高知大学大学院理学研究科

数理情報科学専攻情報科学講座

2006年度修士論文要旨

2端子ネットのグローバル配線問題に関する研究

数理情報科学専攻　情報科学講座　木坂有男

高度情報化社会を迎え，情報処理機能を持つ電子機器や家電製品が一般化している。LSI(大規模集積回路)はこれらにコア部品として多数組み込まれて、社会的要求により更なる高速化、高性能化が求められている。製造プロセスを微細化すれば素子集積率が高まり，配線距離が短縮して高速化できるため，長年に渡りムーアの法則(Moore's Law)が支持されてきた。しかし，0.13μmを超える今日の微細化プロセスにおいて，DSM(Deep sub Micron)問題が深刻になってきた。DSM問題とは，細線化による抵抗増化や，配線間隔の近接による電荷容量の発生などにより信号遅延が不確かになる問題で，設計タイミング仕様上，配線設計における対策が不可欠である。

詳細な配線は，グローバル配線が決定した配線経路に従って局所的に行われる。従って，グローバル配線レベルでのDSM問題の対策もまた重要となる。

本論文は、配線の経路や密度を大局的に決めるグローバル配線問題に関し，グローバル配線問題の最善手法について提案するものである。

グローバル配線問題は，レイアウト領域を荒い格子で分割し，各格子上に配された端子間の配線経路を決定する問題で，各格子を通過する配線数を評価し，各経路の分散の程度を解品質として評価する。LSI回路の配線は膨大で，配線順で局所集中を生じる。そこで本研究では，Rip-up/Rerouteで改善する従来法 1)ランダムウォークの経路をグリーディ評価する方法、2) ランダムウォークの経路をSimulated-Annealing法で評価する方法，さらに3)密度最小経路をBreadth-First Search(ダイクストラ)法で求める方法を，二端子ネット(入力と出力が1のみの配線)で評価した。

その結果３）の方法が，最短時間で最善結果となることがわかった。単純なダイクストラ法は，局所解に陥ることは自明であるが，実装した繰り返し改善と組合せることで最適な手法となることが見出された。

キー入力リズムによる個人認証について
－大規模実験での検証－

数理情報科学専攻　情報科学講座　　重岡　有貴

2001 年 1 月，5 年以内に世界最先端の IT 国家となることを目指し，e-japan 戦略が策定された．それにより我が国の IT 化は大きく進展した．更に 2006 年以降も引き続き世界最先端の IT 国家であり続けるために“u-japan 構想”が打ち出され，ユビキタス社会を目指した政策が進められている．どの政策においても“個人情報の保護”,“セキュリティの確保”は，最重要課題に位置づけられており，今後もネットワークが巨大化し，ICT が浸透するにつれて，更なる強化が必要不可欠である．

現在のセキュリティ技術には，さまざまなものがあり，個人認証の分野では，パスワードなどを用いた最も基本的な認証方法から，指紋や虹彩，網膜，静脈などといった本人しか持ち得ない情報であるバイオメトリクスによる認証方法（生体認証）などがある．それらの中でも特に信頼性の高いセキュリティとして，バイオメトリクスを中心とした研究が多くなされているが，現在の個人認証についての研究は，入り口を守るだけの前認証を対象としたものであり，一度認証をパスしてしまえば，その後に本人であることを確認することは行われない．この方法では，何らかの方法でパスワード等を入手してしまえば，他人が本人になりすまして使用することが可能となる．

この問題に対して，認証後にも引き続きユーザを常時監視する「追認証」という方法を行うことによって,セキュリティをより高めることができる．追認証では,“盗めない”,“真似できない”本人の確認方法として，人の行動的特徴を用いる．当研究室ではこれまでマウスやキー入力を用いた追認証が先行研究として行われてきた．しかし，どちらも小規模での実験であり，ある程度の人数を対象とした検証は行われていない．

本研究では，これまで行われてきたキーボートによる追認証技術を見直すとともに，100 人規模での実験を行うことを目的とした．まず実験環境として，ネットワークを介して実験を行えるよう，認証プログラムを web ベースの Flash に移行した．そして事前調査を繰り返すことで，個人の特徴が出やすい用語を選定し,無作為に選んだ 100 人を対象に実験を行った．その結果，100 人規模でも有効性が認められる特徴を捉えることができ，本手法がある程度の規模で利用できる可能性を検証することができた．

浮動小数点形式を用いた行列演算プロセッサの設計研究

数理情報科学専攻　情報科学講座　城間周博

LSIの大規模化、複雑化に対応するために設計技術にも変化が起き、現在ではHDL（ハードウェア記述言語）というハードウェアを記述するための言語が広く用いられるようになっている。HDLが開発される前の設計手法はセル部から設計を始め、最終的に製品を作成するボトムアップ設計だったのに対し、HDLを用いる設計手法ではRTL回路から設計することができるトップダウン設計となっており、回路記述の簡易化、シミュレーションの早期開始ができるということ、ゲートレベル設計の自動化などの点から、LSIを開発する上で重要となっている。

本研究室では、HDLを用いて浮動小数点プロセッサ(Floating point Processing Unit)の設計を目的に研究を行っている。私は以前設計された浮動小数点プロセッサを元に、専用プロセッサの研究を行った。具体的には

３２ビット浮動小数点プロセッサ（FPU）の

１命令フォーマットの変更
２処理ステップ数の削減

をなどを考慮し、画像処理における３次元座標変換を高速に行える行列演算プロセッサを設計した。

行列演算プロセッサの特徴として、３２ビットの命令フォーマット、マルチポートレジスタなどがある。命令フォーマットは４ビットを演算の種類を指定するオペレーションコードにあて、２８ビットをレジスタのアドレス指定にあてている。マルチポートレジスタ部に関しては、読み出し５ポート、書き込み３ポートの複数のポートを備えており、同時に複数のデータがやりとりできるようになっている。

また、HDLで設計したRTL記述が正しく動作するかを、回路にテスト信号を与えHDLシミュレータで確認し、シミュレーションを行なった後、HDL記述をゲートレベルに変換する論理変換をザイリンクス社の論理合成ツールにより実行した。

楕円曲線の位数計算アルゴリズムの研究

数理情報科学専攻　情報科学講座　　森　陽介

1. 序論

現在、公開鍵暗号で最も利用されているのは素因数分解の困難性を利用した RSA 暗号であるが、コンピュータの性能向上により従来の鍵サイズでは必ずしも安全ではなくなりつつある。それに伴い、注目されているのが楕円曲線を用いた暗号理論である。

有限体上の楕円曲線は無数に存在するが、任意の楕円曲線が必ずしも暗号化に適しているとは限らない。Pohlig-Hellman 法による攻撃を回避するためには、曲線の位数を調べる必要がある。そこで、本研究では楕円曲線の位数計算について研究および実験を行った。

2. Schoof-Elkies-Atkin 法

Schoof-Elkies-Atkin 法は、 Schoof 法の計算上の実効性を改良するために開発された。

F_p 上の楕円曲線 E の位数は『 Frobenius 写像 ψ のトレース』t を用いて、

$$\sharp E(F_p) = p + 1 - t$$

と表される。Schoof 法の主要部分は、素数 l について l-等分点上の Frobenius 写像の特性方程式

$$W_l(\psi) = \psi^2 - t_l\psi + p = 0$$

を考え、$t_l = t \mod l$ を求めることにある。その際、次数の非常に高い l-等分多項式を使う必要がある。これに対し、 Schoof-Elkies-Atkin 法はより小さい次数の多項式で処理するものである。

3. Elkies 素数

Frobenius 写像 ψ の特性多項式 W_l が 2 つの根 λ と μ を有限体 F_l に持つ場合、 l を Elkies 素数という：Frobenius の特性方程式は

$$\psi^2 - t_l\psi + p = (\psi - \lambda)(\psi - \mu)$$

に分解し、λ は、

$$(x^p, y^p) = [\lambda](x, y)$$

の関係を使って探索できる。このとき

$$t_l = \lambda + \frac{p}{\lambda} \mod l$$

となる。

4. Atkin 素数

Frobenius 写像 ψ の特性多項式 $\psi^2 - t\psi + p \pmod l$ が F_l で根を持たない場合、 l を Atkin 素数という:このとき、Frobenius 写像 ψ の特性多項式は F_{l^2} で分解し、2 つの根 $\lambda, \mu \in F_{l^2} - F_l$ を持つ。$\gamma_r = \frac{\lambda}{\mu}$ がとり得る値は限られ、関係式

$$t_l \equiv \lambda + \mu \pmod l,\ p \equiv \lambda\mu \pmod l$$

から トレース $t_l = t \mod l$ に対する候補値の集合が得られる。

5. トレース決定アルゴリズム

入力：
有限体 F_p 上の楕円曲線 E、
Elkies 素数・Atkin 素数で計算された結果。

出力：
有限体 F_p 上の楕円曲線 E のトレース t。

1. Elkies 素数から得られた情報は中国剰余定理を使って、ひとつの合同式
$$t \equiv t_3 \mod m_3$$
に統合する。
2. Atkin 素数は 2 つの集合に分け、それぞれのトレースの候補を中国剰余定理を使って以下のようにまとめる。
$$t \equiv r_1 \mod m_1, \quad t \equiv r_2 \mod m_2$$
3. 以上の結果を統合してトレースを決定する。

Step 2 においては、
- 2 つの集合への分割方法の選択、
- 候補値を多く持ち過ぎる Atkin 素数の削除

が、大きく計算量に影響するので工夫を要する。

6. 結論

楕円曲線によって位数は変化し、楕円曲線のパラメータでは位数を推測することは出来ない。

位数計算アルゴリズムは代表的なものとして 4 つある。その内、Weil 予想を用いる方法などは高速に計算可能であるが、適用できる曲線が限定され、その限定が暗号解読の手がかりになりかねない。一番暗号への応用性・自由度が高い位数計算アルゴリズムは、Schoof 法や Schoof-Elkies-Atkin 法である。

本研究で実装した Schoof-Elkies-Atkin 法は推奨されている鍵長 170bit を超える楕円曲線の位数を実用的な時間で計算することが出来た。

配線長を保証するスタンダードセル再配置法の研究

数理情報科学専攻　情報科学講座　　山崎　雅史

近年，LSI設計では，微細化にともない信号配線の抵抗，配線間の電荷容量の増加や，高速動作によるクロストークなどでタイミング保証が難しくなるDSM(Deep Sub-Micron)問題が深刻である．さらに微細化は回路規模を増やすため，回路ミスや仕様変更も増加する．このような回路変更・修正やタイミング修正を支援するレイアウト設計法は，最先端LSIの設計フローにおいて重要技術課題となっている．

本論文は，最先端LSI設計フローにおいて，しばしば生じる部分論理回路の修正（セルサイズ変更や回路構成追加・変更）に対して，元の配置結果の配線長からの増減範囲を保証するインクリメンタル配置モデルとその再配置法について述べたものである．

一般にインクリメンタル配置法とは，元の配置から若干の変更で新たな配置を得る試みを指す．従来法には，局所的な変更のみに限定するものや，大局的なシミュレーテドアニーリング(SA)による配置法を低温範囲に限定する配置法などであった．しかし，前者は，配置密度が高い場合には，セル追加が不可能になる．また，低温SA法では，たとえ低温に限っても予想外の配線長の増減を防止できず，配線長予測が不可能となる．そのためは再配置後のタイミング仕様を満たす方法がなかった．

そこで，本研究では元の配置を参照しながら，再配置後の配線長が指定範囲内となる配置モデルを提案する．配線長の増減が指定範囲内であれば，配線遅延が予測でき，再配置後のタイミング保証が可能となる．

本スタンダードセル再配置設計手法の評価をISPD2000およびMCNCのベンチマーク回路のネットリストからSA法により得た初期配置に対して，全セル数からランダムに選択した5%，10%および20%のセルを各々セルサイズを元の5%，10%および20%の増減させ修正ネットリストを用いて本手法を評価したところ，全配線について元の線長と増減差を指定範囲内に保証できることがわかった．

浮動小数点プロセッサの設計と展開
-画像処理を意図した命令セットと性能の関係-

数理情報科学専攻　情報科学講座　横山真登

近年、パーソナルコンピューターのソフトウェアや家庭用・業務用ゲーム、またカーナビや携帯用端末などで、３次元画像を用いたものが普及している。それらの演算は高速に行う必要がある。

それらの演算では、画像処理のデータは広範囲の実数を使用するためにFPU（Floating point Processing Unit：浮動小数点演算装置）が利用される。FPUとは、浮動小数点演算を専門に行う処理装置のことで、単独では動作せず、主装置であるCPUから利用されるのが一般的である。

一般的なFPUを利用する場合各画像処理内部の演算を一つ一つ順番に処理する必要がある。

そこで､画像処理演算において大きなウエイトを占めるアフィン変換(座標変換)､レイトレーシングによる陰面消去､反射光の強さや視線の屈折などの各種シェーディング処理の演算を効率よく処理することのできるようなG-FPU（Floating point Processing Unit for Graphics：画像処理用浮動小数点演算器）の設計を行った。ここで、G-FPUの特徴について簡単に述べる。

G-FPUにはデータの読み書きに必要なポートを複数備えたマルチポートレジスタを採用している。また、加減算、乗算、除算、開平演算、および、入力された値を２倍にして出力する演算をそれぞれ専用のハードウェアでサポートしている。このことにより､「加算と乗算」というように複数の演算を同一クロックで行うことが可能である。また、乗算器、除算器及び開平演算器には冗長２進アルゴリズムを採用しておりそれぞれの演算を従来の２進数体系での演算よりも高速に行うことが可能となっている。マルチポートレジスタと独立した演算器を搭載することにより、複数のデータの演算を同時に行うことができるようになり、画像処理全体で必要なクロック数を大幅に削減し、高速処理を可能にしている。

XMLを用いた教育用コンテンツ配信の方法に関する研究
—高知大学ラジオ公開講座のポッドキャストによる配信—

数理情報科学専攻　情報科学講座　吉田勝彦

現在、インターネットの普及により時間や場所などの環境を選ばずに情報の発信が可能になってきている。教育の分野においても、講義内容の要約や教材をウェブページとして提供するだけでなく、音声や動画を配信する例が増えてきている。従来、新しい教材が利用可能になったことを受講生に知らせるには、メールマガジンなどが使われてきた。一方、XML (Extensible Markup Language) の普及により、これを用いたコンテンツサービスも広がってきており、教育面への応用も模索されている。本論文ではXMLを用いたポッドキャストを利用して、高知大学の生涯教育番組である「高知大学ラジオ公開講座」の配信をおこなうシステムを構築し、その効果を検証した。

高知大学では2005年7月からラジオ公開講座として高知県をテーマにした生涯学習の講座をラジオ放送で行っており、同10月からは通常のラジオに加えて、従来の音声データファイル配信であるストリーミング形式の配信と、ポッドキャストによる音声ファイル配信を開始した。

高知大学ラジオ公開講座のポッドキャスト配信ではウェブブラウザから手軽に講座情報や講座題目情報を投稿できるシステムを構築、運用している。アクセスログから判明した受講者数は配信開始直後の増加と減少を経て、徐々に増加しており、ラジオ放送の受信できない海外から利用者の声もあった。

配信開始から利用しているシステムは講座題目情報を投稿した際に静的配信データファイルを生成する構成のため、リクエストパフォーマンスは非常に良いが、ポッドキャスト配信の最低限の機能しか持ち合わせていない。そこで、CMS　(Content Management System) のZope/Plone/COREBlogを利用したシステムを構築、提案した。Zopeはオブジェクトデータベースを備えたウェブパブリッシングシステムであり、Plone, COREBlogはZope上で動作するプラグイン（プロダクト）である。Ploneの持つ検索機能、講座題目情報の投稿者と最終的な公開承認者を分けるワークフローの機能などを利用することができた。

また、すでに稼働しているシステムからZope/Plone/COREBlogのシステムへ移行するPythonスクリプトを作成し、移行する事が可能となった。

以上の研究を通じて、オープンソースCMSの利用によって、従来よりも安価に十分な機能を備えたポッドキャストシステムを構築できることが明らかとなった。