完全1因子分解から誘導されるDudeney集合について

小林 みどり，喜安 善市

Dudeney sets induced from perfect 1-factorizations

Midori KOBAYASHI and Zen'iti KIYASU

Dedicated to Professor G. Nakamura on the occasion of his retirement.

ABSTRACT

A set of Hamilton cycles in the complete graph on n vertices is called a Dudeney set, if every path of length two lies on exactly one of the cycles. It has been conjectured that there is a Dudeney set for every complete graph, but it is still unsettled. Furthermore, little is known about the numder of non-isomorphic Dudeney sets.

In this paper, we construct non-isomorphic Dudeney sets using perfect 1-factorizations and determine the number of the Dudeney sets and the automorphism groups.

1. はしがき

ここで論じるDudeney集合は，円卓問題と呼ばれている一種の数学遊技または数学パズルに由来する．この数学パズルは，19世紀末，米国のC.H.Judson教授が提出した次の懸賞問題である[8, 11].

ある避暑地で7人の仲間が集まった．ここに滞在する日数は，次のようにすることで意見が一致した．毎日一回ずつ，7人で円卓を囲んで会食する．その際テーブルの席順は，各自の両隣りは，左右は無視して，組として毎回異なるようにする．こうして15日間滞在したという．この席順を示せ.

出題から5年後の1904年，米国のT.H.Saffordが懸賞問題の解を発表した[27]．1917年に英国のH.E.Dudeneyは，上記の問題を一般化し，円卓問題と名付けて，米国の文献を引用することなく発表した．そのため，この問題はDudeneyの名前で知られるようになった[4].

この円卓問題は，完全グラフ K_n において，任意の2-path(長さ2の道)をちょうど1回ずつ含むようなHamilton閉路の集合を求める問題と同値である．そのような性質をもつHamilton閉路の集合をDudeney集合と呼ぶ．このDudeney集合の問題は，本学部の中村義作教授が指摘し[25], F.K.Hwangらが研究した[9]一種のブロックデザインと見ることができる．この立場からは，Dudeney集合は，K_n の任意の2-pathをちょうど1回ずつ覆うHamilton閉路の集合として定義することができる.

この問題の応用分野としては，多重変成器，血清学などがある[23, 26].

Dudeney集合の問題は，中村教授が本格的に研究したが，その大きな業績の第1は，現在GK系列とGN(またはGA)系列と呼ばれている完全1因子分解によるDudeney集合の無限系列を発見したこと[21]．第2は，巡回列型Dudeney集合と呼ばれている偶数次のDudeney集合の無限系列を発見したこと[24]．第3は，著者ら(小林，喜安)を指導して，偶数次のDudeney

集合が必ず存在することを証明し，その構成法を明らかにしたこと[18]．第4は，著者の1人(喜安)と協同して，(素数+2)次のDudeney集合の無限系列を発見したことである[13]．

このように，偶数次のDudeney集合の存在も明らかになり，3次から7次までは，その個数 (同型ではないものの個数) $N(n)$ (nは次数) は

$$n=3,4,5,7 \text{のとき} N(n)=1$$
$$n=6 \text{のとき} N(n)=2$$

のように，明らかになっているが ($n=3,4,5$ のときは自明，$n=6,7$ のときは Safford が1904年しらみつぶし法で示した[27])，$n \geqq 8$ では，次数nを偶数に限定しても，

$$N(n) \geqq 1$$

ではあるが，$N(n)$が確定したものは1つもない．次数が増大すれば，$N(n)$も増大すると予想されているが，それらのDudeney集合の自己同型群についても全く研究されていない．

このような事情に鑑みて，この論文では，偶数次のDudeney集合，特に完全1因子分解から誘導されるDudeney集合に限定して，それらの個数と自己同型群とその位数を決定する．これは「部分Dudeney集合」，2つの部分Dudeney集合の「2-path同値」という概念，および置換群による軌道分解を導入することで可能となった。

$N(n)$が確定していない最小のnは，$n=8$である．この場合，$N(n)$の見当をつけるために，電子計算機によって調べたが，$N(n) \geqq 1719$ という予想外の結果を得た．$N(n)$を確定する仕事は，目下進行中である．完了した段階で別論文で報告する．

2. 予備的事項

$K_n=(V_n, E_n)$ を n 個の頂点をもつ完全グラフとする．ここで，V_n は K_n の頂点集合，E_n は 枝集合である．この論文を通して n は偶数であるとし，$n=m+1, r=(m-1)/2$ とおく．

K_n の1因子分解 $\mathcal{F}=\{G_0, G_1, \cdots, G_{m-1}\}$ は，任意の1因子 $G_i, G_j \in \mathcal{F}$ $(i \neq j)$ について $G_i \cup G_j$ が Hamilton 閉路であるとき，完全1因子分解(以後P1Fと略す)とよばれる．K_n において，任意の2-path (長さ2のpath) をちょうど1回ずつ含むようなHamilton閉路の集合をDudeney集合という．$\mathcal{F}=\{G_0, G_1, \cdots, G_{m-1}\}$ が K_n のP1Fのとき，

$$\mathcal{D}=\{G_i \cup G_j \mid 0 \leqq i < j \leqq m-1\}$$

は K_n の Dudeney集合となる．

すべての偶数 n について K_n にP1Fが存在することが予想されているが，まだ解決されていない．P1Fが存在することがわかっている n は，$n=p+1$ と $n=2p$ (p は素数) と若干個の n $(16, 28, 36, 40, 50, 3^5+1, 7^3+1, 11^3+1, 19^3+1, 23^3+1, 31^3+1, 5^3+1, 13^2+1, 3^6+1, 37^2+1, 43^2+1, 13^3+1, 5^5+1)$ のみである[3, 10, 16, 17, 19, 28, 29, 30]．$n=p+1$ についてはこの節で構成法を述べる．

V_n の対称群を S_n とおく．K_n の1因子分解 $\mathcal{F}$ の full symmetry 群 $\mathrm{FS}(\mathcal{F})$ と自己同型群 $\mathrm{Aut}(\mathcal{F})$ を次のように定義する:

$$\mathrm{FS}(\mathcal{F}) = \{\sigma \in S_n \mid \sigma(\mathcal{F}) = \mathcal{F}\}$$
$$\mathrm{Aut}(\mathcal{F}) = \{\sigma : \mathcal{F} \to \mathcal{F} \mid \sigma は V_n の置換から induce される\}.$$

$\mathrm{FS}(\mathcal{F})$ から $\mathrm{Aut}(\mathcal{F})$ への自然な準同型写像が存在するのでその核を Ker とかく:

$$\begin{aligned} Ker &= \{\sigma \in S_n \mid \sigma は \mathcal{F} \to \mathcal{F} の map として identity\ map である\} \\ &= \{\sigma \in S_n \mid \sigma(G) = G,\ G \in \mathcal{F}\}. \end{aligned}$$

定理 (Anderson) $n \neq 4$ とする．$\mathcal{F}$ が完全ならば $Ker = \{1\}$. したがって $\mathrm{FS}(\mathcal{F}) \cong \mathrm{Aut}(\mathcal{F})$.

証明 $\sigma \in S_n, \sigma \neq 1$ とする．任意の $G \in \mathcal{F}$ について，$\sigma(G) = G$ とする．

$V = \{1, 2, \cdots, n\}$ とおき，一般性を失うことなく $\sigma(1) = 2$ としてよい．$\mathcal{F}$ が1因子分解より，$\{1,2\} \in G$ となる $G \in \mathcal{F}$ が存在する．$\sigma(2) = a, a \neq 1, 2$ とすると，$\sigma(\{1,2\}) = \{2, a\}$ となり，$\sigma(G) = G$ に反する．よって $\sigma(2) = 1$ でなければならない．つまり σ は，いくつかの互換の積からなる置換である．σ が固定する点があったとする．たとえば $\sigma(3) = 3$ とする．$\{1,3\}$ を含む1因子 G について，$\sigma(\{1,3\}) = \{2,3\}$ となり $\sigma(G) = G$ に反する．よって σ は固定点をもたない．すなわち，σ は，$n/2$ 個の互換の積である．

次に $\sigma(3) = 4$ とおいても一般性を失わない．そのとき $\sigma(4) = 3$ である．$\{1,3\} \in G_1 \in \mathcal{F}$ とすると，$\sigma(\{1,3\}) = \{2,4\}$ より $\{2,4\} \in G_1$. また $\{1,4\} \in G_2 \in \mathcal{F}$ とすると，$\sigma(\{1,4\}) = \{2,3\}$ より $\{2,3\} \in G_2$. これは $G_1 \cup G_2$ が Hamilton 閉路であることに矛盾する．

よって，$Ker = \{1\}$ であることが示された． □

Anderson の定理により，以後 $\mathrm{Aut}(\mathcal{F}) = \{\sigma \in S_n \mid \sigma(\mathcal{F}) = \mathcal{F}\}$ として扱う．Dudeney 集合 $\mathcal{D}$ の自己同型群 $\mathrm{Aut}(\mathcal{D})$ についても同様に，$\mathrm{Aut}(\mathcal{D}) = \{\sigma \in S_n \mid \sigma(\mathcal{D}) = \mathcal{D}\}$ として扱う．

$m = p$ が奇素数のときは,

$$V_n = \{\infty\} \cup GF(p) = \{\infty\} \cup \{0, 1, 2, \cdots, p-1\}$$

とおき, 1因子 F_i $(0 \leq i \leq p-1)$ を

$$F_i = \{\{\infty, i\}\} \cup \{\{a, b\} \in E_n \mid a, b \neq \infty, a + b \equiv 2i \pmod{p}\}$$

と定義すると, K_n の P1F

$$\mathcal{F}_0 = \{F_i \mid 0 \leq i \leq p-1\}$$

が得られる．頂点の置換 $\sigma_a (a \neq 0)$, τ_a を

$$\sigma_a(y) = \begin{cases} ay & (y \in GF(p)) \\ \infty & (y = \infty) \end{cases}$$

$$\tau_a(y)=\begin{cases} y+a & (y\in GF(p)) \\ \infty & (y=\infty) \end{cases}$$

と定義し, $S=\{\sigma_a \mid 1\leq a\leq p-1\}, T=\{\tau_a \mid 0\leq a\leq p-1\}$ とおくと, よく知られているように, $p\geq 7$ のとき,

$$\mathrm{Aut}(\mathcal{F}_0)=ST \quad (\text{半直積})$$

である [2].

$\{1,2,3,\cdots,p-1\}$ の部分集合 K が, $K\cup(-K)=\{1,2,3,\cdots,p-1\}$, $|K|=(p-1)/2$ を満たすとき, K は mod p の half-set であるという.

3. I型Dudeney集合

K_n のP1F $\mathcal{F}=\{G_0,G_1,\cdots,G_{m-1}\}$ から作られる K_n の Dudeney集合

$$\mathcal{D}=\{G_i\cup G_j \mid 0\leqq i<j\leqq m-1\}$$

を次のように分解する:

$$\begin{aligned} \mathcal{D}_0 &= \{G_0\cup G_i \mid 1\leqq i\leqq m-1\} \\ \mathcal{D}_0^c &= \{G_i\cup G_j \mid 1\leqq i<j\leqq m-1\} \\ \mathcal{D} &= \mathcal{D}_0\cup\mathcal{D}_0^c. \end{aligned}$$

$R=\{\rho\in S_n \mid \rho G_0=G_0\}$ とおくと, R は G_0 を固定する頂点の置換全部の集合である. G_0 の枝は $r+1$ 本ある. それらの枝の入れ換えと向きの定め方で, G_0 を固定する置換が決まるから, $|R|=2^{r+1}(r+1)!$ である.

$\rho\in R$ について, $\mathcal{D}(\rho)$ を次のように定義する.

$$\mathcal{D}(\rho)=\rho\mathcal{D}_0\cup\mathcal{D}_0^c,$$

ここで

$$\begin{aligned} \rho\mathcal{D}_0 &= \rho\{G_0\cup G_1,\cdots,G_0\cup G_{m-1}\} \\ &= \{G_0\cup\rho G_1,\cdots,G_0\cup\rho G_{m-1}\}. \end{aligned}$$

定理3.1 $\rho\in R$のとき, $\mathcal{D}(\rho)$ は K_n のDudeney 集合である.

証明 $\mathcal{D}(\rho)$ の元はHamilton閉路であることは明らかであるので, $\mathcal{D}$ と $\mathcal{D}(\rho)$ に属する 2-path の集合が不変であることを示せばよい. $\mathcal{D}_0^c$ は共通なので, $\mathcal{D}_0$ と $\rho\mathcal{D}_0$ に属する2-path の集合が不変であることを示す.

$$\begin{aligned} G_0\cup(\cup_{i=1}^{m-1}G_i) &= E_n \\ G_0\cup(\cup_{i=1}^{m-1}\rho G_i) &= E_n \end{aligned}$$

であるから, $\cup_{i=1}^{m-1}G_i=\cup_{i=1}^{m-1}\rho G_i$ である. よって, 2-path の集合は不変である. □

$\mathcal{D}(\rho)$ を $\mathcal{F}$ から誘導されるI型Duneney集合とよぶ.

補題3.1 $\rho \in R$ とする. そのとき,

$$\{\rho G_1, \rho G_2, \cdots, \rho G_{m-1}\} = \{G_1, G_2, \cdots, G_{m-1}\} \Longleftrightarrow \rho \in R \cap \mathrm{Aut}(\mathcal{F})$$

証明 ($\Rightarrow$) $\rho(G_0) = G_0$ とあわせると, $\rho\{G_0, G_1, \cdots, G_{m-1}\} = \{G_0, G_1, \cdots, G_{m-1}\}$ となるので, $\rho \in \mathrm{Aut}(\mathcal{F})$ を得る. ($\Leftarrow$) 自明. □

定理3.2 $\rho \in R$ とする. 次は同値である.
(1) $\mathcal{D}(\rho) \cong \mathcal{D}$
(2) $\rho \in R \cap \mathrm{Aut}(\mathcal{F})$
(3) $\mathcal{D}(\rho) = \mathcal{D}$

証明 (1) $\Rightarrow$ (2) Hamilton閉路は2つの1因子から構成されている. $\mathcal{D}$ は $G_0, G_1, \cdots, G_{m-1}$ がそれぞれ $m-1$ 個ずつから構成されており, $\mathcal{D}(\rho)$ は G_0 が $m-1$ 個, $G_1, \cdots, G_{m-1}$ が $m-2$ 個ずつ, $\rho G_1, \cdots, \rho G_{m-1}$ が 1個ずつから構成されている(ただし全て異なるとは限らない).

$\mathcal{D}(\rho)$ と $\mathcal{D}$ が同型であるから, それらに属する1因子の種類と数は同じ型でなければならない. したがって, $\{\rho G_1, \rho G_2, \cdots, \rho G_{m-1}\} = \{G_1, G_2, \cdots, G_{m-1}\}$ である. 補題3.1 より $\rho \in R \cap \mathrm{Aut}(\mathcal{F})$ を得る.

(2)$\Rightarrow$(3) $\rho \in R \cap \mathrm{Aut}(\mathcal{F})$ のとき, 補題3.1 より $\{\rho G_1, \rho G_2, \cdots, \rho G_{m-1}\} = \{G_1, G_2, \cdots, G_{m-1}\}$ である.

$$\begin{aligned} \mathcal{D}(\rho) &= \rho\mathcal{D}_0 \cup \mathcal{D}_0^c = \{G_0 \cup \rho G_1, \cdots, G_0 \cup \rho G_{m-1}\} \cup \mathcal{D}_0^c \\ &= \mathcal{D}_0 \cup \mathcal{D}_0^c \\ &= \mathcal{D} \end{aligned}$$

(3)$\Rightarrow$(1) 自明. □

補題3.2
(1) $\sigma \in R \cap \mathrm{Aut}(\mathcal{F})$, $\rho \in R$ について, $\sigma\mathcal{D}(\rho) = \mathcal{D}(\sigma\rho)$.
(2) $\rho, \rho' \in R$ について, $\mathcal{D}(\rho) = \mathcal{D}(\rho') \Longleftrightarrow \rho^{-1}\rho' \in R \cap \mathrm{Aut}(\mathcal{F})$

証明 (1) $\sigma\mathcal{D}(\rho) = \sigma(\rho\mathcal{D}_0 \cup \mathcal{D}_0^c) = \sigma\rho\mathcal{D}_0 \cup \sigma\mathcal{D}_0^c$ であるが, σ は $\{G_1, \cdots, G_{m-1}\}$ を $\{G_1, \cdots, G_{m-1}\}$ に移すから, $\sigma\mathcal{D}(\rho) = \sigma\rho\mathcal{D}_0 \cup \mathcal{D}_0^c = \mathcal{D}(\sigma\rho)$ である.

(2) ($\Rightarrow$) $\mathcal{D}(\rho) = \rho\mathcal{D}_0 \cup \mathcal{D}_0^c$, $\mathcal{D}(\rho') = \rho'\mathcal{D}_0 \cup \mathcal{D}_0^c$ であるから, $\rho\mathcal{D}_0 = \rho'\mathcal{D}_0$ である. したがって, $\mathcal{D}_0 = \rho^{-1}\rho'\mathcal{D}_0$.

$$\mathcal{D}(\rho^{-1}\rho') = \rho^{-1}\rho'\mathcal{D}_0 \cup \mathcal{D}_0^c = \mathcal{D}_0 \cup \mathcal{D}_0^c = \mathcal{D}$$

と定理3.2 より $\rho^{-1}\rho' \in R \cap \mathrm{Aut}(\mathcal{F})$ を得る.

($\Leftarrow$) 仮定より $\rho^{-1}\rho' = \sigma \in R \cap \mathrm{Aut}(\mathcal{F})$ とかける.

$$\begin{aligned} \mathcal{D}(\rho') &= \rho'\mathcal{D}_0 \cup \mathcal{D}_0^c = \rho\sigma\mathcal{D}_0 \cup \mathcal{D}_0^c = \rho\mathcal{D}_0 \cup \mathcal{D}_0^c \\ &= \mathcal{D}(\rho). \quad \square \end{aligned}$$

定理3.3　$\rho, \rho' \in R$ のとき，$\mathcal{D}(\rho) \cong \mathcal{D}(\rho') \Longleftrightarrow \rho' = \sigma'\rho\sigma$ となる $\sigma, \sigma' \in R \cap \mathrm{Aut}(\mathcal{F})$ が存在する．

証明 ($\Leftarrow$) $\rho' = \sigma'\rho\sigma$ より

$$\begin{aligned}\mathcal{D}(\rho') &= \rho'\mathcal{D}_0 \cup \mathcal{D}_0^c = \sigma'\rho\sigma\mathcal{D}_0 \cup \mathcal{D}_0^c \\ &= \sigma'\rho\mathcal{D}_0 \cup \mathcal{D}_0^c = \sigma'\rho\mathcal{D}_0 \cup \sigma'\mathcal{D}_0^c \\ &= \sigma'(\rho\mathcal{D}_0 \cup \mathcal{D}_0^c) \\ &= \sigma'\mathcal{D}(\rho)\end{aligned}$$

$\sigma' \in S_n$ であるから，$\mathcal{D}(\rho') \cong \mathcal{D}(\rho)$ である．

($\Rightarrow$) $f : \mathcal{D}(\rho) \to \mathcal{D}(\rho'), f \in S_n$ とすると，f は $\{G_0, G_1, \cdots, G_{m-1}\}$ を $\{G_0, G_1, \cdots, G_{m-1}\}$ に移すので，$f \in \mathrm{Aut}(\mathcal{F})$ である．

$f \in R$ であることを以下示す．$\rho G_i \neq G_0$ $(1 \leqq i \leqq m-1)$ であるから，$\{\rho G_1, \ldots, \rho G_{m-1}\} = \{G_1, \ldots, G_{m-1}\}$ の場合と，ある i について，$\rho G_i \neq G_j$ $(1 \leqq j \leqq m-1)$ の場合にわけて考える．

最初の場合は 補題3.1 より $\rho \in R$ である．2番目の場合は，ρG_i は，$\mathcal{D}(\rho)$ に1つだけ属しているから，f で移った先の $\mathcal{D}(\rho')$ でも $f(\rho G_i)$ は1つだけ属する1因子である．つまり，ある j について $f(\rho G_i) = \rho' G_j$ である．$f(G_0 \cup \rho G_i) = G_0 \cup \rho' G_j$ より，$f(G_0) = G_0$ となり，$f \in R$ が示された．

以上より $f \in R \cap \mathrm{Aut}(\mathcal{F})$. よって $f(\mathcal{D}_0^c) = \mathcal{D}_0^c$ であるから

$$\begin{aligned}f(\mathcal{D}(\rho)) &= f(\rho\mathcal{D}_0 \cup \mathcal{D}_0^c) = f\rho\mathcal{D}_0 \cup f\mathcal{D}_0^c \\ &= f\rho\mathcal{D}_0 \cup \mathcal{D}_0^c = \mathcal{D}(f\rho)\end{aligned}$$

すなわち $\mathcal{D}(\rho') = \mathcal{D}(f\rho)$ である．

補題3.2 (2) より $(f\rho)^{-1}\rho' \in R \cap \mathrm{Aut}(\mathcal{F})$ であるので $(f\rho)^{-1}\rho' = \sigma$ とかける ($\sigma \in R \cap \mathrm{Aut}(\mathcal{F})$). 故に $\rho' = f\rho\sigma$ ($f, \sigma \in R \cap \mathrm{Aut}(\mathcal{F})$) である．　□

次に，$\mathcal{D}(\rho)$ の自己同型群を考える．

定理3.4　$\rho \in R$ とする．$\mathrm{Aut}(\mathcal{D}(\rho)) = \{\sigma \in R \cap \mathrm{Aut}(\mathcal{F}) \mid \sigma = \rho\sigma'\rho^{-1}$ となる $\sigma' \in R \cap \mathrm{Aut}(\mathcal{F})$ が存在する.$\}$

証明　$f \in \mathrm{Aut}(\mathcal{D}(\rho))$ とする．定理3.3 の証明において $\rho' = \rho$ とおくと，$f \in R \cap \mathrm{Aut}(\mathcal{F})$ がいえる．よって，$f\rho \in R$ である．$f(\mathcal{D}(\rho)) = \mathcal{D}(\rho)$ より，

$$\begin{aligned}\mathcal{D}(\rho) &= f(\rho\mathcal{D}_0 \cup \mathcal{D}_0^c) = f\rho\mathcal{D}_0 \cup f\mathcal{D}_0^c \\ &= f\rho\mathcal{D}_0 \cup \mathcal{D}_0^c = \mathcal{D}(f\rho).\end{aligned}$$

補題3.2 (2) より $\rho^{-1}(f\rho) \in R \cap \mathrm{Aut}(\mathcal{F})$, すなわち $\rho^{-1}f\rho \in R \cap \mathrm{Aut}(\mathcal{F})$ が示された．

逆に，$\sigma \in R \cap \mathrm{Aut}(\mathcal{F})$, $\sigma = \rho\sigma'\rho^{-1}$ となる$\sigma' \in R \cap \mathrm{Aut}(\mathcal{F})$ があるとする．

$$\begin{aligned}\sigma(\mathcal{D}(\rho)) &= \sigma(\rho\mathcal{D}_0 \cup \mathcal{D}_0^c) = \sigma\rho\mathcal{D}_0 \cup \sigma\mathcal{D}_0^c \\ &= \sigma\rho\mathcal{D}_0 \cup \mathcal{D}_0^c = (\rho\sigma'\rho^{-1})\rho\mathcal{D}_0 \cup \mathcal{D}_0^c \\ &= \rho\sigma'\mathcal{D}_0 \cup \mathcal{D}_0^c = \rho\mathcal{D}_0 \cup \mathcal{D}_0^c \\ &= \mathcal{D}(\rho).\end{aligned}$$

故に $\sigma \in \mathrm{Aut}(\mathcal{D}(\rho))$ である． □

系3.1 $\mathcal{F}$ が K_n の asymmetric P1F, すなわち，$\mathrm{Aut}(\mathcal{F}) = \{1\}$ のとき，
(1) $\rho, \rho' \in R$ について，$\mathcal{D}(\rho) \cong \mathcal{D}(\rho') \Longleftrightarrow \rho' = \rho$
したがって，$\mathcal{F}$ に関するI型Dudeney集合の個数$= |R| = 2^{r+1}(r+1)!$ である．
(2) $\rho \in R$ について，$\mathrm{Aut}(\mathcal{D}(\rho)) = \{1\}$.

K_{12} に asymmetric P1F が 1 個存在することが知られているので[1]，この P1F に関するI型 Dudeney 集合の個数は$2^6 6! = 46080$ である．

4. I型Dudeney集合の個数

$m = p$ を奇素数(≥ 7)とする．$\mathcal{F}_0 = \{F_0, F_1, \cdots, F_{p-1}\}$ を第2節で定義した K_{p+1} のP1Fとし，$\mathcal{D}$ を $\mathcal{F}_0$ からつくられるDudeney集合とする．すなわち，$\mathcal{D} = \{F_i \cup F_j \mid F_i, F_j \in \mathcal{F}_0, F_i \neq F_j\}$ とする．$R = \{\rho \in S_n \mid \rho F_0 = F_0\}$ とおく．

この節では、$\mathcal{F}_0$ から誘導されるI型Dudeney集合の個数を求める。

$\mathrm{Aut}(\mathcal{F}_0) = ST$ (半直積) であるから，$R \cap \mathrm{Aut}(\mathcal{F}_0) = S = \{\sigma_a | 1 \leqq a \leqq p-1\}$ となる．したがって定理3.3, 3.4 は次のようになる．

系4.1 K_{p+1} の $\mathcal{F}_0$ から誘導されるI型Dudeney集合 $\mathcal{D}(\rho), \mathcal{D}(\rho')$ について
(1) $\mathcal{D}(\rho) \cong \mathcal{D}(\rho') \Longleftrightarrow \rho' = \sigma_b\rho\sigma_a$ $(1 \leqq a, b \leqq p-1)$.
(2) $\mathrm{Aut}(\mathcal{D}(\rho)) = \{\sigma_a \in S \mid \sigma_a = \rho\sigma_b\rho^{-1}$となる$\sigma_b \in S$が存在する.$\}$

R に作用 $f_{b,a}$ を次のように定義する．

$$\begin{aligned} f_{b,a}: \quad R &\to R \\ \rho &\to \sigma_b\rho\sigma_a \end{aligned}$$

$G = \{f_{b,a} \mid 1 \leqq a, b \leqq p-1\}$ とおくと，G は R に作用する群である．

$\mathcal{F}_0$ から誘導されるI型Dudeney集合の個数を求めることは，R の元でG 同値でないものの個数を求めることと同じである．それは，R の G軌道の個数と同じである．

Lemma (Burnside)

$$R \text{ の } G\text{軌道の個数} = \frac{1}{|G|}\sum_{f \in G} |F_f|$$

ここで $|F_f|$ は f で固定される R の元の個数である．

以下，各 $f_{b,a}(1 \leq a, b \leq p-1)$ について，$|F_f|$ を求めていく．

(i)$f = f_{1,a}$ または $f_{b,1}$ のとき．

$f_{1,a}(\rho) = \rho$ ならば $\sigma_1 \rho \sigma_a = \rho$ つまり $\rho\sigma_a = \rho$．両辺に左から ρ^{-1} をかけると，$\sigma_a = 1$．よって $a = 1$．$f_{b,1}(\rho) = \rho$ ならば$\sigma_b \rho \sigma_1 = \rho$ つまり $\sigma_b \rho = \rho$．両辺に右から ρ^{-1} をかけると，$\sigma_b = 1$，よって $b = 1$．故に，$f_{1,1}$ のときだけ固定元が存在しうる．

任意の $\rho \in R$ に対して，$f_{1,1}(\rho) = \sigma_1 \rho \sigma_1 = \rho$．よって，$f_{1,1}$ が固定する R の元の個数は $|F_{f_{1,1}}| = |R| = 2^{r+1}(r+1)!$ である．

(ii)$f = f_{-1,a}$ または $f_{b,-1}$ のとき．

$f_{-1,a}(\rho) = \rho$ ならば$\sigma_{-1} \rho \sigma_a = \rho$．このとき ρ は，$\rho(\infty) = \infty, 0$ でなければならない．

補題4.1　$\rho \in R$, $\rho(\infty) = \infty, 0$ のとき，$\sigma_{-1}\rho = \rho\sigma_{-1}$．

(証明略)

補題4.1 より，$\rho\sigma_a = \sigma_{-1}\rho$ から $\rho\sigma_a = \rho\sigma_{-1}$ を得る．左から ρ^{-1} をかけて，$\sigma_a = \sigma_{-1}$．よって$a = -1$.

また $f_{b,-1}(\rho) = \rho$ ならば$\sigma_b \rho \sigma_{-1} = \rho$．この ρ は $\rho(\infty) = \infty, 0$．再び 補題4.1 より，$\sigma_b\rho = \rho\sigma_{-1}$ から $\sigma_b\rho = \sigma_{-1}\rho$ を得る．右から ρ^{-1} をかけて，$\sigma_b = \sigma_{-1}$．よって$b = -1$．故に，$f_{-1,-1}$ のときだけ固定元が存在しうるので，$f_{-1,-1}(\rho) = \rho$ となる ρ の個数を調べる．

$\sigma_{-1}\rho\sigma_{-1} = \rho$, $\rho(\infty) = \infty, 0$ であるから，補題4.1 より$\rho\sigma_{-1}\sigma_{-1} = \rho$ すなわち$\rho = \rho$ となり，これは自明な式である．よって，$\rho(\infty) = \infty, 0$ であれば $f_{-1,-1}(\rho) = \rho$ を満たす．

$\rho(\infty) = \infty, 0$ である $\rho \in R$ の個数を求める．$1, 2, \cdots, r$ の行き先を決めれば，$r+1, \cdots, 2r$ の行き先は決まる．$1, 2, \cdots, r$ の行き先は，$2^r r!$ 通りあり，さらに ∞ の行き先は$\infty, 0$ の 2 通りあるから，$f_{-1,-1}$ が固定する元の個数は $|F_{f_{-1,-1}}| = 2^{r+1} r!$ である．

(iii) $f_{b,a}$ $(a, b \neq 1, -1)$ のとき．

$GF(p)$ の元を原始根 ω の累乗の形で表す:

$$GF(p)^* = \{\omega^0, \omega^1, \omega^2, \cdots, \omega^r, \omega^{r+1}, \omega^{r+2}, \cdots, \omega^{2r-1}\}.$$

$f_{b,a}$ を $f_{\omega^j, \omega^i}(1 \leqq i, j \leqq 2r-1,\ i, j \neq r)$ とかく．

ρ が $f_{b,a}$ で固定されるとすると，(ii) と同じ理由により，$\rho(\infty) = \infty, 0$でなければならない．よって

$$\rho = \begin{pmatrix} \infty & \omega^0 & \omega^1 & \omega^2 & \cdots & \omega^{r-1} \\ * & \omega^{a_0} & \omega^{a_1} & \omega^{a_2} & \cdots & \omega^{a_{r-1}} \end{pmatrix}$$

とかく (ここで $* = \infty, 0$)．ρ は F_0 を固定する置換なので，$\{\omega^{a_0}, \omega^{a_1}, \cdots, \omega^{a_{r-1}}\}$ は half-set mod p でなければならない．

$1 \leqq i, j \leqq 2r-1$,　$i, j \neq r$ なる i, j について，$f_{\omega^j, \omega^i}(\rho) = \rho$ つまり $\sigma_{\omega^j} \rho \sigma_{\omega^i} = \rho$ となる ρ の個数を求めたい．次の補題は半分の i だけ，つまり $1 \leqq i \leqq r-1$ なる i だけ調べればよいことを示している．

補題4.2 $i' \equiv i+r \pmod{2r}$, $j' \equiv j+r \pmod{2r}$ のとき

$$f_{\omega^{j'},\omega^{i'}}(\rho) = \rho \Longleftrightarrow f_{\omega^j,\omega^i}(\rho) = \rho$$

証明

$$\omega^{j'} = \omega^{j+r} = -\omega^j$$
$$\omega^{i'} = \omega^{i+r} = -\omega^i$$

より

$$\begin{aligned} \sigma_{\omega^{j'}}\rho\sigma_{\omega^{i'}} &= \sigma_{-1}\sigma_{\omega^j}\rho\sigma_{-1}\sigma_{\omega^i} \\ &= \sigma_{\omega^j}\rho\sigma_{\omega^i} \quad (\text{補題4.1より}) \end{aligned}$$

よって

$$\sigma_{\omega^{j'}}\rho\sigma_{\omega^{i'}} = \rho \Longleftrightarrow \sigma_{\omega^j}\rho\sigma_{\omega^i} = \rho \quad \square$$

補題4.2 より $1 \leqq i \leqq r-1$ としてよいので下のように書ける.

$(\infty,\ \omega^0,\ \omega^1,\ \omega^2,\ \cdots,\ \omega^{r-1})$
$\xrightarrow{\sigma_{\omega^i}} (\infty,\ \omega^i,\ \omega^{i+1},\ \omega^{i+2},\ \cdots,\ \omega^{r-1},\ -\omega^{a_0},\ -\omega^{a_1},\ \cdots,\ -\omega^{i-1})$
$\xrightarrow{\rho} (*,\ \omega^{a_i},\ \omega^{a_{i+1}},\ \omega^{a_{i+2}},\ \cdots,\ \omega^{a_{r-1}},-\omega^{a_0},\ -\omega^{a_1},\ \cdots,\ -\omega^{a_{i-1}})$
$\xrightarrow{\sigma_{\omega^j}} (*,\ \omega^j\omega^{a_i},\ \omega^j\omega^{a_{i+1}},\ \omega^j\omega^{a_{i+2}},\ \cdots,\ \omega^j\omega^{a_{r-1}},\ -\omega^j\omega^{a_0},\ -\omega^j\omega^{a_1},\ \cdots,\ -\omega^j\omega^{a_{i-1}})$.

$\sigma_{\omega^j}\rho\sigma_{\omega^i} = \rho$ より,

$$\begin{cases} \omega^{a_0} = \omega^j\omega^{a_i} \\ \omega^{a_1} = \omega^j\omega^{a_{i+1}} \\ \omega^{a_2} = \omega^j\omega^{a_{i+2}} \\ \vdots \\ \omega^{a_{r-1-i}} = \omega^j\omega^{a_{r-1}} \\ \omega^{a_{r-i}} = -\omega^j\omega^{a_0} \\ \omega^{a_{r-i+1}} = -\omega^j\omega^{a_1} \\ \vdots \\ \omega^{a_{r-1}} = -\omega^j\omega^{a_{i-1}} \end{cases} \qquad \cdots\cdots\cdots (4.1)$$

この等式の右辺にあらわれる $-$ (マイナス) の数は i 個である.

補題4.3

(1) r は自然数とする. $1,3,5,7,\cdots,2r-1$ のうち, r と互いに素なものの個数は $\varphi(2r)$ である.

(2) r は奇数とする. $0,2,4,6,8,\cdots,2r-2$ のうち, r と互いに素なものの個数は $\varphi(r)$ である.

(証明略)

$1 \leq i \leq r-1$ なる i について $(r,i)=d$, $r=dl$ とおく．(4.1) 式を上から順に，大きさ d の l 個の block に分けておく．−(マイナス) がつく block の個数は i/d であるので，i/d の偶奇により場合わけをする．

(a) i/d が奇数のとき

(4.1) 式より，$\omega^{a_0}=-(\omega^j)^l\omega^{a_0}$, よって $\omega^{jl}=-1$, すなわち，$(\omega^r)^{j/d}=-1$. 故に j/d は奇数となり $j=d,3d,5d,\cdots,(2l-1)d$ である．これらの j は，$(\omega^j)^l=-1$ となり，ω^j は l 乗して -1 となる．l 乗する前に -1 になってしまうと，$\omega^{a_0},\omega^{a_1},\cdots$, が half-set となれないので，$\omega^j$ は l 乗してはじめて -1 となる．

$$
\begin{aligned}
&l\text{乗してはじめて}-1\text{となる}j\text{の個数}\\
&=1,3,5,\cdots,2l-1\text{のうち},l\text{と互いに素なものの個数}\\
&=\varphi(2l)\quad(\text{補題4.3 (1) より})
\end{aligned}
$$

(b) i/d が偶数のとき

このとき，i は r より偶数度が高い．よって，l は奇数である．(4.1) 式より $\omega^{a_0}=(\omega^j)^l\omega^{a_0}$ であるから $\omega^{jl}=1$, すなわち $(\omega^r)^{j/d}=1$. 故に j/d は偶数となり $j=0,2d,4d,\cdots,2(l-1)d$ である．これらの j は，$(\omega^j)^l=1$ となり，ω^j は l 乗して 1 となる．l 乗する前に 1 になってしまうと，half-set であることに矛盾するので，ω^j は l 乗してはじめて 1 となる．

$$
\begin{aligned}
&l\text{乗してはじめて}1\text{となる}j\text{の個数}\\
&=0,2,4,\cdots,2(l-1)\text{のうち},l\text{と互いに素なものの個数}\\
&=\varphi(l)\quad(\text{補題4.3 (2) より})\\
&=\varphi(2l)
\end{aligned}
$$

(a),(b) いずれの場合も，j の個数は $\varphi(2l)$ である．

各 j について，ρ が何個あるかを考える．a_0 の決め方は $2r$ 通りあり，a_0 を決めると，$l-1$ 個の a_i が決まる．それ以外の a_i について，決め方は $2(r-l)$ 通りあり，1つを決めると，$l-1$ 個の a_i が決まる．これを繰り返すことにより，$a_0,a_1,a_2,\cdots,a_{r-1}$ が決まる．結局，$a_0,a_1,a_2,\cdots,a_{r-1}$ の決め方は，

$$2^d r(r-l)(r-2l)\cdots(r-(d-1)l)\text{通り}$$

である．

∞ の行き先は ∞ と 0 の 2通りであるから，各 j について，固定される ρ の個数は，

$$|F_{f_{\omega^j,\omega^i}}|=2^{d+1}r(r-l)(r-2l)\cdots(r-(d-1)l)$$

である．

各 i について j は $\varphi(2l)$ 個あるから，各 i について，固定される ρ の総数は，

$$2^{d+1}r(r-l)(r-2l)\cdots(r-(d-1)l)\varphi(2l)$$

である．故に次の定理を得る．

定理4.1 K_n の $\mathcal{F}_0$ に関するI型Dudeney集合の個数を $N_{\mathrm{I}}(n)$ とおくと

$$N_{\mathrm{I}}(n) = \{2^{r+1}(r+1)! + 2^{r+1}r! + 2\sum_{i=1}^{r-1} 2^{d_i+1}r(r-l_i)(r-2l_i)\cdots(r-(d_i-1)l_i)\varphi(2l_i)\}/4r^2$$
$$= \{2^{r-1}(r+2)(r-1)! + \sum_{i=1}^{r-1} 2^{d_i}(r-l_i)(r-2l_i)\cdots(r-(d_i-1)l_i)\varphi(2l_i)\}/r$$

ここで，$n = p+1, r = (p-1)/2, d_i = (r,i), r = d_i l_i$ である．特にrが奇素数のときは，

$$\begin{aligned} N_{\mathrm{I}}(r) &= \{2^{r-1}(r+2)(r-1)! + \sum_{i=1}^{r-1} 2\varphi(r)\}/r \\ &= \{2^{r-1}(r+2)(r-1)! + 2(r-1)^2\}/r \end{aligned}$$

である．

例 $N_{\mathrm{I}}(8) = 16$, $N_{\mathrm{I}}(12) = 544$, $N_{\mathrm{I}}(18) = 806616$, $N_{\mathrm{I}}(20) = 12615752$, $N_{\mathrm{I}}(24) = 4391507800$, $N_{\mathrm{I}}(32) = 1618773006107264$,

5. II型Dudeney集合

p は素数で $p \equiv 3 \pmod 4$ かつ $<2>$ の $GF(p)^*$ における指数が 2 であるとする．

命題5.1 $<2> = \{1, 2, 4, 8, \cdots,\} \subset GF(p)^*$ は mod p の half-set である．

証明 2 の $GF(p)^*$ における位数が $(p-1)/2$ であることから，2 は $GF(p)^*$ において平方剰余である．$p \equiv 3 \pmod 4$ という仮定から -1 は平方剰余ではない．よって，-1 は $<2>$ には含まれない．

$a, b \in <2>$ $(a \neq b)$ について，もし $a+b \equiv 0 \pmod p$ とすると $a \equiv -b \pmod p$ であり $-1 \in <2>$ となり矛盾する．従って，$|<2>| = (p-1)/2$ であることを考えると，$<2>$ は mod p の half-set である． □

$<2> = \{1, 2, 4, \cdots\}$ が half-set であることから，

$$F_0 \cup F_1, F_0 \cup F_2, F_0 \cup F_4, \cdots$$

を回転させることにより，Dudeney集合が得られる．すなわち

$$\begin{aligned} \mathcal{D} = \{&F_0 \cup F_1, && F_0 \cup F_2, && F_0 \cup F_4, && \cdots \\ &F_1 \cup F_2, && F_1 \cup F_3, && F_1 \cup F_5, && \cdots \\ &F_2 \cup F_3, && F_2 \cup F_4, && F_2 \cup F_6, && \cdots \\ &\vdots && \vdots && \vdots && \\ &F_{p-1} \cup F_0, && F_{p-1} \cup F_1, && F_{p-1} \cup F_2, && \cdots\} \end{aligned}$$

はDudeney集合である．

ここで

$$\begin{aligned}\mathcal{B}_0 &= \{F_0 \cup F_i \mid i \in <2>\}\\ \mathcal{B}_1 &= \tau_1\mathcal{B}_0\\ \mathcal{B}_2 &= \tau_2\mathcal{B}_0\\ &\vdots\\ \mathcal{B}_{p-1} &= \tau_{p-1}\mathcal{B}_0\end{aligned}$$

とおくと，

$$\mathcal{D} = \mathcal{B}_0 \cup \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_{p-1}$$

とかける．

頂点の置換 $\rho_{\infty 0}$ を次のように定義する．

$$\rho_{\infty 0} = (\infty\ 0)$$

命題5.2　$\rho_{\infty 0}(F_1 \cup F_2 \cup F_4 \cup \cdots) = F_1 \cup F_2 \cup F_4 \cdots$

証明

$$\begin{aligned}&F_1 \ni \{\infty, 1\}, \{0, 2\}\\ &F_2 \ni \{\infty, 2\}, \{0, 4\}\\ &F_4 \ni \{\infty, 4\}, \{0, 8\}\\ &F_8 \ni \{\infty, 8\}, \{0, 16\}\\ &\vdots\end{aligned}$$

より明らか．一般に，$F_i \ni \{\infty, i\}, \{0, 2i\}$ であり，$\{0, i\} \in F_{\frac{i}{2}}, \{\infty, 2i\} \in F_{2i}$ よりいえる．ただし F の suffix は，mod p で考える．　□

命題5.3　$\rho_{\infty 0}\{F_0 \cup F_1, F_0 \cup F_2, F_0 \cup F_4, \cdots\}$ に含まれる 2-path の集合と，$\{F_0 \cup F_1, F_0 \cup F_2, F_0 \cup F_4 \cdots\}$ に含まれる 2-path の集合は等しい．

証明　命題5.2 と $\rho_{\infty 0}F_0 = F_0$ より明らか．　□

従って，$\mathcal{D}(0) = \rho_{\infty 0}\mathcal{B}_0 \cup \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_{p-1}$ は Dudeney 集合である．

$\mathcal{B}_0$ だけでなく，他の $\mathcal{B}_i$ を変換しても Dudeney 集合が得られる．次にそれを説明する．頂点の置換を$\rho_{\infty 0} = (\infty\ 0)$, $\rho_{\infty 1} = (\infty\ 1)$, $\rho_{\infty 2} = (\infty\ 2)$, $\cdots$, 一般に $\rho_{\infty i} = (\infty\ i)$ とおく $(0 \le i \le p-1)$.

命題5.4　$\rho_{\infty i}\mathcal{B}_i = \tau_i(\rho_{\infty 0}\mathcal{B}_0)$

証明　自明．　□

$\mathcal{D}=\mathcal{B}_0\cup\mathcal{B}_1\cup\mathcal{B}_2\cup\cdots\cup\mathcal{B}_{p-1}$ であるが，そのうちの $\mathcal{B}_{i_1},\mathcal{B}_{i_2},\cdots,\mathcal{B}_{i_t}$ だけを変換したものを，$\mathcal{D}(\{i_1,i_2,\cdots,i_t\})$ とかく．たとえば，

$$\mathcal{D}(\{0,1\})=\rho_{\infty 0}\mathcal{B}_0\cup\rho_{\infty 1}\mathcal{B}_1\cup\mathcal{B}_2\cup\cdots\cup\mathcal{B}_{p-1}$$
$$\mathcal{D}(\{1,2,3\})=\mathcal{B}_0\cup\rho_{\infty 1}\mathcal{B}_1\cup\rho_{\infty 2}\mathcal{B}_2\cup\rho_{\infty 3}\mathcal{B}_3\cup\mathcal{B}_4\cup\cdots\cup\mathcal{B}_{p-1}$$

などである．

定理5.1 $\mathcal{D}(\{i_1,i_2,\cdots,i_t\})$ はDudeney集合である．

証明 各 i について，$\mathcal{B}_i$ に含まれる2-pathの集合と，$\rho_{\infty i}\mathcal{B}_i$ に含まれる2-pathの集合は等しいことよりいえる．(Hamilton閉路であることは変わらない.) □

このようにして 2^p 個のDudeney集合が得られる．これを，II型Dudeney集合とよぶこととする．これらの中には同型なものもあるので，次にその問題を考える．

補題5.1
(1) $\tau_a(\rho_{\infty i}F_k)=\rho_{\infty(i+a)}F_{k+a}$
(2) $\sigma_a(\rho_{\infty i}F_k)=\rho_{\infty(ai)}F_{ak}$
(3) $\tau_a(\rho_{\infty i}\mathcal{B}_i)=\rho_{\infty(i+a)}\mathcal{B}_{i+a}$
(4) $\sigma_a(\rho_{\infty i}\mathcal{B}_i)=\rho_{\infty(ai)}\mathcal{B}_{ai}\quad(a\in<2>)$

証明 (1),(2) は明らか．(3),(4) は (1),(2) より得られる．(σ_a は a 倍写像であるので $a=0$ は除く.) □

定理5.2
(1) $\tau_a\mathcal{D}(\{i_1,i_2,\cdots,i_t\})=\mathcal{D}(\{i_1+a,i_2+a,\cdots,i_t+a\})$
(2) $\sigma_a\mathcal{D}(\{i_1,i_2,\cdots,i_t\})=\mathcal{D}(\{ai_1,ai_2,\cdots,ai_t\})\quad(a\in<2>)$

証明 (1) 補題5.1 (3) より明らか．
(2) 補題5.1 (4) より明らか．ただし (1),(2) とも $\mathcal{B}$ のsuffixとρ の2nd suffixは mod p で考える． □

系5.1
(1) $\mathcal{D}(\{i_1,i_2,\cdots,i_t\})\cong\mathcal{D}(\{i_1+a,i_2+a,\cdots,i_t+a\})$
(2) $\mathcal{D}(\{i_1,i_2,\cdots,i_t\})\cong\mathcal{D}(\{ai_1,ai_2,\cdots,ai_t\})\quad(a\in<2>)$

補題5.2
(1) $i\neq j$ のとき，$\rho_{\infty i}F_j$ はどれかの F_k と一致することはない．つまり，任意の k に対して
$\rho_{\infty i}F_j\neq F_k\ (i\neq j)$
(2) $\rho_{\infty i}F_j$ は全て異なる．つまり，$\rho_{\infty i}F_j=\rho_{\infty i'}F_{j'}\Longleftrightarrow i=i',j=j'$

証明 (1) p の仮定より $p\geqq 7$ であるから，K_{p+1} の1因子のedgeは4本以上である．$i\neq j$ よ

り $\rho_{\infty i}F_j$ は F_j の edge のうち，2本だけ変えて残りのedge は変えていない．よって，F_k という1因子であることはありえない．

(2) $\rho_{\infty i}F_j = \rho_{\infty i'}F_{j'}$ とする．$\{\infty, j\}, \{i, 2j-i\} \in F_j$ より $\{\infty, 2j-i\}, \{i, j\} \in \rho_{\infty i}F_j$．また $\{\infty, j'\}, \{i', 2j'-i'\} \in F_{j'}$ より $\{\infty, 2j'-i'\}, \{i', j'\} \in \rho_{\infty i'}F_{j'}$．よって $2j-i = 2j'-i' \pmod p$, すなわち

$$2(j-j') = i-i' \qquad \cdots\cdots\cdots\cdots\cdots (5.1)$$

(i) $\{i, j\} = \{i', j'\}$ のとき
$i = i', j = j'$ または $i = j', j = i'$ である．後者のときは，(5.1)式に代入すると $3(j-j') = 0$．$p \neq 3$ より $j = j', i = i'$ を得る．

(ii) $\{i, j\} \in F_{j'}, \{i', j'\} \in F_j$, すなわち, $i+j = 2j', i'+j' = 2j$ のとき
$(i+j)-(i'+j') = 2j'-2j$ であり (5.1)式より $(i+j)-(i'+j') = i'-i$．よって $j-j' = 2(i'-i)$．再び(5.1)式より $2(j-j') = 4(i'-i) = i-i'$．$p \neq 5$ より $i = i'$, $j = j'$ を得る．　□

補題5.3

$$\mathcal{D}(\{i_1, \cdots, i_t\}) = \mathcal{D}(\{j_1, \cdots, j_u\}) \Longleftrightarrow \{i_1, \cdots, i_t\} = \{j_1, \cdots, j_u\}$$

証明 (⇐) 自明. (⇒) $\mathcal{D}(\{i_1, \cdots, i_t\})$ には1因子として

$$\begin{cases} \rho_{\infty i_1}F_{i_1+1},\ \rho_{\infty i_1}F_{i_1+2},\ \rho_{\infty i_1}F_{i_1+4}, \cdots \\ \vdots \\ \rho_{\infty i_t}F_{i_t+1},\ \rho_{\infty i_t}F_{i_t+2},\ \rho_{\infty i_t}F_{i_t+4}, \cdots \end{cases}$$

が属している．$\mathcal{D}(\{j_1, \cdots, j_u\})$ には1因子として

$$\begin{cases} \rho_{\infty j_1}F_{j_1+1},\ \rho_{\infty j_1}F_{j_1+2},\ \rho_{\infty j_1}F_{j_1+4}, \cdots \\ \vdots \\ \rho_{\infty j_u}F_{j_u+1},\ \rho_{\infty j_u}F_{j_u+2},\ \rho_{\infty j_u}F_{j_u+4}, \cdots \end{cases}$$

が属している．補題5.2 (1),(2) より

$$\{i_1, \cdots, i_t\} = \{j_1, \cdots, j_u\}$$

を得る．　□

定理5.3 $S_0 = <2> (\subset S)$, $H = S_0T (\subset \mathrm{Aut}(\mathcal{F}_0))$ とおく．

$\mathcal{D}(\{i_1, \cdots, i_t\}) \cong \mathcal{D}(\{j_1, \cdots, j_u\}) \Longleftrightarrow \{f(i_1), \cdots, f(i_t)\} = \{j_1, \cdots, j_u\}$ となる $f \in H$ が存在する．

証明 (⇐)

$$\begin{aligned} f(\mathcal{D}(\{i_1, \cdots, i_t\})) &= \mathcal{D}(\{f(i_1), \cdots, f(i_t)\}) \ (\text{定理5.2より}) \\ &= \mathcal{D}(\{j_1, \cdots, j_u\}) \ (\text{仮定より}) \end{aligned}$$

従って，同型が示される．

($\Rightarrow$) $\mathcal{D}(\{i_1,\cdots,i_t\})$ には，$F_0,F_1,\cdots,F_{p-1}$ はそれぞれ $(p-1)/2$ 個以上属する．$\rho_{\infty i}F_j$ の形の1因子は全て異なるから，これらは1個ずつ属する．$\mathcal{D}(\{j_1,\cdots,j_u\})$ についても同様である．

補題5.2からまず $t=u$ が分かる．$\{i_1,\cdots,i_t\}=\phi$(空集合)のときと，$\{i_1,\cdots,i_t\}=\{0,1,\cdots,p-1\}$(全体)のときに主張が成り立つことは明らか(たとえば fは恒等置換ととれる)であるから，$1\leq t\leq p-1$ と仮定する．

2つのDudeney集合が同型であることから，頂点の置換 f が存在する．上記のことより，f は$F_0,F_1,\cdots,F_{p-1}$ を$F_0,F_1,\cdots,F_{p-1}$ に移す．したがって，$f\in \mathrm{Aut}(\mathcal{F}_0)$ である．

$f\in H$ ならば，$f(\mathcal{D}(\{i_1,\cdots,i_t\}))=\mathcal{D}(\{j_1,\cdots,j_u\})$ と $f(\mathcal{D}(\{i_1,\cdots,i_t\}))=\mathcal{D}(\{f(i_1),\cdots,f(i_t)\})$ より $\mathcal{D}(\{f(i_1),\cdots,f(i_t)\})=\mathcal{D}(\{j_1,\cdots,j_u\})$ を得る．補題5.3より

$$\{f(i_1),\cdots,f(i_t)\}=\{j_1,\cdots,j_u\}$$

を得る．

$f\notin H$ として矛盾を導く．$f=\sigma_{-1}h$, $h\in H$ と書ける．系5.1より $h\mathcal{D}(\{i_1,\cdots,i_t\})=\mathcal{D}(\{h(i_1),\cdots,h(i_t)\})$ となるから $h(i_1)=i'_1,\cdots,h(i_t)=i'_t$ と書くと，

$$\sigma_{-1}\mathcal{D}(\{i'_1,\cdots,i'_t\})=\mathcal{D}(\{j_1,\cdots,j_t\})$$

を得る．$\mathcal{D}(\{i'_1,\cdots,i'_t\})$ の中には，$\rho_{\infty i}\mathcal{B}_i$ の形のものは t 個含まれており，各 $\rho_{\infty i}\mathcal{B}_i$ の中に $\rho_{\infty i}F_k$ の形の1因子は1個ずつしか含まれていない．F_i の形のものは少なくとも $(p-1)/2$ 個ずつ含まれている．したがって，

$$\sigma_{-1}\{F_{i'}\cup\rho_{\infty i'}F_{1+i'},\ F_{i'}\cup\rho_{\infty i'}F_{2+i'},\ \ F_{i'}\cup\rho_{\infty i'}F_{4+i'},\cdots\}$$
$$=\{F_j\cup\rho_{\infty j}F_{1+j},\ F_j\cup\rho_{\infty j}F_{2+j},\ F_j\cup\rho_{\infty j}F_{4+j},\cdots\}$$

の形の等式が成り立つ．よって $\sigma_{-1}F_{i'}=F_j$，つまり $i'=-j$ となる．故に，

$$\{\rho_{\infty j}F_{-1+j},\rho_{\infty j}F_{-2+j},\rho_{\infty j}F_{-4+j},\cdots\}=\{\rho_{\infty j}F_{1+j},\rho_{\infty j}F_{2+j},\rho_{\infty j}F_{4+j},\cdots\}$$

となる．頂点の変換 $(\infty\ j)$ を施した後，τ_{-j} で移すと

$$\{F_{-1},F_{-2},F_{-4},\cdots\}=\{F_1,F_2,F_4,\cdots\}$$

とならねばならないが，これは矛盾である．　□

系5.2 $\mathcal{D}(\{i_1,\cdots,i_t\})\cong\mathcal{D}(\{j_1,\cdots,j_u\})\Longrightarrow t=u$

系5.3

$$\{0,1,\cdots,p-1\}=I_1\cup I_2=J_1\cup J_2\ \ \text{(disjoint union)}$$

のとき，

$$\mathcal{D}(I_2)\cong\mathcal{D}(J_2)\Longleftrightarrow\mathcal{D}(I_1)\cong\mathcal{D}(J_1)$$

証明 ($\Rightarrow$) 定理5.3より $f(I_2)=J_2$ となる $f\in H$ が存在する．f は $GF(p)$ の1対1写像なので，$f(I_1)=J_1$ でもある．再び定理5.3より $\mathcal{D}(I_1)\cong\mathcal{D}(J_1)$ を得る．　□

定理5.4

$$\mathrm{Aut}(\mathcal{D}(\{i_1,i_2,\cdots,i_t\}))\cong H_{\{i_1,i_2,\cdots,i_t\}}$$

ここで H_s は，S を集合として固定する H の部分群，すなわち $H_s=\{f\in H\mid f(S)=S\}$ である．

証明

$$\begin{aligned}\mathrm{Aut}(\mathcal{D}(\{i_1,\cdots,i_t\})) &= \{f:\mathcal{D}(\{i_1,\cdots,i_t\})\to\mathcal{D}(\{i_1,\cdots,i_t\}),\text{同型写像}\}\\ &= \{f\in H\mid f(\{i_1,\cdots,i_t\})=\{i_1,\cdots,i_t\}\}\quad(\text{定理5.3より})\\ &= H_{\{i_1,\cdots,i_t\}}\quad\square\end{aligned}$$

系5.4　$\{0,1,2,\cdots,p-1\}=I_1\cup I_2$ (disjoint union) とする．そのとき，

$$\mathrm{Aut}(\mathcal{D}(I_1))\cong\mathrm{Aut}(\mathcal{D}(I_2)).$$

証明　定理5.4より，$\mathrm{Aut}(\mathcal{D}(I_1))=H_{I_1}$，$\mathrm{Aut}(\mathcal{D}(I_2))=H_{I_2}$ である．ところが，$H_{I_1}=H_{I_2}$ であることより系が示される．　□

例　$p=7$ のとき，$2^7=128$ 個のII型Dudeney集合の中で同型でないものは次の12個である．( )内は，自己同型群の位数である．

$\mathcal{D}=\mathcal{D}(\phi)$ (42),	$\mathcal{D}(0)$ (3),	$\mathcal{D}(0,1)$ (1),
$\mathcal{D}(0,1,2)$ (1),	$\mathcal{D}(0,1,3)$ (3),	$\mathcal{D}(0,1,5)$ (3),
$\mathcal{D}(0,1,2,3)$ (1),	$\mathcal{D}(0,1,2,4)$ (3),	$\mathcal{D}(0,1,2,5)$ (3),
$\mathcal{D}(0,1,2,3,4)$ (1),	$\mathcal{D}(0,1,2,3,4,5)$ (3),	$\mathcal{D}(0,1,2,3,4,5,6)$ (21).

6. II型Dudeney集合の個数

前節同様 p は素数で，$p\equiv 3\pmod 4$ かつ $<2>$ の $GF(p)^*$ における指数が 2 であるとする．

$N=\{0,1,\cdots,p-1\}$ とおく．N の部分集合 I に対してDudeney集合 $D(I)$ が定義される．そのとき，定理5.3より，$I,I'\subset N$ について

$$\mathcal{D}(I)\cong\mathcal{D}(I')\Longleftrightarrow^{\exists} f\in H,\ f(I)=I'$$

である．

$$\Omega=\{(a_0,a_1,\cdots,a_{p-1})\mid a_i=0,1\ (0\le i\le p-1)\}$$

とおく．$I \subset N$ を Ω の元で表現することとし，これもまた I とかく．たとえば，$\{0,1,2\}$ は $(1110\cdots0)$, $\{1,2,4\}$ は $(11010\cdots0)$, ϕ は $(0\cdots\cdots)$ などである．H は N に作用しているが，Ω にも作用している．N への作用は普通の作用であり，Ω への作用は座標への作用である．たとえば，$\tau_1(1110\cdots0)=(01110\cdots0)$, $\sigma_2(1110\cdots0)=(101010\cdots0)$, $\sigma_2(0110\cdots0)=(001010\cdots0)$ などである．すると，$I, I' \in \Omega$ についても

$$\mathcal{D}(I) \cong \mathcal{D}(I') \Longleftrightarrow^{\exists} f \in H, f(I) = I'$$

が成り立つ．

H は N に作用しているが，その作用の構造を調べる．

$GF(p)$ の原始元を ω とする．$\sigma=\sigma_\omega$ とおくと，$S=\{1,\sigma,\sigma^2,\cdots,\sigma^{p-2}\}, T=\{1,\tau_1,\tau_2,\cdots,\tau_{p-1}\}$, $\mathrm{Aut}(\mathcal{F}_0)=ST$ (半直積) である。$\mathrm{Aut}(\mathcal{F}_0)$ の各元の cycle 構造(cycle の積に分解したときの cycle の長さと個数)を求める．

まず1は，$1=(0)(1)\cdots(p-1)$ とcycle の積に分解されるから，1は，長さ1のcycle が p 個からなる．次に τ_1 は，$\tau_1=(012\cdots p-1)$ となり，長さ p の cycle が1個からなる．τ_j についても同様である．

補題6.1 $\sigma^i \neq 1$ のとき，$\tau_j\sigma^i$ と σ^i のcycle 構造は同じであり，それは

$$\underbrace{(\ )}_{1}\underbrace{(\quad)}_{t}\underbrace{(\quad)}_{t}\cdots\underbrace{(\quad)}_{t}$$

である(ここで t は σ^i の位数, cycle の個数は，$1+(p-1)/t$ である)．

証明 $\sigma^i=\sigma_a$ とする．仮定より $a \neq 1$. すると，

$$\tau_j\sigma_a : x \longrightarrow ax+j$$

である．

$\tau_j\sigma_a$ で固定される元を $x \in N$ とすると，$x=ax+j$ より $x=j/(1-a)$ である．故に固定される元は1個であることがわかった．

$x \in N, x \neq j/(1-a)$ について，$\tau_j\sigma_a$ を繰り返し作用させると

$$\begin{aligned} &x \longrightarrow ax+j \longrightarrow a^2x+aj+j \longrightarrow a^3x+a^2j+aj+j \\ &\longrightarrow a^4x+a^3j+a^2j+aj+j \longrightarrow \cdots \\ &\longrightarrow a^sx+(a^{s-1}+a^{s-2}+\cdots+a+1)j \longrightarrow \cdots \end{aligned}$$

となる．σ_a の $\mathrm{Aut}(\mathcal{F}_0)$ における位数を t とおくと，$s=t$ のとき，

$$a^sx+(a^{s-1}+a^{s-2}+\cdots+a+1)j = x+0 = x.$$

$s<t$ のときは，$a^sx+(a^{s-1}+a^{s-2}+\cdots+a+1)j=x$ とおくと，

$$\begin{aligned} (1-a^s)x &= (a^{s-1}+\cdots+a+1)j \\ x &= (a^{s-1}+\cdots+a+1)j/(1-a^s) \\ x &= j/(1-a) \end{aligned}$$

となり矛盾する．よって，上の cycle の長さは t である．　□

II型Dudeney集合の同値類の個数を求めることは，Ω の元で H 同値でないものの個数を求めることと同じである．

各 $g \in H$ について，g により固定される Ω の元の個数を求める．1 については，固定元は，$|\Omega| = 2^p$ 個ある．τ_j については，固定元は $(0\cdots0)$ と $(1\cdots1)$ の 2 個である．

$\tau_j\sigma^i (i \neq 0)$ については，σ^i の位数を t とおくと，その cycle 構造は，補題6.1より，$1+(p-1)/t$ 個の cycle からなる．したがって $\tau_j\sigma^i (i \neq 0)$ が固定する Ω の元の個数は，$2^{1+(p-1)/t}$ である．

$\{1, \sigma_2, \sigma_3, \cdots, \sigma_{p-1}\}$ のうち位数 t のものは，$\varphi(t)$ 個ある．また，$\sigma \in <2>$ であることと，σ の位数が r の約数であることは同値である．よって Burnside の Lemma より次の定理を得る．

定理6.1　K_n のII型Dudeney集合の個数を $N_{\mathrm{II}}(n)$ とおくと

$$\begin{aligned} N_{\mathrm{II}}(n) &= \tfrac{1}{|H|}\{2^p + 2(p-1) + p\textstyle\sum_{\substack{t|r \\ 1<t\leq r}} \varphi(t)2^{1+(p-1)/t}\} \\ &= \tfrac{4}{(p-1)p}\{2^{p-1} + (p-1) + p\textstyle\sum_{\substack{t|r \\ 1<t\leq r}} \varphi(t)2^{(p-1)/t}\} \end{aligned}$$

例　$N_{\mathrm{II}}(8) = 12$, $N_{\mathrm{II}}(24) = 33164$.

7. あとがき

本論文では，P1Fから誘導されるDudeney集合のうち，I型とII型，およびその個数について論じた．これによって，次数の増大につれて，Dudeney集合は急激に多様化することが明らかになった．しかし次の二つは，紙幅の事情と論旨の錯雑化とを考慮して割愛した．

1. I型とII型の概念をそれぞれ拡張すること．

2. これを総合して"P1Fから誘導されるDudeney集合" の概念を展開すること．

これらについては，すっきりした形に纏めることができれば発表したいと考えている．本論文で述べた研究の種は，長年にわたる中村教授との共同研究の土壌に発芽した．これを中村教授退官記念論文として寄稿することは，著者らの光栄とするところである．また本論文の寄稿に際しては，査読を担当された林田侃，大駒誠一の両教授より有益なご指摘とご教示とを受けた．記して両教授ならびに中村教授に深謝の意を表する次第である．

参考文献

[1] B.A.Anderson, Some perfect 1-factorizations, *Proc. 7th S-E Conf. Combinatorics, Graph Theory and Computing*, Utilitas Math., Winnipeg (1976) 79-91.

[2] B.A.Anderson, Symmetry groups of some perfect 1-factorizations of complete graphs, *Discrete Math.* **18** (1977) 227-234.

[3] J.H.Dinits and D.R.Stinson, Some new perfect one-factorizations from starters in finite fields, *J. Graph Theory* **13** (1989) 405-415.

[4] H.E.Dudeney, Amusements in Mathematics, Thomas Nelson and Sons, London, 1917, Dover Reprint, New York, 1970.

[5] H.E.Dudeney, The Canterbury Puzzles, Thomas Nelson and Sons, London, 1919, Dover Reprint, New York, 1958.

[6] K.Heinrich, M.Kobayashi and G.Nakamura, Dudeney's Round Table Problem, *Annals of Discrete Math.* **92** (1991) 107-125.

[7] K.Heinrich, M.Kobayashi and G.Nakamura, A Solution of Dudeney's Round Table Problem for p^eq^f+1, *Ars Combinatoria* (in press).

[8] K.Heinrich and G.Nonay, Exact Coverings of 2-paths by 4-cycles, *J. Combinatorial Theory* (*A*) **45** (1987) 50-61.

[9] F.K.Hwang and S.Lin, Neighbor Designs, *J. Combinatorial Theory* (*A*) **23** (1977) 302-313.

[10] E.Ihrig, E.Seah and D.R.Stinson, A Perfect One-factorization of K_{50}, *J. Comb. Math. Comb. Comput.* **1** (1987) 217-219.

[11] C.H.Judson, Problems for Solution (Algebra), *Amer. Math. Monthly* **6** (1899) 92.

[12] C.H.Judson, Solutions of Problems (Algebra), *Amer. Math. Monthly* **7** (1900) 72-73.

[13] Kiyasu-Z. and G.Nakamura, 円卓問題の部分解ふたつ, 別冊数理科学 (1979) 83-89.

[14] M.Kobayashi, Perfect one-factorizations of the complete graph, *Annual Review of Economics*, Nagasaki University **4** (1988) 85-90.

[15] M.Kobayashi, On Perfect One-Factorization of the Complete Graph K_{2p}, *Graphs and Combinatorics* **5** (1989) 351-353.

[16] M.Kobayashi, H.Awoki, Y.Nakazaki and G.Nakamura, A perfect one-factorization of K_{36}, *Graphs and Combinatorics* **5** (1989) 243-244.

[17] M.Kobayashi and Kiyasu-Z., Perfect one-factorizations of K_{1332} and K_{6860}, *J. Combinatorial Theory* (A) **51** (1989) 314-315.

[18] M.Kobayashi, Kiyasu-Z. and G.Nakamura, A solution of Dudeney's round table problem for an even number of people, *J. Combinatorial Theory* (A) **62** (1993), 26-42.

[19] M.Kobayashi, Kiyasu-Z. and G.Nakamura, New perfect one-factorizations of complete graphs, *Administration and Informatics, University of Shizuoka* **3** (1991) 33-38.

[20] E.Mendelsohn and A Rosa, One-factorizations of the complete graph — A survey, *J. Graph Theory* **9** (1985) 43-65.

[21] G.Nakamura, デュードニーの円卓問題と完全グラフの色分け, 数学セミナー **159** (1975) 24-29.

[22] G.Nakamura, いろいろの円卓問題, 別冊数理科学 (1976) 65-69.

[23] G.Nakamura and M.Hosoda, 多重変成器への組み合わせ数学の応用, 信州大学工学部紀要 **41** (1976) 77-81.

[24] G.Nakamura, Kiyasu-Z. and N.Ikeno, Solution of the round table problem for the case of $p^k + 1$ persons, *Commentarii Mathematici Universitatis Santi Pauli* **29** (1980) 7-20.

[25] G.Nakamura and M.Tanaka, 円卓問題のコンピュータによる解法, 数理解析研究所講究録 **371** 実験整数論 (1979) 47-64.

[26] D.H.Rees, Some designs of use in serology, *Biometrics* **23** (1967) 779-791.

[27] F.H.Safford, Solutions of problems, *American Mathematical Monthly* **11** (1904) 169-170.

[28] E.Seah, Perfect one-factorizations of the complete graph — A survey, *Bulletin of the ICA* 1 (1991) 59-70.

[29] E.Seah and D.R.Stinson, A Perfect One-Factorization of K_{36}, *Discrete Math.* **70** (1988) 199-202.

[30] E.Seah and D.R.Stinson, A perfect one-factorization of K_{40}, *Congressus Numerantium* **68** (1989) 211-214.

※ 本論文の査読者は大駒誠一（慶応義塾大学），林田侃（お茶の水女子大学）の両氏である．（順不同）