

高知大学理学部数理情報科学科

情報科学コース

2009年度卒業論文要旨

伊藤研究室 2009 年度卒業論文要旨

経路探索における距離の短縮化

内田 優太

## 岡本研究室 2009 年度卒業論文要旨

### 教育・学習支援システムにおける ユーザ操作履歴の活用方法の検討

白山 裕美子

教育工学分野における研究開発においては、教育支援システムのユーザ操作履歴をシステムの評価やユーザの行動の分析などに利用する試みが行われている。しかし、これらの先行研究では特定の機能や事象、入力デバイスなどに限定したものが多く、他の教育支援システム開発者が容易に利用できる方法を提案する例は少ない。本研究では、教育支援システムが提供する任意の機能の有効性の検証を目的とし、一般的な PC の標準入力装置であるキーボードとマウスの操作履歴のみに着目して、これらの組み合わせによる操作系列を統計的に評価・利用する方法を提案した。

### 研究の進捗状況に着目した知識継承支援に関する研究

杉原 勇太

大学の研究室などの研究グループにおいては、その活動の継続性を保持し、より良い成果を挙げるために、新たに加わったメンバに対する知識の継承が重要な問題であり、この問題に対するアプローチの 1 つとして研究ポータルに関する研究がある。本研究では、プレゼンテーション資料に着目し、完成された成果資料のみでなく、途中段階の成果物も併せて収集・蓄積して利用することにより、研究の進捗状況に着目した知識継承を行う方法の検討と試作を行った。

### アプリケーション間通信に着目した 市販ソフトウェアの教育的利用

徳永 勝也

ソフトウェアの中には、Microsoft 社の Office など、社会全体に広く認知され一般に普及している市販ソフトウェアがある。これらは、教育の場で日常的に利用されており、しばしば、それらを使いこなすこと自体が目的とされる場合もある。一方、教育工学の分野においては、教育のための独自の支援機能をもつソフトウェアの研究開発も盛んに行われているが、その独自性ゆえに普及が難しいことが知られている。そこで、本研究では一般に普及しているソフトウェアを用いながらも、補足的に教育的な支援を実現することが可能な、IAC 技術の教育的利用の提案と試作を行った。

## 暗号メールの現状と課題

村居 祐宜

インターネットメールを利用する上で、送信者のなりすましや、メール転送経路における盗聴を避けるためには、暗号の利用が不可欠である。PGP と S/MIME による技術は確立されているが、実際には暗号メールは普及していない現状である。ここでは、メールソフトとして Thunderbird をとりあげ、これら暗号メールの利用方法を検証することによって、普及の妨げとなっている要因を考察した。今後、教育現場での積極的な利用など暗号に触れる機会を増やす必要がある。

## 迷惑メールの傾向と対策について

善家 梨奈

迷惑メール (spam) 受信専用メールアドレスを Web 上に公開し、受信されたメールの SpamAssassin による判定項目の統計と、spam 送信 IP アドレスの統計を取ってその傾向を調べた。送信 IP アドレスの統計では 1 回だけ送信して以後は 2 度と送ってこないケースが圧倒的に多く、Greylisting による spam 対策が有効であることが示された。

## 地上気象観測データの DB 化と衛星画像検索への応用

小野 裕明

「高知大学気象情報頁」に蓄積された衛星雲画像を検索するには、どのような気象状況であったかを把握する事が重要であるが、画像自体からはそのような情報を知る事が困難である。このため、気象庁で公開している過去の気象データをデータベース化する事で、画像検索に応用する事を試み一応の成果を得た。

# **Xgrid を用いた長時間アニメーションの制作**

**梶原 裕一**

気象衛星画像のアニメーション化のために、分散計算環境である Xgrid を応用する事を試み、計算の分割化にいくつかのパターンを適用することで、Xgrid のボトルネックとなる要素を洗い出した。Xgrid の制限事項としては、入出力の上限が 2GB であることの他に、計算の（中間）結果を入出力するための NFS プロトコル (UDP 又は TCP) の問題があるが、これらの問題を解決しても最終的に結果が単一のファイルシステムに格納される際の出力がボトルネックとなっていた。

# **動的生成される Web ページの脆弱性について**

**鳥谷 英里子**

CGI や PHP などの動的に生成される Web ページにおいては、書き込み権限者の認証を Cookie に保存しているため、不用意に Javascript を実行されるとその情報が外部に漏れる恐れがある。クロスサイトスクリプティングは脆弱性としてよく知られているが、実際にはその影響が過小評価されることが多い。ここでは、簡単な認証を行う動的生成 Web ページを実際に作成し、どのようにしてクロスサイトスクリプティングによって Cookie が漏洩するかを実証実験した。

## 複数多項式二次ふるい法における最適なパラメータの解析

大西 佑輝・木下 泰彰・玉本 義典・西岡 努

RSA 暗号等の公開鍵暗号が基づく素因数分解問題に関し，素因数分解法のひとつである複数多項式二次ふるい法を取り上げ，これを Python により実装して数値実験を行った．複数多項式二次ふるい法には3つのパラメータが用いられるが，その最適な組合せを入力サイズから推定することに成功したほか，Python の言語仕様に基づいて掃き出し処理部分を改良することで実行時間を大幅に短縮することにも成功している．

## LSI 配置の ECO 有効範囲の特定法

杉本 聖

電子器機のコア部品である VLSI 設計で設計修正が必須となりつつある。これは微細化で設計規模が増大し、設計変更や、ミスおよびタイミングエラーなどが多発するためである。これら設計修正を、効率よくする一部修正でおこなう ECO (Engineering Change Order) が注目されている。

一方、ECO を設計段階のどこでおこなうべきかは、設計コストや期間に重大な影響を及ぼすが、これを判定する技術は提案されていない。そこで著者は、配置 ECO における改善値、改善場所、改善範囲について調べその判定方法を検討する。

本論文で、ランダム配置を利用して配置 ECO 改善値を推定した判定法を紹介し、ECO について設計段階の「どの段階で修正するか」「どの領域を修正するか」について最適化のための推定方法の基本技術について述べる。

## 配線形状を考慮したクロストーク回避配置手法

寺田 翔太

近年の電子機器の高性能化のため VLSI の微細化がすすんでいるが、それに伴ってクロストークやエレクトロマイグレーションといったさまざまな物理現象が起きている。

本論文で、著者は、物理現象によるクロストーク問題を回避するための新設計手法について述べる。本研究が提案する配置設計におけるクロストーク回避の精度を改善するため詳細な配線形状を考慮し、他の配線設計へ影響が少ない配置モデルを構築する。実証実験として簡単な配置モデルで評価したところ、総配線長の増加が 1 % 程度まで抑えられることがわかった。

## 3 分木クロックツリーのスキュー評価

細木 一生

LSI の同期式回路設計でタイミング制御をおこなうクロック回路は、LSI レイアウト設計の全領域にわたりフリップフロップに遅延差 (クロックスキュー) なしでクロック信号を供給しなければならない。一方、回路規模や消費電力の改善も必要となる。

本研究では三分木構造のクロック回路により、従来の二分木構造に比べ小規模なクロック回路設計法の確立を目指している。本研究では、この三分木クロック回路と二分木回路のスキューを実験で評価する。遅延時間計算プログラムをエルモアモデルで構築し、クロック回路の配線から各遅延を求めたところ、三分木の遅延差が、二分木より約 20 % ~ 59 % 小さくなることがわかった。また、45 度多層配線をもちいることで、より効果的な三分木回路ができることが判明した。

# パッケージ配線の検討

有田 順平

BGA などのパッケージ配線は、一層配線が主流で人手で行っている。これは配線層数が限られ、端子位置が一部自由に設定できるなど配線モデルの特殊性のためである。しかし、パッケージに搭載する素子数が増大すると人手配線は難しくなる。

そこで本論文では配線長と層数を最適化する多層配線アルゴリズムについて検討をおこなう。ここでは、配線の特殊性を評価関数で扱う方法として、配線折れ曲がりの点を素子とみなして交差数、配線長を評価する配線問題に置き換える。

提案手法を端子数 10, 25, 40 のパッケージ配線で実験をおこなったところ、処理時間が 1 秒～10 分程度で配線長削減と配線層数削減する配線結果を得ることができた。

## 回避アルゴリズム研究のための Java ツールの作成

小畠 拓也

車等がさまざまな障害物(他の車, 壁等)を自動的に回避するためのアルゴリズムのシミュレーション研究に使えるソフトウェアを JAVA アプリケーションとして作成した. このアプリケーションでは, 回避アルゴリズムを記述したクラスは後からいくらでも追加できるようになっている. これは JAVA のメタクラス機能すなわち Class クラスを用いて実現している. また, 車や障害物は任意に複製配置できるが, これは JAVA の Cloneable 機能を使っている. さらに, 回避行動の状況をファイルに保存することができ, 後から再現できるようになっている. これは JAVA の Serializable 機能を使って実現している. なお, 実際に試した回避アルゴリズムは進行方向の推進力, ハンドル操作による進行方向に直交する力, ブレーキ力を回避対象に応じて簡単な規則で制御するものを用いた. 実用には程遠いが, 面白い JAVA アプリケーションができた.

## 追跡アルゴリズム研究のための Java ツールの作成

園田 雄介

ミサイル等がさまざまなターゲット(固定目標, 他のミサイル等)を自動的に追跡するためのアルゴリズムのシミュレーション研究に使えるソフトウェアを JAVA アプリケーションとして作成した. このアプリケーションでは, 追跡アルゴリズムを記述したクラスは後からいくらでも追加できるようになっている. これは JAVA のメタクラス機能すなわち Class クラスを用いて実現している. また, ミサイルや固定目標は任意に複製配置できるが, これは JAVA の Cloneable 機能を使っている. さらに, 追跡行動の状況をファイルに保存することができ, 後から再現できるようになっている. これは JAVA の Serializable 機能を使って実現している. なお, 実際に試した追跡アルゴリズムは進行方向の推進力, 方向舵の操作による進行方向に直交する力, ブレーキ力を追跡対象に応じて簡単な規則で制御するものを用いた. 実用には程遠いが, 面白い JAVA アプリケーションができた.

## グラフの offensive alliance に関する研究

江藤 量平

本論文では、次数が偶数である頂点を含むグラフの offensive alliance number に対して既存の結果よりも良い上界を与えた。また、サイクルの square で表わされるグラフの offensive alliance number を決定した。

## Favaron 達の定理の証明の訂正

篠原 綾

Favaron ら [Discuss. Math. Graph Theory 24 (2004), no. 2, 263-275] は頂点数  $n$  個の木の strong offensive alliance number が高々  $3n/4$  の切り上げになると示している。本論文ではその証明の誤りを指摘し、正しい証明を与えた。

## 最小次数が 2 以上のグラフにおける strong offensive alliance について

田中 敦士

本論文では、最小次数が 2 以上のグラフの strong offensive alliance number に対して新たな上界を与えた。これは次数 3 の頂点数が全頂点数の  $1/4$  未満であるとき、既存の結果を改善するものとなっている。また、本論文では下界に関する考察を行った。

## 本田研究室 2009 年度卒業論文要旨

### 植生指標の時空間変動マイニング

— Xgrid による高速化と不適合データの決定木によるフィルタリング —

上田 英之

最尤法, MAP 法による植生指標の長期年間変動のモデリングには, ノイズや欠落への耐性が強いものの, 1-10 万回の反復計算を要しグローバルデータへの適用が困難であるという問題があった. 本研究ではその対策として xgrid による分散処理と決定木学習による不適合データの事前フィルタリングを検討した. 前者についてはエージェント数 16 で約 9.3 倍の高速化が確認された. 後者については 95 % の不適合データの除去が実現されたが, 適合データについては 50 % の誤認識と見落としを生じた. この問題に対しては今後時系列データの区分化などの対策が必要と考えられる.

### 月周回衛星「かぐや (SELENE)」 ハイビジョン映像参照システムの構築

國廣 賢史

月周回衛星「かぐや (SELENE)」に搭載されたハイビジョンカメラは 6.3TB に及ぶ月と地球の映像を取得した. 膨大な映像のフレーム画像への効率的なアクセスを実現するためにデータベースと連携した「かぐや」ハイビジョン映像参照システムを構築した. 本システムではユーザ認証機能により, ユーザのアクセスレベルによってクレジットや圧縮状態などが異なる画像を提供することが可能となった.

## ソーシャルデータに基づく学術書籍の難易度推定アルゴリズム

入野 美弥

情報推薦手法として協調フィルタリングが一般的に用いられているが、これはユーザの嗜好情報に基づいて推薦を行うものである。推薦対象を学術書籍とした場合は、嗜好に基づくだけでなく、その分野におけるユーザの習熟度に応じた適切な難易度の書籍を推薦したい。そこで本研究では、一般的な協調フィルタリングと同様に、誰がどの書籍を読んだかという関係を示すソーシャルデータのみを用いて、学術書籍の難易度の推定を試みた。

## 読書習慣化支援のための読書履歴取得方法

大林 高明

本研究では、メンタリングによる読書習慣化支援を目指し、読書履歴取得方法の検討を行っている。メンタリングを行うにはユーザの状況をリアルタイムに把握する必要がある。また、ユーザに読書履歴を毎次登録させることは習慣化を目指すユーザにとって大きな負担となる。そこで本研究では Eye-Fi や PSoC を利用したしおり型読書履歴記録デバイスを開発し、本を開いた時間情報を自動的に読書習慣化支援システムのデータベースへ登録する機能を実装した。

## ソーシャルブックマークにおける目的に応じた ブックマーク再利用促進機能の実装

田所 亮

ブックマークを Web アプリケーション上に保存できるソーシャルブックマークサービスでは、ブックマークの分類方法としてタギングが用いられている。しかし、ブックマークの再利用に対する支援については十分に検討されていない。そこで本研究では、ブックマークの再利用時には必ず目的があることに着目し、目的に合わせたグルーピングによるブックマーク管理を提案する。また、提案したブックマーク管理を実現するプロトタイプシステムを実装した。

# 時間表現の持つ意味を考慮した日付・時刻モジュールの設計

田谷 知子

一般的なプログラミング言語で標準的に提供されている時間を扱うライブラリ群では、日付や時刻の表現（時間表現）に整数値のみを用いる。しかし、時間表現の中には“中頃”など整数値では表現が困難なものも存在する。そこで本研究では、時間表現をそのままの意味で取り扱うことを目的に、新たな日付・時刻モジュールの設計を行った。まず、時間表現を対象概念や補足概念に分類し、軸や時点、目盛などを定義した。そしてそれらを基にクラス図の作成を行った。

## 配線間距離に起因するクロストーク遅延変動の解析手法

仙頭 航

半導体の微細化に伴い従い顕著になってきたクロストークの問題をレイアウト前段階で回避する方法について検討した。レイアウトにおける隣接配線長および配線間距離とクロストークに起因する遅延時間の増加割合を回路シミュレーションにより計測した。この実験結果を基に、隣接配線長と配線間距離からクロストークによる遅延時間増加割合を算出する式を導出した。

## 暗号化アルゴリズム AES の FPGA 化による性能評価

坂本 文昌

本研究では、暗号化アルゴリズム AES のソフトウェアアルゴリズムを FPGA に実装する際のハードウェアアルゴリズムの提案およびハードウェア化の課題を明確にして解決方法を示した。また、FPGA を使用したハードウェアの実装方法を提示し、その性能についても評価を行った結果、ARM プロセッサ上のソフトウェアと比較すると約 160 倍の性能向上を達成できる見通しを得た。

森研究室 2009 年度卒業論文要旨

手話認識用データグローブの改良

明神 有紀

自走式倒立制御装置の製作 4

— センサ・駆動系 —

原 久美子

自走式倒立制御装置の製作 4

— 内部処理系 —

西尻 良介

FDL 統合開発環境の開発

森池 桃子