フォールトトレラントシステムの領域分割モデル

森永 聡

日本電気株式会社 Ｃ＆Ｃ研究所
〒216 神奈川県川崎市宮前区宮崎 4-1-1
(044)-856-2134, morinaga@sbl.cl.nec.co.jp

フォールトトレラントシステムのモデル化の方法を提案する。このモデル (領域分割モデル) によって広いクラスのフォールトトレラントシステムを統一的に表現し信頼度を解析することができる。

与えられた冗長性の下での信頼度最大化問題をこのモデルを使って定式化し、その解を予想した。解は Kuhn-Tucker 条件を満たしている。しかし局所的最大点にさえならない場合がある。

キーワード　フォールトトレラントシステム、領域分割モデル、信頼度最大化、冗長性

Representation and Analysis of Fault-Tolerant Systems using Domain-Partition Model

Satoshi Morinaga

C&C Research Laboratories
NEC Corporation
4-1-1 Miyazaki,Miyamae-ku,Kawasaki 216 Kanagawa JAPAN
+81-44-856-2134, morinaga@sbl.cl.nec.co.jp

In this paper we propose a new model of fault-tolerant systems. This model, called Domain-Partition model, gives a unified representation of most types of fault-tolerant systems and a method for reliability analysis.

The reliability maximization problem under given redundancy is formulated using this model, and a solution is conjectured for this problem. The solution satisfies Kuhn-Tucker condition, but the solution is not even locally maximum in some cases.

keywords　fault-tolerant system, domain-partiton model, reliability maximization, redundancy

1 はじめに

フォールトトレラントシステムを実現する方法としては、誤り訂正符号を用いる方法や、システムをサブシステムに分解しそれぞれを冗長化する方法、一つの計算を繰り返し行なう方法、一つの計算を複数のプロセッサに行なわせて多数決をとる方法などが提案され、それぞれ数学的モデルで表現することによりある故障の仮定の下での信頼度が求められている [2]。

ところがそれらを統一的に表現するモデルがないために、システムに許される冗長性が指定された時の、信頼度最大化問題の定式化および解析が困難であった。

それに対して我々は、サブシステムを冗長化する方法、同一の計算を複数のプロセッサに行なわせて多数決をとる方法、FPGA(field programmable gate array) などで欠陥セルを迂回してシステムを再構成する方法などを統一的に表現するモデル (領域分割モデル) を提案し、ある故障の仮定の下での信頼度を求めることにより、フォールトトレラントシステムの広いクラスを統一的に論じる方法を与え、冗長性固定信頼度最大化問題の定式化とその解析を行なった [1]。

ここでは、モデル化の方法と冗長性固定信頼度最大化問題の数理的側面を中心に報告する。

2 フォールトトレラントシステムの領域分割モデルによる表現

2.1 システムの分解と信頼度

フォールトトレラントシステムを構成している要素を、故障に対する性質を用いてグループわけする。A をシステムを構成する全てのハードウェアからなる集合とする。また A の部分集合の族 B および C を

$$
\begin{aligned}
B &= \{\, a \subset A \mid && \bar{a}\text{すべてが故障していても} \\
  & && \text{システムが動作可能}\} \\
C &= \{\, b \in B \mid && b \subset b' \in B\text{なる}b'\text{に対して、} \\
  & && \bar{b'}\text{すべてが故障している状態から} \\
  & && \bar{b}\text{すべてが故障している状態に} \\
  & && \text{移ることでシステムダウンしない}\}
\end{aligned}
$$

と定義する ($\bar{x}$ は x の補集合)。さらに C の部分集合 D を

$$D = \{d \in C \mid d' \subset d\text{なる}d' \in C\text{が存在しない}\}$$

と定義する。D の要素数 p を動作のバリエーションとよぶことにする。また D の要素に適当に順番をつけて d_i $(i = 1, \cdots, p)$ として d_i をパターン i とよぶことにする。D の要素は通常、極小パスと呼ばれるものである。

さて、

- 少なくとも一つのパターンが無傷 (その要素に故障がない) である。→ システムが正常に作動している。
- すべてのパターンに傷がある (無傷でない)。→ システムが正常に作動していないこともある。

ことは明らかである。

あわせて、少なくとも一つのパターンが無傷であることがシステムの正常な動作を保証することがわかる。

ここでパターン i の定義関数 $d_i : A \to \{0, 1\}$

$$d_i(x) = \begin{cases} 1 & (x \in d_i) \\ 0 & \text{otherwise} \end{cases}$$

を用いて関数 $\boldsymbol{f} : A \to \{-1, 1\}^p$ を

$$f_i(x) = 2d_i(x) - 1$$

と定義する。

今、$\boldsymbol{k}$ を ± 1 を成分とする p 次元ベクトルとする。システムの構成要素の集合 $I_{\boldsymbol{k}} \subset A$ を

$$I_{\boldsymbol{k}} = f^{-1}(\boldsymbol{k})$$

で定義する。以上の操作でシステムの構成要素が 2^p 個のグループに分解される。

次に、ある故障の仮定の下でグループ $I_{\boldsymbol{k}}$ が無傷である確率 $P_{\boldsymbol{k}}$ をもちいて $I_{\boldsymbol{k}}$ の有効面積 $N(\boldsymbol{k})$ を

$$N(\boldsymbol{k}) = -\frac{1}{\lambda} \log P_{\boldsymbol{k}}$$

で定義する。λ は

$$\mathrm{Tr}_{\{\boldsymbol{k}\}} N(\boldsymbol{k}) = 1$$

が成立するように決めた規格化定数である。ここで $\mathrm{Tr}_{\{\boldsymbol{k}\}}$ とは $\boldsymbol{k}$ をとり得る値すべてについて変えながら以下を加える、$\sum_{\boldsymbol{k}}$ を表す記号とする。また $P_{\boldsymbol{k}} \leq 1$ から自然に $N(\boldsymbol{k}) \geq 0$ となる。

システムの信頼度 R を、少なくとも一つのパターンが無傷である確率と定義すると、各 $I_{\boldsymbol{k}}$ の故障の有無が独立であると仮定すれば

$$R = \mathrm{Tr}_{\{\boldsymbol{l}\}} (-1)^{|\boldsymbol{l}|+p+1} \exp(\lambda(\mathrm{Tr}_{\{\boldsymbol{k} \leq \boldsymbol{l}\}} N(\boldsymbol{k}) - 1)) + 1 \tag{1}$$

が成立する[1] (付録 A)。$\boldsymbol{l}$ は ± 1 を成分とする p 次元ベクトル、$|\boldsymbol{l}|$ は $\boldsymbol{l}$ の $+1$ の成分の個数を表す記号とする。

以上でフォールトトレラントシステムと故障の仮定が与えられた時の信頼度が求まった。

[1] $k \leq l$ を $\forall i k_i \leq l_i$ で定義する (他の大小関係も同様)。$\mathrm{Tr}_{\{k \leq l\}}$ を $k \leq l$ を満たす k について以下の和をとる記号とする。

2.2 領域分割モデル

前項のフォールトトレラントシステムにモデルを与える。

面積 1 の二次元平面を考える。平面上の点の集合を A とする。この平面上に p 枚のパターン $d_i \subset A$ $(i = 1, \cdots, p)$ を与える。パターン i の面積をパターン i の収納率、その逆数を冗長性ともいうことにする。この p も動作のバリエーションということにする。前項と同様にパターン i の定義関数 $d_i : A \to \{0, 1\}$

$$d_i(x) = \begin{cases} 1 & (x \in d_i) \\ 0 & \text{otherwise} \end{cases}$$

を用いて関数 $f : A \to \{-1, 1\}^p$ を

$$f_i(x) = 2d_i(x) - 1$$

と定義する。

今、$\boldsymbol{k}$ を ± 1 を成分とする p 次元ベクトルとして、$I_{\boldsymbol{k}} \subset A$ を

$$I_{\boldsymbol{k}} = f^{-1}(\boldsymbol{k})$$

で定義する。以上の操作で A 上の点が 2^p 個の領域に分割される。$I_{\boldsymbol{k}}$ の面積を $N(\boldsymbol{k})$ で表すことにする。例えば、この変数を使うと

$$\text{パターン}i\text{の面積} = \mathrm{Tr}_{\{\boldsymbol{k} \geq \vec{i}\}}(N(\boldsymbol{k}))$$

と表せる。ただし、$\vec{i}$ は第 i 成分のみが 1 で残りの成分がすべて -1 である p 次元ベクトルとする。

ここで、平面 A 上にはランダムに傷があり、その分布がパラメータ λ のポアソン分布にしたがっているとする。このとき少なくとも一枚のパターンが無傷になる確率を R とすると、式 (1) が成立する。

あるフォールトトレラントシステムが与えられると p と $N(\boldsymbol{k})$ がきまる。これと全く同じ $N(\boldsymbol{k})$ を与える p 枚のパターンによる領域の分割の方法は必ず存在する。これをこのフォールトトレラントシステムの領域分割モデルによる表現ということにする。フォールトトレラントシステムの信頼度は、領域分割モデルで表現した時の少なくとも一枚のパターンが無傷である確率と等しい。ということは実際のシステムの構造がわからなくてもその領域分割モデルによる表現さえ得られれば信頼度や冗長性[2]について解析することができる。

直列並列ブロックモデルで表現できるフォールトトレラントシステムは、必ず領域分割モデルで表現することができる。逆に、多数決システムなど、領域分割モデルでは表現できても、直列並列ブロックモデルでは表現できないシステムは数多く存在する。

[2] 領域分割モデルで表現したときの冗長性をもとのシステムの冗長性と定義する。自然な定義になっている。

3 冗長性固定信頼度最大化問題

3.1 問題の定式化と解の予想

すべての $i = 1, \cdots p$ に対して $\mathrm{Tr}_{\{\boldsymbol{k} \geq \vec{i}\}} N(\boldsymbol{k}) = x$ を保ったまま、与えられた p, λ で信頼度 R を最大にする $N(\boldsymbol{k}) \geq 0$ を求める。これは与えられた冗長性を持つシステムの中で、信頼度が最大になるものを求めることと同等である。

$p = 1, 2, 3$ のときの厳密解 [1] から類推して、与えられた冗長性のもとで信頼度を最大にするパターンは、対称でなるべく重なりの少ない配置を求めることによって得られると予想される。

このことを定式化する。

冗長性固定信頼度最大化問題 p, λ, x を定数とする。このとき以下の制約条件

$\forall i = 1, \cdots, p$ で

$$\begin{aligned} \mathrm{Tr}_{\{\boldsymbol{k} \geq \vec{i}\}} N(\boldsymbol{k}) &= x \\ \mathrm{Tr}_{\{\boldsymbol{k}\}} N(\boldsymbol{k}) &= 1 \\ N(\boldsymbol{k}) &\geq 0 \end{aligned}$$

を満たし

$$R = \mathrm{Tr}_{\{\boldsymbol{l}\}} (-1)^{|\boldsymbol{l}|+p+1} \exp(\lambda(\mathrm{Tr}_{\{\boldsymbol{k} \leq \boldsymbol{l}\}} N(\boldsymbol{k}) - 1)) + 1$$

を最大にする

$$\boldsymbol{N} = (N(-, \cdots, -), \cdots, N(+, \cdots, +))$$

を求めよ。

解の予想 λ の値に関わらず、面積 x で対称かつなるべく重なりの少ない p 枚のパターン配置の $\boldsymbol{N}$ を求めることによって得られる

予想を満たすパターン配置の $\boldsymbol{N}$ を $\boldsymbol{N}^*$ とする。$\boldsymbol{N}^*$ は、xp 以上の最小の整数を q として

$$N^*(\boldsymbol{k}) = \begin{cases} \frac{1+xp-q}{{}_pC_q} & (|\boldsymbol{k}| = q) \\ \frac{q-xp}{{}_pC_{q-1}} & (|\boldsymbol{k}| = q-1) \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

である (付録 B)。$\boldsymbol{N}^*$ を与えるパターン配置を予想配置と呼ぶことにする。

かなり複雑な計算を経て、予想配置が冗長性固定信頼度最大化問題において、Kuhn-Tucker 条件を満たしていることが証明できる (付録 C)。

ところが局所的最適解さえ与えない p, λ, x の組も存在する [1]。

4 まとめ

広いクラスのフォールトトレラントシステムを統一的に表現する領域分割モデルと、それを用いた冗長性固定信頼度最大化問題の数理的な側面を中心に報告した。

謝辞

日頃御指導いただく山本所長、システム基礎研の皆様、東大吉沢研の皆様に感謝します。

参考文献

[1] 森永聡, 枝廣正人, 藤田友之. "フォールトトレラントシステムの領域分割モデル". 信学技報, Vol. FTS95, No. 15, pp. 31–38, 1995.

[2] 南谷. フォールトトレラントコンピュータ. オーム社, 1991.

[3] 大塚 誠ら. "宇宙搭載用フォールトトレラントコンピュータ". 情報処理, Vol. 35, No. 6, pp. 497–503, 1994.

[4] Paul R. Pukite and Claude L. Berman. "Defect Cluster Analysis for Wafer-Scale Integration". *IEEE Transactions on Semiconductor Manufacturing*, Vol. 3, pp. 128–135, 1990.

A 信頼度の導出

システムの信頼度 R は

$$
\begin{aligned}
&= \Pr\{\text{少なくとも一つのパターンが無傷}\} \\
&= \Pr\{{}^{\exists}i\ (d_i \text{ が無傷})\} \\
&= \Pr\{{}^{\exists}i\ ({}^{\forall}k \geq \vec{i}\ (I_k \text{ が無傷}))\}
\end{aligned}
$$

で表される。さらに $({}^{\forall}k \geq \vec{i}\ (I_k \text{ が無傷}))$ を Q_i と略記して $Q_i \wedge Q_j$ を $Q_{i,j}$ などとすると、和の公式を用いて

$$
\begin{aligned}
R &= \Pr\{{}^{\exists}i\ Q_i\} \\
&= +\Pr\{Q_1\} + \Pr\{Q_2\} + \Pr\{Q_3\} + \Pr\{Q_4\} + \cdots \\
&\quad -\Pr\{Q_{1,2}\} - \Pr\{Q_{1,3}\} - \Pr\{Q_{1,4}\} - \cdots \\
&\quad + \cdots - \cdots + \cdots - \cdots + \cdots - \cdots \\
&= \sum_{J\neq\phi}(-1)^{|J|+1}\Pr\{\bigwedge_{i\in J}({}^{\forall}k \geq \vec{i}\ (I_{\boldsymbol{k}} \text{ が無傷}))\}
\end{aligned}
$$

と表すことができる[3]。

さらに任意の $\boldsymbol{k} \neq \boldsymbol{k}'$ について、事象 "$I_{\boldsymbol{k}}$ が無傷" と "$I_{\boldsymbol{k}'}$ が無傷" が独立であれば、集合 J の要素を指標とする成分だけ $+1$ で 残りの成分が -1 である p 次元ベクトルを $\vec{J}$ と書いて

$$
\begin{aligned}
R &= \sum_{J\neq\phi}(-1)^{|J|+1}\exp(-\lambda(1-\mathrm{Tr}_{\{k\leq-\vec{J}\}}(N(k)))) \\
&= \mathrm{Tr}_{\{l\}}(-1)^{|l|+p+1}\exp(\lambda(\mathrm{Tr}_{\{k\leq l\}}(N(k))-1))+1
\end{aligned}
$$

となる。ただし、

$$\Pr\{I_{\boldsymbol{k}}\text{が無傷}\} = \exp(-\lambda N(\boldsymbol{k}))$$

を用いた。

[3] $\sum_{J\neq\phi}$ は J を空でない $\{1,\cdots,p\}$ の部分集合すべてについて走らせながら、以下を足す記号とする。

B 予想を満たすパターン配置

解の予想 面積 x で対称でなるべく重なりの少ない p 枚のパターン配置の $\boldsymbol{N}$ を求めることによって得られる

この予想を満たすパターン配置の $\boldsymbol{N}$ を $\boldsymbol{N}^*$ とする。$\boldsymbol{N}^*$ の具体的な値を求める。

まずパターンを対称に配置することと $N(\boldsymbol{k})$ の値が $\boldsymbol{k}$ の $+$ の数 $|\boldsymbol{k}|$ だけによって決まることは同値だから

$$N^*(\boldsymbol{k}) = N_{|\boldsymbol{k}|}$$

と表すことができる。この $N_{|\boldsymbol{k}|}$ を求めたい。利用すると

$$
\begin{aligned}
\mathrm{Tr}_{\{\boldsymbol{k}\geq\vec{i}\}}N^*(\boldsymbol{k}) &= \mathrm{Tr}_{\{\boldsymbol{k}\geq\vec{i}\}}(N_{|\boldsymbol{k}|}) \\
&= \sum_{j=1}^{p} N_j \times {}_{p-1}C_{j-1}
\end{aligned}
$$

これが x になる必要がある。

同様に

$$\mathrm{Tr}_{\{\boldsymbol{k}\}}N^*(\boldsymbol{k}) = \sum_{j=0}^{p} N_j \times {}_{p}C_j = 1$$

の必要がある。

また、なるべく重なりが少なくなるようにパターンを配置することと、大きい j にたいしてなるべく N_j を 0 にすることが同値であるから、予想を満たす配置の $\boldsymbol{N}$ つまり $\boldsymbol{N}^*$ を求めるという問題は

$$
\begin{aligned}
\sum_{j=1}^{p} {}_{p-1}C_{j-1}N_j &= x &\quad (3)\\
\sum_{j=0}^{p} {}_{p}C_jN_j &= 1 &\quad (4)\\
N_j &\geq 0 &\quad (5)
\end{aligned}
$$

を満たす $\boldsymbol{N}$ で

$$j_0 = \max\{j|N_j \neq 0\}$$

とした時に j_0 が最小、しかもその中でも N_{j_0} が最小になる $\boldsymbol{N}$ を求める問題へと変形できる。

これを解くと、$\boldsymbol{N}^*$ は、xp 以上の最小の整数を q として

$$
N^*(\boldsymbol{k}) = \begin{cases} \frac{1+xp-q}{{}_pC_q} & (|\boldsymbol{k}| = q) \\ \frac{q-xp}{{}_pC_{q-1}} & (|\boldsymbol{k}| = q-1) \\ 0 & \text{otherwise} \end{cases} \quad (6)
$$

である。予想を満たすパターン配置の $\boldsymbol{N}$ が具体的に求まった。

C　予想が Kuhn-Tucker 条件を満たすことの証明

明らかに R の最大化と $T=e^{\lambda}(R-1)$ の最大化は同値であるので、制約条件
$\forall i=1,\cdots p$ で

$$\begin{aligned}\mathrm{Tr}_{\{\boldsymbol{k}\geq\vec{i}\}}(N(\boldsymbol{k})) &= x\\ \mathrm{Tr}_{\{\boldsymbol{k}\}}(N(\boldsymbol{k})) &= 1\\ N(\boldsymbol{k}) &\geq 0\end{aligned}$$

のもとでの目的関数

$$T=(-1)^{p+1}\mathrm{Tr}_{\{l\}}((-1)^{|l|}\exp(\lambda\mathrm{Tr}_{\{\boldsymbol{k}\leq\boldsymbol{l}\}}(N(\boldsymbol{k}))))$$

の最大化問題において、$\boldsymbol{N}^*$ が Kuhn-Tucker 条件を満たしていることを証明する。ここでは xp が整数になる場合を論じる。すなわち $q=xp$ になる。そうでない場合は非常に繁雑になるが同様に証明できる。

まず、以下のように $\boldsymbol{N}$ を使って新しい変数 $\boldsymbol{n}$ を定義して、問題を定式化し直す。(この変数を使った方が以下、式表示がコンパクトになる)

$$n(\boldsymbol{l})=\mathrm{Tr}_{\{\boldsymbol{k}\leq\boldsymbol{l}\}}(N(\boldsymbol{k})))$$

$\boldsymbol{l}$ は ±1 を成分とする p 次元のベクトルである。さらに $n(\boldsymbol{k})$ が作るベクトルを $\boldsymbol{n}$ とする。この変換の逆変換は

$$N(\boldsymbol{k})=\mathrm{Tr}_{\{\boldsymbol{l}\leq\boldsymbol{k}\}}((-1)^{|\boldsymbol{k}|+|\boldsymbol{l}|}n(\boldsymbol{l})))$$

であるから (付録 C.1)、問題に代入して定式化し直す。

制約条件と目的関数は
$\forall i=1,\cdots p,\forall\boldsymbol{k}$ で

$$\begin{aligned}n(-\vec{i}) &= 1-x\\ n(\vec{\mp}) &= 1\\ \mathrm{Tr}_{\{\boldsymbol{l}\leq\boldsymbol{k}\}}((-1)^{|\boldsymbol{k}|+|\boldsymbol{l}|}n(\boldsymbol{l}))) &\geq 0\end{aligned}$$

$$T=(-1)^{p+1}\mathrm{Tr}_{\{l\}}((-1)^{|l|}\exp(\lambda n(\boldsymbol{l})))$$

となる。ただし成分がすべて $+1$ の p 次元ベクトルを $\vec{\mp}$ とかいた。また $\boldsymbol{N}^*$ に対応する $\boldsymbol{n}$ は

$$n^*(l)=\frac{{}_{|l|}C_q}{{}_pC_q}$$

となる。$n(\vec{\mp}),n(-\vec{i})$ を定数とみなすことによって $n(\boldsymbol{l})$ の $\boldsymbol{l}\neq\vec{\mp},-\vec{i}$ を満たすものだけが作る 2^p-p-1 次元空間内に不等式制約条件が 2^p 本はいる非線形計画問題となる。適切に変数変換をすることによって、等式制約条件の消去で変数の個数が減るのと同時に目的関数も簡単になった。

証明したいことは $\boldsymbol{n}^*$ が制約条件のもとでの目的関数の最大化問題で Kuhn-Tucker 条件を満たしていることである。

いま、$\boldsymbol{n}^*$ でアクティブな制約条件
$\forall\boldsymbol{k}$ s.t. $|\boldsymbol{k}|\neq q$ で

$$\mathrm{Tr}_{\{\boldsymbol{l}\leq\boldsymbol{k}\}}((-1)^{|\boldsymbol{k}|+|\boldsymbol{l}|}n(\boldsymbol{l})))=0$$

に未定乗数 $\lambda_{\boldsymbol{k}}$ をあたえてラグランジュ関数 G を

$$G=T+\mathrm{Tr}_{\{\boldsymbol{k}\mid|\boldsymbol{k}|\neq q\}}\lambda_{\boldsymbol{k}}\mathrm{Tr}_{\{\boldsymbol{l}\leq\boldsymbol{k}\}}((-1)^{|\boldsymbol{k}|+|\boldsymbol{l}|}n(\boldsymbol{l})))$$

とする。このとき
$\forall\boldsymbol{l}$ s.t. $\boldsymbol{l}\neq-\vec{i},\vec{\mp}$ で

$$\frac{\partial G}{\partial n(j)}|_{\boldsymbol{n}^*}=0$$

は 2^p-p-1 本の $\lambda_{\boldsymbol{k}}$ の連立方程式になるが、これがすべて正の解を持てば Kuhn-Tucker 条件を満たす。同じことであるが

$$F=T+\mathrm{Tr}_{\{\boldsymbol{k}\}}\lambda_{\boldsymbol{k}}\mathrm{Tr}_{\{\boldsymbol{l}\leq\boldsymbol{k}\}}((-1)^{|\boldsymbol{k}|+|\boldsymbol{l}|}n(\boldsymbol{l})))$$

として
$\forall\boldsymbol{l}$ s.t. $\boldsymbol{l}\neq-\vec{i},\vec{\mp}$ で

$$\frac{\partial F}{\partial n(j)}|_{\boldsymbol{n}^*}=0$$

が $\lambda_{\boldsymbol{k}}=0$ for $|\boldsymbol{k}|=q$、残りが正の解を持てばよい。

Kuhn-Tucker 条件というのは、各点で目的関数を一次近似した時、制約条件をみたしたままそれ以上目的関数の値を大きくできないことを示している。

実際 Kuhn-Tucker 条件を書き下してみると
$\forall\boldsymbol{l}$s.t. $\boldsymbol{l}\neq-\vec{i},\vec{\mp}$ で

$$\mathrm{Tr}_{\{\boldsymbol{k}\geq\boldsymbol{l}\}}(-1)^{|\boldsymbol{k}|+|\boldsymbol{l}|}\lambda_{\boldsymbol{k}}=(-1)^{p+|\boldsymbol{l}|}\lambda\exp(\lambda\frac{{}_{|\boldsymbol{l}|}C_q}{{}_pC_q})$$

が

$$\lambda_{\boldsymbol{k}}=\begin{cases}0 & (|\boldsymbol{k}|=q)\\ \text{正} & \text{otherwise}\end{cases}\tag{7}$$

なる解を持てばよい。見やすさのために 右辺 (定数) を新しくおき直すと上の連立方程式は
$\forall\boldsymbol{l}$ s.t. $\boldsymbol{l}\neq-\vec{i},\vec{\mp},\forall i=0,\cdots,p-2$ で

$$\begin{aligned}\mathrm{Tr}_{\{\boldsymbol{k}\geq\boldsymbol{l}\}}(-1)^{|\boldsymbol{k}|+|\boldsymbol{l}|}\lambda_{\boldsymbol{k}} &= f_{|\boldsymbol{l}|}\\ f_i &= (-1)^{p+i}\lambda\exp(\lambda\frac{{}_iC_q}{{}_pC_q})\end{aligned}$$

となるが、さらにこれに方程式を付け加えた
$\forall\boldsymbol{l},\forall i=0,\cdots,p-2$ で

$$\begin{aligned}\mathrm{Tr}_{\{\boldsymbol{k}\geq\boldsymbol{l}\}}(-1)^{|\boldsymbol{k}|+|\boldsymbol{l}|}\lambda_{\boldsymbol{k}} &= f_{|\boldsymbol{l}|}\\ f_i &= (-1)^{p+i}\lambda\exp(\lambda\frac{{}_iC_q}{{}_pC_q})\\ f_{p-1} &= \alpha\\ f_p &= \beta\end{aligned}\tag{8}$$

が少なくとも一組の α, β のもとで (8) なる解を持てば十分条件でもとのラグランジュ関数は Kuhn-Tucker 条件を満たす。

ところが式 (9) は $\lambda_{\boldsymbol{k}}$ についてとけて

$$\lambda_{\boldsymbol{k}} = \mathrm{Tr}_{\{\boldsymbol{l} \geq \boldsymbol{k}\}} f_{|\boldsymbol{l}|} = \sum_{j=|\boldsymbol{k}|}^{p} {}_{p-|\boldsymbol{k}|}C_{p-j} f_j$$

となる (付録 C.1)。よって Kuhn-Tucker 条件は

$\forall i = 0, \cdots, p-2, \forall k \neq q$ で

$$\begin{aligned} (-1)^{p+i} \lambda \exp(\lambda \frac{{}_iC_q}{{}_pC_q}) &= f_i \\ \sum_{j=k}^{p-2} {}_{p-k}C_{p-j} f_j + (p-k)\alpha + \beta &> 0 \\ \sum_{j=q}^{p-2} {}_{p-q}C_{p-j} f_j + (p-q)\alpha + \beta &= 0 \end{aligned}$$

となる α, β が少なくとも一組存在することと同値である。最後の式から β を消去して整理すると

$$\begin{aligned} L(k) &= \sum_{j=0}^{p-k} {}_{p-k}C_j (-1)^j \exp(\lambda \frac{{}_{p-j}C_q}{{}_pC_q}) \\ H(k) &= \frac{L(k) - L(q)}{k - q} \end{aligned}$$

とおいて

$$\begin{cases} \alpha > H(k) & (k < q) \\ \alpha < H(k) & (k > q) \end{cases}$$

となる。このような α が存在するためには、十分条件として H が単調増加、さらに十分条件として L が下に凸であればよいことは明らかである。まとめると

$$\hat{L}(k) = L(k+2) - 2L(l+1) - L(k) > 0 \quad \text{for } k = 0, \cdots, p-2$$

ならば $\boldsymbol{n}^*$ は与えられた制約条件のもとで目的関数の最大値を与える一次の条件を満たしていることになる。かなり繁雑な計算の結果

$$\hat{L}(k) = (-1)^{p-k-2} \sum_{j=0}^{p-k-2} {}_{p-k-2}C_j (-1)^j \exp(\lambda \frac{{}_{j+k}C_q}{{}_pC_q})$$

である。これが正になればよい。

ところが式 (1) が任意のパターンの作り方で常に正になることに注目すると、任意の $D_c \geq 0$ で

$$(-1)^b \sum_{a=0}^{b} {}_bC_a (-1)^a \exp(\sum_{c=0}^{a} {}_aC_c D_c) > 0$$

となることがわかる。この左辺は

$$\begin{aligned} a &= j \\ b &= p-k-2 \\ D_c &= \lambda \frac{{}_kC_{q-c}}{{}_pC_q} \end{aligned}$$

とすると $\hat{L}$ と一致する。以上で Kuhn-Tucker 条件が成立していることが証明できた。

C.1 変数変換

まず $\boldsymbol{N}$ と $\boldsymbol{n}$ の変数変換

$$n(\boldsymbol{l}) = \mathrm{Tr}_{\{\boldsymbol{k} \leq \boldsymbol{l}\}}(N(\boldsymbol{k})) \tag{9}$$

の逆変換が

$$N(\boldsymbol{k}) = \mathrm{Tr}_{\{\boldsymbol{l} \leq \boldsymbol{k}\}}((-1)^{|\boldsymbol{k}|+|\boldsymbol{l}|} n(\boldsymbol{l})) \tag{10}$$

となることを証明する。線形変換であるから 2^p 本の互いに異なる単位ベクトル

$$n_{\boldsymbol{l}_0}(\boldsymbol{l}) = \begin{cases} 1 & (\boldsymbol{l} = \boldsymbol{l}_0) \\ 0 & (\boldsymbol{l} \neq \boldsymbol{l}_0) \end{cases}$$

が合成変換 (10)(11) で動かなければよい。変換すると

$$\begin{aligned} n'(\boldsymbol{m}) &= \mathrm{Tr}_{\{\boldsymbol{k} \leq \boldsymbol{m}\}} \mathrm{Tr}_{\{\boldsymbol{l} \leq \boldsymbol{k}\}} (-1)^{|\boldsymbol{k}|+|\boldsymbol{l}_0|} n_{\boldsymbol{l}_0}(\boldsymbol{l}) \\ &= \mathrm{Tr}_{\{\boldsymbol{k} | \boldsymbol{l}_0 \leq \boldsymbol{k} \leq \boldsymbol{m}\}} (-1)^{|\boldsymbol{k}|+|\boldsymbol{l}_0|} \end{aligned}$$

であるが、これは $\boldsymbol{m} = \boldsymbol{l}_0$ のとき 1 、$\boldsymbol{m} \geq \boldsymbol{l}_0$ でないとき 0 が明らかだから $\boldsymbol{m} > \boldsymbol{l}_0$ のとき 0 になることをいえば、逆変換であることの証明になる。$\boldsymbol{m} > \boldsymbol{l}_0$ のとき

$$\begin{aligned} n'(\boldsymbol{m}) &= \mathrm{Tr}_{\{\boldsymbol{k} | \boldsymbol{l}_0 \leq \boldsymbol{k} \leq \boldsymbol{m}\}} (-1)^{|\boldsymbol{k}|+|\boldsymbol{l}_0|} \\ &= (-1)^{|\boldsymbol{l}_0} \sum_{j=|\boldsymbol{l}_0|}^{|\boldsymbol{m}|} (-1)^j \mathrm{Tr}_{\{\boldsymbol{k} | \boldsymbol{l}_0 \leq \boldsymbol{k} \leq \boldsymbol{m}, |\boldsymbol{k}|=j\}} 1 \\ &= \sum_{i=0}^{|\boldsymbol{m}|-|\boldsymbol{l}_0|} (-1)^j {}_{|\boldsymbol{m}|-|\boldsymbol{l}_0|}C_i \\ &= (1 + (-1))^{|\boldsymbol{m}|-|\boldsymbol{l}_0|} = 0 \end{aligned}$$

で、変換 (10) と (11) は互いに逆変換であることがいえた。ただし最後の式は二項定理から導いた。

これを利用すると式 (9) もとける。

$$\mathrm{Tr}_{\{\boldsymbol{k} \geq \boldsymbol{l}\}} \lambda_{\boldsymbol{k}} (-1)^{|\boldsymbol{k}|+|\boldsymbol{l}|} = f_{\boldsymbol{l}}$$

$$\updownarrow$$

$$\mathrm{Tr}_{\{\boldsymbol{k} | -\boldsymbol{k} \leq -\boldsymbol{l}\}} \lambda_{-(-\boldsymbol{k})} (-1)^{p-|-\boldsymbol{k}|+p-|-\boldsymbol{l}|} = f_{-(-\boldsymbol{l})}$$

$$\updownarrow$$

$$\mathrm{Tr}_{\{\boldsymbol{k}' \leq \boldsymbol{l}'\}} \lambda_{-\boldsymbol{k}'} (-1)^{|\boldsymbol{k}'|+|\boldsymbol{l}'|} = f_{-\boldsymbol{l}'}$$

これの逆変換は今導いたばかりでしっているので

$$\begin{aligned} \lambda_{-\boldsymbol{k}'} &= \mathrm{Tr}_{\{\boldsymbol{l}' \leq \boldsymbol{k}'\}} f_{-\boldsymbol{l}'} \\ &= \mathrm{Tr}_{\{\boldsymbol{l}' | -\boldsymbol{l}' \geq -\boldsymbol{k}'\}} f_{-\boldsymbol{l}'} \\ &= \mathrm{Tr}_{\{\boldsymbol{l} \geq -\boldsymbol{k}'\}} f_{-\boldsymbol{l}} \end{aligned}$$

これが任意の $\boldsymbol{k}'$ で成立するのだから

$$\lambda_{\boldsymbol{k}} = \mathrm{Tr}_{\{\boldsymbol{l} \geq \boldsymbol{k}\}} f_{-\boldsymbol{l}}$$

が成立し、式 (9) が解けた。