様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ６ 月　 ８ 日現在

機関番号：１７１０２
研究種目：基盤研究(C)（一般）
研究期間：2013～2015
課題番号：２５３３０２６２

研究課題名（和文）大規模組合せ最適化問題のEPR解法に関する研究

研究課題名（英文）A study on EPR method for solving large scale combinatorial optimization problems

研究代表者
藤田　博（Fujita, Hiroshi）

九州大学・システム情報科学研究院・准教授

研究者番号：７０２８４５５２

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：　大規模組合せ最適化問題を解決する手法に関する研究を行った。ソフト制約に基づく効率的な解探索機構によってSAT技術を強化したシステムSCSatを開発し、これをRamsey数に関する問題解決に応用し、R(4,11)≧101などの新たな結果を得た。
　大規模問題に対応した基数制約の符号化に関して複数の手法を考案し、それらをQMaxSATシステムに実装することにより、従来より広範なMaxSAT問題を解くことが可能となった。国際的競技会において優秀な成績を収めた他、暗号の安全性に関する問題や帰納論理プログラミングの模擬実行などの応用事例研究において有益な成果を得た。

研究成果の概要（英文）：We have developed methods for solving large scale combinatorial problems. As a result, SCSat system which is based on SAT techniques enhanced with a mechanism to utilize soft constraints for effective solution search, succeeded to solve several hard mathematical problems on Ramsey numbers including the new result R(4,11)>=101.
Also we have developed several ways to encode cardinality constraints into SAT problems that are used in solving large MaxSAT problems. Equipped with the encoding mechanism, QMaxSAT system has been improved so that much larger problems can be solved than before, and achieved excellent results in international competitions on systems of this kind. Our successful case studies include security solutions for cryptography and an alternative implementation of inductive logic programming.

研究分野：知能情報学

キーワード：組合せ最適化　Ramsey数　SAT　MaxSAT　基数制約

１．研究開始当初の背景

(1)　近年、命題論理の充足性判定（SAT）技術の進展が目覚しい。しかし、問題の規模の大きさに対する弱点は、NP 完全問題という原理上の困難に起因しており、従来も今後も大きな課題として我々の前に立ちはだかっている。この問題に対処する工学的な能力を増強し、解ける問題の範囲を少しでも拡げることは、実践的に有益である。

(2)　一つの対処方として、SAT より上位の一階述語論理(FOL)の定理証明に関する手法に手掛かりを求めることができる。しかしながら、FOL に規模の問題がないわけではない。むしろ、原理上の困難の度合いは無限領域を基本的な土俵とする FOL の方が、有限的な SAT よりはるかに深刻となる場合が多い。そこで、FOL 対応ながら対象領域が有限な問題を専門に扱う EPR(Effectively PRopositional)と称する分野に我々は着目した。FOL の高度な問題記述能力と、SAT の先進的な求解能力の良い所取りを狙う実践的な分野といえる。

(3)　我々は EPR 解法の一種である MGTP と称するシステムの研究開発に長年携わってきた。本研究はその研究の延長線上にあるが、著しい勢いで発展中の SAT 技術のさらなる進化を目指し、より大規模な問題に適用するための方策を見出すことに焦点を当てた。

２．研究の目的

(1)　SAT 技術および EPR 技術を基盤として、より大規模な問題を解くための手法を確立する。具体的には、探索空間を劇的に削減したり、希少な解を選好的に嗅ぎ分けて探すことを容易にする探索手法を与える。

(2)　最適化問題を MaxSAT 問題に変換し、高効率な SAT 技術によって解く方法を確立する。特に、本手法で一つの中心的な機能となる基数制約について、SAT 符号化の規模に関する弱点を解消し、より実践的問題に対処可能とするため、新たな基数制約方式の考案と実装を行う。

３．研究の方法

(1)　大規模組合せ問題について

数学の未解決問題の一つである Ramsey 数に関して集中的に研究を行う。これは、単純明快な CNF 形式で問題記述が与えられ、かつ規模が極めて大きく、SAT 技術の能力を検定するのに格好の題材である。

(2)　基数制約について

コンパクトな符号化方式を考案し、MaxSAT ソルバーへの組み込みを行う。国際的な競技会での上位入賞を狙い、ベンチマーク問題を用いたチューニングを行う。また、ベースとなる SAT ソルバーの改良を行う。

(3)　MaxSAT 解法の応用について

Ramsey グラフの探索に適用する。さらに、暗号の安全性検定に関する問題、および帰納論理プログラミングの模擬実行など、実践的題材を用いた事例研究を行う。

４．研究成果

(1)　大規模組合せ問題について

主要な事例研究の一つ、Ramsey 数に関する問題とは、以下のようなものである。

「N 頂点の完全グラフ K_N の各辺を２色で塗り分けたとき、その中に第１色の辺のみからなる p 頂点の部分完全グラフ Kp と、第２色の辺のみからなる q 頂点の部分完全グラフ Kq の、どちらも含まれないようにできるか？」N が p,q に比べて十分大きいと、答えは「できない」となる。そのような N の最小数を Ramsey 数といい、R(p,q)と表す。例えば、R(3,3)=6, R(4,4)=18 などが分かっている。

しかしながら、R(5,5)は 43 以上 49 以下としか分かっていない。任意の p,q について R(p,q)を与える一般式は未だ無く、未解決問題となっている。そして、R(p,q)のできるだけ大きな下界を求めるために、コンピュータの利用が不可欠とされている。すなわち、上記の問題に肯定的な答えとなるグラフ（Ramsey グラフといい、RG(p,q,N)と表す）を具体的に示すことにより、R(p,q)＞N を保証するのである。これは SAT 技術の格好の応用問題と言える。

①　付加制約による探索空間の削減

Ramsey グラフは、問題の対称性から極めて対称性の高いものが期待される。しかしながら、実際にはわずかに対称性を損なったものや、複数の対称性を含み、一見統一性に欠くパターンのものが正解の場合がある。我々は、そのような多少いびつな Ramsey グラフを効率的に探索する手法を開発した。

Ramsey グラフを隣接行列（要素は第１色を 1、第２色を 0 とする）で表すと、まずは左上から右下がりの主対角線に関して対称となる。これは、Ramsey グラフが元来無向グラフであることから必然である。ちなみに、主対角線上の要素は未定義である。多くの Ramsey グラフは、この主対角線に沿った綺麗なストライプ模様のものとして得られる。

ところが、Ramsey 数近傍の Ramsey グラフ（Ramsey 数より１少ない頂点数の場合、臨界 Ramsey グラフという）では必ずしも完璧なストライプ模様のものが存在するとは限らない。わずかに乱れたものだったり、まったく異なる対称性に起因する模様だったりする。このような Ramsey グラフの探索にあたっては、想定される対称性について、一旦厳密な制約記述を付加した後、これを徐々に緩和するという方法が有効であった。

対称性の種類としては、ストライプ模様以外に隣接行列の左下から右上がりの副対角線に関する対称性、市松模様などが効果的であった。複数の対称性を組み合わせることも有効であった。実際、RG(4,6,34)では、完全な副対角線対称性と部分的な市松模様制約を満たす解が得られた。さらに、対称性制約の対象領域を隣接行列の全域ではなく一部に限定することも有効であった。

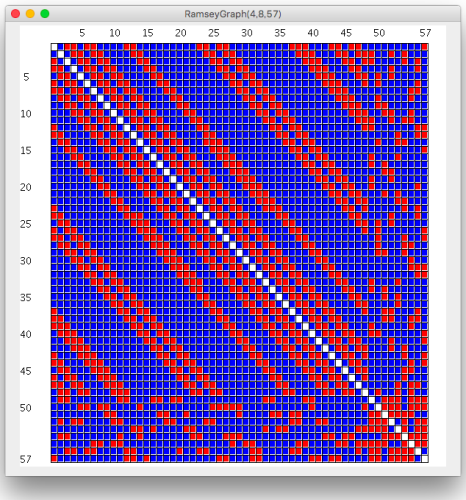

図１　Ramsey グラフ RG(4,8,57)

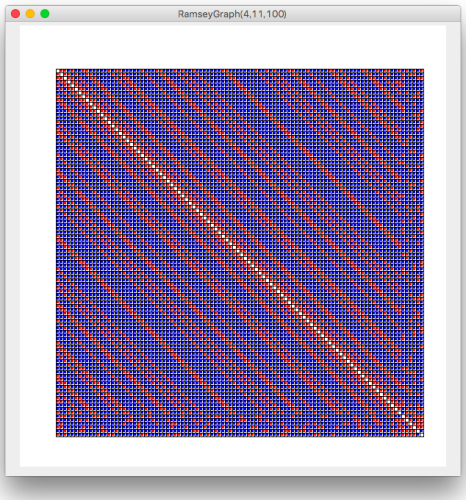

図２　Ramsey グラフ RG(4,11,100)

② SCSat システムの開発

対称性の付加制約を部分的に緩和する手法として、ソフト節の概念が有効であった。問題設定上、満たすことが必須の論理式をハード節、必ずしも満たす必要がない論理式をソフト節という。ソフト節の重要度について、推論探索中の状況に応じて動的に評価更新する機構も有効であった。これらの手法を実装したシステム SCSat を３種類開発した。

SCSat1 は、推論中におけるソフト節とハード節の扱いの差異が限定的である。そして、再試行の際、評価値の低いソフト節たちを一定量棄却する。図１の RG(4,8,57)は SCSat1 によって初めて得られた。

SCSat2 では、SCSat1 の拡張機能として、探索中に得た各種情報から、新たなソフト節を自動的に導く機構を搭載した。しかしながら、この機能の有効性は未だ十分とは言えず、今後の研究課題を残している。

SCSat3 は、推論中におけるソフト節とハード節の扱いの差異が SCSat1 よりさらに限定的である。しかし、より対称性の高い解を選好的に探索するという誘導機能について、SCSat1 と同等以上の能力を有することが分かった。実際、図２の RG(4,11,100)は SCSat3 によって初めて得られた。

③ MaxSAT による Ramsey グラフ探索

対称性ソフト制約を最大限に満たすような Ramsey グラフを得ることは、Ramsey グラフ一般の特性について推論する上で有益である。ただし、Ramsey グラフの場合、１個の解を得るのさえ困難であるから、MaxSAT のように非最適解が多数存在し、その発見が容易であることを前提とした解法は、問題規模が小さいものにしか適用できない。

我々は、最新の QMaxSAT ソルバーを用いて、RG(3,6,17)，RC(3,7,22)，RG(3,8,27)，および RG(5,5,42)などの臨界 Ramsey グラフについて、ストライプ模様の乱れが最小なものを得ることができた。

④ Ramsey 数の下界に関する世界新記録

Ramsey 数に関する世界記録は長らく更新されていなかったが、我々は本研究の成果として RG(4,8,57) や RG(4,11,100) などの Ramsey グラフを発見することができた。それぞれ R(4,8)≧58，R(4,11)≧101 なる下界を保証する。これらは現時点（2016 年 6 月）において世界新記録である。

(2) 基数制約および MaxSat について

我々は、すでに部分 MaxSAT 問題を解決するシステム QMaxSAT を開発し、関連システムの性能を競う国際的な競技会のある部門で優勝するなど、多くの成果を上げていたが、以下の二つの課題を残していた。

① 基数制約のコンパクトな SAT 符号化

基数制約の SAT 符号化が巨大化することが障壁となっており、これを軽減することが喫緊の課題となっていた。そのために Modulo Totalizer と呼ぶ方式を考案した。端的に言えば、単純な数え上げに位取り算術を導入するものだが、効果は覿面であった。

これにより、従来の単純 Totalizer に比べて SAT 符号化後の変数や節の個数は格段に減少し、これを組み込んだ QMamSAT ソルバーの許容する問題は著しく広範になった。

② 重み付き MaxSAT 問題への対応

従来の基数制約は単に個数のカウントを行うもので、量を測るには不適当であった。しかし、加算すべき重みの組合せが有限個数であることに着目すれば、基数制約を比較的容易に拡張できる。実際、我々は Weighted Totalizer と呼ぶ方式を考案、実装した。

これにより、QMaxSAT は重み付き MaxSAT 問題についても、従来より大規模のものを効率良く解くことができるようになった。

この他にも、Weighted Totalizer に Modulo Totalizer 方式を組合せた Weighted Modulo Totalizer を始め、複数の拡張方式を考案し、さらなるコンパクト化および、それらを利用した効率的推論の可能性を示した。

(3) その他、主要な事例研究の成果

① 暗号系の安全性に関する問題

AES 暗号系においては、部分的に得られた暗号処理系内のデータから、鍵情報を復元することが原理的に可能である。従って、復元のための計算量が大きくない場合には、その悪用が現実的な脅威となりかねない。その脆性を確認する目的で、この問題を MaxSAT 問題として定式化し、実際的な設定において解いてみた。その結果、十分警戒すべき事例が生じ得ることが判明した。

② 帰納論理プログラミング

化学実験においては、多くの実験データを基に、各原料の量、温度、湿度、圧力等の各種パラメタに応じて、所望の特性に関する値が如何に変化するか、その一般的な法則を得たい。帰納論理プログラミングは一つの有効な手段であるが、やはり探索空間の規模の莫大さに起因する困難を課題としていた。

我々は、基本的に連続値の諸量を離散的な区間に量子化し、関数記号のない EPR 問題として記述した上、さらに帰納論理プログラミングの処理過程を MaxSAT 問題として記述する手法を考案した。そして、帰納論理プログラミングの規模の限界に関する課題を SAT 技術における解決策を利用して克服することを目指した。幾つかの例題による実験により、本手法が有効であることを確認した。

５．主な発表論文等

〔雑誌論文〕（計７件）

① Xiaojuan Liao, Miyuki Koshimura, Hiroshi Fujita, and Ryuzo Hasegawa, Extending MaxSAT to Solve the Coalition Structure Generation Problem with Externalities Based on Agent Relations, IEICE TRANSACTIONS on Information and Systems, 査読有, Vol.E97-D, No. 7, 2014,1812-1821
DOI: 10.1587/transinf.E97.D.1812

② Xiaojuan Liao, Hui Zhang, Miyuki Koshimura, Hiroshi Fujita, and Ryuzo Hasegawa, Using MaxSAT to Correct Errors in AES Key Schedule Images, Proceedings of IEEE 25th International Conference on Tools with Artificial Intelligence(ICTAI 2013), 査読有, 2013,284-291
DOI: 10.1109/ICTAI.2013.51

③ Toru Ogawa, YangYang Liu, Ryuzo Hasegawa, Miyuki Koshimura, and Hiroshi Fujita, Modulo Based CNF Encoding of Cardinality Constraints and Its Application to MaxSAT Solvers, Proceedings of IEEE 25th International Conference on Tools with Artificial Intelligence(ICTAI 2013), 査読有, 2013,9-17
DOI: 10.1109/ICTAI.2013.13

④ Hiroshi Fujita, Miyuki Koshimura, and Ryuzo Hasegawa, SCSat: A Soft Constraint Guided SAT Solver, Proceedings of 16th International Conference on Theory and Applications of Satisfiability Testing (SAT 2013), 査読有, 2013, 415-421
DOI: 10.1007/978-3-642-39071-5_32

〔学会発表〕（計２５件）

① 藤田 博, SCSat3 によるラムゼーグラフ探索について, 2015 年度人工知能学会全国大会（第 29 回）, 2H5-OS-03b-1, 2015 年 5 月 31 日（公立はこだて未来大学）

② 長谷川 隆三, 〔招待講演〕 モデル生成型定理証明系と SAT ソルバー, 人工知能学会 第 97 回人工知能基本問題研究会（SIG-FPAI）, SIG-FPAI-B404-19, 2015 年 3 月 23 日（別府国際コンベンションセンター）

③ 力 規晃, 越村 三幸, 藤田 博, 長谷川 隆三, MaxSAT ソルバーを用いた帰納論理プログラミング, 人工知能学会 第 97 回人工知能基本問題研究会（SIG-FPAI）, SIG-FPAI-B404-15, 2015 年 3 月 23 日（別府国際コンベンションセンター）

④ 越村 三幸, 有村 寿高. 基数制約の SAT 符号化を用いた MaxSAT ソルバーの試作, 2014 年度 人工知能学会全国大会（第 28 回）, 1D4-OS-11a-4, 2014 年 5 月 12 日（愛媛県県民文化会館）

⑤ 藤田 博. SCSat を用いたラムゼー数の下界更新について, 2013 年度 人工知能学会全国大会(第 27 回), 2E5-OS-09b-5, 2013 年 6 月 5 日（富山国際会議場）

〔その他〕

SCSat のホームページ
http://sites.google.com/site/scminisat/

６．研究組織

(1)研究代表者

藤田 博（FUJITA, Hiroshi）
九州大学・大学院システム情報科学研究院・准教授
研究者番号：７０２８４５５２

(2)研究分担者

長谷川 隆三（HASEGAWA, Ryuzo）
九州大学・大学院システム情報科学研究院・教授
研究者番号：２０２７４４８３

越村 三幸（KOSHIMURA, Miyuki）
九州大学・大学院システム情報科学研究院・助教
研究者番号：３０２７４４９２