

## und.1 Verifying the Representation

tms:und:ver:  
sec

In order to verify that our representation works, we have to prove two things. First, we have to show that if  $M$  halts on input  $w$ , then  $\tau(M, w) \rightarrow \alpha(M, w)$  is valid. Then, we have to show the converse, i.e., that if  $\tau(M, w) \rightarrow \alpha(M, w)$  is valid, then  $M$  does in fact eventually halt when run on input  $w$ .

explanation

The strategy for proving these is very different. For the first result, we have to show that a **sentence** of first-order logic (namely,  $\tau(M, w) \rightarrow \alpha(M, w)$ ) is valid. The easiest way to do this is to give a **derivation**. Our proof is supposed to work for all  $M$  and  $w$ , though, so there isn't really a single **sentence** for which we have to give a derivation, but infinitely many. So the best we can do is to prove by induction that, whatever  $M$  and  $w$  look like, and however many steps it takes  $M$  to halt on input  $w$ , there will be a **derivation** of  $\tau(M, w) \rightarrow \alpha(M, w)$ .

Naturally, our induction will proceed on the number of steps  $M$  takes before it reaches a halting configuration. In our inductive proof, we'll establish that for each step  $n$  of the run of  $M$  on input  $w$ ,  $\tau(M, w) \models \chi(M, w, n)$ , where  $\chi(M, w, n)$  correctly describes the configuration of  $M$  run on  $w$  after  $n$  steps. Now if  $M$  halts on input  $w$  after, say,  $n$  steps,  $\chi(M, w, n)$  will describe a halting configuration. We'll also show that  $\chi(M, w, n) \models \alpha(M, w)$ , whenever  $\chi(M, w, n)$  describes a halting configuration. So, if  $M$  halts on input  $w$ , then for some  $n$ ,  $M$  will be in a halting configuration after  $n$  steps. Hence,  $\tau(M, w) \models \chi(M, w, n)$  where  $\chi(M, w, n)$  describes a halting configuration, and since in that case  $\chi(M, w, n) \models \alpha(M, w)$ , we get that  $T(M, w) \models \alpha(M, w)$ , i.e., that  $\models \tau(M, w) \rightarrow \alpha(M, w)$ .

The strategy for the converse is very different. Here we assume that  $\models \tau(M, w) \rightarrow \alpha(M, w)$  and have to prove that  $M$  halts on input  $w$ . From the hypothesis we get that  $\tau(M, w) \models \alpha(M, w)$ , i.e.,  $\alpha(M, w)$  is true in every **structure** in which  $\tau(M, w)$  is true. So we'll describe a **structure**  $\mathfrak{M}$  in which  $\tau(M, w)$  is true: its domain will be  $\mathbb{N}$ , and the interpretation of all the  $Q_q$  and  $S_\sigma$  will be given by the configurations of  $M$  during a run on input  $w$ . So, e.g.,  $\mathfrak{M} \models Q_q(\bar{m}, \bar{n})$  iff  $T$ , when run on input  $w$  for  $n$  steps, is in state  $q$  and scanning square  $m$ . Now since  $\tau(M, w) \models \alpha(M, w)$  by hypothesis, and since  $\mathfrak{M} \models \tau(M, w)$  by construction,  $\mathfrak{M} \models \alpha(M, w)$ . But  $\mathfrak{M} \models \alpha(M, w)$  iff there is some  $n \in |\mathfrak{M}| = \mathbb{N}$  so that  $M$ , run on input  $w$ , is in a halting configuration after  $n$  steps.

**Definition und.1.** Let  $\chi(M, w, n)$  be the **sentence**

$$Q_q(\bar{m}, \bar{n}) \wedge S_{\sigma_0}(\bar{0}, \bar{n}) \wedge \cdots \wedge S_{\sigma_k}(\bar{k}, \bar{n}) \wedge \forall x (\bar{k} < x \rightarrow S_0(x, \bar{n}))$$

where  $q$  is the state of  $M$  at time  $n$ ,  $M$  is scanning square  $m$  at time  $n$ , square  $i$  contains symbol  $\sigma_i$  at time  $n$  for  $0 \leq i \leq k$  and  $k$  is the right-most non-blank square of the tape at time 0, or the right-most square the tape head has visited after  $n$  steps, whichever is greater.

tms:und:ver:  
lem:halt-config-implies-halt

**Lemma und.2.** *If  $M$  run on input  $w$  is in a halting configuration after  $n$  steps, then  $\chi(M, w, n) \models \alpha(M, w)$ .*

*Proof.* Suppose that  $M$  halts for input  $w$  after  $n$  steps. There is some state  $q$ , square  $m$ , and symbol  $\sigma$  such that:

1. After  $n$  steps,  $M$  is in state  $q$  scanning square  $m$  on which  $\sigma$  appears.
2. The transition function  $\delta(q, \sigma)$  is undefined.

$\chi(M, w, n)$  is the description of this configuration and will include the clauses  $Q_q(\bar{m}, \bar{n})$  and  $S_\sigma(\bar{m}, \bar{n})$ . These clauses together imply  $\alpha(M, w)$ :

$$\exists x \exists y \left( \bigvee_{\langle q, \sigma \rangle \in X} (Q_q(x, y) \wedge S_\sigma(x, y)) \right)$$

since  $Q_{q'}(\bar{m}, \bar{n}) \wedge S_{\sigma'}(\bar{m}, \bar{n}) \models \bigvee_{\langle q, \sigma \rangle \in X} (Q_q(\bar{m}, \bar{n}) \wedge S_\sigma(\bar{m}, \bar{n}))$ , as  $\langle q', \sigma' \rangle \in X$ . □

explanation

So if  $M$  halts for input  $w$ , then there is some  $n$  such that  $\chi(M, w, n) \models \alpha(M, w)$ . We will now show that for any time  $n$ ,  $\tau(M, w) \models \chi(M, w, n)$ .

**Lemma und.3.** *For each  $n$ , if  $M$  has not halted after  $n$  steps,  $\tau(M, w) \models \chi(M, w, n)$ .* tms:und:ver:  
lem:config

*Proof.* Induction basis: If  $n = 0$ , then the conjuncts of  $\chi(M, w, 0)$  are also conjuncts of  $\tau(M, w)$ , so entailed by it.

Inductive hypothesis: If  $M$  has not halted before the  $n$ th step, then  $\tau(M, w) \models \chi(M, w, n)$ . We have to show that (unless  $\chi(M, w, n)$  describes a halting configuration),  $\tau(M, w) \models \chi(M, w, n + 1)$ .

Suppose  $n > 0$  and after  $n$  steps,  $M$  started on  $w$  is in state  $q$  scanning square  $m$ . Since  $M$  does not halt after  $n$  steps, there must be an instruction of one of the following three forms in the program of  $M$ :

1.  $\delta(q, \sigma) = \langle q', \sigma', R \rangle$
2.  $\delta(q, \sigma) = \langle q', \sigma', L \rangle$
3.  $\delta(q, \sigma) = \langle q', \sigma', N \rangle$

tms:und:ver:  
right  
tms:und:ver:  
left  
tms:und:ver:  
stay

We will consider each of these three cases in turn.

1. Suppose there is an instruction of the form (1). By ??, ??, this means that

$$\forall x \forall y ((Q_q(x, y) \wedge S_\sigma(x, y)) \rightarrow (Q_{q'}(x', y') \wedge S_{\sigma'}(x, y') \wedge \varphi(x, y)))$$

is a conjunct of  $\tau(M, w)$ . This entails the following **sentence** (universal instantiation,  $\bar{m}$  for  $x$  and  $\bar{n}$  for  $y$ ):

$$(Q_q(\bar{m}, \bar{n}) \wedge S_\sigma(\bar{m}, \bar{n})) \rightarrow (Q_{q'}(\bar{m}', \bar{n}') \wedge S_{\sigma'}(\bar{m}, \bar{n}') \wedge \varphi(\bar{m}, \bar{n})).$$

By induction hypothesis,  $\tau(M, w) \models \chi(M, w, n)$ , i.e.,

$$Q_q(\bar{m}, \bar{n}) \wedge S_{\sigma_0}(\bar{0}, \bar{n}) \wedge \cdots \wedge S_{\sigma_k}(\bar{k}, \bar{n}) \wedge \forall x (\bar{k} < x \rightarrow S_0(x, \bar{n}))$$

Since after  $n$  steps, tape square  $m$  contains  $\sigma$ , the corresponding conjunct is  $S_\sigma(\bar{m}, \bar{n})$ , so this entails:

$$Q_q(\bar{m}, \bar{n}) \wedge S_\sigma(\bar{m}, \bar{n})$$

We now get

$$\begin{aligned} & Q_{q'}(\bar{m}', \bar{n}') \wedge S_{\sigma'}(\bar{m}, \bar{n}') \wedge \\ & S_{\sigma_0}(\bar{0}, \bar{n}') \wedge \cdots \wedge S_{\sigma_k}(\bar{k}, \bar{n}') \wedge \\ & \forall x (\bar{k} < x \rightarrow S_0(x, \bar{n}')) \end{aligned}$$

as follows: The first line comes directly from the consequent of the preceding conditional, by modus ponens. Each conjunct in the middle line—which excludes  $S_{\sigma_m}(\bar{m}, \bar{n}')$ —follows from the corresponding conjunct in  $\chi(M, w, n)$  together with  $\varphi(\bar{m}, \bar{n})$ .

If  $m < k$ ,  $\tau(M, w) \vdash \bar{m} < \bar{k}$  (??) and by transitivity of  $<$ , we have  $\forall x (\bar{k} < x \rightarrow \bar{m} < x)$ . If  $m = k$ , then  $\forall x (\bar{k} < x \rightarrow \bar{m} < x)$  by logic alone. The last line then follows from the corresponding conjunct in  $\chi(M, w, n)$ ,  $\forall x (\bar{k} < x \rightarrow \bar{m} < x)$ , and  $\varphi(\bar{m}, \bar{n})$ . If  $m < k$ , this already is  $\chi(M, w, n + 1)$ .

Now suppose  $m = k$ . In that case, after  $n + 1$  steps, the tape head has also visited square  $k + 1$ , which now is the right-most square visited. So  $\chi(M, w, n + 1)$  has a new conjunct,  $S_0(\bar{k}', \bar{n}')$ , and the last conjunct is  $\forall x (\bar{k}' < x \rightarrow S_0(x, \bar{n}'))$ . We have to verify that these two **sentences** are also implied.

We already have  $\forall x (\bar{k} < x \rightarrow S_0(x, \bar{n}'))$ . In particular, this gives us  $\bar{k} < \bar{k}' \rightarrow S_0(\bar{k}', \bar{n}')$ . From the axiom  $\forall x x < x'$  we get  $\bar{k} < \bar{k}'$ . By modus ponens,  $S_0(\bar{k}', \bar{n}')$  follows.

Also, since  $\tau(M, w) \vdash \bar{k} < \bar{k}'$ , the axiom for transitivity of  $<$  gives us  $\forall x (\bar{k}' < x \rightarrow S_0(x, \bar{n}'))$ . (We leave the verification of this as an exercise.)

2. Suppose there is an instruction of the form (2). Then, by ??, ??,

$$\begin{aligned} & \forall x \forall y ((Q_q(x', y) \wedge S_\sigma(x', y)) \rightarrow \\ & (Q_{q'}(x, y') \wedge S_{\sigma'}(x', y') \wedge \varphi(x, y))) \wedge \\ & \forall y ((Q_{q_i}(0, y) \wedge S_\sigma(0, y)) \rightarrow \\ & (Q_{q_j}(0, y') \wedge S_{\sigma'}(0, y') \wedge \varphi(0, y))) \end{aligned}$$

is a conjunct of  $\tau(M, w)$ . If  $m > 0$ , then let  $l = m - 1$  (i.e.,  $m = l + 1$ ). The first conjunct of the above [sentence](#) entails the following:

$$(Q_q(\bar{l}', \bar{n}) \wedge S_\sigma(\bar{l}', \bar{n})) \rightarrow \\ (Q_{q'}(\bar{l}, \bar{n}') \wedge S_{\sigma'}(\bar{l}', \bar{n}') \wedge \varphi(\bar{l}, \bar{n}))$$

Otherwise, let  $l = m = 0$  and consider the following [sentence](#) entailed by the second conjunct:

$$((Q_{q_i}(o, \bar{n}) \wedge S_\sigma(o, \bar{n})) \rightarrow \\ (Q_{q_j}(o, \bar{n}') \wedge S_{\sigma'}(o, \bar{n}') \wedge \varphi(o, \bar{n})))$$

Either sentence implies

$$Q_{q'}(\bar{l}, \bar{n}') \wedge S_{\sigma'}(\bar{m}, \bar{n}') \wedge \\ S_{\sigma_0}(\bar{0}, \bar{n}') \wedge \cdots \wedge S_{\sigma_k}(\bar{k}, \bar{n}') \wedge \\ \forall x (\bar{k} < x \rightarrow S_0(x, \bar{n}'))$$

as before. (Note that in the first case,  $\bar{l}' = \bar{m}$  and in the second case  $\bar{l} = o$ .) But this just is  $\chi(M, w, n + 1)$ .

3. Case (3) is left as an exercise.

We have shown that for any  $n$ ,  $\tau(M, w) \models \chi(M, w, n)$ . □

**Problem und.1.** Complete case (3) of the proof of [Lemma und.3](#).

**Problem und.2.** Give a [derivation](#) of  $S_{\sigma_i}(\bar{i}, \bar{n}')$  from  $S_{\sigma_i}(\bar{i}, \bar{n})$  and  $\varphi(m, n)$  (assuming  $i \neq m$ , i.e., either  $i < m$  or  $m < i$ ).

**Problem und.3.** Give a [derivation](#) of  $\forall x (\bar{k}' < x \rightarrow S_0(x, \bar{n}'))$  from  $\forall x (\bar{k} < x \rightarrow S_0(x, \bar{n}'))$ ,  $\forall x x < x'$ , and  $\forall x \forall y \forall z ((x < y \wedge y < z) \rightarrow x < z)$ .

**Lemma und.4.** *If  $M$  halts on input  $w$ , then  $\tau(M, w) \rightarrow \alpha(M, w)$  is valid.*

[tms:und:ver:](#)  
[lem:valid-if-halt](#)

*Proof.* By [Lemma und.3](#), we know that, for any time  $n$ , the description  $\chi(M, w, n)$  of the configuration of  $M$  at time  $n$  is entailed by  $\tau(M, w)$ . Suppose  $M$  halts after  $k$  steps. It will be scanning square  $m$ , say. Then  $\chi(M, w, k)$  describes a halting configuration of  $M$ , i.e., it contains as conjuncts both  $Q_q(\bar{m}, \bar{k})$  and  $S_\sigma(\bar{m}, \bar{k})$  with  $\delta(q, \sigma)$  undefined. By [Lemma und.2](#) Thus,  $\chi(M, w, k) \models \alpha(M, w)$ . But since  $(M, w) \models \chi(M, w, k)$ , we have  $\tau(M, w) \models \alpha(M, w)$  and therefore  $\tau(M, w) \rightarrow \alpha(M, w)$  is valid. □

[explanation](#) To complete the verification of our claim, we also have to establish the reverse direction: if  $\tau(M, w) \rightarrow \alpha(M, w)$  is valid, then  $M$  does in fact halt when started on input  $m$ .

*tms:und.ver:*  
*lem:halt-if-valid*

**Lemma und.5.** *If  $\models \tau(M, w) \rightarrow \alpha(M, w)$ , then  $M$  halts on input  $w$ .*

*Proof.* Consider the  $\mathcal{L}_M$ -**structure**  $\mathfrak{M}$  with domain  $\mathbb{N}$  which interprets 0 as 0, ' as the successor function, and  $<$  as the less-than relation, and the predicates  $Q_q$  and  $S_\sigma$  as follows:

$$Q_q^{\mathfrak{M}} = \{ \langle m, n \rangle : \begin{array}{l} \text{started on } w, \text{ after } n \text{ steps,} \\ M \text{ is in state } q \text{ scanning square } m \end{array} \}$$
$$S_\sigma^{\mathfrak{M}} = \{ \langle m, n \rangle : \begin{array}{l} \text{started on } w, \text{ after } n \text{ steps,} \\ \text{square } m \text{ of } M \text{ contains symbol } \sigma \end{array} \}$$

In other words, we construct the **structure**  $\mathfrak{M}$  so that it describes what  $M$  started on input  $w$  actually does, step by step. Clearly,  $\mathfrak{M} \models \tau(M, w)$ . If  $\models \tau(M, w) \rightarrow \alpha(M, w)$ , then also  $\mathfrak{M} \models \alpha(M, w)$ , i.e.,

$$\mathfrak{M} \models \exists x \exists y \left( \bigvee_{\langle q, \sigma \rangle \in X} (Q_q(x, y) \wedge S_\sigma(x, y)) \right).$$

As  $|\mathfrak{M}| = \mathbb{N}$ , there must be  $m, n \in \mathbb{N}$  so that  $\mathfrak{M} \models Q_q(\bar{m}, \bar{n}) \wedge S_\sigma(\bar{m}, \bar{n})$  for some  $q$  and  $\sigma$  such that  $\delta(q, \sigma)$  is undefined. By the definition of  $\mathfrak{M}$ , this means that  $M$  started on input  $w$  after  $n$  steps is in state  $q$  and reading symbol  $\sigma$ , and the transition function is undefined, i.e.,  $M$  has halted.  $\square$

## Photo Credits

## Bibliography