項書換えシステム
証明支援システム

ICOT第2研究室
問題解決とプログラミングの研究グループ
(Problem-solving & Programming Group:PPG)

プログラミング支援環境

・オペレーティングシステム

エディタ，コンパイラ，デバッガ，etc.

・プログラミング・エキスパート

プログラム知識ベース

・プログラム検証・プログラム合成システム

プログラムの正しさ

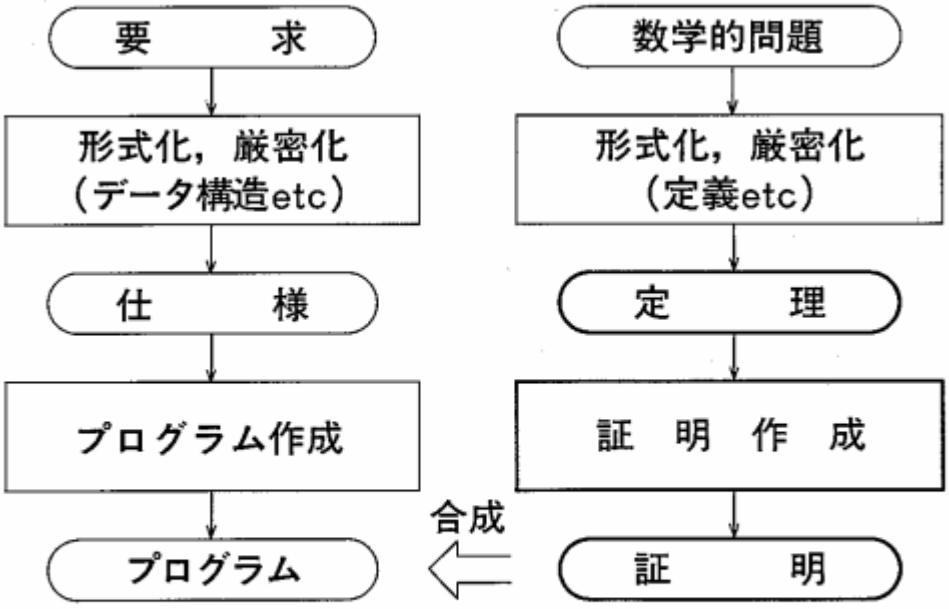
＝アルゴリズムの正しさ（数学的証明）

　　＋インプリメンテーションの正しさ

インプリメンテーションの正しさの確認

- 仕様とプログラム間の検証
- 仕様からプログラムへの変換
- 数学的証明とインプリメンテーションの一体化

プログラミングと定理証明



数学的証明の2大要素

◦ 計算 … 等号「＝」の処理

項書換えシステム

◦ 論理 … 論理結合子「∧, ∨, →, ¬」の処理

証明支援システム

証明支援システムの応用

◦ 数学を使う研究者のノートがわり

証明記述の支援(証明記述言語, エディタ)

証明行為の支援(計算, 証明戦略のアドバイス, 証明チェック)

論文執筆の支援(2次元プリティプリンタ)

◦ 数学を学ぶ学生の教育用

証明の誤り指摘

コンピュータによる証明例

◦ 知識情報処理への応用

プログラミングの支援(合成, 検証)

エキスパート・システム, 問題解決・推論システム

対象分野

◦線型代数

誰もが知っている。視覚的な要素が多い。

様々な分野が関連している。

◦総合微分幾可

代数的理論である。新しい分野である。

◦記号算術(QJ/Quty)

超数学を扱ってる。構成的数学に基づいている。

CAP-LAシステム(60年度成果)

目的：大学初年級程度の線形代数の理論構築の支援

機能：証明記述の支援(エディタ)

証明の理論展開のチェック

(チェッカ，理論知識ベース)

証明の誤り訂正の支援

証明支援システムの今後の課題

・CAP-LAシステムの充実(汎用化，高機能化)

・CAP-SDGシステムの設計とインプリメント

・CAP-QJシステムの設計

・プログラム合成への応用の検討

項書換えシステムの応用

◦等式の正当性検証システムとして

証明支援システムの等式検証

等号公理系の定理証明

一階述語論理の定理証明

◦プログラム作成支援に

プログラムの実行機構

プログラムの検証・合成

(論理＋関数)型プログラミング言語の実現

代数的仕様記述

◦計算機構として

数式処理の計算エンジン

項書換えシステム

目的：等号「＝」による書換え処理を効率的かつ効果的に扱う。

機能：書換えに方向性を持たせる。

書換えの曖昧性を除去する。

書換えを実行する。

・書換えの方向性（無限の書換えの禁止）

× $X \rightarrow X+O$

$a \rightarrow a+O \rightarrow (a+O)+O \rightarrow \cdots$

○ $X+O \rightarrow X$

$(a+O)+O \rightarrow a+O \rightarrow a$

・書換えの無曖昧性

× $X/X \rightarrow 1, O/X \rightarrow O$

$1 \leftarrow O/O \rightarrow O$

○ $O+X \rightarrow X, (X+y)+Z \rightarrow X+(y+Z)$

$X+y \leftarrow (O+X)+y \rightarrow O+(X+y) \rightarrow X+y$

項書換えシステムの60年度成果

- 曖昧性の検定および除去手続きのインプリメント
  （Knuth & Bendixの完備化手続き）
- 様々な方向づけ手法の研究とインプリメント
- 書換え実行部のインプリメント
- 証明支援システムへの応用
- 上記機能の会話利用環境の設計と試作

項書換えシステムの今後の課題

- システムとしての充実
  マンマシンインタフェース，高機能化
- 方向づけできない等式の処理
  結合法則と交換法則の組み込み
  Unfailing Knuth-Bendix完備化手続き
- プログラム作成支援への応用の検討
- 計算機構としての利用の検討