群論と対称性 (2017 年度) – 組合せ論

花木 章秀

このテキストは 2017 年度信州大学大学院講義のために、主に「J. S. van Lint & R. M. Wilson, A course in Combinatorics, 2nd edition」の一部を参考に作成されたものである。

1 順序集合に関する定理と極値集合論

S を集合とする。S 上の**関係** (relation) とは、直積集合 $S \times S$ の部分集合のことである。$a, b \in S$ に対して $(a, b) \in R$ であることを aRb と表す。R を S 上の関係とするとき、集合と関係の組 (S, R) が**順序集合** (半順序集合, ordered set, partially ordered set, poset) であるとは、以下の 3 つの条件が成り立つことである。

- (反射律) aRa $(\forall a \in S)$
- (推移律) aRb and $bRc \Longrightarrow aRc$
- (非対称律) aRb and $bRa \Longrightarrow a = b$

このとき、単に S を順序集合と言ったり、R を S 上の順序と言ったりもする。以下では、抽象的な順序を表す記号に $\leq$ を用いる。$a \leq b$ かつ $a \neq b$ であるとき $a < b$ とも表す。また $a \leq b$ (または $a < b$) を $b \geq a$ (または $b > a$) とも表す。

順序集合 S の任意の 2 元 a, b に対して $a \leq b$ または $a \geq b$ が成り立つとき、S を**全順序集合** (totally ordered set) という。

例 1.1. (1) $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$ は通常の数の大小で全順序集合である。$\mathbb{C}$ を順序集合と見るには、その順序を明確にする必要がある。

(2) X を集合とし、その**べき集合** (power set)、すなわち X の部分集合全体の集合、を 2^X で表す。2^X は集合の包含関係によって順序集合であるが、$|X| \geq 2$ ならば全順序集合ではない。

(S, R) を順序集合とし、T をその部分集合とする。このとき $(T, R \cap (T \times T))$ はまた順序集合となる。これを**順序部分集合**という。紛らわしくないときは、順序を表す記号には同じものを用いる。例えばこの場合は (T, R) と表す。

以下では、有限な順序集合を考える。特に断らなくても、集合は有限集合であるとする。

$(S, \leq)$ を順序集合とし T を S の順序部分集合とする。T が全順序集合であるとき、これを **chain** という。すなわち $T = \{x_1, \ldots, x_m\}$, $x_1 < x_2 < \cdots < x_m$ と表されるとい

うことである。T の任意の異なる 2 元 a, b に対して、$a \leq b$ も $a \geq b$ も成り立たないとき (a と b が比較不能であるとき)、T を **antichain** という。

例 1.2. $X = \{1, 2, 3\}$, $S = 2^X$ とするとき、$T = \{\emptyset, \{1\}, \{1, 2\}, \{1, 2, 3\}\}$ は chain である。また $T = \{\{1\}, \{2\}, \{3\}\}$ や $T = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$ は antichain である。

定理 1.3 (Dilworth, 1950)**.** P を有限順序集合とする。P は m 個の共通部分のない chain の和集合に分割され、m 未満の個数の chain の共通部分のない和集合には分割されないものとする。このとき m は antichain の要素数の最大値に等しい。

証明. M を antichain の要素数の最大値とし、U を $|U| = M$ である antichain とする。また $P = T_1 \cup \cdots \cup T_m$ を chain の共通部分のない和集合への分割とする。

U の 2 元がある chain に同時に含まれることはないから $m \geq M$ である。

$m = M$ を $|P|$ に関する帰納法で示す。$|P| = 0$ のときは明らかである。$|P| > 0$ とする。T_m が極大な chain でないならば、$T_m \cup \{x\}$ がまた chain となる $x \in P$ がある。$x \in T_i$ とするとき、T_i を $T_i \setminus \{x\}$ で、T_m を $T_m \cup \{x\}$ で置き換えても chain の和集合になるという条件はみたされる。これを繰り返せば T_m は極大な chain であるとしてよい。$P' = P \setminus T_m$ に帰納法の仮定を用いる。$P' = T_1 \cup \cdots \cup T_{m-1}$ は chain の和集合への分割であり、これよりも少ない個数の chain への分割があれば、P も m 個より少ない chain に分割され矛盾である。したがって $m' = m - 1$ が P' の分割の最小数である。P' の antichain の要素数の最大値 M' について $M' \leq M - 1$ が成り立てば、帰納法の仮定から $m - 1 = m' = M' \leq M - 1$ となり $m = M$ が成り立つ。$M' \leq M$ は明らかなので $M' = M$ と仮定する。

$\{a_1, \ldots, a_M\}$ を P' の antichain とする。$S^- = \{x \in P \mid$ ある i について $x \leq a_i\}$, $S^+ = \{x \in P \mid$ ある i について $x \geq a_i\}$ とおく。T_m は極大 chain なので、T_m の最大元は S^- に含まれない。よって $|S^-| < |P|$ であり、帰納法の仮定から S^- は M 個の chain の和集合となる。異なる a_i, a_j が同じ chain に含まれることはないから、S^- の chain S_i^- を用いて、$S^- = S_1^- \cup \cdots \cup S_M^-$, $a_i \in S_i^-$ と表すことができ、a_i は S_i^- の最大元である。同様に $S^+ = S_1^+ \cup \cdots \cup S_M^+$, $a_i \in S_i^+$ と表すことができ、$S_i = S_i^- \cup S_i^+$ とおけば $P = S_1 \cup \cdots \cup S_M$ は P の chain への分割となる。したがって $m \leq M$ となり $m = M$ が成り立つ。 $\square$

定理 1.4 (Milsky, 1971)**.** P を有限順序集合とし、元の数が $m + 1$ 以上の chain をもたないとする。このとき P は m 個の antichain の共通部分のない和集合に分割される。

証明. 主張を m に関する帰納法で示す。$m = 1$ のときは P 自身が antichain となるので、主張は成り立つ。

$m > 1$ とする。M を P の極大元全体の集合とする。M は antichain である。$P' = P \setminus M$ に長さ m の chain があれば、それは P の極大な chain となるから、その最大元は M に入り、矛盾である。したがって P' は長さ $(m-1)+1$ の chain をもたない。帰納法の仮定から P' は $m - 1$ 個の antichain の和集合となり、M と併せて P は m 個の antichain の和集合となる。 $\square$

定理 1.5 (Sperner, 1966)**.** $N = \{1, 2, \ldots, n\}$ とする。$A_1, \ldots, A_m$ を N の部分集合で $i \neq j$ のとき A_i が A_j の部分集合ではないものとする。このとき $m \leq \binom{n}{\lfloor n/2 \rfloor}$ である[1]。

[1] $\lfloor n/2 \rfloor$ は $n/2$ を超えない最大の整数を表す (ガウス記号)。

証明. 順序集合 2^N を考える。$A_1,\dots,A_m$ の条件は、$\mathfrak{A}=\{A_1,\dots,A_m\}$ が 2^N の antichain であるということである。2^N の 極大な chain は、要素数が $0,1,\dots,n$ となるもので、その長さは $n+1$ で、全部で $n!$ 個あることが分かる。$A\in 2^N$, $|A|=k$ なる A に対して、A を含む極大 chain は $k!(n-k)!$ 個ある。

$\mathfrak{C}=\{(A,C)\mid A\in\mathfrak{A},\ C$ は 2^N の極大な chain で A を含むもの $\}$ とおいて、その要素数を数える。極大な chain は高々 1 つの $\mathfrak{A}$ の元を含むので $|\mathfrak{C}|\le n!$ である。$\alpha_k=\sharp\{A\in\mathfrak{A}\mid \sharp A=k\}$ とおく。このとき $|\mathfrak{C}|=\sum_{k=0}^n\alpha_k k!(n-k)!$ である。$\binom{n}{k}\le\binom{n}{\lfloor n/2\rfloor}$ であるから、$m=\sum_{k=0}^n\alpha_k$ と併せて

$$1\ge\sum_{k=0}^n\alpha_k\frac{k!(n-k)!}{n!}=\sum_{k=0}^n\frac{\alpha_k}{\binom{n}{k}}\ge\frac{\sum_{k=0}^n\alpha_k}{\binom{n}{\lfloor n/2\rfloor}}=\frac{m}{\binom{n}{\lfloor n/2\rfloor}}$$

となる。 □

2^N のすべての $\lfloor n/2\rfloor$-部分集合 (n が奇数のときは $\lfloor n/2\rfloor+1$ でもよい) を antichain として取るとき、この定理の等号は成立する。

ここで定理 1.3 の一つの応用を示す。

命題 1.6. $a_1,\dots,a_{n^2+1}$ を $1,\dots,n^2+1$ を任意の順番に並べ替えたものとする。このとき、長さ $n+1$ の増加部分列、または減少部分列が存在する。

証明. $N=\{1,2,\dots,n^2+1\}$ に関係 $\preceq$ を「$i\le j$ かつ $a_i\le a_j$ のとき $i\preceq j$」で定めれば、これは順序となる。N に $\preceq$ に関する長さ $n+1$ の chain $C=\{c_1,\dots,c_{n+1}\}$ ($c_1\preceq\cdots\preceq c_{n+1}$) があれば、$a_{c_1},\dots,a_{c_{n+1}}$ は増加部分列である。したがって N の chain の長さは高々 n であると仮定する。このとき、N を共通部分のない chain の和集合に分割すれば、その chain の数は少なくとも $n+1$ 個ある。定理 1.3 から、N には要素数 $n+1$ の antichain $D=\{d_1,\dots,d_{n+1}\}$ ($d_1<\cdots<d_{n+1}$) があり、順序の定義から $a_{d_1}>\cdots>a_{d_{n+1}}$ となる。すなわち D は長さ $n+1$ の減少部分列を定める。 □

命題 1.6 には、次のように「鳩の巣原理」[2]を用いた直接的な証明もある。

命題 *1.6* の別証明. 長さ $n+1$ の増加部分列がないと仮定する。b_i を a_i で始まる増加部分列の長さの最大値とする。$1\le b_i\le n$ であるから「鳩の巣原理」より、ある k があって $\sharp\{i\mid b_i=k\}\ge n+1$ である。$b_i=b_j=k,\ i<j$ とする。$a_i<a_j$ であるとすると、a_i に a_j で始まる長さ k の増加列をつないで、長さ $k+1$ の増加列ができ $b_i=k$ に矛盾する。したがって $a_i>a_j$ である。よって $\{i\mid b_i=k\}$ は長さ $n+1$ 以上の減少部分列を定める。 □

定理 1.5 のように「ある条件をみたす部分集合の集合を最大 (最小) で何個とれるか」を考える理論を**極値集合論** (extremal set theory) という。簡単な例から始める。

命題 1.7. $N=\{1,2,\dots,n\}$ の部分集合 $A_1,\dots,A_m$ が、任意の i,j に対して $A_i\cap A_j\neq\emptyset$ をみたすならば $m\le 2^{n-1}$ である。また等号をみたす $A_1,\dots,A_m$ が存在する。

[2]「鳩の巣原理」とは「$n>m$ のとき m 個の巣箱に n 羽の鳩が入っているならば、少なくとも 1 つの巣箱には 2 羽以上の鳩が入っている」ということである。

証明. $\mathfrak{A} = \{A_1, \dots, A_m\}$ が命題の条件をみたすとする。$A_i \cap A_i^C = \emptyset$ (A_i^C は A_i の補集合) であるから $A_i^C \notin \mathfrak{A}$ である。$\mathfrak{A} \cap \{A_1^C, \dots, A_m^C\} = \emptyset$ であるから $m = |\mathfrak{A}| \le 2^n/2 = 2^{n-1}$ である。

固定した i を含む部分集合全体は条件をみたし、その個数は 2^{n-1} である。 □

定理 1.8 (Erdös-Ko-Rado, 1961)**.** $k \le n/2$ とする。$N = \{1, 2, \dots, n\}$ の k-部分集合 $A_1, \dots, A_m$ が、任意の i, j に対して $A_i \cap A_j \neq \emptyset$ をみたすならば $m \le \binom{n-1}{k-1}$ である。

証明. $\mathfrak{A} = \{A_1, \dots, A_m\}$ とおく。また $i = 1, \dots, n$ に対して $F_i = \{i, i+1, \dots, i+k-1\}$ とおく。ただし、数は n を法として考える。$\mathfrak{F} = \{F_1, \dots, F_n\}$ とおく。

$|\mathfrak{A} \cap \mathfrak{F}| \le k$ であることを示す。$F_i \in \mathfrak{A}$ とする。$\mathfrak{A}$ の要素は F_i と共通部分をもたなければならないので $\mathfrak{A} \cap \mathfrak{F} \subset \{F_{i-k+1}, \dots, F_{i-1}, F_i, F_{i+1}, \dots, F_{i+k-1}\}$ である。ここで $1 \le \ell \le k-1$ に対して $F_{i-k+\ell}$ と $F_{i+\ell}$ は共通部分がないので、高々その一方だけが $\mathfrak{A}$ に入る。したがって $|\mathfrak{A} \cap \mathfrak{F}| \le k$ である。$\pi \in S_n$ (S_n は n 次対称群) とすると $|\mathfrak{A} \cap \mathfrak{F}^\pi| = |(\mathfrak{A}^{\pi^{-1}} \cap \mathfrak{F})^\pi| = |\mathfrak{A}^{\pi^{-1}} \cap \mathfrak{F}| \le k$ も成り立つ。よって

$$\sum_{\pi \in S_n} |\mathfrak{A} \cap \mathfrak{F}^\pi| \le k \cdot n!$$

である。$\pi \in S_n$ を固定すれば $|\mathfrak{A} \cap \mathfrak{F}^\pi| = \sharp\{(A_j, F_i) \in \mathfrak{A} \times \mathfrak{F} \mid A_j = F_i^\pi\}$ である。したがって

$$\sum_{\pi \in S_n} |\mathfrak{A} \cap \mathfrak{F}^\pi| = \sharp\{(A_j, F_i, \pi) \in \mathfrak{A} \times \mathfrak{F} \times S_n \mid A_j = F_i^\pi\}$$

である。任意の $A_j \in \mathfrak{A}$, $F_i \in \mathfrak{F}$ に対して $A_j = F_i^\pi$ となる $\pi \in S_n$ は $k!(n-k)!$ 個あるから、右辺の値は $mn \cdot k!(n-k)!$ である。以上を併せて

$$m \le \frac{k \cdot n!}{n \cdot k!(n-k)!} = \frac{(n-1)!}{(k-1)!((n-1)-(k-1))!} = \binom{n-1}{k-1}$$

となる。 □

定理 1.8 の等号が成立する場合を考える。すぐに分かるように、$\mathfrak{A}$ として、固定した i を含むすべての k-部分集合をとれば、等号が成り立つことが分かる。また $n = 2k$ のときには $\mathfrak{A}$ として、固定した i を含まないすべての k-部分集合をとれば、次のようにして、等号が成立することが分かる。まず $A, B \in \mathfrak{A}$ とすれば、その要素数の和は $2k = n$ で、いずれも i を含まないので、共通部分は空ではない。また i を含まない部分集合は $\binom{n-1}{k} = \binom{n-1}{k-1}$ 個あるのでこの場合にも等号が成立している。このように等号が成立する例を作ることは難しくないが、等号が成立するものをすべて決定することは容易ではない。

2 q-類似

前節で有限集合の部分集合で、ある性質をもつものの個数に関するいくつかの結果を見た。類似の結果がベクトル空間の部分空間についても成り立つことが知られている。ただし、個数に関する結果なので考える係数体は有限体である。(実数体のような無限体

では多くのものの個数が無限となる。) $\mathbb{F}_q$ で q 個の元をもつ有限体を表す。q はある素数 p を用いて $q = p^e$ と表され、$\mathbb{F}_q$ の標数は p である。

$\mathbb{F}_q$ 上の n 次元ベクトル空間 $\mathbb{F}_q^n$ の部分空間全体の集合を包含関係によって順序集合と見る。極大 chain は次元が $0, 1, \ldots, n$ となる部分空間の列である。極大 chain の個数を数える。まず 0 次元空間は 1 つである。1 次元空間は、$\mathbf{0}$ でない 1 つのベクトルで表されるが、0 でないスカラー倍では同じ空間を定めるので、$(q^n - 1)/(q - 1)$ 個ある。1 次元空間 V_1 を固定したとき、V_1 を含む 2 次元空間 V_2 は V_1 に含まれない 1 つのベクトルで定まる。同じ空間を定めるベクトルは $|V_2 \setminus V_1|$ 個ある。したがって V_1 を含む 2 次元空間は $(q^n - q)/(q^2 - q)$ 個ある。同様にして k 次元部分空間 V_k を含む $(k + 1)$ 次元空間は $(q^n - q^k)/(q^{k+1} - q^k)$ 個あることが分かる。したがって極大 chain の数は

$$\begin{aligned} M(n, q) &= \frac{q^n - 1}{q - 1} \frac{q^n - q}{q^2 - q} \cdots \frac{q^n - q^k}{q^{k+1} - q^k} \cdots \frac{q^n - q^{n-1}}{q^n - q^{n-1}} \\ &= \frac{(q^n - 1)(q^{n-1} - 1) \ldots (q^2 - 1)(q - 1)}{(q - 1)^n} \end{aligned}$$

となる。先に断ったように q は素数べきでなければならないが、これを q に関する多項式とも見て、素数べき以外の値も代入できると考える。$(q - 1)$ の項はすべて約分されることに注意して $q = 1$ を代入すれば $M(n, 1) = n!$ であることが分かる。

$\mathbb{F}_q^n$ の k 次元部分空間の数を $\begin{bmatrix} n \\ k \end{bmatrix}_q$ と表し**ガウス数** (Gaussian number) という。$M(n, k)$ を求めた方法でも $\begin{bmatrix} n \\ k \end{bmatrix}_q$ は求められるが、ここでは違う表記を求める。集合

$$\mathfrak{S} = \{(U, C) \mid U \text{ は } k \text{ 次元部分空間、} C \text{ は極大 chain で } U \text{ を含むもの} \}$$

の要素数を数える。極大 chain に対して k 次元部分空間はただ一つ定まるので $|\mathfrak{S}| = M(n, k)$ である。k 次元部分空間 U を固定して考える。U の部分空間の順序集合の極大 chain は $M(k, q)$ 個ある。また商空間 $\mathbb{F}_q^n/U$ の部分空間の順序集合の極大 chain は $M(n - k, q)$ 個あり、これが U を含む $\mathbb{F}_q^n$ の部分空間の chain に対応する。よって U を含む極大 chain は $M(n - k, q)M(k, q)$ 個あることになる。したがって $|\mathfrak{S}| = \begin{bmatrix} n \\ k \end{bmatrix}_q M(n - k, q)M(k, q)$ が成り立ち

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{M(n, q)}{M(n - k, q)M(k, q)} = \frac{(q^n - 1) \ldots (q^{n-k+1} - 1)}{(q^k - 1) \ldots (q - 1)}$$

となる。$M(n, 1) = n!$ であったことと合わせると、$\begin{bmatrix} n \\ k \end{bmatrix}_q$ が二項係数 $\binom{n}{k}$ の類似物であることが分かる。

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ n - k \end{bmatrix}_q, \quad \begin{bmatrix} n \\ k \end{bmatrix}_q \leq \begin{bmatrix} n \\ \lfloor n/2 \rfloor \end{bmatrix}_q$$

などがすぐに確認できる。

定理 1.5 (Sperner) の類似が次のように成り立つ。このように集合に対して成立する定理の類似を **q-類似**という。

定理 2.1. $\mathfrak{A}$ を $\mathbb{F}_q^n$ の部分空間のなす順序集合の antichain とする。このとき $|\mathfrak{A}| \leq \begin{bmatrix} n \\ \lfloor n/2 \rfloor \end{bmatrix}_q$ が成り立つ。

証明. $\mathfrak{S} = \{(U, C) \mid U \in \mathfrak{S}$、$C$ は極大 chain で U を含むもの $\}$ とおく。各極大 chain は高々 1 つの $\mathfrak{A}$ の要素を含むので $|\mathfrak{S}| \leq M(n,q)$ である。また $U \in \mathfrak{A}$ の次元を k とすれば、それを含む極大な chain は $M(n-k,q)M(k,q)$ 個ある。$\mathfrak{A}$ に含まれる k 次元部分空間の数を c_k とすると、$|\mathfrak{S}| = \sum_{k=0}^{n} c_k M(n-k,q)M(k,q)$ である。よって

$$1 \geq \sum_{k=0}^{n} c_k \frac{M(n-k,q)M(k,q)}{M(n,q)} = \sum_{k=0}^{n} c_k \frac{1}{\begin{bmatrix} n \\ k \end{bmatrix}_q} \geq \frac{\sum_{k=0}^{n} c_k}{\begin{bmatrix} n \\ \lfloor n/2 \rfloor \end{bmatrix}_q} = \frac{|\mathfrak{A}|}{\begin{bmatrix} n \\ \lfloor n/2 \rfloor \end{bmatrix}_q}$$

となり、結果を得る。 $\square$

よく知られているように二項係数は有理数の形で表されるが、すべて自然数である。$M(n,q)$ は q を不定元と見て多項式になるが $\begin{bmatrix} n \\ k \end{bmatrix}_q$ は有理式である。しかし、これは実際には q の有理整数係数多項式である。これを示しておこう。一つの補題を用意する。

補題 2.2. $r(x)$ を不定元 x に関する $\mathbb{Q}$ 上の有理式とする。すなわち $f(x), g(x) \in \mathbb{Q}[x]$, $g(x) \neq 0$ があって $r(x) = f(x)/g(x)$ である。$r(x)$ が無限個の整数に対して整数値をとるとき、$r(x) \in \mathbb{Q}[x]$ である。

証明. $r(x) = f(x)/g(x)$, $f(x), g(x) \in \mathbb{Z}[x]$, $g(x) \neq 0$, $f(x)$ と $g(x)$ は共通の因子をもたない、としてよい。$\deg g(x) \geq 1$ とする。多項式の割り算をして

$$f(x) = \widetilde{h}(x)g(x) + \widetilde{k}(x), \quad \deg \widetilde{k}(x) < \deg g(x)$$

とする。ただし $\widetilde{h}(x), \widetilde{k}(x) \in \mathbb{Q}[x]$ である。ここで $\widetilde{k}(x) = 0$ ならば $r(x)$ は多項式となるので $\widetilde{k}(x) \neq 0$ と仮定する。

$$r(x) = \frac{f(x)}{g(x)} = \widetilde{h}(x) + \frac{\widetilde{k}(x)}{g(x)}$$

である。$\widetilde{h}(x), \widetilde{k}(x)$ の係数の分母の公倍数を c とし $h(x) = c\widetilde{h}(x)$, $k(x) = c\widetilde{k}(x)$ とおけば $h(x), k(x) \in \mathbb{Z}[x]$ で

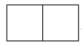
$$cr(x) = h(x) + \frac{k(x)}{g(x)}, \quad 0 \leq \deg k(x) < \deg g(x)$$

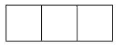
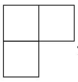
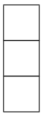
である。$\lim_{x \to \pm\infty} k(x)/g(x) = 0$ なので、ある N があって $|a| \geq N$ ならば $|k(a)/g(a)| < 1$ となる。よって $a \in \mathbb{Z}$, $|a| > N$ ならば $cr(a) \in \mathbb{Z}$ となるには $k(a) = 0$ が必要であるが、$k(x) = 0$ の根は有限個である。よって $cr(a) \in \mathbb{Z}$ となる $a \in \mathbb{Z}$ は有限個しかなく、$r(x)$ についても同様である。 $\square$

$\begin{bmatrix} n \\ k \end{bmatrix}_q$ は q に関する有理式であり、素数べき q に対しては $\mathbb{F}_q^n$ の k 次元部分空間の個数だから整数値である。したがってこの補題から $\begin{bmatrix} n \\ k \end{bmatrix}_q$ は q に関する多項式であることが分かる。次にこの多項式の係数を組合せ論的に記述することを考える。少し準備が必要である。

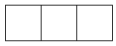
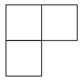
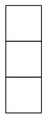
n を自然数とする。n の**分割**とは、数列 $\lambda = (\lambda_1, \ldots, \lambda_d)$ で $\lambda_1 \geq \cdots \geq \lambda_d \geq 0$, $\sum_{i=1}^{d} \lambda_i = n$ をみたすものである。ただし d は固定しない。n の分割 $\lambda = (\lambda_1, \ldots, \lambda_d)$ に対して、各行に λ_i 個の箱を並べた図形を**ヤング図形**という。

例 2.3. (1) $n=1$ のとき。分割は (1) のみで、ヤング図形は  である。

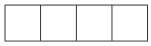
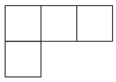
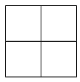
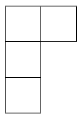
(2) $n=2$ のとき。分割は (2), $(1,1)$ で、ヤング図形は、それぞれ ,  である。

(3) $n=3$ のとき。分割は (3), $(2,1)$, $(1,1,1)$ で、ヤング図形は、それぞれ , ,  である。

(4) $n=3$ のとき。分割は (3), $(2,1)$, $(1,1,1)$ で、ヤング図形は、それぞれ以下の通りである。

(5) $n=4$ のとき。分割は (4), $(3,1)$, $(2,2)$, $(2,1,1)$, $(1,1,1,1)$ で、ヤング図形は、それぞれ以下の通りである。

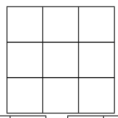
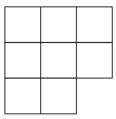
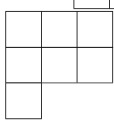
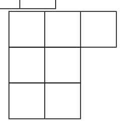
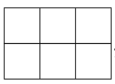
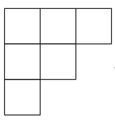
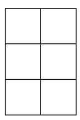
$\begin{bmatrix} n \\ k \end{bmatrix}_q$ の係数は以下のように記述される

定理 2.4. $\begin{bmatrix} n \\ k \end{bmatrix}_q = \sum_{\ell=0}^{k(n-k)} a_\ell q^\ell$ とする。このとき a_ℓ は ℓ の分割でそのヤング図形が $k \times (n-k)$ の箱に収まるものの数に等しい。特に a_ℓ はすべて非負整数である。

証明の前に簡単な例を確認しておく。

例 2.5. $(n,k)=(6,3)$ とする。直接計算によって

$$\begin{bmatrix} 6 \\ 3 \end{bmatrix}_q = q^9 + q^8 + 2q^7 + 3q^6 + 3q^5 + 3q^4 + 3q^3 + 2q^2 + q + 1$$

が分かる。$\ell = 9$ ならば $k \times (n-k) = 3 \times 3$ の箱に収まるものは  のみの 1 個である。$\ell = 8$ ならば  の 1 個である。$\ell = 7$ ならば ,  の 2 個である。$\ell = 6$ ならば , ,  の 3 個である。以下同様に、定理の主張が確かめられる。

定理 2.4 の証明. 無限個の値で値が等しくなる二つの多項式は等しいので、素数べき q に対して成り立つことを示せばよい。$\mathbb{F}_q^n$ の k 次元部分空間を考える。

$\mathbb{F}_q^n$ の k 次元部分空間 V の基底を行ベクトルとして並べれば階数 k の $k \times n$ 行列ができる。これを行の基本変形によって、一意的に被約階段行列[3]にすることができる。被約階段行列は V の基底のとり方に依らず V のみによって定まるものであるから、これを V と考えることができる。例えば、$*$ を任意の $\mathbb{F}_q$ の元として、

$$\begin{pmatrix} 0 & 1 & * & 0 & * & * & 0 \\ 0 & 0 & 0 & 1 & * & * & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

は被約階段行列である。$*$ のある成分の上にある成分はすべて $*$ であることが分かる。したがって $*$ の数を ℓ とすれば、$*$ だけを抜き出して ℓ の分割が得られる。上の例では $\ell = 5$ で、分割は $(3, 2)$ である。このようにして得られる分割 $\lambda = (\lambda_1, \dots, \lambda_d)$ は、長さ d が k 以下で、角のある列がちょうど k 個あることから $\lambda_1 \leq n - k$ である。すなわち λ は $k \times (n - k)$ の箱に収まるものである。$*$ には $\mathbb{F}_q$ の任意の元を入れることができるので、同じ分割を定める部分空間は q^ℓ 個ある。

逆に $k \times (n - k)$ の箱に収まる任意の分割に対して、上記のような被約階段が得られることを見よう。式で書き表すのはやや面倒なので、例を確認して理解することとする。例えば $(n, k) = (6, 3)$ とすると $k \times (n - k) = 3 \times 3$ である。この箱に収まる分割として、例えば $(3, 3, 1)$ をとれば

$$\begin{pmatrix} 1 & 0 & * & * & 0 & * \\ 0 & 1 & * & * & 0 & * \\ 0 & 0 & 0 & 0 & 1 & * \end{pmatrix}$$

が条件をみたすものとなる。以上をまとめれば定理が成り立つことが分かる。 □

[3]階段行列であって、角のある列は角の成分だけが 1 で、その他の成分がすべて 0 であるもの。