

平成 28 年度

卒業研究要旨集

高知大学理学部応用理学科

情報科学コース

推論による情報漏えいリスクの評価手法
— アクセス確率を考慮した手法の提案 —

小笠原 凌

本研究は、秘密情報が推論によって導かれ漏えいすることを防ぐために、どの情報が推論されやすく漏えいリスクがあるのかを評価する手法の研究である。当研究室でこれまでに研究してきた漏えいリスク手法では、サブジェクトがオブジェクトにアクセスする確率が一様であると暗黙に仮定していた。しかし、現実的にはサブジェクトやオブジェクトごとにアクセス確率は異なると考えられる。本研究では、サブジェクトがオブジェクトにアクセスする確率があらかじめ与えられた際のリスク評価手法を提案し、シミュレーション実験機能も実装した。さらに、実装した実験機能を用いて、提案手法の妥当性を検証した。

推論による情報漏えいリスクの評価手法
— ハイパーグラフモデルにおける手法の提案 —

児玉 洋祐

本研究は、秘密情報が推論によって導かれ漏えいすることを防ぐために、どの情報が推論されやすく漏えいのリスクがあるのかを評価する手法の研究である。当研究室では、これまでに、有向グラフモデルと有向ハイパーグラフモデルに対する評価手法を提案してきた。しかし、有向ハイパーグラフモデルにおける従来のリスク評価手法ではリスクを求めることができない場合があった。そこで、本研究では、有向ハイパーグラフモデルを有向グラフモデルに変換して、有向グラフモデルにおける従来のリスク評価手法によってリスクを求める手法を新たに提案し、いくつかのグラフに対して提案手法の妥当性を検証した。

ペアワイズ交換法を伴う自己組織化マップによる TSP 解法

齋田 悟志

ネットショッピングに伴う商品配送などの流通網の高度化が求められている。なかでも、トラベリングセールスマン問題(TSP)解法は、商品配送のコスト削減や時間削減で重要である。本研究は、短時間に良好な解を得る TSP 解法である自己組織化マップ SOM 法の改善法を目指すもので、アンジェニオール法を基本として、ペアワイズ交換法を組み入れた新手法を提案する。実験により、アンジェニオール法でみられる経路の『ねじれ』の解消による良質な解が得られた。

バス路線改善に向けた乗客データの SOM 分析法

以西 正人

路線バスは、高齢者の移動手段として重要である。しかし、地方の路線バスの多くは赤字であり、存廃の危機に陥っている。そこで本研究は、バス経営に役立つ情報を分析するため、バス乗客データの SOM 分析法について検討する。まず擬似乗客データにより SOM 分析の特徴づけの可能性を調べ、次に、実データ(とさでん交通株式会社提供)に適用した。以上の分析の結果、乗客数に基づくバス停の分類、乗客属性自体の分類ができた。今後、これらの分析結果をさでん交通へ提供し、役立てていただく予定である。

バス路線改善に向けたバス乗客データ生成法

三戸 理誠

近年、地方のバス路線赤字が問題となっている。赤字解消のために、乗客属性の分析が重要となる。一方、本年度改正される個人情報保護法の点から、実データを自由に扱えない。そこで本手法では、ビッグデータ分析に利用可能な乗客データを疑似的に生成する方法について検討する。検討では、まず乱数に基づくランダム乗客データを試作し、その問題点を明確にし、次に実データの統計から生成する方法を提案する。提案手法の疑似乗客データと元の実データを比較したところ、ほぼ再現する統計結果となることが分かった。

オブジェクト指向で理解する有限オートマトン

藤原 尚也

有限オートマトンの定義と様々な演算をオブジェクト指向言語である Java を用いて実装した。Symbol とその集合の実装に基づき有限オートマトンの定義とそれに関する諸概念を Java クラスととして実装し、有限オートマトンの和、積、連結、閉包、決定性変換、状態最小化などの演算を実行する諸関数を実装し、さらに有限オートマトンによる語の判定システム実装した。これにより、有限オートマトンに関する諸概念がオブジェクト指向の立場から理解できるようになった。

JavaFX で見る有限オートマトン

向井 志

Java の GUI 作成システムとして最近注目されている JavaFX を用いて有限オートマトンを扱う GUI を作成した。JavaFX の特徴である Scene グラフの中に有限オートマトンの遷移図を配置することにより、有限オートマトンの定義、諸演算が視覚化され、さらに語の判定の過程をアニメーションで表すことができ、直感的理解を助けるシステムとなっている。なお、この GUI システムは藤原尚也担当の有限オートマトンプログラムと連動しており、有限オートマトンに関する諸演算はそちらで行い、結果をこちらの GUI に戻す仕組みになっている。

電子ホログラフィのための3次元物体モデル作製ソフトウェア開発

伊藤 弘紀

計算機合成ホログラム(CGH)を用いた電子ホログラフィは、究極の3次元テレビになると考えられている。しかし、電子ホログラフィによる3次元テレビを実現するには仮想的な3次元物体モデルを作製するソフトウェアが必要不可欠である。本研究では、階調を持つ3次元物体モデル、階調を持つ画像からの物体モデル、そして、深度マップからの3次元物体モデルを作製することができるソフトウェアを開発した。しかし、作製したモデルから綺麗な再生像が得られない場合があった。この問題が生じた場合、時空間分割法が有効であることが確認された。

電子ホログラフィによるDMDを用いた3次元動画の高速再生

OOI CHUN WEI

3次元物体を構成する物体点数が膨大になると、計算機合成ホログラム(CGH)による再生像の画質が劣化することが知られている。時空間分割法により高精細な3次元物体像を再生することができるが、動画の各フレームにおいて3次元物体を時空間分割するためフレーム数が増加する。本手法により高精細な3次元動画再生を実現するには動画の高速再生が必要となる。本研究では、DMDによる動画の高速再生手法を提案する。最終的に、720HzのリフレッシュレートでのCGH表示を実現し、高精細な3次元物体の動画再生に成功した。

白杖型歩行支援デバイスの開発
— 実用化に向けての検討 —

藪中 奎介

本研究室では視覚障害者の外出を支援することを目的とする白杖型歩行支援デバイスの開発を行っている。しかし、現在このデバイスは障害物の検知を行うデバイスに屋外では使用できないセンサを利用している。本研究はこのセンサを屋外の太陽光下の環境で使用できるデバイスに置換することを目指し、センサの選定とその性能評価を行う。実際に太陽光下における検知能力を試し、従来のセンサとの差異や問題点等について考察を行い、今後の研究方針について言及した。

手話における手指動作取得の高精度化
— 回転運動について —

山岸 由依

本研究室では手話学習支援システム「手話トレーニングマシン」の研究・開発を行なっている。先行研究のシステムでは、異なる手話動作であるにも関わらず同一の教師データを持つ手話単語が存在した。本研究では、こうした異なる手話動作の区別を明確に行なうため「手の回転」に注目し、手話の手指動作における回転運動の取得にジャイロセンサを導入した。検証実験ではその性能を確認し、新たな判別項目を設けることの有効性を検証・考察した。

RSA 暗号におけるミラー・ラビン素数判定法についての研究

渡邊 莉奈

代表的な公開鍵暗号である RSA 暗号の鍵生成においては、512 ビット程度の大きな素数を生成する必要がある。その素数判定には確率的素数判定法のひとつであるミラー・ラビン法が用いられることが多い。ミラー・ラビン法では複数の「底」に対して強擬素数テストを反復することによって判定精度を高めているが、判定精度と実行速度は当然トレードオフの関係にある。本論文では、ミラー・ラビン法において、用いる底の個数と判定精度の関係について研究を行った。

フェルマ法を用いた RSA 暗号の暗号解析

田中 亨志

公開鍵暗号の一種である RSA 暗号の安全性は素因数分解問題の困難さを根拠としている。すなわち、RSA 暗号の公開鍵は現在知られているいかなる素因数分解法を用いても現実的な時間では素因数分解が不可能であることが要求される。本論文ではフェルマ法と呼ばれる素因数分解法を取り上げる。これは合成数の素因数を 2 つの平方数の差から求める方法であるが、我々は平方剰余を考慮することにより更なる高速化を図っている。この改良されたフェルマ法に対する RSA 暗号の耐性について実験を行った。

混合モデルによる時系列 3 次元データからのホットスポットの自動抽出・追跡

— フェーズドアレイ気象データへの適用 —

林 諒

フェーズドアレイ気象レーダデータ等の 3 次元時系列格子データからのホットスポット自動抽出、追跡を目的として、EM アルゴリズムによる多変量正規分布の混合モデルでのモデリング手法(松岡 2016)の高精度化を検討した。先行研究では閾値を超えた格子の座標値だけを使用したため、BIC による最適成分数の選択を行っても、適切な成分数が求められない現象が確認されていた。本研究では、格子上の原データのフィールド値を用いた重み付けや初期値のランダム性の増加による改善を試みた。人工データで評価した結果、抽出成分数の正答率が大きく改善したことが確認された。

三好研究室

モチベーション維持のためのチーム機能を実装した習慣化支援スマートフォンアプリの開発

中城 将太郎

本研究室ではペアでエールを送り合うことで励まし合いながら習慣化を目指す、習慣化支援システムの開発が続けられている。先行研究にて、このシステムをグループで利用するとなると、グループの作成に時間がかかる、エールを1人1人に送る必要があるということがユーザの負担となるため、改善策としてグループでエールを送り合う機能が提案された。そこで本卒業研究では、チーム機能を新たに実装したスマートフォンアプリを開発し、長期的な評価実験を実施するための準備を行った。

スマートフォンを用いたコンテキスト適応型通知のための機械学習によるユーザの状況判別

南 祐希

本研究では、スマートフォンアプリにおいてユーザのコンテキストに応じた通知を行うことを目標とし、ユーザの状況判別機能を実装するための iPhone, Android に対応したセンサデータ収集用アプリを開発した。ユーザが所持するスマートフォンのセンサデータを収集し、それらのデータを機械学習することで、ユーザの状況判別を行うことができる。静止中、歩行中、放置中の3つの状況を定義して状況判別の評価を行ったところ、入力された1秒間ごとのデータをF値が約96%の性能で正しく状況分類することができた。

岡本研究室

プレゼンテーション・リハーサル支援システムを用いたピアレビューにおける分析と評価方法の検討

森 亜優美

レビュー支援研究においては、その有効性を検証するための一般的な評価方法は確立されていない。特にプレゼンテーション・リハーサルにおけるレビュー支援を対象とした研究事例は少なく、そのシステムの有用性を高めるためには、適切な評価方法の検討が必要である。そこで本研究では、我々の研究室で従来より開発している、指摘対象として、スライド、さらに、口頭説明を加えた2種類の視覚的提示を用いた支援システムについて評価実験を行い、その結果の比較による分析からシステムの有効性を評価する方法について検討・考察を行った。