formalizing choreographies in coq

luís cruz-filipe

(joint work with fabrizio montesi & marco peressotti)

department of mathematics and computer science
university of southern denmark

cl workshop
november 20th, 2020

the work in a nutshell

goal

formalize a research article in choreographic programming

- language of core choreographies
- language of stateful processes
- endpoint projection
- turing completeness

the work in a nutshell

goal

formalize a research article in choreographic programming

- language of core choreographies
- language of stateful processes
- endpoint projection
- turing completeness

why?

- proof of principle
- referee management
- hopes of a better future

methodology

- theorem prover: coq
- follow the reference as closely as possible
- expected issue: granularity

initial successes...

lots of good things

- syntax and semantics of core choreographies (with examples)
- formalization of partial recursive functions (ever heard of them?)
- encoding of partial recursive functions in choreographies
- soundness of the encoding (with termination)

...very, very close to the original article!

. . . then some challenges. . .

some tricky issues

- the "fatsemi" lemma – completeness of the encoding (very obvious result)
- reasoning about structural precongruence (stratified, commuting lemmas, interesting insights, nightmares)
- branching terms and partial functions
- merging and more partial functions
- the epp theorem (and the `more_branches` relation)

. . . and then all hell breaks loose

the unsurmountable obstacles

- recursion variables, α-equivalence, and structural precongruence
- the "fatsemi" lemma – requires confluence
  (still very obvious, but not for coq)
- multiplication of (unprovable) results
  (including the strangest properties about unfolding)
- nightmare on epp street

sideplot: fabrizio's course notes

a new way of formalizing choreographies

- no structural precongruence
- out-of-order execution and explicit unfolding
- global procedures (we knew that!)

sideplot: fabrizio's course notes

a new way of formalizing choreographies

- no structural precongruence
- out-of-order execution and explicit unfolding
- global procedures (we knew that!)

psychological implications

- six months of work (nearly) down the drain
- mental preparation required for restarting

sideplot: fabrizio's course notes

a new way of formalizing choreographies

- no structural precongruence
- out-of-order execution and explicit unfolding
- global procedures (we knew that!)

psychological implications

- six months of work (nearly) down the drain
- mental preparation required for restarting

the bright side

- much more reusable development than expected
- even more reusable *experience*

current status

done

- syntax and semantics of choreographies
- confluence lemmas
- bigstep semantics (instead of the "fatsemi" lemma)
- encoding of partial recursive functions
- soundness and completeness of the encoding

(planned submission in early february)

current status (cont'd)

in progress

- syntax and semantics of networks
  (still undecided on partiality of branching)
- merging (and epp)
- the epp theorem

$\rightsquigarrow$ basically one design decision, the right choice should unblock everything

(optimistically planned submission in mid-february)

the future

modular development

- add new features without breaking the old development
- streamline paper submission
- avoid endless discussions with referees
- generate correct-by-construction code
- (of course) publish a lot of papers

thank you!