On strong fairness in UNITY

H.P.Gumm, D.Zhukov

Fachbereich Mathematik und Informatik
Philipps Universität Marburg
{gumm,shukov}@mathematik.uni-marburg.de

Abstract. In [6] Tsay and Bagrodia present a correct and complete proof rule for proving within UNITY statements of the form "$(true \mapsto p) \Rightarrow (true \mapsto q)$. Their result is obtained by specializing a proof rule due to Manna and Pnueli [5] and translating premises and conclusions into the UNITY framework. However, specializing the rule from [5] is not sufficient, details of the proof have to be invoked and modified.
Here we give a straightforward and selfcontained proof of a rule that is more general in several respects. Firstly, our transition systems may have an infinite number of transitions, and secondly, p and q may be any temporal properties, as long as p is "observable" and q is "bounded".
In particular, temporal properties such as $\Box\Diamond Enabled_i \Rightarrow \Box\Diamond Taken_i$, in which $Taken_i$ is not naturally a state property, can be dealt with. Our main tool is a predicate transformer "w(p,q)" that specializes to the well known "wlt(q)" for $p = true$.

1 Definitions

1.1 Transition systems

Let $G = (S, I, T)$ be a transition system, i.e. S is a nonempty set, $I \subseteq S$, and T a set of binary relations on S. Elements of S are called *states*, I is the set of *initial states* and each $t \in T$ is called a *transition*. We allow T to be countably infinite. For any $X \subseteq S$ and $t \in T$ we set $t(X) := \{s \in S \mid \exists x \in X.(x, s) \in t\}$. We assume that every transition is *left total*, that is for every $s \in S$ and $t \in T$ there exists an s' with $(s, s') \in t$. G, S, I, and T will remain fixed for the rest of this article.

1.2 Sequences, properties and temporal operators

If σ is any sequence of elements of S, we denote its i-th element by σ_i and its k-th rest by σ^k. Thus $\sigma = (\sigma_0, \sigma_1, \ldots)$ and $\sigma^k = (\sigma_k, \sigma_{k+1}, \ldots)$. Each initial segment $u = (\sigma_0, \ldots, \sigma_k)$ is called a *prefix* of σ. In this case we write $u \preceq \sigma$. Let S^* be the set of all finite and S^ω the set of all infinite sequences over S. Let $S^\infty = S^* \cup S^\omega$.

Given $U \subseteq S^*$ and $V \subseteq S^\infty$, $U \cdot V$ consists of all concatenations $u \cdot v$ with $u \in U$ and $v \in V$. S^k is the set of all sequences of length k over S. We identify S^1 with S.

A *state property* p is a subset of S and a *temporal property* P is a subset of S^ω. Although we do not require that properties be presented syntactically, we prefer to use the familiar logical connectives over the set theoretic operations.

Let $P \subseteq S^*$, and $Q \subseteq S^\omega$. The linear temporal connectives *Init*, $\circ$, $\Diamond$, and $\Box$ are defined as follows:

Definition 1 Temporal Operators.

$$\begin{aligned} Init(P) &= P \cdot S^\omega \\ \circ Q &= S \cdot Q \\ \Diamond Q &= S^* \cdot Q \\ \Box Q &= \bigcap_{n=0}^{\infty} S^n \cdot Q \end{aligned}$$

The operator "Init" is usually dropped, that is if we use some $P \subseteq S^*$ as a temporal property, we actually mean "$Init(P)$".

Definition 2 observable, safety, bounded. A temporal property P is called *observable* if there exists a subset $P_0 \subseteq S^*$ such that $P = P_0 \cdot S^\omega$. P is called *safety* if its complement is observable. We call P *bounded*, if for some k there exists $P_0 \subseteq S^k$ so that $P = P_0 \cdot S^\omega$.

The above notion of safety agrees with the one introduced and investigated by Alpern and Schneider in [1]. Note that a bounded property is an observable safety property. If S is finite, the converse is also true.

1.3 Paths, traces, weak fairness

A *path* of the transition system G is a sequence $\sigma \in S^\omega$ such that $(\sigma_i, \sigma_{i+1}) \in \bigcup T$ for all $i \in \omega$. σ is called *weak fair*, if for every $t \in T$ and every $i \in \omega$ there exists a $j \geq i$ with $(\sigma_j, \sigma_{j+1}) \in t$. In short: every transition of T is taken infinitely often. With S_T^ω we denote the set of all weak fair paths of $G = (S, I, T)$. If P is a temporal property and $\sigma \in S^\omega$ we sometimes say "σ *satisfies* P" for $\sigma \in P$.

A path α with $\alpha_0 \in I$ is called a *trace* of G. For a transition system G we write $G \models P$ and say "G *satisfies* P", if every weak fair trace of G satisfies P, that is if $I \cdot S^\omega \cap S_T^\omega \subseteq P$.

In the following we shall use the letters u, v, w for elements (words) of S^*, p, q for state properties, P, Q, R for subsets of S^* or of S^ω, σ, τ for paths and α, β, γ for traces of G. All paths and traces that we consider will be assumed to be weak fair with respect to T.

1.4 UNITY

UNITY is a methodology for the specification and verification of transition systems. In K.M. Chandy and J. Misra's original presentation [2], T consists of a finite set of conditional parallel assignments, thus, in particular, transitions are deterministic. UNITY logic is not quite a subset of temporal logic. Given state properties p and q, the following are UNITY properties together with their semantically equivalent temporal logic counterparts :

$$\begin{aligned} \textit{initially } p &:= \mathit{Init}(p) & (1)\\ \textit{invariant } p &:= \Box p & (2)\\ p \textit{ unless } q &:= \Box((p \wedge \neg q) \Rightarrow \circ(p \vee q)) & (3)\\ p \ \mapsto\ q &:= \Box(p \Rightarrow \Diamond q) & (4) \end{aligned}$$

The operator "$\mapsto$", pronounced *"leads to"*, is the main connective for expressing progress. Its proof theory is based on an operator *"ensures"* which describes how progress is achieved with a single transition:

$$p \textit{ ensures } q := (p \text{ unless } q) \wedge \exists t \in T.\ t(p \wedge \neg q) \subseteq q.$$

"p ensures q" is not a temporal property, since it is easy to come up with transition systems G and G' having the same weakly fair traces but different ensures-properties.

The above definition of the UNITY operators is purely extensional. In contrast to this, Chandy and Misra [2] introduce the UNITY operators via proof rules. The rules for "$\mapsto$" are :

$$\frac{p \text{ ensures } q}{p \mapsto q} \quad \frac{p \mapsto q, q \mapsto r}{p \mapsto r} \quad \frac{\forall_{k \in K} \cdot (p_k \mapsto q)}{(\exists_{k \in K} \cdot p_k) \mapsto q}$$

In [3] and [4] it has been shown that these rules are correct and complete with respect to the above extensional definition of "$\mapsto$". In particular, the statement "infinitely often p" ($\Box\Diamond p$) can be expressed in UNITY as "$\mathit{true} \mapsto\ p$".

The above definitions of UNITY properties "invariant", "unless" and "$\mapsto$", can straightforwardly be extended to the case where p and q are arbitrary temporal properties; "initially p" can be extended to the case where $p \subseteq S^*$. Thus P is observable iff $P = \textit{initially } P_0$ for some $P_0 \subseteq S^*$.

2 Rules for conditional progress

Conditional properties provide an extension of UNITY logic useful for describing properties of components within a given context. Y.-K. Tsay and R.L. Bagrodia argue in [6] that strong fairness can be expressed within UNITY using temporal properties of the form "(true $\mapsto$ p) $\Rightarrow$ (true $\mapsto$ q)" where p and q are state properties. The main result of their paper is a sound and complete rule for proving temporal properties of this form:

Theorem 3 Tsay, Bagrodia. *With some map M from S into a wellfounded partial order $(W, \preceq)$, the following is a sound and complete rule for proving statements of the form "(true $\mapsto p$) $\Rightarrow$ (true $\mapsto q$)" in UNITY :*

$$\frac{\begin{array}{c} M \preceq r \textit{ unless } q \\ p \wedge (M = r) \mapsto (M \prec r) \vee q \end{array}}{(\mathit{true} \mapsto p) \Rightarrow (\mathit{true} \mapsto q)}$$

Tsay and Bagrodia's proof invokes a sound and complete proof rule given by Manna and Pnueli in [5] for proving statements of the form "$\Box[(r \wedge \Box\Diamond p) \Rightarrow \Diamond q]$". When this rule is specialized to the case at hand, they show that all premises may be transformed into UNITY expressions.

Unfortunately though, applying Manna and Pnueli's rule is not enough. The argument in [6] requires to invoke and modify details of Manna and Pnueli's proof, thus making the paper not selfcontained.

Secondly, the type of temporal property commonly used to specify strong fairness for a transition t,

$$\Box\Diamond Enabled_t \Rightarrow \Box\Diamond Taken_t,$$

does not immediately fit the above framework, since $Taken_t$ is not a state property, but rather a property of consecutive pairs of states. In fact, written as a temporal property, $Taken_t = t \cdot S^\omega$.

Finally, Manna and Pnueli's proof on which Theorem 1 is based, works only for transition systems with finitely many transitions. We shall therefore generalize the above to the following:

Theorem 4. *Let P be observable and $Q = Q_0 \cdot S^\omega$ bounded with $Q_0 \subseteq S^k$. With some map M from S^k into some wellfounded partial order $(W, \preceq)$ the following rule is correct and complete:*

$$\frac{\begin{array}{c} M \preceq r \ \mathit{unless}\ q \\ P \wedge (M = r) \mapsto (M \prec r) \vee Q \end{array}}{\Box\Diamond P \Rightarrow \Box\Diamond Q}$$

As a special case we consider state properties $p_1, \ldots, p_n$ together with the condition "$\mathit{true} \ \mapsto p_1 \wedge \ldots \wedge \mathit{true} \ \mapsto p_n$". This is equivalent to $\Box\Diamond P$ where P is the observable property $P = p_1 \cdot S^* \cdot p_2 \cdot \ldots \cdot S^* \cdot p_n \cdot S^\omega$. A slight modification of the general proof is needed to yield the following corollary:

Corollary 5. *With a map $\tilde{M}$ from S into some wellfounded partial order $(\tilde{W}, \preceq)$ and a map $\xi : \tilde{W} \to \{1, \ldots, n\}$ the following rule is correct and complete:*

$$\frac{\begin{array}{c} \tilde{M} \preceq r \ \mathit{unless}\ q \\ p_{\xi(r)} \wedge (\tilde{M} = r) \mapsto (\tilde{M} \prec r) \vee q \end{array}}{(\mathit{true} \mapsto p_1 \wedge \ldots \wedge \mathit{true} \mapsto p_n) \Rightarrow (\mathit{true} \mapsto q)}$$

2.1 Weak temporal implication

The main tool in our proof is an operator $w(\_, \_)$ which is a weak form of a temporal implication.

Definition 6. Let $P \subseteq S^*$ and $Q \subseteq S^k$ then

$$w(P, Q) := \{u \in S^k | \forall \sigma \in S^\omega_T . \sigma \in \mathit{Init}(u) \cap \Diamond P \Rightarrow \sigma \in \Diamond Q\}.$$

Note that for $p = true$, $w(p, q)$ specializes to the well known *weakest-leads-to*, $wlt(q)$. Moreover, the operator $w(\_, \_)$ is monotone in the second and antitone in the first argument. The following properties will be of relevance in this note:

Lemma 7. *$w(P,Q)$ satisfies:*

(i) $w(P, Q) \supseteq Q$
(ii) $w(P, Q)$ *unless* Q
(iii) $P \wedge w(P, Q) \mapsto Q$

Proof: For (i), let $u \in Q$. If $\sigma \in Init(u)$, then $\sigma \in Q$. Hence $u \in w(P, Q)$.

For (ii), let $\sigma \models w(P, Q) \wedge \neg Q$, thus $(\sigma_0, \dots, \sigma_{k-1}) \in w(P, Q) - Q$. We need to show $\sigma^1 \models w(P, Q)$, i.e. $(\sigma_1, \dots, \sigma_k) \in w(P, Q)$. So let $\tau \in S_T^\omega$ be a path with $(\sigma_1, \dots, \sigma_k) \preceq \tau$ and $\tau \models \Diamond P$. Then $\sigma_0 \cdot \tau$ is also a path from S_T^ω, satisfying $\Diamond P$, hence $\sigma_0 \cdot \tau \models \Diamond Q$. But $(\sigma_0, \dots, \sigma_{k-1}) \preceq \sigma_0 \cdot \tau$, so $\sigma_0 \tau \not\models Q$, hence $\tau \models \Diamond Q$.

For (iii), suppose $\sigma \models P \wedge w(P, Q)$, then $u \preceq \sigma$ for some $u \in w(P, Q)$. Then $\sigma \models \Diamond P$, so by definition of $w(P, Q)$, $\sigma \models \Diamond Q$.

Lemma 8. *If $G \models \Box\Diamond P \Rightarrow \Box\Diamond Q$, then for every $R \supseteq Q$ with $w(P, R) = R$ we have $G \models \Box R$.*

Proof: Assume, $R \supseteq Q$ with $w(P, R) = R$ is given, but $G \not\models \Box R$. For any chosen map $\phi : \omega \to T$ we show how to construct a trace

$$\alpha = w_0 u_0 w_1 u_1 \dots$$

such that for all $i \geq 0$

1. $u_i \in S^k - R$
2. $u_i w_{i+1} u_{i+1}$ contains no subword from Q
3. $u_i w_{i+1}$ contains a subword from P
4. w_{i+1} contains a transition from $\phi(i + 1)$

From 4. and 3. it will follow that α can be constructed as a weak fair trace satisfying $\Box\Diamond P$. From 1. and 2. and the fact that $Q \subseteq R \subseteq S^k$ it follows that $u_0 w_1 u_1 w_2 \dots \models \Box\neg Q$, hence $\alpha \models \Diamond\Box\neg Q$, contradicting the assumption $G \models \Box\Diamond P \Rightarrow \Box\Diamond Q$.

Let us now begin constructing α. From the assumption $G \not\models \Box R$, we obtain a weak fair trace $w_0 u_0 \cdot \sigma$ with $u_0 \in S^k - R$.

Assume now that for some $n \geq 0$ we have already found a path

$$\sigma = u_0 w_1 u_1 \dots w_n u_n \cdot \tau$$

such that 1. through 4. are satisfied for $0 \leq i \leq n$. We shall show how to construct $w_{n+1} u_{n+1}$.

From $u_n \in S^k - R$, we get $u_n \in S^k - w(P, R)$, so we can find a weak fair path σ' with $u_n \preceq \sigma'$, $\sigma' \models \Diamond P$ and $\sigma' \models \Box\neg R$. This permits us to choose a prefix $v_{n+1} = u_n w_{n+1} \preceq \sigma'$ large enough so that

- v_{n+1} contains a subword $p_{n+1} \in P$
- w_{n+1} contains a transition from $\phi(n+1)$.

Let now u_{n+1} be the word consisting of the k subsequent letters of σ', i.e. such that $u_n w_{n+1} u_{n+1} \preceq \sigma'$. Then 1. - 3. follow from the inductive assumption and from the fact that $\sigma' \models \Box\neg R$ and from $R \supseteq Q$. 4. is part of the construction of w_{n+1}.

We note in passing, that the converse of this lemma is also true. To show this, consider

$$w^{\infty}(P,Q) := \{u \in S^k | \forall \sigma \in S_T^{\omega}.\sigma \in \mathit{Init}(u) \cap \Box\Diamond P \Rightarrow \sigma \in \Diamond Q\}.$$

It is easy to verify that $R = w^{\infty}(P,Q)$ is a fixed point of the map $w(P, \_)$ containing Q. From $G \models \Box R$ it follows $G \models \Box\Diamond P \Rightarrow \Box\Diamond Q$.

2.2 Measuring progress

The above fixed point of $w(P, \_)$ can also be constructed by a transfinite iteration:

$$\begin{aligned} M_0 &= Q \\ M_{\alpha+1} &= w(P, M_\alpha), \text{and} \\ M_\beta &= \bigcup_{\alpha \prec \beta} w(P, M_\alpha), \text{if } \beta \text{ is a limit ordinal.} \end{aligned}$$

We now turn to the proof of theorem 2. Correctness of the rule is easy and left to the reader. Let

$$\begin{aligned} W &= \{\alpha \in \mathit{Ord} | \forall \beta \prec \alpha. M_\alpha \neq M_\beta\} \\ M(u) &= \mathit{min}\{\alpha \in W | u \in M_\alpha\} \end{aligned}$$

Note that $M(u)$ will always be 0 or a successor ordinal. Assuming $G \models \Box\Diamond P \Rightarrow \Box\Diamond Q$, Lemma 2 yields that the above map $M : S^k \to \gamma$ is well defined on the *reachable part* of S^k, that is on all k-tuples u for which there exists a weak fair trace σ, containing u as a subword. For all other k-tuples of S^k, M may be defined arbitrarily, say 0. We have to show that for any ordinal $r \in W$ the premises of the rule in theorem 2 are true.

We use ordinal induction to show "$M \preceq r$ *unless* Q". The case $r = 0$ is trivial, since $M_0 = Q$.

Suppose the claim is true for all $\alpha \prec r$. If $r = \alpha + 1$ then $M_r = w(P, M_\alpha)$ and M_r *unless* M_α by lemma 1. Since $M_r \supseteq M_\alpha \supseteq Q$ and by induction hypothesis, we get M_r *unless* Q, that is $M \preceq r$ *unless* Q.

The premise "$P \wedge M \preceq r \mapsto M \prec r \vee Q$" is similarly shown by induction. $M_0 = Q$, so $P \wedge M \preceq 0 \mapsto Q$. If $r = \alpha + 1$ then $P \wedge M_r = P \wedge w(P, M_\alpha)$ and the statement follows from Lemma 2(iii).

Finally, we indicate how to modify M to yield the corollary. We have to measure the progress of the individual state properties p_i on those subsets of S where M is constant. For $s \in M_{\alpha+1} - M_\alpha$ we therefore define

$$\xi(s) := \mathit{max}\{j | s \in w(p_j \cdot S^* \cdot \ldots \cdot S^* \cdot p_n \cdot S^{\omega}, M_\alpha)\}.$$

Let $N = \{1, \ldots, n\}$. We consider $\tilde{W} = W \times N$ with the lexicographic order and define $\tilde{M}(s) = (M(s), \xi(s))$ and $\xi : \tilde{W} \to N$ as the second projection. With this it is straightforward to verify the corollary.

3 Conclusion

We have given a correct and complete rule for temporal properties of the form $\Box\Diamond P \Rightarrow \Box\Diamond Q$ when P and Q are temporal properties with P observable and Q bounded.

In comparison with a corresponding result by Tsay and Bagrodia for state properties p and q, our proof is selfcontained, and our results are more general in two ways: Firstly, we can deal with transition systems having an infinite number of transitions, and secondly, we can deal with more general types of temporal properties.

References

1. B. Alpern, F.B. Schneider, Defining Liveness, *Inform. Process. Lett.* 21 (1985) 181–185.
2. K.M. Chandy,J. Misra. *Parallel Program Design.* Addison–Wesley Co., Inc., Reading, Mass, 1988.
3. C.S. Jutla, E. Knapp, J.R. Rao, A predicate transformer approach to semantics of parallel programs, *Proc. 8th Annual ACM Symp. on Principles of Distributed Computing*, Edmonton, Alberta 1989.
4. J. Pachl. Three definitions of *leads-to* for UNITY. In *Notes on UNITY: 23:90.* Department of Computer Sciences, The University of Texas at Austin.
5. Z. Manna, A. Pnueli. Completing the temporal picture. *Theoretical Computer Science* 83 (1991) 97–130.
6. Y.-K- Tsay, R.L. Bagrodia. Deducing Fairness Properties in UNITY Logic – A New Completeness Result. *ACM Transactions on Programming Languages and Systems*17 (1995) 16–27.

This article was processed using the LaTeX macro package with LLNCS style