MGTP による有限代数の新事実の発見

藤田正幸† 粂野文洋†

本稿では，定理証明器 MGTP によって解いて準群に関する未解決問題とそこで用いたヒューリスティックスならびに並列化について報告する．有限代数の存在問題はコンピュータを利用した数え上げによる証明が有望な研究分野であるが，ただ単純に数え上げを行っただけでは，探索空間の爆発により証明が困難である．有限準群の存在問題もその例に洩れず，これまで定理証明システムによる適用はごく限られていた．本研究では，準群問題に対しモデル生成法と呼ばれる定理証明手法を適用し，探索候補の選択に関連したヒューリスティックスを導入することによって探索空間の削減を行った．モデル生成法は場合分けによる OR 並列化が容易であり，ここで導入したような探索木の枝刈り戦略とは互いにその効果を損なわないという特長を持つ．本研究で得られた結果は，準群問題が非ホーン節で簡単に表現できたことと，導入した枝刈り戦略およびこうしたモデル生成法の特長が本質的であった．ただし，MGTP およびここで与えた手法は準群問題を証明するために特化したものではなく，他の非ホーン表現の探索問題にも適用が期待できる．一方，準群問題は実験計画法などへの応用を持つブロック問題と深い関連を持つ．本研究の結果はそうした分野への定理証明の応用可能性を示唆したと考えられる．

New Results in Finite Algebra by a Parallel Model Generation Theorem Prover

Masayuki Fujita† and Fumihiro Kumeno†

This paper reports some new results in finite algebra by MGTP, a parallel theorem prover developed at ICOT. Finite algebra is a good field for mechanical search by computer. But a naive search often falls into the combinational explosion. The application of theorem provers to existence problems of finite quasi-groups is also limited by that reason. For the application to the problems, we introduced pruning strategies on the selection from candidates for the next search. The strategies and OR parallelization that we introduced to MGTP worked well for obtaining some new existence and nonexistence theorems of interesting classes of quasi-group. They are not special for solving existence problems of finite quasi-groups and applicable to finite search problems in non-Horn expression. On the other hand, the field on finite quasi-groups is closely associated with design problems one of which applications is design of experiment. Our results also suggest the applicability of theorem provers to such fields.

1. はじめに

有限代数は機械的な計算によって証明可能な問題が多く存在している研究分野である．例えば，サイズが奇数の倍数の Euler 方陣が存在しないという Euler の予想が計算機のチェックによって覆されている．最近の研究では，位数 10 の射影平面が存在しないことを証明した Lam の研究[9]が知られている．特に有限代数の存在問題の証明には，その数え上げに自動証明や制約充足といった技術が有効に利用できる．

本研究では，有限準群とよばれる有限代数の存在問題に，モデル生成法という定理証明の枠組みを適用する．有限準群の存在問題は，実験計画法やネットワークの認証理論などに応用されている BIBD (Balanced Incomplete Block Design) などのデザイン問題と密接な関係を持った研究分野である．一方，有限領域のモデル生成法はファクトから前向き推論を行うボトムアップ型の探索方法に基づく方法で，場合分けによる OR 並列化が容易であり，探索木の枝刈り戦略がその並列化を損なわないという特長を持つ．

この適用の結果として，有限準群に関する幾つかの未解決問題を証明することができたが，これには準群問題が非ホーン節を使って簡潔に表現できたことと，上記のモデル生成法の特長が本質的に貢献した．また，ここで与えた方法は準群問題向けに特化したものではなく，汎用的であるため，他の非ホーン節表現の有限領域探索問題においても適用可能である．さらにモデル生成法では，問題の解が存在する場合，実際

† 株式会社三菱総合研究所
Mitsubishi Research Institute, Inc.

にその解を構成する．したがって準群の存在がモデル生成法で証明できたときは，その準群を実際に得ることができ，対応する組合せデザインの解として利用することができる．

本論文では，われわれが取り組んだ準群問題とそのために用いたヒューリスティックスおよび並列化を示し，その結果および評価を報告する．まず，2章で準群問題を示し，3章においてモデル生成の枠組みとモデル生成に導入したヒューリスティックスおよび並列化を与える．4章ではその結果および評価を示す．そして最後に，今後の展望として，モデル生成法の問題点とその1つの解決策を議論し，さらに本研究をきっかけとして始まった関連研究を述べる．

2. 準群の存在問題

本章では準群について説明する[3]．ある集合 Q 上で積・が定義されており，任意の元 a, b に対して以下の等式を満たす解 x, y が一意に存在する場合，ペア $\langle Q, \cdot \rangle$ を Q 上の準群と呼ぶ．

$a \cdot x = b$

$y \cdot a = b$

$N = \{1, 2, \cdots, n\}$ 上の準群 $\langle N, \cdot \rangle$ は，k 行目の l 列目に $k \cdot l$ を並べることにより $n \times n$ の配列として表現できる．このような配列はラテン方陣と呼ばれ，各行各列に各数字がただ一度だけ現れるという特性を持つ．したがって，準群はラテン方陣とも呼ばれている．

元の数が有限の準群の存在問題は，組合せ論におけるデザイン問題と密接な関係がある．以下にデザイン問題を表すさまざまな準群を定義する．デザイン問題との対応についての詳しい記述は文献 3) を参照のこと．

準群の直交性 (orthogonality) は次のようにして定義される．$\langle Q, \cdot \rangle$ と $\langle Q, \bigstar \rangle$ を Q 上の準群とする．ここで，$x \cdot y = z \cdot t$ かつ $x \bigstar y = z \bigstar t$ ならば $x = z$ かつ $y = t$ が成立するとき，これらの準群は直交 (orthogonal) しているという．

直交準群の存在問題は，Euler が 1779 年に発表した論文中に与えた以下の組合せの問題と同値であることが知られている．

> 階級の異なる6人の士官からなる6つの師団がある．この 36 人の士官を6行6列に並べ，各行各列に同じ師団または同じ階級の士官が並ばないようにできるか？

ちなみに5階級5師団のケースに関しては**図1**のような並べ方がある．

ここで，例えば aB は師団 a に属する階級 B の士官を意味する．

この問題の解と準群の対の間の具体的な対応関係は次のようなものである．$N = \{1, \cdots, n\}$ 上の直交する2つの準群として $\langle N, \cdot \rangle$ と $\langle N, \bigstar \rangle$ が与えられたとする．師団名を $a_1, \cdots, a_n$ とし階級名を $A_1, \cdots, A_n$ としたとき，師団 a_k に属する階級 A_l の士官を $k \cdot l$ 行 $k \bigstar l$ 列目に並ぶようにする．$\langle N, \cdot \rangle$ と $\langle N, \bigstar \rangle$ が直交することより二人の士官が並ぶべき場所が重複することはなく，また準群の定義からこれがこの問題の解を与えることがわかる．

逆にこの問題の解が与えられたときには，$k \cdot l$ と $k \bigstar l$ を士官 $a_k A_l$ のならんでいる行と列にそれぞれ定めることにより互いに直交する準群 $\langle N, \cdot \rangle$ と $\langle N, \bigstar \rangle$ を得ることができる．

例えば，図1で示した5師団5階級の問題の解に対応する準群の対をラテン方陣の形で表現したものは**図2**のようになる（ただし，$a_1 = a$, $a_2 = b$, $\cdots$, $a_5 = e$ および $A_1 = A$, $A_2 = B$, $\cdots$, $A_5 = E$ とする）．

Euler は，n が奇数の2倍であるときには互いに直交する位数 n の準群の対はない（したがって，n 師団 n 階級の Euler の問題を解決する並べ方はない）と予想したが，この予想は計算機によるチェックをきっかけとして覆された．

次にベキ等準群および共役の概念を導入する．

$x = x \cdot x$ が成り立つ準群をベキ等準群と呼ぶ．

任意の $\langle Q, \cdot \rangle$ に対し，次のような Q 上の積 $\circ_{ijk}$ を定義する．ここで i, j, k は，$\{1, 2, 3\}$ の互いに異なる要素である．

$x \circ_{123} y = z \Leftrightarrow x \cdot y = z$

$x \circ_{213} y = z \Leftrightarrow y \cdot x = z$

```
b B e C a E d A c D
c E d D b A a C e B
e A a B c C b D d E
a D b A d B e E b C
d C b E e D c B a A
```

図 1 Euler の問題の解
Fig. 1 A solution of Euler's problem.

```
5 3 2 4 1    5 2 4 1 3
2 1 4 3 5    3 1 5 4 2
4 5 3 1 2    2 4 3 5 1
1 4 5 2 3    4 3 1 2 5
3 2 1 5 4    1 5 2 3 4
```

図 2 問題の解を表す直交準群
Fig. 2 Orthogonal quasi-groups for a solution of Euler's problem.

$x \circ_{132} y = z \Leftrightarrow x \cdot z = y$

$x \circ_{312} y = z \Leftrightarrow z \cdot x = y$

$x \circ_{231} y = z \Leftrightarrow y \cdot z = x$

$x \circ_{321} y = z \Leftrightarrow z \cdot y = x$

このとき，各 $\langle Q, \circ_{ijk} \rangle$ とも準群となる．この準群を $\langle Q, \cdot \rangle$ の共役 (conjugate) 準群と呼び，$\langle Q, \cdot \rangle$ の (i, j, k)- 共役と書く．

$\langle Q, \cdot \rangle$ に対して，その (i, j, k)- 共役と直交する準群を (i, j, k)- 共役直交と書く．また，$(2, 1, 3)$- 共役直交準群を特に自己直交 (self-orthogonal) と呼ぶ．以降では COLS(Conjugate-Orthogonal Latin Square の略) で共役直交を表し，COILS (Conjugate-Orthogonal Idempotent Latin Square の略) で共役直交ベキ等を表す．また，(i, j, k)-COLS(v) で位数 v の (i, j, k)-COLS を表し，(i, j, k)-COILS(v) で位数 v の (i, j, k)-COILS を表す．ここでは，以下の2タイプの準群のスペクトル☆を決定する問題を対象とする．

- 共役直交（ベキ等）準群の存在

  ある位数の共役直交（ベキ等）準群のスペクトルを決定する問題．こうした種類の問題は，例えば以下のようなデザイン問題と関連がある．

  n 組の夫婦が参加するテニスクラブで親睦試合を行うことになった．各対戦はミックスダブルスで行うが以下の1～3の条件を満たすようにしたい．

  1. 配偶者同士はペアを組まず対戦相手にもならない．
  2. 同性同士は必ず1回ずつ対戦する．
  3. 配偶者以外の異性とは必ず1回ずつペアを組み1回ずつ対戦する．

このような対戦方法の存在の可否と位数 n の $(2, 1, 3)$-COLS の存在問題とは，以下のような対応を付けることによって同値となる．

n 組の夫婦の姓を $A_1, \cdots, A_n$ とする．対戦の組合せを (A_i 氏, A_j 夫人)×(A_k 氏, A_h 夫人) としたとき，$i \cdot k = j$ かつ $k \cdot j = h$ とする．

例えば，**図3**で示した $(2, 1, 3)$-COLS と対応する問題の解は**図4**のようになる（ただし，$A_1 = A, A_2 = B, \cdots, A_5 = E$ とする）．

- ある等式が成り立つ準群のスペクトル

  ある等式が成り立つ準群について，そのスペクトルを決定する問題．こうした種類の問題は，例えば以下のようなデザイン問題と関連がある．

  2人の競技者が攻守に分かれて対戦するカードゲームがある．ゲーム “directed table” はこのカードゲームを4人が交替で2人ずつ計4ラウンドの対戦を行うことで1試合となるが，その際に前ラウンドの守備者は次のラウンドでは攻撃側になるようにする．具体的には，試合の参加者を A, B, C, D としたときの1試合（これを $|ABCD|$ と記すことにする）は**表1**の4ラウンドからなるものである．

  n 人で Directed table のトーナメント戦を行う．ただし，どの2人も攻守と守攻の関係で各1ラウンドずつ対戦するようにしたい．そのような対戦方法はあるか？

この問題と $(y \cdot x) \cdot (x \cdot y) = x$ を満たすベキ等準群の存在問題と次のような対応によって同値となる．競技を行う n 人を $A_1, \cdots, A_n$ とする．第1ラウンドにおいて A_i が，第3ラウンドにおいて A_j が攻撃側で行う試合を $|A_i A_k A_j A_h|$ としたとき，$i \cdot j = k$ かつ $j \cdot i = h$ とする．

例えば，**図5**の準群と対応するこの問題の解は**表2**のようになる（$A_1 = A, A_2 = B, \cdots, A_5 = E$ とする）．また，この問題は $k = 4$, $\lambda = 2$ というパラメータ設定によって (v, k, λ)-BIBD 問題を表している．

本研究では，すべてのスペクトルが明らかになっていない以下の7クラスの問題について，各位数での全

1 3 4 5 2
4 2 5 3 1
5 1 3 2 4
2 5 1 4 3
3 4 2 1 5

図3 位数5の $(2, 1, 3)$-COLS
Fig. 3 $(2, 1, 3)$-COLS, order = 5.

(A氏, C夫人)×(B氏, D夫人)　(A氏, D夫人)×(C氏, E夫人)
(A氏, E夫人)×(D氏, B夫人)　(A氏, B夫人)×(E氏, C夫人)
(B氏, E夫人)×(C氏, A夫人)　(B氏, C夫人)×(D氏, E夫人)
(B氏, A夫人)×(E氏, D夫人)　(C氏, B夫人)×(D氏, A夫人)
(C氏, D夫人)×(E氏, B夫人)　(D氏, C夫人)×(E氏, A夫人)

図4 5組の夫婦の時の解
Fig. 4 A solution of the problem (5 couples).

表1 Directed table ゲーム
Table 1 Directed table game.

1ラウンド 攻×守	2ラウンド 攻×守	3ラウンド 攻×守	4ラウンド 攻×守
$A \times B$	$B \times C$	$C \times D$	$D \times A$

☆ スペクトルは準群の存在する位数の分布のことをいう．

解探索を試みた.

1. (3, 2, 1)-COILS(v) が存在するかどうかを各 v について確かめよ.
2. (3, 1, 2)-COILS(v) が存在するかどうかを各 v について確かめよ.
3. 位数 n の Schröder's second law を満たす準群を見つけよ. 特にベキ等のものを見つけよ.
4. Stein's third law $yx\cdot xy=x$ を満たす位数 n の準群を見つけよ. 特にベキ等のものを見つけよ. ここで, yx や xy はそれぞれ $(y\cdot x),(x\cdot y)$ の省略形である. 以降でも同様の省略形を用いる.
5. $(xy\cdot y)=x$ を満たす (ベキ等) 準群のスペクトルを決定せよ.
6. $xy\cdot y=x\cdot xy$ を満たす (ベキ等) 準群のスペクトルを決定せよ. 位数 n が $n\equiv 0$ または 1(mod 4) のときだけ存在するかどうかを確かめよ.
7. $yx\cdot y=x\cdot yx$ を満たす (ベキ等) 準群のスペクトルを決定せよ. 位数 n が $n\equiv 1$(mod 4) のときだけ存在するのかどうかを確かめよ.

各問題の説明を簡略に示す. 詳しい説明は文献 3) を参照のこと.

1. $v=12$ の場合が未解決である. それ以外では $v=2, 3, 6$ の場合を除いて存在することが知られている.
2. $v=10, 12, 14, 15$ の場合が未解決である. それ以外では $v=2, 3, 4, 6$ の場合を除いて存在することが知られている.
3. Schröder's second law $xy\cdot yx=x$ を満たす準群を Schröder 準群という. Schröder 準群は自己直交であることが知られている. この問題に関しては, 位数 n について $n=5, 12$ の場合 ($n=12$ の場合は予想) を除いて $n\equiv 0$ または 1(mod 4) の場合のみ存在することが知られている. これはベキ等準群に関しても同じである.
4. Stein's third law を満たす準群は自己直交であることが知られている. この問題に関しては, 位数 n について $n=12$ の場合を除いて $n\equiv 0$ または 1(mod 4) の場合のみ存在することが知られている. また, $n=12$ の場合は存在しないと予想されている. 本研究より以前ではベキ等準群に関しては, $n=4, 8, 12$ の場合 ($n=12$ の場合は未解決) を除いて $n\equiv 0$ または 1(mod 4) の場合のみ存在することが知られている.
5. $(yx\cdot y)y=x$ が成立する準群のスペクトルは文献2)で詳しく研究されている. 本研究より以前では, 位数 n に関して $n=2, 6$ の場合と $n\in\{10, 14, 18, 26, 30, 38, 42, 158\}$ の場合 (この場合は未解決) を除いて存在が知られている. ベキ等準群の場合は, $n=2, 3, 4, 6$ では存在しないことが知られている. また $n=9, 10, 12, \cdots, 16$ の場合など, 存在の有無が確かめられていない場合が 56 ケース存在している.
6. $xy\cdot y=x\cdot xy$ (この等式は Schröder's first law と呼ばれている) を満たすスペクトルについてはあまり正確には知られていない. 位数 n に関して, $n=5$ の場合は存在しないことが知られている. また, $n=9, 12, \cdots, 177$ の 35 ケースで存在しないと予想されている. これ以外では $n\equiv 0$ または 1(mod 4) の場合に存在が確認されているが, $n\equiv 0$ または 1(mod 4) 以外で存在するかどうかは不明である.
7. $yx\cdot y=x\cdot yx$ を満たす準群については, 位数 n が $n\equiv 1$(mod 4) であれば, $n=33$ を除いて存在することが確認されている. $n=33$ では存在しないと予想されている. $n\equiv 1$(mod 4) 以外の場合で存在するかどうかは知られていない.

1 3 2 5 4
5 2 4 3 1
4 5 3 1 2
2 1 5 4 3
3 4 1 2 5

図 5 $(y\cdot x)\cdot(x\cdot y)=x$ を満たす位数 5 のベキ等準群
Fig. 5 Idempotent quasi-group (order 5) which satisfies $(y\cdot x)\cdot(x\cdot y)=x$.

表 2 5人のトーナメント戦に関する問題の解
Table 2 A solution of directed table game problem (5 players).

	1ラウンド 攻×守	2ラウンド 攻×守	3ラウンド 攻×守	4ラウンド 攻×守
第一試合	$A\times C$	$C\times B$	$B\times E$	$E\times A$
第二試合	$A\times B$	$B\times C$	$C\times D$	$D\times A$
第三試合	$A\times E$	$E\times D$	$D\times B$	$B\times A$
第四試合	$A\times D$	$D\times E$	$E\times C$	$C\times A$
第五試合	$B\times D$	$D\times C$	$C\times E$	$E\times B$

3. MGTP: Model Generation Theorem Prover

MGTP/G は有限領域 (range restricted)* の問題

* すべての節で, 正リテラルに現れる変数が, 負リテラルにかならず一度は現れる.

を対象としたモデル生成法に基づく，一階述語論理の並列定理証明器である．MGTP/G では，Prolog 処理系の節コンパイル技術を利用した Satchmo[5] を拡張し，問題を並列プログラミング言語 KL1 の節に直接変換する方法がとられているが，その実現法はそれほど自明ではない．MGTP/G が Satchmo の実行効率を保ったまま KL1 化した方法については，参考文献 7),8) を参照されたい．本章ではモデル生成法の概要と導入したヒューリスティックスおよび並列化について説明する．

3.1 モデル生成法

モデル生成法は与えられた節集合に対し，それを充足する基底モデルをすべて生成するアルゴリズムである．節は以下のようなシークエント形式で記述する．

$$p_0(t_0^0, \cdots, t_0^{k_0}), \cdots, p_n(t_n^0, \cdots, t_n^{k_n})$$
$$\rightarrow$$
$$q_0(s_0^0, \cdots, s_0^{l_0}); \cdots; q_m(s_m^0, \cdots, s_m^{l_m})$$

→は含意を表し，その左を前件部，右を後件部と呼ぶ．前件部のコンマは連言，後件部のセミコロンは選言を表す．モデル生成法では，証明の対象とする問題は便宜的に次の3種類の節に分類する．

正節 前件部のない節であり，range-restricted の条件により，リテラルはすべて変数を含まない．

負節 後件部のない節であり，一貫性制約 (integrity constraint) とも呼ばれる．

モデル生成節 正節，負節以外の節である．

MGTP では負節とモデル生成節が KL1 言語にコンパイルされる．プログラムは，モデル中の正リテラルと，モデル生成節，負節の間の導出により新しい正節を生成する．負節は生成されたモデルから空節を導く．負節が空節を導くと，この基底モデルは棄却される．この方法は，実は古くから知られているタブロー法[1]と本質的には同じである．

図 6 に，有限領域の問題例を MGTP の問題形式で示す．この問題に対し，モデル生成法では，**図 7** のような証明木を生成し，各推論の分岐で空節に相当する false を導き，与えられた節集合が充足不可能であることを示している．

節集合が充足可能となった場合，そこで見出されたモデルは元の節集合の節をすべて真とするエルブランモデルである．**図 8** は，n クィーン問題を MGTP の問題形式で記述したものである．$p(a, b)$ は，a 行 b 列にクィーンがあることを意味する．C_1 から C_n までの節は，“同じ行には二つ以上クィーンを置くことができない” という条件下での，可能なすべての配置の組合せを意味する．一方，述語 constraint は，“(X1, Y1), (X2, Y2) が同じ列あるいは対角線上ではない” ことを意味する．この場合，得られた各モデルが，n クィーン問題の解となる各クィーンの配置を表す．

3.2 ヒューリスティックス

MGTP による探索で用いられる場合分けは，注意深く順序を選ばなければ組合せの爆発を招くことが多い．これに対処するためのヒューリスティックスを導入したモデル生成の手続きを以下に示す．

Procedure *mgtp*:
input: P 問題の節集合
output: M モデルの集合
手続き *mgtp* は問題の節集合 P が充足可能
であれば，すべてのモデルを M に返し，
充足不能であれば，0 を M に返す．
ここで *MC*, *NC*, *PC* をそれぞれ，
モデル生成節の集合，負節の集合，

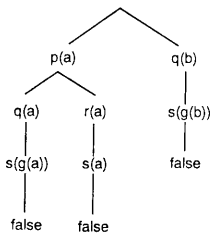


図 7 証明木の例
Fig. 7 Proof search tree.

```
(C1)  p(X),s(X) → false.
(C2)  q(X),s(Y) → false.
(C3)  q(X) → s(g(X)).
(C4)  r(X) → s(X).
(C5)  p(X) → q(X);r(X).
(C6)  true → p(a);q(b).
```

図 6 有限領域の問題例
Fig. 6 A finite domain problem.

```
(C1)    true → p(1,1);p(1,2);...;p(1,n).
(C2)    true → p(2,1);p(2,2);...;P(2,n).
        ....
(Cn)    true → p(n,1);p(n,2);...;p(n,n).
(Cn+1)  p(X1,Y1),p(X2,Y2),
        constraint(X1,X2,Y1,Y2) → false.
```

図 8 n クィーン問題の記述
Fig. 8 MGPT input for n-queen ploblem.

正節の集合とする.

1. $P=MC\cup NC\cup PC$ とする;
2. $M:=\emptyset$;
3. $MD:=\emptyset$ とし,
   modelgen(PC, MD)
   を実行する. ここで MD はモデルである;

end_Procedure

Procedure *modelgen*(PC, MD);

1. (a) PC が空のとき, $M:=M+\{MD\}$ として終了;
   (b) PC が空ではなく, 空節を含めば, 終了;
   (c) PC が空でなく, 空節を含まないとき, PC からリテラル数が最も少ない節の1つ C を選択し, $PC:=PC-\{C\}$ とする;
2. C に含まれるすべてのリテラル L_i に対し, PC をコピーし, 順次以下を行い, それらがすべて終了したら, 終了;
   (a) $MD_i:=MD\cup\{L_i\}$ とする;
   (b) NC の節と L_i の間の超導出の成功集合を SNC とし, MD_i と SNC の間の超導出節のうち長さが1以下のものの集合を F とする;
   (c) i. F が空節を含むとき, 終了;
   ii. F が空節を含まないとき, PC から F のリテラルの逆符号のリテラルをすべて除いた節集合 PC' を作る;
   A. PC' が空節を含めば終了;
   B. PC' が空節を含まなければ, MC の節と L_i の間の超導出の成功集合を HR とする;
   (d) MD_i と HR の間の超導出により得られるすべての基底正節から, MD_i および PC の節に包摂されないものの集合を PC_s とする;
   (e) PC_s のすべてのリテラルのうち MD_i および NC との間で超導出により空節を導くものを削除して PCs' を作る;
   i. PCs' が空節を含む場合, 終了;
   ii. PCs' が空節を含まない場合,
   $PCi:=PCs'\cup PC'$ とする;
   (f) *modelgen*(PCi, MDi)
   を実行して終了;

end_Procedure

このプログラムで導入されたヒューリスティックスは以下の2つである.

1. 正節の集合 PC から常にリテラル数(場合分けの数)の最も少ない節を選択する (1c).
2. 新たに MDi にリテラル L を追加するとき, MDi とともに負節と超導出に成功する PC の各節のリテラルを消去する (2(c)ii). また, モデル生成節によって新しく生成された節に対しても PC に追加するとき (2e) に同じ操作を行う.

2の操作は, 2箇所に分けられているが, 新しい節が生成されたときと, 新しいリテラルがモデルに登録されたときに, それぞれ新しい節やリテラルを含む超導出を試すことにより, 完全性を失わずに同じリテラルの組合せによる負節の超導出を避けることができている (証明略).

以上のヒューリスティックスは, 問題によっては劇的な探索空間の削減をもたらすことがわかる (**表 3**). クィーン問題以上に, 準群の問題 (表3の QG5(4)〜QG5(12), 問題の内容については4章を参照) に対して大きな枝刈り効果が得られており, このヒューリスティックスが未解決問題を解くにあたって本質的であることを示している.

3.3 並 列 化

3.3.1 モデル生成法の OR 並列性

有限領域を対象としたモデル生成法では選言

$q_0(s_0^0, \cdots, s_0^{l_0}); \cdots; q_m(s_m^0, \cdots, s_m^{l_m})$

の各リテラルをそれぞれ加えたモデルごとに探索木が分岐する (アルゴリズム中では 2.). ここで追加される各リテラル $q_i(s_i^0, \cdots, s_i^{l_i})$ には変数が含まれていないため, 各場合の計算は全く独立して並行に行うことができる. したがって, 個々の場合を別々のプロセッサで実行することによって並列化することが可能であ

表 3 ヒューリスティックスの効果
Table 3 Pruning search trees by the heuristics.

問 題	探索枝数		解の数
	導入前	導入後	
10クィーン	312,612	4,942	724
11クィーン	1,639,781	21,528	2,680
QG5(4)	104	1	0
QG5(5)	2,400	1	1
QG5(6)	179,171	3	0
QG5(7)	52,249,612	6	3
QG5(8)	—	33	1
QG5(9)	—	239	0
QG5(10)	—	7,026	0
QG5(11)	—	51,899	5
QG5(12)	—	2,749,676	0

—は証明ができなかったことを示す

る．これが有限領域を対象としたモデル生成法における OR 並列性である．

また，前節のヒューリスティックスを導入しても，この並列性は損なわれるものではない．トップダウンの探索法では，バックトラック時にそれまでの探索情報を記憶することによって冗長な探索を枝刈りするため，単純な並列化できないのに対し，モデル生成法はボトムアップ探索であり，ヒューリスティックスと OR 並列性の両方の特長を容易に得ることができる．

3.3.2 負荷分散

前節からわかるように，モデル生成法では疎結合並列マシンでの OR 並列化が容易に実現できる．本研究では PIM/m を利用し，2種類の負荷分散方式を組み込んで並列化を行った．PIM/m は ICOT で開発された並列推論マシンの一つであり，最大256プロセッサの2次元メッシュ疎結合 MIMD マシンで，160 M LIPS (Logical Instruction Per Second) の性能を持つ．

探索の並列化では単純な負荷分散方式として，特定の探索レベルまで1プロセッサで問題を解き，そこでできた枝を各プロセッサに割り当てる，という方法が考えられるが，探索空間は事前に知ることができないため，最適な並列化が得られる探索レベルを設定できない．そこで，ここでは OR 分岐が行われた時点でその中のいくつかの枝を自分のプロセッサ内で解き，他の枝は他のプロセッサに渡すことを繰り返す方法を導入している（**図 9**）．

また，枝を渡すプロセッサの決定を以下の2方式によって実現した．

確率方式 問題を渡す先のプロセッサを乱数によって決める．乱数の計算には，OR 分岐が起こった時点の探索木の深さ，場合分けの枝の位置（左から数える）および分岐元のプロセッサ番号をパラメータとする．

テーブル管理式 この方式では，各プロセッサは OR 分岐が生じたときや1つの探索の枝が終了したときには，管理プロセッサに逐次報告する．管理プロセッサは，それぞれが並列に解いている問題数をテーブル管理し，次にタスクを渡すべきプロセッサをすべて指示する．

4. 実行結果および評価

4.1 実行結果

2章の各問題の条件はすべて以下のような等式条件として表すことができる．ここで，x/y は $y\circ_{321}y$ を表している．

QG 1 $ab=cd$ かつ $a/b=c/d$ ならば
$a=c$ かつ $b=d$ である．

QG 2 $ab=cd$ かう $b/a=d/c$ ならば
$a=c$ かつ $b=d$ である．

QG 3 $ab\cdot ba=a$

QG 4 $ba\cdot ad=a$

QG 5 $(ba\cdot b)b=a$

QG 6 $ab\cdot b=a\cdot ab$

QG 7 $ba\cdot b=a\cdot ba$

各問題は，**図 10** のように MGTP の節集合として表現される．$p(X,Y,Z)$ は $X\cdot Y=Z$ を表す．最後の負節は等式条件 $(ba\cdot b)b=a$ を表現している．最初の負節は，準群が各要素を置き換えても同じ準群(同型)を表す性質をもつため，同型なものの探索を枝刈りするための条件節である．残りの3つの負節はベキ等準群の定義の条件である．上にあげた7つの問題につき，結果を得ることができた主な位数について，256 プロセッサ PIM/m 上の MGTP による実行結果を**表 4** に示す．問題は，ほとんどの場合，準群がベキ等であることを仮定している．MGTP は，各位数ごとに各問題の条件を満たす準群を全解探索する．負荷分散は確

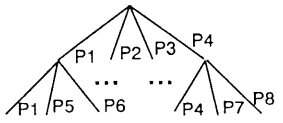


図 9 枝の割り付け
Fig. 9 Processor allocation to search tree.

```
true → dom(1),dom(2),dom(3),
dom(4),dom(5),dom(6).
dom(M),dom(N) →
p(M,N,1);p(M,N,2);p(M,N,3);
p(M,N,4);p(M,N,5);p(M,N,6).
p(X,6,Y), {Y+1<X} → false.
p(X,X,U), {X≠U} → false.
p(X,Y,U), p(X,Y1,U), {Y≠Y1} → false.
p(X,Y,U), p(X1,Y,U), {X≠X1} → false.
p(E,X,Y), p(Y,E,Z), p(Z,E,U), {X≠U}
→ false.
```

図 10 位数6の QG 5 準群問題
Fig. 10 MGTP input for quasi-group problem QG 5, order 6.

率方式とテーブル管理式の2方式で行った．ただし表4では，実行時間は2つのバージョンによる実行のうち，時間の短いほうを選択してある．

4.2 並列化の効果

ここで，準群問題の証明に対する並列化の効果について検討を行う．まず，確率方式とテーブル管理式を比較している．**表5**は，両方式での実行時間（256台プロセッサを使用）と1台のプロセッサでの実行時間を示したものである．わずかであるがテーブル管理式の方が確率式よりも良い結果を得ていることがわかる．QG 5(10) を調べると，確率方式は，各プロセッサの処理量に大きな差があることがわかった．テーブル管理式ではプロセッサが枝をいくつ解いているのかを厳密に管理しているのに対し，確率式ではプロセッサの稼働状況とは無関係にタスクが割り付けられていく．したがって，タスク分岐数が小さい場合は，大数の法則が働かないので，各プロセッサの負荷に差が生じて，並列効果が出ない可能性が高い．しかし，問題の規模とともに，大数の法則によって負荷が平準化され，より良い並列効果が期待できる．一方，テーブル管理方式では逆に，問題の規模が大きくなると，プロセッサ割り付け管理の手間がボトルネックになる可能性がある．例えば，枝分岐が急激に増える pigeon hole 問題（hole=8，場合分けは 8! だけ起こる）で実験したところ，確率式では実行時間が4秒であったのに対し，テーブル管理式では113秒であった．個々の処理が軽い pigeon hole 問題は，テーブル管理している1つのプロセッサが問題を解くプロセッサに対して飛び抜けて高負荷になり，ボトルネックとなってしまった．準群の問題でも，規模の大きな問題になると，確率方式しか解が得られないようなものもあった（**表6**）．

台数効果（表5）は，QG 5(11) のように比較的規模の大きな問題に対しても，256 台で最高 154 倍の効果に留まっている．探索木の解析結果では，QG 5(11) の探索木は各枝の深さが不均一であり，しかもモデルが見つかった5つの枝は他の枝よりも 50 レベル以上枝が深かった．モデル生成法は，モデルの要素数の n 乗（n は問題節の前件部のリテラルの数）のオーダーで負荷が重くなる処理である．探索の各枝が深くなればなるほど，枝（1段深くなるごとにモデル要素数は

表4 MGTP による証明結果
Table 4 The results on quasi-group problems.

問題	位数	探索枝数	準群数	実行時間 (seconds)
QG 1	8	180,414	16	1894
QG 2	7	1,100	14	24
QG 3	7	183	0	4
	8	3,857	18	20
	9	312,321	0	1017
QG 4	7	123	0	5
	8	3,516	0	17
	9	314,847	178	1092
QG 5	7	6	3	2
	8	33	1	4
	*9	239	0	9
	*10	7,026	0	35
	11	51,899	5	231
	*12	2,749,676	0	13715
	†*10	4,473,508	0	13101
QG 6	*7	7	0	2
	8	18	2	4
	*9	156	4	9
	*10	2,881	0	21
	*11	50,888	0	208
	*12	2,420,467	0	8300
QG 7	*7	182	0	3
	*8	160	0	3
	9	37,025	1	85
	*10	1,451,992	0	2809

* これまで未解決であった問題
† ベキ等を仮定していない場合

表5 256 プロセッサによる並列化の効果
Table 5 Speed up on three problems by using 256 processors.

問題（位数）	QG 5 (9)	QG 5 (10)	QG 5 (11)
1プロセッサ	84 s	3552 s	35528 s
確率方式	11 s	50 s	244 s
台数効果	8	71	146
テーブル管理式	9 s	35 s	231 s
台数効果	9	101	154

表6 大きな問題での各方式の実行時間
Table 6 The results on large scale problems.

問題（位数）	QG 1 (8)	QG 3 (9)	QG 4 (9)
確率方式	1894 s	1022 s	1127 s
テーブル管理式	1937 s	1017 s	1092 s
問題（位数）	QG 5 (12)	QG 7 (10)	QG 6 (12)
確率方式	13715 s	8300 s	2809 s
テーブル管理式	—	—	—

—は証明ができなかったことを示す

それぞれの分岐で1ずつ増加する）の数がプロセッサ数に比べて急激に減少してしまう準群問題では，遊休プロセッサが次にタスクをもらうまでの待ち時間は多項式オーダ以上で増大していくことになる．これはOR並列探索の限界を示しており，負荷分散のチューニングだけでは回避できないものである．

5. 議　　論

5.1 問題変換による探索空間の枝刈り

MGTPによる準群問題の証明では，準群の定義や性質である等式条件を制約として記述し，テスト生成法によっての解（制約を満たす準群）を見つける方法をとっている．すなわち，正節やモデル生成節によって準群の候補を生成し，準群の等式条件の否定を負節として表現して等式条件を満たさない候補を棄却する．そして最後まで生成し終わった時点で残っている候補が準群になるわけである．こうした方法では，負節がいわゆる受動的制約としての機能しているだけであり，効率的な探索とはいえない．そこで等式条件を表した節どうしで導出を行い，導出された節をも新たな制約として用いる．こうした操作によって，関連した複数の制約からより解の探索に効果的な制約を作るという一種の能動的制約が実現でき，探索空間の枝刈りに貢献することが期待できる．

このことをQG5問題を例にとって説明する．QG5(6)の等式条件*は，モデル生成のための節を

dom(M), dom(N)→
p(M, N, 1);p(M, N, 2);p(M, N, 3);p(M, N, 4);
p(M, N, 5);p(M, N, 6).

としたとき，**図11**のように記述できる．以上の条件と4章に示した問題表現とは，$p(X, Y, Z)$ の引数の組 X, Y, Z が唯一であるという条件により，同値である．

この条件に対し，例えば(3)と(5)の導出を行うと，

p(E, X, Y), p(Y, E, Z), p(Z, E 1, X)→{E=E 1}.

```
(1)  p(X,6,Y) → {Y+1≥X} .
(2)  true → p(X,X,X).
(3)  p(X,Y,U), p(X,Y1,U) → { Y=Y1} .
(4)  p(X,Y,U), p(X1,Y,U) → { X=X1} .
(5)  p(E,X,Y), p(Y,E,Z) → p(Z,E,X).
```

図11 QG5(6) の等式条件
Fig. 11 Equational condition for QG5(6).

* 同型な準群の探索を避ける条件も含める．

という節を得ることができる．この節を負節として表現すると，

p(E, X, Y), p(Y, E, Z), p(Z, E 1, X), {E≠E 1}→
false.

となる．この節との導出に成功する正リテラルのパターンは，これまでの問題表現の負節と導出できる正リテラルのパターンとは異なるものである．例えば，この負節と導出できる正リテラルのパターンと

p(E, X, Y), p(Y. E, Z), p(Z, E, U), {X≠U}→
false.

と導出できる正リテラルのパターンを比べてみる．ここで $p(E, X, Y), p(Y, E, Z)$ がそれぞれ $p(1, 2, 3), p(3, 1, 4)$ にマッチングしたとすると，導出できる正リテラルのパターンはそれぞれ，$p(4, X, 2)$（ただし，$X \neq 1$），$p(4, 1, X)$（ただし，$X \neq 2$）となる．他の負荷節でも同様のことがいえる．

したがって，この節は，モデル生成の途中の段階におけるモデルの集合に対し，これまでの問題表現で棄却できなかったものを棄却する可能性を持っている．こうした節を加えることにより，探索している枝のモデル棄却がより早い時点で分かり，枝刈りが期待できる．

等式条件(1)～(5)から導出したこのような節を加えた問題表現は以下のようになる．$n1$～$n5$ が新しく加えた節である．

ここで，(1)～(5)から導出した節をすべて加えているわけではない．例えば，(2)と(3)からは

p(X, X, Z)→p(Z, X, X)

を導出でき，

```
(a)   p(X,6,Y), {Y+1<X} → false.
(b)   p(X,X,U), {X≠U} → false.
(c)   p(X,Y,U), p(X,Y1,U), {Y≠Y1} → false.
(d)   p(X,Y,U), p(X1,Y,U), {X≠X1} → false.
(e)   p(E,X,Y), p(Y,E,Z), p(Z,E,U), {X≠U} →
      false.
(n1)  p(6,X,Y), p(Y,6,Z), { X+1<Z} → false.
(n2)  p(X,Y,X), { X ≠ Y} → false.
(n3)  p(Y,X,X), { X ≠ Y} → false.
(n4)  p(E,X,Y),p(Y,E,Z),p(Z,E1,X),{ E≠E1} →
      false.
(n5)  p(E,X,Y),p(Y,E,Z1),p(Z,E,X),{ Z≠Z1} →
      false.
```

図12 新しい負節
Fig. 12 New false clauses.

p(X, X, Z), p(Z 1, X, X), $\{Z \neq Z1\} \rightarrow$false.

p(X, X, Z), p(Z, X 1, X 1), $\{X \neq X1\} \rightarrow$false.

といった負節を得ることができる．しかしこれらの節と導出できる正リテラルのパターンは，(b)，(*n*2)，(*n*3) と導出可能な正リテラルのパターンと同じであり，しかもマッチを行うリテラル数が1つ多い．こうした節は枝刈りには貢献しないので，問題には加えない．

この問題表現による実行結果を**表7**に示す．表7にあるように探索空間のかなり枝刈りに成功していることがわかる．

ここで与えた新しい問題表現は，導出を1レベル行なっただけであったが，さらに新しい導出を続け，負節を追加していくことも可能である．以上の導出を続けて，負節の極大集合を与えてやれば，枝刈りがもっとも効果的に現れることが予想される．しかし，負節の数が増えるにつれ，MGTP での負節の導出処理の負荷は指数関数的に増大していくし，極大集合が無限集合になる可能性もあるので，負節の導出処理の負荷との調整によって，ある一定のレベルで導出を止めておくのが現実的であろうと考えられる．

こうした枝刈りの効果は，新たに導出された負節がこれまでの負荷と異なるパターンの正リテラルと導出可能なときに期待でき，これは準群問題に限ったものではない．

準群問題の場合には，以下の定理を等式条件として加え，同様の問題変換をすることによって，より探索空間が削減できることがわかっている．

$p(E, X, Y), p(Z, E, X) \rightarrow p(Y, E, Z)$.

$p(Y, E, Z), p(Z\ E, X) \rightarrow p(E, X, Y)$.

以上の問題変換の手法を使うことによって，MGTP 自身に手を加えずに探索の枝刈りが実現でき，これまで解けなかった問題 (QG 5(13) など) も，この問題変換を施すことによって解けるようになっている．

また，本節で述べた手法も先に述べたヒューリスティックスと同様，MGTP の OR 並列化の特長を損なうものではない．

表 7 新しい問題表現による実行結果 (探索枝数)
Table 7 The new results by the problem translation.

問 題	元の問題表現	新しい問題表現
QG 5 (10)	7026	361
QG 5 (11)	51889	2888
QG 5 (12)	2749676	36858

5.2 関 連 研 究

MGTP による有限準群の未解決問題への適用をきっかけとして，他の定理証明システムによる試みも行われ，準群固有のいくつかのヒューリスティックスも研究され始めている．たとえば，M. Stickel が準群固有のヒューリスティックスを Davis-Putnam 法の命題論理定理証明システムに導入し，さらに進んだ結果を出したり，J. Slaney も Finder[6] に(2)のヒューリスティックスを組み込んで同様な結果を出すなど，大きな進展を見ている．これらの研究の詳細および MGTP と比較検討については別途発表する予定であるが，これら他の研究によって得られた結果の主なものを以下にまとめる．

QG 3, 4: ベキ等な位数 12 のものが存在する．これは，全解探索ではなく縦型探索により発見された．それぞれ Davis-Putnam, Finder で数分の実行時間で発見された．全解はまだ得られていない．

QG 5: ベキ等なモデルは位数 13, 14 で発見されなかった．これは Davis-Putnam による結果であるが，位数 14 の場合，Sparc-2 で約 12 日の CPU 時間を必要とした．

QG 7: 位数 11, 12 の場合にベキ等なものが存在しないことがわかった．

6. む す び

本稿では，並列探索の応用例として，OR 並列型定理証明システム MGTP の有限準群への適用を示した．この適用の結果，いくつかの未解決問題の証明を通して，有限準群の研究の進展に寄与することができた．定理証明の準群問題への適用は，Finder などによって以前から試みられていたが，本稿で述べたようなヒューリスティックスや並列化は導入されていなかったため，未解決問題を解くまでには至らなかった．ヒューリスティックスや関連研究の項からわかるように，準群問題への適用では枝刈り戦略が本質的に重要であるが，位数が大きくなるに従い，その探索空間が膨らむため，並列化は不可欠なものになってくる．本研究で利用した枝刈り戦略や並列化は比較的単純なものであるが，モデル生成法ではこれらが互いの効果を損なうことなく導入できたことが本結果につながった．

一方，有限準群の存在問題はさまざまな組み合わせデザインの問題と同値であることが示されている．

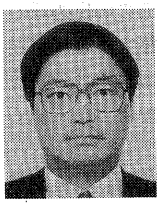
MGTP による証明では準群が存在するときには実際に準群を構成するため，デザイン解を自動生成していることになる．本稿で用いた準群の実例も MGTP によって生成したものである．こうした構成的な証明を行うのは，他の自動証明のアプローチでも同様である．今後の展開としては，デザイン問題が実験計画法などの応用領域を持つことから，MGTP においてもこうした領域への応用可能性を追究することが一つの課題となる．そのためには，まず，より大きな位数の有限準群問題を解くための枝刈り・並列化の手法を研究していくのが当面の課題である．

謝辞 この研究は(財)新世代コンピュータ技術開発機構 (ICOT) の研究の一環として行われたものである．ICOT の定理証明 WG メンバー，ANU の Slaney 氏，SRI の Stickel 氏からは有意義な議論をいただいた．Mt. St. Vincent 大学の Bennett 教授には準群の未解決問題を多数教えていただいた．以上の方々に感謝致します．また，渕 ICOT 所長には定理証明の研究の機会ならびに，示唆に富むアイデアを与えていただいたことに感謝致します．

参 考 文 献

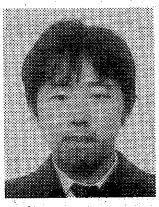
1) Smullyan, R. M.: First-Order Logic, Springer-Verlag, Berlin, Heidelberg, New York (1971).
2) Bennett, F. E.: Quasigroup Identities and Mendelsohn Designs, *Canadian Journal of Mathematics*, Vol. 41, No. 2, pp. 341-368 (1989).
3) Bennett, F. E. and Zhu, L.: Conjugate-Orthogonal Latin Squares and Related Structures, in Dinitz, J. H. and Stinson, D. R. (eds.), *Contemporary Design Theory: A Collection of Surveys* Wiley, New York (1992).
4) Fujita, M., Hasegawa, R., Koshimura, M. and Fujita, H.: Model Generation Theorem Provers on A Parallel Inference Machine, *Proc. of FGCS '92* (1992).
5) Manthey, R. and Bry, F.: SATCHMO: A Theorem Prover Implemented in Prolog, *Proc. of CADE 88*, Argonne, Illinois (1988).
6) Slaney, J. K.: FINDER Finite Domain Enumerator VERSION 2.0 NOTES AND GUIDE, The Public Domain Softwares, The Australian National University (1992).
7) Fuchi, K.: KL1 プログラミング雑感—Prover の並列化の体験より—, *Proc. of KL1 Programming Workshop '90*, pp. 131-139 (1990) (in Japanese).
8) Fujita, H. and Hasegawa, R.: A Model Generation Theorem Prover in KL1 Using Ramified-Stack Algorithm, *Proc. of ICLP 91*, pp. 535-548 (1991).
9) Lam, C. W. H.: The Search for a Finite Projective Plane of Order 10, *Canadian Mathematial Journal*, Ppr. (1991).

(平成5年9月27日受付)
(平成6年4月21日採録)



藤田 正幸（正会員）

昭和32年生．昭和55年東京大学教養学部基礎科学科卒業．昭和57年同理学系大学院修士課程修了．昭和58年同大学院博士課程中退，(株)三菱総合研究所入社．昭和64年～平成4年財団法人新世代コンピュータ技術開発機構へ出向．定理証明，プログラム合成等の研究に従事．日本ソフトウェア科学会会員．



粂野 文洋

1965年生．1988年早稲田大学理工学部数学科卒業．1990年同大学院理工学研究科修士課程修了．同年(株)三菱総合研究所入社．並列定理証明，プログラム合成等の研究に従事．現在，情報処理事業協会 (IPA) に出向し，協調アーキテクチャの研究に従事．日本ソフトウェア科学会会員．