2002.2

高知大学大学院 理学研究科 情報科学専攻

平成13年度 学位論文発表会

2002年2月12日 (火)　於 高知会館

平成 13 年度 高知大学大学院 理学研究科 情報科学専攻 学位論文発表会 プログラム

2002 年 2 月 12 日 (火)　於 高知会館

発表者	論文題目	時間
王　　帥	時空間データからのオブジェクトベース知識発見の研究 – 時系列気象画像への応用 –	9：40–10：00
岳　振輝	地下水流解析を例題とした Java Application による simulation 技法の研究	10：00–10：20
邱　　軍	XML に基づく保険情報連携システムの構築	10：20–10：40
左　風華	分散オブジェクト技術による BankMed システムの設計	10：40–11：00
森田尚亨	複素ニューラルネットワークを用いた核磁気共鳴スペクトル推定法	11：00–11：20
岩村友和	二次元における多角形のインタラクティブな操作法の基礎研究	11：20–11：40
奥　　倫	人工衛星画像を用いた海面温度分布の推定	11：40–12：00
昼休み		
窪添瑠実	バイオメトリクスを用いた追認証の提案	13：20–13：40
滝澤宏行	企業団地における無線 LAN 構築と VPN の導入	13：40–14：00
谷脇圭介	量子テレポーテーションを用いた通信の基礎	14：00–14：20
前園　淳	忘却効果を利用したニューラルネットワークの融合	14：20–14：40
今村　育	ネットワーク学習環境における教材提示支援サーバの構築	14：40–15：00
小川　実	C 言語演習を対象とした統合型教育支援環境の構築	15：00–15：20
葛目悠輔	捕食者と被食者の相互作用系のカオス – 拡張されたロトカ・ヴォルテラモデルを用いたデータ解析 –	15：20–15：40
杜　　忠	円相場のフラクタル解析 – 予測モデルの提案 –	15：40–16：00
長瀬　匠	音楽の情報理論的解析の試み	16：00–16：20
李　曦光	超楕円曲線暗号に関する研究 – システム設計とその実装 –	16：20–16：40

時空間データからのオブジェクトベース知識発見の研究

——時系列気象画像への応用——

情報科学専攻　　計算機科学講座　　氏名　王　帥

リモートセンシングやGISなどの様々な分野において、時間・空間で変動するデータ集合からのパターン発見が重要になっている。この際、空間データ内の特徴であるオブジェクト（例えば気象画像中の台風）の属性（位置、広がりなど）を抽出して時系列データとして記述できれば、より有効な時空間変動パターンの発見が可能になると考えられる。このような個々の特徴に着目した情報抽出は従来のクラスタリング方法（例えば片山 1998）では困難であった。

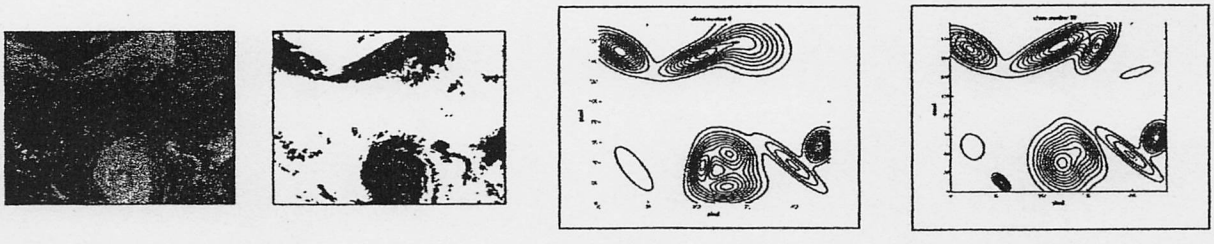
本研究では、画像内の不特定形状・不特定数のオブジェクトの分布を多変量正規分布の混合密度分布でモデル化し、フレーム画像のクラスタリング結果からオブジェクトを含む可能性が高いシーンを抽出後、EM アルゴリズムを用いて対数尤度最大化の方針に従いオブジェクトの属性を混合密度分布のモデルパラメータ（各成分の重心、分散、重み係数）をして求めることを試みた。ここで、画像中に含まれるオブジェクトの個数に相当する混合密度の成分の数はあらかじめ決定することができないため、解の精度劣化や自動化の妨害などの問題を起こす。本研究ではこの問題に対して下記の 2 つの方針を検討した。

1．　想定される最大の成分数を与えて得られた結果から重なりのある成分を統合する。

2．　複数の成分数に対して試行を行い、離散的な観測に対する確率密度分布の適合基準として有用な BIC（Bayesian Information Criterion: $-2L+d_k \log n$, L は対数尤度, d_k はモデルの自由度、n は観測点数）を最小化する解を選択する。

これらの 2 手法に対し、GMS5 による気象画像（2000 年、1997 年各 8 月分、計 1025 枚）を用いて実験を行った。平均抽出成分数は 1，2 の手法に対しそれぞれ 10.6、10.3 であり、さらに 100 枚の眼視による評価の結果、平均検出失敗成分数はともに 0.01、誤って融合されて検出された平均成分数はそれぞれ 1.45、1.3 であった。この結果は両者とも十分な性能を示し、手法間で優位な差がないことを示した。ただしより細かい検証では、図 1 に示すように統計的に有意な成分数を検出しやすいという点で BIC は有用であった。しかし BIC による検証を導入すると計算時間が数倍以上になるため、大量データからの知識発見の目的、および計算機資源の限られた状況では前者の手法で十分であると考えられる。

抽出されたオブジェクトの情報から、同一オブジェクトを認識して時空間内に関して R*-tree などの手法を用いてインデクス付けをしたデータベースを作成することにより、オブジェクトベースの時空間知識発見の基礎データを作成することが可能である。



(a)　(b)　(c)　(d)

図 1 気象画像からの抽出結果。(a)原画像、(b) は混合密度推定に用いた雲点を示す 2 値画像、(c) (d) はそれぞれ手法 1、2 で得られた混合密度分布の等高線図

地下水流解析を例題としたJava Applicationによる Simulation技法の研究

情報科学専攻　　計算機科学講座　　岳　振　輝

本研究の目的はJava Applicationによる Simulation技法を研究することである。Java Applicationの利用と Simulationをうまく表現できるようにするため、地下水流のモデルを例題にした。地下水位変化の規則をVisualで表現できるように研究することである。

Javaプログラミング言語は1995年に登場して間もなく急速広まり、一瞬にして輝かしい地位を確立した。Java言語はプラットフォーム依存しない、シンプル、オブジェクト指向など利点がある。特に、Java言語は、GUIの表現が非常に優れている。音声や動画を用いたプログラムを作成することができる。このことによって、よりリアルでわかりやすく楽しいアプリケーションを実現することができ、さらに、ユーザに対してきめ細かなサービスを提供することができる。そのため、本研究には、Java applicationを利用することにした。

本研究の動機は四国地方の高知県が地下水利用量は農業用として利用が中心である。しかし、海岸に面した平野部で地下水が大量に利用されている地域では、帯水層に海水が浸入して地下水の塩水化現象が見られる。この現象の発生の程度と規模および時間スケールは、地域における地形、地質、帯水層の構造とその水理定数・降水量などのさまざまな自然条件に規定されるとともに、揚水場所の分布や揚水量の多寡といった人為的な要因とも密接に関連している。

Simulationの手法は、Java applicationを利用し、基本データをそれぞれの性質に応じた動作を含むデータクラスとして定義し、そのインスタンスを空間を表すSpaceクラスに配置し、Cellular Automaton理論を実現することである。

以上の手法により、分かりにくく、複雑なSimulationを可視的に、ユーザの細かなサービスも対応できるようになり、複雑な数値解析もより分かりやすく理解できるようになった。

XMLに基づく保険情報連携システムの構築

情報科学専攻　計算機科学講座　　邱　軍

世界的にインターネットの急速な普及と技術革新に伴い、最大規模でかつ最もコストの安いデジタルネットワークインフラが確立されつつある。そこで、多くの企業の活動に影響を及ぼすものがインターネットでの電子データ交換である。ネット上で情報を共有し、ビジネスの効率を高め、いかに顧客に対する新しいサービスを作り出していくかが企業の抱える課題となっている。

しかし、電子データ交換に於いて、HTML文書には「構造化されたデータ」としての取扱いには困難な点がある。それは、人が介在せずにコンピュータによる自動処理を行うことが困難だということである。この限界を打破するのはXML（eXtensible Markup Language）である。XMLは、タグと呼ばれるマークを使って文書構造を記述するための言語である。データ構造をユーザが自由に定義でき、全てのデータに属性を持たせ、ブラウザなどで表示するための定義を分離したことで、コンピュータでの自動処理などに適用できる。また、システムのデザイン変更にも柔軟に対応することが可能である。

本研究の目的は、従来の企業内システムの情報統合、再利用、及びインターネットを介して企業間のシステム連携を可能とするXMLに基づく情報システムの設計と実装である。応用例として、中国に於ける保険のWEBアプリケーションを構築した。本システムの特徴は、以下のようである。

[1]ブラウザを介して検索するユーザインタフェースを提供することによって、保険の公用情報データベースをWEB経由で検索することができる。また　再利用の為、検索結果のXMLファイルを作成することもできる。

[2] 業界、関係する企業によって決められた標準のフォーマットに従い、XMLファイルをXSLT（XML Stylesheet Language Transformation）プロセッサでXSLスタイルシートを適用することで標準フォーマットのXMLファイルに変更する。これで、企業間のデータフォーマットの違いにシームレスに対応し、システム連携、情報資産の共有が可能である。

[3]関係する企業から取得したXMLファイルを、XMLパーサーで解析し、DOM（Document Object Model）ツリー構造から必要なデータを取得し、データーベースに登録する。

このシステムは、貿易金融取引に於いて、保険証書、賠償計算書や清算書のやり取りなどの手続きのXMLベース化によって、保険会社間で、また、銀行、運輸業界等の関係する企業などの組織間で、同一標準に従った内容のデータをもとに各種電子書類が作成され交換ができるように設計と実装がされている。

分散オブジェクト技術によるBankMed システムの設計

情報科学専攻　　計算機科学講座　　左　風華

インターネットを世の中に広めた決定的なアプリケーションはWWW（World Wide Web）であろう。これは最も広く普及しているクライアント/サーバアプリケーションである。現在のWWWは「すべてのクライアント/サーバシステムの母」という構想を持つ情報ハイウェイには到達していない。この非常に高い目標を達成するためには、安くて豊富な回線容量と、WWW及び分散オブジェクト技術の統合が必要である。

本研究では、大企業の集中処理から分散処理（特に本社—支社間での情報の流れを完全に自動化することなど。)へ、複数ユーザによる資源の共有、資源の遠隔アクセス、支社と本社間の非同期通信、ブラウザからの振り替え伝票データ登録、検索及び必要な帳務データを選択することができるような分散システムを考える。本研究の目的は、このようなシステムの実現によって、分散オブジェクト技術CORBAを用いてリレーショナルデータベース(RDB)、オブジェクト指向データベース(ODB)、HTMLなど異種情報源の統合という問題を解決することである。本研究で行ったことを以下に示す。

1) 分散オブジェクト技術CORBA（Common Object Request Broker Architecture）を導入したBankMedシステムのモデルを提唱した。
2) 上記のモデルにおいてCORBA Naming Serviceを用いたBankMedシステム上による、情報源のBank情報の登録・選択機能や、CORBA IDL(Interface Definition Language)で各情報源のラッパーの共通インタフエースを定義することによるRDB、ODB、HTMLなど情報源への統一的なアクセス機能、ラッパーの情報変換の機能を実現した。
3) BankMedシステムにおけるCORBA環境をJavaIDLで実装した。
4) BankMedシステムが扱う情報、RDB, ODB, そしてHTML, といった分散情報源からの同種情報の統合利用という形での実験を行い、分散情報源の統合を実現した。

分散オブジェクト技術CORBAを用いたBankMedシステムによって情報源のデータ間に存在するプラットフォーム・レベル及びデータモデル・レベルの分散性を解決し、分散情報源の統一的な利用が可能であることを示した。

複素ニューラルネットワークを用いた核磁気共鳴スペクトル推定法

情報科学専攻　計算機科学講座　　森田 尚亨

生体代謝物の核磁気共鳴（NMR）スペクトルを収集することはMRS（magnetic resonance spectroscopy）と呼ばれている．MRSでは1.5Tesla程度の低磁場下で自由誘導減衰波形（FID）を高速フーリェ変換（FFT）することにより周波数スペクトルを得ている．FIDは時間的に振動し，指数関数的に減衰していく波形成分の集合であるが，このような波形にフーリェ変換を適用すると，得られるスペクトルピークはLorentz曲線と呼ばれる形状をなす．このとき元の波形の減衰が激しいとスペクトルの強度と分解能は低下する．この結果，FFTにより得られるスペクトルピークは対象原子核が本来持っているスペクトル分布とは大きく異なったものになる．このときピークの高さを用いると正確な定量ができないので，カーブフィッティング法により各ピークの面積を推定することによって，スペクトルの定量を行っている．このカーブフィッティングは人的介入を要するため，大量のデータを処理する場合には多大な時間的浪費を強いることになる．

本研究の目的は，人的介入や複雑な計算などが不要なNMRスペクトル推定法を開発することである．そのために，学習過程が不要なHopfield型ニューラルネットワークを導入する．そして，それが持つ最適問題の極小解あるいは最小解探査能力をパラメータ推定に利用する．さらにNMR信号が複素信号であることに注目して，Hopfield型複素ネットワークよるNMRスペクトル推定法を開発する．またシミュレーション実験により開発した手法の性能評価を行う．

以下，本研究で行ったことを示す．

1．対象信号として，生体内^{31}P-NMRスペクトルの3つの異なるスペクトルパターンに対応する7つの波形成分を持つシミュレーション信号を用いた．
2．FID信号を用いる実数型ネットワークを実装，推定を行った．
3．NMR信号（複素信号）を用いる複素型ネットワークを実装，推定を行った．
4．スペクトル推定時に，FIDの波形パターンに注目した逐次区間拡大法を発案・導入し，これを併用して上記の推定を行った．
5．異なった雑音レベル（SNR=10,5,2）のNMR信号を用いて推定を行い，雑音下での本手法の能力を検討した．

実験の結果，FIDでは十分な結果は得られなかったが，適切な逐次区間推定法を併用した複素ネットワークでは，7成分中4成分に関してはほぼ正確な推定が可能であり，低SNRにおいても良好な推定傾向は維持され，複素ネットワークの優位性が示された．しかし，対象信号のパターンによって推定精度に差があり，3パターン中良好なものは1パターンだけであった．また逐次区間推定法を併用しない場合では，複素ネットワークの推定精度は低下した．本研究が用いた手法では逐次区間拡大における区間選定が重要な要素となった．汎用性のある適切な区間選定法が見つかれば，本手法はより実用的なものになると思われる．

二次元における多角形のインタラクティブな操作法の基礎研究

情報科学専攻　情報数理学講座　　氏名　岩　村　友　和

本研究は卒業研究に引き続きタングラムのようなパズルを仮想的に楽しむ為に必要となるための基本操作を開発する研究である。

タングラムの木片を多角形としてとらえ、平面上の多角形の操作法の開発として研究を始めた。又ドラッグする多角形の基本操作を平行移動・回転移動に大別して研究を始めた。多角形が接するまでは平行移動とし、接した後は回転移動させる。又、接した後、離れる方向への平行移動も必要でその判定法を研究した。

移動させる多角形をＰ、もう一方の多角形をＱとする。

平行移動においてポイントとなる処理は、Ｐをドラッグ方向に平行移動する場合のＱにぶつかる（ぶつかる点 nearest_point)までの移動可能距離(min_data)を計算する処理である。平行移動においてＰの各頂点がＱと接するまでの min_data を求めるだけでなくＱの各頂点がＰと接するまでの min_data を求めて小さい方をＰの移動可能距離（min_data）とし、ドラッグ量と対応させ最終的なＰの移動量を決定した。

以下多角形Ｐ，Ｑが接してる状態 min_data=0 の時の説明である。min_data=0 の時の平行移動は、始めは nearest_point におけるドラッグ判定を行い平行移動させていた。しかしながら、点の位置関係に基づくドラッグ判定では不十分で、ドラッグ方向の情報を用いたベクトル判定に改める必要があることが分かった。Ｐをドラッグ方向に平行移動するとき、Ｑは相対的に反ドラッグ方向に平行移動するから nearest_point において、反ドラッグ方向がＰの内部を向いているかどうかで平行移動不可かどうかを判定するベクトル判定に改めた。

回転移動においてポイントとなる処理は、nearest_point を中心にＰが回転してＱにぶつかるまでの回転可能角を求める処理である。ここでも同じようにＰの各頂点がＱにぶつかるまでの角と、Ｑの各頂点がＰにぶつかるまでの角を求め、その最小値をドラッグ角と対応させＰの回転移動量を決定した。

回転移動における改善策の説明。

ある nearest_point だけの回転可能性がなかったとしても、別の nearest_point については回転可能な場合がある為、各 nearest_point について順次回転可能性を調べることにした。

人工衛星画像を用いた海面温度分布の推定

情報科学専攻　情報処理学講座　　奥　倫

人工衛星からのリモートセンシングの応用のための研究各方面でなされており、海洋の観測にも有効であると期待されている。海上における観測点は地上に比べて少ないため、海面温度分布情報は人工衛星から観測するのに適した情報である。本研究では、気象観測衛星NOAAと静止気象衛星GMS-5の赤外チャンネルの画像からの情報を用い、GRASS-GISによる海面温度の推定を行った。地理情報システムGIS（Geographical Information System）の利用は空間（地域､地理）情報の整理､解析において必要な手法となりつつある。GISであるGRASS(Geographic Resource Analysis Support System)はパブリック･ドメインのラスター型およびベクトル型のデータを扱うことができる。本報告ではGRASS主要な機能（ファィル出入力・変換、画像表示、ファィル・地域管理、画像処理、ラスタープログラムモジュール等）を利用し、海面温度分布図を作成することを試みた。

気象観測衛星NOAAにはAVHRR（Advanced Very High Resolution Rediometer）と呼ばれる超高解像度赤外放射計が搭載されていて、観測対象の温度情報を得ることができる。本研究では東北大学が受信し、公開している「日本画像データベース」から、熱赤外チャンネルであるCH4の画像を入手し、西日本の内海域を中心に北緯３１度から３５度、東経１２９．５度から１３５．６度の範囲を切り出した。また、画像はメルカトール図法で提供されているが、実際に海岸線との対応を見ると誤差があり、幾何補正が必要であった。幾何補正には、GRASSの機能を用い、地上基準点GCP（Ground Control Point）による線形のアフィン変換補正式を適用した。補正した画像はGLOBE（Global Land One-km Base Elevation）による地図情報を用いて、陸域をマスクして海面域だけを表示した。また、データを処理する前にヒストグラムを作成し、データの範囲や平均、分散を求めておくことにより、データの統計的特徴を把握しておくことで、画像情報の直感的把握が可能となる。GRASSのカラーテーブル機能を利用することで擬似カラー表示を行って、NOAA/AVHRR赤外CH4の輝度温度を推定海面温度として表示した。作成した海面温度分布図は瀬戸内海、有明海、西日本付近の太平洋の氷温分布およびその海域の海洋暖流の様子を表現できた。

静止気象衛星GMS-５熱赤外画像データ（IR1）は、高知大学の「気象情報頁」から入手した。ここでは、研究対象となる海域を広げ、赤道から北緯５５度、東経１０５度から１６０度の範囲を解析した。NOAAと同様にGRASSを用いて、幾何補正を行い、ETOPO５（NOAA NGDC Global Relief Data）による、地図データに重ね合わせた。また、ここでは、雲によって海面が覆われることを考慮し、数日間で最大値を取り出す最大値抽出法を用いて海面温度を推定した。最大値抽出にはGRASSのカテゴリ値再分類機能を応用することができた。つまり、カテゴリ（属性データ）情報を含んでいる各レイヤー（層）図を作成し､数日間の各レイヤー図を重ね合わせることで､合成海面温度図を完成した。

バイオメトリクスを用いた追認証の提案

情報科学専攻　情報処理学講座　　窪添　瑠実

近年，ネットワークの巨大化にあわせて，あらゆるサービスや情報提供等がインターネット化されている．また，政府でも2000年より，“すべての国民が情報リテラシーを備え，豊富な知識と情報を交流しうる”ことを目指し，『e-Japan戦略』として，5年以内に超高速アクセスが可能な世界最高水準のインターネット網の整備を促進すると共に，電子商取引の促進や行政・教育の情報化等の目標を掲げている．同時に，この計画の中でも最重要課題として個人情報の保護等のセキュリティに関する問題が挙げられている．つまり，これらのサービスや情報を利用するには，本人であることを確認する，“個人認証”が必要不可欠となる．

これまで，この個人認証にはパスワードやカードなどによる方法が用いられてきた．しかし，これらの方法では，解読や盗難，紛失などを考えると安全性に欠けていると思われる．現在でもこの認証は利用されているが，情報化が進むにつれ，セキュリティに対する意識は改革され，パスワードなどを用いた最も基本的な認証方法に，本人しか持ち得ない情報（バイオメトリクス）を利用する方法が併用されつつある．現在では，このバイオメトリクスを用いた個人認証システムが最先端の技術であり，様々なものが製品化されはじめている．

このような，現在，研究・開発されている認証システムや装置は，情報端末または公開された情報を利用する場合，利用前に個人認証を行うという形態がとられている．しかしこの方法では，何らかの方法で認証をパスしてしまえば，その後の操作は本人であるかどうかを判断することはできない．本研究では，この点に注目し，一度認証された後のさらなるセキュリティ対策として，新たな認証システムの形態である，“追認証”を提案し，その有効性について述べる．

本研究では，追認証を“利用前に認証した後も，続けて操作状況を監視し，利用中でも本人であるかを随時確認していくこと”と定義する．この認証の一手法として，人間の生体的特徴である，バイオメトリクスの中でも“マウス操作”に注目し，パソコン利用時において，パスワードなどにより一度認証された後の利用者の，マウス操作の特徴を調査することにより，その軌跡から利用者の特徴を抽出して個人認証を行う方法を提案し，追認証の可能性を考察した．

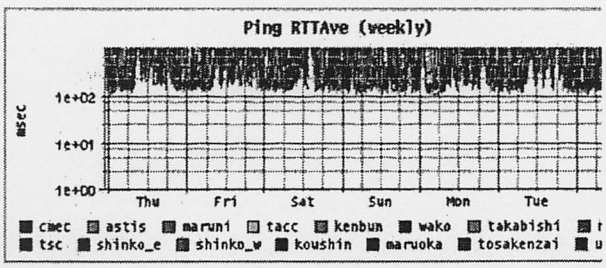
企業団地における無線 LAN 構築と VPN の導入

情報科学専攻　情報処理学講座　　滝澤　宏行

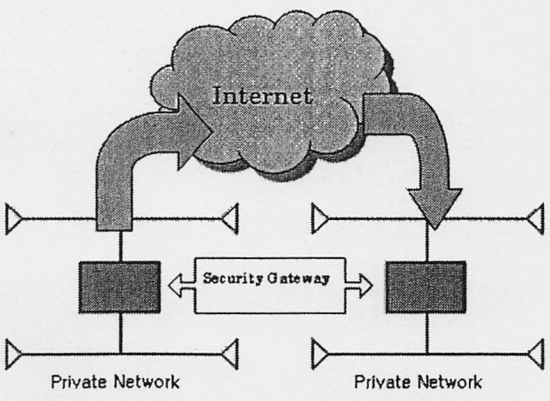
近年のインターネット利用者の拡大により、中小企業においてもネットワーク活用の必要性が高まっている。個別企業における IT 化の動きもあるが、企業団地を形成しているところでは共同によるネットワーク導入のメリットが考えられる。高知県においても流通企業団地でのネットワーク構築の試みが行われている。本研究では約１３ヘクタールの企業団地において１４社（１５箇所）を無線 LAN で結ぶ実験を行い、ネットワークの性能計測を長期間にわたって行った。無線 LAN には Root 社の RTB2400 を使っており、団地事務局を中心にして論理的にはブリッジによる中継でバックボーンネットワークを形成している。中心となる事務局にはメールサーバ、プロキシサーバなどの、各種サービスを行うサーバをおき、OCN 経由でインターネットへ接続している。各企業からはメール交換、WWW 閲覧などのトラフィックが事務局 LAN に集中している。そこで、この事務局のサーバから ping コマンドによって各企業の無線ルータに ICMP パケットを送出し応答データの計測を行った。第１図には帰ってきたパケットの応答時間の平均をグラフにしたもので、単位はミリ秒である。

グラフの作成には RRDtool を使用した。各企業に Ping を送出するシェルスクリプトを用意し、10 分ごとに実行させている。グラフの呼び出しには SSI を用い、Web サーバを介し、表示させる。このことにより、Web サーバにアクセスできるところであればどこでもその状況を確認することができる。グラフにより昼夜を問わず、また週日休日を問わずパケット落ちが多く、RTT も大きいことがわかる。これは使用している無線 LAN の特性によるものと考えられる。

以上の実験結果により、常時接続手段の多様化を考慮すると、必ずしも無線 LAN だけに頼る必要は薄れてきており、インターネット経由でセキュリティを確保する VPN の利用も考慮する必要があることが明らかとなった。このため専用線接続を用いて VPN 構築の実験を行った。第２図は実験の概要でありインターネット経由のパケットが暗号化されることで、安全に企業情報を交換できる。VPN の導入により、事務局の各種サーバへのアクセスも可能になり、通信状況も改善されるものと思われる。



第１図



第２図

量子テレポーテーションを用いた通信の基礎

情報科学専攻　情報処理学講座　谷脇圭介

Einstein—Podolosky—Rosen の論文以来，エンタングルメントは，量子的な絡み合いを形付けるものの１つであり，ここ近年，自然の中におけるエンタングルメントの効果を理解するために，量子情報理論での基礎的応用が発見された．そのエンタングルドメントの一例として，上記の３人の名前を使って EPR 状態と呼ばれる状態を，次のようにＡとＢの２つの粒子を用いて表す．

$$\left|\Psi^{-}\right\rangle_{AB}=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_{A}\left|1\right\rangle_{B}-\left|1\right\rangle_{A}\left|0\right\rangle_{B}\right)$$

量子情報理論でエンタングルメントを使う例として，テレポーテーションを記述する．テレポーテーションとは，1993 年に Bennett 等により提案され，送信者(アリス)から受信者(ボブ)に，その情報をもつ量子状態，そのものを送らずにエンタングルメントを用いた通信である．この方法は，エンタングルメントの粒子をアリスとボブに分け，アリスが量子状態と片方の粒子を合わせて観測することで得られる古典的情報をボブに送り，ボブの下でもう一方の粒子の状態にその情報を用いて再構築できるというものである．アリスの下ではその量子力学的な情報は失われる．この方法の概観は，映画等の SF で扱われるテレポーテーションに類似している．

この情報を持った量子状態やテレポーテーションで扱われるエンタングルド状態は，純粋な量子チャンネル必要とする．しかし，周囲の熱や他の気体分子との相互作用等により，これらの状態を乱す物理過程が多くあり，そのようなチャンネルを構築することは困難である．したがって，純粋な量子状態やエンタングルメントを得るためには，その影響を元に戻す方法が必要である．主に，量子状態での方法を量子誤り訂正で，エンタングルメントでの方法を量子純化プロトコルにて記述し，その特徴や違いを検証していく．

忘却効果を利用したニューラルネットワークの融合

情報科学専攻　情報処理学講座　　氏名　前園　淳

ニューラルネットワークの抱える大きな問題としてネットワーク内部のブラックボックス化があげられる. しかし結果的に適切な答えを得ることができればこの問題に関して内部の処理, ネットワーク内のリンクの意味づけなど把握する必要なく, あまりフォーカスされなかった点でもある. その結果ネットワーク内部を対象としての研究があまり行われていないのが現状である. しかし, ブラックボックスである内部リンクの意味を理解する事ができるならば, 数多くの利益を得られることは明らかである. 内部のブラックボックスを解明することにより多くのことが可能になる. 例えば機能単位毎にニューラルネットワーク内の任意のネットワークを抽出することが出来れば, 最適化した新たなネットワーク構築, 外部からのネットワーク内の操作などが可能になると考えられる. また更に, 抽出されたネットワーク内に格納されている情報からニューラルネットワークで獲得された学習ルールをも得ることが可能になると考えられる. ファジィ理論は人間の主観を用いてファジィルールを作れるという柔軟性を持つが, 自己学習機能は持ち合わせていない. 内部のブラックボックス化で理解し難い学習後のルールを獲得することができるならば, ファジィ理論の欠点を補うことに利用できるのではないかと考えられる.

本研究はニューラルネットワーク内部に構築されたブラックボックスの解明に向けて, 人間の記憶モデルにあてはめた情報の抽出, 融合を試み, 考察することを目的とする. 本論文ではまず簡単な情報を持つ単純なネットワークから情報の抽出を行う. そして抽出された複数の機能単位のネットワークを1つのネットワークに融合することで, 新たな多機能ネットワークを合成する. 具体的には, 文字認識用に学習させたネットワークを対象に実験を行った. この, 融合により情報の合成を試み, その特徴などを考察していく.

ネットワーク学習環境における教材提示支援サーバの構築

情報科学専攻　情報基礎学講座　　今村　育

従来，授業における教材提示には，黒板などに記述する方法，プリントなどの資料を配付する方法などが用いられてきた．しかし，近年のコンピュータの普及に伴い，教材提示にもコンピュータが使用されるようになった．特に情報系の教育現場においては，この傾向はさらに顕著である．

現在，コンピュータを利用して教材提示を行う方法としては，WWW の HTML によるオンライン教材，プロジェクタによる OHP や，スライドの投影といった教材提示方法が一般的である．しかし，これらの提示方法には以下のような問題点が存在する．

オンライン教材の場合，教材ページの表示操作を行うのは学習者自身であるため，教師が意図するタイミングで必要な教材画面が提示されているとは限らず，教師の解説と教材の内容が一致しない場合がある．スライド投影の場合は，プロジェクタなどを用いて表示するため，学習者の座席の位置によっては視認性が低下することもある．また，一度に表示できる情報量も制限されてしまうので，プリントなどの他の教材を必要とする場合がある．以上の３点から，学習者は教師による解説を十分に理解することが困難な場合がある．この問題は学習者の集中力を低下させ，授業の理解を妨げる要因となり，学習意欲の低下を引き起こす．

本研究では，学習者の端末に表示される教材提示画面を教師がリアルタイムにコントロールする方法により，教材の解説・提示の同期や視認性の問題を解消することを目的とした，教材提示支援システムの提案と試作を行った．本システムは Java を用いたサーバ・クライアント型のシステムである．教師は専用のオーサリング・システムにより教材知識のオーサリングを行う．解説を行う際は，教材データベースに蓄積された解説スライドをリアルタイムに呼び出し，学習者の Web ブラウザ上に Java アプレットを用いて提示する．この機能により学習者は確実に解説と同期した教材画面を参照することが可能となり，教師の音声による指示に従った煩雑な画面操作から解放される．また，本システムでは学習者の理解促進のために，表示されるスライドに関連する補足的な教材情報を同時に表示する機能も備えている．本システムにより，教師が自分の意図するタイミングで教材を学習者に分かり易く提示し，学習者の教材理解以外の負荷を軽減することで，解説に集中させることができ，学習意欲の低下を防ぐことが可能である．また教師は授業に用いる教材データをデータベースとしての効率良い管理・運用を実現できる．

C言語演習を対象とした統合型教育支援環境の構築

情報科学専攻　情報基礎学講座　　小川　実

プログラミング演習において，学習者は教師により提示された課題プログラムの作成・提出を行う．教師は提出されたプログラムおよび考察文などから，学習者の理解度などを把握し，以後の授業内容に反映させる．このように演習授業では，課題提出によって行われる学習者と教師間のコミュニケーションが重要である．

現在，課題の提出方法には電子メールを利用した方法が一般的である．電子メールの場合ネットワークに接続できる場所であれば，時間的な制約にとらわれず課題を提出することができる．しかし電子メールは一方向のコミュニケーション手段であるため，学習者は正しく提出できているか，また提出した課題がもれなく成績処理されているかを確認することができない．一方，教師は大量の課題メールを受信し，内容の確認や採点を手作業で行う必要があり極めて非効率的である．そのため多大な時間が必要となり，各学習者の状況を即座に把握することは困難である．

我々の研究室では既に電子メールを利用した課題提出システムの開発を行っている．このシステムは，Webブラウザ経由で電子メールを送信することによる学習者の負荷軽減と，送信内容の確認を行うためのフィードバック機能を備えている．しかし，これらの機能はあくまで学習者に対する負荷軽減のみを目的としており，送信されたデータの解析や集計などの高度な機能をもたず，教師側が抱える問題点は解決されていない．そこで本研究ではWeb環境からアクセス可能なデータベースサーバ構築技術を利用し，学習者と教師の抱える問題点を統合的に解決することを目的とした新しい形態のシステムを構築した．

本システムは主にCGI技術を用いて，Webブラウザからアクセス可能な課題提出・閲覧機能を備えたシステムとして実現した．学習者はWebブラウザを通じて個人認証を行い，いつでも課題を提出できる．課題提出時の記入項目は必要最小限にとどめ，他の必要な情報は可能な限り自動的に取得することで学習者の入力に関わる負荷を軽減する．提出された課題データはデータベースに蓄えられており，Webブラウザを通して学習者は課題受理の確認や提出済み課題の再利用などが容易に行える．また教師は同様の方法により，学習者の課題提出状況に関する最新の統計的な情報や，個別の課題レポートを閲覧することで学習者の理解状況を容易に把握することができる．本システムは平成13年度に数理情報科学科情報コースで実施された「計算基礎実験」のための課題提出・提出物確認システムとして半年に渡る試験運用を行った．また，演習を受講した学生にシステムに対するアンケートを実施し，システムの実用性についての評価実験を行い，その内容についての検討を行った．

捕食者と被食者の相互作用系のカオス
— 拡張されたロトカ・ヴォルテラモデルを用いたデータ解析 —

情報科学専攻　情報基礎学講座　　葛目悠輔

現在、自然界(nature)には「食う食われる」という弱肉強食(The strong preys upon the weak)の関係が存在する。この関係は捕食者(predator)と被食者(prey-predator)の相互作用によって成り立っている。

これら二者間の相互作用によって二種の生物の個体数がどのような変動を示すのかを数学的に記述する方程式がアメリカの数理科学者ロトカ(A.J.Lotoka,1925)とイタリアの数学者ヴォルテラ(V.Voltera,1926)によって初めて独立に提示された。彼らが提出した種間競争や捕食者—被食者相互作用を考慮した方程式は、現在でも生物の種間相互作用を取り扱う方程式として常に基礎的な役割を果たしてきている。またその形は、

$$\frac{dn_1}{dt} = \alpha n_1 - \beta n_1 n_2 \quad , \quad \frac{dn_2}{dt} = \beta' n_1 n_2 - \gamma n_2$$

でありn_1は被食者の個体数、n_2は捕食者の個体数を、パラメータα、β、β'、γは捕食者、被食者の増減の効果を示している。本論文はこの生態系(ecosystem)のモデルである、ロトカ・ヴォルテラ方程式について計算機で数値計算を行った。また、数値計算の方法として４次のルンゲ・クッタ法を採用した。今回このモデルに季節変動を表す項、

$$\alpha(t) = \alpha_0(1 + \varepsilon\cos\omega t)$$

を加える事によりロトカ・ヴォルテラモデル方程式の拡張を行った。拡張されたモデル方程式は季節変動振幅パラメータεを変化(増大)させる事により不規則な運動を出現させ、且つ、その軌道は有限なアトラクターを構成する事が判明した。そこでカオス判定に用いられるリアプノフ指数(Lyapunov Exponent)を数値計算により求めた結果、指数Λの値が正になった。この不規則運動は不安定であり且つ、カオスである可能性が高い事が分かった。また、実際の時系列データ(ウサギと山猫の毛皮の出荷数;1844～1934,カナダ)を拡張されたロトカ・ヴォルテラモデルを用いて解析し、モデルパラメータα、β、β'、γの値を求めた。n_1の増殖率α及びn_2の減衰率(死亡率)γの時間依存性を実際の時系列データについて解明する事に成功した。

円相場のフラクタル解析

— 予測モデルの提案 —

情報科学専攻　情報基礎学講座　　杜　忠

株式や相場は毎日目まぐるしく変動している。金融関係者や経済学者がいろいろな方法で株や相場の値動きを分析し、その値動きの将来の動向予測に努力している。フラクタル理論の創始者マンデルブロは、その分析方法の欠点を指摘し、自身が考案したフラクタル理論を用いて独特な株の分析方法を提案した。

本論文では、マンデルブロの提案を基礎として、マンデルブロの分析法の拡張並びに円相場の予測モデルを作った。以下にその手順を示す。

1．円相場の変動時系列中に存在するフラクタル現象の分析。

a. 円相場の変動は、データ抽出時間の単位によらず、統計的に相似である。

b. 円相場の変動の大きさの頻度分布がフラクタル的性質を持っている。

2．1971－2000 の 29 年間の円相場変動値を I 日飛びで測ったときの変動値の絶対値の総和

$$N(I)=\sum_{J=1}^{n-I}\left|k_J-k_{J+I}\right| \times\frac{1}{n-I}\times\frac{1}{I}\times\frac{n-1}{I}$$

の対数 $\mathrm{Log}N(I)$ を $\mathrm{Log}I$ に対してプロットしたときに得られた直線の勾配によって、円相場のフラクタル次元 d を求めることができる。最小二乗法により確からしい値として、$d=1.28$ を得た。

3．フラクタルとは全体を縮小したものが部分を構成するような構造である。フラクタル理論を援用して、“ N 字型”のジェネレーター折れ線を縮小（または縮小反転）することにより、円相場変動時系列のモデル計算例を作った。

4．マンデルブロの株分析方法の拡張を行った。マンデルブロの“ N 字型”分析法及びそのいくつかの類型の分析法を比較することによって、“ N 字型”分析法が精確度が高いことを明らかにした。

5．マンデルブロの“ N 字型”及び拡張された“ N 字型”分析法にフラクタル解析法を援用して、円相場の予測モデル（“次元同定法”と命名）を提案した。

音楽の情報理論的解析の試み

情報科学専攻　情報基礎学講座　　長瀬　匠

1. 動機　パソコンを購入してから、思いつくフレーズを曲にしています。しかし、思いつくフレーズをつなぎ合わせて曲にしてみても、音楽的な知識がなければ心地よい音楽を作ることは難しいです。私は、音楽的知識はほとんどありませんが、数学的な知識はある程度ありますので、音楽を数学的に解析し、作曲等に応用することを考えました。

2. 音楽　音楽とは「瞬間的に発生された音から作られる時間芸術」と辞書にはあります。音楽は「瞬間的に発生された音」が主要素ですので、現在、音楽を記録するのには、本来のアナログ時系列信号から、周波数と時間間引きを行い、デジタルデータ化し保存しています。これらは音楽の記録法として問題ありませんが、楽器、場所、演奏者などによって内容が変化します。 また、音楽というものは古くからありましたが、上のような理由から時代を越えて後世に伝えるには難しかったようです。そこで、楽譜というものが作られました、最初は単なる個人的なメモとして。音楽というもの、作曲家というものが存在し始めるのは音楽の記録体系が確立した後になります。このような理由から、音楽の本質は楽譜に存在すると考え、以下楽譜に対する情報化を行います。

3. 情報化　ここでは情報化のひとつとして数値化を行います。楽譜を構成する、もしくは音楽を構成する主要な要素は、いうまでもなく音とその持続時間であると考えられます。よって音の高さを数値の大きさに対応させてデータを構成することが考えられます。この場合、高い音に大きい数字を割り当てるため、高い音ほど強いと考えることができます。もうひとつは、すべての音に同じ強さを与えるために音一つ一つを一人一人が別々に演奏していると考えて、データを構成することを考えます。ほかにも数値化の方法はあるかもしれませんが、今回はこのような2通りのデータ構成について、解析を行いました。

4. 解析手法と解析例　数値化したデータを解析する手法はフーリエ変換を使いました。音楽を解析すると 1/f 揺らぎが存在するという研究がされていますが、今回のデータに同様の処理をしましたところ、同じように 1/f 揺らぎの存在を確認できました。よって、このような数値化がある意味で正しいといえると思われます。

5. 作曲　音楽を数値化することによって、簡単に編曲、作曲を行うことができます。まったく同じスペクトルを持つ、互いに位相を変えた曲を作ってみました。この2つの曲は、全く同じ1/f揺らぎ特性をもつように作られていますが、まるで違う曲に聞こえます。

6. 可視化 音楽を情報化することにより、可視化することができます。音楽を画像にすることにより、全体の流れを一度に見ることがでます。また、画像処理分野と関連付けることができます。

7. 言語化　音楽はあるフレーズの繰り返し、展開、拡大縮小などによりできていると考えることができます。このような数値化により、音楽を文章と考え、あるフレーズをひとつの単語として考えることができます。よって、言語統計分野と関連付けることができます。解析の結果、言語統計で知られているジップ(Zipf)の法則を音楽でも発見しました。

8. まとめと今後の課題　音楽を情報化することにより、情報理論的解析、作曲、可視化、言語化など、いろいろな分野と関連付けることができました。その結果を報告します。音楽の分野が広がるにつれて音楽を情報化する手法を考え直す必要があるでしょう。

超楕円曲線暗号に関する研究

—システム設計とその実装—

情報科学専攻　　情報基礎学講座　　氏名　李　曦光

最近，公開鍵暗号系の発展に伴い，他の公開鍵暗号系より短い鍵に対しても安全性を保つと考えられている楕円曲線暗号が注目され，その実用化が進んでいる。

公開鍵暗号システムとは，暗号システムにおいて，「暗号化鍵」と「復号化鍵」という２つのキーをペアで使い，しかもそのうちの「暗号化鍵」は公開してもかまわないという暗号系である。楕円曲線暗号は公開鍵暗号システムの一種であり、有限体上の楕円曲線群を利用して暗号化を行なう。代表的な公開鍵暗号系であるRSAに比べて暗号化を高速で行なえるほか，鍵の長さを短くできる特徴がある。楕円曲線より更に高次の代数曲線を利用する方式を便宜上超楕円暗号と言う。

超楕円暗号を研究する重要な理由は，以下のとおりである。暗号学的に安全な超楕円曲線の数は，楕円曲線より豊富であり，楕円曲線は超楕円曲線の部分集合であるから，万一楕円暗号が破られても，超楕円暗号は生き残る可能性が考えられる。そうした具体的なことよりも，楕円暗号も含めて代数曲線上の暗号についての体系を構築することが，将来の暗号学にとって本質的に欠かせない。

この研究は、超楕円曲線のヤコビ多様体の群演算を利用して，高い安全性をもつ暗号を作成することを目的としている。ElGamal型の公開鍵暗号系を構成するためには、有限群と、その群上の離散対数問題が必要である。有限体上の楕円曲線は、その有理点の集合が有限群を成し、その上の離散対数問題(楕円離散対数問題EDLP)は、有限体の離散対数問題より計算が難しい傾向がある。楕円曲線暗号系はそれに基づく公開鍵暗号方式として構成される。しかし、超楕円曲線はそのままでは群を成さないので、ヤコビ多様体を導入する必要がある。ヤコビ多様体は因子の同値類で定義されるので、以下のことを解決しなければならない。

① 因子で群（ヤコビ多様体）の元を一意的に表すこと(被約因子)

② 加法を因子で表すこと

③ 加法の結果を被約因子として表すこと

本研究では、種数 g＝２、方程式 $y^2 = x^5 + \cdots$ で与えられる超楕円曲線のヤコビ多様体に対して，被約因子の加法アルゴリズムを用いて，ElGamal 型暗号システムを作成し、UNIXマシン上で実装した。