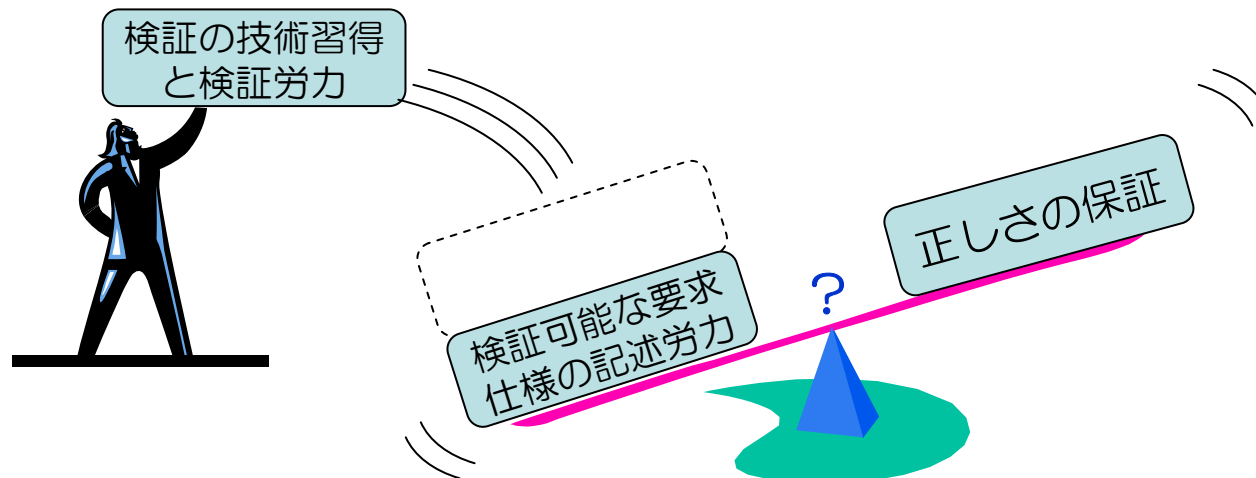


要求仕様の自動検証システムの開発

- この要求仕様で期待通りの実装が可能なはず
- この条件さえ満たしていれば正しいはずだけれど、満たしてる？
- 1つ1つの動作は単純なのに、組み合わせると・・・
- 割り込み処理を全パターン追うのは、きびしい・・・
- 誤りはあるらしい、でもどこにあるの？

検証技術に対するニーズはあっても、実際の作業量・技術習得が障壁

- 検証を自動化することで、利用しやすさを向上
 - 特に証明で困難な問題である問題固有の補題を、独自の手法により自動発見



自動検証システム Crème の持つ7つの特徴

■ 補題の利用

自動で発見した証明に必要な知識を設計・下流工程でも利用

検証には、補題など発見的な知識が必要得られた問題固有の補題からより安全な設計・実装との一貫性チェックに利用

■ 正しさの保証・理由の提示

要求仕様が期待する性質を満たす事を厳密に保証。追試可能な証明も出力

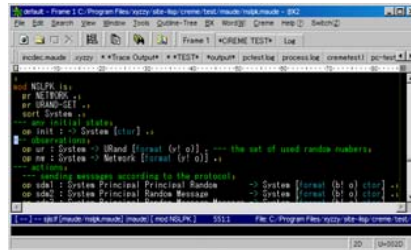
致命的誤りによる損失を防ぐ証明により要求仕様の理解を深める

■ 検証の自動化

検証を
・省力化
・効率化
・簡単化

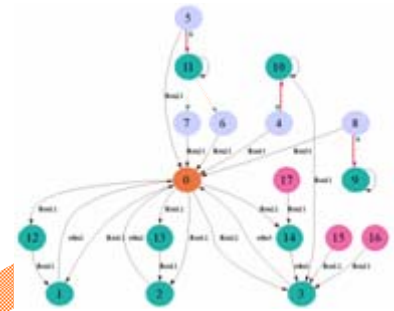
検証技術の普及を阻む多くの問題の解決に効果的

■ 自動検証システム Crème



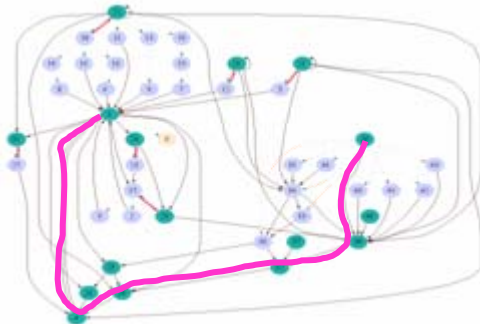
エディタ [xyzyx](#) 上に実装。要求仕様の記述・検証環境を統合

■ 証明を可視化



検証状況の確認
証明の持つ隠れた構造の発見
Crème 自身の直感的理解にも役立つ

■ 誤りを反例で提示



要求仕様の誤りの発見・修正を強力に支援
誤りを含む要求仕様から、少しずつ完全なものへと近づける上でとても有用

■ 高い記述能力

要求仕様記述言語の高い記述能力とそれを処理可能な証明系

要求仕様は、遷移機械としてモデル化
それを数学的基盤を持つ代数仕様で記述