

5 人の管理者の場合の (k, n) しきい値法と 整数計画法による秘密分散法

日大生産工(院) ○新聞 祐太郎 日大生産工 柄窪孝也

1 まえがき

情報化社会において、盗難対策と紛失対策の両方を実現する情報の安全な保管の手段である秘密分散法は、重要な技術の一つだと言える。1979年にShamir[1]とBlakleyは、 (k, n) しきい値法とよばれる秘密分散法をそれぞれ発表した。しかし、 (k, n) しきい値法ではごく一部のアクセス構造しか実現できない。そこで、 (k, n) しきい値法のシェアを n 人の管理者に複数配布することで秘密分散法を構成する複数割り当て法は、一般アクセス構造をもつ秘密分散法を容易に構成することが可能である。また、岩本ら[2]は、2003年に (k, n) しきい値法と整数計画法による一般アクセス構造を実現する秘密分散法の構成法を提案している。しかしながら、その効率の評価は不十分である。

一方、JacksonとMartin[3]は、管理者が5人の場合におけるすべての管理者グループ180通りの情報比を評価している。そこで、本研究では、5人の管理者の場合の180通りのアクセス構造に岩本らの手法を適用し、その効率を評価する。

2 秘密分散法

(k, n) しきい値法とは、秘密情報を n 個に分割し、それぞれのシェアを n 人の管理者で管理する手法である。秘密情報を復元する際には、任意の管理者 k 人の持つシェアを使うことで秘密情報の復元が可能である。一方、 $k-1$ 個のシェアを用いても秘密に関する情報は得られない。 n 人の管理者の中で、秘密情報を復元可能な権限を持つ集合をアクセス集合という。

また、 n 人の管理者集合 $P = \{P_1, \dots, P_n\}$ の部分集合のうち、秘密情報を復号できる集合の族を $\mathcal{A}_1$ 、秘密情報に関する情報が全く得られない集合の族を $\mathcal{A}_0$ とすると、 (k, n) しきい値法の $\mathcal{A}_1$ 、と $\mathcal{A}_0$ は以下のように表せる。

$$\mathcal{A}_1 = \{A: k \leq |A| \leq n\}$$

$$\mathcal{A}_0 = \{A: 0 \leq |A| \leq k-1\}$$

ここで、 $\mathcal{A}_1$ の極小集合族、 $\mathcal{A}_0$ の極大集合族は以下のように定義できる。

$$\mathcal{A}_1^- = \{A \in \mathcal{A}_1: A - \{P\} \notin \mathcal{A}_1 \text{ for any } P \in A\}$$

$$\mathcal{A}_0^+ = \{A \in \mathcal{A}_0: A \cup \{P\} \notin \mathcal{A}_0 \text{ for any } P \in P - A\}$$

また、非アクセス集合に属する管理者のシェアから、秘密に関する情報が全く得られない手法を完全秘密分散法という。完全秘密分散法の情報比 ρ と管理者 P_i に対する情報比 ρ_i は以下のように定める。

$$\rho = \min\{\rho_i: 1 \leq i \leq n\}, \rho_i = \frac{\log |S|}{\log |W_i|}$$

ここで、秘密情報の集合を S 、管理者 P_i が持つ可能性のあるシェアの集合 W_i を表す。また、 $\rho = 1$ を満たす完全秘密分散法を理想的秘密分散法という。

3 整数計画法による複数割り当て法

岩本らは整数計画法を用いて平均割り当て数と最大割り当て数を最小にする最適な複数割り当て写像を構成する手法を提案している。

まず、複数割り当て写像 $\alpha_\Gamma: P \rightarrow 2^{W_{(t,m)}}$ および集合 $A \subseteq P$ に対し、 $W_{(t,m)}$ の 2^n 個の部分集合 $X_{[k]_2^n}^A, k = 0, 1, 2, \dots, N$ を以下のように定める。

$$X_{[k]_2^n}^A = \left[\bigcap_{i: [k]_2^n = 1} \alpha_\Gamma(P_i) \right] \cap \left[\bigcap_{i: [k]_2^n = 0} \overline{\alpha_\Gamma(P_i)} \right] \quad (1)$$

ここで、 $N = 2^n - 1$ 、 $[k]_2^n$ は非負整数 k を n ビットの2進数表示したものであり、 $[k]_2^n$ は $[k]_2^n$ の下

General Secret Sharing Schemes Based on (k, n) -threshold Schemes and Integer Programming on Five Participants.

Yutaro Shimma and Kouya Tochikubo

から i ビット目を指す。以下では $X_{[k]_2^n}$ を X_k と表記する。 $X_k, k = 0, 1, \dots, N$ は $\alpha_\Gamma(P_i), i = 1, 2, \dots, n$ のすべてに関する包含関係から定められる $W_{(t,m)}$ の 2^n 個の部分集合すべてを表しており、一般の n, N に対して、 X_k は次を満たす。

$$X_0 = \emptyset \quad (2)$$

$$X_k \cap X_{k'} = \emptyset \text{ if } k \neq k' \quad (3)$$

$$\alpha_\Gamma(P_i) = \bigcup_{k:[k]_2^{n,i}=1} X_k \quad (4)$$

$$\alpha_\Gamma(A) = \bigcup_{k=1}^N X_k - \bigcup_{\substack{k:[k]_2^{n,i}=0 \\ \text{for all } P_i \in A}} X_k \quad (5)$$

$$\alpha_\Gamma(P) = \bigcup_{k=1}^N X_k \quad (6)$$

式(3)(5)から、 $|X_k| = x_k$ おくと、

$$|\alpha_\Gamma(A)| = \sum_{k=1}^N x_k - \sum_{\substack{k:[k]_2^{n,i}=0 \\ \text{for all } P_i \in A}} x_k \quad (7)$$

が成り立つ。ここで、 $x = [x_1, x_2, \dots, x_N]$ 、ベクトル $a(A) = [a(A)_1, a(A)_2, \dots, a(A)_N] \in \{0, 1\}^N$ を $A = \{P_{i_1}, P_{i_2}, \dots, P_{i_u}\}$ に対して

$$a(A)_k = \begin{cases} 0 & \text{if } [k]_2^{n,i_1} = \dots = [k]_2^{n,i_u} = 0 \\ 1 & \text{otherwise.} \end{cases} \quad (8)$$

と定義すると式(7)の右辺は $a(A) \cdot x$ と表せる。よって、 $[k]_2^n$ のハミング重みを h_k とし $h = [h_1, h_2, \dots, h_N] \in \mathbb{Z}^N$ とすると、式(4)から、

$$\sum_{i=1}^n |\alpha_\Gamma(P_i)| = \sum_{i=1}^n \sum_{k:[k]_2^{n,i}=1} x_k = \sum_{k=1}^N h_k x_k = h \cdot x \quad (9)$$

が成り立つ。以上より、平均割り当て数 $\bar{\rho}$ を最小化する複数割り当て写像 $\tilde{\alpha}_\Gamma$ を与える整数計画問題 $\text{IP}_{\bar{\rho}}(\Gamma)$ が次のように定式化できる。

$$\begin{aligned} & \text{minimize } h \cdot x \\ & \text{subject to} \\ & a(A) \cdot x \geq t \quad \text{for } A \in \mathcal{A}_1^- \\ & a(B) \cdot x \leq t - 1 \quad \text{for } B \in \mathcal{A}_0^+ \\ & a(P) \cdot x \geq 1 \quad \text{for } P \in \mathcal{P} \\ & x \geq 0 \end{aligned}$$

制約式 $a(P) \cdot x \geq 1$ は、それぞれの管理者に最低1つのシェアを配るために必要な式である。

整数計画問題 $\text{IP}_{\bar{\rho}}(\Gamma)$ 最適解を与える x, t を $\tilde{x} = [\tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_N]$ および $\tilde{t}$ とし、 $\tilde{m} \equiv |\alpha_\Gamma(P)| = \sum_{k=1}^N \tilde{x}_k$ に対して、 $(\tilde{t}, \tilde{m})$ しきい値のシェアを $W_{(t,m)} = \{w_1^{(\tilde{t})}, w_2^{(\tilde{t})}, \dots, w_{\tilde{m}}^{(\tilde{t})}\}$ とする。このとき、式(3)(6)及び $\tilde{x}_k = |X_k|$ を満たすように X_k を構成でき、式(4)によって $\tilde{\rho}$ を最小化するような $\tilde{\alpha}_\Gamma$ が構成できる。

同様に、最大割り当て数 ρ^* を最小化する整数計画問題 $\text{IP}_{\rho^*}(\Gamma)$ を次のように定式化することで、 ρ^* を最小化する写像 α_Γ^* が構成できる。

$$\begin{aligned} & \text{minimize } M \\ & \text{subject to} \\ & a(A) \cdot x \geq t \quad \text{for } A \in \mathcal{A}_1^- \\ & a(B) \cdot x \leq t - 1 \quad \text{for } B \in \mathcal{A}_0^+ \\ & a(P) \cdot x \leq M \quad \text{for } P \in \mathcal{P} \\ & a(P) \cdot x \geq 1 \quad \text{for } P \in \mathcal{P} \\ & x \geq 0 \end{aligned}$$

4 効率の評価

JacksonとMartinにより評価された5人の場合におけるすべての管理者グループ180通りのアクセス構造とその情報比、及び、岩本らの手法を適用した場合の情報比をまとめたものが付録1である。なお、岩本らの手法では、割り当て数の逆数が情報比となる。結果として、平均割り当て数が最適となるアクセス構造は31通りであり、最大割り当て数が最適となるアクセス構造は14通り存在することが分かった。また、平均割り当て数を最小化する手法と比べて割り当て数が増えるものの、一人の持つシェアの最大数が減る最大割り当て数を最小化する手法は、アクセス構造52、67、136、145、168の計5通り存在することが分かった。

参考文献

- [1] Shamir, "How to share a secret," Communications of the ACM, vol.22, no.11, pp.612-613, 1979.
- [2] 岩本貢, 山本博資, 小川博久, "(k, n)しきい値法と整数計画法による秘密分散法の一般的構成法", 電子情報通信学会技術研究報告, vol. 103, no. 61, pp. 63-70, 2003.
- [3] Wen-Ai Jackson and Keith M.Martin, "Perfect Secret Sharing Schemes on Five Participants," Designs, Codes and Cryptography, 9, pp.267-286, 1996.
- [4] D. R. Stinson "Cryptography: Theory and practice," CRC Press, 2005.

付録1 5人の場合のすべてのアクセス構造180通りに岩本らの手法を適用した結果

	アクセス構造	非アクセス構造	岩本らの手法の情報比		情報比の上限	
			平均割り当て数	最大割り当て数	平均割り当て数	最大割り当て数
1	a+b+c+d+e		1	1	1	1
2	a+b+c+de	d+e	5/8	1/2	1	1
3	a+b+cd+ce	c+de	5/7	1/2	1	1
4	a+b+cd+ce+de	c+d+e	5/7	1/2	1	1
5	a+b+cde	cd+ce+de	5/9	1/3	1	1
6	a+bc+bd+be	d+ce+de	5/9	1/3	5/6	2/3
7	a+bc+bd+be+cd	b+c+de	5/6	1/2	1	1
8	a+bc+bd+be+cd+ce	b+c+d+e	5/6	1/2	1	1
9	a+bc+bd+be+cd+ce+de	b+cde	5/6	1/2	1	1
10	a+bc+bd+be+cde	b+cd+ce+de	5/8	1/3	5/6	2/3
11	a+bc+bd+cde	be+cd+de	5/9	1/3	5/6	2/3
12	a+bc+bd+ce	be+cd	5/6	1/2	1	1
13	a+bc+bd+ce+de	be+cd+ce+de	5/8	1/3	5/6	2/3
14	a+bc+bde	bd+be+de+ce	5/12	1/4	1	1
15	a+bc+bde+cde	bd+be+cde	5/8	1/3	1	1
16	a+bc+de	bd+be+cd+ce+de	2	1/4	1	1
17	a+bcd+bce	bc+bde+cde	5/7	1/3	1	1
18	a+bcd+bce+bde	bc+bd+be+cde	5/9	1/4	1	1
19	a+bcd+bce+bde+cde	bc+bd+be+cd+ce+de	5/7	1/3	1	1
20	a+bcde	bcd+bce+bde+cde	5/8	1/4	1	1
21	ab+ac+ad+ae	a+be+ce+de	5/8	1/2	5/6	2/3
22	ab+ac+ad+ae+bc	a+b+ce+de	5/8	1/2	5/7	2/3
23	ab+ac+ad+ae+bc+bd	a+b+c+de	1	1	1	1
24	ab+ac+ad+ae+bc+bd+be	a+b+c+d+e	1	1	1	1
25	ab+ac+ad+ae+bc+bd+be+cd	be+cde	5/7	1/2	5/6	2/3
26	ab+ac+ad+ae+bc+bd+be+cd+ce	a+b+cde	1	1	1	1
27	ab+ac+ad+ae+bc+bd+be+cd+ce+de	a+b+cd+ce+de	5/7	1/2	5/7	2/3
28	ab+ac+ad+ae+bc+bd+be+cde	a+be+cd+de	5/8	1/2	5/7	2/3
29	ab+ac+ad+ae+bc+bd+cd	a+be+cd	1	1	1	1
30	ab+ac+ad+ae+bc+bd+cde	a+be+cd+ce+de	5/7	1/2	5/7	3/5,2/3
31	ab+ac+ad+ae+bc+bd+ce	ae+be+cd+de	5/8	1/2	5/6	2/3
32	ab+ac+ad+ae+bc+bd+ce+de	ae+be+cd	5/8	1/2	5/7	2/3
33	ab+ac+ad+ae+bc+bde	ae+be+cd+ce+de	5/7	1/2	5/7	2/3
34	ab+ac+ad+ae+bc+bde+cde	a+bde+cde	5/7	1/2	5/6	2/3
35	ab+ac+ad+ae+bc+de	a+bd+be+cd+ce	2	1/2	5/6	2/3
36	ab+ac+ad+ae+bcd	bd+be+cde	5/7	1/2	5/6	2/3
37	ab+ac+ad+ae+bcd+bce	a+bd+be+cd+ce+de	5/9	1/3	5/6	2/3
38	ab+ac+ad+ae+bcd+bce+bde	ae+bd+cde	5/8	1/2	10/13	2/3
39	ab+ac+ad+ae+bcd+bce+bde+cde	ae+bd+cd+ce	2	1/2	5/7	2/3
40	ab+ac+ad+ae+bcde	ae+bd+cd+ce+de	5/7	1/2	5/7	7/12,2/3
41	ab+ac+ad+bc+bd+cde	ae+bd+be+cd+ce	5/11	1/3	5/6	2/3
42	ab+ac+ad+bc+bd+ce	ae+bd+be+cde	5/7	1/2	5/6	2/3
43	ab+ac+ad+bc+bd+ce+de	ae+bd+be+cd+ce+de	5/9	1/2	5/6	2/3
44	ab+ac+ad+bc+bde	ad+ae+bd+be+cd+ce	3	1/3	1	1
45	ab+ac+ad+bc+bde+cde	ad+ae+bde+cde	5/8	1/2	5/6	2/3
46	ab+ac+ad+bc+be	ad+ae+bd+be+cde	5/8	1/2	1	1
47	ab+ac+ad+bc+be+cde	ad+ae+bd+be+cd+ce+de	5/8	1/2	1	1
48	ab+ac+ad+bc+be+de	a+bce+bde+cde	5/8	1/3	5/7	3/5
49	ab+ac+ad+bc+de	bc+bde+cde	5/6	1/2	5/6	2/3
50	ab+ac+ad+bcd+bce	bc+bd+be+cde	5/8	1/3	5/6	2/3
51	ab+ac+ad+bcd+bce+bde	a+bc+bd+be+cd+ce+de	5/6	1/2	5/6	2/3
52	ab+ac+ad+bcd+bce+bde+cde	ae+bc+bd+cde	5/11	1/3	5/6	2/3
53	ab+ac+ad+bcde	ae+bc+bd+cd+de	2	1/2	5/8<5/7	3/5,2/3
54	ab+ac+ad+bce	ae+bc+bd+cd	5/7	1/2	5/7	2/3
55	ab+ac+ad+bce+bde	ae+bc+bd+cd+ce+de	5/9	1/3	5/6	2/3
56	ab+ac+ad+bce+bde+cde	ae+bc+bde+cde	5/9	1/2	5/7	3/5
57	ab+ac+ad+be	ae+bc+bd+be+cde	5/8	1/3	5/6	2/3
58	ab+ac+ad+be+bcd	ae+bc+bd+be+cd+ce+de	5/6	1/2	5/6	2/3
59	ab+ac+ad+be+bcd+cde	a+bcde	1	1	1	1
60	ab+ac+ad+be+cde	a+bcd+bce+bde+cde	5/7	1/3	5/7	2/3
61	ab+ac+ad+be+ce	ae+bcd+cde	5/7	1/2	5/6	2/3
62	ab+ac+ad+be+ce+bcd	ae+bcd+de	5/8	1/2	5/6	2/3
63	ab+ac+ad+be+ce+de	ae+bcd	1	1	1	1
64	ab+ac+ad+be+ce+de+bcd	ae+bcd+ce+de	5/7	1/2	5/6	2/3
65	ab+ac+ade	ae+bcd+bde+cde	5/8	1/3	5/7	3/5
66	ab+ac+ade+bcd	ae+bcd+be+cde	5/6	1/2	5/6	2/3
67	ab+ac+ade+bcd+bce	ae+bcd+be+ce+de	5/8	1/2	5/6	2/3
68	ab+ac+ade+bcd+bce+bde	ae+bcd+bce+bde+cde	5/7	1/3	5/7	3/5
69	ab+ac+ade+bcd+bce+bde+cde	ade+bc+be+ce	5/7	1/2	5/7	2/3
70	ab+ac+ade+bcd+bde	ad+ae+bc+be+ce+de	5/9	1/2	5/7	2/3
71	ab+ac+ade+bcd+bde+cde	ade+bc+be+cd	5/11	1/3	5/6	2/3
72	ab+ac+ade+bcdde	ad+ae+bc+be+cd	2	1/2	2/3	2/3
73	ab+ac+ade+bde	ad+ae+bc+be+cd+de	2	1/2	5/8<5/7	3/5,2/3
74	ab+ac+ade+bde+cde	ade+bc+be+cde	5/9	1/2	5/7	3/5
75	ab+ac+bc+ade	ad+ae+bc+be+cde	2	1/2	5/7	2/3
76	ab+ac+bc+ade+bde	ad+ae+bc+be+cd+ce+de	5/9	1/2	5/7	2/3
77	ab+ac+bc+ade+bde+cde	ade+bc+be+cd+ce	5/9	1/2	5/6	2/3
78	ab+ac+bc+de	ade+bce+ce	5/7	1/2	5/6	2/3
79	ab+ac+bcd+bce	ade+bc+bde+cde	5/6	1/2	5/6	2/3
80	ab+ac+bcd+bce+bde	ad+ae+bc+bd+be+cd+ce	5/12	1/3	5/7<5/6	2/3
81	ab+ac+bcd+bce+bde+cde	ad+ae+bc+bde+cde	5/9	1/3	5/7	3/5
82	ab+ac+bcd+bde	ad+ae+bc+bd+be+cde	2	1/3	5/7<5/6	3/5,2/3
83	ab+ac+bcd+bde+cde	ad+ae+bc+bd+be+cd+ce+de	5/8	1/2	5/7<5/6	2/3
84	ab+ac+bcde	ade+bc+bd+be+cde	5/8	1/3	5/7	3/5
85	ab+ac+bd+ade	ade+bc+bd+be+cd+ce	5/6	1/2	5/6	2/3
86	ab+ac+bd+ade+bce	ad+ae+bce+bd+cd	5/12	1/3	5/7 5/6	2/3
87	ab+ac+bd+ade+bce+cde	ad+ae+bce+bde+cde	5/8	1/2	5/7	3/5
88	ab+ac+bd+ade+cde	ad+ae+bce+bd+cde	5/8	1/2	5/7<5/6	2/3
89	ab+ac+bd+cd+ade	ad+ae+bce+bd+cd+de	2	1/3	5/7<5/6	2/3
90	ab+ac+bd+cd+ade+bce	ade+bce+bd+cde	5/8	1/2	5/7	3/5

	アクセス構造	非アクセス構造	岩本らの手法の情報比		情報比の上限	
			平均割り当て数	最大割り当て数	平均割り当て数	最大割り当て数
91	ab+ac+bd+cde	ade+bce+bd+cd	5/8	1/3	5/6	2/3
92	ab+ac+bd+ce	ad+ae+bcd+bce	2	1/2	1	1
93	ab+ac+bd+ce+ade	ad+ae+bcde	5/7	1/2	1	1
94	ab+ac+bd+ce+de	ad+ae+bcd+bce+cde	2	1/3	5/6	2/3
95	ab+ac+bde	ad+ae+bcd+bce+de	5/8	1/2	1	1
96	ab+ac+bde+cde	ad+ae+bcd+bce+bde+cde	5/9	1/3	5/6	2/3
97	ab+ac+de	ade+bcd+bce+cde	5/8	1/3	5/6	2/3
98	ab+ac+de+bcd	ade+bcd+bce	5/6	1/2	1	1
99	ab+ac+de+bcd+bce	ade+bcd+bce+bde+cde	5/7	1/3	5/6	2/3
100	ab+acd+ace	ac+ade+bce+bde	5/9	1/2	5/6	2/3
101	ab+acd+ace+ade	ac+ade+bc+bde+ce	5/11	1/3	5/6	2/3
102	ab+acd+ace+ade+bcd	ac+ad+ae+bc+bde+ce	5/11	1/3	1	1
103	ab+acd+ace+ade+bcd+bce	ac+ad+ae+bc+bd+be+ce+de	5/9	1/2	1	1
104	ab+acd+ace+ade+bcd+bce+bde	ac+ade+bce+bd	2	1/2	1	1
105	ab+acd+ace+ade+bcd+bce+bde+cde	ac+ade+bce+bde+cde	5/8	1/2	5/6	2/3
106	ab+acd+ace+ade+bcd+bce+cde	ac+ade+bc+bde+cde	5/7	1/2	1	1
107	ab+acd+ace+ade+bcd+cde	ac+ad+ae+bc+bde+cde	5/9	1/3	5/7<5/6	3/5,2/3
108	ab+acd+ace+ade+bcde	ac+ad+ae+bc+bd+be+cde	5/7	1/2	1	1
109	ab+acd+ace+ade+cde	ac+ad+ae+bc++bd+be+cd+ce+de	5/8	1/2	1	1
110	ab+acd+ace+bcd	ac+ad+ae+bc+bde+cd+ce	5/9	1/2	1	1
111	ab+acd+ace+bcd+bce	ac+ade+bc+bde+cd+ce	5/11	1/3	5/6	2/3
112	ab+acd+ace+bcd+bce+cde	ac+ad+ae+bce+bde+cde	5/7	1/2	5/6	2/3
113	ab+acd+ace+bcd+bde	ac+ad+ae+bce+bde+cd	5/8	1/2	5/7<5/6	2/3
114	ab+acd+ace+bcd+bde+cde	ac+ade+bce+bd+cde	5/11	1/3	5/7	3/5
115	ab+acd+ace+bcd+cde	ac+ade+bce+bd+cd	5/11	1/3	1	1
116	ab+acd+ace+bcde	ac+ade+bce+bde+cd	2	1/3	5/6	2/3
117	ab+acd+ace+bde	ace+ade+bce+bde+cd	5/11	1/3	5/7	3/5
118	ab+acd+ace+bde+cde	ade+bcde	5/6	1/2	1	1
119	ab+acd+ace+cde	ac+ad+ae+bcde	5/7	1/2	1	1
120	ab+acd+bcd+cde	ac+ad+ae+bcd+bce+bde	2	1/3	5/6	2/3
121	ab+acd+bcde	ac+ad+ae+bcd+bce+bde+cde	5/8	1/3	5/6	2/3
122	ab+acd+bce	ac+ade+bcd+bce+cde	5/9	1/3	5/6	2/3
123	ab+acd+bce+cde	ac+ade+bcd+bce	5/9	1/2	5/7 5/6	2/3
124	ab+acd+cde	ac+ade+bcd+bce+bde	5/11	1/3	5/6	2/3
125	ab+acde	ac+ade+bcd+bce+bde+cde	2	1/3	5/6	2/3
126	ab+acde+bcde	ace+ade+bcd+bde+cde	5/7	1/2	10/13	2/3
127	ab+cd+ace	ace+ade+bcd+bde	5/8	1/2	5/6	2/3
128	ab+cd+ace+ade	ace+ade+bcd+bce+bde	2	1/3	5/6	2/3
129	ab+cd+ace+ade+bce	ace+ade+bcd+bce+bde+cde	5/8	1/3	5/6	2/3
130	ab+cd+ace+ade+bce+bde	acd+ace+ade+bcd+bce+bde	5/12	1/3	1	1
131	ab+cd+ace+bde	acd+ace+ade+bcde	5/7	1/3	1	1
132	ab+cde	acd+ace+ade+bcd+bce+bde+cde	5/9	1/3	1	1
133	abc+abd+abe	ab+ace+ade+bce+bde+cde	5/8	1/2	5/7	3/5
134	abc+abd+abe+acd	ab+ac+ade+bce+bde+cde	5/7	1/2	5/6	2/3
135	abc+abd+abe+acd+ace	ab+ac+ade+bc+bde+cde	1	1	1	1
136	abc+abd+abe+acd+ace+ade	ab+ac+ad+ae+bc+bde+cde	5/9	1/2	5/7<5/6	2/3
137	abc+abd+abe+acd+ace+ade+bcd	ab+ac+ad+ae+bc+bd+be+ce+cde	5/7	1/2	1	1
138	abc+abd+abe+acd+ace+ade+bcd+bce	ab+ac+ad+ae+bc+bd+be+cd+ce+de	1	1	1	1
139	abc+abd+abe+acd+ace+ade+bcd+bce+bde	ab+ac+ad+ae+bce+bde+cde	5/9	1/2	5/6	2/3
140	abc+abd+abe+acd+ace+ade+bcd+bce+bde+cde	ab+ac+ade+bce+bd+cde	2	1/2	5/7	3/5
141	abc+abd+abe+acd+ace+ade+bcde	ab+ac+ade+bce+bd+cd	5/9	1/2	1	1
142	abc+abd+abe+acd+ace+bcde	ab+ace+ade+bce+bde+cd	5/13	1/3	5/7	3/5
143	abc+abd+abe+acd+ace+bcd+bce	ace+ade+bcde	5/7	1/2	5/6	2/3
144	abc+abd+abe+acd+ace+bcd+bde	ade+bcde	5/6	1/2	1	1
145	abc+abd+abe+acd+ace+bcd+bde+cde	ab+ac+ad+ae+bcde	5/7	1/2	1	1
146	abc+abd+abe+acd+ace+bcde	ab+ac+ad+ae+bcd+bce+bde+cde	5/6	1/2	5/6	2/3
147	abc+abd+abe+acd+ace+bde	ab+ac+ade+bcd+bce+cde	5/11	1/3	5/6	3/5
148	abc+abd+abe+acd+ace+bde+cde	ab+ac+ade+bcd+bce	5/11	1/3	5/7<5/6	2/3
149	abc+abd+abe+acd+bcd	ab+ac+ade+bcd+bce+bde+cde	5/8	1/2	5/6	2/3
150	abc+abd+abe+acd+bcd+cde	ab+ace+ade+bcd+bde+cde	5/9	1/2	5/7	3/5
151	abc+abd+abe+acd+bcde	ab+ace+ade+bcd+bde	5/11	1/3	5/8<5/7	3/5,2/3
152	abc+abd+abe+acd+bce	ab+ace+ade+bcd+bce+bde	5/13	1/3	5/8<5/7	3/5,2/3
153	abc+abd+abe+acd+bce+cde	ab+ace+ade+bcd+bce+bde+cde	2	1/3	5/7	3/5
154	abc+abd+abe+acd+cde	abe+ace+ade+bcd+bde+cde	5/9	1/2	5/6	2/3
155	abc+abd+abe+acde	abe+ace+ade+bcd+cde	5/9	1/3	5/6	2/3
156	abc+abd+abe+acde+bcde	abe+ace+ade+bcde	5/7	1/2	1	1
157	abc+abd+abe+acde	abe+ace+ade+bcd+bce+bde+cde	5/6	1/2	5/6	2/3
158	abc+abd+acd+bcde	ab+acde+bcde	1	1	1	1
159	abc+abd+acd+bce	ab+acd+ace+ade+bcd+bce+bde	3	1/3	5/7	3/5
160	abc+abd+acd+bce+bde	acd+ace+ade+bcde	5/7	1/3	5/6	2/3
161	abc+abd+acd+bce+bde+cde	ab+acd+ace+ade+bcd+bce+bde+cde	5/7	1/2	5/7	3/5
162	abc+abd+acde	abe+acd+ade+bcde	5/7	1/2	5/6	2/3
163	abc+abd+acde+bcde	abe+acd+bcde	1	1	1	1
164	abc+abd+ace	abe+acd+bcd+bce+bde+cde	2	1/2	5/6	2/3
165	abc+abd+ace+ade	abe+acd+ade+bcd+bce+cde	5/11	1/3	5/7	3/5
166	abc+abd+ace+ade+bcde	abe+acd+ade+bcd+bce	2	1/2	2/3	2/3
167	abc+abd+ace+bcde	abe+acd+ade+bcd+bce+bde+cde	5/11	1/3	5/7	3/5
168	abc+abd+ace+bde	abe+acd+ace+ade+bcd+bce+bde	5/13	1/3	5/7	3/5
169	abc+abd+ace+bde+cde	abe+acd+ace+ade+bcde	5/7	1/2	5/6	2/3
170	abc+abd+cde	abe+acd+ace+ade+bcd+bce+bde+cde	5/8	1/2	5/7	3/5
171	abc+abde	abd+abe+acd+ace+bcde	5/9	1/2	1	1
172	abc+abde+acde	abd+abe+acd+ace+bcd+bce+bde+cde	5/14	1/3	1	1
173	abc+abde+acde+bcde	abd+abe+acde+bcde	5/6	1/2	1	1
174	abc+ade	abd+abe+acd+ace+ade+bcde	5/9	1/2	1	1
175	abc+ade+bcde	abd+abe+acd+ace+ade+bcd+bce+bde+cde	5/8	1/2	1	1
176	abcd+abce	abc+abde+acde+bcde	1	1	1	1
177	abcd+abce+abde	abc+abd+abe+acde+bcde	5/7	1/2	1	1
178	abcd+abce+abde+acde	abc+abd+abe+acd+ace+ade+bcde	5/6	1/2	1	1
179	abcd+abce+abde+acde+bcde	abc+abd+abe+acd+ace+ade+bcd+bce+bde+cde	1	1	1	1
180	abcde	abcd+abce+abde+acde+bcde	1	1	1	1