

A05 班: ハードウェアアルゴリズムの性能評価 に関する研究

「新世代の計算限界」
2007 年度 第 1 回 全体会議 資料

高木 一義, 高木 直史

名古屋大学 大学院情報科学研究科

A05 班: 「ハードウェアアルゴリズムの性能評価」

メンバー

- 高木 直史 名古屋大学大学院情報科学研究科 教授
- 高木 一義 名古屋大学大学院情報科学研究科 准教授

研究課題

- ハードウェアアルゴリズムと回路の設計
 - アルゴリズムの設計
 - 実用的規模での定量的評価
- 回路の性質と性能の解明
 - 新しい回路モデル、性能評価モデル
- 回路設計技術
 - 新しい論理表現構造
 - ハードウェアアルゴリズムの自動合成

ハードウェアアルゴリズム

ハードウェア実現を前提としたアルゴリズム

- 回路規模、計算時間で評価
 - 組合せ回路モデル、配線を考慮した VLSI モデル
- 並列性の利用、規則的な繰返し構造
 - データ表現の工夫などが重要
- 専用回路としてのコストを考慮
 - 四則演算、初等関数などの専用回路を持つメリットとコストのトレードオフ
 - 「 n ビット」演算回路 — 実用的な規模での効率が重要

ハードウェアアルゴリズムの性能評価

- 集積システムの大規模化、高速化、低消費電力化
 - より精密なモデルと性能評価、設計入力へのフィードバックが必要
 - より抽象度の高い設計記述 — 論理記述から演算手順の記述、計算式や演算定義の記述へ
- 配線遅延の比率の増大
 - 論理ゲート段数より配線の引き回しやバッファ挿入が計算速度に影響
 - 従来の組合せ回路モデルで評価できるか？

「より現実に即した性能評価基準の確立」

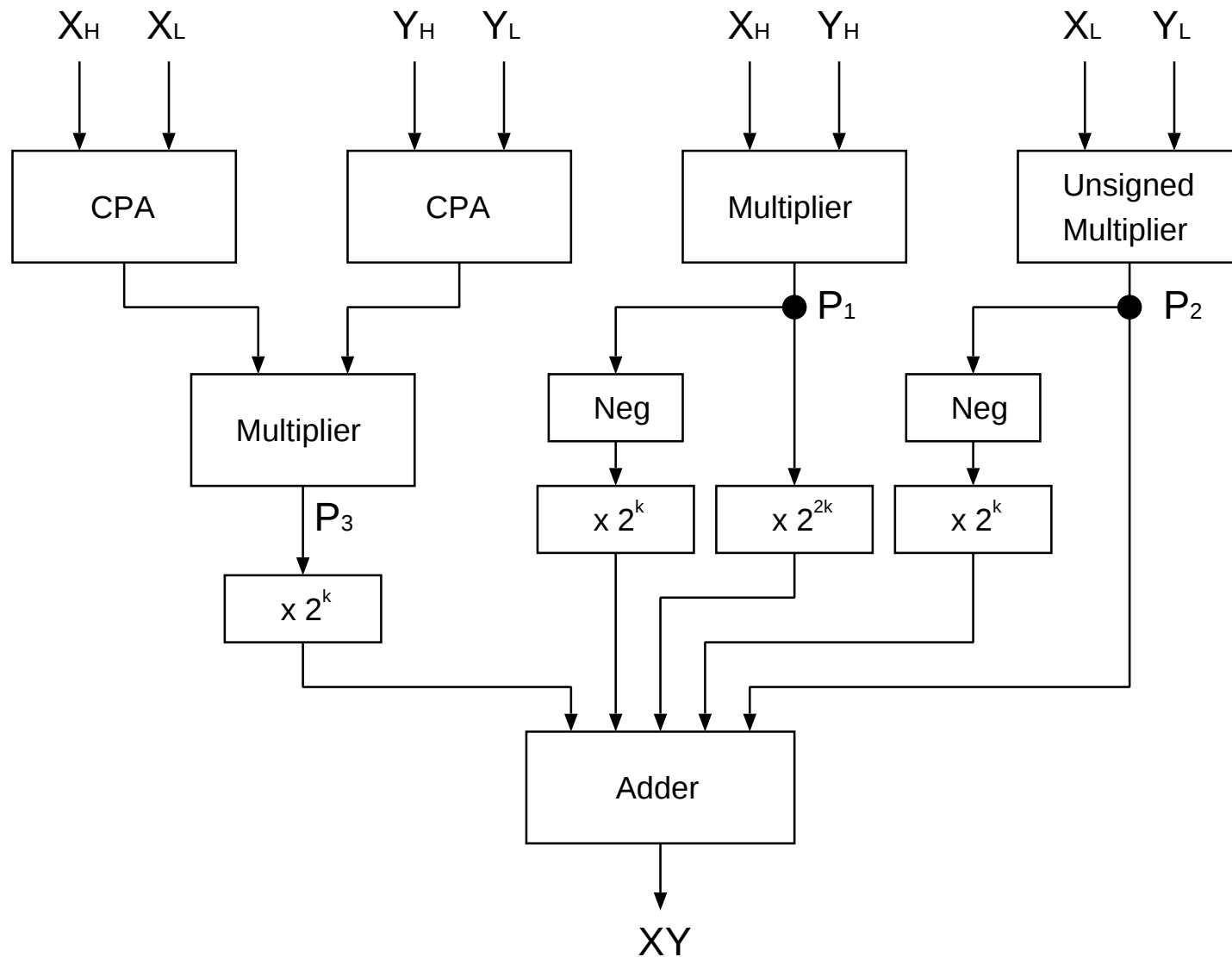
研究成果

1. Karatsuba アルゴリズムに基づく乗算のハードウェアアルゴリズム (H16–H17)
2. 乗算器の回路面積の評価 (H17–H18) 1
3. 整数除算のハードウェアアルゴリズム (H16–H17)
4. 整数開平のハードウェアアルゴリズム (H18) 2
5. 算術演算ハードウェアアルゴリズムの自動合成手法 (H16–)
6. 暗号処理のための乗算剰余算の新しいアルゴリズム (H17)
7. ガロア体 $GF(2^m)$ 上の乗算と逆元計算の統合アルゴリズム (H18) 3

1. 乗算器の回路面積の評価

- Karatsuba アルゴリズム [1963]
 - n ビット乗算を加算と 3 回の $n/2$ ビット乗算に分解
 - 論理素子は比較的少ないが配線は複雑
- ⇒ 32bit 程度でも高速かつ小面積の LSI が実現可能
- 配線層数の回路面積への影響
 - 今の半導体 LSI では配線領域 (層数) は十分
 - 「複雑な配線」は回路面積の面では必ずしも不利ではない
 - 実用的なサイズの回路を条件を変えて設計し検証

Karatsuba 乗算回路



64bit 乗算回路の面積

	素子面積 (μm^2)	LSI 面積増加率 (%)	
		配線 3 層	配線 5 層
Array	404413	1.5	1.5
Wallace	409054	1.5	1.5
Karatsuba	320140	1.5	1.5
Array+Booth	290543	25.0	1.5
Wallace+Booth	294023	66.7	1.5
Karatsuba+Booth	253342	100.0	1.5

- 配線層数が多いと配線の複雑さや規則性の影響少
— 論理素子数を重視したアルゴリズムが有利

2. 整数除算/開平アルゴリズム

■ 整数除算アルゴリズム

- 冗長 2 進表現の絶対値計算を繰り返し
- 筆算と同様の減算シフト型
- 符号の検出と絶対値計算を並列に実行
- 計算時間 $O(n)$ 、面積 $O(n^2)$
- 数クロックで計算する順序回路も構成可能

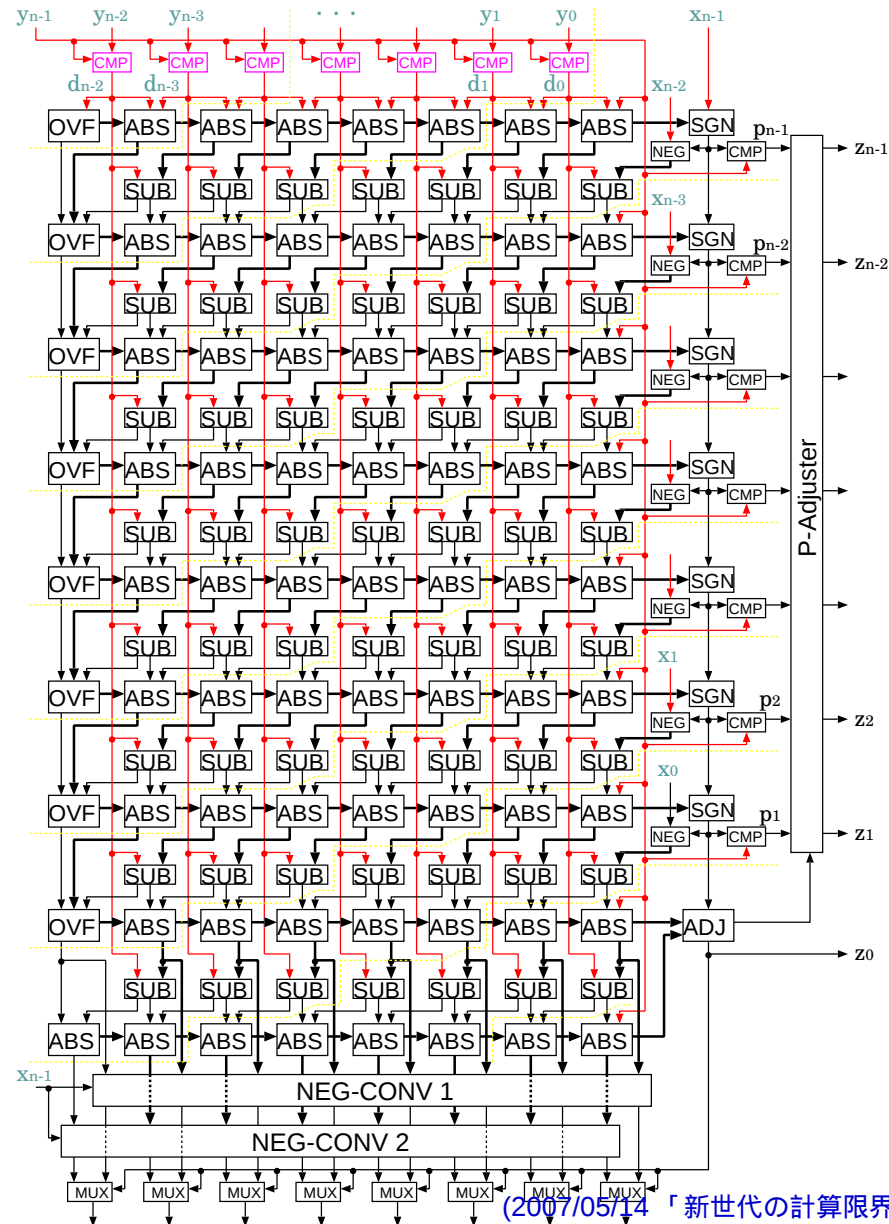
■ 整数開平アルゴリズム

- 除算と同様に計算可能

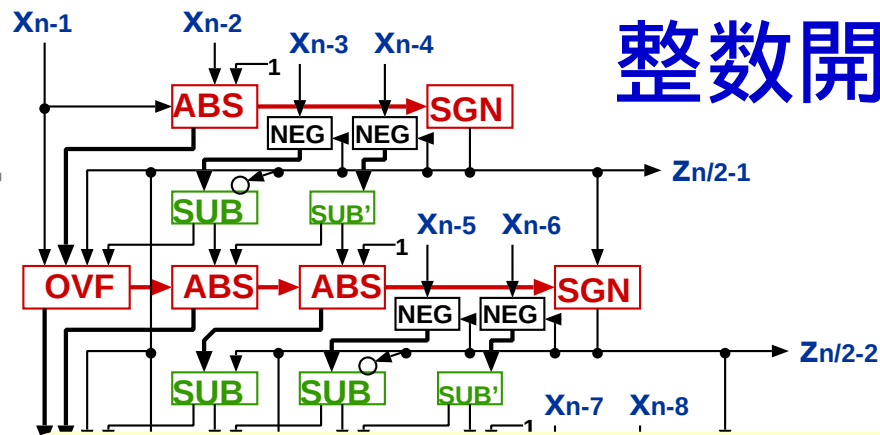
■ 回路の設計と評価

- オーダ的には通常の減算シフト型除算/開平より有利
- 定数項が大きい $\Rightarrow$ ビット数 n が小さい範囲では不利

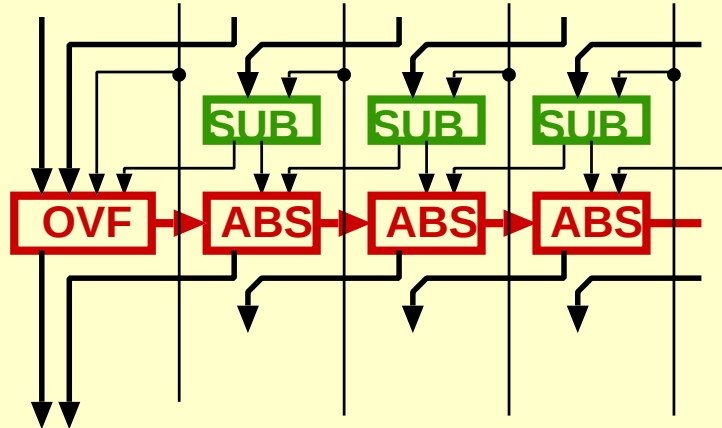
整数除算回路



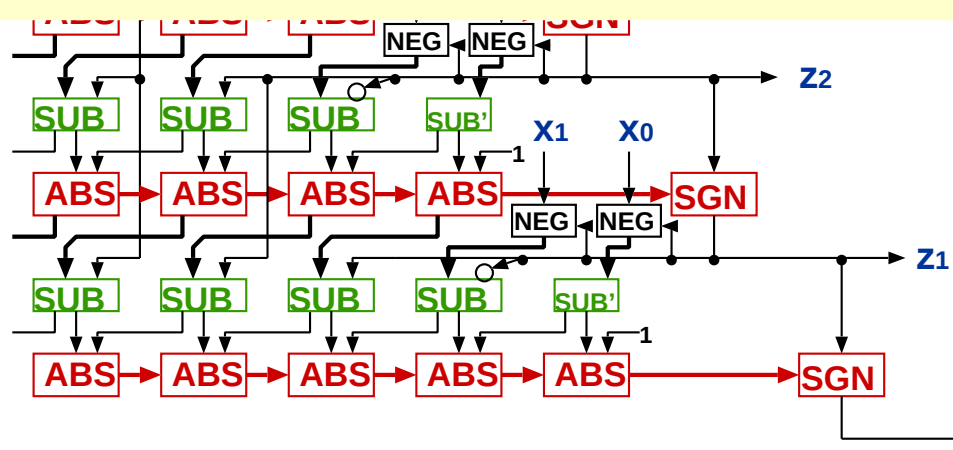
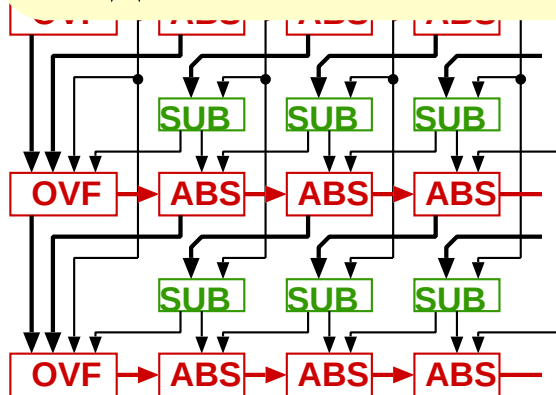
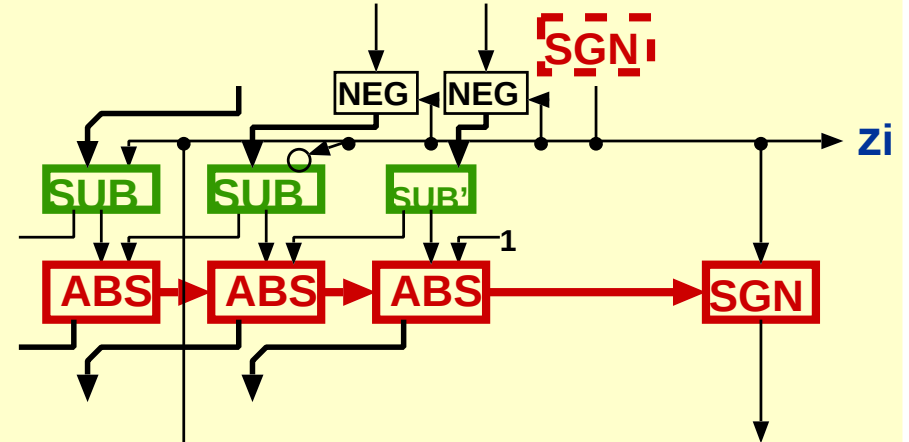
整数開平回路



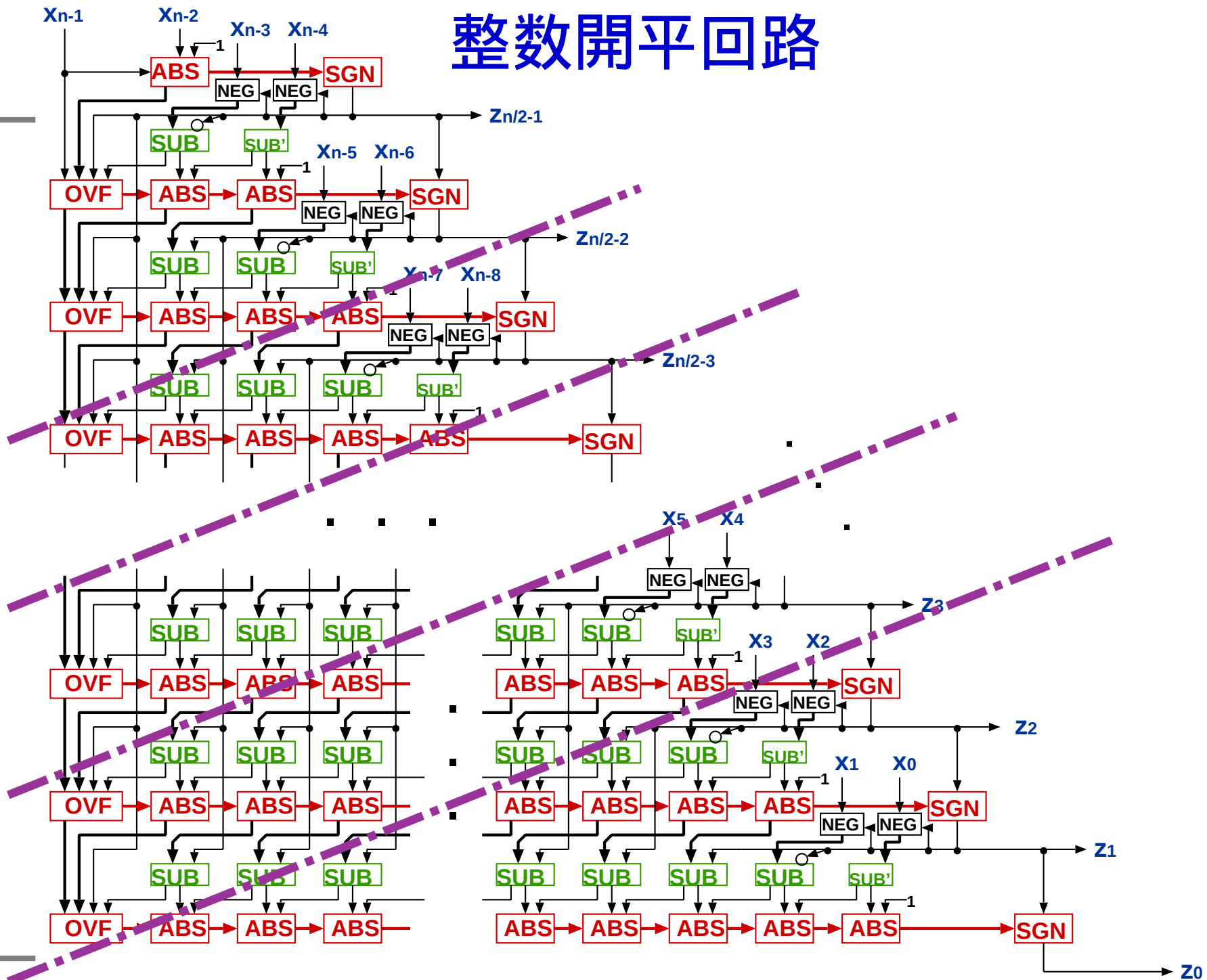
$z(n/2-1) z(n/2-2) z(n/2-3) z(n/2-4)$



$x(2i-1)x(2i-2)$



整数開平回路



3. ガロア体 $GF(2^m)$ 上の乗算・逆元計算の統合

- $GF(2^m)$: 楕円曲線暗号で利用、乗算と逆元計算の高速化が重要
- 統合ハードウェアアルゴリズム
 - 乗算と逆元計算アルゴリズムの類似性に着目
 - ─ 乗算: MSB-first アルゴリズム
 - ─ 逆元計算: 拡張ユークリッド法
 - 複合回路を構成
 - ─ 乗算/逆元計算モード切り替え
 - ─ 演算器などデータパスを共有
 - 両者を個別に作るより小面積

研究課題「ハードウェアアルゴリズムの性能評価」

■ 研究課題

- ハードウェアアルゴリズムと回路の設計
 - － アルゴリズムの設計 (H16–H18)
 - － 実用的規模での定量的評価 (H16–H18)
- 回路の性質と性能の解明
 - － 新しい回路モデル、性能評価モデル (H18–)
- 回路設計技術
 - － 新しい論理表現構造 (H16–H17)
 - － ハードウェアアルゴリズムの自動合成 (H16–)

■ 今後の方針

- ハードウェアアルゴリズムの現実的な性能評価のための VLSI モデルの構築
- ハードウェアアルゴリズムの自動合成