Conscriptions: a new relational model for sequential computations

Steve Dunne

School of Computing
University of Teesside, UK

Hoare-He Designs

$$p \vdash r \;\widehat{=}\; ok \wedge p \Rightarrow r \wedge ok'$$

	$\neg\, ok'$	ok'
$\neg\, ok$	T	T
ok	$\neg\, p$	$\neg\, p \vee r$

Extreme Hoare-He designs

$$\begin{aligned}
\mathbf{skip}_{\mathsf{d}} &\mathrel{\widehat{=}} \mathrm{true} \vdash v' = v \\
\mathbf{abort}_{\mathsf{d}} &\mathrel{\widehat{=}} \mathrm{false} \vdash \mathrm{true} \\
\mathbf{magic}_{\mathsf{d}} &\mathrel{\widehat{=}} \mathrm{true} \vdash \mathrm{false} \\
\mathbf{chaos}_{\mathsf{d}} &\mathrel{\widehat{=}} \mathrm{true} \vdash \mathrm{true}
\end{aligned}$$

Sequential Composition of Designs

	$\neg\, ok'$	ok'
$\neg\, ok$	T	T
ok	$\neg\, p$	$\neg\, p \vee r$

	$\neg\, ok'$	ok'
$\neg\, ok$	T	T
ok	$\neg\, q$	$\neg\, q \vee s$

$(p \vdash r)\,;(q \vdash s)$

	$\neg\, ok'$	ok'
$\neg\, ok$	$(\mathrm{T}\,;\mathrm{T}) \vee (\mathrm{T}\,;\neg\, q)$	$(\mathrm{T}\,;\mathrm{T}) \vee (\mathrm{T}\,;\neg\, q \vee s)$
ok	$(\neg\, p\,;\mathrm{T}) \vee (\neg\, p \vee r\,;\neg\, q)$	$(\neg\, p\,;\mathrm{T}) \vee (\neg\, p \vee r\,;\neg\, q \vee s)$

which simplifies to

	$\neg\, ok'$	ok'
$\neg\, ok$	T	T
ok	$(\neg\, p\,;\mathrm{T}) \vee (r\,;\neg\, q)$	$(\neg\, p\,;\mathrm{T}) \vee (r\,;\neg\, q) \vee (r\,;s)$

which is the matrix representation of the design

$$\neg\,(\neg\, p\,;\mathrm{T}) \wedge \neg\,(r\,;\neg\, q) \quad \vdash \quad (r\,;s)$$

Skip left-unit property for designs

$$\begin{aligned}
& \mathbf{skip}_{\mathrm{d}} \,;\, (p \vdash r) \\
= \quad & (\mathrm{true} \vdash v' = v) \,;\, (p \vdash r) \\
= \quad & \neg\, (\neg\, \mathrm{true} \,;\, \mathrm{T}) \wedge \neg\, (v' = v \,;\, \neg\, p) \;\vdash\; (v' = v \,;\, r) \\
= \quad & (\mathrm{true} \wedge p) \;\vdash\; r \\
& p \vdash r
\end{aligned}$$

Skip right-unit property for designs

$$
\begin{aligned}
& (p \vdash r)\,;\, \mathbf{skip}_{\mathrm{d}} \\
= \quad & (p \vdash r)\,;\, (\mathrm{true} \vdash v' = v) \\
= \quad & \neg\,(\neg\, p\,;\, \mathrm{T}) \wedge \neg\,(r\,;\, \neg\, \mathrm{true}) \;\vdash\; (r\,;\, v' = v) \\
= \quad & \neg\,(\neg\, p\,;\, \mathrm{T}) \wedge \neg\,(r\,;\, \mathrm{false}) \;\vdash\; r \\
= \quad & \neg\,(\neg\, p\,;\, \mathrm{T}) \wedge \neg\, \mathrm{false} \;\vdash\; r \\
= \quad & \neg\,(\neg\, p\,;\, \mathrm{T}) \wedge \mathrm{true} \;\vdash\; r \\
= \quad & \neg\,(\neg\, p\,;\, \mathrm{T}) \;\vdash\; r
\end{aligned}
$$

So $\mathbf{skip}_{\mathrm{d}}$ is a right unit of sequential composition only for designs $p \vdash r$ where $\neg\,(\neg\, p\,;\, \mathrm{T}) = p$, which is equivalent to requiring that $(p\,;\, \mathrm{T}) = p$.

Normal Designs

We call designs which do satisfy the skip right-unit law for sequential composition **normal designs**.

A homogeneous binary relation A with input alphabet $\{v, ok\}$ is a normal design if and only if it satisfies

$$\mathbf{skip}_{\mathsf{d}} \,;\, A \quad = \quad A \quad = \quad A \,;\, \mathbf{skip}_{\mathsf{d}}$$

and

$$\mathbf{abort}_{\mathsf{d}} \,;\, A \quad = \quad \mathbf{abort}_{\mathsf{d}}$$

and in that case we have that

$$A \quad = \quad \neg\, (\neg\, A_{\mathsf{tf}} \,;\, \mathrm{T}) \vdash A_{\mathsf{tt}}$$

where A_{tf} is $A[\mathrm{true}, \mathrm{false}/ok, ok']$ and A_{tt} is $A[\mathrm{true}, \mathrm{true}/ok, ok']$.

Prescriptions

$$p \vdash r \;\widehat{=}\; (ok \wedge p \Rightarrow ok') \wedge (ok' \Rightarrow r \wedge ok)$$

	$\neg\, ok'$	ok'
$\neg\, ok$	T	F
ok	$\neg\, p$	r

Extreme Prescriptions

$$\begin{aligned}
\mathbf{skip}_{\mathsf{p}} &\mathrel{\widehat{=}} \mathrm{true} \Vdash v' = v \\
\mathbf{abort}_{\mathsf{p}} &\mathrel{\widehat{=}} \mathrm{false} \Vdash \mathrm{false} \\
\mathbf{anarchy}_{\mathsf{p}} &\mathrel{\widehat{=}} \mathrm{false} \Vdash \mathrm{true} \\
\mathbf{magic}_{\mathsf{p}} &\mathrel{\widehat{=}} \mathrm{true} \Vdash \mathrm{false} \\
\mathbf{chaos}_{\mathsf{p}} &\mathrel{\widehat{=}} \mathrm{true} \Vdash \mathrm{true}
\end{aligned}$$

Sequential Composition of Prescriptions

	$\neg\, ok'$	ok'
$\neg\, ok$	T	F
ok	$\neg\, p$	r

	$\neg\, ok'$	ok'
$\neg\, ok$	T	F
ok	$\neg\, q$	s

$(p \Rightarrow r)\,;\,(q \Rightarrow s)$

	$\neg\, ok'$	ok'
$\neg\, ok$	$(\mathrm{T}\,;\,\mathrm{T}) \vee (\mathrm{F}\,;\,\neg\, q)$	$(\mathrm{T}\,;\,\mathrm{F}) \vee (\mathrm{F}\,;\,s)$
ok	$(\neg\, p\,;\,\mathrm{T}) \vee (r\,;\,\neg\, q)$	$(\neg\, p\,;\,\mathrm{F}) \vee (r\,;\,s)$

which simplifies to

	$\neg\, ok'$	ok'
$\neg\, ok$	T	F
ok	$(\neg\, p \,;\, \mathrm{T}) \vee (r \,;\, \neg\, q)$	$(r \,;\, s)$

which is the matrix representation of the prescription

$$\neg\,(\neg\, p \,;\, \mathrm{T}) \wedge \neg\,(r \,;\, \neg\, q) \;\Vdash\; (r \,;\, s)$$

Algebraic Characterisation of Prescriptions

A homogeneous binary relation A with input alphabet $\{v, ok\}$ is a prescription if and only if it satisfies both

$$\mathbf{skip}_{\mathsf{p}} \,;\, A \quad = \quad A$$

and

$$\mathbf{abort}_{\mathsf{p}} \,;\, A \quad = \quad \mathbf{abort}_{\mathsf{p}}$$

and in that case we have that

$$A \quad = \quad \neg\, A_{\mathsf{tf}} \Vdash A_{\mathsf{tt}}$$

where A_{tf} is $A[\mathrm{true}, \mathrm{false}/ok, ok']$ and A_{tt} is $A[\mathrm{true}, \mathrm{true}/ok, ok']$.

Normal Prescriptions

We call prescriptions which do satisfy the skip right-unit law for sequential composition **normal prescriptions**.

A homogeneous binary relation A with input alphabet $\{v, ok\}$ is a normal prescription if and only if it satisfies

$$\mathbf{skip}_{\mathsf{p}} \,;\, A \quad = \quad A \quad = \quad A \,;\, \mathbf{skip}_{\mathsf{p}}$$

and

$$\mathbf{abort}_{\mathsf{p}} \,;\, A \quad = \quad \mathbf{abort}_{\mathsf{p}}$$

and in that case we have that

$$A \quad = \quad \neg\,(\neg\, A_{\mathsf{tf}} \,;\, \mathrm{T}) \Vdash A_{\mathsf{tt}}$$

where A_{tf} is $A[\mathrm{true}, \mathrm{false}/ok, ok']$ and A_{tt} is $A[\mathrm{true}, \mathrm{true}/ok, ok']$.

Conscriptions

$$p \nVdash r \quad \widehat{=} \quad (ok \wedge p \Rightarrow ok') \wedge (ok' \Rightarrow r \wedge ok) \wedge (\neg\, ok \Rightarrow v' = v)$$

	$\neg\, ok'$	ok'
$\neg\, ok$	$v' = v$	F
ok	$\neg\, p$	r

Extreme Conscriptions

$$\begin{aligned}
\mathbf{skip}_c &\mathrel{\widehat{=}} \text{true} \Mapsto v' = v \\
\mathbf{abort}_c &\mathrel{\widehat{=}} \text{false} \Mapsto \text{false} \\
\mathbf{anarchy}_c &\mathrel{\widehat{=}} \text{false} \Mapsto \text{true} \\
\mathbf{magic}_c &\mathrel{\widehat{=}} \text{true} \Mapsto \text{false} \\
\mathbf{chaos}_c &\mathrel{\widehat{=}} \text{true} \Mapsto \text{true}
\end{aligned}$$

Sequential Composition of Conscriptions

	$\neg\ ok'$	ok'
$\neg\ ok$	$v' = v$	F
ok	$\neg\ p$	r

	$\neg\ ok'$	ok'
$\neg\ ok$	$v' = v$	F
ok	$\neg\ q$	s

$(p \Longmapsto r) ; (q \Longmapsto s)$ where I_v stands for $v' = v$

	$\neg\ ok'$	ok'
$\neg\ ok$	$(\mathrm{I}_v ; \mathrm{I}_v) \vee (\mathrm{F} ; \neg\ \mathrm{q})$	$(\mathrm{I}_v ; \mathrm{F}) \vee (\mathrm{F} ; \mathrm{s})$
ok	$(\neg\ p ; \mathrm{I}_v) \vee (\mathrm{r} ; \neg\ \mathrm{q})$	$(\neg\ p ; \mathrm{F}) \vee (r ; s)$

which simplifies to

	$\neg\ ok'$	ok'
$\neg\ ok$	$v' = v$	F
ok	$\neg\ p \vee (r\ ;\neg\ q)$	$(r\ ;s)$

which is the matrix representation of the conscription

$$p \wedge \neg\ (r\ ;\neg\ q) \ \nVdash\ (r\ ;s)$$

Algebraic Characterisation of Conscriptions

A homogeneous binary relation A with input alphabet $\{v, ok\}$ is a conscription if and only if it satisfies

$$\mathbf{abort_c} \,;\, A \quad = \quad \mathbf{abort_c}$$

and in that case we have that

$$A \quad = \quad \neg\, A_{\mathsf{tf}} \leftthreetimes A_{\mathsf{tt}}$$

where A_{tf} is $A[\mathrm{true}, \mathrm{false}/ok, ok']$ and A_{tt} is $A[\mathrm{true}, \mathrm{true}/ok, ok']$.

Since $\mathbf{skip}_c$ is $\mathrm{true} \Rightarrow v' = v$, its matrix representation is

	$\neg\, ok'$	ok'
$\neg\, ok$	$v' = v$	F
ok	F	$v' = v$

which is clearly both a left and right unit of matrix multiplication.

Hence every conscription is **normal**, in the sense that $\mathbf{skip}_c$ is both a left and a right unit of sequential composition for all conscriptions.

$$\mathbf{skip}_c \,;\, A \quad = \quad A \quad = \quad A \,;\, \mathbf{skip}_c$$

Extended models

Use a second boolean auxiliary variable *term* in addition to *ok* to distinguish between non-termination and abortion, where *term* is only significant when *ok* is true.

Extended designs

$$p \vdash_X r \quad \widehat{=} \quad (ok \wedge term \wedge p \Rightarrow r \wedge ok') \wedge (term' \Rightarrow term) \\ \wedge (\neg\, term \Rightarrow ok) \wedge (\neg\, term' \Rightarrow ok') \ .$$

where p is of the form $p(v)$, and r is of the form $r(v, v', term')$ such that $r[\mathrm{false}/term']$ does not constrain v' when p holds.

	$\neg\, ok' \wedge term$	$ok' \wedge \neg\, term'$	$ok' \wedge term'$
$\neg\, ok \wedge term$	T	T	T
$ok \wedge \neg\, term$	F	T	F
$ok \wedge term$	$\neg\, p$	$\neg\, p \vee r_{\mathsf{f}}$	$\neg\, p \vee r_{\mathsf{t}}$

where r_{f} is $r[\mathrm{false}/term']$ and r_{t} is $r[\mathrm{true}/term']$.

Extended Conscriptions

$$p \Vdash_X r \quad \widehat{=} \quad (ok \wedge term \wedge p \Rightarrow ok') \wedge (ok' \wedge term \Rightarrow r \wedge ok) \\ \wedge (term' \Rightarrow term) \wedge (\neg\, term \Rightarrow ok) \wedge (\neg\, term' \Rightarrow ok') \\ \wedge (\neg\, ok \Rightarrow v' = v \wedge term = term')$$

where p is of the form $p(v, v')$, and r is of the form $r(v, v', term')$ such that $r[\mathrm{false}/term']$ does not constrain v'.

	$\neg\, ok' \wedge term$	$ok' \wedge \neg\, term'$	$ok' \wedge term'$
$\neg\, ok \wedge term$	$v' = v$	F	F
$ok \wedge \neg\, term$	F	T	F
$ok \wedge term$	$\neg\, p$	r_f	r_t

where r_f is $r[\mathrm{false}/term']$ and r_t is $r[\mathrm{true}/term']$.

Extreme Extended Conscriptions

$$
\begin{aligned}
\mathbf{skip}_{xc} &\ \widehat{=}\ \ \text{true} \Vvdash_X v' = v \land \mathit{term}' \\
\mathbf{abort}_{xc} &\ \widehat{=}\ \ \text{false} \Vvdash_X \text{false} \\
\mathbf{anarchy}_{xc} &\ \widehat{=}\ \ \text{false} \Vvdash_X \text{true} \\
\mathbf{magic}_{xc} &\ \widehat{=}\ \ \text{true} \Vvdash_X \text{false} \\
\mathbf{chaos}_{xc} &\ \widehat{=}\ \ \text{true} \Vvdash_X \text{true} \\
\mathbf{terminate}_{xc} &\ \widehat{=}\ \ \text{true} \Vvdash_X \mathit{term}' \\
\mathbf{forever}_{xc} &\ \widehat{=}\ \ \text{true} \Vvdash_X \neg\, \mathit{term}' \\
\mathbf{mortal}_{xc} &\ \widehat{=}\ \ \text{false} \Vvdash_X \mathit{term}' \\
\mathbf{noterm}_{xc} &\ \widehat{=}\ \ \text{false} \Vvdash_X \neg\, \mathit{term}' \\
\mathbf{bone\text{-}idle}_{xc} &\ \widehat{=}\ \ \text{true} \Vvdash_X \mathit{term}' \Rightarrow v' = v
\end{aligned}
$$

Sequential Composition of Extended Conscriptions

$(p \nparallel_X r) \,;\, (q \nparallel_X s)$

	$\neg\, ok' \wedge term$	$ok' \wedge \neg\, term'$	$ok' \wedge term'$
$\neg\, ok \wedge term$	$(\mathrm{I}_v \,;\, \mathrm{I}_v)$ $\vee\ (\mathrm{F} \,;\, \mathrm{F})$ $\vee\ (\mathrm{F} \,;\, \neg\, q)$	$(\mathrm{I}_v \,;\, \mathrm{F})$ $\vee\ (\mathrm{F} \,;\, \mathrm{T})$ $\vee\ (\mathrm{F} \,;\, s_\mathrm{f})$	$(\mathrm{I}_v \,;\, \mathrm{F})$ $\vee\ (\mathrm{F} \,;\, \mathrm{F})$ $\vee\ (\mathrm{F} \,;\, s_\mathrm{t})$
$ok \wedge \neg\, term$	$(\mathrm{F} \,;\, \mathrm{I}_v)$ $\vee\ (\mathrm{T} \,;\, \mathrm{F})$ $\vee\ (\mathrm{F} \,;\, \neg\, q)$	$(\mathrm{F} \,;\, \mathrm{F})$ $\vee\ (\mathrm{T} \,;\, \mathrm{T})$ $\vee\ (\mathrm{F} \,;\, s_\mathrm{f})$	$(\mathrm{F} \,;\, \mathrm{F})$ $\vee\ (\mathrm{T} \,;\, \mathrm{F})$ $\vee\ (\mathrm{F} \,;\, s_\mathrm{t})$
$ok \wedge term$	$(\neg\, p \,;\, \mathrm{I}_v)$ $\vee\ (r_\mathrm{f} \,;\, \mathrm{F})$ $\vee\ (r_\mathrm{t} \,;\, \neg\, q)$	$(\neg\, p \,;\, \mathrm{F})$ $\vee\ (r_\mathrm{f} \,;\, \mathrm{T})$ $\vee\ (r_\mathrm{t} \,;\, s_\mathrm{f})$	$(\neg\, p \,;\, \mathrm{F})$ $\vee\ (r_\mathrm{f} \,;\, \mathrm{F})$ $\vee\ (r_\mathrm{t} \,;\, s_\mathrm{t})$

which simplifies to

	$\neg\, ok' \wedge term$	$ok' \wedge \neg\, term'$	$ok' \wedge term'$
$\neg\, ok \wedge term$	$v' = v$	F	F
$ok \wedge \neg\, term$	F	T	F
$ok \wedge term$	$\neg\, p \vee (r_{\mathrm{t}} \,;\, \neg\, q)$	$r_{\mathrm{f}} \vee (r_{\mathrm{t}} \,;\, s_{\mathrm{f}})$	$r_{\mathrm{t}} \,;\, s_{\mathrm{t}}$

which, since $(r_{\mathrm{t}} \,;\, s_{\mathrm{f}}) = (r_{\mathrm{t}} \,;\, s)_{\mathrm{f}}$ and $(r_{\mathrm{t}} \,;\, s_{\mathrm{t}}) = (r_{\mathrm{t}} \,;\, s)_{\mathrm{t}}$, is a matrix representation of the extended conscription

$$p \wedge \neg\, (r_{\mathrm{t}} \,;\, \neg\, q) \;\; \Vdash\!\!-_{X} \;\; r_{\mathrm{f}} \vee (r_{\mathrm{t}} \,;\, s)$$

Timed Models

- Refine the extended models by distinguishing between different finite times as well as infinite time.
- Auxiliary variable τ recording the current time replaces *term*.
- The domain of time values can be either natural numbers or real numbers, in each case supplemented by infinity (∞) to represent non-termination.

Timed Designs

$$p \vdash_T r \quad \widehat{=} \quad (ok \wedge \tau < \infty \wedge p \Rightarrow ok' \wedge r) \wedge (\tau \leq \tau') \\ \wedge (\tau = \infty \Rightarrow ok) \wedge (\tau' = \infty \Rightarrow ok')$$

where p is of the form $p(v, \tau, \tau')$, and r is of the form $r(v, v', \tau, \tau')$.

Furthermore, p and r must satisfy these conditions:

$$\tau \leq \tau'' < \tau' \wedge p \Rightarrow p[\tau''/\tau']$$

$$\tau \neq \infty \wedge p \wedge \tau' = \infty \Rightarrow (r \Leftrightarrow \forall\, v' \,.\, r)$$

Timed Conscriptions

$$p \Vdash_{\mathrm{T}} r \quad \widehat{=} \quad (ok \wedge \tau < \infty \wedge p \;\Rightarrow\; ok') \wedge (ok' \wedge \tau < \infty \;\Rightarrow\; r \wedge ok)$$
$$\wedge\, (\tau = \infty \;\Rightarrow\; ok) \wedge (\tau' = \infty \;\Rightarrow\; ok') \wedge (\tau \leq \tau')$$
$$\wedge\, (\neg\, ok \;\Rightarrow\; v = v' \wedge \tau = \tau')$$

where p is of the form $p(v, \tau, \tau')$, and r is of the form $r(v, v', \tau, \tau')$.

Furthermore, p and r must satisfy the condition

$$\tau < \tau' = \infty \;\Rightarrow\; (r \Leftrightarrow \forall\, v' \,.\, r)$$

$p \Vdash\!\!\!\vdash_{\mathrm{T}} r$

	$\neg\, ok' \wedge \tau' < \infty$	$ok' \wedge \tau' = \infty$	$ok' \wedge \tau' < \infty$
$\neg\, ok \wedge \tau < \infty$	$v' = v \wedge$ $\tau = \tau' < \infty$	F	F
$ok \wedge \tau = \infty$	F	$\tau = \tau' = \infty$	F
$ok \wedge \tau < \infty$	$\neg\, p \wedge$ $\tau \leq \tau' < \infty$	$r \wedge$ $\tau < \tau' = \infty$	$r \wedge$ $\tau \leq \tau' < \infty$

Extreme Timed Conscriptions

$$
\begin{aligned}
\textbf{skip}_{\mathrm{tc}} &\mathrel{\widehat{=}} \quad \mathrm{true} \;\; \Vdash_{\mathrm{T}} \;\; v = v' \wedge \tau = \tau' \\
\textbf{idle}_{\mathrm{tc}} &\mathrel{\widehat{=}} \quad \mathrm{true} \;\; \Vdash_{\mathrm{T}} \;\; v = v' \wedge \tau' < \infty \\
\textbf{bone-idle}_{\mathrm{tc}} &\mathrel{\widehat{=}} \quad \mathrm{true} \;\; \Vdash_{\mathrm{T}} \;\; \tau' < \infty \Rightarrow v = v' \\
\textbf{eagerabort}_{\mathrm{tc}} &\mathrel{\widehat{=}} \quad \tau < \tau' \;\; \Vdash_{\mathrm{T}} \;\; \mathrm{false} \\
\textbf{lazyabort}_{\mathrm{tc}} &\mathrel{\widehat{=}} \quad \mathrm{false} \;\; \Vdash_{\mathrm{T}} \;\; \mathrm{false} \\
\textbf{anarchy}_{\mathrm{tc}} &\mathrel{\widehat{=}} \quad \mathrm{false} \;\; \Vdash_{\mathrm{T}} \;\; \mathrm{true} \\
\textbf{magic}_{\mathrm{tc}} &\mathrel{\widehat{=}} \quad \mathrm{true} \;\; \Vdash_{\mathrm{T}} \;\; \mathrm{false} \\
\textbf{chaos}_{\mathrm{tc}} &\mathrel{\widehat{=}} \quad \mathrm{true} \;\; \Vdash_{\mathrm{T}} \;\; \mathrm{true} \\
\textbf{terminate}_{\mathrm{tc}} &\mathrel{\widehat{=}} \quad \mathrm{true} \;\; \Vdash_{\mathrm{T}} \;\; \tau' < \infty \\
\textbf{forever}_{\mathrm{tc}} &\mathrel{\widehat{=}} \quad \mathrm{true} \;\; \Vdash_{\mathrm{T}} \;\; \tau' = \infty \\
\textbf{mortal}_{\mathrm{tc}} &\mathrel{\widehat{=}} \quad \mathrm{false} \;\; \Vdash_{\mathrm{T}} \;\; \tau' < \infty \\
\textbf{noterm}_{\mathrm{tc}} &\mathrel{\widehat{=}} \quad \mathrm{false} \;\; \Vdash_{\mathrm{T}} \;\; \tau' = \infty \; .
\end{aligned}
$$

Sequential Composition of Timed Conscriptions

Interval Composition

For homogeneous binary relations A and B with a common input alphabet which includes τ, define their **interval composition** as

$$A \;;_\tau\; B \quad \widehat{=} \quad A \wedge \tau \leq \tau' < \infty \;;\; B \wedge \tau \leq \tau'$$

Then for timed conscriptions $p \nVdash_X r$ and $q \nVdash_X s$ over the same alphabet

$$(p \nVdash_{\mathrm{T}} r) \,;\, (q \nVdash_{\mathrm{T}} s) \quad =$$

$$p \wedge \neg\,(r \;;_\tau \neg\, q) \quad \nVdash_{\mathrm{T}} \quad (r \wedge \tau' = \infty) \vee (r \;;_\tau\; s)$$

Expressivity of timed conscriptions *versus* timed designs

The timed design

$$\tau' \leq \tau + 5 \vdash_T \text{false}$$

runs for at least 5 time units before becoming anarchic.

But what about

$$\tau' > \tau + 5 \vdash_T \text{false} \ ?$$

In fact this is not a healthy timed design, but we can instead write the timed conscription

$$\tau' > \tau + 5 \nvdash_{\mathrm{T}} \text{false}$$

which **must** abort within no more than 5 time units of starting.

Similarly, the timed conscription

$$\tau' > \tau + 5 \;\; \nVdash_{\mathrm{T}} \;\; \tau' = \infty$$

is at risk of aborting within its first 5 time units of execution, but if it manages to survive these first 5 time units it is then guaranteed to run forever.