信州大学工学部

学士論文

ラテン方陣の効率の良い数え上げに向けた基礎的考察

指導教員　西新 幹彦 准教授

学科　電気電子工学科
学籍番号　12T2015J
氏名　岡田 航

2018 年 3 月 13 日

目次

1　はじめに

ラテン方陣は特別な MDS 符号の別表現である．ラテン方陣を効率よく見つけることで符号の構成を効率よく行うことができる．また，ラテン方陣の効率の良い見つけ方を拡張すれば，一般の MDS 符号の効率の良い見つけ方を構成することができる．MDS 符号とは，シングルトン限界を等号で満たす最大距離分離符号である [1]．実際に広く使われている MDS 符号としては，例えばリード・ソロモン符号などがある．リード・ソロモン符号は誤り訂正の能力が高く，地上デジタル放送や DVD，QR コードなどに使われている [2]．本研究では，ラテン方陣の特徴を利用して，効率よくラテン方陣を数え上げる方法のいくつかを考案し，5×5 ラテン方陣の数え上げに適用した．

2　ラテン方陣と符号の関係

$n \times n$ ラテン方陣とは，n 個の異なる数字が，各行及び各列に 1 回だけ現れるよう各セルに配置された $n \times n$ の格子のことである．ラテン方陣の行と列を表すインデックスをそれぞれ w_1, w_2 と表し，セル (w_1, w_2) の値を w_3 とすると，(w_1, w_2, w_3) の取りうる値の一覧は直交配列になる（図 1）．

この直交配列は，どの 1 列を隠してもすべての行は異なる値をとるという性質がある．この性質より，ラテン方陣は MDS 符号の別表現であることが言える [1]．

本研究では，ラテン方陣の数え上げを効率よく行うために，ラテン方陣の構造を明確にする．

	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

w_1	w_2	w_3
1	1	1
1	2	2
1	3	3
2	1	2
2	2	3
2	3	1
3	1	3
3	2	1
3	3	2

図 1　ラテン方陣と直交配列

3　3 × 3 ラテン方陣の数え上げ

まず，3 × 3 ラテン方陣を数え上げる方法を考える．「3 × 3 ラテン方陣はいくつあるか?」という問いに対して，1 行 1 列目のセルから値を固定していき，ラテン方陣が一つ出来上がるまで行う (図 2)．どのように固定していくかというと，同じ構造のもので固定していく．例えば図 2 では，1 行 1 列目には 1，2，3 のどれかの数字が入るが，どの数字を入れても数え上げの値に影響がないので，1 と固定して，数え上げてきた値に対して 3 を掛けることでまとめて数え上げている．すべてのセルの値が決まりラテン方陣が出来上がると，逆に折り返して計算することで数え上げることができる．以降は，同じ構造を見つける為の，ラテン方陣の特徴を述べていく．

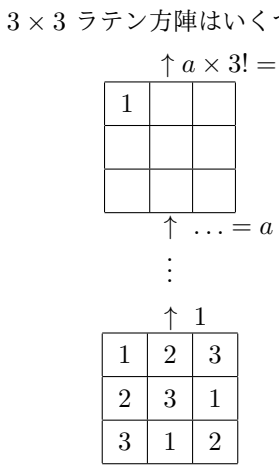

図 2　3 × 3 ラテン方陣の数え上げ

3.1　1 行目の対称性

ラテン方陣は列または行を交換してもやはりラテン方陣である為，対称性があると言える．例えば，図 3 の左側のラテン方陣の 1 列目と 2 列目を交換すると右側のラテン方陣になる．これより 1 行目のセルの値を固定することで数える個数を 3! 分の 1 に減らすことができる．

3.2　2 行 1 列目の対称性

3 × 3 ラテン方陣の 1 行目を固定した状態で，2 行 1 列目のマスに入る数を考える（図 4）．2 行 1 列目は 1 以外の 2,3 のどちらかが入り、どちらを入れても数え上げの値に影響がない為，

1	2	3	2	1	3
2	3	1	3	2	1
3	1	2	1	3	2

図 3　3 × 3 ラテン方陣

1	2	3	1	2	3
2			3		

図 4　3 × 3 ラテン方陣の 2 行 1 列目

1	2	3	1	3	2	1	2	3
2			3			3		

図 5　3 × 3 ラテン方陣の 2 行 1 列目

対称性があると言える．2 行 1 列目を決定することで，数える個数を 2 分の 1 に減らすことができる．

ここで，ラテン方陣は数字を置換してもラテン方陣としての特徴が崩れないため，ラテン方陣の数字を置換したものもラテン方陣といえる．これで，上記で述べた対称性の証明ができる。例えば図 5 左のラテン方陣を考える．$1 \to 1$, $2 \to 3$, $3 \to 2$ と数字を置換すると図 5 中となる．そして列を交換すると，図 5 右となる．これが図 4 右と等しくなるため，図 4 の 2 つのラテン方陣は構造等しい，つまりラテン方陣の 2 行 1 列目には対称性があると言える．

3.3　3 × 3 ラテン方陣の数え上げ

図 6 は，3 × 3 ラテン方陣はいくつあるかという問いに対して，同じ構造のものでまとめて，逆から数え上げている。例えば↑(i) では，3! 個の同じ構造のものをまとめているので，末端から数え上げてきたものに 3! を掛ければ同じ構造のものをまとめて数えた値が得られる．すると，図 7 の様に数え上げることができる．数え上げの末端では，1 つのラテン方陣が完成しているので，矢印↑(ii) では 1 × 2 となる．次の矢印↑(i) でも同様にすると，$2 \times 3! = 12$ 個と得られ，3 × 3 ラテン方陣の個数が数え上げられる．

3×3 ラテン方陣はいくつか?

↑(i)

1	2	3

↑(ii)

1	2	3
2		

↑(iii)

1	2	3
2	3	1
3	1	2

図 6　3×3 ラテン方陣の数え上げ

3×3 ラテン方陣はいくつか?

↑ $2 \times 3! = 12$(個)

1	2	3

↑ $1 \times 2 = 2$

1	2	3
2		

↑ 1

1	2	3
2	3	1
3	1	2

図 7　3×3 ラテン方陣の数え上げ

1	2	3	4
2	1		

1	2	3	4
2	3		

図 8　4×4 ラテン方陣の 2 行 2 列目

4　4×4 ラテン方陣の数え上げ

この章では，4×4 ラテン方陣の数え上げを 3 章と同様の方法で数え上げる．3×3 ラテン方陣から 4×4 ラテン方陣へとサイズを上げた場合どのような特徴が増えるのか，また 3×3 ラテン方陣の特徴が同様に 4×4 ラテン方陣にも表れるのか考える．

4.1　2 行 2 列目の対称性と構造の変化

4×4 ラテン方陣の 2 行 1 列目までを固定した状態で，2 行 2 列目の数を考える（図 8）．2 行 2 列目を 1 かそれ以外の 3，4 か決定することで，2 行 3 列目以降に構造の変化が生じる．また，3 または 4 のどちらかを入れる場合、どちらを入れても数え上げの個数に影響がない為，対称性があると言える．

1	2	3	4
2	1	4	3

1	2	3	4
2	3	4	1

図 9　4 × 4 ラテン方陣の対称性

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

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

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

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

図 10　グループ化可能

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

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

図 11　グループ化不可能

4.2　最後の 2 行について

図 9 の 4 × 4 ラテン方陣を考える．左は 3 行目の場合の数が 4 個であるが，右は 2 個である．この違いは，1 行目と 2 行目を列で見たときにグループで分けることができるかどうかである．左では，(1, 2)(3, 4) の 2 グループに分けることができるが，右ではグループに分けることができない．4 × 4 ラテン方陣の 2 行目まで固定された状態で，グループ化可能 (図 10) であると，3 行目の数は 4 個あるが，グループ化不可能 (図 11) であると 2 個しかない．これは，図 9 左のラテン方陣では，1 列目と 2 列目に (1，2) のグループ，3 列目と 4 列目に (3，4) のグループがあり，グループになっていると 3 行目以降の (1，2) と (3，4) はそれぞれ独立しているとみなせるため，それぞれ (1，2)，(3，4) のグループ同士を入れ替えてもラテン方陣としての特性は崩れないからである．

4.3　4×4 ラテン方陣の数え上げ

3 章で述べた 3×3 ラテン方陣の数え上げに用いたルールを，4×4 ラテン方陣の数え上げに応用することができる．これらに 4.1 節及び 4.2 節のルールを加えると，4×4 ラテン方陣を数え上げることができる (図 12).

5　2 行目の場合の数の再帰構造

ここで話を少し逸らして，2 行目のみの場合の数を考える．5×5 までのラテン方陣の 2 行目の場合の数は，比較的短時間で求められる．結果，$3 \times 3, 4 \times 4, 5 \times 5$ ラテン方陣の 2 行目の場合の数はそれぞれ 2, 9, 44 通りあると分かった．

次に 6×6 ラテン方陣の 2 行目の場合の数を考える．3.3 節で述べたように，1 行目が決まった状態で，2 行 2 列目のマスに 1 かそれ以外を入れるかで 2 行 3 列目以降の数え上げの値が変化する (図 5)．すると，2 行 2 列目に 1 を入れた時，3 列目から 6 列目に入る数列の数が 4×4 の 2 行目の場合の数と同じであり，1 以外を入れた時には，2 列目から 6 列目に入る数列の数が 5×5 の 2 行目の場合の数と同じである事が分かった．これより，4×4 と 5×5 ラテン方陣の 2 行目の場合の数から 6×6 の 2 行目の場合の数は

$$S_6 = (S_4 + S_5) \times 5 = (9 + 44) \times 5 = 265$$

のように得られる．ただし，S_n を $n \times n$ ラテン方陣の 2 行目の場合の数とする．この式を一般化すると

$$S_n = (S_{n-2} + S_{n-1}) \times (n - 1)$$

が得られる．

6　5×5 ラテン方陣の数え上げ

6.1　5×5 ラテン方陣におけるグループ化

5×5 ラテン方陣においても，図 14 や図 15 の様にラテン方陣の中にグループがある場合は，それぞれのラテン方陣が同じ構造であると言うことができる．図 14 では，1，2 行 1，2 列に 1 と 2 のグループができているので，3 行 4，5 列目の 1 と 2 を入れ替えても 4 行目以降に影響がない為，同じ構造であるといえる．同様に図 15 では 1，2 行 4，5 列に 4 と 5 のグループができているので，3 行 1，3 列目の 4 と 5 を入れ替えても 4 行目以降に影響がないため同じ構造であるといえる．これは，4.2 節と同様考えられ，それぞれの (1，2) と (3，4) は独立

4×4 ラテン方陣はいくつか?

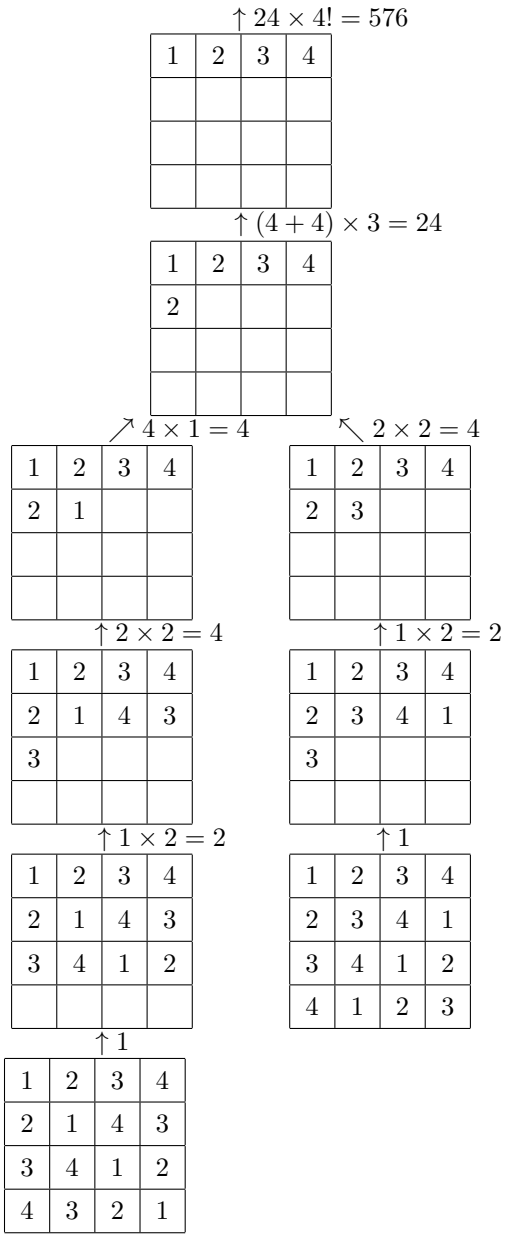

図 12　4×4 ラテン方陣の数え上げ

していると考えられるからである．これらのラテン方陣は，セルがすべて埋まった状態であれば，数字の置換及び行列の交換によって等しいと証明することもできるが，グループ化することで 3 行目までしか決まってない状態でも等しい構造であると言える．

6.2　5 × 5 ラテン方陣の数え上げ

5 × 5 ラテン方陣は，これまでのルールに加えて 6.1 節のグループ化を用いることで，図 17 の (iv)，(v) の数え上げをまとめることができる．(1，2) と (4，5) のグループが出来ているため，図 14 と図 15 のようなラテン方陣を，それぞれまとめて数え上げている．5 × 5 ラテン方陣は 161,280 個存在するが，数え上げの末端を 7 つまで省略することができているので，数え上げの効率はとても良いと考えられる．

1	2	3	4	5	6
2	1				

1	2	3	4	5	6
2	3				

図 13　6 × 6 ラテン方陣の 2 行目

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

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

図 14　5 × 5 ラテン方陣 (1，2) グループ

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

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

図 15　5 × 5 ラテン方陣 (4，5) グループ

5 × 5 ラテン方陣はいくつあるか？

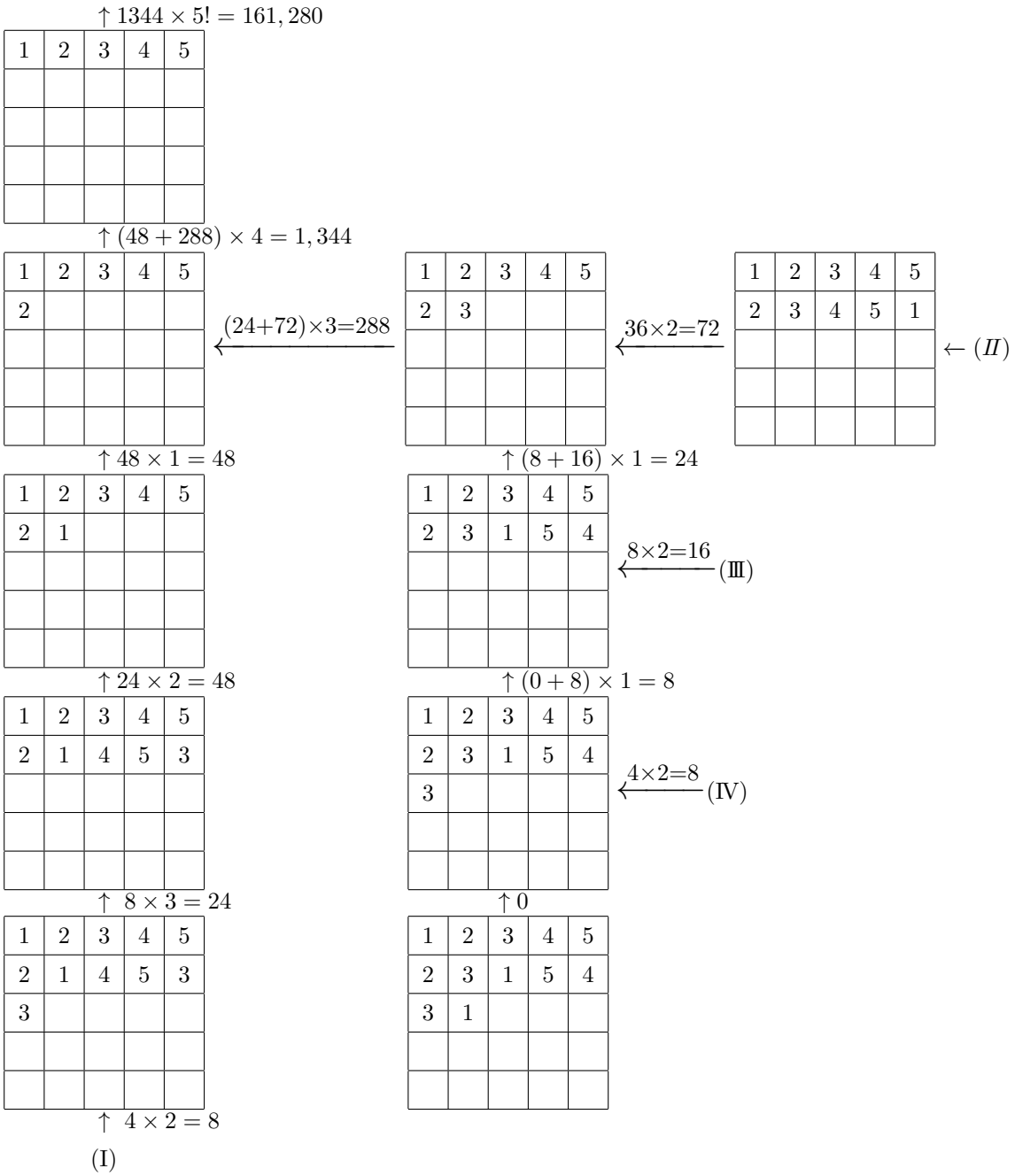

図 16　5 × 5 ラテン方陣の数え上げ (1)

(I)

↑

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

↑ $2 \times 2 = 4$(iv)

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

↑ $1 \times 2 = 2$

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

↑ 1

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

(Ⅳ)

↑

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

↑ $2 \times 2 = 4$(v)

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

↑ $1 \times 2 = 2$

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

↑ 1

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

(Ⅲ)

↑

1	2	3	4	5
2	3	1	5	4
4				

↑ $4 \times 2 = 8$

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

↑ $2 \times 2 = 4$

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

↑ $1 \times 2 = 2$

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

↑ 1

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

図 17　5×5 ラテン方陣の数え上げ (2)

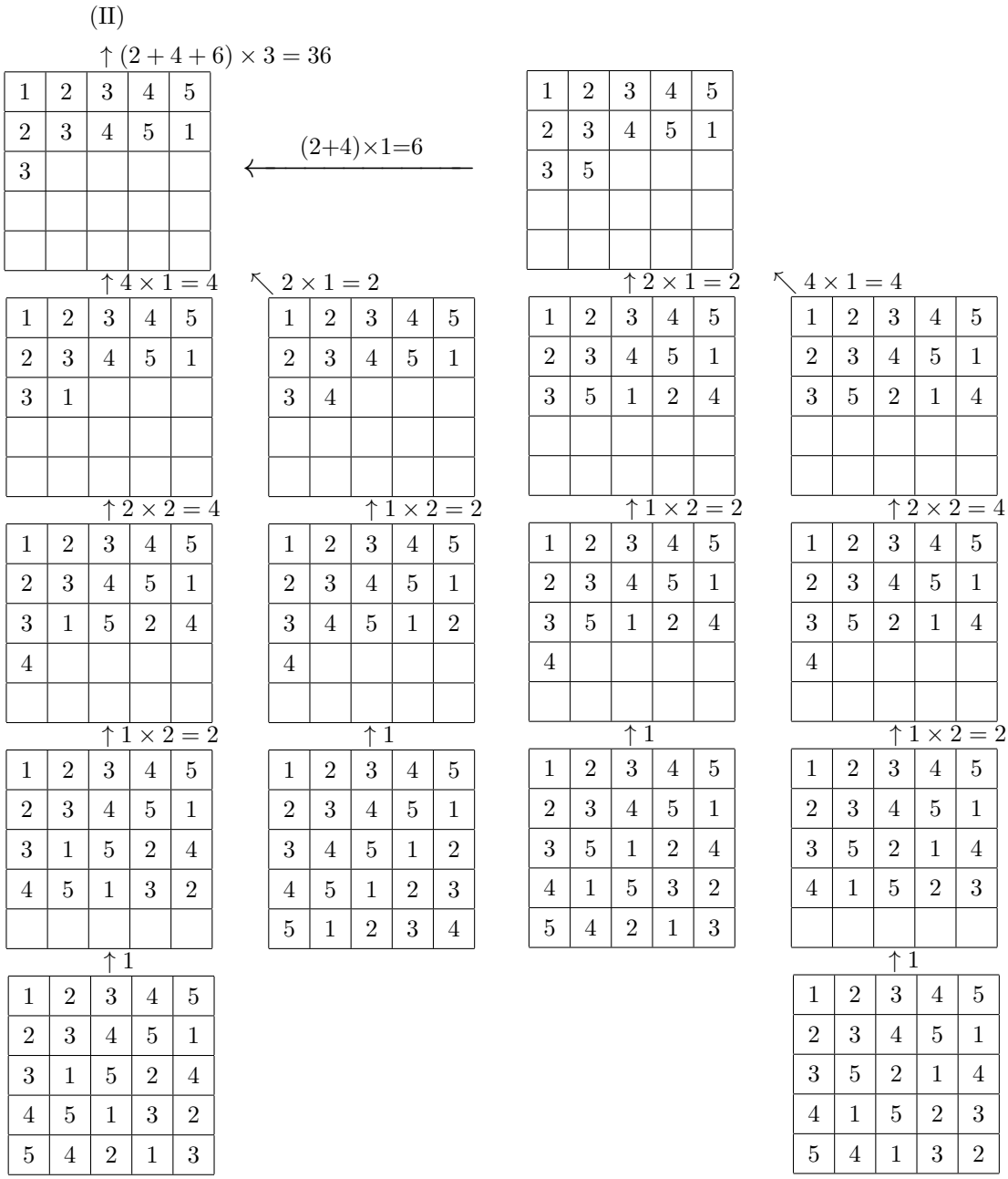

図 18　5 × 5 ラテン方陣の数え上げ (3)

7　まとめと今後の課題

5 × 5 までのラテン方陣を 1 行 1 列，2 列と順に固定していき，構造を明確にすることで，構造が同じ場合はまとめ，構造が異なる場合は分岐して数え上げることができた．5 × 5 ラテン方陣の総数は 161,280 個あるが，本研究の数え上げでは，数え上げの末端を 7 つにまで省略することができたので，効率がとても上がったと考えられる．また，2 行目以外の行に依存しない，2 行目のみの場合の数が得られる式を一般化することができた．4 × 4 までのラテン方陣の構造が 5 × 5 ラテン方陣の数え上げに応用出来たので，5 × 5 までのラテン方陣の構造が 6 × 6 ラテン方陣の数え上げに応用できると予想できる．また，これらの構造を基礎として，次数を挙げた場合，例えば 3 × 3 × 3 ラテン立方体の数え上げに応用できると予想できる．今後は，本研究で得られたラテン方陣の構造をプログラム化することと、サイズや次数を上げた場合にどのような特徴があるかを調べることが課題である．

謝辞

本研究を行うにあたり，指導をしてくださった指導教員西新幹彦准教授，また西新研究室の皆様に感謝の意を表する．

参考文献

[1] A. S. Hedayat, N. J. A. Sloane, John Stufken, *Orthogonal Arrays*, Springer, 1999.
[2] 和田山正，誤り訂正技術の基礎，森北出版，2010.