集中講義: 高次元エクスパンダーとその応用

清水 伸高 (東工大)

2024 年 5 月

Contents

序文

一般に「ランダムウォーク」という用語は文脈によって様々である. 例えば物理学や金融の文脈でブラウン運動を離散化したモデルを考える際は数直線上を等確率で左右どちらかに移動する粒子の軌跡をランダムウォークと呼ぶことがある. 一方でネットワーク解析の文脈ではグラフ上の単純ランダムウォークをランダムウォークと呼ぶこともある.

どの理論でも大体そうだが, 文脈に応じて様々な捉え方があり, それぞれに適した定義がされる. ある定義が別の定義を特殊ケースとして含んでいるようなこともあるかもしれない. しかしそれぞれの定義はその分野特有の目標 (解きたい問題) があり, その目標に達成するために必要と思われる理論を独自に展開していくことになる. そしてその独自性にもまた一般化への余地があり, これがさらなる数学の発展に寄与していくと私は思っている.

本講義では高次元エクスパンダーと呼ばれる近年の理論計算機科学の多くのブレイクスルーの立役者について解説する. 理論計算機科学 (theoretical computer science) とは計算機の能力や限界に迫る分野であり, いわゆる「情報系」の分野ではあるが, 実は純粋数学の抽象的な概念や道具が非常に大きな活躍を見せる分野である. 例を挙げればキリがないが, 例えば私がパッと思いつくものを挙げると

- 楕円曲線に基づく楕円曲線暗号
- 加法的組合せ論に基づく学習器のブースティングやアルゴリズムの設計
- 関数解析の道具に基づくランダムウォークの収束性解析
- 代数学の理論に基づくエクスパンダーグラフの構成とそれに基づく脱乱択化
- 楕円曲線から得られる代数幾何符号

がある. その中でグラフ理論のエクスパンダー性と呼ばれる性質を単体複体に拡張した高次元エクスパンダーと呼ばれる概念が近年の理論計算機科学の大きな潮流となっている.

本講義ではまず理論計算機科学においてスタンダードなランダムウォークの定義に基づいてグラフや単体複体上のランダムウォークの理論を構築していく. 私は数学科を出ているわけではないから, 残念ながら高度に抽象的な理論に明るくない. おそらく本講義で展開される理論の一部はより高度な抽象化がすでに知られていて, その枠組みから簡単に導出できると思われる. 例えば単体複体上のランダムウォークをさらに抽象化することができるかもしれない. こういった抽象化や理論の整備は純粋数学の人間の方が間違いなく得意であろうことから, もしも講義でそのようなアイディアが思いついたらメールでも話しかけるでも何でも良いので気軽に私にご指摘いただけると幸いである (仮に誤った指摘であったとしても, その視点は私自身の勉強になるので非常に有難い). 本講義が, 日本国内における数学と理論計算機科学の間のつながりをより強固なものするきっかけになれば幸いである.

Chapter 1

ランダムウォークの概論

1.1 定義

本講義では斉時性をもつ有限状態離散時間マルコフ連鎖をランダムウォークと呼ぶ.

定義 1.1.1 （ランダムウォーク）

有限集合 V と確率行列[a] $P \in [0,1]^{V\times V}$ に対し, V 上に値をとる確率変数列 $(X_t)_{t\geq 0}$ であって, 任意の $t \geq 0$, 頂点列 $(v_0, \ldots, v_{t-1}) \in V^t$, および $v \in V$ に対して

$$\Pr[X_t = v \mid X_0 = v_0, \ldots, X_{t-1} = v_{t-1}] = \Pr[X_t = v \mid X_{t-1} = u] = P(u, v)$$

を満たすものを V 上の**ランダムウォーク (random walk)** という. 特に確率行列 P をランダムウォーク $(X_t)_{t\geq 0}$ の**遷移確率行列 (transition matrix)** と呼ぶ.

[a] 各行和が 1 となる非負行列を**確率行列 (stochastic matrix)** と呼ぶ.

初期地点 X_0 もまた確率変数であるためランダムに決まることに注意されたい. また, 決定的に $X_0 = u$ からスタートしていても良い. 初期頂点 X_0 の分布が決まれば各時刻 t における X_t の分布は一意に定まる. 実際, $t \geq 0$ に対し $p_t \in [0,1]^V$ を X_t の分布とする (すなわち, $p_t(u) = \Pr[X_t = u]$). 任意の $t \geq 1$ に対し

$$\begin{aligned} p_t(v) &= \Pr[X_t = v] \\ &= \sum_{u\in V} \Pr[X_t = v \text{ and } X_{t-1} = u] \\ &= \sum_{u\in V} \Pr[X_t = v \mid X_{t-1} = u] \Pr[X_{t-1} = u] \\ &= \sum_{u\in V} P(u, v) p_{t-1}(u) \end{aligned}$$

という漸化式を得る. これは $p_t = p_{t-1}P$ とも表せる (ここで p_t は行ベクトルとして扱う) ので

$$p_t = p_0 P^t \tag{1.1}$$

を得る.

1.2 収束性

ランダムウォーク $(X_t)_{t\geq 0}$ を考え, 時刻 t における X_t の周辺分布を p_t とする. すなわち, $p_t \in [0,1]^V$ は $p_t(v) = \Pr[X_t = v]$ で定義されるベクトルである. 本講義では総じて時刻 t を大きくしていくときの p_t の収束性とそのスピードについて議論していく.

まずは収束性について議論するために分布間の距離として全変動距離を導入する.

定義 1.2.1 （全変動距離）

有限集合 V 上の二つの分布 $\mu, \nu \in [0,1]^V$ に対し, **全変動距離 (total variation distance)** を

$$d_{\mathrm{TV}}(\mu,\nu) := \frac{1}{2}\sum_{u\in V}|\mu(u)-\nu(u)| = \frac{1}{2}\|\mu-\nu\|_1$$

で定める.

全変動距離は単に ℓ^1 ノルムを 2 で割った値だが, 次の性質を持つがゆえに統計学, 情報理論, 機械学習, 計算機科学を含む様々な分野で非常に重要な役割を果たしている.

命題 1.2.2

有限集合 V を考え, 分布 $\pi \in [0,1]^V$ と部分集合 $U \subseteq V$ に対し $\pi(U) := \sum_{u\in U}\pi(u)$ とする. 任意の二つの分布 $\mu, \nu \in [0,1]^V$ と任意の部分集合 $U \subseteq V$ に対して

$$|\mu(U) - \nu(U)| \leq d_{\mathrm{TV}}(\mu,\nu).$$

すなわち, 全変動距離が小さいということは任意の事象の発生確率の差が小さいことを意味する. なお, この不等式はタイトである. 実際, $U = \{u \in V : \mu(u) > \nu(u)\}$ とすれば等号が成り立つ.

次に, ランダムウォークが収束するための条件を与える.

定義 1.2.3 （既約性、非周期性）

遷移確率行列 $P \in [0,1]^{V\times V}$ をもつランダムウォークを考える.

- 任意の頂点対 $u, v \in V$ に対しある $t \geq 0$ が存在して $P^t(u,v) > 0$ を満たすとき, ランダムウォーク $(X_t)_{t\geq 0}$ は**既約 (irreducible)** であるという.
- 各頂点 $u \in V$ に対し, 有向閉路長の集合 $L_u = \{t \geq 1 : P^t(u,u) > 0\}$ を考え, その最大公約数を頂点 u の**周期 (period)** と呼ぶ. 全ての頂点の周期が 1 であるとき, ランダムウォーク $(X_t)_{t\geq 0}$ は**非周期的 (aperiodic)** であるという.

既約性は任意の頂点対 u, v に対し u からスタートしたランダムウォークが v に到達可能であることを意味している.

非周期性は, ランダムウォークが「振動」しないことを意味する性質である. 例えば遷移

確率行列が

$$P = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

で与えられるランダムウォークは全ての有向閉路の長さは 3 の倍数であるためどの頂点の周期も 3 に等しい. 特に, ランダムウォーク X_t は周期 3 でループしており, 例えば確率 1 で特定の頂点からスタートしたときに p_t は収束しないことがわかる. 非周期性はこのようなケースを排除するという意味を持つ.

1.3 定常分布

ランダムウォークの分布 p_t がある分布 $\pi \in [0,1]^V$ に収束するならば, 分布の漸化式 $p_t = p_{t-1}P$ より収束先の分布 π は

$$\pi = \pi P \tag{1.2}$$

を満たすはずである.

定義 1.3.1 （定常分布）

遷移確率行列 P をもつ V 上のランダムウォークに対し, 式 (1.2) を満たす分布 π を**定常分布 (stationary distribution)** と呼ぶ.

任意のランダムウォークは必ず定常分布をもつ. 詳細は省くがこれは以下の議論から証明できる:

- 定常分布 π は転置行列 $P^\top$ の固有値 1 の固有ベクトルに対応する.
- P と $P^\top$ の固有値は全て同じ (転置をとっても行列式は変わらないから) であり, 最大固有値 1 を持つ.
- Perron–Frobenius の定理から $P^\top$ の最大固有値 1 に対応する固有ベクトルの成分は非負なので, 正規化すると分布になる.

定理 1.3.2 （一般のランダムウォークの収束性）

遷移確率行列 P を持つ V 上の任意のランダムウォークは定常分布 $\pi \in [0,1]^V$ を持つ. さらに,

- ランダムウォークが既約的ならば, 定常分布 π は一意に存在し, 全ての頂点 $v \in V$ に対し $\pi(v) > 0$ である.
- ランダムウォークが非周期的ならば, 任意の初期分布 p_0 に対してある定常分布 π が存在して $d_{\mathrm{TV}}(p_t, \pi) \to 0$ $(t \to \infty)$ が成り立つ.

特に, 既約的かつ非周期的なランダムウォークの分布は一意に定まる定常分布に d_{TV} の意味で収束する.

すなわち, 既約性とは定常分布の一意性を保証する性質であり, 非周期性は収束性を保証する性質である.

1.4 混交時間

定理 1.3.2 ではランダムウォークの一意収束性の条件を与えた. では, その収束の速さはどれくらいだろうか? この問題は日常的には例えば次のような状況で現れる:

- トランプカードで遊ぶとき, 何回シャッフルすればカードが「混ざり合う」か?
- 料理で調味料をスープに入れたとき, 何回かき回せば味が「混ざり合う」か?

ここでは「混ざり合う」とは定常分布への全変動距離の意味での収束性で定義し, ランダムウォークの混交時間を次で定義する:

定義 1.4.1 （混交時間）

既約なランダムウォーク $(X_t)_{t\geq 0}$ を考え, $t \geq 0$ に対し $p_t \in [0,1]^V$ を時刻 t における X_t の分布とする. 定常分布を $\pi \in [0,1]^V$ とする. 正の実数 $\varepsilon > 0$ に対し, ε-混交時間 $t_{\mathrm{mix}}(\varepsilon)$ を

$$t_{\mathrm{mix}}(\varepsilon) := \inf\{t \geq 0 \colon d_{\mathrm{TV}}(p_t, \pi) \leq \varepsilon\}$$

とする. また, $(1/2)$-混交時間を単に**混交時間 (mixing time)** と呼ぶ.[a]

[a] $1/2$ という数字に特に本質的な意味はない.

注釈 1.4.2 （初期分布）

ランダムウォークの混交時間はその初期分布に依存する. 例えば初期分布が定常分布 π であった場合, 混交時間は 0 である. 基本的には任意の初期分布を考え, その中で混交時間の最大値を考える. 任意の分布はディラック測度の凸結合で表せるため, 全ての初期分布での最大を考える代わりに, 各ディラック測度 (確率 1 で特定の頂点を選択する測度) に関する最大値だけ考えればよい. すなわち, 本講義で初期分布を指定していないランダムウォークに対して混交時間の上界を議論する際は

$$\max_{u\in U} \inf\bigl\{t \geq 0 \colon d_{\mathrm{TV}}(P^t(u,\cdot), \pi) \leq \varepsilon\bigr\}$$

を上から抑えることを意味する.

本講義では全体を通じてランダムウォークの混交時間 (特にその上界) を評価することに取り組む. 中でも特に強力な固有値に基づく解析について説明し, これに基づいてグラフや単体複体のエクスパンダー性を定義し, その性質を解説していく. 最後にマトロイドと呼ばれる重要な離散構造上のランダムウォークを解析し, 重要な未解決問題であり近年ようやく解決された Micali–Vazirani 予想の証明を与える.

1.5 グラフ上のランダムウォーク

グラフ上のランダムウォークとして最も有名な単純ランダムウォークを紹介する. まず本講義におけるグラフの定義を与える. グラフの定義に詳しい読者は定義 1.5.5 まで読み飛ばしても構わない. もしくは, 必要に応じて後から定義を参照すればよい.

定義 1.5.1 （グラフ）

有限単純無向グラフを単に**グラフ (graph)** と呼ぶ. すなわち, グラフとは有限集合 V とその二元部分集合 $E \subseteq \binom{V}{2}$ の組 $G = (V, E)$ である. V の元を**頂点 (vertex)**, E の元を**辺 (edge)** と呼ぶ.
二頂点 $u, v \in V$ が $\{u, v\} \in E$ を満たすとき, u は v に**隣接 (adjacent)** しているという (v もまた u に隣接している). 頂点 u と辺 $e \in E$ が $u \in e$ を満たすとき, e は u に**接続 (incident)** しているという. 頂点 u に接続している辺の本数を u の**次数 (degree)** といい, $\deg(u)$ で表す. 全ての頂点の次数が d に等しいとき, G は d-**正則 (d-regular)** であるという.
二つのグラフ $G = (V, E), H = (U, F)$ に対して $U \subseteq V, F \subseteq E$ を満たすとき G は H を**部分グラフ (subgraph)** として含むといい, $H \subseteq G$ で表す.

グラフの路と閉路を定義する.

定義 1.5.2 （路と閉路）

グラフ $G = (V, E)$ を考える. 頂点列 $(v_0, \dots, v_\ell) \in V^{\ell+1}$ は $\{v_0, v_1\}, \dots, \{v_{\ell-1}, v_\ell\} \in E$ を満たすとき, v_0 から v_ℓ への**路 (walk)** といい, ℓ を長さと呼ぶ. 路 $(v_0, \dots, v_\ell)$ に対し v_0 と v_ℓ をそれぞれ始点, 終点と呼ぶ. 路 $(v_0, \dots, v_\ell)$ が $v_0 = v_\ell$ であって満たすものを**閉路 (cycle)** という.

グラフの連結性を定義する.

定義 1.5.3 （連結性）

グラフ $G = (V, E)$ を考える. 二頂点 $u, v \in V$ に対し, u から v への路が存在しかつそのときに限り $u \sim v$ とすることで頂点集合 V 上の同値関係 $\sim$ を定義する. このとき, 商集合 $V/\sim$ の各同値類を G の**連結成分 (connected component)** という. 商集合 $V/\sim$ が単一の連結成分からなるとき, G は**連結 (connected)** であるという.

最後にグラフの二部性を定義する.

定義 1.5.4 （二部グラフ）

グラフ $G = (V, E)$ を考える. ある頂点分割 $V = L \sqcup R$ が存在して $E \cap \binom{L}{2} = \emptyset$ かつ $E \cap \binom{R}{2} = \emptyset$ が成り立つとき, G は**二部 (bipartite)** であるといい, 頂点部分集合 L, R を G の**部集合 (partite set)** と呼ぶ.

直感的には, G が二部グラフであるというのは, ある頂点分割 $V = L \sqcup R$ に対して G の

全ての辺が L と R の間を跨いでいることを意味する. なお, 部集合への分割 $V = L \sqcup R$ は必ずしも一意であるとは限らない. よく知られる事実として, グラフ G が二部グラフであることの必要十分条件は G の全ての閉路の長さが偶数であることである.

単純ランダムウォーク 単純ランダムウォークとは, 初期地点 X_0 を選び, 現在いる頂点から一様ランダムな隣接点を選びそこに遷移するという確率的な操作を繰り返して得られるランダムウォークである.

定義 1.5.5 (単純ランダムウォーク)

グラフ $G = (V, E)$ を考える. 遷移確率行列が

$$P_{\mathrm{SRW}}(u, v) := \begin{cases} \frac{1}{\deg(u)} & \text{if } \{u, v\} \in E, \\ 0 & \text{otherwise} \end{cases}$$

で与えられる V 上のランダムウォークを G 上の**単純ランダムウォーク (simple random walk)** という.

単純ランダムウォークの定常分布はの一つは

$$\pi(u) = \frac{\deg(u)}{2|E|}. \tag{1.3}$$

で与えられる. 一般に単純ランダムウォークは既約性や非周期性を持つとは限らない. 既約的であることの必要十分条件はグラフ G が連結であることであり, 非周期的であることの必要十分条件はグラフ G の全ての連結成分のなす誘導部分グラフが二部グラフでないことである. 実際, 全ての連結成分が二部グラフでないならばそれぞれに長さ奇数の閉路 C が存在する. 各頂点 u について, 辺 $\{u, v\}$ 上で $u \to v \to u$ という遷移を考えれば長さ 2 の閉路になっている. また, 頂点 u から奇閉路 C に向い, C に沿って遷移した後に再び u に戻るという経路を考えればこれは奇数長の閉路である. すなわち $P^2(u, u) > 0$ かつある奇数 ℓ に対し $P^\ell(u, u) > 0$ となるため頂点 u の周期は 1 である. 逆に二部グラフならば全ての閉路が偶数長なので任意の奇数 ℓ と頂点 $u \in V$ に対し $P^\ell(u, u) = 0$ である.

遅延単純ランダムウォーク. 単純ランダムウォークは二部グラフ上では分布が収束しないという問題点があったが, これは以下のようにランダムウォークの遷移に自己ループを許容することによって解決することができる.

定義 1.5.6 (遅延単純ランダムウォーク)

グラフ $G = (V, E)$ 上の単純ランダムウォークの遷移確率行列を P_{SRW} とする. 確率行列 $P_{\mathrm{LSRW}} := \frac{1}{2}(I + P_{\mathrm{SRW}})$ を遷移確率行列とする V 上のランダムウォークを**遅延単純ランダムウォーク (lazy simple random walk)** という. ここで I は単位行列.

要するに遅延単純ランダムウォークとは各頂点に確率 $1/2$ の自己ループの遷移を許したランダムウォークである. 遷移確率行列の定義より単純ランダムウォークと同じ定常分布を持つ. 自己ループの遷移を許すことによって各頂点の周期が必ず 1 となるため, 遅延単純ラ

ンダムウォークは必ず非周期的である. 従って, 連結グラフ上の遅延単純ランダムウォークは式 (1.3) で与えられる定常分布に一意収束する.

1.6 グラフ上での上昇ウォークと下降ウォーク

グラフ $G=(V,E)$ 上の遅延単純ランダムウォークの 1 回の遷移は次の 2 つのステップに分解して考えることができる:

1. 現在いる頂点 $u \in V$ に接続している辺 $e \in E$ を一様ランダムに選ぶ.
2. 選んだ辺 e に含まれる二頂点を一様ランダムに選び, その頂点に遷移する.

ステップ 1 でどの辺を選んだとしてもステップ 2 で確率 $1/2$ で元の頂点 u に戻る. 一方でステップ 2 で u でない方の頂点を選んだ場合は, u にとって一様ランダムな隣接点に遷移したことになる. 従ってこの 2 ステップに基づく遷移は遅延単純ランダムウォークと同じ遷移確率行列をもつ. ステップ 1 を頂点 u から開始したときに辺 e が選ばれる確率を $P_0^{\uparrow}(u,e) \in [0,1]^{V\times E}$ とし, 同様にステップ 2 を辺 e から開始したときに頂点 $w \in \{u,v\}$ が選ばれる確率を $P_1^{\downarrow}(e,w)$ とする. すなわち

$$P_0^{\uparrow}(u,e) = \begin{cases} \frac{1}{\deg(u)} & \text{if } u \in e, \\ 0 & \text{otherwise.} \end{cases}$$

$$P_1^{\downarrow}(e,w) = \begin{cases} \frac{1}{2} & \text{if } e \ni w, \\ 0 & \text{otherwise.} \end{cases}$$

このとき, 遅延単純ランダムウォークの遷移確率行列 P_{LSRW} は $P_{\mathrm{LSRW}} = P_0^{\uparrow}P_1^{\downarrow}$ と表せる.

逆に, 二つのステップを入れ替え, $P' := P_1^{\downarrow}P_0^{\uparrow} \in [0,1]^{E\times E}$ を遷移確率行列としてもつ E 上のランダムウォークも考えることができる. このランダムウォークの遷移は次の 2 ステップで与えられる:

1. 現在いる辺 $e=\{u,v\}$ に含まれる頂点を一様ランダムに選び $w \in e$ とする.
2. 選んだ頂点 w に接続している辺 $e' \in E$ を一様ランダムに選び, その辺に遷移する.

このランダムウォークの遷移確率行列 P' の対角成分は全て正なので非周期的である. さらに元のグラフ G が連結ならば既約的である. 従って定理 1.3.2 より定常分布が一意に存在し, その分布への収束性が成り立つ.

演習問題 1 （easy）

グラフ G が連結であるとする. 上記の P' を遷移確率行列としてもつ辺上のランダムウォークの定常分布を求めよ. 答えだけでよい.

1.7 重み付きグラフ上のランダムウォーク

単純ランダムウォークでは接続している全ての辺は同じ重みを持っている. 各辺に重みと呼ばれる正の実数を割り当てることによって, 重みの大きい辺がより選ばれやすくなるようなランダムウォークを考えることができる.

定義 1.7.1 （重み付きランダムウォーク）

有限集合 V に対し, $V \times V$ の非負対称行列 $W \in \mathbb{R}_{\geq 0}^{V \times V}$ を重み行列と呼ぶ. 頂点 $u \in V$ に対し $\deg_W(u) = \sum_{w \in V} W(u, v)$ を**重み付き次数 (weighted degree)** という. 遷移確率行列 P が $P(u, v) = \frac{W(u,v)}{\deg_W(u)}$ で与えられるランダムウォークを**重み付きランダムウォーク (weighted random walk)** と呼ぶ.

重み行列 W をグラフ G の隣接行列とすれば G 上の単純ランダムウォークになる. 同様に単純遅延ランダムウォークも重み付きランダムウォークの特殊ケースとして表現できる.

1.8 混交時間解析の実例

講義とは直接な関係はないが, 最後にランダムウォークの混交性解析の応用例をいくつか簡単に説明する.

1.8.1 到達時間, 全訪問時間の解析

1.8.2 マルコフ連鎖モンテカルロ法

1.8.3 イジングモデル

Chapter 2

ランダムウォークの固有値とエクスパンダーグラフ

遷移確率行列 $P \in [0,1]^{V\times V}$ に従う V 上の既約的かつ非周期的なランダムウォーク $(X_t)_{t\geq 0}$ を考え, その一意な定常分布を π とする. 定理 1.3.2 より収束性が保証されるが, その速さを遷移確率行列の固有値に基づいて評価するのが本チャプターの目標である. この議論の土台となるのがランダムウォークの可逆性という概念である. 一般の遷移確率行列は対称とは限らないが, 可逆性を仮定することによって遷移確率行列を対称行列として扱うことができ, 対称行列に対して展開される固有値分解などの理論を同じように遷移確率行列に対しても適用することができる. これに基づいて既約性, 非周期性, 可逆性を持つランダムウォークの混交時間の上界を与える. また, エクスパンダーグラフの概念をそのグラフ上の単純ランダムウォークに基づいて定義し, その組合せ論的な性質をいくつか紹介する.

2.1 ランダムウォークの固有値と可逆性

遷移確率行列 $P \in [0,1]^{n\times n}$ の固有値[1] $\lambda_1, \dots, \lambda_n$ について考える. 全ての成分が 1 であるベクトル $\mathbf{1} \in \mathbb{R}^n$ を考えると $P\mathbf{1} = \mathbf{1}$ であるから P は固有値 1 を持つことがわかる. また, 以下の結果が知られている (Perron–Frobenius の定理や Gershgorin の定理から従う):

補題 2.1.1 （遷移確率行列の固有値）

既約的かつ非周期的なランダムウォークの遷移確率行列 $P \in [0,1]^{n\times n}$ の固有値を $\lambda_1, \dots, \lambda_n$ とすると, 全ての $i \in \{1, \dots, n\}$ に対して $|\lambda_i| \leq 1$ を満たす. さらに, 固有値 1 の多重度は 1 であり (つまり固有値 1 に対応する固有空間は $\{c\mathbf{1} : c \in \mathbb{R}\}$ となる), 他の固有値は全て絶対値が真に 1 より小さい.

一方でこれまで見ていたグラフ上のランダムウォークは可逆性と呼ばれる嬉しい性質を持っており, ある意味で対称行列のように扱うことができる.

[1] 本講義では左固有値, すなわち $Px = \lambda x$ を満たす $\lambda \in \mathbb{C}$ を考える.

定義 2.1.2 （可逆性）

遷移確率行列 P を持つ V 上のランダムウォークは, ある V 上の分布 $\pi \in [0,1]^V$ が存在して

$$\forall u, v \in V, \pi(u)P(u,v) = \pi(v)P(v,u) \tag{2.1}$$

を満たすとき**可逆 (reversible)** であるという.

式 (2.1) で表される条件を**詳細釣り合い条件 (detailed balanced equation)** という. 分布 $\pi \in [0,1]^V$ を対角成分に並べた対角行列 $\Pi \in [0,1]^{V\times V}$ を用いると (2.1) $\iff$ $\Pi P = (\Pi P)^\top$ となる.

可逆性とは直感的に言うと, 逆再生しても同じ分布のランダムウォークになるという性質である. ランダムウォーク $(X_t)_{t\geq 0}$ であって初期頂点 X_0 が分布 π に従って選ばれたものを考えよう. 適当な時刻 $t = T$ で打ち切って得られる頂点列 $(X_0, \ldots, X_T)$ に対し, 順序を逆にした系列 $(X_T, \ldots, X_0)$ はランダムウォークから得られた系列と見做せるだろうか? 仮にこれがある遷移確率行列 $P^* \in [0,1]^{V\times V}$ に従うランダムウォークであったとしよう. 簡単のため $T = 1$ とする ($T \geq 2$ に関しても同じ議論が適用できる). 初期頂点 X_0 の分布 π が定常分布だとすると, X_1 の分布も π である. また, ランダムウォークの条件から $\Pr[X_1 = v \text{ and } X_0 = u] = \pi(u)P(u,v)$ である. 従って条件付き確率の定義より

$$P^*(v,u) = \Pr[X_0 = u | X_1 = v] = \frac{\Pr[X_0 = u \text{ and } X_1 = v]}{\Pr[X_1 = v]} = \frac{\pi(u)P(u,v)}{\pi(v)} \tag{2.2}$$

が得られる. もし元のランダムウォークが可逆ならば, 式 (2.1) から $P^* = P$ を得る. すなわち, ランダムウォークの可逆性とはそのランダムウォークが時間反転に関して対称性を持つことを意味する. なお, 式 (2.2) で得られる遷移確率行列に従って生成されるランダムウォークを**時間反転ランダムウォーク (time-reversal random walk)** と呼ぶ.

例 1. 単純ランダムウォーク 連結グラフ $G = (V, E)$ 上の単純ランダムウォークを考えよう. 式 (1.3) で与えられる定常分布を π とすると任意の二頂点 $u, v \in V$ に対して

$$\pi(u)P(u,v) = \frac{\deg(u)}{2|E|} \cdot \frac{\mathbf{1}_{\{u,v\}\in E}}{\deg(u)} = \frac{\deg(v)}{2|E|} \cdot \frac{\mathbf{1}_{\{u,v\}\in E}}{\deg(v)} = \pi(v)P(v,u)$$

より, 単純ランダムウォークは可逆である (連結なので全ての頂点に対して $\deg(u) > 0$ である). ここで, $\mathbf{1}_{\ldots}$ は指示関数である.

例 2. 重み付きランダムウォーク 重みつきグラフ $G = (V, E, W)$ 上の重み付きランダムウォークを考えよう. 重み行列 W の成分和を $S = \sum_{u,v\in V} W(u,v)$ として分布 $\pi(u) = \frac{\deg_W(u)}{S}$ を考えると,

$$\pi(u)P(u,v) = \frac{\deg_W(u)}{S} \cdot \frac{W(u,v)}{\deg_W(u)} = \frac{\deg_W(v)}{S} \cdot \frac{W(v,u)}{\deg_W(v)} = \pi(v)P(v,u)$$

より, 可逆である.

例 3. 有向グラフ上のランダムウォーク 可逆で**ない**例として次の遷移確率行列で与えられるランダムウォークを考えてみよう:

$$P = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

この例は遷移が決定的なのでランダムウォークとしては面白くないが, 次のようにして可逆でないことが確認できる: 頂点集合を $V = \{0, 1, 2\}$ とし, $i \in V$ に対して $(i+1) \bmod 3$ を省略して $i+1 \in V$ と書くと

$$\pi(i) = \pi(i)P(i, i+1) = \pi(i+1)P(i+1, i) = 0$$

より $\pi = 0$ となってしまい, 分布であることに矛盾.

演習問題 2 （easy）

可逆なランダムウォークの遷移確率行列を P とする. 式 (2.1) を満たす分布 π は定常分布であることを示せ.

2.2 定常分布から定まる内積とノルム

可逆なランダムウォークは遷移確率行列の固有値を考える上で非常に扱いやすいランダムウォークのクラスとなっている. ランダムウォークの分布は遷移確率 P を右から掛けて得られるのに対し, 固有値に基づく議論では左固有値を考えており, この左右の差異に違和感を覚える読者もいるであろう. 実は可逆なランダムウォークでは遷移確率行列を対称行列のように扱うことができ, ゆえに左右どちらから作用させようが本質的に同じとなる. このことを説明するために, $\mathbb{R}^V$ に次の内積を導入する.

定義 2.2.1

有限集合 V 上の分布 $\pi \in (0, 1]^V$ に対し, $\mathbb{R}^V$ に以下の内積 $\langle \cdot, \cdot \rangle_\pi$ を定めた内積空間を $\ell^2_\pi(V)$ で表す:

$$\langle f, g \rangle_\pi := \sum_{u \in V} \pi(u) f(u) g(u) = f^\top \Pi g.$$

ここで f, g は列ベクトルとして扱い, $\Pi = \mathrm{diag}(\pi)$ はベクトル π の成分を対角に並べた行列である. また, 内積 $\langle \cdot, \cdot \rangle_\pi$ が誘導するノルムを $\|\cdot\|_\pi$ で表す. すなわち, $f \in \mathbb{R}^V$ に対して

$$\|f\|_\pi := \sqrt{\langle f, f \rangle_\pi}.$$

定義 2.2.1 で考える分布 π は全ての成分が正であるため, 上記の内積 $\langle \cdot, \cdot \rangle_\pi$ はちゃんと実ベクトル空間の内積の公理 (対称双線形性, 非退化性, 半正定値性) を満たしており, 確かに $\ell^2_\pi(V)$ は内積空間である.

$\mathbb{R}^V$ 上の通常の内積 $\langle \cdot, \cdot \rangle$ を考えたとき, 任意の対称行列 $M \in \mathbb{R}^{V \times V}$ とベクトル $f, g \in \mathbb{R}^V$ に対して $\langle f, Ag \rangle = \langle Af, g \rangle$ が成り立っていたが, 可逆なランダムウォークの遷移確率行列 P は内積 $\langle \cdot, \cdot \rangle_\pi$ に関して同様の性質を持つ.

補題 2.2.2

定常分布 π をもつ可逆なランダムウォークの遷移確率行列 P は, 任意の $f, g \in \mathbb{R}^V$ に対して

$$\langle f, Pg \rangle_\pi = \langle Pf, g \rangle_\pi$$

を満たす.

証明. 定常分布 π を対角成分に並べた対角行列 Π を考えると

$$\begin{aligned} \langle f, Pg \rangle_\pi &= f^\top \Pi P g \\ &= f^\top (\Pi P)^\top g && \because \text{可逆性より } \Pi P \text{ は対称} \\ &= (Pf)^\top \Pi g && \because \Pi^\top = \Pi \\ &= \langle Pf, g \rangle_\pi. \end{aligned}$$

□

一般に P が可逆とは限らない場合, 式 (2.2) で与えられる時間反転ランダムウォークの遷移確率行列 P^* に対し $\langle f, Pg \rangle_\pi = \langle P^* f, g \rangle_\pi$ が成り立つ. この意味で P^* は P の随伴とみなすことができる.

対称行列に対して展開される固有値分解などの理論は可逆なランダムウォークの遷移確率行列に対しても同様に展開できる. 例えば, 対称行列と同様に可逆なランダムウォークの遷移確率行列は実固有値をもつ.

補題 2.2.3 （実固有値性）

既約的かつ可逆なランダムウォークの遷移確率行列 P と定常分布 π に対し, 行列

$$A := \sqrt{\Pi} P \sqrt{\Pi}^{-1} \tag{2.3}$$

を考える. P と A は (多重度も含め) 同じ固有値をもち, これらは全て実数である.

証明. 行列 A は対称である. 実際,

$$\begin{aligned} A^\top &= \sqrt{\Pi}^{-1} P^\top \sqrt{\Pi} && \because \sqrt{\Pi}, \sqrt{\Pi}^{-1} \text{ は対称} \\ &= \sqrt{\Pi} \cdot \Pi^{-1} P^\top \Pi \cdot \sqrt{\Pi}^{-1} \\ &= \sqrt{\Pi} \cdot \Pi^{-1} (\Pi P)^\top \cdot \sqrt{\Pi}^{-1} \\ &= \sqrt{\Pi} \cdot \Pi^{-1} \Pi P \cdot \sqrt{\Pi}^{-1} && \because \text{可逆性より } \Pi P \text{ は対称} \\ &= A. \end{aligned}$$

A は対称なので全ての固有値は実数である.

A の固有値 λ に対する固有ベクトルを x とし, ベクトル $y := \sqrt{\Pi}^{-1}x$ を考える. 固有ベクトルの式

$$Ax = (\sqrt{\Pi}P\sqrt{\Pi}^{-1})x = \lambda x$$

の両辺に左から $\sqrt{\Pi}^{-1}$ を掛けると

$$Py = \lambda y$$

を得る. すなわち, P と A は同じ固有値を持つ. 特に, P の固有値も全て実数である. □

補題 2.2.3 において既約性の仮定は除去できる. 実際, P が定める状態遷移を表す有向グラフを強連結成分に分解し, 各成分ごとに補題 2.2.3 を適用すればよい.

定理 2.2.4 （固有分解）

既約的かつ可逆なランダムウォークの遷移確率行列を P とし, その定常分布を π とする. $|V| = n$ とする. P の固有値を $1 = \lambda_1 \geq \cdots \geq \lambda_n \geq -1$ とする. 空間 $\ell^2_\pi(V)$ の正規直交基底 $x, \ldots, x_n$ が存在して任意の $t \geq 1$ に対して

$$P^t\Pi^{-1} = \sum_{i=1}^{n} \lambda_i^t x_i x_i^\top$$

と表せ, さらに各 x_i は P の固有値 λ_i に対応する固有ベクトルとなる.
特に $x_1 = \mathbf{1}$ であり, $J \in \mathbb{R}^{V\times V}$ を全成分が 1 の行列とすると

$$P^t\Pi^{-1} - J = \sum_{i=2}^{n} \lambda_i^t x_i x_i^\top$$

と表せる.

証明. 式 (2.3) で定義された行列 A は対称なので, 対称行列に対する固有分解の定理より, 通常の内積 $\langle\cdot,\cdot\rangle$ の意味での $\mathbb{R}^V$ の正規直交基底 $y_1, \ldots, y_n$ が存在して

$$A = \sum_{i=1}^{n} \lambda_i y_i y_i^\top$$

と表せ, さらに各 y_i は A の固有値 λ_i に対応する固有ベクトルとなる. 一方で $A^t = \sqrt{\Pi}P^t\sqrt{\Pi}^{-1}$ だから,

$$\sqrt{\Pi}P^t\sqrt{\Pi}^{-1} = \sum_{i=1}^{n} \lambda_i^t y_i y_i^\top.$$

両辺に左右から $\sqrt{\Pi}^{-1}$ を一つずつ掛けて $x_i = \sqrt{\Pi}^{-1}y_i$ とおくと

$$P^t\Pi^{-1} = \sum_{i=1}^{n} \lambda_i^t x_i x_i^\top$$

を得る. ここで

$$\langle x_i, x_j \rangle_\pi = \langle \sqrt{\Pi} x_i, \sqrt{\Pi} x_j \rangle = \langle y_i, y_j \rangle = \mathbf{1}_{i=j}$$

より, 確かに $(x_i)_{i=1,\dots,n}$ は空間 $\ell^2_\pi(V)$ の正規直交基底である. さらに

$$Px_i = P\sqrt{\Pi}^{-1} y_i = \sqrt{\Pi}^{-1} A y_i = \lambda_i x_i$$

より確かに x_i は P の固有値 λ_i に対応する固有ベクトルである.

特に, $\lambda_1 = 1$ に対応する A の固有ベクトルは $y_1 = (\sqrt{\pi(u)})_{u\in V}$ なので, 対応する P の固有ベクトルは $x_1 = \mathbf{1}$ となる. □

系 2.2.5

定理 2.2.4 と同じ仮定の下で空間 $\ell^2_\pi(V)$ 上の関数 $f\colon V \to \mathbb{R}$ に対し,

$$\mathbf{E}_\pi f := \langle f, \mathbf{1} \rangle_\pi = \sum_{u\in V} \pi(u) f(u), \tag{2.4}$$

$$\mathbf{Var}_\pi f := \left\| f - \mathop{\mathbb{E}}_\pi \mathbf{1} \right\|^2_\pi = \mathop{\mathbb{E}}_\pi f^2 - (\mathop{\mathbb{E}}_\pi f)^2 \tag{2.5}$$

とする. 任意の $f, g\colon V \to \mathbb{R}$ に対し

$$\left| \langle f, g \rangle_\pi - \mathop{\mathbb{E}}_\pi f \cdot \mathop{\mathbb{E}}_\pi g \right| \le \max\{|\lambda_2|, |\lambda_n|\} \sqrt{\mathbf{Var}_\pi f \cdot \mathbf{Var}_\pi g}.$$

演習問題 3

系 2.2.5 を証明せよ.

2.3 ランダムウォークのスペクトルと混交時間

非自明な固有値が絶対値の意味で小さいときに混交時間が上から抑えられることを示す.

定義 2.3.1

サイズ n の集合 V 上の可逆なランダムウォークを考え, その遷移確率行列 P の固有値を $1 = \lambda_1 \ge \cdots \ge \lambda_n \ge -1$ に対し, $\lambda(P) := \max\{|\lambda_2|, |\lambda_n|\}$ とする. 特に, $\gamma := 1 - \lambda(P)$ を**スペクトルギャップ (spectral gap)** と呼ぶ.

既約性と非周期性を仮定するとスペクトルギャップは正となる. スペクトルギャップが大きいほど混交時間が小さくなる.

補題 2.3.2 (混交時間とスペクトルギャップ)

集合 V 上の既約, 非周期的, 可逆なランダムウォークを考え, そのスペクトルギャップ

を γ とする. 定常分布 π に対し $\pi_{\min} = \min_{u\in V} \pi(u)$ とすると, 任意の初期分布に対して

$$t_{\mathrm{mix}}(\varepsilon) \le \frac{\log\left(\frac{1}{2\pi_{\min}\varepsilon}\right)}{\log(1/\lambda)}.$$

特に, スペクトルギャップが $\gamma > 0$ のとき, $t_{\mathrm{mix}}(\varepsilon) \le \frac{1}{\gamma}\log\left(\frac{1}{2\pi_{\min}\varepsilon}\right)$.

証明. 定理 2.2.4 の正規直交基底を $x_1, \dots, x_n$ とする. ピタゴラスの定理より任意のベクトル $f \in \mathbb{R}^V$ は

$$\|f\|_\pi^2 = \sum_{i=1}^n \langle f, x_i\rangle_\pi^2$$

を満たす. 特に, 頂点 u を固定し f としてディラック測度 $f = \delta_u$ とすると

$$\begin{aligned}
\pi(u) &= \|\delta_u\|_\pi^2 \\
&= \sum_{i=1}^n \langle \delta_u, x_i\rangle_\pi^2 \\
&= \sum_{i=1}^n \pi(u)^2 x_i(u)^2 \\
&= \pi(u)^2 + \pi(u)^2 \sum_{i=2}^n x_i(u)^2 && (\because x_1 = \mathbf{1})
\end{aligned}$$

を得る. 特に, $\sum_{i=2}^n x_i(u)^2 = \frac{1}{\pi(u)} - 1 \le \frac{1}{\pi(u)}$ である.

ここで, 定理 2.2.4 より, $P^t\Pi^{-1} - J$ の第 (u,v) 成分に着目すると

$$\begin{aligned}
\left|\frac{P^t(u,v)}{\pi(v)} - 1\right| &\le \sum_{i=2}^n |\lambda_i|^t |x_i(u)x_i(v)| \\
&\le \lambda^t \sum_{i=2}^n \sqrt{\sum_{i=2}^n x_i(u)^2}\sqrt{\sum_{i=2}^n x_i(v)^2} && \because \text{Cauchy–Schwarz の不等式} \\
&\le \frac{\lambda^t}{\sqrt{\pi(u)\pi(v)}} \\
&\le \frac{\lambda^t}{\pi_{\min}}
\end{aligned}$$

を得る. 特に, 任意の頂点 $u \in V$ に対して

$$d_{\mathrm{TV}}\big(P^t(u,\cdot), \pi\big) = \frac{1}{2}\sum_{v\in V}\big|P^t(u,v) - \pi(v)\big| \le \frac{\lambda^t}{2\pi_{\min}}$$

なので, 任意の初期分布に対して混交時間は

$$t_{\mathrm{mix}}(\varepsilon) \le \inf\left\{t \ge 0 \colon \frac{\lambda^t}{2\pi_{\min}} \le \varepsilon\right\} \le \frac{\log\left(\frac{1}{2\pi_{\min}\varepsilon}\right)}{\log(1/\lambda(P))} \le \frac{1}{\gamma}\log\left(\frac{1}{2\pi_{\min}\varepsilon}\right).$$

最後の不等式では $\forall x \in \mathbb{R}, x \le \mathrm{e}^{x-1}$ を用いた. □

2.4 エクスパンダーグラフ

グラフ $G = (V, E)$ は, 単純ランダムウォークの非自明な第二固有値 $\lambda(P)$ が小さいときにエクスパンダーであるという. 多くの文脈では通常, 正則グラフに対してのみエクスパンダー性が定義されるが本講義では一般のグラフに対してエクスパンダー性を定義する.

定義 2.4.1 （エクスパンダー）

グラフ $G = (V, E)$ 上の遷移確率行列 P が $\lambda(P) \le \lambda$ を満たすときグラフ G は **λ-エクスパンダー (λ-expander)** という. また, P の第二固有値が $\lambda_2 \le \lambda$ を満たすとき, グラフ G は**片側 λ-エクスパンダー (one-sided λ-expander)** という.

本講義ではエクスパンダー性を持つ単体複体も取り扱うため, エクスパンダー性を持つグラフのことを**エクスパンダーグラフ**と呼んで区別する.

要するにグラフのエクスパンダー性とは単純ランダムウォークの混交時間が小さいという性質を意味する. 二部グラフは周期的であり特に最小固有値が $\lambda_{|V|} = -1$ となるためこの意味ではエクスパンダーグラフになりえないが, 片側エクスパンダーであるならば遅延単純ランダムウォークの混交時間は小さくなる.

ランダムウォークの混交時間が小さいとはランダムウォークが「すぐに混ざり合う」ことを意味する. この「すぐに混ざり合う」性質から, ランダムウォーク $(X_t)_{t\ge 0}$ が時刻 t までに訪れた頂点の集合を $U_t = \{X_0, \dots, X_t\}$ とすると, $|U_t|$ はすぐに拡大 (expand) していく.

例 1 完全グラフ.

例 2 閉路グラフ.

例 3 Petersen グラフ.

2.4.1 エクスパンダーの擬似ランダム性 (*)

この節は高次元エクスパンダーの本筋から少し外れるが, エクスパンダーグラフの重要であることの理由の一つとしてその擬似ランダム性について概説する.

加法的組合せ論や計算量理論では**擬似ランダム性 (pseudorandomness)** と呼ばれる概念が非常に重要な役割を果たしている.

定義 2.4.2 （分布の擬似ランダム性）

有限集合 Ω 上のある分布 μ と関数族 $\mathcal{F} = \{f\colon \Omega \to \{0,1\}\}$ を考える．分布 μ は, 任意の $f \in \mathcal{F}$ に対して

$$\left| \mathop{\mathbb{E}}_{x\sim\mu}[f(x)] - \mathop{\mathbb{E}}_{y\sim U_\Omega}[f(y)] \right| \leq \varepsilon$$

を満たすとき, $\mathcal{F}$ **に対して** ε**-擬似ランダムである**という (ここで, $y \sim U_\Omega$ とは Ω 上一様ランダムに y が選ばれたことを意味する).

直感的には, 分布が擬似ランダムであるとは, その分布が任意の $f \in \mathcal{F}$ を使っても一様分布と**識別できない (indistinguishable)** ことを意味する．例えば全変動距離に関する命題 1.2.2 では, $\mathcal{F}$ を V 上の二値関数全体 (すなわち任意の V の部分集合) の族としたときの識別不可能性のパラメータ ε が全変動距離で与えられることを意味する．すなわち μ は常に $d_{\mathrm{TV}}(\mu, U_\Omega))$-擬似ランダムである．関数クラス $\mathcal{F}$ をより制限したときにパラメータ ε がどこまで小さくなるかに興味がある．

組合せ論では $\mathcal{F}$ としてある特殊な関数クラスを仮定することによって**組合せ論的擬似ランダム性**を定義する．例えばグラフ理論や加法的組合せ論のコーナーストーンの一つと呼ばれる Szemerédi の正則化補題と呼ばれる結果は, 非常に大雑把に言えば任意の密なグラフが定数個の擬似ランダムな二部グラフと疎な部分に分解できることを主張する定理である．組合せ論的擬似ランダムネスの概念は特に加法的組合せ論において非常な協力な道具となっており, Green–Tao の定理の証明においても重要な役割を果たしている (驚くべきことに, 識別不可能性の枠組みで Green–Tao の定理の証明を理解してそれを学習理論におけるブースティングの証明に応用するという研究もなされている!).

計算量理論では $\mathcal{F}$ を「効率的なアルゴリズムの全体」や「素子数の少ない論理回路の全体」とすることで**計算量的擬似ランダム性**を定義できる．任意の効率的なアルゴリズムに対して一様ランダムな文字列と識別できないということは, その分布に従って生成されたメッセージを盗み見てもそこから得られる情報が何もない (ランダムな文字列を見てるのと同じ) であることから, 計算量的擬似ランダム性は暗号の計算量的安全性の定義の根幹をなすことがわかる．

エクスパンダーグラフの組合せ論的擬似ランダム性を説明する．正則 λ-エクスパンダー $G = (V, E)$ を考える．集合 $\Omega = V \times V$ 上の分布 $\mu = \mu_G$ として一様ランダムな辺 $\{u, v\} \in E$ を選び, (u, v) もしくは (v, u) どちらかを等確率で選んだ時の頂点対の分布とする．すなわち,

$$\Pr_{(u,v)\sim\mu}[(u,v) = (s,t)] = \frac{\mathbf{1}_{\{s,t\}\in E}}{2|E|} = \frac{\mathbf{1}_{\{s,t\}\in E}}{nd} \tag{2.6}$$

とする．関数族 $\mathcal{F}$ を

$$\mathcal{F} = \{f_{S,T}\colon (s,t) \mapsto \mathbf{1}_{s\in S, t\in T}\colon S, T \subseteq V\} \tag{2.7}$$

で定める．

補題 2.4.3 （エクスパンダー混交補題）

グラフ G が n 頂点 d-正則 λ-エクスパンダーであるとき, 式 (2.6) で定義された分布 μ は式 (2.7) で定義された関数族 $\mathcal{F}$ に関して ε-擬似ランダムである. すなわち, 任意の頂点部分集合 $S, T \subseteq V$ に対して, $e(S,T) = \sum_{s\in S, t\in T} \mathbf{1}_{\{s,t\}\in E}$ を S,T 間の辺の本数 ($S\cap T$ 内の辺は 2 回数える) とすると,

$$\left| e(S,T) - \frac{d}{n}|S||T| \right| \leq d\lambda \sqrt{|S||T|\left(1-\frac{|S|}{n}\right)\left(1-\frac{|T|}{n}\right)}.$$

証明. 系 2.2.5 を適用する.

□

2.4.2 エクスパンダー性の限界とラマヌジャングラフ

あとの節 (セクション 2.5) で説明するが, 応用上では正則なエクスパンダーグラフであってできるだけ辺の少ないものが重要である.

2.5 エクスパンダーグラフの応用

グラフのエクスパンダー性は組合せ論的な興味だけでなく, 理論計算機科学において多くの定理の証明の道具として非常に重要な役割を果たしている. ここではその一端を軽く紹介する.

2.5.1 脱乱択化

Albert Einstein は「量子は確率的に振る舞う」とする量子力学の枠組みに対して懐疑的であり, 1926 年に Max Born に宛てた手紙において

> Der Alte würfelt nicht. (神はサイコロを振らない)

と述べている. では, アルゴリズムの神はサイコロを振るだろうか? より具体的には, 乱択は計算能力を真に向上させるだろうか? この哲学的な問いは 90 年代から今もなお計算量理論において深く研究されており, その中心的なリーダーの一人である Avi Wigderson は 2021 年に Abel 賞, 2023 年に Turing 賞を受賞している.

ここではエクスパンダーグラフを使って「少ないサイコロで多くのサイコロの出目を hitting 性の意味で模倣できる」という結果を紹介する. $R_1, \ldots, R_t \in \{0,1\}^n$ を独立な確率変数で各 R_i を $\{0,1\}^n$ 上一様ランダムな文字列とする. 集合 $S \subseteq \{0,1\}^n$ を一つ固定し, $|S| \geq \delta 2^n$ とする. 直感的にはある n ビットの乱数を用いて確率 δ で成功する乱択アルゴリズム $\mathcal{A}$ を考え, そのアルゴリズムが成功するランダムシードの集合を S としている. アルゴリズム $\mathcal{A}$ を一度実行するだけでは成功確率は δ であるが, 独立に t 回走らせるとその確率を増加させることができ, t 回の試行の中で少なくとも一度は成功する確率は

$$\Pr[\exists i \in \{1,\ldots,t\}, R_i \in S] = 1-(1-\delta)^t \geq 1-\mathrm{e}^{-\delta t}$$

である. 従って試行回数 t を増やすと t に関して指数的に成功確率が上昇する. このとき, 全体で用いたランダムビットの長さは nt ビットである.

エクスパンダーグラフ上のランダムウォークを考えると成功確率に少しのロスが生じるものの, ランダムビットの長さを $n + t \log d$ ビットに減らすことができる ($d \in \mathbb{N}$ はパラメータで, 大きくするほど成功確率のロスが小さくできる). グラフ $G = (\{0,1\}^n, E)$ を d-正則 λ-エクスパンダーグラフとする (頂点集合が $V = \{0,1\}^n$ であることに注意).

2.5.2 誤り訂正符号

2.5.3 PCP 定理

2.5.4 擬似乱数生成器

2.5.5 エクスパンダーハッシュ

Chapter 3

高次元エクスパンダー概論

高次元エクスパンダーとはグラフのエクスパンダー性を単体複体に拡張した概念であり, 具体的にはエクスパンダー性を持つ単体複体を指す. 本チャプターでは高次元エクスパンダーの概要と重要な性質を紹介し, 次のチャプターにおいて具体的な応用として近年解決されたマトロイドに関する重要な未解決問題 Micali–Vazirani 予想の証明を与える.

3.1 定義

まずは単体複体に関する基礎的な用語を定義していく. 文脈によっては単体複体は多面体などを貼り合わせた幾何的な概念を指すこともあるが, 本講義では組合せ的ないわゆる set system としての単体複体を扱う.

定義 3.1.1 （単体複体）

有限集合 V と V の部分集合族 $\mathcal{F} \subseteq 2^V$ であって部分集合で閉じているもの (すなわち, $\sigma \subseteq \tau \in \mathcal{F} \Rightarrow \sigma \in \mathcal{F}$) の組 $X = (V, \mathcal{F})$ を**単体複体 (simplicial complex)** という. 集合族 $\mathcal{F}$ の元を**面 (face)** と呼び, 面 $\sigma \in \mathcal{F}$ の**次元 (dimension)** を $\dim \sigma = |\sigma| - 1$ とする[a]. 単体複体 X の次元を $\dim X = \max\{\dim \sigma \colon \sigma \in \mathcal{F}\}$ とする.
次元 d の単体複体 X は (包含関係に関して) 極大な面の次元が全て d に等しいとき, **純粋 (pure)** であるという. 整数 $-1 \leq k \leq \dim X$ に対し $X(k) = \{\sigma \in \mathcal{F} \colon \dim \sigma = k\}$ とする. 特に断りのない限り, $X(0) = V$ を仮定する (そうでなければ V として $V = X(0)$ とした単体複体を考える).

[a] 特に, 空集合 $\emptyset \in \mathcal{F}$ の次元は -1 である.

面の次元の概念は単体複体の幾何的な表現に由来する. このイメージになぞらえて, 次元 0 の面を**頂点 (vertex)**, 次元 1 の面を**辺 (edge)** と呼ぶことがある.

例 1. グラフ $G = (V, E)$ に対し, $\mathcal{F} = \{\emptyset\} \cup \{\{v\} \colon v \in V\} \cup E$ とすると, $(V, \mathcal{F})$ は単体複体である. また, 次元 2 以上の任意の単体複体 X に対して $(X(0), X(1))$ はグラフである.

例 2. 有限集合 V に対し, $\mathcal{F} = \binom{V}{\leq k} := \{\sigma \subseteq V \colon |\sigma| \leq k\}$ としたとき, $(V, \mathcal{F})$ は純粋な $(k+1)$-次元の単体複体である.

例 3. 閉路を含まないグラフを**森 (forest)** といい, 連結な森を**木 (tree)** という. 連結グラフ G の部分グラフであって木であるものを**全域木 (spanning tree)** という.

グラフ $G = (V, E)$ に対し, 森であるような部分グラフの辺集合からなる集合族 $\mathcal{F} \subseteq 2^E$ は単体複体である. すなわち,

$$\mathcal{F} = \left\{F \subseteq E \colon \text{部分グラフ } (V, F) \text{ は森}\right\}$$

に対して $(E, \mathcal{F})$ は単体複体である. 簡単のため G を連結グラフであるとすると, $(E, \mathcal{F})$ の極大面は G の全域木に対応し, その次元は $n-2$ に等しい. すなわち $(E, \mathcal{F})$ は純粋な $(n-2)$-次元単体複体である.

例 4. 実行列 $A \in \mathbb{R}^{n \times m}$ (ただし $m \geq n$) の行ベクトルを $\mathbf{a}_1, \ldots, \mathbf{a}_n$ とする. 集合 $V = \{1, \ldots, n\}$ の部分集合族であって, 線形独立な行ベクトル集合のインデックスとなるものの全体を $\mathcal{F}$ とする. すなわち

$$\mathcal{F} = \left\{I \subseteq V \colon (\mathbf{a}_i)_{i \in I} \text{は線形独立}\right\}$$

とすると, $(V, \mathcal{F})$ は純粋な単体複体であり, その次元は A のランク $\operatorname{rank}(A)$ に対し $\operatorname{rank}(A) - 1$ となる.

例 5. 部集合 L, R を持つ二部グラフ $G = (V, E)$ を考える. 辺部分集合 $M \subseteq E$ は, 部分グラフ (V, M) の全ての頂点の次数が高々 1 であるとき**マッチング (matching)** という. マッチング M の部分集合 $M' \subseteq M$ もまたマッチングであるため, グラフ G のマッチング全体からなる辺部分集合族 $\mathcal{F} \subseteq 2^E$ に対し, $(E, \mathcal{F})$ は単体複体である. 一般に極大マッチングのサイズは異なる場合があるのでこの単体複体は純粋ではない (図 3.1).

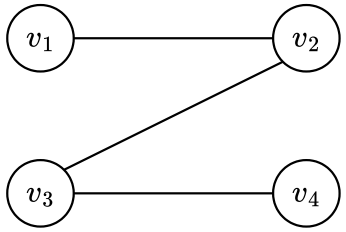

Figure 3.1: マッチング $M_1 = \{v_1, v_2\}, \{v_3, v_4\}\}$ と $M_2 = \{\{v_2, v_3\}\}$ はどちらも極大である.

定義 3.1.2 （リンクとスケルトン）

単体複体 $X = (V, \mathcal{F})$ を考える. 面 $\sigma \in \mathcal{F}$ の**リンク (link)** とは単体複体 $(V \setminus \sigma, \mathcal{F}_\sigma)$ であって集合族 $\mathcal{F}_\sigma$ が

$$\mathcal{F}_\sigma = \{\tau \setminus \sigma \colon \sigma \subseteq \tau \in \mathcal{F}\}$$

で与えられるものである. 次元 k 以下の面の集合

$$\mathcal{F}_k = \{\sigma \in \mathcal{F} \colon \dim \sigma \leq k\}$$

に対し $(V, \mathcal{F}_k)$ を **k-スケルトン (k-skelton)** という.

3.2 単体複体上のランダムウォーク

グラフ上のランダムウォークは頂点集合上で遷移するものを考えていたが, 単体グラフ上のランダムウォークは同じ次元の面の間で遷移するものを考える. アイデアとしては, セクション 1.6 で考えたようにある次元 k の面から次元 $k+1$ の面に遷移する上昇ウォークと逆に次元 $k+1$ の面から次元 k の面に遷移する下降ウォークを組み合わせることによって, $X(k)$ 上のランダムウォークを定義する.

定義 3.2.1 （上昇ウォークと下降ウォーク）

純粋な d 次元単体複体 $X = (V, \mathcal{F})$ を考える.

3.3 局所スペクトルエクスパンダー

3.4 Oppenheim のトリクルダウン定理

Chapter 4

マトロイド

マトロイド (matroid) は「行列 (matrix) のようなもの (-oid)」という名を冠するが, 線形代数における線型独立性をグラフの全域木などに拡張した概念である.

4.1 定義

定義 4.1.1 （マトロイド）

次の性質を持つ単体複体 $(V, \mathcal{F})$ を**マトロイド (matroid)** という: 任意の $\sigma, \tau \in \mathcal{F}$ に対し, $|\sigma| < |\tau|$ ならば, ある $u \in \tau \setminus \sigma$ が存在して $\sigma \cup \{u\} \in \mathcal{F}$.

4.2 例

4.2.1 グラフ的マトロイド

4.2.2 線形マトロイド

4.3 モチベーション

4.3.1 組合せ最適化

4.3.2 組合せ論

4.4 基の数え上げ

4.5 Anari, Liu, Gharan, Vinzant の定理