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. 一方でその特殊性はときに重要な意義を持ち, その分野において重要な役割を果たすことがある. そしてこの独自性を俯瞰的に見て一般化した理論を整備していくこともまた数学の重要なプロセスであろう.

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, いわゆる応用数学の一つだが, そのレイヤーは (機械学習や最適化と比べると) 非常に低い階層にあるため, 実は純粋数学の抽象的な概念や道具をある程度の原型を保ったまま応用できる貴重な分野である. 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, 日本国内における純粋数学と理論計算機科学の間のつながりをより強固にするきっかけの一つになれば幸甚である.

Chapter 1

ランダムウォーク概論

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び, ランダムウォークが収束するために必要な条件を与える.

1.1 記号

まず, 本講義の全てのチャプターで共通する記法とその定義を与える.

- 有限集合 V 上の確率分布 μ を V 次元ベクトルと同一視する. すなわち, 固定した $u \in V$ に対し, 分布 μ に従ってランダムに選ばれた元が u である確率を $\mu(u)$ で表す.
- 分布 $\mu \in [0,1]^V$ と部分集合 $S \subseteq V$ に対し $\mu(S) = \sum_{u \in S} \mu(u)$ とする.
- 有限集合 V 上の確率分布 $\mu \in [0,1]^V$ に対し, $u \sim \mu$ と書くと u は分布 μ に従ってランダムに選ばれた要素とする.
- 全ての行和が 1 に等しい非負行列を**確率行列 (stochastic matrix)** と呼ぶ. すなわち, $P \in [0,1]^{U \times V}$ が確率行列であるとは, 全ての $u \in U$ に対し $\sum_{v \in V} P(u,v) = 1$ が成り立つことを意味する.
- 確率行列 $P \in [0,1]^{U \times V}$ と $u \in U$ に対し, $P(u,\cdot) \in [0,1]^V$ を P の第 u 行ベクトルから定まる分布とする. 例えば, $v \sim P(u,\cdot)$ は分布 $P(u,\cdot)$ に従ってランダムに選ばれた元を意味する.

1.2 定義

定義 1.2.1 （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.

厳密には初期分布 X_0 と遷移確率行列 P を定めないとランダムウォークは一意に定まらないが, しばし遷移確率行列 P だけを指定して「P に従うランダムウォーク」という言い回しをする. このとき, 暗に初期分布 X_0 は任意の分布を考えており, 例えば「P に従うランダムウォークは性質 $\mathcal{P}$ を満たす」と言ったときは「遷移確率行列が P で与えられた任意のランダムウォークは性質 $\mathcal{P}$ を満たす」ということを意味する.

1.3 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 1.3.1 (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 1.3.2

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 1.3.3 （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.

1.3.1 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 1.3.4 （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 1.3.5 （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.

1.3.2 混交時間

定理 1.3.5 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 1.3.6 （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 1.3.7 （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.

1.4 グラフ上のランダムウォーク

まずグラフ理論の基礎的な概念の定義を与える. 読者は定義 1.4.3 まで読み飛ばし, 必要に応じて後から定義を参照してもよい.

定義 1.4.1 （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.

- 隣接行列 $A \in \mathbb{R}^{V\times V}$ を以下で定義する:

$$A(u,v) = \mathbf{1}_{\{u,v\}\in E} = \begin{cases} 1 & \text{if } \{u,v\} \in E, \\ 0 & \text{otherwise.} \end{cases}$$

- 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.

- 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.

- 二頂点 u,v の間の**距離 (distance)** を, uv 間の路のうちの最小長さで定義し, $\mathrm{dist}(u,v)$ で表す (uv 路が存在しない場合は $\mathrm{dist}(u,v) = \infty$ とする). グラフ G の**直径 (diameter)** を $\mathrm{diam}(G) = \max_{u,v\in V} \mathrm{dist}(u,v)$ で定める.

- 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.

- 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.

路とは辺を辿って始点から終点に至るまでの経路を表す. なお, 同じ頂点や辺を 2 回以上通ってもよいことに注意せよ.

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.

隣接行列 A に対し, A^ℓ の各成分は長さ ℓ の路の個数に等しい.

補題 1.4.2

グラフ $G=(V,E)$ の隣接行列 A と $\ell \in \mathbb{N}$ を考える. 任意の $u,v \in V$ に対し, $A^\ell(u,v)$ は頂点 u から v への長さ ℓ の路の個数に等しい.

証明. 長さ $\ell \geq 1$ に関する帰納法で示す. $\ell = 1$ のときは明らか. $W_\ell(u,v)$ を頂点 u から v への長さ ℓ の路の個数とすると, $A^\ell = W_\ell$ を示せばよい. 帰納法の仮定として $A^{\ell-1} = W_{\ell-1}$ とする. W_ℓ に関する漸化式を考える. 頂点 u から v への長さ ℓ の任意の路は, ある $w \in V$ に対して uw 間の長さ $\ell-1$ の路と辺 wv を連結させることによって得られる. 従って漸化式

$W_\ell(u,v) = \sum_{w\in V} W_{\ell-1}(u,w)\cdot A(w,v)$ が成り立つので, 帰納法の仮定より $W_\ell = W_{\ell-1}A = A^\ell$ を得る. □

1.4.1 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 1.4.3 （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.

1.4.2 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 1.4.4 （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.

1.4.3 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 1.3.5 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集合 E 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.

1.4.4 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 1.4.5 （重み付きランダムウォーク）

グラフ $G = (V, E)$ に対し, 関数 $w\colon E \to \mathbb{R}_{>0}$ を**辺重み (edge weight)** という. 頂点 u から v に遷移する確率 $P(u, v)$ が辺重み $w(\{u, v\})$ に比例するような V 上の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. すなわち, 重み付きランダムウォークとは以下の定常分布 P を持つランダムウォークである:

$$P(u,v) = \begin{cases} \frac{w(\{u,v\})}{\deg_W(u)} & \text{if } \{u,v\} \in E, \\ 0 & \text{otherwise.} \end{cases}$$

ここで, $\deg_W(u) = \sum_{v\colon \{u,v\}\in E} w(\{u, v\})$ は頂点 u の重み付き次数とする.

辺重み w を常に 1 を返す関数とすれば, G 上の単純ランダムウォークと同一である. 自己遷移は発生しないので単純遅延ランダムウォークは表現できない. 重み付きランダムウォークの概念は後で単体複体上での局所的なランダムウォークの定義 (定義 3.3.1) で用いる.

1.5 ランダムウォークの固有値と可逆性

遷移確率行列 $P \in [0, 1]^{V\times V}$ 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 1.3.5 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できる.

遷移確率行列 $P \in [0, 1]^{n\times n}$ の固有値[1] $\lambda_1, \ldots, \lambda_n$ 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 1.5.1 （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 $\lambda_1, \ldots, \lambda_n$ とすると, 全ての $i \in \{1, \ldots, n\}$ 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 $\{c\mathbf{1}\colon c \in \mathbb{R}\}$ となる), 他の固有値は全て絶対値が真に 1 より小さい.

ランダムウォークの固有値の議論の土台となるのが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.

定義 1.5.2 （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

$$\forall u, v \in V, \pi(u)P(u, v) = \pi(v)P(v, u) \tag{1.4}$$

[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.

を満たすとき**可逆 (reversible)** であるという.

式 (1.4) 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 (1.4) $\iff$ $\Pi P = (\Pi P)^\top$ 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

$$P^*(v,u) = \Pr[X_0 = u | X_1 = v] = \frac{\Pr[X_0 = u \text{ and } X_1 = v]}{\Pr[X_1 = v]} = \frac{\pi(u)P(u,v)}{\pi(v)} \tag{1.5}$$

が得られる. もし元のランダムウォークが可逆ならば, 式 (1.4) 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 (1.5) 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. 同様に, 重み付きランダムウォークもまた可逆である.

例 2. 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 (1.4) を満たす分布 π は定常分布であることを示せ．

1.6 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 1.6.1

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 1.6.1 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 1.6.2

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 (1.5) 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 1.6.3 （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

$$A := \sqrt{\Pi} P \sqrt{\Pi}^{-1} \tag{1.6}$$

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 1.6.3 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 1.6.3 を適用すればよい.

定理 1.6.4 （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 (1.6) 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 $(x_i)_{i=1,\ldots,n}$ は空間 $\ell^2_\pi(V)$ の正規直交基底である. さらに

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

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. □

空間 $\ell^2_\pi(V)$ 上での期待値と分散を以下のように定義する:

定義 1.6.5 （期待値と分散）

定理 1.6.4 と同じ仮定の下で, $f \in \ell^2_\pi(V)$ の期待値と分散を

$$\mathbf{E}_\pi[f] := \langle f, \mathbf{1} \rangle_\pi = \sum_{u \in V} \pi(u) f(u), \tag{1.7}$$

$$\mathbf{Var}_\pi[f] := \left\| f - \mathop{\mathbb{E}}_\pi[\mathbf{1}] \right\|^2_\pi = \mathop{\mathbb{E}}_\pi[f^2] - (\mathop{\mathbb{E}}_\pi[f])^2 \tag{1.8}$$

とする.

すなわち, 関数 $f \colon V \to \mathbb{R}$ を, ランダムに選ばれた $u \sim \pi$ に対して $f(u)$ を出力する確率変数とみなしてその平均と分散をそれぞれ $\mathbf{E}_\pi[f], \mathbf{Var}_\pi[f]$ とした. 以後, 特に混乱がない限り, $\mathbf{E}_\pi[f]$ や $\mathbf{Var}_\pi[f]$ は $\mathbf{E}_\pi f$ や $\mathbf{Var}_\pi f$ などとも表す. 同様に共分散 $\mathrm{Cov}_\pi(f, g)$ を $\langle f, g \rangle_\pi - \mathbf{E}_\pi f \cdot \mathbf{E}_\pi g$ で定義できるが, この値は以下の性質を持つ.

補題 1.6.6

任意の $f, g \in \ell^2_\pi(V)$ に対し,

$$|\langle f, g \rangle_\pi - \mathbf{E}_\pi f \cdot \mathbf{E}_\pi g| \le \sqrt{\mathbf{Var}_\pi f \cdot \mathbf{Var}_\pi g}.$$

証明. 定理 1.6.4 で得られる $\ell^2_\pi(V)$ の正規直交基底を $x_1, \ldots, x_n$ とし, 関数 f, g をこれらの線形結合

$$f = \mathbf{E}_\pi f \cdot \mathbf{1} + \sum_{i=2}^{n} f_i x_i,$$

$$g = \mathbf{E}_\pi g \cdot \mathbf{1} + \sum_{j=2}^{n} g_j x_j$$

で表す. ここで $f_i = \langle f, x_i \rangle_\pi, g_j = \langle g, x_j \rangle_\pi$ であり, $x_1 = \mathbf{1}$ なので $f_1 = \mathbf{E}_\pi f, g_1 = \mathbf{E}_\pi g$ である. 特に, 基底 (x_i) の直交性より従って

$$\begin{aligned} |\langle f, g \rangle_\pi - \mathbf{E}_\pi f \cdot \mathbf{E}_\pi g| &\le \sum_{i \ge 2} |f_i||g_i| \\ &\le \sqrt{\sum_{i \ge 2} f_i^2} \cdot \sqrt{\sum_{j \ge 2} g_j^2} \qquad \because \text{Cauchy–Schwarz の不等式} \\ &= \sqrt{\mathbf{Var}_\pi f} \cdot \sqrt{\mathbf{Var}_\pi g} \end{aligned}$$

より主張を得る. □

1.7 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 1.7.1

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 $1=\lambda_1 \geq \cdots \geq \lambda_n \geq -1$ に対し, $\lambda_i(P)=\lambda_i$, $\lambda(P):=\max\{|\lambda_2|,|\lambda_n|\}$ とする. 特に, $\gamma:=1-\lambda(P)$ を**スペクトルギャップ (spectral gap)** と呼ぶ.

先確率行列 P を作用させると分散が減少する.

補題 1.7.2

遷移確率行列 P と関数 $f \in \ell^2_\pi(V)$ に対し

$$(Pf)(u) := \sum_{v\in V} P(u,v)f(v)$$

とする. このとき,

$$\begin{aligned}&\mathbf{E}_\pi[Pf] = \mathbf{E}_\pi f,\\ &\mathbf{Var}_\pi[Pf] \leq \lambda(P)^2 \cdot \mathbf{Var}_\pi[f].\end{aligned}$$

証明は演習問題とする.

演習問題 3

補題 1.7.2 を証明せよ.

この補題の重要な系としてエクスパンダー混交補題と呼ばれる重要な結果を得る. エクスパンダー混交補題についてはセクション 2.3.3 でより詳しく紹介する.

系 1.7.3 (可逆ランダムウォークに対するエクスパンダー混交補題)

可逆なランダムウォークの遷移確率行列 P を考える. 任意の関数 $f,g \in \ell^2_\pi(V)$ に対し,

$$|\langle f, Pg\rangle_\pi - \mathbf{E}_\pi f \cdot \mathbf{E}_\pi g| \leq \lambda(P)\cdot\sqrt{\mathbf{Var}_\pi f \cdot \mathbf{Var}_\pi g}.$$

混交時間とスペクトルギャップの間には以下の関係が知られている:

補題 1.7.4 (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

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

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

証明. 定理 1.6.4 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

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

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

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

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. □

Chapter 2

エクスパンダーグラフ

2.1 定義

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 2.1.1 （エクスパンダー）

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 P が $\lambda(P) \leq \lambda$ 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 $\lambda_2 \leq \lambda$ 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 $(X_t)_{t\geq 0}$ が時刻 t までに訪れた頂点の集合を $U_t = \{X_0, \ldots, X_t\}$ とすると, $|U_t|$ はすぐに拡大 (expand) していく.

例 1 完全グラフ. グラフ $\left(V, \binom{V}{2}\right)$ を**完全グラフ (complete graph)** という. n 頂点完全グラフ上の単純ランダムウォークの遷移確率行列 P は, 単位行列 I と全成分が 1 の行列 J を用いて $P = \frac{1}{n-1}(J - I)$ で表せる. 完全グラフは正則グラフなので定常分布 π は V 上の一様分布である. 第一固有値は $\mathbf{1}$ であり, その他の固有ベクトル $x_i (i \geq 2)$ は全て $\mathbf{1}$ に直交し, 特に $Jx_i = 0$ となる. 従って $Px_i = -\frac{1}{n-1}x_i$ なので, $\lambda_1 = 1$, $\lambda_2 = \cdots = \lambda_n = -\frac{1}{n}$ である. よって, n 頂点完全グラフは $(1/n)$-expander であると同時に片側 $(-1/n)$-エクスパンダーグラフである ($\lambda(P)$ の定義では絶対値をつけているが片側エクスパンダー性の定義では絶対値をつけていないことに注意).

例 2 閉路グラフ. 頂点数 n の閉路グラフとは, 頂点集合 $V = \{v_1, \dots, v_n\}$ に対して辺集合 E が $E = \{\{v_1, v_2\}, \dots, \{v_{n-1}, v_n\}, \{v_n, v_1\}\}$ で与えられるグラフ (V, E) である. 頂点数 n が偶数のとき, 閉路グラフは二部グラフとなる.

ここでは $\omega = \exp\left(\frac{2\pi \mathrm{i}}{n}\right)$ を 1 の冪根とし, 頂点集合を $V = \{\omega^i : i = 0, \dots, n-1\}$ とし, 各辺を $\{\omega^i, \omega^{i+1}\}$ で表す. 任意の関数 $f : V \to \mathbb{R}$ に P を作用させると

$$Pf(\omega^i) = \frac{f(\omega^{i-1}) + f(\omega^{i+1})}{2}$$

を得る. 関数 $x_k : \omega^j \mapsto \omega^{kj}$ を考えると, $Px_k(\omega_j) = \frac{\omega^{k(j-1)} + \omega^{k(j+1)}}{2} = \frac{\omega^{-k} + \omega^{-k}}{2} \cdot x_k(\omega_j)$ を得る. 従って各 $k = 0, \dots, n-1$ に対し x_k はそれぞれ固有値 $\frac{\omega^k + \omega^{-k}}{2} = \cos\frac{2\pi k}{n}$ に対応する固有ベクトルである.

これらの固有値を降順に並べて $1 = \lambda_1 \geq \cdots \geq \lambda_n \geq -1$ とすると, $\lambda_2 = \cos\frac{2\pi}{n} = 1 - \frac{4\pi^2}{2n^2} + O(n^{-4})$ である. 頂点数 n が偶数のときは $\lambda_n = -1$, 頂点数 n が奇数のときは $\lambda_n = \cos\pi\left(1 - \frac{1}{n}\right) = -\cos\frac{\pi}{n} = -1 + \frac{\pi^2}{2n^2} - O(n^{-4})$ である. 従って頂点数 n が奇数のときの閉路グラフは $\cos\frac{\pi}{n}$-エクスパンダーであり, $n \to \infty$ の漸近を考えると n のスペクトルギャップは $\Theta(1/n^2)$ となる.

2.2 存在性と陽な構成

エクスパンダー性はランダムウォークがすぐに混ざり合うということを意味し, これを満たすグラフは多くの辺を持つべきである. 例えば完全グラフは非常に強いエクスパンダー性を持つ一方で閉路グラフのエクスパンダー性は乏しい. では, 疎でありかつエクスパンダー性をもつグラフは存在するだろうか? また, 陽に構成できるだろうか?

2.2.1 ケイリーグラフ

エクスパンダーグラフを陽に構成する最も重要なアプローチの一つとして幾何学的群論におけるケイリーグラフと呼ばれる概念が知られている.

定義 2.2.1 （ケイリーグラフ）

G を有限群, $A \subseteq G$ を G の生成系[a]であって単位元を含まず, 逆元で閉じている (i.e., $A^{-1} = \{a^{-1} : a \in A\} = A$) ものとする. 頂点集合 $V = G$, 辺集合 $E = \{\{g, ag\} : g \in G, a \in A\}$ に対し (V, E) で与えられるグラフを**ケイリーグラフ (Cayley graph)** といい, $\mathrm{Cay}(A, G)$ で表す. 頂点 $g \in G$ に対し, $E_g = \{\{g, ag\} : a \in A\}$ を g を含む辺の集合とする.

[a] 任意の $g \in G$ に対してある有限個の $a_1, \dots, a_m \in A$ を用いて $g = \prod_{i=1}^{m} a_i$ と表せるとき, $A \subseteq G$ は生成系であるという.

ケイリーグラフは生成系 A の幾何学的な性質を調べる幾何学的群論における重要な研究対象の一つである. A は単位元を含まないため自己ループは存在しない. また, $A^{-1} = A$ より $\{ag, a^{-1}(ag)\} \in E$ となるため $\mathrm{Cay}(A, G)$ は無向グラフとなっている. 同様にケイリーグラフ $\mathrm{Cay}(G, A)$ も考えることができるが, 写像 $x \mapsto x^{-1}$ を考えると $\mathrm{Cay}(A, G)$ と $\mathrm{Cay}(G, A)$ が同型になっているので本質的には同じである. ケイリーグラフ $\mathrm{Cay}(A, G)$ は $|A|$-正則グラフである.

2.2.2 エクスパンダー性の限界とラマヌジャングラフ (*)

グラフの辺数を固定したとき, エクスパンダー性のパラメータ λ はどこまで小さくできるだろうか? ここでは厳密な証明は与えずに直感的な議論によって正則グラフに絞ってエクスパンダー性の限界を説明する.

あとの節 (セクション 2.4) で詳しく述べるが, 応用上は正則なエクスパンダーグラフが重要である. 正則グラフ上のランダムウォークの遷移確率行列は単に隣接固有値を次数で割ったものであり定常分布も一様分布なので単に隣接行列の固有値を考えれば良いことがわかる.[1]

固定した自然数 $d \geq 3$ に対して最もエクスパンダー性の強い (つまり λ が最小となる)d-正則グラフはどのようなグラフだろうか? 問題を言い換えればランダムウォークがより多くの頂点を訪れやすくするにはグラフをどのように構成すれば良いだろうか?

理想的なグラフ: d-正則無限木. 直感的な議論だが, 短い閉路があるとそれに沿って同じ頂点を訪れてしまうので, そのような閉路はない方が良いと思われる. 従ってそのグラフを虫眼鏡でズームすると局所的には木構造になっているべきであろう. そこで「理想的な」グラフとして d-正則で頂点数が無限の木 T を考える. 頂点集合 V は加算無限であるため, 有限グラフに対する隣接行列や固有値の概念を無限グラフに拡張したものが必要である. 集合 $\ell^2(V) \subseteq \mathbb{R}^V$ を $\ell^2(V) = \left\{f\colon V \to \mathbb{R}\colon \sum_{u\in V} f(u)^2 < \infty\right\}$ とする. 隣接作用素 $A\colon \ell^2(V) \to \ell^2(V)$ を

$$Af(u) = \sum_{v\in N_T(u)} f(v)$$

で定める. ここで $N_T(u) \subseteq V$ は T において u と隣接している頂点の集合であり, T の d-正則性から有限集合である. 作用素 A のスペクトルを

$$\mathrm{spec}(A) = \left\{\lambda \in \mathbb{R}\colon A - \lambda I \text{ は可逆でない}\right\}$$

とする.

定理 2.2.2

d-正則無限木 T の隣接作用素 A のスペクトルは以下を満たす:

$$\mathrm{spec}(A) \subseteq [-2\sqrt{d-1}, 2\sqrt{d-1}].$$

従って, 理想的なグラフを考えるとその隣接行列の非自明な固有値はその絶対値が高々 $2\sqrt{d-1}$ である (第一固有ベクトル $\mathbf{1}$ に対応する関数は $\ell^2(V)$ に属さない). よって任意の d-正則グラフは $\lambda(P) \geq \frac{2\sqrt{d-1}}{d}$ を満たすであろうことが予想される.

Alon-Boppana の定理. 定数次数の正則グラフの直径は $\Omega(\log n)$ を満たす.

[1] これらの理由からエクスパンダーグラフの理論は多くの教科書では正則グラフ上でのみ展開されている.

補題 2.2.3

$d \geq 3$ のとき, n 頂点 d-正則連結グラフ $G = (V, E)$ の直径は $\operatorname{diam}(G) \geq \log_{d-1} \frac{(d-2)(n-1)}{d}$ を満たす.

証明. 頂点 $u \in V$ を固定すると, u から ℓ 本以下の辺を辿って辿り着ける頂点は高々

$$1 + d + d(d-1) + \cdots + d(d-1)^{\ell-1} \leq 1 + d(d-1)^{\ell-1} \sum_{i=0}^{\ell-1} \left(\frac{1}{d-1} \right)^i \leq 1 + \frac{d(d-1)^\ell}{d-2}$$

この値が n より真に大きいとき, u から ℓ 本以下の辺を辿って辿り着けない頂点が存在し, これは $\operatorname{diam}(G) \geq \ell$ を意味する. これを解くと $\ell > \log_{d-1} \frac{(d-2)(n-1)}{d}$ を得る. □

定理 2.2.4 （Alon–Boppana の定理）

ある定数 $c > 0$ が存在し, 任意の n 頂点 d 正則グラフ G 上の単純ランダムウォークの遷移確率行列 P の第二固有値 λ_2 は

$$\lambda_2 \geq \frac{2\sqrt{d-1}}{d} \left(1 - \frac{c}{\operatorname{diam}(G)^2} \right)$$

を満たす.

特に, 補題 2.2.3 より, 次数 $d \geq 3$ を固定して頂点数 $n \to \infty$ の漸近において $\ell = \Omega(\log n)$ であるため, $\lambda_2 \geq \frac{2\sqrt{d-1}}{d}(1 - O(1/\log^2 n))$ を満たす. この結果は次数 d を固定したときの正則グラフのエクスパンダー性のパラメータの限界を表している.

ここでは少し弱い下界として

$$\lambda_2 \geq \frac{2\sqrt{d-1}}{d} \left(1 - O\left(\frac{\log \operatorname{diam}(G)}{\operatorname{diam}(G)} \right) \right) \tag{2.1}$$

を証明する. この下界でも $\lambda_2 \geq \frac{2\sqrt{d-1}}{d}(1 - o(1))$ を示すには十分である.

式 (2.1) の証明. 遷移確率行列を P とし, 隣接行列を A とする. 二頂点 u, v を uv 間の最短路が $\operatorname{diam}(G)$ に等しくなるように固定し関数 $f \colon V \to \mathbb{R}$ を $f = \delta_s - \delta_t$ とすると, 任意の $k \geq 1$

に対して

$$\begin{aligned}
\lambda(P^{2k}) &= \lambda(P^k)^2 \\
&\geq \frac{\mathbf{Var}_\pi[P^k f]}{\mathbf{Var}_\pi[f]} && \because \text{補題 1.7.2} \\
&= \frac{\left\|P^k f\right\|_\pi^2}{\|f\|_\pi^2} && \because \mathbf{E}_\pi f = \mathbf{E}_\pi[P^k f] = 0 \\
&= \frac{\left\langle f, P^{2k} f\right\rangle_\pi}{\|f\|_\pi^2} && \because \text{補題 1.6.2} \\
&= \frac{P^{2k}(u,u) + P^{2k}(v,v) - 2P^{2k}(u,v)}{2} \\
&= \frac{A^{2k}(u,u) + A^{2k}(v,v) - 2A^{2k}(u,v)}{2d^{2k}}. && \because P = \frac{1}{d}A
\end{aligned}$$

補題 1.4.2 より, $k = \left\lfloor \frac{\mathrm{diam}(G)-1}{2} \right\rfloor$ とすると, u, v の選び方より $A^{2k}(u,v) = 0$ である. 補題 1.4.2 より, $A^{2k}(u,u)$ は頂点 u を含む長さ $2k$ の閉路の個数に等しい. さらに, この値は d-正則無限木 T において固定した頂点を含む長さ $2k$ の閉路の個数で下から抑えることができる.

補題 2.2.5 （正則グラフの閉路数の下界）

$d \geq 3$ に対し, T を d-正則無限木とし, 頂点を一つ固定する. この頂点を含む長さ $2k$ の閉路の個数を t_{2k} とすると

$$t_{2k} = d(d-1)^{k-1} \cdot \frac{1}{k+1}\binom{2k}{k}$$

である. さらに, 任意の d-正則グラフ $G = (V, E)$ の任意の頂点 u に対し, u を含む長さ $2k$ の閉路の個数は少なくとも t_{2k} である.

まずは補題 2.2.5 を認めて定理 2.2.4 の証明を完成させる (補題 2.2.5 は後で証明する). 二項係数 $\binom{2k}{k}$ は Stirling の近似により $\binom{2k}{k} \geq \frac{4^k}{\sqrt{\pi k}}\left(1 - \frac{1}{8k}\right)$ を満たすことが示せる. 従って, 補題 2.2.5 より,

$$\begin{aligned}
\lambda(P)^{2k} &\geq d^{-2k} t_{2k} \\
&\geq d^{-2k} \cdot (d-1)^k \cdot \frac{2^{2k}}{(k+1)\sqrt{\pi k}}\left(1 - \frac{1}{8k}\right).
\end{aligned}$$

特に, ある定数 $c > 0$ が存在して

$$\begin{aligned}
\lambda(P) &\geq \frac{2\sqrt{d-1}}{d} \cdot k^{-c/k} \\
&\geq \frac{2\sqrt{d-1}}{d} \cdot \left(1 - O\left(\frac{\log k}{k}\right)\right).
\end{aligned}$$

最後の不等号は $k^{-k} = \mathrm{e}^{-\frac{\log k}{k}} = 1 - O\left(\frac{\log k}{k}\right)$ を用いた. $k = \left\lfloor \frac{\mathrm{diam}(G)-1}{2} \right\rfloor$ を代入すれば式 (2.1) を得る. □

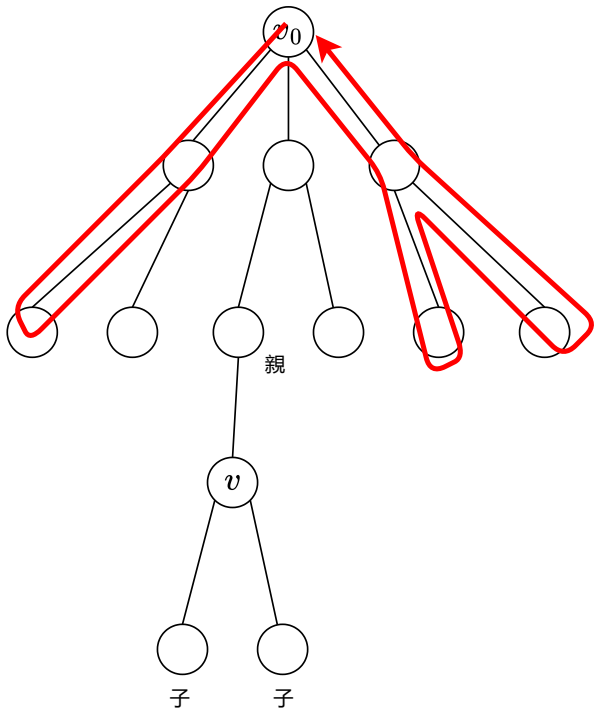

図 2.1: 3 正則木 T 上の長さ 10 の閉路. 親から子への遷移と子から親への遷移を 5 回ずつ行う.

最後に補題 2.2.5 を証明する.

補題 *2.2.5* の証明. d-正則無限木 T の特別な頂点 v_0 を一つ固定し, (グラフ理論においてスタンダードな) 幾つかの用語を定義する. 固定した特別な頂点 v_0 を**根 (root)** と呼び, T の頂点 v に対し, $\mathrm{dist}(v_0, v)$ を**深さ (depth)** と呼び $\mathrm{depth}(v)$ で表す (特に $\mathrm{depth}(v_0) = 0$ である). 頂点 v に T 上で隣接している d 個の頂点からなる集合を $N_T(v)$ と表す ($N_T(v)$ に v は含めない). これらの隣接頂点のうち, 深さが $\mathrm{depth}(v) - 1$ となるただ一つの頂点を v の**親 (parent)** と呼び, 残りの深さ $\mathrm{depth}(v) + 1$ の頂点を v の**子 (child)** と呼ぶ.

木 T において根を始点とする長さ $2k$ の閉路 $(v_0, \ldots, v_{2k})$ を考える (ここで $v_0 = v_{2k}$). 各 i に対して $d_i = \mathrm{depth}(v_i)$ とし, 列 $(d_0, \ldots, d_{2k})$ を考える. まず $d_0 = 0$ であり, その後は $d_{i+1} \in \{d_i \pm 1\}$ であり, 常に非負性を保ちながら最後に $d_{2k} = 0$ となる. このような列 $(d_0, \ldots, d_{2k})$ の総数はカタラン数と等しく, $\frac{1}{k+1}\binom{2k}{k}$ に等しい. 特に, 各 $d_i - d_{i-1}$ の符号を見ると $d_0 = d_{2k} = 0$ より正と負がそれぞれ k 個ずつ含まれている.

次に, 各 $(d_1, \ldots, d_{2k})$ に対して深さの履歴がこれと等しくなるような閉路の個数を考える. まず, $i = 1$ において, 頂点 v_0 からは子に遷移するため v_1 の取り方は d 通りある. 各 $i \geq 2$ において, $d_i = d_{i-1} + 1$ (すなわち v_i が v_{i-1} の子である) とき, v_i の選び方は $d - 1$ 通りある. 一方で親に遷移する場合はその遷移先は一意である. 子への遷移はちょうど k 回発生するため, 深さの履歴が与えられた $(d_1, \ldots, d_{2k})$ に等しくなるような閉路の個数は $d(d-1)^{k-1}$ に等しい. 従って $t_{2k} = \frac{1}{k+1}\binom{2k}{k} \cdot d(d-1)^{k-1}$ を得る.

後半の主張を証明する. d-正則グラフ G の頂点 u_0 を一つ固定する. 木 T の頂点集合を U, グラフ G の頂点集合を V とし, N_T の定義と同様にグラフ G の頂点 $v \in V$ に対しその d 個の隣接頂点の集合を $N_G(v)$ で表す. G から T への準同型写像 $\phi\colon U \to V$ を以下のように構成す

る[2]: 深さに関して帰納的に定義する.

- まず, $\phi(v_0) = u_0$ とする. 根 v_0 の子 $N_T(v_0)$ から $N_G(u_0)$ への全単射 ϕ_0 を任意に一つ選び, $\phi\colon N_T(v_0) \ni v' \mapsto \phi_1(v') \in N_T(u_0)$ によって $N_T(v_0)$ における ϕ を定義する.
- T における深さ ℓ 以下の全ての頂点に対し $\phi(v)$ が定義されているとする. 深さ ℓ の各頂点 v に対し, その親を p, 子を $c_1, \dots, c_{d-1}$ とする. v とその親 p に対しては $u := \phi(v)$, $u_p := \phi(p) \in U$ が定義されている. このとき, 全単射 $\psi\colon N_T(v) \setminus \{p\} \to N_G(u) \setminus \{u_p\}$ を任意に一つ固定し, 各 $\phi(c_j)$ を $\psi(c_j) \in V$ とする.

このようにして定義された写像 $\phi\colon U \to V$ は確かに準同型なので T の閉路 $(v_0, \dots, v_{2k})$ に対して $(\phi(v_0), \dots, \phi(v_{2k}))$ は G の閉路になっている. さらに, $(\phi(v_0), \dots, \phi(v_{2k}))$ の形になっている G の閉路が与えられたとき, v_0 は一意に定まり, 以降の v_i は ϕ の帰納的な定義で用いた全単射の逆写像を用いて順番に復元することができるため, $(v_0, \dots, v_{2k}) \mapsto (\phi(v_0), \dots, \phi(v_{2k}))$ は単射である. 従ってグラフ G に含まれるある頂点を始点とした長さ $2k$ の閉路の個数は少なくとも t_{2k} である. □

ラマヌジャングラフ. 漸近的に定理 2.2.4 を達成するグラフを**ラマヌジャングラフ (Ramanujan graph)** という.

定義 2.2.6 （ラマヌジャングラフ）

d-正則グラフ $G = (V, E)$ は, その単純ランダムウォークの遷移確率行列 P の第二固有値 λ_2 が $\lambda_2 \leq 2\sqrt{d-1}$ を満たすとき, **ラマヌジャングラフ (Ramanujan graph)** という.

定理 2.2.4 を達成するグラフ列, すなわち, 次数 d を固定したときに頂点数が増大していくグラフ列 $(G_n)_{n\in\mathbb{N}}$ であって各 G_n が d-正則ラマヌジャングラフとなるものは存在するだろうか? この漸近的に最適な正則エクスパンダーグラフの構成は Lubotzky, Phillips, and Sarnak [LPS88] and Margulis [Mar88] によって独立同時期に初めてその構成が与えられた. 彼らは $d-1$ が 4 で割った余りが 1 となる素数であるときに d-正則ラマヌジャングラフの列を構成した. なお, 「ラマヌジャングラフ」という名称は [LPS88] の証明がラマヌジャン予想と呼ばれる予想に依拠しているからである (「予想」と書いたが当時は既に解決している). その後, Morgenstern [Mor94] によって次数が素数べき $+1$ の形であってもラマヌジャングラフが構成できることが示された.

定理 2.2.7 （ラマヌジャングラフの陽な構成）

任意の素数 q と任意の $k \in \mathbb{N}$ に対して, 頂点数が発散するある (q^k+1)-正則ラマヌジャングラフの列が存在し, 陽に構成できる.

ランダム正則グラフ. Lubotzky, Phillips, and Sarnak [LPS88] やその後続研究によりラマヌジャングラフ列については様々な構成方法が知られている. では, そもそもラマヌジャン

[2] グラフ $G = (V, E)$ から $H = (W, F)$ への**準同型写像 (homomorphism)** とは, 写像 $\phi\colon V \to W$ であって $\{u, v\} \in E \Rightarrow \{\phi(u), \phi(v)\} \in F$ を満たすものである. ここでは自然に無限グラフに対してこの概念を拡張している.

グラフは何個あるのだろうか? n 頂点 d-正則グラフ全体の集合を $\mathcal{G}_{n,d}$ とし, $\mathcal{G}_{n,d}$ から一様ランダムに選ばれたグラフ $G \sim \mathcal{G}_{n,d}$ を考える (nd は常に偶数とする). この確率変数をランダム正則グラフという. ランダム正則グラフは「ほぼ」ラマヌジャングラフであることが知られている [Fri08].

定理 2.2.8 （Friedman の定理）

任意の $d \geq 3$ と任意の $\varepsilon > 0$ に対し,

$$\lim_{n\to\infty} \Pr\left[\lambda(P) \geq \frac{2\sqrt{d-1}}{d} + \varepsilon\right] = 0.$$

すなわち, ほとんど全ての定数次数正則グラフはラマヌジャングラフと同等のスペクトルを持つ.

2.3 性質

エクスパンダーグラフは固有値によって定義されるが, 様々な興味深い性質を持つことが知られている. ここではグラフ理論的な性質, ランダムウォークに関する性質, そして擬似ランダム性について紹介する.

2.3.1 グラフ理論的な性質

グラフ理論的に非常に興味深い多くの性質を有する.

2.3.2 ランダムウォークの性質

2.3.3 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 2.3.1 （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 $\mathcal{F} = \{f : \Omega \to \{0,1\}\}$ 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 1.3.2 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,

$$\Pr_{(u,v)\sim\mu}[(u, v) = (s, t)] = \frac{\mathbf{1}_{\{s,t\}\in E}}{2|E|} = \frac{\mathbf{1}_{\{s,t\}\in E}}{nd} \tag{2.2}$$

とする. 関数族 $\mathcal{F}$ を

$$\mathcal{F} = \{f_{S,T} \colon (s, t) \mapsto \mathbf{1}_{s\in S, t\in T} \colon S, T \subseteq V\} \tag{2.3}$$

で定める.

補題 2.3.2 （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 (2.2) で定義された分布 μ は式 (2.3) 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,

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

グラフ G の隣接行列 A を考えるとイメージしやすい. この行列は全部で nd 個の 1 を持っているため, 全成分の中で 1 の密度は $\frac{d}{n}$ である. ここで, 部分集合 $S, T \subseteq V$ に対して A の $S \times T$ で定まる部分行列 $A_{S,T}$ を考える. この行列に含まれる 1 の個数 ($e(S, T)$ に等しい) は, $\frac{d}{n} \cdot |S||T|$ に近い値となっている (図 2.2).

補題 *2.3.2* の証明. グラフ G 上の単純ランダムウォーク P を考える. 部分集合 $S, T \subseteq V$ に

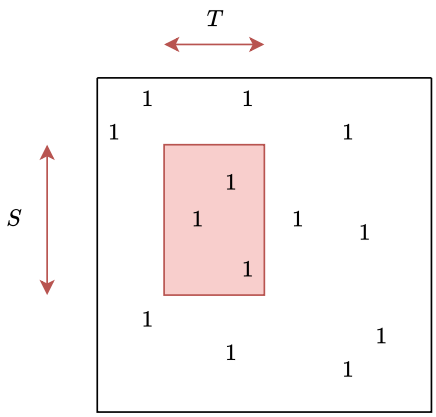

図 2.2: 正則グラフの隣接行列 A を考える．このグラフがエクスパンダーならば, 頂点部分集合 $S, T \subseteq V$ で指定される長方形内に含まれる 1 の密度は行列全体の 1 の密度に近い値をとる．

対し関数 $f = \delta_S, g = \delta_T$ として系 1.7.3 を適用すると

$$\begin{aligned}
\langle f, Pg \rangle_\pi &= \frac{e(S,T)}{nd}, \\
\mathbf{E}_\pi f &= \frac{|S|}{n}, \\
\mathbf{E}_\pi[Pg] = \mathbf{E}_\pi g &= \frac{|T|}{n}, \\
\mathbf{Var}_\pi f &= \frac{|S|}{n}\left(1 - \frac{|S|}{n}\right), \\
\mathbf{Var}_\pi g &= \frac{|T|}{n}\left(1 - \frac{|T|}{n}\right)
\end{aligned}$$

より整理すると主張を得る． □

演習問題 4

補題 2.3.2 の証明で表した五つの等式を実際に確認せよ．

「エクスパンダー混交補題」と言うと聞こえが良いが, 系 1.7.3 を見るとその実は単なる Cauchy–Schwarz の不等式とレイリー商の議論を適用しただけであることがわかる．

2.4 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．より詳細の議論は [HLW06] を参照されたい．

2.4.1 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.

2.4.2 誤り訂正符号

誤り訂正符号 (error-correcting code) または単に**符号 (code)** とは文字列に冗長性を持たせることでノイズに対する頑健性を与える手法である. 数学的には符号はビット列の集合 $\mathcal{C} \subseteq \mathbb{F}_2^n$ であり, その元 $f \in \mathcal{C}$ を**符号語 (codeword)** と呼ぶ[3]. ここで n を符号 $\mathcal{C}$ の**符号長 (code length)** と呼ぶ. 符号には, 任意の相異なる二つの符号語が互いにハミング距離の意味で離れていることが望まれる. 形式的には, 正規化されたハミング距離 $\operatorname{dist}(f,g) = n^{-1}\sum_{i\in[n]} \mathbf{1}_{f(i)\neq g(i)} = \Pr_{i\sim[n]}[f(i) \neq g(i)]$ を考え, $\min_{f\neq g\in\mathcal{C}} \operatorname{dist}(f,g)$ を符号 $\mathcal{C}$ の**距離 (distance)** という. 文字列 $f \in \mathbb{F}_2^n$ と $\mathcal{C} \subseteq \mathbb{F}_2^n$ に対して $\operatorname{dist}(f,\mathcal{C}) = \min_{w\in\mathcal{C}} \operatorname{dist}(f,w)$ を f の $\mathcal{C}$ への距離とする.

符号 $\mathcal{C} \subseteq \mathbb{F}_2^n$ が線形部分空間となるとき, 符号 $\mathcal{C}$ を**線形符号 (linear code)** と呼ぶ. 文脈によっては線形符号のことを単に符号と呼ぶこともあり, 本講義も以降は特に断りのない限りこの慣習に従う. すなわち符号と言えばそれは線形部分空間を意味する. 符号長 n, ランク k の線形符号に対し, k/n をその符号の**レート (rate)** と呼ぶ. 直感的には符号のレートはその符号が空間 $\mathbb{F}_2^n$ 内でどれほど密に充填しているかを表すため, 符号のレートと距離にはトレードオフがある. 線形符号 $\mathcal{C}$ の距離は最小ハミング重みを持つ非ゼロの符号語によって与えられることに注意されたい.

ここでは, ケイリーグラフ (定義 2.2.1) を用いて構成される符号を紹介する.

定義 2.4.1 （ケイリーエクスパンダー符号）

ケイリーグラフ $\operatorname{Cay}(A,G) = (V,E)$ と符号 $\mathcal{C}_A \subseteq \mathbb{F}_2^A$ を考える. 頂点 $g \in V$ と関数 $f\colon E \to \mathbb{F}_2$ に対し, $f_g = (f(\{g,ag\}))_{a\in A} \in \mathbb{F}_2^A$ と定める. 符号 $\mathcal{C}_A \subseteq \mathbb{F}_2^A$ に対して

$$\mathcal{C}(A,G,\mathcal{C}_A) = \{f \in \mathbb{F}_2^E \colon \forall g \in V, f_g \in \mathcal{C}_A\}$$

を**ケイリーエクスパンダー符号**と呼ぶ.

一般の (ケイリーグラフとは限らない) 正則エクスパンダーグラフを用いて定義される**エクスパンダー符号 (expander code)** が有名だが, 定義の簡潔さを優先してあえてケイリーグラフに限定したエクスパンダー符号を紹介した. もし仮に A を生成系とするケイリーグラ

[3] 文脈によってはビット列の代わりに有限集合 Σ に対して $\mathcal{C} \subseteq \Sigma^n$ を符号と定義することもある. 実際には計算機上では Σ の元を $\lceil \log_2 |\Sigma| \rceil$ ビットで表すため $\Sigma = \mathbb{F}_2$ とすることが多い.

フの列 $(\mathrm{Cay}(A, G_n))_{n\in\mathbb{N}}$ とレートと距離の良い性質をもつ一つの符号 $\mathcal{C}_A$ があったとしよう. すると, この一つの符号から符号の列 $(\mathcal{C}_n)_{n\in\mathbb{N}} := (\mathcal{C}(A, G_n, \mathcal{C}_A))_{n\in\mathbb{N}}$ を構成できる.

さらに興味深いことに, 構成に用いたケイリーグラフがエクスパンダー性を持つならば元の符号 $\mathcal{C}_A$ のレートと距離の性質を符号列 $(\mathcal{C}_n)$ も受け継ぐ.

補題 2.4.2

$\mathcal{C}_A$ のレートが r_A ならば $\mathcal{C}(A, G, \mathcal{C}_A)$ のレートは少なくとも $2r_A - 1$ である.

証明. 符号 $\mathcal{C}_A \subseteq \mathcal{F}_2^A$ のレートが r_A なので, その任意の符号語 $f_0 \in \mathcal{C}_A$ は $|A|(1-r_A)$ 個の線形制約を満たす. ケイリーエクスパンダー符号 $\mathcal{C}(A, G, \mathcal{C}_A)$ の符号語 f は, 全ての頂点 $g \in G$ に対して f_g が $|A|(1-r_A)$ 個の線形制約を満たしているので, f は高々 $|G||A|(1-r_A)$ 個の線形制約を満たしている. つまり f の自由度は少なくとも $|E| - |G||A|(1-r_A) = |E|(1-2(1-r_A))$ なので, $\mathcal{C}(A, G, \mathcal{C}_A)$ のレートは少なくとも $1-2(1-r_A) = 2r_A - 1$ となる. □

補題 2.4.3

符号 $\mathcal{C}_A$ の距離が δ_A, ケイリーグラフ $\mathrm{Cay}(A, G)$ が λ-エクスパンダーならば, ケイリーエクスパンダー符号 $\mathcal{C}(A, G, \mathcal{C}_A)$ の距離は少なくとも $\delta_A(\delta_A - \lambda)$ である.

証明にはエクスパンダー混交補題からすぐに従う以下の系を用いる:

系 2.4.4

d-正則な λ-エクスパンダー $G = (V, E)$ の頂点部分集合 $S \subseteq V$ が $e(S, S) \geq cd|S|$ を満たす (言い換えると, 誘導部分グラフ $G[S]$ の平均次数が cd 以上) ならば, $|S| \geq (c-\lambda)n$ を満たす.

系 *2.4.4* の証明. $S = T$ として補題 2.3.2 を適用すると

$$cd|S| \leq e(S, S) \leq \frac{d}{|V|}|S|^2 + \lambda d|S|.$$

これを解くと $|S| \geq (c-\lambda)n$ を得る. □

補題 *2.4.3* の証明. 任意の非ゼロの符号語 $f \in \mathcal{C}(A, G, \mathcal{C}_A)$ が少なくとも $\delta_A(\delta_A - \lambda)|E|$ 個の 1 を持つことを言えばよい. 符号語 $f \neq 0$ に対し, $F = \{e \in E \colon f(e) = 1\}$ とし, $S = \bigcup_{e\in F} e$ を F の辺と接続している頂点の全体とする (辺 e を要素数 2 の頂点部分集合として見ている). $|F| \geq \delta_A(\delta_A - \lambda)|E|$ を示せばよい.

$\mathcal{C}_A$ の距離の条件より, 各 $g \in S$ に対して $f_g \in \mathcal{F}_2^A$ は少なくとも $\delta_A|A|$ 本の辺が接続している. すなわち, $\mathrm{Cay}(A, G)$ の部分グラフ (S, F) の最小次数は $\delta_A|A|$ を満たすので $|F| \geq \frac{\delta_A|A|}{2}|S|$. 誘導部分グラフ $G[S]$ は (S, F) を部分グラフとして含むので $e(S, S) \geq 2|F|$. さらに (S, F) に対する握手補題より

$$e(S, S) \geq 2|F| \geq \delta_A|A||L|.$$

系 2.4.4 より $|S| \geq (\delta_A - \lambda)|G|$ なので, $|F| \geq \frac{\delta_A|A|}{2}|S| \geq \delta_A(\delta_A - \lambda)\frac{|G||A|}{2} = \delta_A(\delta_A - \lambda)|E|$ を得る. □

2.4.3 PCP 定理

2.4.4 Goldreich の擬似乱数生成器

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る. 単体複体上では, 大域的なランダムウォークと局所的なランダムウォークの二つのタイプのランダムウォークを自然に考えることができ, これらに基づいてそれぞれ大域的なエクスパンダー性と局所的なエクスパンダー性の概念が定義できる. 端的に述べると高次元エクスパンダーの理論はこれら二つの概念がほぼ等価であることを明らかにしており, これは単体複体における「局所大域原理」[1]を体現しているといえる.

本チャプターではまず単体複体とその上でのランダムウォークを定義し, これに基づいて高次元エクスパンダーの定義と重要な性質を紹介する.

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図形を指すこともあるが, 本講義ではいわゆる抽象的単体複体を単体複体とする.

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).
- 純粋な d-次元単体複体 X に, d 次元の面全体 $X(d-1)$ 上の何らかの分布 $\pi \in [0,1]^{X(d-1)}$ が付随している場合, X を**重み付き単体複体 (weighted simplicial**

[1]局所大域原理 (local-global principle) とは整数論などで知られる不定方程式の解の存在性に関して, 局所的な情報が大域的な情報を導くという現象の総称である.

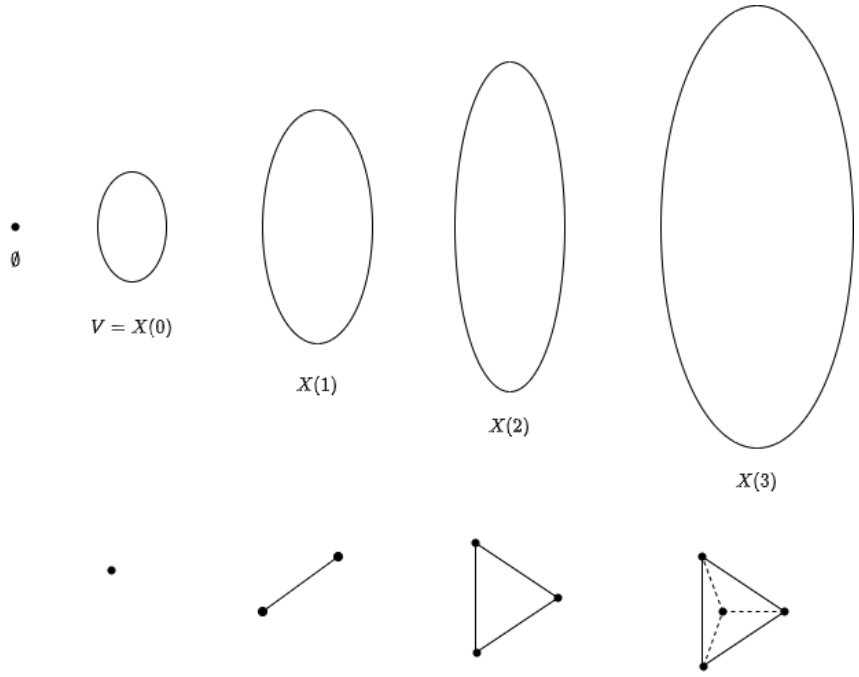

図 3.1: 各面の図形的な意味合い.

complex) (もしくは π で重みつけられた単体複体) と呼ぶ. 特に断りのない限り は π は一様分布とする.

[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. 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.

重み付き単体複体は重み付きグラフ (定義 1.4.5) の単体複体への自然な拡張である.

例 1. グラフ $G = (V, E)$ に対し, 空集合, V, E からなる部分集合族 $\mathcal{F} = \{\emptyset\} \cup \{\{v\} : v \in V\} \cup E$ 考えると, $(V, \mathcal{F})$ は単体複体である.

例 2. 有限集合 V に対し, $\mathcal{F} = \binom{V}{\leq k} := \{\sigma \subseteq V : |\sigma| \leq k\}$ 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 (cf. 定義 1.4.1). 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,

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

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.

なお, グラフ G が連結でない場合, 異なる連結成分に属する二頂点 u, v を縮約し一つの頂点として扱うことによって $(V, \mathcal{F})$ の構造を変えないまま連結成分数を減らすことができるので, 連結性を仮定しても一般性を失わない.

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 3.2).

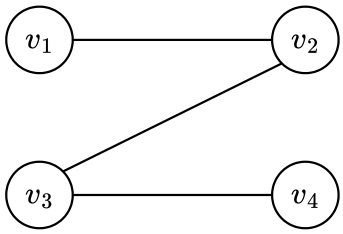

図 3.2: マッチング $M_1 = \{v_1, v_2\}, \{v_3, v_4\}\}$ と $M_2 = \{\{v_2, v_3\}\}$ はどちらも極大である.

例 6. グラフ $G = (V, E)$ の頂点部分集合 $U \subseteq V$ は, U に属する任意の二頂点間に辺がある (すなわち $\binom{U}{2} \subseteq E$) とき, **クリーク (clique)**[2]という. 特に, 単一頂点からなる集合 $\{u\}$ や $\emptyset$ もクリークである. クリークの部分集合もまたクリークなので, グラフ G の全てのクリークからなる頂点集合族を $\mathcal{F}$ とすると, $(V, \mathcal{F})$ は単体複体である.

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

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

[2]clique とは派閥を意味する英単語である.

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.

面 σ のリンクとは, σ をある意味で「縮約」して得られる単体複体であり, 面 σ の周りの局所的な構造を表している. 例えば連結グラフ $G = (V, E)$ の森の全体からなる単体複体 $X = (E, \mathcal{F})$ を考えよう. $\sigma \in \mathcal{F}$ を一つ固定したとき, リンク X_σ はどのような単体複体になっているだろうか? X_σ の全ての面は辺集合 F を含むので, F に含まれる全ての頂点を縮約して得られるより小さなグラフを考え, そこから F の辺を除去して得られるグラフ G' の森全体からなる単体複体とみなせる.

3.2 大域エクスパンダー性

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異なる次元の面の間で遷移するものを考える. 具体的には, セクション 1.4.3 で考えたようにある次元 i の面から次元 $i+1$ の面に遷移する上昇ウォークと逆に次元 $i+1$ の面から次元 i の面に遷移する下降ウォークである. 上昇ウォークと下降ウォークが互いに随伴の関係になるようにするため, 各 $X(i)$ 上での定常分布を定義し, $X(i)$ と $X(i+1)$ の間で詳細釣り合い条件が満たされるように定義される.

3.2.1 下降ウォークと定常分布

まず, セクション 1.4.3 で考えた下降ウォークを単体複体に拡張し, $X(d-1)$ 上では一様分布を定常分布とすることによって帰納的に各 $X(i)$ 上での定常分布を定める.

定義 3.2.1 （下降ウォークと面上の定常分布）

純粋な d 次単体複体 $X = (V, \mathcal{F})$ を考える. 各 $i = 0, \ldots, d-1$ に対し確率行列 $P_i^{\downarrow} \in [0,1]^{X(i) \times X(i-1)}$ を

$$P_i^{\downarrow}(\tau, \sigma) = \begin{cases} \frac{1}{i+1} & \text{if } \sigma \subseteq \tau, \\ 0 & \text{otherwise} \end{cases}$$

とする. 各 $i = 0, \ldots, d-1$ に対して, $X(i)$ 上の分布 $\pi_i \in [0,1]^{X(i)}$ を

- $i = d-1$ のとき: X が $\pi \in [0,1]^{X(d-1)}$ で重み付けられた単体複体ならば $\pi_{d-1} = \pi$ とする. そうでないならば π_{d-1} は $X(d-1)$ 上の一様分布. すなわち $\pi_{d-1}(\sigma) = \frac{1}{|X(d-1)|}$.
- π_{i+1} が定義されているとき, $\pi_i = \pi_{i+1} P_{i+1}^{\downarrow}$

で定める. 分布 π_i を (i 次の) 定常分布と呼ぶ.

面 $\tau \in X(i+1)$ に対して $P_{i+1}^{\downarrow}(\tau, \cdot)$ で定まる $X(i)$ 上の分布は, 面 τ に含まれる頂点 u を一

様ランダムに選んだときの $\sigma = \tau \setminus \{u\}$ の分布と等しい. この分布は, まず一様ランダムに $X(d)$ から面を選び, その中から一様ランダムに選ばれた $i+1$ 個の頂点からなる $X(i)$ の面のなす分布である. 従って $\pi_i(\sigma)$ は σ を含む極大な面の個数に比例する. これは遅延単純ランダムウォークの定常分布 $\pi(u)$ が次数 $\deg(u)$ に比例することの一般化である.

ある面 $\tau \in X(i+1)$ から分布 $P^{\downarrow}_{i+1}(\tau, \cdot)$ に従ってランダムに選ばれた面 σ に遷移する過程を**下降ウォーク (down walk)** と呼ぶ.

3.2.2 上昇ウォーク

定義 3.2.1 では次元 i の面から次元 $i-1$ に遷移する下降ウォークを与えた. 同様に, 次元 i の面から次元 $i+1$ の面に遷移する上昇ウォークを, $X(i)$ と $X(i+1)$ の間の詳細釣り合い条件が成り立つように定義する.

定義 3.2.2 (上昇ウォーク)

純粋な d 次単体複体 $X = (V, \mathcal{F})$ を考える. 各 $i = -1, \ldots, d-2$ に対し確率行列 $P^{\uparrow}_i \in [0,1]^{X(i)\times X(i+1)}$ を

$$\begin{aligned} P^{\uparrow}_i(\sigma,\tau) &= \frac{\pi_{i+1}(\tau)}{\pi_i(\sigma)} P^{\downarrow}_{i+1}(\tau,\sigma) \\ &= \begin{cases} \frac{\pi_{i+1}(\tau)}{(i+1)\pi_i(\sigma)} & \text{if } \sigma \subseteq \tau, \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

で定める[a].

[a] 全ての $\sigma \in X(i)$ に対し $\pi_i(\sigma) > 0$ である (そうでなければ, π_d が一様分布であることに反する).

二つの面集合 $X(i)$ と $X(i+1)$ を部集合とする二部グラフを考えればわかりやすい. それぞれの部集合には π_i, π_{i+1} が定常分布として付随しており, 上昇ウォーク $P^{\uparrow}_i$ と下降ウォーク $P^{\downarrow}_{i+1}$ は詳細釣り合い条件

$$\forall \sigma \in X(i), \tau \in X(i+1),\ \pi_i(\sigma) P^{\uparrow}_i(\sigma,\tau) = \pi_{i+1}(\tau) P^{\downarrow}_{i+1}(\tau,\sigma)$$

を満たしている.

なお, 下降ウォーク $P^{\downarrow}_i$ と上昇ウォーク $P^{\uparrow}_i$ の添字 i は遷移の開始地点の面の次元としている.

最後に, 上昇ウォークと下降ウォークを組み合わせることによって面 $X(i)$ 上の 2 種類のランダムウォークが定義できる:

定義 3.2.3 (上昇下降と下降上昇ウォーク)

定義 3.2.1, 3.2.2 と同じ設定を考える.

$$\begin{aligned} P^{\triangle}_i &:= P^{\uparrow}_i P^{\downarrow}_{i+1}, \\ P^{\triangledown}_i &:= P^{\downarrow}_i P^{\uparrow}_{i-1} \end{aligned}$$

を遷移確率行列として持つ $X(i)$ 上のランダムウォークをそれぞれ**上昇下降ウォーク**

(up-down walk), 下降上昇ウォーク (down-up walk) と呼ぶ. ここで, $X(-1)$ 上での下降上昇ウォークと $X(d-1)$ 上での上昇下降ウォークは定義されない.

上昇下降ウォークはグラフ上の遅延単純ランダムウォークの自然な一般化になっている (セクション 1.4.3).

演習問題 5

常に行列 $P_i^{\triangle}$ の対角成分が全て $\frac{1}{i+2}$ であることを示せ.

補題 3.2.4 (定常分布)

面 $X(i)$ 上の上昇下降ウォークと下降上昇ウォークはどちらも π_i を定常分布としてもつ.

証明. 計算によって簡単に確認できる. 実際,

$$\pi_i P_i^{\triangle} = \pi_i P_i^{\uparrow} P_{i+1}^{\downarrow} = \pi_{i+1} P_{i+1}^{\downarrow} = \pi_i,$$
$$\pi_i P_i^{\triangledown} = \pi_i P_i^{\downarrow} P_{i-1}^{\uparrow} = \pi_{i-1} P_{i-1}^{\uparrow} = \pi_i$$

より主張を得る. □

注釈 3.2.5 (「上昇」「下降」の名称)

非常にややこしいのだが, 上昇ウォークと下降ウォークの遷移確率行列と左右どちらから作用させるかによって「上昇」「下降」の意味合いが反転してしまう. 確率行列としての上昇ウォークは $P_i^{\uparrow} \in [0,1]^{X(i)\times X(i+1)}$ で表せる. 一般によくある左から作用させる作用素の感覚で考えると $P_i^{\uparrow} \colon \mathbb{R}^{X(i+1)} \to \mathbb{R}^{X(i)}$ であるので, 次元を一つ落とすように見えてしまうのである. 下降ウォークについても同様である. 特に上昇下降ウォーク $P_i^{\triangle} = P_i^{\uparrow} P_{i+1}^{\downarrow}$ を左から作用させると「次元を下げてから上げる」ものになるので, 下降上昇ウォークと混同しやすい.
本講義はランダムウォークを主眼におき, 右から作用させるときの $P_i^{\uparrow}, P_i^{\downarrow}$ に興味があるので定義 3.2.1, 3.2.2 の呼称を採用している. ランダムウォークの遷移確率行列として扱う場合は右から作用させ, 内積空間を考え随伴性などを考える場合 (セクション 3.2.3) は左から作用させる (このときの行列 P をマルコフ作用素と呼ぶことがある). なお, 可逆なランダムウォーク (定義 1.5.2) は内積 $\langle \cdot, \cdot \rangle_\pi$ の意味で左右どちらから作用させても本質的に同じであるので左右どちらから作用させるかについてこのような煩雑な話は考えなくて良い.

3.2.3 各次元の内積空間

各次元 i に対して $X(i)$ とそれに付随する定常分布を定義できたので, 定義 1.6.1 の特殊ケースの内積空間を考えることができる.

定義 3.2.6

単体複体 X を考え, 各次元の定常分布を $\pi_i \in [0,1]^{X(i)}$ としたとき, $\ell_i^2 = \ell_{\pi_i}^2(X(i))$ と表す. すなわち, 各 $i = 0, \dots, d-1$ に対し, $\mathbb{R}^{X(i)}$ に内積 $\langle \cdot, \cdot \rangle_{X(i)}$ を

$$\langle f, g \rangle_{X(i)} = \sum_{\sigma \in X(i)} \pi_i(\sigma) f(\sigma) g(\sigma)$$

で定義して得られる内積空間を ℓ_i^2 とする.

上昇ウォーク $P_i^{\uparrow} \colon \ell_{i+1}^2 \to \ell_i^2$ と下降ウォーク $P_{i+1}^{\downarrow} \colon \ell_i^2 \to \ell_{i+1}^2$ は互いに随伴の関係にある. すなわち, 任意の $f \in \ell_{i+1}^2$ と $g \in \ell_i^2$ に対して

$$\left\langle P_{i+1}^{\downarrow} f, g \right\rangle_{X(i+1)} = \left\langle f, P_i^{\uparrow} g \right\rangle_{X(i)} \tag{3.1}$$

が成り立つ.

演習問題 6

式 (3.1) を確認せよ.

単体複体の大域的なエクスパンダー性を下降上昇ウォークのエクスパンダー性で定める.

定義 3.2.7 （大域エクスパンダー性）

純粋な d 次元単体複体 $X = (V, \mathcal{F})$ は, 任意の $0 \le i \le d$ に対して $X(i)$ 上の下降上昇ウォーク P_i^{∇} が $\lambda_i(P_i^{\nabla}) \le \lambda_i$ を満たすとき, **大域 $(\lambda_0, \dots, \lambda_d)$-エクスパンダー (global $(\lambda_0, \dots, \lambda_d)$-expander)** であるという.

エクスパンダーグラフ (定義 2.1.1) と比較すると, 片側 (第二固有値) だけの上界だけでエクスパンダー性を定義している. これは, 単体複体上の上昇下降ウォークがグラフ上の遅延単純ランダムウォークに対応しており, 常にその遷移確率行列が半正定値行列であるため λ_2 だけがバウンドされてあればよい.

なお, 二つの行列 A, B に対し, AB の非ゼロ固有値と BA の非ゼロ固有値は同じなので, 定義 3.2.7 において上昇下降ウォークを考えても等価な定義になる.

本講義の目標は単体複体の大域エクスパンダー性を証明することである. 特にマトロイドと呼ばれる単体複体の大域エクスパンダー性は Mihail–Vazirani 予想 [FM92] と呼ばれる 30 年来の未解決問題であった[3] が, 2019 年に Anari, Liu, Gharan, and Vinzant [ALGV24] に解決された. 詳細は chapter 4 にて解説する.

3.3 局所エクスパンダー性

単体複体における局所的なランダムウォークを定義し, これに基づいて単体複体の局所エクスパンダー性を定義する. また, 局所エクスパンダー性を確認するための非常に強力な定理

[3] [FM92] にはこの予想は Micalli と Vazirani が立てたものらしいのだが, この予想を陽に述べた最初の文献は私が調べた限りでは Feder and Mihail [FM92] であった.

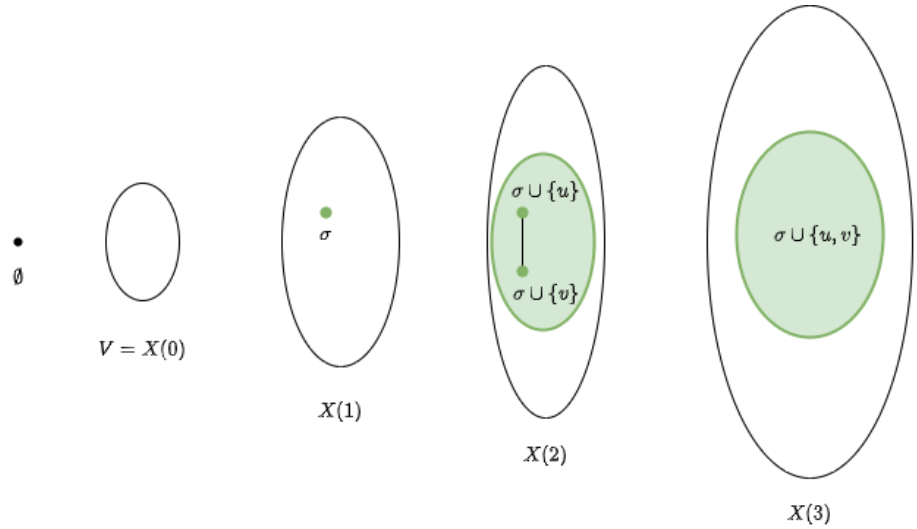

図 3.3: リンク X_σ の 2-スケルトンでは, $\sigma \cup \{u, v\} \in \mathcal{F}$ のときに u, v 間に辺を張る.

として Oppenheim のトリクルダウン定理を証明する.

3.3.1 局所的なランダムウォーク

各リンク X_σ の 2-スケルトン上での局所的な重み付きランダムウォークを考える (図 3.3). 重み付きランダムウォークについては定義 1.4.5 を参照されたい.

定義 3.3.1 (局所ランダムウォーク)

純粋な d 次元単体複体 $X = (V, \mathcal{F})$ を考える. 次元 $i \leq d-2$ の面 $\sigma \in \mathcal{F}$ に対し, リンク X_σ の 2-スケルトンを $G_\sigma = (V_\sigma, E_\sigma)$ とする. このグラフの辺重み $w_\sigma \colon E_\sigma \to [0, 1]$ を

$$w_\sigma(e) = \pi_{i+2}(\sigma \cup e)$$

で定め, これによって定まる V_σ 上の重み付きランダムウォークを面 σ に関する**局所ランダムウォーク (local random walk)** と呼び[a], 遷移確率行列を $P_\sigma \in [0, 1]^{V_\sigma \times V_\sigma}$ とする.

[a] このランダムウォークの概念は高次元エクスパンダーの文脈ではほぼ必ず登場するが, 特に標準的な用語が与えられてはいないので、「局所ランダムウォーク」という用語は本講義だけの局所的なものとする.

必ずしも局所ランダムウォークが既約性や非周期性を持つとは限らない (すなわち, グラフ G_σ が非連結だったり二部グラフになりうる) が, 可逆性は必ず満たすことに注意せよ.

グラフ (1 次元単体複体) だと面 $\emptyset$ に対する局所ランダムウォークのみ存在するが, これは上昇下降ウォーク (すなわち遅延単純ランダムウォーク) と同じである. 従って局所ランダムウォークの概念はより高次元の単体複体を考える際に意味を持つ.

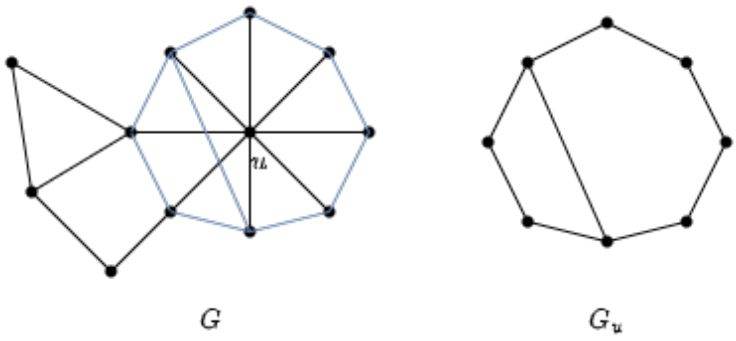

図 3.4: 頂点 u のリンクの 2-スケルトン G_u は頂点 u の隣接頂点からなる誘導部分グラフである.

3.3.2 局所エクスパンダー

純粋な単体複体の局所的なエクスパンダー性を定義する. 任意の面 σ に対し G_σ 上での局所ランダムウォークの第二固有値が小さいとき, その単体複体は局所的エクスパンダー性をもつという.

定義 3.3.2 （局所エクスパンダー性）

純粋な d 次元単体複体 $X = (V, \mathcal{F})$ を考える. 任意の $i = -1, 0, \ldots, d-2$ と任意の面 $\sigma \in X(i)$ に対し $\lambda_2(P_\sigma) \leq \gamma_i$ を満たすとき, **局所 $(\gamma_{-1}, \ldots, \gamma_{d-2})$-エクスパンダー (local spectral $(\gamma_{-1}, \ldots, \gamma_{d-2})$-expander)** であるという. 特に, $\gamma_{-1} = \cdots = \gamma_{d-2} = \gamma$ であるとき, 局所 γ-エクスパンダーであるという.

あくまでも G_σ の片側エクスパンダー性のみを議論していることに注意. 従って, 局所エクスパンダーだからといって G_σ 上の局所ランダムウォークの混交時間が小さいとは限らない (そもそも二部グラフになりうるので, 一般に収束しない).

例 1. 三角形複体. グラフ $G = (V, E)$ 上の頂点数 3 以下のクリークからなる単体複体を X とする (セクション 3.1 の例 6 参照). 頂点 $u \in V$ のリンク $X_u := X_{\{u\}}$ を考える. u の隣接頂点の集合を $N(u)$ とする. G 辺 $\{u, v_1\}, \{u, v_2\} \in E$ に対し, $\{v_1, v_2\} \in E$ のときに三角形 $\{u, v_1, v_2\}$ が単体複体 X の面となる. 従って, リンク X_u は頂点 u の誘導部分グラフ $G[N(u) \setminus \{u\}]$ に等しい . また, 全ての三角形に対し一様な重みを与えているため, G_u 上のランダムウォークは単純ランダムウォークと同一である.

例 2. 全域木複体. 連結グラフ $G = (V, E)$ 上の森からなる辺集合 E 上の単体複体を X とする (セクション 3.1 の例 3 参照). 極大でない森 $F \subseteq E$ に対するリンクの 2-スケルトン G_F を考える. このグラフの頂点集合は $E \setminus F$ であり, $e_1, e_2 \in E \setminus F$ が G_F 上で辺をなすのは $F \cup \{e_1, e_2\}$ が森でありかつその時に限る.

さて, G の部分グラフ (V, F) を考えよう. 森 F の非極大性からこの部分グラフは二つ以上の連結成分 $C_1, \ldots, C_\ell \subseteq V$ からなる. 従って, $e_1, e_2 \in E \setminus F$ が森であることの必要十分条件は e_1, e_2 が同じ連結成分間を繋がないことである.

3.4 単体複体の局所大域原理

単体複体における局所大域原理, すなわち, 局所エクスパンダー性は大域エクスパンダー性を導くという結果は比較的最近, Kaufman and Oppenheim [KO20] によって証明された.

定理 3.4.1 （Kaufman–Oppenheim の定理）

純粋な d-次元単体複体 $X = (V, \mathcal{F})$ が局所 γ-エクスパンダーならば,

$$\lambda_i = 1 - \frac{1}{i+1} + \gamma i$$

で定義された λ_i $(i = 0, \dots, d)$ に対して X は大域 $(\lambda_0, \dots, \lambda_d)$-エクスパンダーである.

その後, Alev and Lau [AL20] によって改善され以下の結果が示されている:

定理 3.4.2 （Alev–Lau の定理）

純粋な d-次元単体複体 $X = (V, \mathcal{F})$ が局所 $(\gamma_{-1}, \dots, \gamma_{d-2})$-エクスパンダーならば,

$$\lambda_i = 1 - \frac{1}{i+1} \prod_{j=-1}^{i-2} (1 - \gamma_j)$$

で定義された λ_i $(i = 0, \dots, d)$ に対して X は大域 $(\lambda_0, \dots, \lambda_{d-1})$-エクスパンダーである.

定理 3.4.1 and 3.4.2 を証明するために上昇下降ウォーク $P^{\triangle}$ に対し, 自己ループを除去したウォークを定義する.

定義 3.4.3 （非遅延上昇下降ウォーク）

定義 3.2.1, 3.2.2 と同じ設定において, 確率行列 $P_i^{\wedge} \in [0,1]^{X(i) \times X(i)}$ を

$$P_i^{\wedge} = \frac{i+2}{i+1} \left(P_i^{\triangle} - \frac{1}{i+2} I \right)$$

とする. ここで I は $X(i) \times X(i)$ の単位行列である.

演習問題 5 より $P_i^{\triangle}$ に従うランダムウォークは確率 $\frac{1}{i+2}$ の自己ループを持つ. 従って $P_i^{\triangle}$ から $\frac{1}{i+2} I$ を引くと自己ループの確率は 0 になる. しかしこうすると行和が $1 - \frac{1}{i+2} = \frac{i+1}{i+2}$ になるので, $\frac{i+2}{i+1}$ 倍して確率行列になるよう正規化したものが $P_i^{\wedge}$ である. 例えばグラフ上の単純遅延ランダムウォーク (定義 1.4.4) に対して同様の操作を行うと単純ランダムウォーク (定義 1.4.3) を得る. すなわち, グラフ G を 1 次元単体複体とみなしたときの $P_0^{\wedge}$ は G 上の単純ランダムウォークと等しい.

定義 3.4.4

$f \in \ell_i^2$ と面 $\sigma \in X(i-1)$ に対し f の $X_\sigma(0)$ への制限を f_σ とする. すなわち, $f_\sigma \colon X_\sigma(0) \to \mathbb{R}$ を

$$f_\sigma(u) = f(\sigma \cup \{u\})$$

で定める.

以下の補題は ℓ_i^2 上の内積が各リンク X_σ 上の内積の線形和に分解できることを表す.

補題 3.4.5

純粋な d 次元単体複体 X と任意の $0 \le i \le d, f \in \ell_i^2$ に対し

$$\langle f, P_i^\wedge f \rangle_{X(i)} = \mathop{\mathbb{E}}_{\sigma \sim \pi_{i-1}} \left[\langle f_\sigma, P_\sigma f_\sigma \rangle_{\pi_0^\sigma} \right].$$

ここで, $\pi_0^\sigma \in [0,1]^{X_\sigma(0)}$ はリンク X_σ の頂点集合 $X_\sigma(0)$ 上の定常分布である.

3.5 Oppenheim のトリクルダウン定理

ある単体複体 X に対して定義 3.3.2 に基づいて局所エクスパンダー性を示すには全ての面に対して $\lambda_2(P_\sigma)$ を上から抑える必要がある. 一般にそもそも辺重み w_σ (定義 3.3.1) を求めることすら非自明であり, ましてや固有値を抑えるなど非常に大変な作業となる. Oppenheim のトリクルダウン定理は局所エクスパンダー性を確認するのに非常に有用な定理である. 端的に言えば, 次数 $d-2$ の面 $\sigma \in X(d-2)$ に対して $\lambda(P_\sigma)$ を抑えれば全ての次元の面に対しても第二固有値が上から抑えられるという結果である.

定理 3.5.1 (Oppenheim のトリクルダウン定理)

純粋な d-次元単体複体 $X = (V, \mathcal{F})$ が以下の二つを満たすとする:

- 全ての $i \le d-2$ と全ての $\sigma \in X(i)$ に対してグラフ G_σ は連結.
- 全ての $(d-2)$-次元の面 $\tau \in X(d-2)$ に対して $\lambda_2(P_\tau) \le \gamma$.

このとき, $\gamma_i := \frac{\gamma}{1-(d-2-i)\gamma}$ $(i = -1, \dots, d-2)$ に対して X は局所 $(\gamma_{-1}, \dots, \gamma_{d-2})$-エクスパンダーである.

例えば, $\gamma = 0$ で定理 3.5.1 を適用すると, X は局所 0-エクスパンダーである. 実はマトロイドと呼ばれる単体複体はこの定理を使って局所 0-エクスパンダーであることが示せる.

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 $\sigma \cup \{u\} \in \mathcal{F}$.

4.1.1 例 1. グラフ的マトロイド

4.1.2 例 2. 線形マトロイド

4.1.3 例 3. 分割マトロイド

4.2 モチベーション

4.2.1 組合せ最適化

4.2.2 組合せ論

4.3 基の数え上げ

4.4 Anari, Liu, Gharan, Vinzant の定理

補題 4.4.1

マトロイド $(V, \mathcal{F})$ は局所 0-エクスパンダーである.

4.5 その他の応用

理論計算機科学における (マトロイド以外への) 高次元エクスパンダーの応用を簡単にまとめる. 多くの応用は本質的には高次元エクスパンダーがもつ局所大域原理に基づいている.

Bibliography

[AL20] V. L. Alev and L. C. Lau. "Improved analysis of higher order random walks and applications". In: **Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing**. STOC 2020. Chicago, IL, USA: Association for Computing Machinery, June 2020, pp. 1198–1211. DOI: 10.1145/3357713.3384317 (cit. on p. 46).

[ALGV24] N. Anari, K. Liu, S. O. Gharan, and C. Vinzant. "Log-concave polynomials II: High-dimensional walks and an FPRAS for counting bases of a matroid". en. In: **Annals of Mathematics** 199.1 (Jan. 2024), pp. 259–299. DOI: 10.4007/annals.2024.199.1.4 (cit. on p. 43).

[FM92] T. Feder and M. Mihail. "Balanced matroids". In: **Proceedings of the twenty-fourth annual ACM symposium on Theory of Computing**. STOC '92. Victoria, British Columbia, Canada: Association for Computing Machinery, July 1992, pp. 26–38. DOI: 10.1145/129712.129716 (cit. on p. 43).

[Fri08] J. Friedman. "A Proof of Alon's Second Eigenvalue Conjecture and Related Problems". In: **Memoirs of the American Mathematical Society** 195 (2008) (cit. on p. 30).

[HLW06] S. Hoory, N. Linial, and A. Wigderson. "Expander graphs and their applications". en. In: **Bull. Am. Math. Soc.** 43.4 (2006), pp. 439–561. DOI: 10.1090/S0273-0979-06-01126-8 (cit. on p. 32).

[KO20] T. Kaufman and I. Oppenheim. "High Order Random Walks: Beyond Spectral Gap". In: **Combinatorica** 40.2 (Apr. 2020), pp. 245–281. DOI: 10.1007/s00493-019-3847-0 (cit. on p. 46).

[LPS88] A. Lubotzky, R. Phillips, and P. Sarnak. "Ramanujan graphs". In: **Combinatorica** 8.3 (Sept. 1988), pp. 261–277. DOI: 10.1007/BF02126799 (cit. on p. 29).

[Mar88] G. A. Margulis. "Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators". In: **Problems Inform. Transmission** (1988) (cit. on p. 29).

[Mor94] M. Morgenstern. "Existence and Explicit Constructions of q + 1 Regular Ramanujan Graphs for Every Prime Power q". In: **Journal of Combinatorial Theory Series B** 62.1 (Sept. 1994), pp. 44–62. DOI: 10.1006/jctb.1994.1054 (cit. on p. 29).