Certified Matchbox

Johannes Waldmann, HTWK Leipzig

WST 22, Haifa

What and Why

- every (termination) proof should ultimately be machine-checked . . .
  especially if no human ever will read the proof
- for SRS termination, CeTA includes many powerful methods: interpretations, labeling, DP
- . . . and misses: RFC matchbounds, sparse tiling
- how far can we get with current CeTA?
  (how strongly do we need missing methods)
- Matchbox 2022 on SRS-Std (1651 problems):
  cert: 1495 (misses 156), avg. CPU: 36 sec
  uncert: 1587 (misses 64), avg. CPU: 20 sec

How

- natural and arctic matrix interpretations
  (SAT encoding with ersatz library, Kissat solver)
  method and (some) detail of encoding:
  see my course at ISR 2022 (Tbilisi)
- quasi-periodic interpretations (not in CeTA)
  presented as arctic (but smaller constraints)
- sparse tiling (for RFC) not in CeTA, but full tiling is (semantic labelling in the shift algebra)
- for tiled (labelled) system: weights only (GLPK)
- loops by enumeration of forward closures
- . . . and of transport systems (compressed loops)
  (not in CeTA) presented as loops

Certificate size, CeTA performance

- MB produces some large certificates:
  fully 2-tiled `ICFP_2010/26132` : 325 MB,
  expanded transport system of
  `Wenzel_16/abaaaaa-aaaaaaababababab` : 173 MB
- total size 24 GB, compressible to 0.3 % redundancies in CPF repr. of proofs (abstract syntax), in XML repr. of CPF (concrete syntax).
- CeTA handles large certificates well.
  Inefficient `Char -> Int` conversion quickly repaired by René Thiemann, cut time in half
  (CeTA slow on *-bounds? - not used by MB'22)

Summary, Discussion

- Matchbox 2022 on SRS-Std gets (slightly) more cert proofs than MB 2021 uncert
- all proof methods were in CeTA for some years, MB'22 has: efficient constraint solving, strategy and optimized parameters for proof search
- suggested challenge for next termcomp: write better strategy expression for other team's tool
- if you are, or have, a student: add to CeTA:
  - local termination (semantic labelling w.r.t. partial algebra)
  - RFC theorem
  - drop (cf. Dieter's talk)