stress that termination was still under development in [8], while it has been completely proved in the current version.

<table>
<thead>
<tr>
<th>file name</th>
<th>mono</th>
<th>multi</th>
<th>content</th>
</tr>
</thead>
<tbody>
<tr>
<td>marks.ma</td>
<td>901</td>
<td>0</td>
<td>management of marks</td>
</tr>
<tr>
<td>alphabet.ma</td>
<td>110</td>
<td>59</td>
<td>alphabet of the universal machine</td>
</tr>
<tr>
<td>normalTM.ma</td>
<td>319</td>
<td>257</td>
<td>normal Turing machines</td>
</tr>
<tr>
<td>tuples.ma</td>
<td>276</td>
<td>229</td>
<td>the table of tuples</td>
</tr>
<tr>
<td>match.ma</td>
<td>727</td>
<td>729</td>
<td>matching a tuple in the table</td>
</tr>
<tr>
<td>uni_step_aux.ma</td>
<td>778</td>
<td>521</td>
<td>auxiliary machines</td>
</tr>
<tr>
<td>uni_step.ma</td>
<td>585</td>
<td>458</td>
<td>emulation of a high-level step</td>
</tr>
<tr>
<td>universal.ma</td>
<td>394</td>
<td>120</td>
<td>the universal machine</td>
</tr>
<tr>
<td>total</td>
<td>4090</td>
<td>2373</td>
<td></td>
</tr>
</tbody>
</table>

Figure 3: Main files and their dimension in lines.

The universal machine presented in this article is a multi-tape machine simulating mono-tape normal machines. To provide a truly universal machine two auxiliary mappings are needed, one transforming a multi-tape machine to a mono-tape one (possibly enlarging the alphabet) and one mapping a mono-tape machine to a Normal machine. We implemented both these transformations and proved them correct: the proofs are not trivial: the first one takes about 2 KLOC, and the second one 1 KLOC. Both transformations are quite interesting, for different reasons, but their description would add very little to this article and, also due to space limitations, we prefer to postpone their discussion for a future work.

13. Related works

As we mentioned in the introduction, at the time we first submitted this article there was no other mechanizations of Turing Machines to compare with. Very recently, however, Xu, Zhang and Urban published an alternative formalization of the theory of Turing machines [35], partially inspired by our previous work [8].

The approach followed by Xu, Zhang and Urban is sensibly different from ours, and mostly based on Boolos et al. textbook [16]. Starting from a simple notion of Turing machine similar to our normal Turing machine, they consider a small hierarchy of higher level computation models, implementing each layer on the previous one. The intermediate layer is provided by abacus machines, that
are random access machines with an infinite number of registers, each able to store an arbitrarily large natural number. The highest level is the language of recursive functions with primitive recursion and minimization. The interpreter for Turing machines is written in this language, and then compiled into a Turing machine to give a truly universal machine.

At the semantic level, Xu, Zhang and Urban develop a Hoare-style technique to reason about concrete Turing machines (and abacus programs). A Hoare-triple \( \{P\} M \{Q\} \) expresses the idea that a program \( M \) starting the computation with a tape satisfying \( P \) will terminate with a tape satisfying \( Q \). As admitted by the authors themselves, the idea is very similar to our notion of realizability. As a matter of fact, we considered the possibility of expressing semantics in the form of triples. However, one is often interested in expressing the properties of the output tape \textit{in terms} of the properties of the input tape, that amounts to saying that \( Q \) should be a relation, in which case there is no need for \( P \) at all (unless you are interested in expressing guards, an approach that we developed as well and finally did not use). From a practical point of view, our approach to the construction of Turing machines seems to be much more modular and compositional than the one in \cite{35}. All our basic machines have very few states (up to 4) and all other machines are derived by composition: on the contrary, Xu, Zhang and Urban define very complex and monolithic machines with a lot of states (e.g. the copy machine has 15 states, and other machines with even more states are mentioned). This is admittedly due to a deficiency of their semantical approach\footnote{see the discussion at page 158}.

Even if one is not interested - as we are, in the long term - to use Turing machines as a foundational model for Complexity Theory, the efficiency of the Universal machine remains an interesting issue. The machine described in this paper is fairly efficient: the slow-down with respect to the simulated program \( M \) is constant, where the constant depends polynomially on the size of \( M \) (we have not proved it formally yet, though). With some care, the transformations from multi-tape to mono-tape machines, and from mono-tape to normal machines should not change this complexity (one needs to exploit the fact that the size of all tapes but one is fixed along the computation). So, our interpreter seems to be fair, in the sense of \cite{4} (that remains to be formally checked).

The complexity of the universal machine in \cite{35} is much worse. The simulation of abacus machines on Turing Machines results in a cubic slow-down: fetching the parameters of an instruction has a complexity that is proportional to the dimension of the tape, and such a dimension grows quadratically with time. The cost of simulating recursive functions on abacus machines is not so clear, and the issue is not discussed in \cite{35}; in particular, a pretty delicate issue is related to the adoption of a unary notation for the natural numbers, that could sensibly alter the cost model for recursive functions.

From the point of view of the complexity of the formalization, our approach seems to be sensibly more compact than the one in \cite{35}. Even counting the
correctness proofs for the operations transforming a multi-tape machine into a
normal machine our development takes, in the whole, less than 6,000 lines (plus
about 4,700 lines for the formalization of mono and multi-tape machines).

According to the figures provided by the authors in [35], the formalization of
the universal machine takes by itself more than 10,000 lines of code, plus 4,600
lines for the formalization of abacus machines and their translation to Turing
machines, and 2,800 lines for the formalization of recursive functions and their
implementation on abacus machines.

14. Conclusions

Proving the correctness of a universal Turing machine is a quite complex
task: Norrish describes it as a “daunting prospect” ([29], page 310), and Xu,
Zhang and Urban admit that “is not a project one wants to undertake too
many times” ([35], page 160). Still, it is an interesting exercise, stressing the
potentialities of interactive provers on a relatively elementary topic, and we hope
more people belonging to different proof assistant communities will undertake
the job.

For us, the long term goal is to define a solid ground that could allow us to
talk about Complexity at a higher level of abstraction. Due to their finitistic
nature, the notions of time and space complexity for Turing machines are par-
ticularly clear and universally accepted, that is not the case for other, higher
level programming paradigms. So, even modern textbooks in Complexity The-
ory (see e.g. [3]) start with introducing Turing Machines, possibly to claim,
immediately after, that the computational model does not matter. The natural
question is to understand what matters, then.

The final goal of our research would be to obtain a formal, axiomatic treat-
ment of Complexity Theory at a comfortable level of abstraction, expressing
it in terms of a few basic assumptions (e.g. the ability to perform bound in-
terpretation with a given, possibly parametric complexity) and suitable closure
properties. We plan to derive such an abstract framework from a reverse inves-
tigation of major results of Complexity Theory, reconstructing from proofs the
key assumptions underlying them (see [5] for a first, preliminary result in this
direction).

Eventually, the resulting axiomatization will need to be validated with re-
spect to concrete cost models, and in particular with respect to Turing ma-
chines, that provides the actual foundation for Complexity Theory. Hence, in
conjunction with the “reverse” approach, it is also important to promote a more
traditional forward approach, deriving out of concrete models the key notions
and results for the formal study of their complexity aspects. The work in this
paper, is meant to be a contribution along this second line of research.
References


