平成15年度

高知大学大学院 理学研究科 数理情報科学専攻

情報科学講座 修士論文要旨集

把持状態計測実験システムの製作

数理情報科学専攻　情報処理講座　下釜洋一

わが国の身体障害者（18歳以上）は年々増加しており、厚生省（現、厚生労働省）の平成8年実態調査によれば、2,933,000人、18歳以上の人口千人比で28.9人、すなわち、1,000人のうち約29人が身体上に何らかの障害を持っていることになる。

本研究は、まず障害者の職業相談及びカウンセリングに着目し、現在行われている雇用に向けた職業カウンセリングの調査を行った。その調査結果から、カウンセリングの一環としては、モノをつかむ、把持力に関する作業法を取り入れて、その作業成功率を測定し、雇用のための評価データの一つとしていることがわかった。この一連システムを工学的支援できるように、把持状態を定量化するシステムを製作し、基礎実験を行い、把持状態の詳細について考察を行った。

製作した計測実験システムは、直径50mm、高さ100mmの物体を人差し指と親指にて側面から把持した状態の圧力変化を電圧信号へ変換し、この電圧信号をディジタル化し、コンピュータで解析できるよう構築されている。センサは導電性ゴムを使用し、A/D 変換ボードは、逐次演算方式および分解能 14bit の性能を持つものを使用した。また、センサからのA/D変換ボードへのインタフェース部は、キルヒホッフの法則に基づいて出力された電圧信号から、導電性ゴムの抵抗値を算出できるように設計した。

実験方法としては、次の2つの方法にて行った。まず物体の質量を変化させ、その時の把持力を測定し、最小二乗法を用いて解析を行った。その結果、物体の質量が重くなるほど、把持力は強くなることを確認した。また把持力と物体の質量から、把持状態における物体の傾きを算出した。その結果、被験者が意識的には垂直に把持を行っているつもりであっても、実際は若干ながら物体は傾いていることがわかった。また、複数の健常者に実験協力をしてもらい、健常者の把持状態の特徴を解析するということで、10回の繰り返し実験を行い、標準偏差を導き比較検討を行った。その結果、親指の変動が人差し指よりも大きいということがわかった。把持力の変動周波数を分析したところ、1Hz の周辺に、強度の高いスペクトルが見られた。改めて、把持力と心電図を同時に測定し、心電図のR波（最大波）の周波数と一致する把持力スペクトルを得た。

著者は、現在作業成功率によって評価されている障害者の職業相談を、より具体的に定量化するために、この計測実験装置が使用できると考えている。また、心電図との関係を深く追求することによって、心理的な状態と把持力の関係を導きたいと思っている。

量子誤り訂正の最適化

数理情報科学専攻 情報科学講座　　近藤敏幸

量子コンピュータは周りの熱などのデコヒーレンスにより、コヒーレントな状態が破壊される為に、実現は不可能だと考えられていた。しかし、Shorらの研究により、コヒーレントな状態を維持しながら、量子計算の計算過程で起きた誤りから回復する量子誤り訂正コードが発見された。

先行の研究により、nビットの量子ビットを訂正する為に、X(ビット反転エラー)と恒等写像I,量子特有のエラーのZ(位相エラー)とY(ビット位相エラー)のテンソル積によって作られる群G、1ビットのエラーである部分集合E、Gの可換群をNとすると、

$M_i \in G, (i = 1, \cdots, a)$と$e^\mu \in G, (\mu = 1, \cdots, \alpha)$に対して、
$e^\mu M_i = s_i^\mu M_i e^\mu$で定義される$s_i^\mu$によって
$e_i^\mu = \frac{1}{2}(1 + s_i^\mu)$を定義したときに、
ベクトル$e_\mu = (e_1^\mu, e_2^\mu, \cdots, e_a^\mu)$が全て異なる.

このような可換群Nがあれば$C = \{|c\rangle \mid M_i|c\rangle = |c\rangle, i = 1, 2, \cdots, a\}$は誤りを訂正できるコードになっていることが示されている。

群Gの元(演算子)は5ビットの場合で1024個,6ビットの場合で4096個,nビットの場合で4^n個作られる。全ての演算子の組み合わせを考えると$\begin{pmatrix} 1024 \\ 4 \end{pmatrix}$,約$4.5 \times 10^{10}$ステップの計算が必要になる。本研究では、5ビットの場合に特化し、以下のような条件を用いて演算子の1024個の演算子から150個の演算子に絞りこみ、計算のステップを$\begin{pmatrix} 150 \\ 4 \end{pmatrix}$,約$2.0 \times 10^7$ステップに押さえ、5ビットの場合の全ての誤り訂正コード作成の為の演算子161280組を発見した。

絞りこみの条件

1. M演算子はYを含まないか、もしくは2つだけ含む。

2. M演算子はIを1つだけ必ず含まなければならない。

これらの演算子によって作られる量子誤り訂正コードを訂正するためには、それぞれ独自の量子誤り訂正回路が必要となる。つまり、量子通信を行う際に、送り手と受け手が全く同じ回路を持っていないと通信ができないということになり、量子通信の1つの手段として用いることができるのではないかと考えられる。

ネットワーク応用ソフトウェアに関する研究
山間地域における学校教育教材データベースの構築

数理情報科学専攻　数理科学講座　　楊　興

高知県は山間地域の占める割合が多く，このような地域では情報インフラの整備が課題となっているが，一方で地域における児童生徒の減少に伴い，いくつもの学年が同時に授業を受ける複式授業が一般化するなど，教育面においても課題が多い。高知県北部の本川村，大川村，土佐町，本山町，大豊町の5町村で構成される嶺北地域においては，嶺北教育研究所を中心に山間地域固有の教育問題に取り組んでおり，学校教育に関する事項の研究と教育関係職員の研修，地域学校教育の充実振興，各種教育活動の援助，学習指導案の共用・統合活用などの事業を行っている。この中でも学習指導案や各種教材を利用するにあたって情報インフラの整備と活用が課題となっている。本研究においては，嶺北教育研究所における学校教育教材のデータベース化の要求に応じて実際に利用できるデータベースを構築し関連する諸問題を明らかにすることを目的とする。

嶺北教育研究所におけるデータベースの要求仕様は概略以下のようになる:1.各学校の教員が作成した教材を自由に登録できること，2.教員は教材をダウンロードして自由に再利用できること，3.教材の登録と同時にキーワードを登録し，データベースから検索によって必要な教材を探すことができることである。これらの要求を満たすものとして，谷・菊地(2002)は，データベース管理システムとして PostgreSQL を，ウェブサーバとして Apache httpd を用い，HTTP と SQL のプロトコル変換に PHP によるプログラムを用いたウェブデータベースシステムを開発した。このシステムは機能的には要求仕様を満たしているものの，実際には十分利用されてはいなかった。

本研究においては，従来のプロトコル変換を必要とする構成ではなく，最初からデータベース管理システムを含んだウェブ・パブリッシング・システムとして，最近注目されている Zope (Z Object Publishing Environment) を用い，その上にコンテンツ管理システムとして，CMF (Content Management Framework) と Plone を採用し，上記の要求仕様に加えて，教員が教材検索だけでなくその利用法などについて情報交換ができるような，ポータル・サイトとしての機能を追加した。

CMF の「スキン」として設計されている Plone は，ニュースやリンク，予定表などポータルサイトとしての機能をひととおり備えているが，日本語の検索機能については追加が必要で，また，教材登録で必要なキーワードについても工夫が必要であった。これらの機能を追加することで，情報機器の操作に熟練していない教員にも利用しやすい学校教育教材データベースを構築することができた。

医療情報データベースの構築に関する研究

A Study of Database for Medical Information by Using the Data of Achenbach Child Behavior Checklist

数理情報科学専攻　情報科学講座　　王　培花

The CBCL (Achenbach child behavior checklist) is a viable tool to assess a child's behaviors, via parent report, in a clinical or research environment. The CBCL model for Chinese child ages 4~16 consists of 113 items related to behavior problems which are scored on a 3-point scale ranging from not true to often true of the child, and it will cost a doctor significant time to collect the material and gain the evaluating result of behavior problem of a child by using this questionnaire paper and hand-scoring model. It is important how easily to collect and administer this psychological material for studying child's behavior and how conveniently and quickly to get the diagnosis during examining the out-patients.

In order to realize this purpose, it needs to create a database and an interface, which can be used by doctors or psychologists to input the data of the patients to database and immediately gain the analysis result in which the data in database are utilized.

What has been done in this study are shown as the followings:

(1). A relational database for CBCL has been created with PostgreSQL, which includes a serial of tables divided into two kinds, ones are for accumulating individual information, other ones are for analyzing behavior problem of group population ages 4~6 and 6~12.

(2). The collected data were stored into CBCL database.

(3). A series of interfaces about CBCL have been made using Python program, some interfaces (cchild.cgi, evaluation.cgi and gc.cgi) are what can be applied to collect the individual child's general information, behavior symptoms and the information of influence factor on behavior. Other some interfaces (assess.cgi, group.cgi and group1.cgi) are what can be used to obtain the results of individual diagnosis, of analyzing group children's behavior and of analyzing the influence factors, all of which are displayed on Web pages.

In this paper, such conclusions were obtained as: (1) It is quicker and more accurate to make a diagnosis (2) It is more convenient to analyze a large sample of group children's behavior (3) It can get the result of influence factors directly (4) It can collect the data from worldwide via network.

It is necessary to be improved in this study that is the analysis method to influence factor and how to guarantee the security of operation system.

Verilog−HDLを用いた冗長2進高速乗除算回路の設計

数理情報科学専攻　　計算機科学講座　　李天慧

加減乗除の算術演算は計算機などのディジタルシステムにおいて、基本演算として広く用いられている。乗算を実現する基本方法は加算シフト法であり、除算を実現する基本方法を減算シフトである。この方法を用いて種々の乗（除）算器が実現されている。特に，その初期においては，マイクロプログラム制御を用いて加（減）算シフトを逐次実行する方法が取られた。しかし，加（減）算シフトを各桁逐次実行する方式は処理速度が遅く，現在要求される乗算の速度から見れば全く不十分である。従来から乗除算の高速化が望まれている。特に近年は、集積回路技術の進歩に伴い，LSI 化に適したセル配列構造の高速算術演算回路に関する研究が盛んである。本論文では、Verilog-HDL による高速乗算器と高速浮動小数点乗（除）算器を設計する。これは、システム LSI の演算コアを提供することを目的としている。

HDL（Hardware Description Language；ハードウェア記述言語）が出現して以来、VLSI 設計の手法は大きく変わった。従来、設計者がゲートを組合せて回路を構築していくボトムアップ的設計手法が取られていた。1980 年代後半になって VHDL や Verilog−HDL といったハードウェア記述言語が開発された。これにより RTL 回路を HDL で記述し、HDL シミュレータにより検証を行い、論理合成ツールにより論理合成を自動生成することが可能となった。LSI をトップダウン的に設計する手法が開発され、広く用いられるようになってきた。HDL とこれらの桁上げ先見加算器ツールの出現により VLSI 設計の生産性は著しく向上した。

2 進数の加減算においては、桁上げ（桁借り）の伝搬のため、桁上げ先見加算アルゴリズムは、演算数の桁数の対数に比例する時間が必要である。これに対し、冗長 2 進数体系では、その冗長性を利用し、加減算において桁上げ（桁借り）が高々1 桁しか伝搬しないようにすることができ、組み合わせ回路による並列加減算が演算数の桁数に関係なく一定時間で行える。本論文では、2 ビットの 2 進数 {0, 1} で冗長 2 進数 {-1, 0, 1} を表現するという冗長 2 進数体系を用いて、Verilog−HDL による (1) 冗長 2 進乗算器、(2) 浮動小数点乗算器、(3) 浮動小数点乗算型除算器と (4) 浮動小数点冗長 2 進減算シフト型除算器を設計したので、この件に関して発表する。冗長 2 進乗算器は、冗長 2 進加算器を用いるために、部分積の加算で、桁上げを伝播しない加算を行うことが可能である。冗長 2 進乗算器の計算速度は、従来の乗算回路（配列型乗算器と Wallace 型乗算器）より高速動作が可能である。単精度浮動小数点乗算型除算器は、乗算の繰り返しにより除算を行うもので、高速乗算器を持つ計算機などで用いられている。浮動小数点冗長 2 進減算シフト型除算器は、減算とシフトの繰返しにより商を上位桁から順に求める演算回路である。

与えられた位数を持つ楕円曲線の構成

数理情報科学専攻　情報科学講座　　王　向輝

1. 序　楕円曲線を公開鍵暗号に利用する方法は最初に Kobilitz と Miller によって提案されたものである. この方法は有限体上定義された楕円曲線上の離散対数問題を利用しており, ElGamal 型暗号, 鍵交換, 電子署名等の標準的な暗号プロトコルを実現できる.

楕円曲線の群位数によっては離散対数問題が解きやすくなる. そのため, 暗号への応用に適した楕円曲線を決定するのに, 現在三つの主要なテクニックが使われている:

- 適当な曲線が見つかるまでランダムに曲線を生成し, それらの群位数を, 例えば Schoof のアルゴリズム等を用いて計算する.
- 虚数乗法 (CM) の理論を使って与えられた群位数をもつ曲線を生成する. その様な曲線は CM 曲線と呼ばれる.
- 相対的に小さい体 F_q 上定義された曲線 E の, F_{q^n} 有理点の群 $E(F_{q^n})$ を使う. その様な曲線は部分体曲線と呼ばれる.

本研究では CM 曲線を構成するアルゴリズムの実装を行っている. 最大整環で CM を持つ曲線については先行研究があるが, 本研究では導手付きの整環も扱い, 曲線を構成できる確率が向上している.

2. CM 曲線のアイデア　体の標数が 0 ならば, 虚数乗法を持つ楕円曲線 E の自己準同型環 $\mathrm{End}(E)$ はある虚二次体 $k = Q(\sqrt{D})$ の整数環 $\mathcal{O}_k = \mathcal{O}_D$ ($D < 0$ は k の判別式) の部分環である.

E の標数 p への還元 $\tilde{E}$ が素体 F_p 上で定義できれば, 群位数を $\sharp\tilde{E}(F_p) = p + 1 - t$ と置いたときの t は $4p = x^2 - Dy^2$ の整数解 x, y の x と (± を除いて) 等しい. このことを利用して目的の曲線をみつける.

3. CM 曲線を構成するアルゴリズム

1) $Q(\sqrt{D})$ のイデアル類と各イデアル類の代表 $Z + Z\tau_i$ を求める
2) 楕円モジュラ関数の値 $j(\tau_i)$ を高精度に計算する
3) Hilbert 類多項式 $H_D(X) = \Pi_i(X - j(\tau_i))$ を計算する（整数係数になる）
4) $H_D(X)$ が素体 F_p 上の解 $X = j$ を持ち, かつ, $4p = x^2 - Dy^2$ が整数解を持つような素数 p をみつける
5) j-不変量が j であるような F_p 上の楕円曲線 E を求める

4. 実行例　以上のアルゴリズムを Mathematica で実装した. 例えば暗号応用のための, 150 桁の素体上の CM 曲線の例として次の様な曲線が得られる:

```
p = 1315739383530685647915253893604824788413372041270948626339974816682871253506782350948186357677825418047749670475650280639641023782786814250013532011081
D = -16
# E(Fp) = 1315739383530685647915253893604824788413372041270948626339974816682871253507254311775794899246398118741513247340451720181584654579752294589223330090372
E : y^2 = x^3 + 730966324183714248841807718669347104674095578483860347966652675934928474170434639415659087598791898915416483597583489244245013212659341250007517783786 x + 1218277206972857081403012864448911841123492630806433913277754459891547456950724399026098479331319831525694139329305815407075022021098902083345862972533
```

5. CM 曲線の構成可能状況

$$\begin{cases} \text{標数 } p \quad : 150 \text{ 桁の素数 (固定)} \\ \text{判別式 } D : -1 \sim -2000 \text{ 全て} \end{cases} \Rightarrow \begin{cases} \text{生成できた CM 曲線の個数} & : 1014 \text{ 個} \\ \text{曲線生成確率} & : 27\% \\ \text{実行時間 (Sun GP500S, 750MHz)} & : 4078.2 \text{ 秒} \end{cases}$$

楕円曲線上の秘密分散法

数理情報科学専攻 情報科学講座　嶋岡 哲夫

1　まえがき

複数の人間で情報管理が可能な (k,n) しきい値秘密分散法がある．これは，もとの情報から n 個の暗号化された分散情報 (シェア) を作成し (分散符号化)，得られた n 個のシェアのうち k 個以上 $(k \leq n)$ 集めるともとの情報が得られる (復号) という暗号システムである [1]

秘密分散は一般に有限体上で実装されるが，本研究では楕円曲線上での実装を行う．これによりセキュリティレベルを落とさずにシェアサイズを縮小することが見込める．例えば，従来の公開鍵暗号では 1024bit に相当する安全性が楕円曲線で実装することにより 173bit で得られることがわかっている [2]．シェアサイズが小さくなることで，メモリーが節約でき，高い計算処理能力を必要としなくなるため IC カード等にも暗号システムを導入することが可能になる．

2　有限体上の秘密分散法

秘密情報 S を有限体の元に埋め込み，管理者の人数分 ID $x_i (i = 1, \cdots, n)$ を用意する．x_i は復号を考慮して原始根が用いられる [1]．この n 個の ID をもとに作成した n 行 k 列の行列と S を埋め込んだ元から

$$\begin{pmatrix} W_1 \\ W_2 \\ \vdots \\ W_n \end{pmatrix} = \begin{pmatrix} 1 & x_1 & \cdots & x_1^{k-1} \\ 1 & x_2 & \cdots & x_2^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \cdots & x_n^{k-1} \end{pmatrix} \begin{pmatrix} S_1 \\ \vdots \\ S_k \end{pmatrix} \quad (1)$$

を計算した結果 W_i をシェアとして (x_i, W_i) のように保管しておく．復号は，これを k 個以上集め逆算する．

2.1　問題点

秘密分散法は安全のため大きな有限体上で行う必要がある．しかし，大きな有限体や原始根の計算量は膨大なものであり問題視されている．また，楕円曲線は群構造をしているためこのままでは応用できない．

本研究はこれらを解決する原始根を用いない有限群上での構成法を提案し，楕円曲線への応用に成功した．

2.2　有限群上での秘密分散法

有限群上で構成するには，ランダムに集めた k 個の ID で作成する k 次行列式の値が位数 (元の個数) と互いに素であればよいことを証明した．そこで ID には

$$(x_i - x_j) \text{ のすべてが位数と互いに素} \quad (2)$$

であるものを選出する．

3　楕円曲線上の秘密分散法

p を素数，$f \geq 1$ として有限体 F_{p^f} 上の楕円曲線

$$E : Y^2 = X^3 + aX + b \quad a, b \in \mathrm{F}_{p^f} \quad (3)$$

の有理点 (X, Y) が群構造を持っていることを利用する．

3.1　分散符号化

秘密情報 S を E 上の有理点の X 座標に埋め込み，管理者の人数分 ID : x_i を用意する．$(x_i - x_j)$ はすべて位数 (有理点の個数) と互いに素である．位数 (有理点の個数) を法として式 (1) と同様に ID で作成した n 行 k 列の行列と S を埋め込んだ有理点を掛け合わせる．得られた W_i も E 上の有理点であり，(x_i, W_i) のように保管しておく．

3.2　復号

k 個の ID : x_i をもとに掃き出し法で逆行列を作成する，これとシェア W_i を掛け合わせて秘密情報 S を得る．

$$\begin{pmatrix} S_1 \\ \vdots \\ S_k \end{pmatrix} = \begin{pmatrix} 1 & x_1 & \cdots & x_1^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_k & \cdots & x_k^{k-1} \end{pmatrix}^{-1} \begin{pmatrix} W_1 \\ \vdots \\ W_k \end{pmatrix} \quad (4)$$

4　処理速度

SunMicrosystems (CPU 750MHz) 上で実行した際の処理速度について評価する．一度に処理できる情報量はしきい値 k と有限体の大きさに依存する．300bit を処理する例，$(k,n) = (3,5)$，$p = 1031 (\approx 10\text{bit})$，$f = 11$ で実行し，以下の結果を得た．

	分散符号化	復号
300bit	0.7 秒	0.68 秒
bit/秒	428bit/秒	441bit/秒

5　今後の展望

秘密情報を AES や DES 等の古典暗号で暗号化し，その暗号鍵を秘密分散法で管理する暗号システムに応用していく．

参考文献

[1] 岡本 龍明, 山本 博資, 現代暗号, 産業図書,1997

[2] I.Blake , G.Seroussi , N.Smart , Elliptic Curves in Cryptography , 1999

メモリ状態の可視化にもとづく知的C言語学習支援システムの構築

数理情報科学専攻　情報科学講座　　藤原　宏記

本研究ではC言語学習におけるポインタ概念の獲得支援を目的とし，学習を妨げる要因についての認知科学的な考察，及びそれにもとづく知的学習支援システム・フレームワークの提案を行った．

C言語は実用・教育の場面で広く使用されている手続き型プログラミング言語である．特にプログラミング教育の場においては，他のプログラミング言語を学ぶための基礎として重要な位置づけにある．

プログラミングとは，ソースコードの作成・コンパイル・実行を繰り返し，発見された誤りを逐次，修正していく過程である．学習者はこの過程を通じて，プログラミングに必要となる知識や，その使い方を獲得する．C言語学習では，様々な事柄の習得が必要となるが，特にポインタの概念を獲得することが最も困難といわれており，その要因として以下の2点が挙げられる．(1)ポインタの概念は，メモリとその入出力手続きで構成される抽象概念である．したがって，学習者は間接的にポインタ操作の挙動を理解して内部状態を予測することしかできない．(2)ポインタに関する誤りは，コンパイルおよび観測される状態から予測される．しかし，正確な予測を行うための十分な情報が得られない場合が多い．

ポインタの概念に関連した誤り修正には，ポインタ操作に関する知識をもとに実行時のメモリ状態の遷移を想起・理解することが必要となる．しかし，プログラミング経験の少ない初学者の場合，一般的に自ら誤り原因の同定を行うことは困難である．この状況は学習を停滞させ，学習動機を低下させる．したがって，計算機が誤り原因を同定し，分かり易く伝達できれば，学習者は行き詰まりから復帰し，学習を継続できる．

現状では，これらの問題に対する計算機支援として，開発環境に含まれるデバッガの利用が考えられる．しかし，初学者はその出力情報を活用できない場合が多い．また，既存の学習支援システムには前述の問題解決を指向した支援機能をもつ事例はない．そこで本研究ではC言語におけるポインタ学習を対象に，プログラム実行時のメモリ状態の可視化とポインタ誤りの自動検出を行う知的学習支援システムを構築した．本システムでは，図示されたメモリ状態を満たすプログラム作成を学習者に指示し，その診断結果にもとづき，より適切な出題や助言などの積極的支援を行う．これにより学習者は，より深い理解を得ることで学習を継続できる．