2008. 6
特 集 号

国立大学法人 高知大学学報
（題字：相良祐輔学長）

高知大学学位授与記録第二十四号

総務課広報室発行

本学は、次の者に博士（理学）の学位を授与したので、高知大学学位規則第１５条に基づき、その論文の内容の要旨及び論文審査の結果の要旨を公表する。

目　次

ふりがな 氏　名（本籍）	ひろせ　ちおり 廣瀬　智織　（東京都）
学位の種類	博士（理学）
学位記番号	甲理博第20号
学位授与の要件	学位規則第4条第1項該当
学位授与年月日	平成20年3月24日
学位論文題目	地震に伴う電磁気現象観測の為の陸上海底電磁場環境の研究
発表誌名	(1) Physics and Chemistry of the Earth Vol.31, pp.352-355、2006
	審査委員　主査　教授　小玉　一人 副査　教授　田部井隆雄 副査　教授　岩崎　正春

論文の内容の要旨

近年、地震発生に伴う電磁気現象の報告が多数されている。それらの現象としては、震源から直接放射される電磁場変動や地震に伴う大気圏や電離層の電磁的擾乱現象などがある。報告されている周波数帯はDC～HF帯と広帯域であり、観測手法も多岐に渡る。これらに共通する問題点として、地震に伴う信号は微弱であり、観測点におけるノイズ環境に大きく左右される事である。

周囲を海で囲まれた日本において、地震発生源は陸上に限らず海底においても発生する。また、地震に伴う微弱な電磁気現象の観測に当たって、大気中の電場変化と気象条件は密接に関係し、これらの研究は必要不可欠である。特に報告されている地震に伴う電磁気現象の周波数帯域とほぼ一致する空電は最大のノイズとして考えられ、逆に地震に伴う電磁気現象の振る舞いを予測するに当たり重要な役割を果たすと考えられる。本論文では、一般的に高い周波数の電磁場が地殻表面や海水中を通過できない表皮効果の問題から、ULF～VLF帯の低周波に着目し、陸上海底における電磁場環境の研究を行った。

本論文では、空電を信号とし陸上海底における同期観測、そして陸上において様々な電場変動を見る為に長期観測を行った。陸上海底の同期実験は、陸上でボールアンテナを用い海底では極板アンテナを用いた。また、陸上における長期観測ではボールアンテナを用いた。これらの観測装置の利点としては、測定環境に応じた設計変更が可能である事や、安価である事かつ精度が良い事が挙げられる。

Ⅰ．　陸上海底における同期観測

本研究により同期観測用海底観測装置の最小検出感度を従来の約2倍向上させ、5.5nV/m/√Hzを実現した。この為、大気中から海水へ進入してくる空電の今まで観測できていなかった成分(4～5kHz)の抽出も一部可能になった。観測を行うに当たって、ボールアンテナの校正を行った。その結果、ボールアンテナの受信周波数特性は、ボールアンテナに内蔵している回路のインピーダンス計算と非常に良く一致する事が証明された。理論と実験値の比較は、15Hz～1.5kHz及び4～6kHzにおいて適度な一致を見た。しかし、主な成分は1kHz以下であり、そこから考察すると海底下から到来する地震に伴う電磁場は、1kHz以上の周波数が伝番してくる事は難しいと容易に判断できた。また、陸上のボールアンテナは、海上自衛隊が対潜水艦用に用いている22.2kHzも受信していることから、感度は十分であると言える。

Ⅱ．　陸上長期観測

大気電場の長期観測により、大気の静穏日における電場の日変化、気象条件による変化のデータを得る事ができ、ボールアンテナの性能として電場の変化が激しい雷から、台風の影響、穏やかな日の大気電場の変化、細かい霧の発生まで敏感に受信する事の証明となり、現在地震に関係するデータは得られてないが、有用な観測ツールとしての提案はできたと考える。実際に地震に伴う電磁気現象の観測をするには、最適観測地点の発見や、地下からの信号検出の為地中に埋めるか夜間の人口雑音の少ない時間帯を選ぶなど、工夫をする必要がある事も分かった。

論文審査の結果の要旨

本論文は、DC－HF 帯までの広帯域にわたる自然電磁場変動のうち、特に ULF－VLF 帯の低周波電磁場に着目し、野外観測を基礎として陸上や海底における電磁場環境を明らかにしようとするものである．近年、地震発生に伴うさまざまな電磁気現象が報告されており、それらは震源から直接放射される電磁場変動、あるいは地震に起因する大気圏や電離層の電磁的擾乱現象と考えられている．本論文は、これらのみならず、広く空電現象として扱われる微弱な電磁場ノイズを、独自に開発した観測機器やモデルシミュレーションを駆使することによって、これまでにない高精度・高分解能で解析しようとする先駆的研究である．

本論文で行った観測は、１）空電を信号ととらえ、これを陸上と海底で同時に観測する海陸同期観測、および２）気象変化（台風、雷、濃霧等）に伴う大気電場の長期陸上観測のふたつから構成される．１）では、海陸それぞれの測定環境の相違に応じて、海底観測に極板アンテナ、陸上観測にはボールアンテナというふたつの異なるアンテナを使い分けている．海底観測では、アンテナ本体や測定電子回路の工夫等により、最小電場検出感度を従来の約２倍に向上させることに成功した結果、いままでにない帯域成分（4-5 kHz）の観測が可能となった．さらに、陸上観測用ボールアンテナの綿密な校正を行うことによって、その受信周波数特性がアンテナ回路の理論インピーダンス計算結果とよく一致することを示した．これらをもとに同期観測データを検討した結果、海底に到達する電磁場の主要帯域が 1 kHz 以下であることが判明した．

一方、２）の陸上長期観測では、台風や雷等の顕著な気象擾乱に伴う急激な電場変化から、大気静穏日における電場の日変化、さらには濃霧の発生に伴う微弱な電場変化に至る、広帯域の大気電場観測に成功した．残念ながら本論文では、地震発生に伴うと結論できる明瞭な電場変動の観測には至っていない．本論文で指摘しているように、より長期の多点観測による最適観測地点の発見や、雑音除去のための地下埋没型観測装置の開発など、さらなる改善も必要であろう．しかしながら、本論文で提示された観測機器と解析手法が、地震発生の前兆現象としての電磁場変動を観測するための有力な方法のひとつとなる高い可能性を秘めていることは疑いがない．なお本論文の主要な内容は、複数の関連学会で口頭発表されるとともに、国際学術誌にも掲載されている．

以上より、本論文は、地震発生を含む広範な自然電磁気現象研究について重要な知見を得たものとして価値ある集積であると認める．よって、学位申請者廣瀬智織は、博士（理学）の学位を得る資格があると認める．

ふりがな 氏　名（本籍）	ラビーン　ラビネシュ　ガウンデル Raveen Ravinesh Goundar　（フィジー）
学位の種類	博士（理学）
学位記番号	甲理博第21号
学位授与の要件	学位規則第4条第1項該当
学位授与年月日	平成20年3月24日
学位論文題目	Addition Chains in Application to Elliptic Curve Cryptosystems. （加法連鎖の楕円曲線暗号システムへの応用）
発表誌名	(1) *International Association of Engineers-International Journal of Applied Mathematics.*
審査委員	主査　教授　豊永　昌彦 副査　教授　下村　克己 副査　教授　松村　政博

論文の内容の要旨

Elliptic curve cryptography is widely accepted due to its fascinating feature of having smaller key length than RSA key length to provide same level of security. The basic building block of most elliptic curve cryptosystems over a finite field are computation of scalar multiplication kP and multi-scalar multiplication $k_1P_1 + k_2P_2 + \ldots + k_nP_n$, where P_i is an elliptic curve point, and k_i is an arbitrary integer. These computations are direct application of exponentiation and multi exponentiation, respectively. In the following four sections, we discuss the efficient computations by utilizing addition chains.

In section 1, the author proposes a strategy to find doubling-free (SPA resistant) short addition-subtraction chain for an arbitrary integer by utilizing a precise golden ratio. The proposed method, named *the golden ratio addition-subtraction chain method* (GRASC), has attained 12% to 28% reduced in the average chain length compared to other doubling-free addition chain methods.

In section 2, an efficient and secure (SPA resistant) elliptic curve scalar multiplication algorithm over odd prime fields, called *golden ratio addition chain method* (GRAC), is proposed as an application of GRASC. A GRAC based scalar multiplication algorithm can compute faster by 3% to 18% over the previous methods.

In section 3, GRAC in section 1 is extended to two-dimensional case. Simultaneous methods could be the most efficient for multi exponentiation, while efficiency of the cryptosystems is based on multi exponentiation. The author proposes a novel method to construct an addition chain for simultaneous multi exponentiation, then discusses the strategy for the two dimension case, a^eb^f and assume that such strategy could be generalized for arbitrary cases.

In section 4, the author has generalized the result of section 3 and applies a novel algorithm for simultaneous multi-scalar multiplication to cryptosystems. The previous methods utilizes double-and-add algorithm with binary representations, while the proposed method utilizes an efficient empirical method for finding addition chains.

The search for shortest addition chain is known to be an NP-complete problem. However, the challenge still remains to find shorter addition chains in order to enhance further efficiency, i.e. the further storage capacity reduction for the proposed algorithms can have greater impact on elliptic curve cryptosystems.

論文審査の結果の要旨

本論文「Addition Chains in Application to Elliptic Curve Cryptosystems」は，楕円曲線暗号の高速倍算に用いられる加法連鎖に関する新算法の提案とその応用に関する研究を述べたものである．

楕円曲線暗号法では、ＲＳＡ暗号における鍵の長さより短いキーで同等のセキュリティレベルが得られる（例えばＲＳＡ暗号で 1024 ビットのキー長は，楕円暗号では 160-ビットのキー長となる）ことからその実用化が期待されている．しかし、楕円曲線暗号法における基本的な演算操作はより複雑になり、その結果、楕円曲線暗号法における効果的な演算法が重要である。

本論文において，著者は楕円曲線暗号法における加法連鎖の重要性を示し，加法減法連鎖を使った新算法の提案をおこない，倍算と多重倍算への利用，および加法減算連鎖のその他への応用について述べている．

第１章は，本研究の動機付けと暗号の歴史的背景，および近年までの研究動向について詳細を述べている．

第２章は，楕円曲線に関する基本的な概念・群演算などについて述べ，次いで楕円曲線暗号について詳細を述べている．

第３章は，倍算と多重倍算について，二進数に基づく方法など幾つかのアルゴリズムを紹介している．

第４章は，加法連鎖と累乗法について，様々な種類の加法連鎖の定義と累乗計算方法について述べられている．

第５章は，黄金比を利用して，任意の整数の，倍算を含まない短い加法減算連鎖を見つける新算法（黄金比利用の加法減算連鎖法：ＧＲＡＳＣ法）を提案し，ＳＰＡ（Simple Power Analysis）攻撃に対する耐性に関しても言及している．

第６章は、第５章の結果であるＧＲＡＳＣ法を拡張し，楕円曲線暗号にける有限体上の楕円曲線の倍算法としてＧＲＡＣ法（黄金比加法連鎖法）を提案している．

第７章は、アーベル群における多重べき乗計算を効率よくおこなう新算法を提案している．具体的にはアーベル群 G と 2 つの要素 a, b においてより少ない群演算で $a^e b^f$ の計算手続きを目指したものである．これらは公開鍵方式において，特に楕円曲線に基づく暗号において重要であることを述べている．

第８章は、上記の加法連鎖計算法を用いて多重倍算の新アルゴリズムを提案し，楕円曲線暗号法における利用について述べている．

以上で提案されたアルゴリズムは，楕円曲線暗号法の演算法として高い価値をもち，また海外学会誌において採択され，高い評価を得ている．

本論文は，楕円曲線暗号における新算法とその応用に関する多くの有用な研究成果をあげ，またアルゴリズム・情報数学研究分野に寄与するところが大である．

以上から本論文の重要な提案と多くの価値ある知見は博士（理学）の学位論文として十分な価値を有するものと判断される．

ふりがな 氏　名（本籍）	テイ　リンリン 郑　琳琳　（中国）
学位の種類	博士（理学）
学位記番号	甲理博第22号
学位授与の要件	学位規則第4条第1項該当
学位授与年月日	平成20年3月24日
学位論文題目	量子エンタングルメント判定・定量法と物理シミュレーション法の研究
発表誌名	(1) International, ISBN: 0-7803-9240-X, Page (1313 ~ 1314), 2005 July 11
審査委員	主査　教授　豊永　昌彦 副査　教授　國信　茂郎 副査　教授　逸見　豊

論文の内容の要旨

量子コンピュータでは，計算素子（量子ビット）の量子状態の重ね合わせとビット間のもつれ相関（エンタングルメント）の非局所的な関係を使うことで超並列計算を実現すると理解されている．そのため現在のデジタルコンピュータで指数的な時間を要する計算問題が，量子コンピュータを用いることで短時間に解が得られる(例えば，数値因数分解問題は，量子計算を前提としたショアのアルゴリズムで短時間に解を得ることができる)．量子コンピュータの演算は，閉じた系(演算途中で他の系と一切相互作用しない系)で行わなければならないが，物理的に実装した量子コンピュータを完全に環境から孤立させることは不可能である．一方，エンタングルメント状態は，外界からの影響で容易に壊れる．もしエンタングルメント状態が壊れたなら，もはや正しい計算結果を得ることができない．そのため量子コンピュータの実装において計算精度を保証するには，計算途中のエンタングルメントの存否の判定やその定量化が不可欠である．また量子計算の途上において，エンタングルメント状態がどのような役割を果たすかが解明されていないという問題がある．

そこで申請者は，まず従来法よりもより少ない演算回数でエンタングルメントの存否を判定するアルゴリズムを研究した．

従来法は，全量子ビットを準分離可能なサブシステム(*TSS*)と部分的に準分離可能なサブシステム(*PSS*)に分類し，その数を判定するものであった．サブシステム全ての分割組合せを全て数え上げるため，量子ビット数が増加すると分割組合せを数え上げが指数的に増えてしまい，その作業自身の演算回数が膨大となる．

提案手法では，個々の量子ビットの組合せを全て調べる必要がないため、素子数と同程度の演算回数で判定することができる．

次に，申請者は，エンタングルメント定量化において新手法を提案した．同手法は，量子ビット間の相関関係の強弱からエンタングルメントを効率よく定量するものである．エンタングルメント状態において、量子ビット間の相関関係が強いほど重ね合わせた基底状態の数が少ない．また，各基底状態の確率振幅が異なるときより，各基底状態の確率振幅が同じときの方が相関関係は強い．従って，重ね合せた基底状態の数を基準とすると，エンタングルメントを定量できる．また，各々の基底状態の確率振幅を使えば，エンタングルメントの程度がもっと詳しく評価できる．

最後に，量子エンタングルメント状態が量子計算途上でどのように利用されているかを，解明する方法の１つとして，物理シミュレーション手法による実験的分析方法の研究を行った．

近年，磁性体研究モデルの１つである「1 次元のハイゼンベルグスピンモデル」が，量子コンピュータアーキテクチャの１つとなりうることが証明された．そこで同量子コンピュータを鈴木ートロッター展開原理に基づく磁性体スピンの量子モンテカルロ法を用いて物理シミュレーションすることで数値的にエンタングルメント状態が計算途上でどのような役割を果たすか観測する方法を検討した．現在，8 量子ビットの量子計算シミュレーターの実装を終え，量子計算精度の検証を終了している．これらに量子演算を実装すればエンタングルメント状態の種類を確認できることが期待される．

論文審査の結果の要旨

本論文「量子エンタングルメント判定・定量法と物理シミュレーション法の研究」は、量子計算における計算の正当性および有効性を判定する上で欠かせない量子ビット間のエンタングルメント量について，その存在判定と，量的判定法および具体的な実験方法に係る量子コンピュータのシミュレーション法に関する研究をまとめたものである．

量子素子を用いる計算では，量子状態をもつ素子の可干渉性（コヒーレンス）と素子間の量子絡み合い（エンタングルメント）を利用することで，古典的計算手法に見られない超並列計算が特徴の１つとされる．これらの性質により，既存のパソコンや大型計算機等で指数的時間を要する計算問題を短時間に解くことができる．ショア等は，近代的な暗号等が前提とする数値因数分解問題が量子計算を用いることで短時間に解けることを示している．（ショアのアルゴリズム）．量子計算機の実装における課題の１つとして，量子計算途中においてエンタングルメント状態の保持のため外界からの影響の低減である．さらには，精度の高い量子計算のためには，計算途中におけるエンタングルメント状態の定量的測定が重要となる．

本論文において，著者はこれら量子計算に伴うエンタングルメント状態について，その存否をより少ない手数（観測回数）で判定するアルゴリズム，エンタングルメント状態の量的評価方法，および量子系物理シミュレーション法を用いた実装を通じて実証する提案について述べており，従来に比べて優れた判定方法，定量的評価モデルの提案と新たな知見について述べている．

本論文の構成は，第1章において研究の背景となる量子計算の発祥から研究の歴史的流れについて説明し，量子計算を有効に利用したアルゴリズムにおいて量子素子のエンタングルメント状態が果たす演算における役割について説明している．これらを通じて本研究のエンタングルメント状態の存否とその定量的判定方法の意義を述べている．

続く第２章は，エンタングルメント状態の存否判定法について，その方法と従来提案されてきた手法について説明した後に．著者が提案するより少ない手数となる新判定アルゴリズムについて説明をおこなっている，まず，量子計算機を構成する多数の量子素子系（多量子ビット系）のもつ性質について．各素子が独立して振舞う「分離状態」と相互が従属的に振舞う「分離不可能状態」（エンタングルメント状態）について説明し，多量子ビット系の「分離」判定によりエンタングルメント状態の存否判定ができる原理（Gilles 等による存在の十分条件）を説明している．これらの原理を元に著者は，Gilles らの用いた分離状態に関する２つの概念 TSS（準分離）と PSS（部分的準分離）の両方を巧妙に利用してエンタングルメント状態の存否を少ない手数（観測回数）で可能とするアルゴリズムを提案している．具体的にはビット数を５とした多量子ビット系において，従来 65 回程度の観測回数が必要であった判定法と同じ結果を４回程度まで改善していることを示した．本提案手法は量子計算に関する国際会議で採択され評価されている．

第３章は，エンタングルメント状態の定量的判定法について，前章と同様に従来提案されてきた手法について説明した後に．著者が提案する新定量化モデルについて説明をおこなっている，まず，多量子ビット系のエンタングルメント状態の「強さ・弱さ」という概念について説明し，その様々な定量的指標について説明している．これらの説明を元に著者は，基底状態の確率振幅，基底状態数，またエンタングルメント状態を含む混合状態数等を用いた定量評価モデルを提案している．各指標の妥当性については具体的な例を挙げてその妥当性について明らかにしている．本提案モデルも，量子計算に関する国際会議で採択され評価されている．

第４章は，以上で提案した量子計算におけるエンタングルメント状態の判定法を量子計算機上で確認する方法についての提案である．その方法の１つとして計算機物理シミュレーションを用いた検証方法について説明している．具体例として磁性体スピンの鈴木－トロッター展開原理に基づく量子モンテカルロ法を用いた物理シミュレーションを作成し，その定量的観測をおこなっている．

これら量子計算において物理シミュレーションを用いる研究は，今後の量子計算の研究への新たな視点となることが期待できる．

以上より本論文の重要な提案と多くの価値ある知見は博士（理学）の学位論文として十分な価値を有するものと判断される。

ふりがな 氏　名（本籍）	ニエ　テイエン 聶　廷遠　（中国）
学位の種類	博士（理学）
学位記番号	甲理博第23号
学位授与の要件	学位規則第4条第1項該当
学位授与年月日	平成20年3月24日
学位論文題目	Post Layout Watermarking Design Method for IP Protection （知的財産（設計資産）保護のためのポストレイアウト設計におけるウォーターマーキング手法）
発表誌名	(1) International Symposium on Circuit and Systems 2005 (ISCAS2005), pp. 6206-6209, May, 2005. (2) 42th Conference on Design Automation (DAC'05), pp. 218-221, June 13-17, 2005. (3) IEICE Trans. Fundamentals E90-A, No. 9, pp. 1932-1939, Sep. 2007.
	審査委員　主査　教授　豊永　昌彦 副査　教授　國信　茂郎 副査　教授　大坪　義夫

論文の内容の要旨

The progress of semiconductor manufacture process technology has made it possible to mount a huge number of transistors on a chip that includes a perfect system on it. IP (Intellectual Property) reuse plays an important role in modern IC design. Nevertheless, while the re-useable design, so-called IP, is effective in reducing both the SOC design cost and TAT (Turn Around time) of development, the design method also exposes the risk on security. As most IP designs need a great deal of time and efforts for development or verification, the IP owners desire some guarantees that those contents are not illegally re-distributed by the consumer. IP users also desire some guarantee that the contents they bought are legal. Therefore IP Protection (IPP) technique is get concerned inevitably.

In recent years, watermarking technology has become an effective fashion for IPP, both in pre-processing and post-processing. Most of the techniques converge on the pre-processing that the watermark-constrained IC design is designed form the top stage so that it leads to extra design costs such as wire-length, interconnection delay, etc. There are several watermarking techniques on post-processing which try to add watermark constraints into the designed IC without damaging the origin. But the extra cost brought by the watermarking is really a trouble to the designers.

In this thesis, the author introduced a new and different watermarking system for IPP on post-layout design stage. The author conducted the watermarking system in such process:

First, the signature of the designer is encrypted with a secret key by DES (Data Encryption Standard) to produce a bit string. Second, the bit string is then embedded into the layout design as constraints by using a specific incremental router. Third, the signature can be extracted accurately from the watermarked design by the system.

The proposed IPP system also has a strong resistance to the attack on watermarking due to the DES functionality. This watermarking technique uniquely identifies the circuit origin, yet is difficult to be detected or fabricated without our tool.

We evaluated the watermarking system on IBM-PLACE 2.0 benchmark suites. The experimental results show the system robustness and strength: the system success probability achieves 100% in suitable time with no extra area and wire length cost on design performances.

論文審査の結果の要旨

本論文「Post Layout Watermarking Design Method for IP Protection」は、大規模化するＬＳＩ設計において，有用とされる既存設計資産（ＩＰ：設計知的財産）の普及の障害となる「不正利用防止」「正規品認証」など設計資産保護について，レイアウト設計完了後に適用可能な新手法の提案とその検証についての研究をまとめたものである．

既存の回路設計資産（IP）は，膨大な数のトランジスタを利用するＬＳＩ設計を迅速にすすめる上で不可欠となり，これら設計資産を正規に流通させる認証技術や不正利用防止技術が望まれている．これらを総じてＩＰ Protection（ＩＰＰ）技術と呼ばれている．一方，ＩＰＰ技術の導入に伴い，設計コストの増加や性能低下への対策が重要となる．

本論文において，著者はこれらＩＰＰ技術について，レイアウト設計後に「電子透かし（Watermarking）」を印する新手法，および，これらを有機的に活用するための印加から情報抽出までの総合的システムの提案と従来システムに比べた強靭性や実用性について新たな知見を述べている．

本論文の構成は，第１章において研究の背景となるＬＳＩ設計システムと設計資産（IP）の意義の説明，および防護技術として電子透かし（Watermarking）の概要について述べ，本研究の新たなレイアウト設計後の電子透かし法の意義を述べている．

第２章は，ＬＳＩ設計システムにおけるレイアウト設計を計算機支援するソフトウェア技術について，ＬＳＩ機能レベルから直接半導体製造で用いられる回路パターン設計までの構成を述べ，本研究が対象とする回路パターン設計（レイアウト設計）が回路分割技術，配置設計技術，配線技術で構成されることについて概要を説明している．

第３章は，本研究に関する先行研究の概要を紹介し，これら先行論文等での保護技術の提案がほぼＬＳＩ設計システムの中心あるいは，その前段階において適用されていることに関した問題点や課題を整理して述べている．さらに本提案であるレイアウト設計以後の段階で電子透かし技術を利用することの利点について説明している．

第４章は，本研究で提案するレイアウト設計後（Post-Layout）の電子透かし方法について，システム構成の概要，印加情報の暗号化処理についての意義と実装方法の概要，さらに電子透かしを実現するために考案した特殊な配線手法についてアルゴリズム，動作とうについて紹介し，ＬＳＩレイアウト設計データに情報を印加する方法（エンコーダ），これを読み出す方法（デコーダ）について詳細に説明している．

第５章は，提案するＩＰＰのための電子透かし法を，ソフトウェアシステムとして実装し，簡単な試験用データを用いた実験，実回路データを用いた実験等を緻密に豊富におこなったことを説明し，さらにその安全性や強靭性について詳細に評価している．

本提案手法は，配線部について，またシステム全体として国内・国際会議で発表され高い評価をうけている．得に，ＬＳＩ設計支援ソフトウェア分野において最高レベルとされている国際会議 Design-Automation Conference において採択された実績は，特筆できるものである．

以上から本論文の重要な提案と多くの価値ある知見は博士（理学）の学位論文として十分な価値を有するものと判断される。

ふりがな 氏　名（本籍） 学位の種類 学位記番号 学位授与の要件 学位授与年月日 学位論文題目 発　表　誌　名	ふくとめ　たかひこ 福留　孝彦　（高知県） 博士（理学） 甲理博第24号 学位規則第4条第1項該当 平成20年3月24日 Effect of Soft Modes on the Shear Viscosity of Quark Matter （クォーク物質のずれ粘性に対するソフトモードの効果） (1) Phys. Rev. D 72, 094016 (2005) 審査委員　主査　教授　岩崎　正春 副査　教授　松村　政博 副査　教授　津江　保彦

論文の内容の要旨

超高温・超高密度状態を地上の実験室で実現するために、高エネルギー重イオン反応実験が進められ、米国立ブルックヘブン研究所の相対論的重イオン衝突型加速器(RHIC)では非閉じ込め相転移温度を超えたと考えられている。その実験データは、そこで生成されたクォーク・グルオン・プラズマと呼ばれる物質が、これまで予想されていた気体のようなものではなく、実際には粘性がほとんどない液体のように振る舞うことを示している。

この研究は、量子色力学の有効模型の一つである Nambu-Jona-Lasinio 模型のもとで、線型応答理論による久保公式を用いてクォーク物質の粘性係数を計算したものである。

久保公式から出発して、粘性係数を遅延グリーン関数で表した。この遅延グリーン関数を虚時間形式に変換し準粒子ＲＰＡを適用して計算した結果、粘性係数をクォーク・スペクトル関数で表現する簡明な公式を得た。この粘性係数を求める公式は、クォーク・スペクトル関数の２次形式をエネルギーと運動量に関して積分する形で与えられており、クォーク物質の粘性係数は、クォーク・スペクトル関数を決定する自己エネルギーがわかれば計算できることを示している。

カイラル相転移の前駆現象の一つとして相転移温度を超えた付近で存在すると考えられているソフトモード（クォーク・反クォーク対の集団モード）はボソン型の準粒子として振るまい、粘性係数を含む輸送係数に大きな影響を与えると考えられる。我々はクォークの自己エネルギーがこのソフトモードとのカップリングにより獲得されるとして計算し、自己エネルギーをソフトモードのスペクトル関数の積分として表した。

以上の結果を用いて、相転移温度を超える領域でのクォーク物質の粘性係数及びそのエントロピー比の数値計算を行った。相転移温度を超えた付近（161<T<200 MeV）でのソフトモードにおける粘性係数はほぼ一定値で、比較のために計算した粒子モードにおける粘性係数よりも１桁オーダーが小さく、実験が示唆する完全流体に近い振る舞いと整合する結果を得た。これは、クォークがソフトモードとのカップリングにより大きな自己エネルギーを獲得し、そのスペクトル関数が抑制される結果として粘性係数が小さくなっていると解釈される。一方、この領域を超えて温度が上昇すると、粘性係数は増大し粒子モードによる値に近づく。これは温度の上昇に伴いソフトモードが減衰し、そのことによってクォーク・スペクトル関数が増大することに対応している。化学ポテンシャルを変化させて同様の計算を行ったが、粘性係数は化学ポテンシャルに殆ど依存しなかった。これはソフトモードの強さが殆ど化学ポテンシャルに依存しないことで説明される。これらの結果は、クォーク物質の粘性係数に対して、ソフトモードの存在が本質的な役割を果たしていることを強く示唆している。

論文審査の結果の要旨

最近のRHICでの高エネルギー重イオン衝突実験によると、クォーク物質(クォーク・グルオン・プラズマ)が生成され、しかもその状態は予想に反して、粘性を持たない完全流体に近いものであることが明らかになった。この研究は、量子色力学の有効模型の一つである Nambu-Jona-Lasinio 模型のもとで、線型応答理論による久保公式を用いてクォーク物質の粘性係数を計算し、粘性が小さくなる物理的要因を明らかにしようとするものである。

ずれ粘性率に対する久保公式を温度グリーン関数で表し、準粒子乱雑位相近似(リング近似)を用いて計算した結果、粘性係数はクォーク・スペクトル関数の２次形式の積分形で書けることを示した。したがって、粘性係数の計算は、クォーク・スペクトル関数を決定すること、つまりクォークの自己エネルギーがわかれば求まることが示された。特にその虚数部はクォークの平均自由行程を表し、粘性係数に強く関係することが指摘された。

本論文では、クォークの運動を妨げ自己エネルギーを決定する主要な要因としてカイラル相転移の前駆現象の一つであるソフトモード（クォーク・反クォーク対の集団運動モード）に着目した。すなわち、クォークの自己エネルギーがこのソフトモードとの結合により決定されると仮定して、自己エネルギーをソフトモードのスペクトル関数の積分として表した。

以上の結果を用いて、カイラル相転移温度を超える温度領域でのクォーク物質の粘性係数およびそのエントロピー比の数値計算を行った。相転移温度を超えた付近（170 MeV<T<200 MeV）でのソフトモードにおける粘性係数はほぼ一定値で、実験が示唆する完全流体に近い振る舞いと整合する結果を得た。比較のために、粒子モードとの結合によって計算された粘性係数よりも１桁オーダーが小さくなっていることを確かめた。これは、クォークが集団的なソフトモードとの強い結合により大きな自己エネルギーを獲得し、そのスペクトル関数がブロードな形になる結果として理解される。一方、温度がさらに上昇すると、ソフトモードは弱くなりスペクトル関数は自由粒子のスペクトル関数に近づき、粘性係数は増大する。また、クォーク密度(化学ポテンシャル)を大きくして同様の計算を行ったが、粘性係数はクォーク密度にあまり依存しなかった。これはソフトモードの強さが殆ど化学ポテンシャルに依存しないことで理解される。本研究により、クォーク物質の小さい粘性係数はクォーク物質のカイラル相転移に伴うソフトモードにより説明されることが結論づけられた。また、この理論的モデルが、「粘性係数は温度の上昇とともに増加する」という新たな予想を提起している点も重要である。

以上より、申請論文はハドロン物理学分野に新たな知見を加えるものであり、博士論文としての充分な価値を有するものと認める。

ふりがな 氏　名（本籍）	ミン　リン　ウー Min Lwin Oo　（ミャンマー）
学位の種類	博士（理学）
学位記番号	甲理博第25号
学位授与の要件	学位規則第4条第1項該当
学位授与年月日	平成20年3月24日
学位論文題目	The stable extendibility of the power of the normal bundle associated to an immersion of RP^n and its complexification. （RP^n のはめ込みに従属する法束とその複素化の巾の安定拡張性）
発表誌名	(1) Hiroshima Math. J. 37 (2007)
審査委員	主査　教授　逸見　豊 副査　教授　下村　克己 副査　教授　大坪　義夫

論文の内容の要旨

Let F stand for either the real number field R or the complex number field C. Let X be a space and A its subspace. A t-dimensional F-vector bundle ζ over A is said to be extendible to X if and only if there is a t-dimensional F-vector bundle over X whose restriction to A is equivalent to ζ. The first purpose is to study the extendibility and stable extendibility on the power $\upsilon^r=\upsilon\otimes\cdots\otimes\upsilon$ (r-fold) of the normal bundle υ of RP^n in R^{n+k} and its complexification $c\upsilon$, where $r>0$ and $k>0$. Then we have the following results.

Theorem A. Let k, n and r be positive integers with $n<k^r$. Then, the following three conditions are equivalent:

(1) υ^r is extendible to RP^m for every $m\geq n$.

(2) υ^r is stably extendible to RP^m for every $m\geq n$.

(3) There is an integer a satisfying

$$(2n+k+2)^r-k^r \leq a2^{P(n)+1} \leq (2n+k+2)^r+k.$$

Here, $P(n)$ is the number of integers s such that $0<s\leq n$ and $s\equiv 0, 1, 2$ or $4 \bmod 8$.

Theorem B. Let k, n and r be positive integers with $\langle n/2\rangle \leq k^r$, where $\langle x\rangle$ is the smallest integer n with $x\leq n$ for a real number x. Then, the following three conditions are equivalent:

(1) $c\upsilon^r$ is extendible to RP^m for every $m\geq n$.

(2) $c\upsilon^r$ is stably extendible to RP^m for every $m\geq n$.

(3) There is an integer b satisfying

$$(2n+k+2)^r-k^r \leq b2^{[n/2]+1} \leq (2n+k+2)^r+k^r.$$

Here, $[x]$ denotes the largest integer n with $n\leq x$ for a real number x.

Furthermore, we give an example of a 2-dimensional R-vector bundle over RP^8, which is stably extendible to RP^9 but is not extendible to RP^8. The second purpose is to study the maximum $s(\upsilon)$ of the dimensions m such that υ is stably extendible to RP^m.

論文審査の結果の要旨

空間Xの部分空間A上のベクトル束ξがXに拡張可能であるとは，X上のベクトル束αでAに制限したときξと同型になるものが存在するときをいう．また，Aに制限したときξと安定同値になるαで，ξと同次元のものが存在するとき，ξは安定拡張可能であると呼ぶ．Imaoka-Kuwanaは1999年にSchwarzenbergerの定理を改良し，実射影空間上のベクトル束に対しては，それが任意の高次元実射影空間に安定拡張可能であることと，線束のWhitney和に安定同値であることが同値であることを示した．これにより，実射影空間上のベクトル束に対して，どのような条件下で任意の高次元実射影空間に安定拡張可能であるかということが重要な問題であることがわかる．

この問題について，これまでに実射影空間の接束に関しては多くの結果が得られている．本論文では，実射影空間からユークリッド空間へのはめ込みを考え，その法束の任意のベキが高次元実射影空間に拡張可能あるいは安定拡張可能になるための条件を調べている．方法は，KO理論を用いたものである．実射影空間のKO群は，標準線束で生成される有限巡回群であることが知られている．そこで，法束の任意のベキをKO群のなかで標準線束を用いてあらわし，それにより，任意の高次元実射影空間に安定拡張可能であるための条件を調べるというのが本研究の主なる方法である．申請者はこの方法を用いて，安定拡張可能であるための必要十分条件を決定した．さらにその条件が拡張可能であるための必要十分条件にもなっていることも示している．

次に，法束の複素化についても同じ問題を考え，それの任意のベキについて，任意の高次元実射影空間に安定拡張可能であるための必要十分条件を決定し，同時にそれが拡張可能である必要十分条件になっていることも示している．

これらの結果は，安定拡張可能であることと拡張可能であることが同値であることを示しているが，これは一般には成り立たないことが知られている．申請者は，これを示す興味深い例を与えている．それは，２次元実射影空間上の２次元実束で３次元実射影空間に安定拡張可能であるにもかかわらず，拡張可能ではないという例である．

最後に，任意の高次元実射影空間に安定拡張可能とはならない場合の法束について，安定拡張可能となる実射影空間の次元の最大値に関する研究成果を述べている．これはすべての場合を網羅したものでなく，部分的な結果に過ぎないが，多くの典型的な場合について調べており，興味あるリストといえる．

本研究遂行には，ベクトル束の一般論や，KO理論，さらにはコホモロジー環やStiefel-Whitney類などについての知識が必要である．また，本論文は射影空間の法束の研究に対して価値ある結果であると認められ，以上のことより，学位申請者Min Lwin Ooは，博士（理学）の学位を得る資格があると認める．

ふりがな 氏　名（本籍） 学位の種類 学位記番号 学位授与の要件 学位授与年月日 学位論文題目 発表誌名	オウ　トウセイ 王　冬青　（中国） 博士（理学） 甲理博第26号 学位規則第4条第1項該当 平成20年3月24日 フラクタル次元による配線推定とSimulated Annealing法の改善に関する研究 (1) IEEE Asia Pacific Conference on Circuit and System (APCCAS 2006), pp.485-488(Dec., 2006) 審査委員　主査　教授　豊永　昌彦 副査　教授　國信　茂郎 副査　教授　逸見　豊

論文の内容の要旨

携帯電話をはじめとする多くの情報家電に，IC（集積回路：Integration circuit）チップやLSI（大規模集積回路：Large Scale Integration）がコア部品として利用されている．

これらLSIの高性能化は，製造プロセス技術の微細化の進展が欠かせない．しかし微細化が0.5μmを超えたころからLSI製造におけるDSM（Deep-Sub-Micron）問題が顕著になった．DSM問題の１つに，製造パターンの微細化により，配線幅が狭くなるために抵抗が増大し，また配線間に寄生電荷容量が発生し，信号遅延が長大化する問題である。この問題解決には、回路パターンを設計するレイアウト設計の考慮が不可欠である．また，これら複雑な設計制約に対して効率よくレイアウト設計を行う手法が求められる．

そこで申請者は，論理設計段階においてネットリスト（論理素子とその接続関係を記述したリスト）からレイアウト配線遅延を推定する手法を提案した．提案手法は，ネットリストを二部グラフで表現し，個別の配線についてフラクタル次元解析手法を用いて次元の高さ(接続の複雑さ)に基づいてそのレイアウトにおける配線長を推定するものである．従来の推定方法は，ネットリストのグラフにおける次元(接続端子数)に基づく推定が中心であった．提案手法の特徴は，素子（セル）個別に「局所的なフラクタル次元」を求める点にある．この個別フラクタル次元がセル相互の遠近と相関を持つと考えた．具体的な相関関数は，レイアウト設計分野で用いられるベンチマーク回路を用いて自動配置結果とフラクタル次元から決めることができ，配線長さと相関係数-0.3 が得られた．すなわち、個別フラクタル次元とその配線長に弱い反比例関係があることを見出した．

DSM 問題のような複雑な課題が設計制約に加わるとレイアウト設計の処理時間は長期化する．そこで，申請者は，LSI レイアウト設計における配置法において用いられる最適化手法Simulated-Annealing（SA:擬似焼きなまし）法の高速化への新手法を提案した．SA手法は結晶成長(Crystal Growth)を配置モデルに置き換えて物理シミュレーション法を用いて組み合わせ解を求める方法である．同手法は，モンテカルロシミュレーション法に基づいており，乱数精度やくり返し計算回数等により結果がばらつく。本来，SA 過程は単純マルコフ過程(1 つ前の状況のみに依存して次の状態が決まる)であるが，申請者はあえてSA過程において毎温度に熱平衡達後にばらつく解を記憶させておき，次の温度過程において最良の解を初期値として続けていくという方法，TOSA（Tracing Optimal SA）手法を考案した．理想的なモンテカルロ法と異なり，乱数の精度，熱平衡実現へのくり返し回数の不十分さから，現実のシミュレーションにおいて単純マルコフ過程が実現していないと考えたからである．

本手法の効果を検証するためにレイアウト自動配置として実装し，ベンチマーク回路で実験したところ，SA手法に比べて８％～１４％の配線長の改善が見られた。また，同等な品質の解を得るまでの計算時間は，20％の改善が見られた。

論文審査の結果の要旨

本論文「フラクタル次元による配線推定とSimulated Annealing法の改善に関する研究」は、大規模化するＬＳＩ設計において，重要となる設計性能見積もりにおける論理設計段階からの「配線性能見積もりの不確実性」を解決するための提案手法に基づく配線長推定法と検証，また，大規模レイアウト設計において問題となる配置品質の劣化に関する改善法の提案およびその検証についての研究をまとめたものである．

ＬＳＩ製造技術の微細化に伴い，回路上の配線に起因する信号遅延が著しく大きくなる．そのため高性能ＬＳＩ設計において，製品の性能は，製造パターンを作成するレイアウト設計後まで確定しない．ＬＳＩ設計後にタイミング等で不都合があれば，設計の初期段階に戻るという設計期間の長期化と製造コスト増大になる．この設計繰り返しをなくすには，設計途中においてレイアウト設計後の配線長を見積もる技術が重要となる．一方，レイアウト設計そのものにおいても，微細化に伴い扱う素子数が増大し設計目標（性能目標）そのものを達成することが難しくなっている．より高品質なレイアウト設計方法が望まれる．

本論文において，著者はLSI設計の論理設計段階で利用できるネットリストからレイアウト配線長を推定する新手法を提案し，レイアウト設計における配置設計で用いられる最適化手法Simulated-Annealing 法の改善法を提案しており，これらを通じた高性能ＬＳＩ設計フローについて述べている．

本論文の構成は，第1章において研究の背景となるＬＳＩ設計支援システムにおける配線推定法の概要とその意義，また配置設計で用いる最適化手法Simulated Annealing法について簡単に紹介し，本研究の意義を述べている．

第2章は，ＬＳＩ設計支援システムの各設計段階における詳細な説明をおこない，先進的なＬＳＩ設計における課題について述べている．

第3章は，レイアウト設計後の配線長を推定するために導入するフラクタル次元について，その歴史的背景や具体的な例を用いて概念説明をおこない，これを論理回路の素子群と素子間の接続情報（ネットリスト）に適用した回路のフラクタル次元で接続の複雑さを表す先行技術の紹介とその方法について述べ，著者が提案する各素子個別の配線長推定の指標とした個別フラクタル次元について説明をしている．新たに導入した個別フラクタル次元と素子間の推定配線長との相関について，実用回路に近いベンチマーク回路primaryとIBM01の実験をおこない配線長との相関を見出している．本研究は，国内学会において発表されたものである．

第4章は，著者が提案する最適化手法Simulated-Annealing（擬似焼きなまし）法の高品質化法について述べている．新手法は，簡単な配置プログラムのSimulated-Annealing過程において見られた初期値依存性に注目し，現状のSimulated-Annealing法では単純マルコフ過程でないことを実験的に示し，解を選択的に採用した改善法 TOSA について述べている．また，その処理手数の削減についても言及している．これらの新手法は，ベンチマーク回路を通じて計算機実験により，従来手法と比較されており，Simulated-Annealing 法と比べて最大１４％の配線長改善を得ている．また処理時間についても20％程度の改善された結果を得ている．本研究は，国際学会において採択され高い評価を得たものである．

本論文は，ＬＳＩ設計自動化ソフトウェアにおける配線推定問題と素子配置設計の最適化問題に関して２つの提案により有用な研究成果をあげ，情報科学研究分野に寄与するところが大である．

以上から本論文の重要な提案と多くの価値ある知見は博士（理学）の学位論文として十分な価値を有するものと判断される。