

Introduction to

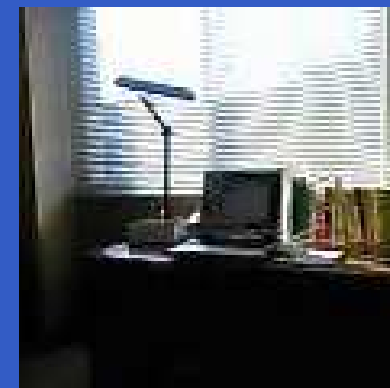
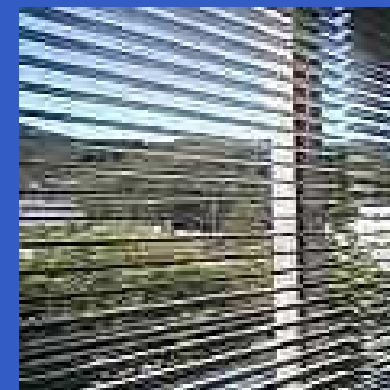
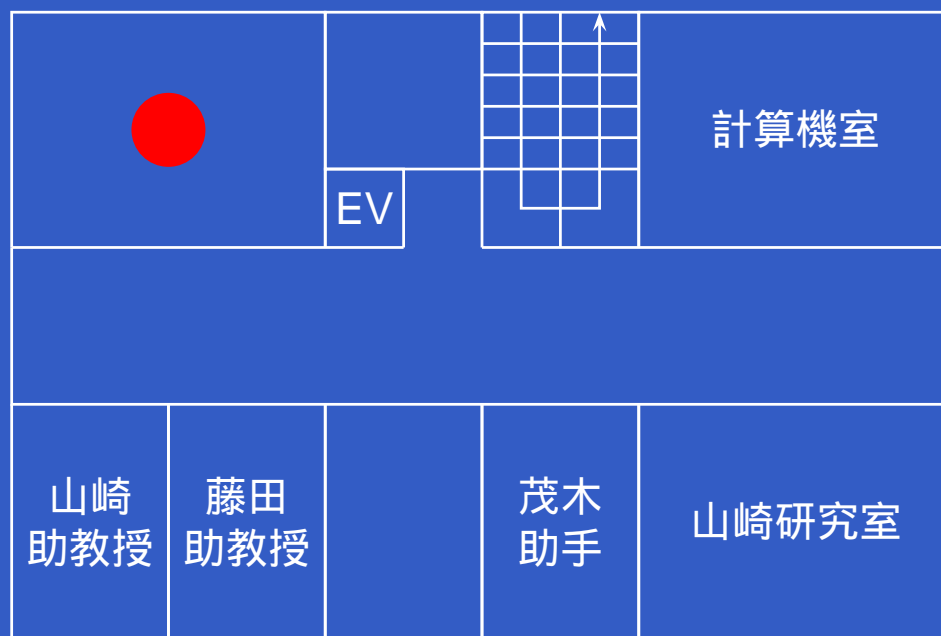
Fujita Lab.

教官：藤田 憲悦 助教授

<http://www.comp.cs.gunma-u.ac.jp/fujita/index.html>

研究室の様子

情報工学科西棟 3F



研究体制

2006 年度研究室構成

- 助教授：1 名
- M2：1 名
- M1：2 名
- B4：3 名

研究テーマ

ソフトウェア基礎科学の研究

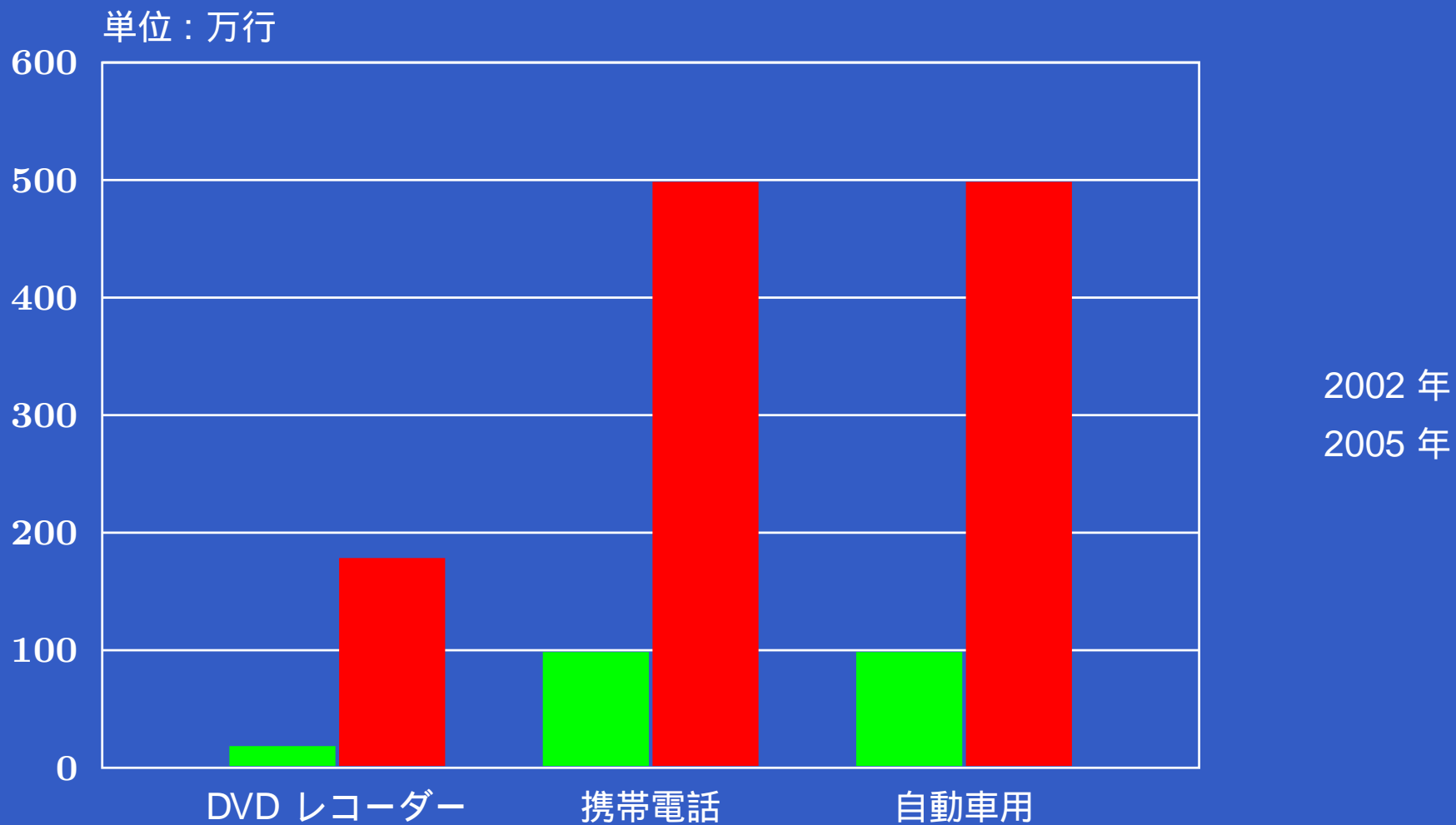
- プログラムの型と論理式との対応関係
- 計算機支援によるソフトウェアの検証
- プログラム変換と抽象機械
- Web グラフの構造解析

研究テーマ

ソフトウェア基礎科学の研究

- プログラムの型と論理式との対応関係
- 計算機支援によるソフトウェアの検証
- プログラム変換と抽象機械
- Web グラフの構造解析

巨大化するソフトウェアの規模



出展：日経ビジネス

組み込みソフトウェアの不具合の事例

公表日	メーカー/製品名	不具合の内容
2005/1/21	東芝「V601T」,「V602T」	特定の条件化でメール操作や発着信ができなくなる
2004/10/21	京セラ「W21K」	特定の条件化で記憶させている情報が消失
2004/9/13	三洋電機「W21SA」	定額課金すべきパケット通信料を従量課金にするソフトの不具合
2004/7/2	パナソニック「P252iS」	サービスエリア内でも発着信ができなくなる
2004/3/29	三洋電機「A5503SA」	本体内に保存したファイルの消失やメールの送受信ができなくなる
2004/3/3	富士通「F900i」	折り畳んだ状態でのメールの自動受信ができなくなる

出展：日経ビジネス

手作業によるテストの限界

- 検査項目は50万件を超える(携帯電話)
- 製品出荷後の不具合の原因はソフトウェアが4割を越えると推定
- 計算機の支援によるソフトウェアの検証が必要
 - モデル検査
 - 定理証明

モデル検査

システムを有限状態遷移系にモデル化
有限の「状態」、「遷移関係」、「初期状態」

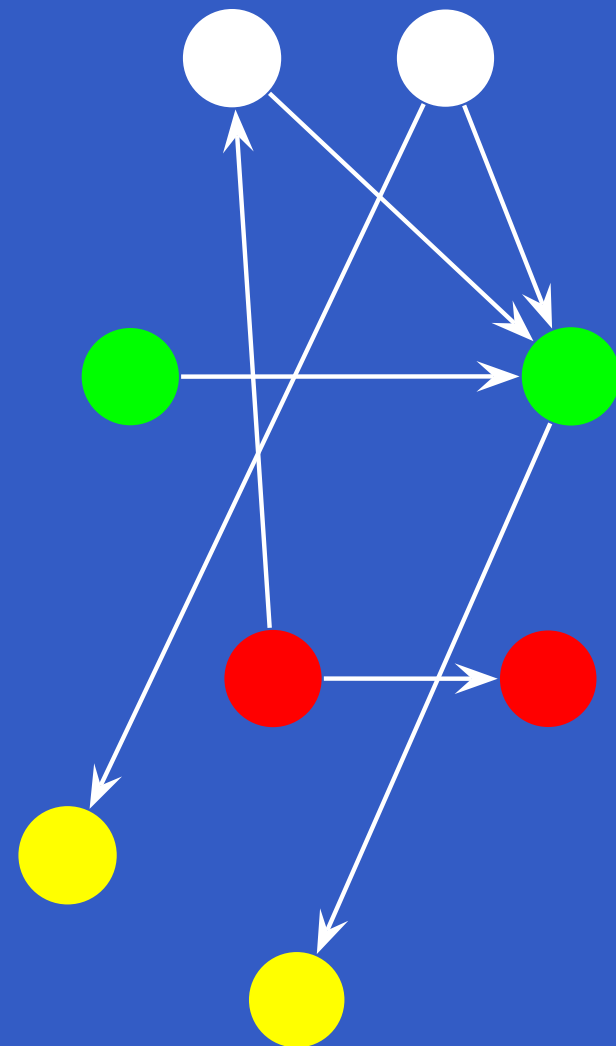


検証したい性質を論理式で記述

- 赤には決して到達しない
- 黄色に到達するまでに必ず白を通る



モデル検査器による全数探索 (全自動)



定理証明

ϕ : 仕様

P : プログラム



定理証明系により「 P が ϕ を満たす」ことを証明

入力された二つの整数の
最大値を返す



```
\result >= x && \result >= y &&  
(\forall int z; z >= x && z >= y; z >= \result)
```



仕様とプログラムは一致する?

```
public static int max(int x, int y) {  
    if (x > y) returun x; else retutn y;  
}
```

Thank You!