「ちゃんと動くコンピュータ」のために

ー数学的理論にもとづくソフトウェアづくりー

ソフトウェア基礎科学分野　住井・松田研究室

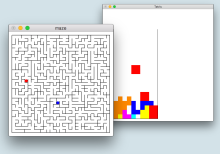
展示会場：電気情報システム・応物系3号館 206号室

再帰の考え方

漸化式のようにプログラミング

偽装迷惑メール送信

創造工学研修作品集



逆プログラム導出

$f \xrightarrow{\text{導出}} f^{-1}$

例：圧縮プログラム　　例：展開プログラム

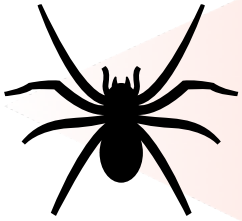
スマートコントラクト

```
foreach (…)
  x += f(a)
Xfer(sender
…
…
```

ブロックチェーン上で動くプログラム

遍在するソフトウェア▶遍在するバグ

パソコン，携帯電話，車，飛行機，調理機器，証券取引，医療機器，発電所，電子政府，…



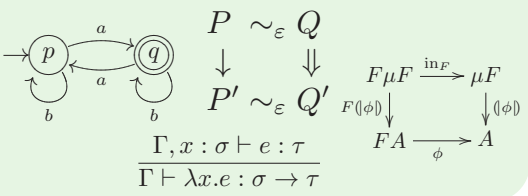
もしバグがあると…

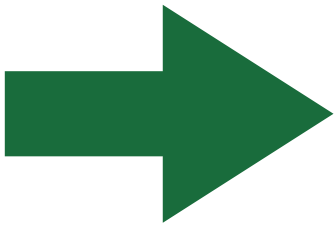
過去のバグの脅威の例

- 死傷者6名 ———Therac-25 (1985-87)
- ロケット爆発 ——— Ariane 5 (1996)
- 107億円賠償 — 東京証券取引所 (2006)

数学にもとづき，バグのない「ちゃんと動く」ソフトウェアを！

さまざまな数学





具体的な研究テーマの例

関数プログラミング

```
δ = 0.000001
diff(f,x) = (f(x+δ)−f(x))/δ
square(x) = x*x
ans = diff(square,1)
⇒ 2.0000009999243673
```

スマートコントラクト検証

```
if (balances[caller] >= amt) {
    Transfer(caller, amt);
    balances[caller] -= amt;
}
```

大切な資産を扱うプログラム，気をつけて作ったけれど本当に正しい？

双方向変換