数理解析研究所講究録
第833巻 1993年 42-52

ϵ-偏りの確率変数と ϵ-依存の確率変数の間の関係について
On Relationship between ϵ-biased Random Variables and ϵ-dependent Random Variables

東北大·工·情報 神保 秀司 (Shuji Jimbo)
東北大·工·情報 丸岡 章 (Akira Maruoka)

1 まえがき

確率アルゴリズムで使われる無作為抽出は確率変数と看做せる. 例えば, アルゴリズム中で $\{0,1\}$ の中から一様に n ビットを選ぶ無作為抽出は $\{0,1\}$ の中の値を取る n 個の独立な確率変数系 $x_1,\ldots,x_n$ で各確率変数 x_i の分布が全て一様, つまり,

$$\Pr[x_i=0]=\Pr[x_i=1]=\frac{1}{2}$$

となっているものと看做せる.

アルゴリズム中でランダムな n 個のビットが要求される場合は一様分布の n 個の独立確率変数系と看做すことが多いが, 実際にはしばしばより弱い性質を持った確率変数系と看做しても問題が無いことがある. そのような, 確率変数系 $x_1,\ldots,x_n$ に要求される独立性に関する弱い性質として **k-限定 ϵ-依存**と **k-限定 ϵ-偏り**がある. ただし, k は $1\leq k\leq n$ を満足する整数, $0\leq\epsilon\leq 1/2$ とする.

これらの独立性に関する弱い性質を持つ確率変数系の利点の一つは, その定義域となる確率空間の標本空間のサイズの小さいものが存在するという点である. もし, 標本空間のサイズが十分小さければ, その標本空間に属する全ての値に対して必要な処理を施すことによって, その確率変数系を用いる確率アルゴリズムを実用性をそれほど失うこと無く決定性のものに変更できる. この方向での最近の結果として, [NN90], [LV91] がある.

本論文の主結果は, k,n を $1\leq k\leq n$ を満足する整数として, 確率変数系 $\{x_1,\ldots,x_n\}$ が k-限定 ϵ-偏りならば, 最大値ノルムの意味で k-限定 $4(1-2^{-k})\epsilon$-依存であり, かつ最大値ノルムの意味で, 一様分布に関して k-限定 $2(1-2^{-k})\epsilon$-依存であるというものである.

関連する従来の結果として, [NN90], [AGHP90] では次の点が指摘されている.

1. 確率変数系 $(X_1,\ldots,X_n):\Omega\to\{0,1\}^n$ が n-限定 $\epsilon/2$-偏りならば, 任意の $1\leq k\leq n$ に対して,
   (a) 最大値ノルムの意味で, 一様分布に関して k-限定 ϵ-依存であり,
   (b) L_1 ノルムの意味で, 一様分布に関して k-限定 $2^k\epsilon$-依存である.
2. k,n を $1\leq k\leq n$ を満足する整数として, 確率変数系 $(X_1,\ldots,X_n):\Omega\to\{0,1\}^n$ が k-限定 $\epsilon/2$-偏りならば, L_1 ノルムの意味で, 一様分布に関して k-限定 $2^k\epsilon$-依存である.

従って, 本論文の結果によって, 最大値ノルムの意味で k-限定 δ-依存の確率変数系を要求する確率アルゴリズムを決定性のものに変更するような状況下で変更後のアルゴリズムの効率化が期待できるようになった. なぜなら, 従来, k-限定 δ-依存の確率変数を構成するために k-限定 ϵ-偏りの確率変数を転用していたからである ([NN90], [LV91]) .

2. では, 確率空間と確率変数に関する基本的な概念の定義を与える. **3.** では, 本論文の主結果を証明する. **4.** では, 本論文の結果の具体的な応用例として, [LV91] で扱われた問題: DNF 式を充足する変数への割当の

個数の全体の個数 (変数の個数を n として 2^n) に対する割合の近似値を求める問題, を解く決定性アルゴリズムの効率化を紹介する.

2 準備

定義 1 有限集合 A に対して, $\sum_{x\in A} D(x) = 1$ を満足する関数 $D : A \to [0,1]$ を A 上の確率分布と呼ぶ. □

$(\Omega, \mathcal{F}, \Pr)$ は確率空間, $f : \Omega \to S$ は確率変数とする. $D(s) = \Pr[\{\omega \in \Omega \mid f(\omega) = s\}]$ によって定義される関数 $D : S \to [0,1]$ は確率変数 f の分布であると言われる. S の部分集合 T に対しては $D(T) = \Pr[\{\omega \in \Omega \mid f(\omega) \in T\} = \sum_{s\in T} D(s)$ と定義する. また, 同一の確率空間を定義域とする複数の確率変数がある場合, それらを一まとめにして**確率変数系**と呼ぶことがある. $\{0,1\}$ の中の値を取る確率変数系 $x_1, \ldots, x_k$ の結合分布とは,

$$D(a_1, \ldots, a_k) = \Pr[x_1 = a_1 \wedge \ldots \wedge x_k = a_k]$$

を満足する関数 $D : \{0,1\}^k \to [0,1]$ のことである.

定義 2 $\{x_1, \ldots, x_n\}$ を $\{0,1\}$ の中の値を取る確率変数系, $k \le n$ は正整数かつ $0 \le \epsilon \le 1/2$ とする. $S, s_1, \ldots, s_j, j, \sigma, \sigma_1, \ldots, \sigma_j$ の動く範囲は, $S = \{s_1, \ldots, s_j\} \subseteq \{1, \ldots, n\}$, $s_1 < \ldots < s_j$, $j \le k$, $\sigma = (\sigma_1, \ldots, \sigma_j) \in \{0,1\}^j$ とする. さらに,

$$\Delta_A(S,\sigma) = \left|\Pr[x_{s_1} = \sigma_1 \wedge \cdots \wedge x_{s_j} = \sigma_j] - \Pr[x_{s_1} = \sigma_1] \cdots \Pr[x_{s_j} = \sigma_j]\right| ,$$

$$\Delta_B(S,\sigma) = \left|\Pr[x_{s_1} = \sigma_1 \wedge \cdots \wedge x_{s_j} = \sigma_j] - \frac{1}{2^j}\right|$$

と表す. $\{x_1, \ldots, x_n\}$ は,

$$(\forall S)(\forall \sigma)\,(\Delta(S,\sigma) \le \epsilon)$$

が成立するとき**最大値ノルムの意味で k-限定 ϵ-依存**であると言い,

$$(\forall S)\left(\sum_{\sigma} \Delta(S,\sigma) \le \epsilon\right)$$

が成立するとき L_1 **ノルムの意味で k-限定 ϵ-依存**であると言う. ただし, 定義式の中の Δ は Δ_A または Δ_B を表すものとする. Δ が Δ_A なのか, それとも Δ_B なのかを区別するためにΔ が Δ_B の場合は**一様分布に関して k-限定 ϵ-依存**であると言う. □

定義 3 $\{x_1, x_2, \ldots, x_n\}$ は $\{0,1\}$ の中の値を取る確率変数系, k, n は $1 \le k \le n$ を満足する整数, $0 \le \epsilon \le 1/2$ とする. $S, s_1, \ldots, s_j, j, \sigma, \sigma_1, \ldots, \sigma_j$ の動く範囲は, $S = \{s_1, \ldots, s_j\} \subseteq \{1, \ldots, n\}$, $s_1 < \ldots < s_j$, $j \le k$ とする. $\{x_1, \ldots, x_n\}$ は

$$(\forall S)\left(\left|\Pr[x_{s_1} \oplus \cdots \oplus x_{s_j} = 0] - \frac{1}{2}\right| \le \epsilon\right)$$

が成立するとき k-**限定 ϵ-偏り**であると言う. ただし, $\oplus$ は排他的論理和の演算を表す. □

上記の k-限定 ϵ-偏りの定義の中の$\left|\Pr[x_{s_1} \oplus \cdots \oplus x_{s_j} = 0] - \frac{1}{2}\right| \le \epsilon$ は, [NN90] では,

$$\left|\Pr[x_{s_1} \oplus \cdots \oplus x_{s_j} = 0] - \Pr[x_{s_1} \oplus \cdots \oplus x_{s_j} = 1]\right| \le \epsilon$$

と定義されているが, この意味で k-限定 ϵ-偏りであることは本論文の意味では k-限定 $(\epsilon/2)$-偏りとなり特に異なる概念を表しているものではない.

従来の文献に見られる k-限定 ϵ-依存の概念には幾つかの変種があり, それらを整理する為に, 最大値ノルムの意味でのものと L_1 ノルムの意味でのものの 2 種類に分類し, またそれとは別の観点から, 一様ノルムに関するものとそうでないものの 2 種類に分類した. 例えば, [LV91] では最大値ノルムの意味での k-限定 ϵ-依存の概念が使われ, [NN90] では L_1 ノルムの意味でかつ一様分布に関しての k-限定 ϵ-依存の概念が使われている.

定義から, 確率変数系が k-限定 ϵ-依存であるかどうか, あるいは k-限定 ϵ-偏りであるかどうかはその定義域となる確率空間とは無関係に分布だけで決まる点に注意されたい.

3 確率変数における偏りと依存の間の関係

本論文では, 正整数 m に対して $[m] = \{1, \ldots, m\}$ と表し, 有限集合 S に対して 2^S で S のベキ集合, つまり S の部分集合全体からなる集合を表す. 以下では, 正整数 n を固定し, $X = 2^{[n]}$ とおく. さらに, X と $\{0,1\}^n$ の間の自然な 1 対 1 の対応に従ってこれら二つの集合を同一視する. つまり, 各 $(a_1, \ldots, a_n) \in \{0,1\}^n$ と $\{i \in [n] \mid a_i = 1\} \in 2^{[n]}$ を同一視する. さらに, 次に述べる定義に従って, X を定義域とし $\boldsymbol{R}$ の中の値を取る関数全体の集合 $\boldsymbol{R}^X$ に内積を導入し, $\boldsymbol{R}^X$ を X を添字の集合とする 2^n 次元ユークリッドベクトル空間と考える.

定義 4 $f, g \in \boldsymbol{R}^X$ に対して f と g の内積 $\langle f, g \rangle$ を $\langle f, g \rangle = \sum_{x \in X} f(x)g(x)$ と定義する. □

$I \in X$ に対して $\lambda_I : X \to \boldsymbol{R}$ を

$$\lambda_I(x) = \begin{cases} 1 & (x = I \text{ の場合}) \\ 0 & (x \neq I \text{ の場合}) \end{cases}$$

と定義すれば, $\{\lambda_I\}_{I \in X}$ は, 明らかに $\boldsymbol{R}^X$ の正規直交基底となる.

また, $I \in X$ に対して $\chi_I : X \to \boldsymbol{R}$ を

$$\chi_I(x) = \begin{cases} 1 & (|x \cap I| \equiv 0 \pmod 2 \text{ の場合}) \\ -1 & (|x \cap I| \equiv 1 \pmod 2 \text{ の場合}) \end{cases}$$

と定義すれば, $\{2^{-n/2}\chi_I\}_{I \in X}$ は $\boldsymbol{R}^X$ の正規直交基底となる. これは次のようにして示される.

任意の $I \in X$ に対して $\|\chi_I\| = 2^{n/2}$ が成立することは明らかであるので, $A \neq B$ を満足する $A \in X, B \in X$ を任意に選んだとき,

$$\langle \chi_A, \chi_B \rangle = 0$$

となることを示せば十分である. A, B をこのように選んだとき, χ_A, χ_B の定義から

$$\langle \chi_A, \chi_B \rangle = |\{x \in X : |x \cap A| \equiv |x \cap B| \pmod 2\}| - |\{x \in X : |x \cap A| \not\equiv |x \cap B| \pmod 2\}|$$

が成立する. A と B の対称差を $A \triangle B = (A \setminus B) \cup (B \setminus A)$ とおけば, $A \triangle B \neq \emptyset$ であり, さらに,

$$\{x \in X : |x \cap A| \equiv |x \cap B| \pmod 2\} = \{x \in X : |x \cap (A \triangle B)| \equiv 0 \pmod 2\}$$

かつ

$$\{x \in X : |x \cap A| \not\equiv |x \cap B| \pmod 2\} = \{x \in X : |x \cap (A \triangle B)| \equiv 1 \pmod 2\}$$

が成立する. 従って, 一般に空でない有限集合 S に対して, 偶数サイズの S の部分集合の個数と奇数サイズの S の部分集合の個数が等しいことから,

$$\langle \chi_A, \chi_B \rangle = |\{x \in X : |x \cap (A \triangle B)| \equiv 0 \pmod 2\}| - |\{x \in X : |x \cap (A \triangle B)| \equiv 1 \pmod 2\}| = 0$$

が導かれる.

定義 5 $K \subseteq I \in X$ を満足する有限集合 K, I に対して,

$$R(I,K) = \{x \in X : x \cap I = K\}$$

と定義する. □

D は $\{0,1\}$ の中の値を取る確率変数系 $\{x_1, \ldots, x_n\}$ の結合分布を X 上の確率分布と看做したもの, $s_1, \ldots s_j$ は $1 \leq s_1 < \cdots < s_j \leq n$ を満足する整数, $S = \{s_1, \ldots, s_j\}$, $\sigma = (\sigma_1, \ldots, \sigma_j) \in \{0,1\}^j$, $j \leq n$ とする. このとき, $\sigma = \{s_i \mid i \in \{1, \ldots, j\} \wedge \sigma_i = 1\} \subseteq S$ と看做せば, 定義 2 と定義 5 より,

$$\Delta_B(S,\sigma) = \left| \left(\sum_{x \in R(S,\sigma)} D(x) \right) - \frac{1}{2^{|S|}} \right| \text{ および } \Delta_A(S,\sigma) = \left| \left(\sum_{x \in R(S,\sigma)} D(x) \right) - \prod_{y \in S} \left(\sum_{z \in R(\{y\}, \sigma \cap \{y\})} D(z) \right) \right|$$

が成立する.

補題 1 k は高々 n の正整数, $D \in \boldsymbol{R}^X$ は X 上の確率分布とし,

$$(\forall A \in X)(1 \leq |A| \leq k \Rightarrow |\langle D, \chi_A \rangle| \leq 2\epsilon) \tag{1}$$

を満足すると仮定する. このとき, $1 \leq |I| \leq k$ および $K \subseteq I$ を満足する任意の $I \in X$, $K \in X$ に対して,

$$\left| \left\langle D, \left(\sum_{x \in R(I,K)} \lambda_x \right) - \frac{1}{2^{|I|}} \chi_\emptyset \right\rangle \right| \leq 2 \left(1 - \frac{1}{2^{|I|}} \right) \epsilon$$

が成立する.

(証明) $\sum_{x \in R(I,K)} \lambda_x$ は $\{\chi_A\}_{A \in 2^I}$ の張る部分空間に属することが次のようにして示される. $B \in X$ を任意に選んで $B \setminus I \neq \emptyset$ と仮定すれば, 一般に空でない有限集合 S に対して, 偶数サイズの S の部分集合の個数と奇数サイズの S の部分集合の個数が等しいことから以下の等式が導かれる.

$$\begin{aligned}
\left\langle \chi_B, \sum_{x \in R(I,K)} \lambda_x \right\rangle &= \sum_{x \in R(I,K)} \langle \chi_B, \lambda_x \rangle \\
&= |\{x \in R(I,K) : |x \cap B| \equiv 0 \pmod 2\}| - |\{x \in R(I,K) : |x \cap B| \equiv 1 \pmod 2\}| \\
&= |2^{(B \cup I)^C}| \Big(|\{x \in 2^{(B \setminus I)} : |x| \equiv |K \cap B| \pmod 2\}| \\
&\quad - |\{x \in 2^{(B \setminus I)} : |x| \not\equiv |K \cap B| \pmod 2\}| \Big) = 0 .
\end{aligned}$$

さらに, $\{2^{-n/2} \chi_I\}_{I \in X}$ が $\boldsymbol{R}^X$ の正規直交基底であることから

$$\sum_{x \in R(I,K)} \lambda_x = 2^{-n} \sum_{A \in 2^I} \left\langle \sum_{x \in R(I,K)} \lambda_x, \chi_A \right\rangle \chi_A$$

と展開できる.

このことと

$$\left\langle \sum_{x\in R(I,K)} \lambda_x, \chi_\emptyset \right\rangle = \sum_{x\in R(I,K)} \langle \lambda_x, \chi_\emptyset \rangle = |R(I,K)| = 2^{n-|I|}$$

から

$$\left(\sum_{x\in R(I,K)} \lambda_x \right) - \frac{1}{2^{|I|}}\chi_\emptyset = 2^{-n} \sum_{A\in 2^I\setminus\{\emptyset\}} \left\langle \sum_{x\in R(I,K)} \lambda_x, \chi_A \right\rangle \chi_A \,.$$

が成立する. 従って, D に対する条件 (1) より,

$$\begin{aligned}
\left| \left\langle D, \left(\sum_{x\in R(I,K)} \lambda_x \right) - \frac{1}{2^{|I|}}\chi_\emptyset \right\rangle \right| &= \left| \left\langle D, 2^{-n} \sum_{A\in 2^I\setminus\{\emptyset\}} \left\langle \sum_{x\in R(I,K)} \lambda_x, \chi_A \right\rangle \chi_A \right\rangle \right| \\
&= 2^{-n} \left| \sum_{A\in 2^I\setminus\{\emptyset\}} \left(\langle D, \chi_A \rangle \sum_{x\in R(I,K)} \langle \lambda_x, \chi_A \rangle \right) \right| \\
&\le 2^{-n} \sum_{A\in 2^I\setminus\{\emptyset\}} \left(|\langle D, \chi_A \rangle| \left| \sum_{x\in R(I,K)} \langle \lambda_x, \chi_A \rangle \right| \right) \\
&\le 2^{-n} 2\epsilon \sum_{A\in 2^I\setminus\{\emptyset\}} \left| \sum_{x\in R(I,K)} \langle \lambda_x, \chi_A \rangle \right| \\
&= 2^{-n} 2\epsilon \sum_{A\in 2^I\setminus\{\emptyset\}} \left| |R(I,K)\cap \chi_A^{-1}(1)| - |R(I,K)\cap \chi_A^{-1}(-1)| \right| .
\end{aligned}$$

ただし, χ_A^{-1} は χ_A の逆関数を表す.

任意の $A \subseteq I$ に対して, $A \neq \emptyset$ ならば $R(I,K) \subseteq \chi_A^{-1}(1)$ または $R(I,K) \subseteq \chi_A^{-1}(-1)$ のいずれか一方のみが必ず成立するので,

$$\begin{aligned}
&2^{-n} 2\epsilon \sum_{A\in 2^I\setminus\{\emptyset\}} \left| |R(I,K)\cap \chi_A^{-1}(1)| - |R(I,K)\cap \chi_A^{-1}(-1)| \right| \\
&\qquad = 2^{-n} 2\epsilon \left(2^{|I|} - 1 \right) |R(I,K)| = 2^{-n} 2\epsilon \left(2^{|I|} - 1 \right) 2^{n-|I|} = 2\left(1 - \frac{1}{2^{|I|}} \right) \epsilon \,.
\end{aligned}$$

従って, 補題 1 は証明された. □

系 1 $0 \le \epsilon \le 1/2$ かつ k は高々 n の正整数とする. $\{0,1\}$ の中の値を取る確率変数系 $\{x_1,\ldots,x_n\}$ が k-限定 ϵ-偏りならば $\{x_1,\ldots,x_n\}$ は最大値ノルムの意味で一様分布に関して k-限定 $2\left(1-\frac{1}{2^k}\right)\epsilon$-依存である.

(証明) 定義から, $\{x_1,\ldots,x_n\}$ が k-限定 ϵ-偏りであることは, D をその結合分布として,

$$(\forall A \in X)(1 \le |A| \le k \Rightarrow |\langle D, \chi_A \rangle| \le 2\epsilon)$$

と同値であり, 従って, 補題 1 より, これを仮定すれば $1 \le |I| \le k, K \subseteq I$ を満足する任意の $I \in X, K \in X$ に対して,

$$\Delta_B(I,K) = \left| \left(\sum_{x\in R(I,K)} D(x) \right) - \frac{1}{2^{|I|}} \right| = \left| \left\langle D, \left(\sum_{x\in R(I,K)} \lambda_x \right) - \frac{1}{2^{|I|}}\chi_\emptyset \right\rangle \right| \le 2\left(1-\frac{1}{2^{|I|}}\right)\epsilon \le 2\left(1-\frac{1}{2^k}\right)\epsilon$$

が導かれる. これは, $\{x_1,\ldots,x_n\}$ が最大値ノルムの意味で一様分布に関して k-限定 $2\left(1-\frac{1}{2^k}\right)\epsilon$-依存であることを表している. □

定理 1 $0 \leq \epsilon \leq 1/2$ かつ k は高々 n の正整数とする. $\{0,1\}$ の中の値を取る確率変数系 $\{x_1,\ldots,x_n\}$ が k-限定 ϵ-偏りならば $\{x_1,\ldots,x_n\}$ は最大値ノルムの意味で k-限定 $4\left(1-\frac{1}{2^k}\right)\epsilon$-依存である.

(証明) $1 \leq |I| \leq k$ を満足する $I \in X = 2^{[n]}$ と $J \in X$ を任意に選ぶ. 補題 1 と $\{x_1,\ldots,x_n\}$ が k-限定 ϵ-偏りであるという仮定から, D をその結合分布として,

$$\left|\left(\sum_{x\in R(I,K)} D(x)\right) - \frac{1}{2^{|I|}}\right| = \left|\left\langle D, \left(\sum_{x\in R(I,K)} \lambda_x\right) - \frac{1}{2^{|I|}}\chi_\emptyset\right\rangle\right| \leq 2\left(1-\frac{1}{2^{|I|}}\right)\epsilon$$

が成立し, 従って,

$$\frac{1}{2^{|I|}} - 2\left(1-\frac{1}{2^{|I|}}\right)\epsilon \leq \sum_{x\in R(I,J\cap I)} D(x) \leq \frac{1}{2^{|I|}} + 2\left(1-\frac{1}{2^{|I|}}\right)\epsilon$$

および,

$$(\forall x \in I)\left(\frac{1}{2} - \epsilon \leq \sum_{x\in R(\{x\},J\cap\{x\})} D(x) \leq \frac{1}{2} + \epsilon\right)$$

が成立する. 従って,

$$\begin{aligned}\frac{1}{2^{|I|}} - 2\left(1-\frac{1}{2^{|I|}}\right)\epsilon - \left(\frac{1}{2}+\epsilon\right)^{|I|} &\leq \left(\sum_{x\in R(I,J\cap I)} D(x)\right) - \prod_{y\in I}\left(\sum_{z\in R(\{y\},J\cap\{y\})} D(z)\right) \\ &\leq \frac{1}{2^{|I|}} + 2\left(1-\frac{1}{2^{|I|}}\right)\epsilon - \left(\frac{1}{2}-\epsilon\right)^{|I|} \qquad (2)\end{aligned}$$

が成立する. $0 \leq \epsilon \leq 1/2$ に注意されたい. 従って, 不等式 (2) より次の不等式が導かれ定理 1 の証明は完了する.

$$\begin{aligned}\Delta_A(I, J\cap I) &= \left|\left(\sum_{x\in R(I,J\cap I)} D(x)\right) - \prod_{y\in I}\left(\sum_{z\in R(\{y\},J\cap\{y\})} D(z)\right)\right| \\ &\leq \max\left\{\left|\frac{1}{2^{|I|}} - 2\left(1-\frac{1}{2^{|I|}}\right)\epsilon - \left(\frac{1}{2}+\epsilon\right)^{|I|}\right|, \left|\frac{1}{2^{|I|}} + 2\left(1-\frac{1}{2^{|I|}}\right)\epsilon - \left(\frac{1}{2}-\epsilon\right)^{|I|}\right|\right\} \\ &= \max\left\{\left(\sum_{i=1}^{|I|}\frac{1}{2^{|I|-i}}\binom{|I|}{i}\epsilon^i\right) + 2\left(1-\frac{1}{2^{|I|}}\right)\epsilon, \left(\sum_{i=1}^{|I|}\frac{1}{2^{|I|-i}}\binom{|I|}{i}(-1)^{i-1}\epsilon^i\right) + 2\left(1-\frac{1}{2^{|I|}}\right)\epsilon\right\} \\ &= 2\left(1-\frac{1}{2^{|I|}}\right)\epsilon + \sum_{i=1}^{|I|}\left(\frac{1}{2^{|I|-i}}\binom{|I|}{i}\epsilon^i\right) \leq 2\left(1-\frac{1}{2^{|I|}}\right)\epsilon + \sum_{i=1}^{|I|}\left(\frac{1}{2^{|I|-i}}\binom{|I|}{i}\left(\frac{1}{2}\right)^i 2\epsilon\right) \\ &= 2\left(1-\frac{1}{2^{|I|}}\right)\epsilon + \frac{2\epsilon}{2^{|I|}}\sum_{i=1}^{|I|}\binom{|I|}{i} = 2\left(1-\frac{1}{2^{|I|}}\right)\epsilon + \frac{2\epsilon}{2^{|I|}}\left(2^{|I|}-1\right) = 4\left(1-\frac{1}{2^{|I|}}\right)\epsilon.\end{aligned}$$

□

4 ϵ-偏りの確率変数の応用

十分小さい ϵ に対する k-限定 ϵ-依存の確率変数の組が k-限定独立な確率変数の組の代用となる例を挙げ, 本論文の前節までに導かれた結果がどのように活用されるかを見る. その例は, [LV91] で研究された, DNF 式を充足する, 変数への値の割り当ての割合の近似評価方法に関するものである.

F は m 個の項を持つ n 変数の DNF 式とする. 通常の方法で, F を $\{0,1\}^n$ から $\{0,1\}$ への関数と看做すことができる. F を充足する変数への値の割り当ての割合は次の値である:

$$\Pr[F(x_1,\ldots,x_n)=1]=\frac{|\{x\in\{0,1\}^n \mid F(x)=1\}|}{|\{0,1\}^n|}=\frac{1}{2^n}|\{x\in\{0,1\}^n \mid F(x)=1\}|.$$

この式の中の $\{x_1,\ldots,x_n\}$ は, それぞれ, 分布が一様な, つまり, 各 $i=1,\ldots,n$ に対して, $\Pr[x_i=0]=\Pr[x_i=1]=1/2$ を満足する独立確率変数系である. $x=(x_1,\ldots,x_n)$ とおく. この $\Pr[F(x)=1]$ を正確に計算する問題は, Valiant [Val79] によって, #P 完全であることが示されているので, 現在この問題を解決することは大変困難であると考えられている. [LV91] では, 確率アルゴリズムを確定的なアルゴリズムに変形した形の $\Pr[F(x)=1]$ の近似値を計算するアルゴリズムを紹介している. その近似値を Y としたとき, 真の値 $\Pr[F(x)=1]$ との誤差は

$$(1-\delta)\Pr[F(x)=1]-\epsilon\le Y\le\Pr[F(x)=1]+\epsilon$$

の形で評価される. 与えられた引数 δ および ϵ に対して, この許容範囲に入る近似値 Y を計算するための時間を如何に短くするかが問題となる. [LV91] に詳しく書かれているアルゴリズムは 2-限定独立な確率変数系と, 適当な l に対する l-限定独立な確率変数系を用いている. しかし, 適当な $\theta>0$ を選んで, l-限定 θ-依存の確率変数系を用いる方法も言及されていて, 実際, その方法を用いるとより計算時間の短いアルゴリズムが得られた. なお, どちらの方法の場合でも, 評価された計算時間の上界は引数 n, m, δ および ϵ の多項式を超えるものになっていることに注意する必要がある.

4.1 アルゴリズムの概要

以下, 近似値を計算するアルゴリズムの概要を述べる. このアルゴリズムは [LV91] のものを次の二つの点に関して改良したものである. 一つ目は, ある整数 k に対する k-限定独立な確率変数系の替わりにある正の値 ϵ に対する k-限定 ϵ-依存の確率変数系を用いている点である. 二つ目は, 変数の色付を値とする確率変数を実現する場合, その確率変数に対して要求する性質が異なる点である. [LV91] のアルゴリズムでは, δ-良性 (原文では "δ-good") と呼ばれる性質を持つように実現したが, 本論文では, (δ,c)-良性と呼ばれる性質を持つように実現する. (δ,c)-良性に関しては後の節で述べる. これらの改良に関しては [LV91] で言及されているが, その改良による具体的な影響に関しては述べられていない.

なお, 記述中の変数 $t,c,k=2^\nu,\eta,l,\theta$ は, $n,m,1/\delta$ および $1/\theta$ の値に基いて, 予め設定される.

1. F の項で長さが t より大きいものを除去し, DNF 式 G を作る.

2. 変数の集合上の色付けの類 $\mathcal{C}$ を次のように定義する. $\eta>0$ ならびに整数 $c, 1\le c\le t$, および $\nu\ge 0$ は予め設定されている. $k=2^\nu$ とおく. 最大値ノルムの意味で, 一様分布に関して $(c+1)\nu$-限定 η-依存の νn 個の確率変数の系 $\{b_1,b_2,\ldots,b_{\nu n}\}$ を定め, それらを添え字の順に ν 個ずつ連結して, $k=2^\nu$ 色中の一色を表す n 個のベクトル $c_1=(b_1,\ldots,b_\nu),\ldots,c_n=(b_{n-\nu+1},\ldots,b_n)$ を作り, $f=(c_1,\ldots,c_n)$ とおく. $f=(c_1,\ldots,c_n)$ は n 個の変数の色付の一つを値として取る確率変数である. f の取り得る全ての色付からなる類を $\mathcal{C}$ と表し, f の定義域となっている標本空間を $\Omega^{\mathcal{C}}$ と表す.

3. 各 $g\in\mathcal{C}$ および各 $i=1,\ldots,k$ に対して, X_i^g で色付 g により色 i が付けられた変数の集合を表す. 最大値ノルムの意味で, 一様分布に関して l-限定 θ-依存の $|X_i^g|$ 個の確率変数の系 $\mathcal{X}_i^g$ を実現し, その系に属する確率変数を X_i^g に属する DNF 式の変数に対応させる. $\mathcal{X}_i^g$ は $\{0,1\}^{X_i^g}$ の中の値を取る単一の確率変数と看做せる. このように看做したとき, $\{\mathcal{X}_1^g,\ldots,\mathcal{X}_k^g\}$ が独立確率変数系となるように, $\mathcal{X}_1^g,\ldots,\mathcal{X}_k^g$ を

実現する. このようにして得られた n 個の確率変数の系を $\mathcal{X}^g$ と表す. $\mathcal{X}^g$ の定義域となる標本空間 Ω^g は有限集合となるようにできる.

4. DNF 式 G と色付 g に対して, G を g で色付したとき, どの色も高々 c 色しか現れない G の項からなる DNF 式を G_g と表す. f の各標本点 $\tau \in \Omega^C$ と, $|\Omega^{f(\tau)}|$ 個の標本点 $\omega \in \Omega^{f(\tau)}$ の全ての組 (τ, ω) に対して, $G_{f(\tau)}$ と $x = \mathcal{X}^{f(\tau)}(\omega)$ を求め, さらに, $G_{f(\tau)}(x) = 1$ かどうかを判定することによって, 各 $\tau \in \Omega^C$ に対する

$$Y_\tau = \Pr[\{\omega \in \Omega^{f(\tau)} \mid G_{f(\tau)}(\mathcal{X}^{f(\tau)}(\omega)) = 1\}]$$

を計算する.

$$Y = \max_{\tau \in \Omega^C} Y_\tau$$

がこのアルゴリズムの返す近似値である.

4.2 アルゴリズムの実行時間の評価

アルゴリズムの変数 t, c, k, η, l, θ の設定と与えられた k, ϵ に対する k-限定 ϵ-依存の確率変数の実現方法を明確にすればアルゴリズムは具体的なものとなる. さらに, アルゴリズムが正しく動作する為には, 計算された近似値 Y が許容範囲に入っていなくてはならない. このことを保証する為に, 変数 t, c, k, η, l, θ の設定方法にある制限が付く. この制限に関しては, 後の節で述べる.

以下では, 本論文の前節までの結果がこのアルゴリズムの実行時間の減少にどのように効果があるかを見る為に, 変数 t, c, k, η, l, θ に対して求まるアルゴリズムの実行時間の上界が, 本論文の結果を利用した場合としない場合でどのように異なるかを見る.

明らかに, 概要の 1 の動作は n と m に関する多項式時間で可能である. また, 2 あるいは 3 に現れる各確率変数に対して, その確率変数の標本空間中の標本点を一つずつ逐次発生する為の時間, 確率変数の値を標本点から計算する為の時間およびそれらの計算を容易にする為の前処理の時間は, [NN90] あるいは [AGHP90] で紹介された方法を用いることにより, 全て $n, m, c, \nu, 1/\eta, l$ および $1/\theta$ の多項式時間で可能である. 変数 t, c, k, η, l, θ の設定を工夫することにより, これらの時間は $n, m, 1/\delta$ および $1/\epsilon$ の多項式時間になるようにできる. 従って, 概要の 4 において調べるべき (τ, ω) の組の個数が $\sum_{\tau \in \Omega^C} |\Omega^{f(\tau)}|$ であるので, $n, m, 1/\delta$ および $1/\epsilon$ を引数とする二つの多項式 P_1 および P_2 を用いて, アルゴリズムの実行時間は,

$$P_1(n, m, 1/\delta, 1/\epsilon) + P_2(n, m, 1/\delta, 1/\epsilon) \sum_{\tau \in \Omega^C} |\Omega^{f(\tau)}| \tag{3}$$

と表すことができる. 従って, $P_3 = P_1 + P_2$ とおけば,

$$P_3(n, m, 1/\delta, 1/\epsilon) \sum_{\tau \in C} |\Omega^{f(\tau)}| \tag{4}$$

はアルゴリズムの実行時間の上界となる. なお, 本論文の方法では, 式 (4) の中の $\sum_{\tau \in \Omega^C} |\Omega^{f(\tau)}|$ が多項式で上から抑えられるようにはできていない.

上記の P_1 および P_2 は, 本論文の結果を利用する場合としない場合でそれほど違わないと考えられるので, $\sum_{f \in C} |\Omega^f|$ がどのように異るかを見ることによって実行時間の違いを概略的に知ることができる.

[AGHP90] によると, $\{0, 1\}$ の中の値を取る, 最大値ノルムの意味で, 一様分布に関して k-限定 ϵ-偏りの n 個の確率変数の組を作り, その標本空間のサイズが高々 $\left(\frac{k\lceil \log_2 n \rceil}{2\epsilon}\right)^2$ となるようにできる. さらに, [NN90]

では, BCH 符号の理論を用いて, 任意の正整数 k と m に対して, ϵ-偏りの km 個の確率変数の系を k-限定 ϵ-偏りの 2^m 個の確率変数の系に変形する方法が紹介されている. その方法は, 有限体 $GF(2)$ を成分とする適当な $km \times 2^m$ 行列を掛けるというものである. これらの結果と本論文の結果から, $\{0,1\}$ の中の値を取る, 最大値ノルムの意味で, 一様分布に関して k-限定 ϵ-依存の n 個の確率変数の系を作り, その標本空間のサイズが高々 $\left(\frac{k\lceil\log_2 n\rceil}{\epsilon}\right)^2$ となるようにできる. 一方, [LV91] あるいは [NN90] にある依存と偏りに関する記述では $\{0,1\}$ の中の値を取る, 最大値ノルムの意味で, 一様分布に関して k-限定 ϵ-偏りの確率変数系は最大値ノルムの意味で, 一様分布に関して k-限定 $2^k\epsilon$-依存であることだけを保証している. 従って, 上記と同様の n 個の確率変数の系の標本空間のサイズの上界は $2^{2k}\left(\frac{k\lceil\log_2 n\rceil}{\epsilon}\right)^2$ である. 以上から, $\{0,1\}$ の中の値を取る, 最大値ノルムの意味で, 一様分布に関して k-限定 ϵ-依存の n 個の確率変数の系を作った場合の標本空間のサイズの上界の評価値は, [LV91] あるいは [NN90] にあるような従来の方法の場合は, 本論文の評価方法を利用する場合と比べて, 2^{2k} 倍大きくなってしまうことが解る.

本論文では, $\sum_{\tau\in\Omega^C}|\Omega^{f(\tau)}|$ の精密な評価が困難な為, その上界として, $|\Omega^C|\cdot\max_{\tau\in C}|\Omega^{f(\tau)}|$ を採用する. 色付 g に対して, Ω^g は $\mathcal{X}^g$ の定義域である. $\mathcal{X}_i^g$ の定義域をΩ_i^g と表すと, 各 $\mathcal{X}_i^g$ は $\{0,1\}$ の中の値を取る, 最大値ノルムの意味で, 一様分布に関して l-限定 θ-依存の $|X_i^g| \le n$ 個の確率変数の系であり, さらに, Ω^g は直積 $\Omega_1^g \times \cdots \times \Omega_k^g$ と同型であるので, 本論文の結果を利用した場合は

$$|\Omega^C|\cdot\max_{\tau\in\Omega^C}|\Omega^{f(\tau)}| \le \left(\frac{(c+1)\log_2 k\lceil\log_2\log_2 k+\log_2 n\rceil}{\eta}\right)^2\left(\frac{l\lceil\log_2 n\rceil}{\theta}\right)^{2k} \tag{5}$$

という上界が得られ, 従来の方法に従った場合はこの値よりも $k^{2(c+1)}2^{2kl}$ 倍大きい上界が得られる.

4.3 アルゴリズムの変数に関する制限

この節では, アルゴリズムの変数に関する, 近似値 Y が許容範囲に入るための十分条件を示し, その十分条件を満足する変数の値の設定例を挙げる. 実行時間の上界である式 (5) を最適化するような設定例を求めるのは困難なので, より粗い評価式を最適化する設定例を求め, その値を式 (5) に代入して本論文での検討の対象とする実行時間の上界を求める. また, この設定例から, 従来の方法に従った場合の実行時間の, 利用した場合の実行時間に対する評価値 $k^{2(c+1)}2^{2kl}$ の値を n, m, δ および ϵ によって表す.

命題 2 アルゴリズムの計算する近似値 Y と真の値 $\Pr[F(x)=1]$ は不等式

$$(1-\tilde{\delta})\Pr[F(x)=1]-\tilde{\epsilon} \le Y \le \Pr[F(x)=1]+\tilde{\epsilon}$$

を満足する. ただし,

$$\tilde{\delta}(t,c,k,\eta)=\binom{t}{c+1}\left(\frac{1}{k^c}+k\eta\right),\ \tilde{\epsilon}(m,t,c,k,l,\theta)=m2^{-t}+k\left(e^{-l/c2^c}+2^{l+1}\theta\right)$$

である.

この命題は以下に述べる四つの補題から得られる. これらの補題は [LV91] にある定理あるいは補題を本論文で利用できる形に修正したものである. これらの証明は省略する.

補題 3 $x_1,\ldots,x_n$ は確率空間 $(\Omega_1,\mathcal{F}_1,\Pr_1)$ 上の $\{0,1\}$ の中の値を取る, 最大値ノルムの意味で, 一様分布に関して l-限定 θ-依存の確率変数の系とし, $y_1,\ldots,y_n$ は確率空間 $(\Omega_2,\mathcal{F}_2,\Pr_2)$ 上の $\{0,1\}$ の中の値を取る, 一様分布の独立確率変数系とする. G を項の長さの最大値が高々 c の DNF 式としたとき,

$$|\Pr_1[G(x_1,\ldots,x_n)=1]-\Pr_2[G(y_1,\ldots,y_n)=1]| \le e^{-l/c2^c}+2^{l+1}\theta$$

が成立する.

補題 4 c および k を $c \leq k$ を満足する正整数とする. G は *DNF* 式, g は G の変数上の k 色使った色付とする. どの項にも g により同じ色が付けられた c 個の変数は存在しないとする. 各 $i = 1, \ldots, k$ に対して X_i で g により色 i が付けられた変数の集合を表す. 確率空間 $(\Omega_1, \mathcal{F}_1, \Pr_1)$ とその上の $\{0,1\}$ の中の値を取る確率変数系 $\{x_1, \ldots, x_n\}$ を次のように実現する. 各 $i = 1, \ldots, k$ に対して, 確率変数系 $\mathcal{X}_i = \{x_j \mid j \in X_i\}$ は最大値ノルムの意味で, 一様分布に関して l-限定 θ-依存であり, 各 $i = 1, \ldots, k$ に対して $\mathcal{X}_i$ を確率変数と看做したとき, $\{\mathcal{X}_1, \ldots, \mathcal{X}_k\}$ は独立な確率変数系である. 一方, $y_1, \ldots, y_n$ は確率空間 $(\Omega_2, \mathcal{F}_2, \Pr_2)$ 上の $\{0,1\}$ の中の値を取る, 一様分布の独立確率変数系とする. このとき,

$$|\Pr_1[G(x_1, \ldots, x_n) = 1] - \Pr_2[G(y_1, \ldots, y_n) = 1]| \leq k\left(e^{-l/c2^c} + 2^{l+1}\theta\right)$$

が成立する.

定義 6 G を n 変数かつ m 項の DNF 式, $\mathcal{C}$ を k 色使った G の変数の色付の類とする. X_i^g で色付 $g \in \mathcal{C}$ により色 i が付けられた変数の集合を表す. T_j で G の第 j 項に現れる変数の集合を表す. $\eta > 0$ および正整数 c に対して, $\mathcal{C}$ の中の値を取る確率変数 f が (η, c)-良性であるとは, 各項 $j = 1, \ldots, m$ に対して,

$$\Pr[(\forall i = 1, \ldots, k)(|X_i^f \cap T_j| \leq c)] = \sum_{g \in W_j} \Pr[f = g] \leq \eta$$

が成立することを言う. ただし, $W_j = \{g \in \mathcal{C} \mid (\forall i = 1, \ldots, k)(|X_i^g \cap T_j| \leq c)\}$ とする. □

補題 5 ν を正整数とし, $k = 2^\nu$ とおく. 最大値ノルムの意味で, 一様分布に関して $(c+1)\nu$-限定 η-依存の νn 個の確率変数の系 $\{b_1, b_2, \ldots, b_{\nu n}\}$ を定め, それらを添え字の順に ν 個ずつ連結して, $k = 2^\nu$ 色中の一色を表す n 個のベクトル $c_1 = (b_1, \ldots, b_\nu), \ldots, c_n = (b_{n-\nu+1}, \ldots, b_n)$ を作り, $f = (c_1, \ldots, c_n)$ とおく. このとき, n 個の変数の色付の一つを値として取る確率変数 f は (η, c)-良性である.

補題 6 $\eta > 0$ かつ c は正整数とする. G を *DNF* 式とする. $\mathcal{C}$ を G の変数の集合上の色付の類とする. $\{x_1, \ldots, x_n\}$ を $\{0,1\}$ の中の値を取る, 一様分布の独立確率変数系とし, その定義域となっている確率空間を $(\Omega_1, \mathcal{F}_1, \Pr_1)$ とする. f を $\mathcal{C}$ の中の値を取る (η, c)-良性な確率変数とし, その定義域となっている確率空間を $(\Omega_2, \mathcal{F}_2, \Pr_2)$ とする. また, アルゴリズムの概要 4 にある通り, 色付 g に対して, G を g で色付したとき, どの色も高々 c 色しか現れない G の項からなる *DNF* 式を G_f と表す. このとき,

$$\sum_{g \in \mathcal{C}} \Pr_1[G_g(x_1, \ldots, x_n) = 1] \Pr_2[f = g] \geq (1 - \eta) \Pr_1[G(x_1, \ldots, x_n) = 1]$$

が成立する.

命題 2 により, $\delta \leq \tilde{\delta}(t, c, k, \eta)$ および $\epsilon \leq \tilde{\epsilon}(m, t, c, k, l, \theta)$ が成立するように変数 t, c, k, η, l および θ を設定すれば, アルゴリズムが正しく動作することが保証される.

$\epsilon \leq \tilde{\epsilon}(m, t, c, k, l, \theta)$ より $t \geq \log_2(m/\epsilon)$ が成立する. また, $\delta \leq \tilde{\delta}(t, c, k, \eta)$ より,

$$k \geq \left(\frac{1}{\delta}\left(\left(\log_2 \frac{m}{\epsilon} - c\right) \Big/ (c+1)\right)^{c+1}\right)^{1/c}$$

が成立する. c を未定にした上で, このような考察を続けることにより, 以下の式を得る.

$$\log\left(|\Omega^c|\cdot\max_{\tau\in\Omega^c}|\Omega^{f(\tau)}|\right)=O\left(\left(\frac{1}{\delta}\right)^{1/c}\left(\log\frac{m}{\epsilon}\right)^{\left(1+\frac{1}{c}\right)}\left(\log\log n+\log\log\frac{m}{\epsilon}+c2^c\log\frac{1}{\epsilon}+2^c\log\frac{1}{\delta}\right)\right).$$

この値を最小値に近付ける為に, $c=\sqrt{\log_2(1/\delta)}$ とおく. この c の値から, 次の k および l の下界が得られる.

$$\log k=\Omega\left(\sqrt{\log\frac{1}{\delta}}+\log\log\frac{m}{\epsilon}\right),\ l=\Omega\left(c2^c\left(\log\frac{1}{\epsilon}+\log k\right)\right).$$

これらは, 本論文を利用しない場合の実行時間の, 利用した場合の実行時間に対する比の評価値 $k^{2(c+1)}2^{2kl}$ が無視できない大きさであることを示している.

5 むすび

確率変数系の弱い独立性として, k-限定 ϵ-偏りと k-限定 ϵ-依存の二種類を取り上げ, k-限定 ϵ-偏りの任意の確率変数系に対して, それを k-限定 δ-依存と看做すことを考えた場合, $\delta\leq 4$ とできることを示した. 弱い独立性の定義には幾つかの変種が有るが, 現在, 一般的に提案されている定義に関してはこの不等式が成立する. また, 従来, k-限定 δ-依存の確率変数を構成するために k-限定 ϵ-偏りの確率変数を転用しているため, 本論文の結果は, 弱い独立性を持つ確率変数系で, その標本空間のサイズが小さいものを構成して, その標本空間の要素全てを調べるような形のアルゴリズムの効率化に効果的であり, その一例を紹介した.

本論文では, k-限定 ϵ-偏りの任意の確率変数系に対して, それを k-限定 δ-依存と看做すことを考えたが, 逆に, k-限定 ϵ-依存の任意の確率変数系に対して, それを k-限定 δ-偏りと看做すことを考えることもできる. この場合, 偏りの度合 δ が依存の度合 ϵ に対して, どの程度の大きさになるかは知られていない. これは, 今後の興味深い課題の一つである.

謝辞

御討論頂いた丸岡研究室の皆様に感謝致します. なお, 本研究は一部, 文部省科学研究費奨励研究 (A) (04750293) の援助を受けている.

参考文献

[AGHP90] N. Alon, O. Goldreich, J. Håstad, and R. Peralta. Simple constructions of almost k-wize independent random variables. In *Proceedings of the 31st Annual Symposium on Foundations of Computer Science*, pp. 544–553, 1990.

[LV91] M. Luby and B. Veličković. On deterministic approximation of DNF. In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*, pp. 430–438, 1991.

[NN90] J. Naor and M. Naor. Small-bias probability spaces: efficient constructions and applications. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*, pp. 213–223, 1990.

[Val79] L. G. Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, Vol. 8, pp. 189–201, 1979.