並列推論マシン上の
並列定理証明系による
有限代数の新事実

藤田 正幸　　John K. Slaney　　長谷川 隆三
ICOT　　ANU　　ICOT
mfujita@icot.or.jp　jks@ceres.anu.edu.au　hasegawa@icot.or.jp

1992 年 8 月 6 日

概要

本概要では，ICOT で開発された並列定理証明システム MGTP が，有限代数の分野における新事実を導いたことについて報告する．

MGTP/G[FH92] は，ICOT で開発されたタブロー法，あるいは，モデル生成法に基づく，有限領域 (range restricted)[1] の問題を対象とした一階述語論理の並列定理証明器である．MGTP は，ECRC で開発された Prolog をベースとした定理証明器 Satchmo[MB88] を参考に開発し，問題を並列論理型言語 KL1 に直接変換することにより，非常に高いパフォーマンスを得ている．

MGTP/G にとっては，場合分けが高い効率と組合せの爆発という正反対の結果を導く原因になっている．MGTP/G ファミリーの一員である MGTP/G/MERC/PF は，組合せの爆発の問題に対して，次のような単純ではあるが効果の大きい 2 つの仕組みを利用して対応している．まず，場合分けの原因となる論理和節 (Disjunctive Clause) をその場合分けの数で昇順に整列し，場合分けの木をできるだけ広がらないようにする戦略が導入されている．もうひとつの方法は，否定節（正リテラルを持たない節）と順次生成される単位モデルを利用して，論理和節の各々の単位節を棄却することにより，場合分けの数を減らす (Partial Falsification) ことを行なっている．この分岐の動的な制御により，以下で述べる Bennett の準群の問題では劇的な探索空間の削減が行なえている (表 1)．

[Be89] の中で，Bennett は，$x * x = x(idempotent)$, $((y * x) * y) * y = x$, という 2 つの方程式が常に成り立つ有限準群が存在しない要素数 n （order とよぶ）は，n=2, 3, 4, 6 であり，さらに n=9, 10, 12, 13,... の 56 個[2] を除けばすべて存在することを証明した．この 56 個の例外は，現状の代数的な方法では存在，非存在が不明なものとして残された．準群 (*quasigroup*) はペア $(Q, *)$ で，Q は集合，$*$ は Q 上の 2 項演算であり，方程式 $a * x = b$ と $y * a = b$ がすべての Q 上の組合せ a, b に対して唯一解を持つようなものを指す．Q が有限の場合，掛け算の表を作ると，すべての行と列に必ず Q の要素が 1 つづつ現れる．*idempotent* な場合は，表の対角線

[1] 後件に現れる変数がすべて前件にかならず 1 度は現れるような節形式の問題

[2] E={9, 10, 12, 13, 14, 15, 16, 18, 20, 22, 24, 26, 28, 30, 34, 38, 39, 42, 44, 46, 51, 52, 58, 60, 62, 66, 68, 70, 72, 74, 75, 76, 86, 87, 90, 94, 96, 98, 99, 100, 102, 106, 108, 110, 114, 116, 118, 122, 132, 142, 146, 154, 158, 164, 170, 174}

問題	失敗の枝の数 MERC/PF	失敗の枝の数 MERC	解の数
10 クイーン	4,942	312,612	724
11 クイーン	21,528	1,639,781	2,680
Bennett 4	1	104	0
Bennett 5	1	2,400	1
Bennett 6	3	179,171	0
Bennett 7	6	52,249,612	3
Bennett 8	33	-	1
*Bennett 9	239	-	0
*Bennett 10	7,026	-	0
Bennett 11	51,899	-	5
*Bennett 12	2,749,676	-	0

表 1: 部分反駁法（Partial Falsification）の効果

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

表 2: Order 5 の Bennett の準群の例

がもとの要素になる．表 2は，Order 5 の場合の Bennett の準群の例である．たとえば，この表から，$3*4=1, 1*3=2, 2*3=4$ より，$3*4*3*3=4$ であることが分かる．

MGTP/G/MERC/PF/ は，このうち 9, 10, 12 の 3 つの order の場合について解が存在しないことを示すことができた．特に order 12 の場合は，PIM/m-256 で 3 時間 4 9 分あまりであり，単一プロセッサの計算機で解くと，優に 1 か月はかかってしまうという大きさの問題であった．また場合分けの数は 2,749,676 に及んでいる．オーストラリア国立大学の Finder[Sl92] という定理証明系は order 9 を SPARCserver-670 上で 26917 秒で解いたが，それ以上の order の問題は解くことができなかった．

Bennett の問題は，図 1で示すように定理証明の問題として表現される．

準群の性質を全く利用しない単純な問題表現で未解決問題の一部が解けたことは，それ以上の大きさの問題に対しても何らかの工夫で解を得ることができるという期待を持たせるものである．MGTP/G/MERC/PF は，この他にも上の例題から *idempotent* を除いた問題について未解決であった Order10 の例題を解いている．この例では，13101 cpu-sec(3 時間 39 分) かかり，4,473,508 の場合分けが試された．今回の実験で解かれた主な例題と計算時間を表 3に記す．ただし，Bennett 9 は単一プロセッサによる実行結果である．

```
dom(1),dom(2),dom(3),dom(4),dom(5),dom(6):- true.
p(M,N,1);p(M,N,2);p(M,N,3);p(M,N,4);p(M,N,5);p(M,N,6):- dom(M),dom(N).
false:- 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}.
```

図 1: Order 6 の Bennett 問題

問題	時間 (秒)
11 クイーン	2.3
12 クイーン	7.0
13 クイーン	27.9
14 クイーン	128.0
*Bennett 9	2116
*Bennett 10	66
Bennett 11	236
*Bennett 12	13,715
No Id 8	42
No Id 9	521
*No Id 10	13,101

表 3: MGTP/G/MERC/PF の実行時間

参考文献

[Be89] Bennett, F. E., "QUASIGROUP IDENTITIES AND MENDELSOHN DESIGNS," in *Can. J. Math., Vol. XLI, No. 2, pp. 341-368*, 1989.

[FH92] Fujita, M., and Hasegawa, R., Koshimura, M., Fujita, H., "Model Generation Theorem Provers on A Parallel Inference Machine," in *Proc. of FGCS'92*, to appear, 1992.

[MB88] Manthey, R. and Bry, F.,"SATCHMO: a theorem prover implemented in Prolog, " in *Proc. of CADE 88, Argonne, illinois*, 1988.

[Sl92] Slaney, J. K., "FINDER Finite Domain Enumerator VERSION2.0 NOTES AND GUIDE," from the public domain softwares, The Australian National University, 1992.