Lemma 1 $n \geq 2$, $2 \leq k \leq n$ とする. このとき, 等式

$$\sum_{\ell \in {}_n\mathbb{C}_k} \sum_{1 \le \alpha < \beta \le k} 2^{i_\alpha + i_\beta} = {}_{n-2}C_{k-2} \sum_{1 \le r < s \le n} 2^{r+s} \qquad (*)$$

が成り立つ. ここで, ${}_n\mathbb{C}_k$ は $\{1, \dots, n\}$ から成る昇順 k タプル全体の集合

(例. ${}_6\mathbb{C}_4 = \{(1234), (1235), (1236), (1245), (1246), (1256), (1345),$

$(1346), (1356), (1456), (2345), (2346), (2356), (2456), (3456)\}$) である.

i_α は ℓ の第 α 成分

proof $n=6$, $k=4$ を例に考える

左辺を展開すると

$$
\begin{aligned}
(\text{左辺}) = \; & 2^{1+2} + 2^{1+3} + 2^{1+4} + 2^{2+3} + 2^{2+4} + 2^{3+4} && \leftarrow (1234) \\
& + 2^{1+2} + 2^{1+3} + 2^{1+5} + 2^{2+3} + 2^{2+5} + 2^{3+5} && \leftarrow (1235) \\
& + 2^{1+2} + 2^{1+3} + 2^{1+6} + 2^{2+3} + 2^{2+6} + 2^{3+6} && \leftarrow (1236) \\
& + 2^{1+2} + 2^{1+4} + 2^{1+5} + 2^{2+4} + 2^{2+5} + 2^{4+5} && \leftarrow (1245) \\
& + 2^{1+2} + 2^{1+4} + 2^{1+6} + 2^{2+4} + 2^{2+6} + 2^{4+6} && \leftarrow (1246) \\
& + 2^{1+2} + 2^{1+5} + 2^{1+6} + 2^{2+5} + 2^{2+6} + 2^{5+6} && \leftarrow (1256) \\
& + 2^{1+3} + 2^{1+4} + 2^{1+5} + 2^{3+4} + 2^{3+5} + 2^{4+5} && \leftarrow (1345) \\
& + 2^{1+3} + 2^{1+4} + 2^{1+6} + 2^{3+4} + 2^{3+6} + 2^{4+6} && \leftarrow (1346) \\
& + 2^{1+3} + 2^{1+5} + 2^{1+6} + 2^{3+5} + 2^{3+6} + 2^{5+6} && \leftarrow (1356) \\
& + 2^{1+4} + 2^{1+5} + 2^{1+6} + 2^{4+5} + 2^{4+6} + 2^{5+6} && \leftarrow (1456) \\
& + 2^{2+3} + 2^{2+4} + 2^{2+5} + 2^{3+4} + 2^{3+5} + 2^{4+5} && \leftarrow (2345) \\
& + 2^{2+3} + 2^{2+4} + 2^{2+6} + 2^{3+4} + 2^{3+6} + 2^{4+6} && \leftarrow (2346) \\
& + 2^{2+3} + 2^{2+5} + 2^{2+6} + 2^{3+5} + 2^{3+6} + 2^{5+6} && \leftarrow (2356) \\
& + 2^{2+4} + 2^{2+5} + 2^{2+6} + 2^{4+5} + 2^{4+6} + 2^{5+6} && \leftarrow (2456) \\
& + 2^{3+4} + 2^{3+5} + 2^{3+6} + 2^{4+5} + 2^{4+6} + 2^{5+6} && \leftarrow (3456)
\end{aligned}
$$

となる.

続く

次に，前掲の展開式において，"2^{r+s}" $(1 \leq r < s \leq n)$ という項が何回現れるか考える．例として，"2^{3+5}" が何回現れるか考える．すると，$\ell = (\boxed{1}\boxed{2}35), (\boxed{1}3\boxed{4}5), (\boxed{1}35\boxed{6}), (\boxed{2}3\boxed{4}5), (\boxed{2}35\boxed{6}), (3\boxed{4}5\boxed{6})$ の時に各1回現れ，計6回であることがわかる．この"6"という数は，$\{1,2,4,6\}$ $(=\{1,2,3,4,5,6\} \setminus \{3,5\})$ から $2\ (=4-2)$ 個の数を選ぶ組合せの数 ${}_{6-2}C_{4-2}$ である．一般の n, k に関しても，$\{1,2,\ldots,n\} \setminus \{r,s\}$ という $n-2$ 個の数から $k-2$ 個の数を選ぶ組合せの数 ${}_{n-2}C_{k-2}$ 回だけ "2^{r+s}" が現れることがわかる．したがって

$$(\text{左辺}) = {}_{n-2}C_{k-2} \sum_{1 \leq r < s \leq n} 2^{r+s}$$

が成り立ち，Lemma が示せた． $\boxtimes$

> $\boxed{\text{Cor.2}}$ $n \geq 2$, $2 \leq k \leq n$ とする．このとき，等式
>
> $$\sum_{\ell \in {}_n\mathbb{C}_k} \sum_{1 \leq \alpha < \beta \leq k} 2^{i_\alpha + i_\beta - 2} = \frac{k(k-1)}{n(n-1)} {}_nC_k \sum_{1 \leq r < s \leq n} 2^{r+s-2}$$
>
> が成り立つ．

<u>proof</u> 前の Lemma の等式の両辺を4で割ればよい．更に

$$ {}_{n-2}C_{k-2} = \frac{(n-2)!}{(k-2)!\,((n-2)-(k-2))!} = \frac{(n-2)!}{(k-2)!\,(n-k)!}$$

$$= \frac{k(k-1)}{n(n-1)} \cdot \frac{n!}{k!\,(n-k)!} = \frac{k(k-1)}{n(n-1)} {}_nC_k$$

であることにも注意． $\boxtimes$

Lemma 3 $n \geqq 2$ とする．次の等式が成り立つ：

$$\sum_{1 \leqq r < s \leqq n} 2^{r+s-2} = \frac{4^n - 3\cdot 2^n + 2}{3}.$$

proof $\left(\sum_{a=1}^{n} 2^{a-1}\right)^2$ を，2通りの方法で計算する．

方法1 $\left(\sum_{a=1}^{n} 2^{a-1}\right)^2 = \left(2^{1-1} + 2^{2-1} + 2^{3-1} + \cdots + 2^{n-1}\right)^2$

$$\begin{aligned}
&= (2^{1-1})^2 + (2^{2-1})^2 + (2^{3-1})^2 + \cdots + (2^{n-1})^2 \\
&\quad + 2\cdot\Big[2^{1-1}\cdot 2^{2-1} + 2^{1-1}\cdot 2^{3-1} + \cdots + 2^{1-1}\cdot 2^{n-1} \\
&\qquad\qquad + 2^{2-1}\cdot 2^{3-1} + \cdots + 2^{2-1}\cdot 2^{n-1} \\
&\qquad\qquad + \cdots \\
&\qquad\qquad + 2^{n-2}\cdot 2^{n-1}\Big]
\end{aligned}$$

「$(A+B+C)^2 = A^2+B^2+C^2+2(AB+AC+BC)$」の一般化

$$\begin{aligned}
&= \left[4^0 + 4^1 + 4^2 + \cdots + 4^{n-1}\right] \\
&\quad + 2\Big[2^{1+2-2} + 2^{1+3-2} + \cdots + 2^{1+n-2} \\
&\qquad\qquad + 2^{2+3-2} + \cdots + 2^{2+n-2} \\
&\qquad\qquad + \cdots \\
&\qquad\qquad + 2^{(n-1)+n-2}\Big]
\end{aligned}$$

等比数列の和

$$= \frac{1\cdot(4^n - 1)}{4-1} + 2\cdot \sum_{1 \leqq r < s \leqq n} 2^{r+s-2}$$

$$= \frac{4^n - 1}{3} + 2\cdot \sum_{1 \leqq r < s \leqq n} 2^{r+s-2} \quad \cdots ①$$

方法2 $\left(\sum_{a=1}^{n} 2^{a-1}\right)^2 = \left(2^0 + 2^1 + \cdots + 2^{n-1}\right)^2$

$$= \left(\frac{1\cdot(2^n-1)}{2-1}\right)^2$$

$$= (2^n-1)^2 = 4^n - 2\cdot 2^n + 1 \quad \cdots ②$$

①と②は等しいので,

$$\sum_{1\leq r<s\leq n} 2^{r+s-2} = \left(4^n - 2\cdot 2^n + 1 - \frac{4^n-1}{3}\right) / 2$$

$$= \frac{2\cdot 4^n - 6\cdot 2^n + 4}{3} / 2$$

$$= \frac{4^n - 3\cdot 2^n + 2}{3}$$

☒

Thm. 4 $n \geqq 2$, $k \leqq n$ とする. このとき, n bit 中 k bit 立つ二進数の二乗和 $S_{n,k}$ は下式で与えられる:

$$S_{n,k} = \frac{4^n-1}{3}\cdot\frac{k}{n}\cdot {}_nC_k + \frac{2}{3}(4^n - 3\cdot 2^n + 2)\cdot\frac{k(k-1)}{n(n-1)}\, {}_nC_k \quad ☆$$

proof

case1 $k=0$ の時 $S_{n,0} = 0$ なので自明に☆が成立.

case2 $k=1$ の時.

$$S_{n,1} = (2^0)^2 + (2^1)^2 + \cdots + (2^{n-1})^2$$

$$= 4^0 + 4^1 + \cdots + 4^{n-1}$$

$$= \frac{1\cdot(4^n-1)}{4-1}$$

$$= \frac{4^n-1}{3}\cdot\frac{1}{n}\cdot {}_nC_1$$

なので $k=1$ でも☆が成立.

↓ 続く

case3 $k \geqq 2$ の時.

$$S_{n,k} = \sum_{\underbrace{\ell \in {}_n\mathbb{C}_k}} \left(\sum_{\gamma=1}^{k} 2^{i_\gamma - 1} \right)^2$$

↑Lemma1参照

$$= \sum_{\ell \in {}_n\mathbb{C}_k} \left(2^{i_1-1} + 2^{i_2-1} + \cdots + 2^{i_k-1} \right)^2$$

$$= \sum_{\ell \in {}_n\mathbb{C}_k} \Big[\left(4^{i_1-1} + 4^{i_2-1} + \cdots + 4^{i_k-1} \right) + 2\big(2^{i_1-1}2^{i_2-1} + 2^{i_1-1}2^{i_3-1} + \cdots + 2^{i_1-1}2^{i_k-1} + 2^{i_2-1}2^{i_3-1} + \cdots + 2^{i_2-1}2^{i_k-1} + \cdots + 2^{i_{k-1}-1}2^{i_k-1} \big) \Big]$$

$\boxed{\begin{array}{l} \text{「}(A+B+C)^2 \\ = A^2+B^2+C^2 \\ \quad +2(AB+AC+BC)\text{」} \\ \text{の一般化} \end{array}}$

$$= \sum_{\ell \in {}_n\mathbb{C}_k} \left[\left(\sum_{\alpha=1}^{k} 4^{i_\alpha - 1} \right) + 2 \left(\sum_{1 \leqq \alpha < \beta \leqq k} 2^{i_\alpha + i_\beta - 2} \right) \right]$$

$$= \underbrace{\left[\sum_{\ell \in {}_n\mathbb{C}_k} \sum_{\alpha=1}^{k} 4^{i_\alpha - 1} \right]}_{①} + 2 \underbrace{\left[\sum_{\ell \in {}_n\mathbb{C}_k} \sum_{1 \leqq \alpha < \beta \leqq k} 2^{i_\alpha + i_\beta - 2} \right]}_{②}$$

となる.

② については, Cor. 2 および Lemma 3 が使えて

$$② = \frac{k(k-1)}{n(n-1)} \cdot {}_nC_k \cdot \frac{4^n - 3 \cdot 2^n + 2}{3} \quad \cdots \text{(※※)}$$

となる

↓ 続く.

① について，① =「n bit 中 k bit が 1，残りは 0 であるような 四進数の総和」である．すると別紙1と同様の理屈で

$$① = \left({}_nC_k \times k \div n\right) \times \left(4^0 + 4^1 + \cdots + 4^{n-1}\right)$$

$$= {}_nC_k \cdot \frac{k}{n} \cdot \frac{1\cdot(4^n-1)}{4-1} = \frac{4^n-1}{3} \cdot \frac{k}{n} \cdot {}_nC_k \quad ☆☆☆$$

となる．☆☆ と ☆☆☆ を合せて，

$$S_{n,k} = \frac{4^n-1}{3} \cdot \frac{k}{n} \cdot {}_nC_k + 2 \cdot \frac{k(k-1)}{n(n-1)} \cdot {}_nC_k \cdot \frac{4^n - 3\cdot 2^n + 2}{3}$$

$$= \frac{4^n-1}{3} \cdot \frac{k}{n}\, {}_nC_k + \frac{2}{3}\left(4^n - 3\cdot 2^n + 2\right) \cdot \frac{k(k-1)}{n(n-1)}\, {}_nC_k$$

となる．よって $k \geqq 2$ に対しても ☆ が成立． $\boxtimes$

$\boxed{\text{Rmk. 5}}$ $n=1$ に対しても Thm. 4 は成り立つ．実際，$n=1$，$k=0,1$ に対して ☆ の右辺を計算すると，$n=1$，$k=0$ に対しては 0，$n=1$，$k=1$ に対しては 1 となり，これは $S_{1,0}=0$，$S_{1,1}=1$ であることに符合する //