# 高知大学理学部数理情報科学科

# 情報科学コース

# 2006年度卒業論文要旨

**伊藤研究室 2006 年度卒業論文要旨**

# 自律型ロボットの移動経路の改善

**假 野 貴 史 ・西 野 圭 一 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。本研究ではこれにより得られる移動経路をベースとして、これの改善を行う。

# 自律型ロボットの移動計画アルゴリズムの検証

**岡 上 広 志**

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。これをＣ言語で実装し、いくつかの例で移動経路が正しく求まる事を検証する。

# 菊地研究室 2006 年度卒業論文要旨

## ネットワークを利用した大学教育支援システム (1)

— シラバスの参照とデータベース化 —

**石 川 善 幸**

学生の立場から大学教育を見たとき、習得単位数のチェックは卒業・資格取得の可否に直結するため非常に重要である。このため、学生の立場での大学教育支援システムの構築を目指した。本論文では、その第一歩として公開されているシラバスから授業題目と単位等のデータベース化を行った。高知大学電子シラバスは授業コードが同じであれば実施年度が違っても同じ URL になっている。年度の違いは Cookie を使っているため、プログラムの作成では工夫が必要であった。

## ネットワークを利用した大学教育支援システム (2)

— 履修登録支援システム —

**吉 田 俊 雄**

履修登録は単位取得の前提となるため、学生にとって重要な手続きであるが、十分なチェックを行う時間的余裕が無い。一般に利用されている Cookie を用いたショッピングカートモデルを適用して、授業時間割・シラバス・単位によるチェックを行える学生用履修登録支援システムを構築した。

## ネットワークを利用した大学教育支援システム (3)

— 授業支援システム —

**西 山 裕 太**

大学教育において、授業の資料を配布することがあるが、欠席による配布漏れなどの問題が生じる。資料を PDF で準備することを前提に教員・学生双方にとって利便性が高く安全な配布方法を、Plone によって実現することを試みた。

## 就職活動支援ポータルの構築

**山 野 洋 嗣**

学生の進路選択の場として就職活動が重要になってきていることから、 Web 技術の中でも近年注目されている Content Management System の応用として、大学・就職学生と学生有志による就職活動支援団体（就活会）の三者相互の情報共有ツールとしてのポータルサイト構築を行った。

# Pythonを用いたデータベースについて

伊藤良

オブジェクト指向言語である Python においてデータベースを利用する場合、標準ライブラリの Pickle を使う方法、 ZODB など Python に特化したオブジェクトデータベースを用いる方法に加えて、近年、標準的な SQL データベースを使う Object-Relational Mapper の手法が注目されている。本研究では、これらの方法を比較検討した。

# メールアーカイブのウェブ表示方法に関する研究

新谷諒太

メーリングリストは古くからある、コミュニティ向けの情報交換手段であり、そのアーカイブをウェブで利用することで新しい情報メディアとの融合が可能である。一方、Web2.0 として注目を集めている技術の一つに AJAX (Asynchronous Javascript XML) がある。 AJAX ライブラリのひとつである MochiKit を用いて、メールアーカイブ表示方法を拡張することを試みた。

# Google Earthを用いた衛星雲画像表示の方法について

舛田純平・村上圭太

従来、主に教育用の観点から VRML を用いた衛星雲画像の立体表示を試みてきたが、 VRML ブラウザの普及が進まず利用に不便をきたしていた。一方、新しい形態の地理情報システムとして Google Earth が注目されてきているため、これを用いて衛星雲画像を表示することを試みた。 VRML と比較するとモデルの表現に制限があるが、教育用などの目的では十分利用可能であると思われる。

# ハイブリッド暗号 ―安全性と攻撃法―

塩田研究室
太田聖秀　大槇和則　川窪康之　川野秀雄

## １．はじめに

本研究では共通鍵暗号と公開鍵暗号の利点を併せ持つハイブリッド暗号の安全性について数値実験を行ったので、これを報告する。

## ２．共通鍵暗号

暗号化復号化に同一の鍵を使用する。暗号化処理は高速だが、鍵の管理や受け渡しが困難。

## ３．公開鍵暗号

暗号化復号化に異なる鍵を使用する。暗号化に使った鍵で復号化を行うことは出来ず、片方からもう一方を割り出すことも容易には出来ないようになっている。

鍵の管理や受け渡しが容易だが、暗号化処理は共通鍵暗号に比べて遅い。

## ４．ハイブリッド暗号

共通鍵と公開鍵の欠点を補うため。２つを組み合わせ、利点を取ったもの。

## ５．DES

入出力 64 ビットのブロック暗号で、鍵サイズも 64 ビット。ビット置換と排他的論理和 XOR、非線形関数 S ボックスから構成される。解読する際はこの非線形関数がネックになる。

## ６．DES の解読法

### ６．１．差分解読法

差分（XOR）をとることにより鍵情報を除去し、非線形部分の入出力特性を利用して攻撃する。

### ６．２．線形解読法

実際に DES を解読した攻撃法。非線形関数の入出力に偏りのある部分に注目し、Ｓボックスを線形近似して攻撃する。

### ６．３．全数探索法

全ての鍵（0～$2^{56}$－1 まで）を順に試す。
専用のマシンと 10 万台の PC により 22 時間で解読されている。

TDES（トリプル DES、鍵を 3 個にし、DES を 3 度繰り返すもの）に変えることで解読に必要な時間は $2^{112}$ 倍になる。

実験では段数を落とした DES に対して差分解読・線形解読・全数探索による攻撃を行った。個人レベルの攻撃に対しては１６段 DES でも十分安全と確認できた。

## ７．ＲＳＡ暗号

公開鍵暗号のひとつであり、巨大な整数の素因数分解の困難さに基づく。公開鍵は２つの大きな素数 p,q の積 n = p×q であり、n の素因数がわかれば解読できる。

## ８．ＲＳＡ暗号の解読法

今回は『2 次ふるい法』と『複数多項式 2 次ふるい法』を取り上げた。

### ８．１．2 次ふるい法

ＲＳＡ暗号の解読法のひとつ。

$$x^2 \equiv y^2 \mod n$$

となる $x$ と $y$ を見つけるために２次式

$$f(x) = x^2 - n$$

を用いる。

### ８．２．複数多項式 2 次ふるい法

ＲＳＡ暗号の解読法のひとつ。2 次ふるい法を改良したもので、複数の２次式

$$f(x) = ax^2 + bx + c$$

を用いる。

### ８．３．ＲＳＡ暗号攻撃の現状

－１９９６年

複数多項式 2 次ふるい法により 430bit（10 進数で 129 桁）が解読された。

－２００５年

一般数体ふるい法により 663bit（10 進数で 200 桁）が解読された。

数多くの PC を用いると 512bit 程度の数なら素因数分解できてしまう。したがって、現在では公開鍵 n を 1024-4096（10 進数で 300-1000 桁）にすることが推奨されている。

## ９．まとめ

DES、RSA、それぞれに対し十分安全であることが確認できた。これにより、TDES－RSA のハイブリッド暗号も十分安全といえる。

# MISTY の差分解読法と線形解読法に対する安全性

塩田研究室
森本　憲之　鈴木　宗禎
平成 19 年 2 月 15 日

## 1. はじめに

暗号とは、送信者と受信者以外ではメッセージを読めないようにした上で通信を行うための技術。

## 2. DES

Data Encryption Standard の略称
DES は共通の鍵を用いて、平文を固定の長さで区切り暗号化を行なう秘密鍵ブロック暗号。
DES はアメリカ合衆国商務省標準局 NBS(National Bureau of Standard)が 1977 年に連邦政府関係のコンピュータデータ用の標準暗号として制定されたもので現在では NBS ではなく NIST がこれにあたる。
NBS は、DES の規格を決めるために暗号の公募を行い、IBM 社の応募案を基に作られた。現在、コンピュータの性能向上で、数万台を利用し、約 1 日で解読されるようになり、DES だけでは利用はされなくなっている。

## 3. DES に対する攻撃法

総当たり解読法…鍵の全パターンを検索する方法。
差分解読法…一定の差分を持つ平文と暗号文のペアを複数用いて解読する方法。
線形解読法…非線形処理の S-box を線形で近似して解読する方法。
我々は 1 段・3 段・6 段 DES に対して攻撃を行い、それぞれの解読に成功した。

## 4. 新たな暗号アルゴリズム MISTY

ブロック暗号に対して有効的な攻撃法に対して安全性を持つように設計された暗号アルゴリズムで世界で始めて論理的に安全性を示された。
三菱によって開発された暗号アルゴリズムで MISTY1 と MISTY2 の総称。

## 5. MISTY の安全性証明

MISTY はブロック暗号に対する汎用性の高い解読法である、差分解読法と線形解読法に対して初めて論理的に安全であることを証明した秘密鍵ブロック暗号。
FI 関数の中で用いられる $S_7$、$S_9$ の最大差分特性確率と最大線形特性確率は計算によりそれぞれ $2^{-6}$$2^{-8}$ になる。

## 6. まとめ

本研究では、MISTY が差分解読法と線形解読法に対して、十分な安全性を保持することを証明可能安全性で示した。

**豊永研究室 2006 年度卒業論文要旨**

# 直進性の高い配線手法の考察

— A Study of Straight Forward Maze Routing —

**池野 陽輔**

従来の迷路配線アルゴリズムでは，終点から始点まで隣接点に後戻り記号（トレースバックコード）を１つ設定して，配線経路を確定させる．このとき，折れ曲がりの数については，考慮されない．一方，LSI 配線の折れ曲がりは，余分なヴィア（配線層間の接続部）を必要とするが，ヴィアは製造工程で欠損しやすいため，製造歩留まりを下げてしまう．本研究は，トレースバックコードを 2 つまで多重に設定できる迷路アルゴリズムを研究し，折れ曲がりの削減された配線経路が得られることを実証した．

# 矩形操作による最短経路決定法

— A Path Searching Method based on Rectangles —

**海老江 光**

LSI の動作を決定する配線遅延は，配線長が 1 次要因である．より良い LSI 設計には，配線長の見積もりが不可欠である．本研究は，多数の端子の矩形スタイナー木を高速に作成するアルゴリズムの研究である．１次，２次隣接の端子群から矩形を構成し，その後，各辺を除去する方法で高速化を実現している．実験から，端子数 N の配線について近似スタイナー木が O(N) の手間で得られることを実証している．

# クロストーク配線法の考察

— A Cross-Talk Free Maze Routing Method —

**谷本 俊介**

LSI 製造の微細技術が進み，信号遅延の予想が難しくなっている．特に，異なる信号間のクロストーク現象は，配線間隔が近接するほど深刻化する．本研究は，クロストークを回避する配線アルゴリズムと実証実験を行ったものである．従来の迷路配線法が隣接検索のリストを 1 つもつことに対して，2 次隣接をリストとして持つことで，ターゲットの配線から 1 グリッド離れた配線経路を得る方法を提案している．本手法は，1 グリッドのみの配線経路しかない場合でも経路を検索できる．

## 配線推定法の考察

— A Study of Wire Length Estimation Methods for Multi-Terminal Net —

**張 帆**

LSI 回路の物理的特性は，レイアウト設計まで確定しない．より高性能な LSI 設計では，高精度な配線見積もり法が不可欠となる．本研究は，配置設計で用いる程度の精度で，高速に精度の高い配線長推定法についての検討である．提案手法は，多端子の分布範囲を包含する矩形の半周囲長（MBB）とプリムのアルゴリズムで得られる配線長（Prim）について，処理時間を MBB 程度で，精度を Prim 程度まで改善したものである．

## グラフ距離による一次元による高速配置法の検討

— A Quick Placement Method using Pair of One-Dimensional Placement from the Net-list Graph —

**張 い**

半導体微細化で回路が大規模化し，上流設計から下流設計まで長時間化している．また，配線抵抗の増加などで上流設計で信号遅延見積もりが難しくなってきた．本研究は，レイアウトを推定するための短時間で妥当なの新配置手法について行ったものである．提案手法は，回路の接続情報から 1 次元配置解を 2 種類得て，おのおのを x 軸，y 軸座標として各要素の 2 次元配置解を得る．提案手法を小規模で単純な配置問題に適用したところ，格段に高速化されることが見出された．

## 睡眠測定実験と睡眠判定法の考察

— A Study of Sleep Time Estimation Algorithm for Activity Monitoring Sensor Data —

**大森 雅史**

豊永研究室では昨年，就寝中のみまもりに適した非拘束センシング法として超音波動きセンサを用いた睡眠中の動きを検知する方法を提案している．しかし，得られた睡眠パターンから就寝時間や睡眠の質の分析方法が未確立であった．本研究は，前述の睡眠パターンから就寝時間や睡眠の質を見出す手法について考察するものである．睡眠周期に着目して，睡眠パターンから区間離散フーリエ変換によりそのスペクトルを求めて，その振幅の時間変化から就寝時間を推定するアルゴリズムを試作した．

# 中込研究室 2006 年度卒業論文要旨

## 3D 調和振動子系の Java シミュレーション

赤松 将之

Java を使って調和振動子型運動アルゴリズムを持つ任意個数の球体よりなる３ D 調和振動子系のシミュレーションを行った.

## Java による株式市場のシミュレーション

石本 直也

Java を使ってそれぞれの行動パターン（売買アルゴリズム）を持つ１０００人の株主の設定による株価変動のシミュレーションを行った.

## Java による食物連鎖のシミュレーション

遠藤 雅也

Java を使って格子モデルによる生態系のシミュレーションを行った.

## 車の運転の Java シミュレーション

林 佳宏

Java を使って運転手の行動パターン（運転アルゴリズム）による車の動きのシミュレーションを行った.

**本田研究室 2006 年度卒業論文要旨**

# モンテカルロフィルタと時系列データマイニング

**小 松 学**

モンテカルロフィルタは、状態・観測値とその時間変化を記述する一般状態空間モデルにおいて状態の確率密度分布を粒子の頻度で近似することにより、時間発展するシステムの性質を調べることができる。本研究では、簡単なモデルに対する数値実験より、この手法による状態・１期先観測値の予測成功確率を調べた。実験結果から、長期間のデータに対しても精度よく確率的な状態・観測値の追跡が実施できることがわかり、時系列データマイニングにおいても、状態・観測値の自動予測という点で有効であることがわかった。

# プロ野球投手年間成績のデータマイニング

— K-means 法によるクラスタリングと選手起用法への応用 —

**森 将 人**

2005 年度のセ・リーグ野球投手年間成績に対してデータマイニングの手法の一つである K-means 法によるクラスタリングを適用し、その結果の選手起用法への応用を試みた。記録中すべての属性を利用した実験からは、先発、中継ぎ、その両方など試合での起用のされ方に強く影響を受けた 11 クラスタが得られた。この結果と個人の能力でのクラスタリングとの対応付けから、特別な起用方法（先発エースなど）に対する潜在能力をもつ選手を発掘できる可能性がわかった。

# Actor の適性度の履歴を用いた Actor-Critic アルゴリズムの検証

**市 原 貴 英**

強化学習のアルゴリズムの一種である Actor-Critic 法は、方策に基づき状態から行動を決定する Actor と、行動の良し悪しを判断して Actor へ強化信号を送る Critic の 2 要素から構成される。木村・小林（2001）は改善手法として Actor の方策の修正率である適正度への履歴の導入を提案している。本研究では、線形 2 次形式制御問題において適正度の履歴の効果を再検討し、加えて初期値の変動に対する頑堅性の検証を行なった。その結果、適正度の履歴は、確かに解の収束と精度を改善する効果があるが、初期値によっては解が発散するケースもまれ (20 試行に 1 度程度) にあり、頑堅性という観点ではやや劣る部分もあることがわかった。

# マルチエージェント強化学習における Profit Sharing の有効性検証

— 追跡問題を例に —

**内 海 朋 秀**

強化学習によるマルチエージェント協調動作の獲得には、目標達成に直接関与しなかったエージェントへの間接報酬の設定や、エージェント間の役割分担の実現といった問題がある。本研究では、追跡問題を対象として、Profit Sharing における間接報酬の上限値を与える合理性定理（宮崎他 1999）の検証と、エージェントの行動順序固定による自律的な役割分担の取得を検証した。検証の結果、合理性定理は有効であるが、行動数やエージェント数が大きい問題では上限値が小さくなってしまい間接報酬を導入するメリットがほとんどなくなってしまうことが確認された。また、エージェントの行動順番を固定すると高い確率で自律的に協調動作（役割分担）を獲得することがわかった。

松枝研究室 2006 年度卒業論文要旨

## インターネット広告の制作

巣山 省太郎

## 流行曲の周波数（$1/f^n$）特性

田村 優太

## 簡易型分光器の製作

東 康敬

## ＲＳＡ暗号の速度向上と安全性

森山 賢太朗

**森研究室 2006 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

—安定点の利用—

**栗 田 了 輔**

本卒業論文はキー入力リズムにより個人認証を行った．先行研究の「キー入力リズムによる個人認証についてーゆらぎの発生とその性質ー」（山元健太　2003 年）をもとに,“ 分散 ”と“ 文字の間の間隔の速さ ”に着目し，実験を行った．まず，6 人を対象に基準値を求め，そのあとに自称キー入力の得意な人 30 人を対象に実験を行い，その結果本人を本人と認証する率は 76％，他人を本人と認証する率は 0.37％となった．課題として本人を本人と認証する率を高める必要がある．

# ファジィによる自走式倒立制御装置の製作

—センサー（入力系）編—

**吉 岡 明**

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」で使用した各センサについてまとめたものである．今回使用したセンサはロータリエンコーダとＧセンサの二つで，それぞれの用途を述べるとともに，その仕組みや種類を述べた．　次に実際にロータリエンコーダ・Ｇセンサと Ｈ８とを連携させ，またその際行った A / D 変換についての説明も記述する．その結果，ロータリエンコーダ・Ｇセンサから得られた出力について記述した．

# ファジィによる自走式倒立制御装置の製作

—制御ソフトウェア編—

**山 崎 千 尋**

本卒業論文は,「ファジィによる自走式倒立振子」の制御ソフトウェアについて記述している．ＦＤＬによるプログラミングを行うため，ファジィの説明から始まり，ＦＤＬの機能として，型・メンバーシップ関数・推論についての説明を記述している．また，ＦＤＬを用いた簡単な例のプログラムを記述し，実際にＦＤＬを記述する際の記述方法について説明している．次に，本研究実験について述べＬＵＴを実装する際の処理について述べている．

# ファジィによる自走式倒立制御装置の製作

—モーター（出力系）編—

**山崎晴彦**

自走式倒立振子のモータに関することについてまとめたものである．モータの種類を調べ，制御にはどのようなモータが向いているか，正転逆転のための回路や，ギヤの選択や，モータの回転速度を電圧を変えず，制御できるPWMの説明を記述している．　モータ制御関数の例や，簡単なITUによるPWM制御をあげている．例を基としH8でPWM出力ができるITUポートを2つ使い，正転逆転，回転速度の変更ができるプログラムを作成した．

# ファジィによる自走式倒立制御装置の製作

—ＣＰＵ（演算装置）編—

**島村圭**

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CPUとして候補に挙がった、PICとH8の比較及び選定について述べた．本研究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との連携についてそれぞれ記述した．また、プログラムの作成、H8への実装について述べるとともに、センサ情報の処理や実験についてまとめ、その際行ったRAM増設についても述べた．

# ファジィによる自走式倒立制御装置の製作

—統括編—

**今村木綿子**

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」についてまとめたものである．倒立振子は、制御の理論を実験的に検証する際に用いられることの多い題材である．そこでまず、倒立振子の説明、倒立振子モデルの種類の紹介、また従来の倒立制御とファジィ制御の相違点、及びファジィ制御を用いた利点を述べた．次に、先行研究の問題点を挙げ、その解決策を考慮し、新しく選定したデバイス、ＣＰＵを用いた本研究の全体構成を記述した．