In this paper we investigate total correctness (termination and correctness simultaneously) in Nonstandard Dynamic Logic (NDL). Here we show that despite of the celebrated Kfoury-Park [5] result, termination is a first order notion if approached properly (e.g., via NDL).

In Definition 1 below we recall the famous Manna-Cooper $Q$-method for proving total correctness. Then we do the same things to Manna-Cooper total correctness method $\vdash_{Q}$ that were done in [1] to Floyd’s partial correctness method $\vdash_{F}$. Among others, we shall give an explicit characterization of the information content of $\vdash_{Q}$ as well as prove that NDL is strictly stronger than $\vdash_{Q}$ w.r.t. proving total correctness (that is, more programs can be proved totally correct by NDL than by $\vdash_{Q}$). The same results apply if we replace $\vdash_{Q}$ by Burstall’s method for total correctness (this is because Burstall’s method is very close to our version of $\vdash_{Q}$) as it will be demonstrated in the other paper.

Since these methods (Burstall’s and Manna-Cooper’s) are widely used and accepted to be strong enough for practical purposes we show indirectly that NDL is strong for practical purposes. Since by [1], NDL is also stronger than $\vdash_{F}$ we have evidence at our hand to disagree with those opinions who maintain that nonstandard time in NDL makes it too weak.

Just as is was the case with Floyd’s method in [1], we have to define $\vdash_{Q}$ more precisely than in the original publications. The first careful re-formulation of the Manna-Cooper $\vdash_{Q}$ method was given in Sec. 3.2 of [4] pp. 34-38. The Chang-Lee book [6] on program verification introduced $\vdash_{Q}$

*A detailed version of the present paper (with full proofs) is available from the author.*
in a spirit that is close to ours (and to that of [4]) but that definition is far from being precise enough for our purposes.

We use the notations of [1] and [2]. Recall the notion of a (one-sorted) similarity type from Definition 1 (i) of [1] or [2]. Recall that $X = \{x_i : i \in \omega\}$ is a set of variables. Below $Q^d_i$ is a relation symbol, for $i, k \in \omega$. Further, $(i \neq i_1 \land k = k_1) \Rightarrow Q^d_i \neq Q^d_{i_1}$.

**Definition 1.** (The Manna-Cooper method for proving termination, see 1b) of Theorem 4.3 of [3]). Let $d$ be a similarity type. Assume that $\text{dom } d_1 \cap \{Q^d_i : i, k \in \omega\}$.

(i) We define the new similarity type $dQ$ as follows: $dQ = d < d_0, d_1 \cup \{< Q^d_i, k > : i, k \in \omega\}$. I.e. $dQ$ is the similarity type $d$ extended with the new relation symbols $Q^d_i$, $i, k \in \omega$.

(ii) Let $p \in P_d$ (see §1 of [1] or [2]). We define $K(p) \in F^X_{dQ}$ as follows. Let $p = < (i_0 : u_0), \ldots, (i_n : \text{HALT}) >$. Recall from Convention 1 of [1] or [2] that $c = \min\{w \in \omega : (\forall v \geq w)[x_v \text{ does not occur in } p]\}$. Let $\tau = d < x_0, \ldots, x_{c-1} >$. Now $K(p) = d \wedge \{K_m(p) : m < n\}$ where

$$K_m(p) = d \begin{cases} \forall \tau \{Q^c_m(\tau) \rightarrow Q^c_{m+1}(x_0, \ldots, x_{w-1}, x_{w+1}, \ldots, x_{c-1})\} & \text{if } u_m = \text{"}x_w \leftarrow \tau\text{"} \\ \forall \tau \{Q^c_m(\tau) \land \forall \chi \rightarrow Q^c_{m+1}(\chi)\} & \text{if } u_m = \text{"}IF \chi \text{ GOTO } v\text{"} \\ \end{cases}$$

(iii) Let $g$ be a similarity type. We say that $g$ is a finite sub-similarity type of $d$ (in symbols $g \subseteq_d d$) if $g_1 \subseteq d_1, g_0 = d_0 \cap \text{dom } g_1$ and $|g_1| < \omega$. I.e. $g$ consists of finitely many symbols of $d$ (with the same arities and the same division between function and relation symbols as in $d$).

(iv) Assume $g \subseteq_d d$. Let $v \in X$ and $\varphi \in F_{dQ}$. Then $\text{ind}(\varphi, g, v) = d \{ \land \{ \forall v_1 \ldots v_k [((\varphi(v_1) \land \ldots \land \varphi(v_k)) \rightarrow \varphi(f(v_1 \ldots v_k))] : f \in g_0, k = g_1(f) - 1 \rightarrow \forall \varphi) \} \}$ where $v_1, \ldots, v_m$ are the first $m = \max\{g_1(f) : f \in g_0\}$ variables in $X$ not occurring in $\varphi$ and $\varphi(\tau) = d \varphi(\tau/v) = d \exists u (u = \tau \land \exists v (v = u \land \varphi))$ where $u \in X$ does not occur in $\varphi \land v = \tau$.

(v) Let $\text{Th} \subseteq F_d, \varphi, \psi \in F_d$ and $p \in P_d$. Let $g \subseteq_d d$ and assume $\text{Th} \vdash \{\text{ind}(\varphi, g, v) : \varphi \in F_d, v \in X\}$.

Then we define
\[ Th \vdash Q \varphi \rightarrow \Delta(p, \psi) \Leftrightarrow Q \bigcup \{ \text{ind} (\varphi, g, v) : g \in F_d, v \in X \} \vdash [Q_0(\varphi) \land \varphi \land K(p)] \rightarrow \exists !\varphi (Q_\varphi (\varphi) \land \psi). \]

END OF DEFINITION 1. Next we fix some axiom systems in the underlying language \( L_d \) of \( NDL \) as introduced in [1,2].

From now on, let \( d \) be any similarity type, let \( Th \subseteq F_d, \varphi, \psi \in F_d, p \in P_d \) and \( g \leq \omega d \) (cf. Definition 1(ii) above).

DEFINITION 2. (cf. [1], [2]).

\[ DIA_g \triangleq \{ \text{ind} (\varphi, g, v) : \varphi \in F_d, v \in X \} \cup \text{Lax}, \text{where Lax} \triangleq \{ (j \neq k) : j \text{ and } k \text{ are two different elements of Lab}; \text{cf. the definition of DLA in [1] p. 51.} \]

\[ Ex^0 = \{ \exists y_0 y_0 = y_0, \forall x_0 \forall y_0 \forall z_0 \exists y_1 \forall z_1 ([z_1 \leq z_0 \rightarrow \text{ext}(y_1, z_1) = \text{ext}(y_0, z_1)] \land \neg z_1 \leq z_0 \rightarrow \text{ext}(y_1, z_1) = x_0) \}. \]

\[ Ex^b = \{ \forall z_0 ! x_0 \varphi \rightarrow \forall z_1 \exists y_0 \forall z_0 ([z_0 \leq z_1 \rightarrow \varphi(x_0, \text{ext}(y_0, z_0))] \land \neg z_0 \leq z_1 \rightarrow \text{ext}(y_0, z_0) = \text{ext}(y_0, z_1)) : \varphi \in F_d \text{ and } y_0, z_0 \text{ do not occur in } \varphi \}. \]

\[ Ex = \{ \forall z_0 ! x_0 \varphi \rightarrow \exists y_0 \forall z_0 \varphi(x_0, \text{ext}(y_0, z_0)) : \varphi \in F_d \text{ and } y_0 \text{ does not occur in } \varphi \}, \text{see Definition 16 of [1] and Definition 17 of [2] (the latter is slightly different).} \]

\[ Tpo = \{ \leq \text{ is a partial ordering with 0 as a least element} \} \cup \{ (z_1 \leq z_0 + 1 \land z_1 \neq z_0 + 1) \iff z_1 \leq z_0, z_1 \leq z_0 \rightarrow z_1 + 1 \leq z_0 + 1, z_0 \neq 0 \rightarrow \exists z_1 z_0 = z_1 + 1 \}. \]

\[ PA_t \] denotes the set of Peano axioms for the similarity type \( t \), see Definition 16 of [2] (there \( PA_t \) was denoted by \( Tpa \)) and Definition 14 of [1] (there \( PA_t \) was denoted by \( PA \)).

Assume that \( d \) contains a disjoint copy \( d' \) of \( t \) (see Definition 6 of [1]). Then

\[ PA_d \] denotes the set of Peano axioms for the similarity type \( d \) together with \( \{ \text{ind} (\varphi, x) : \varphi \in F_d, x \text{ does not occur in } \varphi \} \), see Definition 19 of [1] p. 96.

\[ Ia = \{ \text{ind} (\varphi, z) : \varphi \in F_d, z \in Z \} \cup \text{Lax}, \text{where ind} (\varphi, z) = ([\varphi(0) \land \forall z (\varphi \rightarrow \varphi(scz))] \rightarrow \forall z \varphi) \}, \text{see Definition 14 of [2] or [1]. Note that ind} (\varphi, z) \) and \( Ia \) were denoted by \( \varphi^+_z \) and \( IA^+ \) respectively in [1].
Total Correctness in Nonstandard Dynamic Logic

END OF DEFINITION 2. Theorem 1, 2 below say that the axioms $DIA_g \cup Ex^0 \cup Tpo$ of NDL are strictly stronger (w.r.t. total correctness) than $\vdash^Q$.

Let $\vdash^d \forall x_0 x_0 = x_0$.

**Theorem 1.** $Th \vdash^Q g (\varphi \rightarrow \Diamond (p, \psi)) \Rightarrow Th \cup DIA_g \cup Ex^0 \cup Tpo \vdash^N (\varphi \rightarrow \Diamond (p, \psi))$.

**Theorem 2.** There are $d, g \leq_\omega d$, $Th \subseteq F_d$ and $p \in P_d$ such that $Th \vdash^Q g \Diamond (p, \uparrow) \neq Th \cup DIA_g \cup Ex^0 \cup Tpo \vdash^N \Diamond (p, \uparrow)$.

**Remark.** There are $d, g \leq_\omega d$, $Th \subseteq F_d$ and a quantifier-free $\varphi \in F_d$ such that $Th \cup DIA_g \nvdash \varphi$ and $Th \cup DIA_g \cup Ex^0 \cup Tpo \vdash \varphi$.

**Theorem 3 below is a characterization of the reasoning power of the Manna-Cooper $\vdash^Q$ method (w.r.t. total correctness).**

**Theorem 3.** Assume $PA_d \subseteq Th$. Let $g$ consist of $C$ and sc od $d$. Then $Th \vdash^Q g (\varphi \rightarrow \Diamond (p, \psi)) \Leftrightarrow Th \cup DIA_g \cup Ex^0 \cup Tpo \vdash^N (\varphi \rightarrow \Diamond (p, \psi)) \Leftrightarrow Th \cup DIA_g \cup Ex^b \cup PA_t \cup Ia \vdash^N (\varphi \rightarrow \Diamond (p, \psi))$.

In the above characterization $Ex^b$ cannot be replaced with $Ex$ because:

**Theorem 4.** There are $d, g \leq_\omega d$, $PA_d \subseteq Th \subseteq F_d$ and $p \in P_d$ such that $Th \vdash^Q g \Diamond (p, \uparrow) \neq Th \cup DIA_g \cup Ex \cup PA_t \cup Ia \vdash^N \Diamond (p, \uparrow)$.

References


[4] H. Andréka, K. Balogh, K. Lábadi, I. Németi, P. Tóth, Plans to improve our semi-automatic program verifier system (in Hungarian), Re-


*Mathematical Institute of the*  
*Hungarian Academy of Sciences*  
*Budapest 1376, PF 428, Hungary*