様式 C-19

科学研究費補助金研究成果報告書

平成２３年　６月　２４日現在

機関番号：12611
研究種目：若手研究（Ｂ）
研究期間：　2008　～　2010
課題番号：20740051
研究課題名（和文）　情報セキュリティへの離散数学の応用

研究課題名（英文）　Discrete mathematics for coding theory and cryptography

研究代表者　萩田　真理子　（HAGITA MARIKO）
お茶の水女子大学・大学院人間文化創成科学研究科・准教授
研究者番号：70338218

研究成果の概要（和文）：
相互に関係の深い以下の情報セキュリティのための離散数学研究を行った。（１）暗号用擬似乱数発生アルゴリズム及び暗号用でない擬似乱数発生アルゴリズムの乱数性について乱数性の評価を行い検証した。（２）擬似乱数発生法の並列化の際に独立性を保障する彩色問題の研究を行い、グラフの分散彩色アルゴリズムを提案し、また分散彩色の評価関数を定義して評価手法を導入した。（３）射影ド・ブライン系列を用いた誤り訂正符号系列の生成と存在条件に関する研究を進め、研究集会 SETA2008 などで発表し、LNCS で論文"Projective de Bruijn sequences"を発表した。

研究成果の概要（英文）：
We define an (N,k,d) error-correcting sequence over GF(q) as a periodic sequence a_0,a_1,a_2,... of elements in GF(q) with period N, such that its sub k-tuples (a_i, a_{i+1}, ..., a_{i+k-1}) are all distinct for i=0,1,...N-1, and they form an error-correcting code with minimum distance d.
Admitting a moderate conjecture on the existence of primitive polynomials whose coeffients constitute a De Bruijn sequence or a Projective De Bruijn sequence, we prove the existence of a binary (2^{2^m-m-2}-1,2^m-2,3) error-correcting sequence and (q^{¥frac{q^m-1}{q-1}-m}-1,¥frac{q^m-1}{q-1},3) error-correcting sequence over GF(q).

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	1,400,000	420,000	1,820,000
2009 年度	900,000	270,000	1,170,000
2010 年度	900,000	270,000	1,170,000
総　計	3,200,000	960,000	4,160,000

研究分野：離散数学
科研費の分科・細目：数学一般
キーワード：グラフ彩色、ド・ブライン、暗号、誤り訂正符号、離散数学

１．研究開始当初の背景

暗号や擬似乱数に代表される数論的アルゴリズムは、世界中の純粋数学及び応用数学の研究機関が興味を持っている分野である。しかしながら、現代の研究は純粋理論なら純粋理論に特化し、実用分野なら実用理論

に特化する傾向が強い。また、それらを結びつけるはずの応用数学研究も純粋理論にまで深く切りこむものは少ない。

２．研究の目的

本研究テーマは、「先端的純粋数学理論を実用の視点から眺め研究し、実際に用いられるところにまで到達させる」ことを目的として、情報セキュリティのための離散数学研究を行った。具体的には、相互に関係の深い以下の 4 種類の研究を行った ：
（１）暗号アルゴリズムの生成と評価、
（２）シミュレーションのためのグラフの分散彩色研究、
（３）誤り訂正系列符号の存在性と電子署名への応用、
（４）ランダムウォークによる擬似乱数と暗号の乱数性の評価。

３．研究の方法

（１）既に特許出願している暗号鍵更新方法、電子署名強化方法、暗号通信システム、暗号用擬似乱数発生システムを実現するアルゴリズムの作成・評価・改良のための研究を行った。
これらの暗号を評価するため、小さな空間での同種の暗号化関数のプログラムをつくり、現在使われている他の暗号化関数をモデル化したものと比較した。同じ変換を繰り返し施して暗号化する場合には、変換回数を減らして混ざり具合を計ることで変換の乱数性を評価することができた。
（２）擬似乱数発生法の並列化の際に独立性を保障する彩色問題の研究を行った。
並列計算を用いたシミュレーションを行う場合、擬似乱数の配置の仕方により偏ったデータが出てしまうことがある。この問題は、擬似乱数を割り当てる場所を頂点とし、相関の大きな２点を隣接させたグラフを生成し、その分散彩色を求めれば解決する。グラフの分散彩色問題とは、与えられた色数で、グラフの頂点を同色の異なる二点の距離の最小値が大きくなるように彩色する問題で、これまでの研究でシミュレーションに現れることの多い格子グラフの分散彩色の存在範囲を決定していた。本研究では、グラフの分散彩色の存在条件を求め、多項式時間で適当な解を求めるアルゴリズムを作成し、これらの評価方法を検討した。
（３）誤り訂正系列符号の存在性についての研究をすすめた。誤り訂正系列符号は電子署名の強化アルゴリズムをつくるために必要な GF(q)の元の巡回系列で、その k 部分列の集合が符号となるものである。現在、M系列と呼ばれる巡回系列と、符号理論の両方の研究手法を用いて存在条件を求めた。有限体を生成するための原始既約多項式として、よく探されている３項式とは逆に、項数が半分くらいでバラバラに散らばっているものが必要になり、また随分昔に研究されていたド・ブライン系列及び、これを射影化した射影ド・ブライン系列が役立つなど、応用に適さないと思われていた離散数学が実用化に結びつくことがわかった。
（４）ランダムウォークを用いた擬似乱数と暗号の乱数性の評価
Rand, LaggedFibonacci,Mersennne Twister などのいくつかの擬似乱数で、長さ 2n のランダムウォークを z 本発生させて正の領域への滞在時間の実現度数の分布を作り、χ二乗検定を用いて真乱数の場合に期待される度数との適合度を確認してみたところ、周期の短い擬似乱数は棄却された。擬似乱数の検定には様々な方法があるが、比較的長いビット数をまとめて見たときの振る舞いを評価できるため計算量の少なさの割りに、擬似乱数の悪さを見つけやすい手法と考えられる。周期が非常に長く高次元の均等分布性が保障されている Mersennne Twister でも、空回しせずに検定を行うと、恐らく初期状態からの立ち上がりの悪さが原因と思われる若干の悪さが確認された。小型の最新のアルゴリズムでも同様の検定を行い比較してみた。

４．研究成果

それぞれ次のような成果が得られた。
（１）既に特許出願しているブロック暗号と暗号用擬似乱数発生システムを評価するため、小さな空間での同種の暗号化関数のプログラムをつくり、現在使われている他の暗号化関数をモデル化したものと比較する研究を進めた。同じ変換を繰り返し施して暗号化する場合には、変換回数を減らして混ざり具合を計ることで変換の乱数性を評価することができた。
これらの研究に必要になった代数と暗号についてまとめた書籍「暗号のための代数入

門」を出版した。
（２）擬似乱数発生法の並列化の際に独立性を保障する彩色問題の研究が進めた。実際に分散彩色を行う効率の良いアルゴリズムを作成するとともに、その評価方法についての研究を行った。分散彩色の評価方法としては、同色２頂点間の最小距離を大きくすることの他に、同色の頂点がなるべく近くにないように彩色されている方が良い彩色と考え、2 つの彩色の重み w(c):=
¥sum_{c(x)=c(y)}¥frac{1}{(d(x,y))}
と w’(c):=
¥sum _{c(x)=c(y)}¥frac{1}{(d(x,y))^2}
が，より小さい彩色結果を返すアルゴリズムを良い分散彩色アルゴリズムとする指標を提案した。この有効性を検証するとともに、これらの重みの小さな彩色結果を出力する高速な彩色アルゴリズムを作成した。研究結果は応用数学合同研究集会 2010 で紹介し、その報告集に論文発表している。
（３）射影ド・ブライン系列を用いた誤り訂正符号系列の生成に関する研究を進めて、射影ド・ブライン系列を係数とする最適な原始多項式の存在性についての条件を証明した。射影ド・ブライン系列はその定義から、最初の数項を指定すると最後の項の値は一意に定まる。一方、代数的な性質から、モニックな多項式の定数項にも原始多項式になるための条件が示される。ほとんどのパラメータでこれらの条件が同時に成立せず、射影ド・ブライン系列を係数列にもつ原始多項式は存在できないパラメータが多く、期待される最適な誤り訂正符号系列の非存在が示された。
これらの研究成果の一部は研究集会 SETA2008 と応用数学合同研究集会 2009 で発表し、LNCS から論文″Projective de Bruijn sequences″を発表した。その後の研究成果についても、発表準備を進めている。
（４）擬似乱数 rand とＣＳＴについてランダムウォークを用いた統計的検定を行い、rand は下位ビットが棄却されるがＣＳＴについては棄却されないことを確認した。擬似乱数の周期によって棄却しやすいランダムウォークの長さが異なると予想されるため、検定での最適なパラメータの選び方についての研究を引き続き進めている。その結果も含めて論文にまとめて発表することを予定している。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 6 件）
（１）山口真実、萩田真理子
グラフの分散彩色の評価方法
応用数学合同研究集会報告集
2010, 137－138(査読なし)

（２）間宮直子、萩田真理子
グラフの彩色拡張アルゴリズム
応用数学合同研究集会報告集
2010, 139－140(査読なし)

（３）佐藤春菜、萩田真理子、松本眞,
Projectve DeBruijn 系列を係数に持つ多項式の原始既約性の判定,
応用数学合同研究集会報告集,
2009, 2 ページ（査読なし）

（４）山口真実、間宮直子、浅本紀子、萩田真理子
のぞき込まれても良いパスワード入力システム
応用数学合同研究集会報告集
2009, 2 ページ（査読なし）

（５）Mariko Hagita, Makoto Matsumoto, Fumio Natsu, Yuki Ohtsuka,
″Error Correcting Sequence and Projective De Bruijn Graph″ Graphs and Combinatorics 24,185-194,2008(査読あり)

（６）Yuki Ohtsuka, Makoto Matsumoto, Mariko Hagita,
″Projective de Bruijn sequences″,
LNCS 5203, 167-174, 2008(査読あり)

〔学会発表〕（計１０件）

（１）萩田真理子
有限体の暗号アルゴリズムへの応用
2011 年 2 月（慶應義塾大学）
組合せ論若手研究集会（招待講演）

（２） 山口真実、萩田真理子
グラフの分散彩色の評価方法
2010 年 12 月（龍谷大学）
応用数学合同研究集会

（３）間宮直子、萩田真理子
グラフの彩色拡張アルゴリズム
2010 年 12 月（龍谷大学）
応用数学合同研究集会

（４）山口 真実, 萩田真理子
グラフの分散彩色アルゴリズム
2010 年 9 月（明治大学）
日本応用数理学会年会

（５）福田 恵子, 萩田 真理子
共有鍵暗号 Rabbit と AES の乱数性の評価と比較
2010 年 3 月（筑波大学）
日本応用数理学会 研究部会連合発表会 2010

（６）佐藤春菜、萩田真理子、松本眞,
Projectve DeBruijn 系列を係数に持つ多項式の原始既約性の判定,
2009 年 12 月（龍谷大学）
応用数学合同研究集会

（７）山口真実、間宮直子、浅本紀子、萩田真理子
のぞき込まれても良いパスワード入力システム
2009 年 12 月（龍谷大学）
応用数学合同研究集会

（８）遠藤貴世美, 萩田真理子
グラフの彩色アルゴリズム,
2009 年 9 月（大阪大学）
日本応用数理学会 年会

（９）Yuki Ohtsuka, Makoto Matsumoto and Mariko Hagita
Projective de Bruijn sequences,
2008 年 9 月（レキシントン/アメリカ）
SETA2008.

（10）Mariko Hagita and Makoto Matsumoto
″Projective de Bruijn sequence for error-correcting sequence″
2008 年 12 月（オークランド/ニュージーランド）
The Fourth International Conference on Combinatorial Mathematics and Combinatorial Computing.

〔図書〕（計１件）
萩田真理子, サイエンス社, 「暗号のための代数入門」2010, 208.

６．研究組織
(1)研究代表者
萩田　真理子（HAGITA MARIKO）
お茶の水女子大学・大学院人間文化創成科学研究科・准教授
研究者番号：70338218

(2)研究分担者
無し

(3)連携研究者
無し