

高知大学理学部数理情報科学科

情報科学コース

2007年度卒業論文要旨

伊藤研究室 2007 年度卒業論文要旨

自律型ロボットの移動計画問題における 重み付け幅優先探索アルゴリズムの研究

山北 吉郎

自律型ロボットの移動計画問題においては、自由空間を台形分割して、道路地図を作成し、幅優先探索アルゴリズムを用いて移動経路を探索する。本研究では幅優先探索における探索優先順位を枝の長さによる重み付けで制御する研究を行う。

プレゼンテーション・リハーサル支援環境における レビュー支援方法

宮脇 剛志

プレゼンテーションは発表者のもつ知識を他者に伝達するためのコミュニケーション手段であると同時に、他者からの指摘や批評を得ることで、発表に関連する知識の修正・再構成による洗練化を行う機会でもある。本論文では、プレゼンテーション・リハーサルにおけるピア・レビュー作業を効果的に行うための支援環境の構築について、特に発表者によるレビュー結果の再考を目的とするバックレビュー支援環境に関する検討とプロトタイプシステムの実装、および、その試用による検証実験について述べる。

MRTG によるネットワークトラフィック監視システムの研究

高野 健一

高知大学理学部情報科学コースにおいては 2006 年 4 月の教育用システムの更新に伴ってネットワーク構成の変更を行った。新ネットワークでは、各研究室ごとにゲートウェイ・サーバが配置されているため、SNMP によるトラフィックの把握が容易である。本研究では SNMP/MRTG を用いてネットワークを監視するとともに、18 台のサーバの 41 個のインタフェースの状況を一目で把握できるようなウェブインタフェースを構築した。

Web サーバログ解析によるセキュリティリスクの評価

小山 貴和子

高知大学理学部情報科学コースの Web サーバログから、不正アクセスあるいはその試みと思われる記録を取り出し、それらの種類・発生時期・アクセス元の国などを調査した。本コースの Web サーバでは、仮想ホストを用いてログの分別を行っているため、不正アクセスはデフォルトの仮想ホストに相当するログにのみ記録されていた。不正アクセスの種類としては、オープンプロキシの判定、メールの不正中継、phpMyAdmin や WebDAV の脆弱性を狙ったものが見られ、いずれも不成功に終わっていた。またアクセス元は中国が約半数を占め、次いでドイツ・アメリカなどであった。

メールサーバログ解析による SpamAssasin の効果について

新山 正樹

高知大学理学部情報科学コースのメールサーバでは、SPAM（迷惑メール）を判別するために、SpamAssassin を利用しており、その判別結果は syslog を通じて記録される。本研究ではその記録を元に SPAM メールとして判定される特徴を解析した。SPAM でない通常のメールの到着数が時刻・曜日によって特徴あるパターンを示すのに対し、SPAM メールは時刻・曜日を問わず到着していた。また、隔離されている SPAM スコアの高いメールでは、ベイズ確率が高いものや、空白の比率が多いもの、何らかのブラックリストに登録されているものなどが多数を占めていた。

MTSAT 気象衛星画像の幾何変換プログラム

林田 雄一郎

高知大学気象情報頁は 1994 年から継続して静止気象衛星ひまわりの画像をインターネットに提供している。2005 年 7 月より現在の MTSAT が運用されるとともに、画像形式に大きな変更があった。本研究では新しくなった画像形式の仕様について調べるとともに、地理座標系（緯度経度座標）への変換を Python プログラミング言語で実装した。また、Python はインタプリタ言語であるため多数の画素について繰り返し計算を行うと計算速度が極端に遅くなる。このため、繰り返し計算の部分を Python C/API を用いて C 言語に置き換えた。

PHP テンプレートシステム (Smarty) を用いた 大学教育支援システムの試作

菊本 淳美

毎年学期始に学生は履修登録を行わなければならないが、窓口が少ないため混雑したり、OCR の読み取りミスを考慮した確認と再提出など煩雑な手続きとなっている。本研究では大学における履修登録に Web を利用することを考え、そのためのプログラムを試作・開発した。実装にあたりプログラミング言語として近年 Web システムに広く利用されている PHP を用い、また Web デザインとシステムデザインを分離するためのテンプレートシステム (Smarty) を利用した。

キャッシュの付加によるマイクロプロセッサの性能向上と設計

市橋 祐太・近藤 司・松本 圭司・美谷 辰悦・山田 悠貴

RISC 型マイクロプロセッサ MIPS の設計を CPU にキャッシュを付加した構成で高性能化を図り，Verilog-HDL ハードウェア記述言語を用いて実現した．

HDL（ハードウェア記述言語）を用いた 浮動小数点プロセッサの設計（改正版）

川口 大輔・山本 訓影

浮動小数点プロセッサを機能ごとに設計を行い，HDL 記述により実現した．

最短路検索ツールの開発

近本 智輝

グラフ理論の応用として、一般道と高速道路からなる道路地図において最短路を検索させるツールを VisualBasic を用いて開発した。ツールでは、距離、所要時間、燃費と高速料金を加算した必要経費など、多様な検索も可能である。本卒業論文ではその開発報告を行っている。

RSA 暗号の理論とその Python による実装

加藤 慎一

本卒業論文では、まず代表的な公開鍵暗号である RSA 暗号の設計理論を展開し、次いでその鍵生成器、暗号器、復号器を Python を用いて実装し行った検証実験の報告をしている。

連分数法を用いた RSA 暗号の解読実験

前田 純

RSA 暗号に対する主要な攻撃法である素因数分解アルゴリズムのひとつに連分数法がある。これは公開鍵 n の平方根の連分数展開を利用して n の素因数分解を試みる方法である。本卒業論文では連分数法を Python を用いて実装し行った数値実験の報告をしている。

楕円 ElGamal 暗号システムの構築

砂井 真大

楕円曲線暗号はその鍵サイズの小ささから近年広く研究されている。楕円 ElGamal 暗号は、群構造に基づく ElGamal 暗号を楕円曲線上に構成したものである。本卒業論文では楕円 ElGamal 暗号を Python を用いて実装し行った検証実験の報告をしている。

二分木と三分木のクロックツリーの回路規模に関する研究

下川 遥香

LSIのクロック周波数が高まり、消費電力への影響や回路規模への影響が深刻になり、小規模なクロック回路の生成が重要となる。クロック回路規模は配線と素子の総和で決まる。従って回路規模を縮小するには配線長・分木点数・段数を削減しなければならない。そこで、本論文においてクロック分木数を増やして従来の二分木と二分木以上の分木数をもつクロック回路の規模の面からの優位性について定量的な比較をおこなった。端子をランダムに配した簡単なベンチマークデータで評価したところ、三分木が二分木に比べて規模を約7%削減できた。三分木クロック回路により総量が減ると安価・小型化が期待できる。

配線間隔が可変なクロストーク回避配線手法

竹谷 啓

集積回路の微細化はDSM(Deep Sub-Micron)問題と呼ばれるナノレベルの物理現象を顕在化させる。これらDSM問題の解決は集積回路の今後の更なる性能向上に必要不可欠である。本論文は、DSM問題の1つであるクロストーク問題の配線手法からの解決方法の研究について述べるものである。ここで提案する配線手法は、クロストーク現象のみられる2つの信号配線について、配線間隔を変更することでその影響を緩和させる。いままでも、1グリッド間隔のみを広げる配線方法は提案されてきたが、本手法では、その間隔を1グリッド以上離すことができる。本手法の特徴は、距離毎の経路探索点を n 個までリストに保持し、対象となる配線からの距離を指定した値だけ離して配線経路を検索することにより実現した。

ネットリスト接続の削除と再構成による高速配置法

竹内 豪

微細化における信号遅延の詳細は、配線経路により決まるが、配線の概要情報はLSI回路上の端子位置の設計(配置設計)で見積もることができる。そこでネットリストの接続関係から各素子を周辺と内部に分類して残りをレイアウト中央に配置して再構成するという高速配置手法を提案した。単純な配置結果ではPair-wise法よりも高速な処理結果が得られた。また、解の品質に関しても、厳密解との差異が平均で10%程度とかなり良好な結果を得ることができた。

距離最短とビア数削減を目指した多端子配線法

渡邊 真規

LSI 製造技術の向上により電子回路の微細化が進み，配線長に起因する信号遅延が増大している．配線経路において折れ曲がりがあると，高抵抗なビアが挿入されるため，より高速な信号伝播のためには短距離で折れ曲がりの少ない配線が求められる．そこで著者は，配線領域にラベル付けをおこない最短となる擬似スタイナー点と経路選択および経路探索のラベル多重化による折れ曲がりの少ない配線手法を提案する．本手法の特徴は，多端子の擬似スタイナー点と部分経路における L 型経路について最適に選択する点である．実験の結果，より配線長の短い多端子配線が確認できたので報告する．

クロストークを回避する配置評価の検討

吉田 佑馬

高性能な電子機器の重要部品である LSI 製造の微細化が進められている．一方，LSI 製造の微細化は，クロストークや電圧降下など様々な物理現象を顕在化して不良品問題を起こす．本論文は，配線パターンに起因して生じるクロストーク問題に注目し，その回避設計技術の提案を行うものである．従来のクロストーク回避はレイアウト設計における配線段階が主であった．しかし，配線密度が高い近年の LSI 設計において十分回避できない場合がある．本論文で著者は新たな配置設計でクロストーク回避を提案する．提案手法は，配置評価関数に特定配線間にかかわる素子配置を分離するためのペナルティ関数を導入するものである．簡単な配置問題で本手法を評価したところ，総配線長への影響が 10 % 程度で，クロストーク問題となる配線間を完全に分離できる結果が確認された．

障害物のある 2D 空間でのボール運動の Java を使ったシミュレーション

久米 亜友美

さまざまな形の障害物を任意に置いた 2 D 空間内でのボール運動を Java を使ってシミュレートした。特に、重力を入れた場合の障害物での反射の構造を正確に計算することにより、エネルギー保存の法則が維持されるようになった。

3D 調和振動子多体系の Java シミュレーション — オブジェクト指向プログラミングの理解 —

谷口 潤行

Java を使って、任意個のボールからなる調和振動子型の運動系のシミュレーションを行った。時間反転対称性を持つように差分方程式を構成することにより、長時間のシミュレーションでも安定した結果が得られた。

連結ボール運動系の安定状態としての Fullerene 模型の実現

岩佐 和恵

60 個のボールに位置情報は与えずに、Fullerene 模型の連結構造のみを設定し、連結部分に摩擦のある調和振動子型の力と、すべてのボールの間に一定の反発力を与えて、安定状態として Fullerene 模型を実現した。

万華鏡の Java シミュレーション — オブジェクト指向の観点から —

近藤 有美

Java を使って万華鏡をシミュレートした。万華鏡内の物体とその鏡による多数の像をそれぞれ一つのオブジェクトとすることにより像全体が変化するダイナミックな万華鏡が実現できた。

動物の闘争状態の Java によるシミュレーション

松尾 芳樹

Java を使って、2 D 矩形連続空間での動物の闘争状態（追いかける、逃げる）のシミュレーションを行った。ランダム運動をしているうちに一定の距離に別種類の動物が来たときに逃げるあるいは追いかけるの行動を取るアルゴリズムをプログラムした。

Java による L-System の実装

村松 正規

Java を使って、L システムの実装を行った。記号とその解釈を一つのオブジェクトとして表し、文をオブジェクト列として表現した点に特徴がある。特に非決定性文法による確率的 L システムの実装に重点を置いた。

Java による L システムシミュレーション

— フラクタルを一例として —

鈴木 敬太

Java を使って、L システムの実装を行った。記号とその解釈を一つのオブジェクトとして表し、文法規則を記号オブジェクトに与え、記号オブジェクトが文を生成する機能として実現した。特にフラクタル図形の生成を中心に多数の実例を作成した。

気象画像に対する時空間変動の相関性マイニングの試み

坂口 祥太

気象画像の時空間変動の相関関係の検出を目的として、時系列気象画像の時空間変動を可視化する手法を検討した。本研究では、まず、画像をブロック化して各ブロックのテクスチャを FFT パワースペクトラムとして得、この情報を K-means 法を用いてクラスタリングした。そして、得られたクラスタ ID に応じてもとの気象画像のブロックを着色することによって、クラスタ情報と雲のパターンを同時に可視化することを提案した。

地球観測衛星による植生指標データからの 長期年間変動のモデリング — ML 法, MAP 法を用いて —

吉岡 和浩

地球観測衛星による植生指標データからの長期年変動のモデリングを目的として、Honda (2006) の区分化されたロジスティック関数に対する ML, MAP 法によるパラメータ推定法を多年データへ拡張した。評価実験の結果、考案した手法は、ノイズ・欠落への耐性が強く、恣意的なデータ操作なしに安定的にモデルを求めることができた。また、オーバーラップしたセグメントをスライドさせながらパラメータ決定をすることにより、計算時間を $O(N)$ に抑えることができた。よって、データマイニングなどの大量処理に適したアルゴリズムとして構成することができた。

回路シミュレータを用いたクロストーク解析手法

黄 高

ディープ・サブミクロン設計時代の到来を迎え，LSI 内の近接配線間のクロストークが問題となっている．従来のクロストーク検出手法では，擬似エラーが多く含まれるため，検出手法の改善が望まれている．本研究で提案した動的な検出手法により，擬似エラーを取り除くとともに，回路シミュレータを用いてより正確なクロストークを検出することができる．

テストパターンに依存したクロストーク解析システム

小林 政幸

半導体製造技術の微細化が進み，近接配線間の信号干渉がクロストークという現象として問題になってきている．従来は，対象回路の静的タイミング解析を行うことによりクロストークを検出していたが，この手法では多くの擬似エラーも検出される．本研究は，論理シミュレーションによりテストパターンによる動作を考慮したクロストークを解析するため，擬似エラーを検出することなく詳細な解析を行う．

暗号化アルゴリズムのハードウェア化手法の提案

趙 朔

社会の高度情報化に伴い，データをより安全に保護するための暗号技術が重要になっているが，データ量の増加に伴い計算機処理時間の増加が問題となる．本研究では，標準暗号技術の 1 つである DES 暗号処理の高速化を目的としたハードウェア化手法を提案する．ハードウェア化手法としては，ソフトウェア言語で記述された暗号アルゴリズムを元にハードウェア化を行い，さらにパイプライン化による高速化を行い，実現性を評価した．

暗号化アルゴリズムのハードウェア化手法の性能評価

松永 惇弥

ソフトウェア処理では大規模なデータを暗号化処理する場合に長時間を必要とする。本研究は暗号化アルゴリズム DES の一部についてハードウェア化による高速化を検討し、論理シミュレータによりその性能を評価した。

検査データを用いたデータ解析手法の提案

山下 真

近年、蓄積された医療情報の有効活用が求められている。本研究では血液検査データを用いて投薬による検査値の変化を調べる手法を提案した。さらに、提案手法を用いて抗うつ薬 SSRI の一種であるデプロメールが患者に与える影響を調査した。解析の結果、投薬により検査値 GOT,S-CL,GPT,LDH が増加し、CRP が減少することがわかった。

森研究室 2007 年度卒業論文要旨

キー入力リズムによる個人認証について — 習熟度を限定した場合の特性について —

小谷 洋平

本研究はタイピングの習熟度を限定して、個人認証を行った。前年度の「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」(重岡有貴 2006年)をもとに、認証を行う範囲について、更に広範囲の文字に対して有効な認証についての特徴が現れるのかを目的にし、実験を行った。まず、タイピング習熟度の高い被験者を対象に実験を行い、その結果本人拒否率は0%、他人受入率は3.11%となった。課題として他人受入率を改善する必要があることが明らかになった。

ファジィによる自走式倒立制御装置の製作 2 — ハードウェア編 —

高橋 朋大・田中 崇洋

本卒業論文は、本研究室で行った卒業研究「ファジィによる自走式倒立制御装置の製作」で使用するハードウェアとして候補に挙げた、加速度センサ、ロータリエンコーダ、モータ、ギヤの比較及び選定について述べている。また、ハードウェアとH8との連携について述べている。そして、選定した後に実機製作にとりかかり、本研究と先行研究との比較し、先行研究からの改良点を述べると共に実験中に新たにでてきた問題点について述べる。

ファジィによる自走式倒立制御装置の製作 2 — ソフトウェア編 —

深田 耕司・山本 明寛

本卒業論文では、「ファジィによる自走式倒立制御装置の製作2 - ソフトウェア編」に使用しているH8の制御ソフトウェアについて記述している。また、LUT作成のためFDLによるプログラミングを行うため、ファジィ推論の説明として、型・メンバーシップ関数についての説明を記述している。本製作で用いた入出力デバイスはモータ、ロータリエンコーダ、加速度センサであり、それらとH8との連携についてソフトウェア上での処理を中心にそれぞれまとめた。また、加速度センサがモータから受けるノイズの対処方法を含め、各センサの処理や実験についてまとめた。