Not My Problem

Crowdsourcing Code Verification With Video Games

Section 8.2 Program Correctness (for imperative programs)

A theory of program correctness needs wffs, axioms, and inference rules.

Wffs (called Hoare triples) are of the form

$$\{P\}\ S\ \{Q\}$$

Where S is a program statement and P (a *precondition*) and Q (a *postcondition*) are logical statements about the variables of S.

Semantics: The meaning of $\{P\}\ S\ \{Q\}$ is the truth value of the statement:

If P is true before S executes, then Q is true after S halts.

Note that it is assumed that S halts. If $\{P\}\ S\ \{Q\}$ is true, then S is said to be *correct* wrt to precondition P and postcondition Q.

Assignment Axiom (AA): $\{P(x/t)\}\ x := t\ \{P\}$.

Example. $\{x = 4\}\ x := x - 1\ \{x = 3\}$.

Example. $\{x < 4\}\ x := x - 1\ \{x < 3\}$.

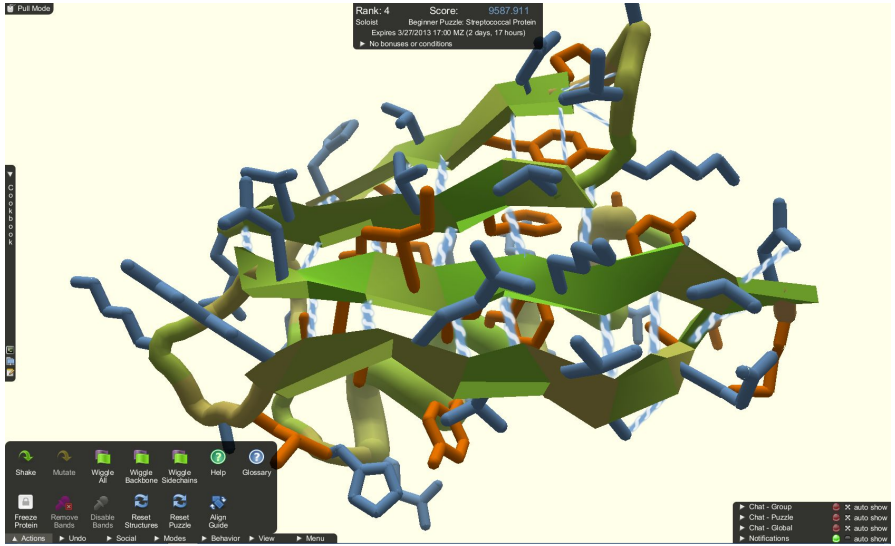
Inference Rules

Consequence Rule: $\dfrac{P \to R \text{ and } \{R\}\ S\ \{Q\}}{\{P\}\ S\ \{Q\}}$ and $\dfrac{\{P\}\ S\ \{T\} \text{ and } T \to Q}{\{P\}\ S\ \{Q\}}$

Example. Prove the correctness of $\{x < 3\}\ x := x - 1\ \{x < 3\}$.

Proof:	1.	$\{x < 4\}\ x := x - 1\ \{x < 3\}$	AA
	2.	$x < 3$	P [for $(x < 3) \to (x < 4)$]
	3.	$x < 4$	2, T
	4.	$(x < 3) \to (x < 4)$	2–3, CP
	5.	$\{x < 3\}\ x := x - 1\ \{x < 3\}$	1, 4, Consequence. QED.

https://www.cs.washington.edu/verigames



http://fold.it/portal/info/about

http://www.theesa.com/article/crowdsourced-video-games-prompt-breakthroughs-in-science-and-technology/