

エクspanderとランダムネスの節約・除去

垂井 淳

1. はじめに

コインを投げて判定問題を解くランダムアルゴリズムがあるとして、次の問いを考えよう。

1. コインを使わずに解けないか？
2. コインを使う回数を減らせないか？
3. コインの出来が悪い場合どうすればいいか？

汎用的な答えに特に興味がある。次の判定問題を考えてみよう。辺に向きのない n 頂点グラフと 2 つの頂点 s, t が与えられる。頂点 s と頂点 t は辺をたどって結ぶことができるか判定したい。

記憶容量を $O(\log n)$ だけ用いてこの判定問題を解きたい。頂点 x からどの頂点へと辺があるのかということは、計算の途中いつでも入力を見て調べられる。しかし、計算の途中経過は記憶として $O(\log n)$ ビット分しか残せない。

次のアルゴリズムを考えよう。頂点につながっている辺から 1 本をランダムに選んでその辺をたどる。このランダムウォークを頂点 s からスタートして $O(n^3)$ ステップ続ける。ウォークの途中で頂点 t を訪れたら s と t は連結していると判定し、最後まで頂点 t を訪れなかったら頂点 s と頂点 t は連結していないと判定する。

実に単純なやり方だ。現在注目している頂点の名前と現在までのステップ数だけ記憶しておけばすむ。だいたい $4\log_2 n = O(\log n)$ ビットですむ。

ランダムビットを使わない記憶容量 $O(\log n)$ の

アルゴリズムはあるだろうか？ すなわち、以上の判定問題はクラス L に属するか？ 無向グラフ上の 2 頂点連結判定問題の重要性は、実はこの問題がクラス L の本質と深く関わっていることによる。

以上の問題は約一年前にレインゴールド (Reingold) が肯定的に解決し、計算量理論において大きなニュースとなった。主なアイデアは次のようなものだった。「任意のグラフ G は弱いパラメーターのエクspanderと考えられる。『グラフのジグザグ積』という操作により、グラフ G を定数次数の強いエクspanderに変換して連結性の判定をすればいい。」

エクspanderとは不思議な性質をもったグラフで、冒頭の 3 つの問いすべてに対して肯定的な答えを出すのに役に立つ。本稿ではエクspanderの紹介をしたい。そしてランダムネスの節約と擬似ランダムネスの生成について、このようなことになじみのない読者を主に想定して説明したい。レインゴールドの結果の証明についてはキーとなる部分のみ一番最後で触れる。

2. グラフのスペクトラム

グラフ $G = (V, E)$ を n 頂点無向グラフとし、その隣接行列を $A = (A_{u,v})_{u,v \in V}$ とする。ここで $A_{u,v}$ は頂点 u と頂点 v を結ぶ辺の数である。行列 A の各行、各列の和が d であるとき G を d -正則であるという。自己ループ、多重辺がなければ

A は対角成分がすべて 0 の $0/1$ 行列である．グラフ G 上のランダムウォークの推移行列は $1/d \cdot A$ となる．

行列 $L = dI - A$ または $1/d \cdot L$ をグラフ G のラプラシアンという．グラフ G の各辺に任意の向きをつけたグラフの $V \times E$ 接続行列を K とすると、 $L = KK^t$ となり、 K と K^t を V 上関数と E 上関数の間の作用素と考えると連続の場合のラプラシアン $\Delta(f) = \text{div}(\text{grad}(f))$ と対応がつく．

隣接行列 A は実対称行列なので直交する実固有ベクトルと実数の固有値 $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$ をもつ．最大固有値に関して $\lambda_1 = d$ が成立し、グラフが連結していることと $\lambda_1 = d$ の重複度が 1 であることは同値である．重複度が 1 のとき $\lambda_1 = d$ に対応する固有ベクトルは $(1, 1, \dots, 1)^t$ である．以下では連結グラフ、または、グラフのひとつの連結成分についてのみ考える．

最小固有値に関して $\lambda_n \geq -d$ が成り立ち等号が成立することはグラフが 2 部グラフであることと同値である．

ここで、 $\lambda = \max(|\lambda_2|, |\lambda_n|)$ とする．我々の議論にとって重要なのはスペクトルギャップ、すなわち $\lambda_1 = d$ にくらべて λ または λ_2 がどのぐらい小さいかという点である．ランダムウォークの定常分布への収束速度を含め我々の議論で主に問題なのは λ であるが、頂点集合の辺境界の拡大については λ_2 が問題となる．ギャップが大きければ大きいほど早い収束速度が保証され、また、境界の大きい拡大が保証される．

3. エクспанダー

エクспанダーを定義するやり方は、パラメーターをいくつどのようにとるかという選択を含めて何通りかある．ここでは、スペクトルギャップを次数 d に関して標準化したパラメーターでエクспанダーを定義しよう．実数 $\alpha \in [0, 1]$ について、 $\lambda \leq \alpha d$ を満たす d -正則グラフを α -エクспанダーと呼ぶことにする．

グラフ G に対して、その 2 乗 G^2 は隣接行列が

A^2 であるグラフのことである．行列 A^2 の (u, v) 成分はグラフ G の頂点 u から頂点 v への長さ 2 のパスの数となる．グラフ G が d -正則であれば A^2 の各対角成分は d 以上なので $\text{trace}(A^2) \geq nd$ となる．これを $\text{trace}(A^2) = \sum \lambda_i^2$ とくらべると、 $n \rightarrow \infty$ において λ が大体 $\sqrt{d}$ 以上であることはすぐわかる．

スペクトルギャップのより精密な限界は d -正則グラフに関する次の不等式によって与えられる．

$$\lambda \geq 2\sqrt{d-1} - o(1) .$$

連結な d -正則グラフ G の $\pm d$ 以外の固有値 λ_i が $|\lambda_i| \leq 2\sqrt{d-1}$ を満たすとき G はラマヌージャングラフと呼ばれる．

次数 d を固定し、 $n \rightarrow \infty$ と考える．任意の $\epsilon > 0$ について、ランダムな d -正則グラフは確率 $1 - o(1)$ で $\lambda \leq 2\sqrt{d-1} + \epsilon$ を満たすことが知られている．

我々の議論にとっては、エクспанダーを効率的に構成できることが重要となる．エクспанダーの構成法としては、群のケーリーグラフとして与える方法がある．ラマヌージャングラフは現在でもケーリーグラフとしての構成しか知られていない．

本稿では、グラフのジグザグ積による構成法を説明する．この方法の拡張により、2 部グラフに関して大きな頂点境界拡大をもつものや左右の大きさの異なるものも構成できる．このような 2 部グラフの代数的構成は知られていない．

4. 境界の拡大

エクспанダーの名前の由来でもある境界の拡大について述べておく．この記事の残りの部分では境界の拡大にはほとんど触れない．

グラフ $G = (V, E)$ に関して以下の用語を使う．頂点の集合 $S, T \subseteq V$ に対して $E(S, T) = \{(u, v) : u \in S, v \in T\}$ とする．ここで、 (u, v) は順序対としていることに注意してほしい．頂点の集合 S に対して S の辺境界 (edge boundary) とは $E(S, \bar{S})$ のことで、 S の頂点境界 (vertex bound-

ary) とは $\Gamma(S) = \{v \notin S : u \in S, (u, v) \in E\}$ のことである.

グラフ G の辺拡大係数 $h(G)$ を次のように定義する.

$$h(G) = \frac{|E(S, \bar{S})|}{\min(|S|, |\bar{S}|)}.$$

辺拡大係数 $h(G)$ と連結 d -正則グラフの第2固有値 λ_2 に関して次が成り立つ.

$$\frac{d - \lambda_2}{2} \leq h(G) \leq \sqrt{2d(d - \lambda_2)}. \quad (1)$$

頂点境界の拡大については, (1) の最初の不等式から直ちに次のことがわかることだけを指摘しておく. 任意の $S \subseteq V, |S| \leq n/2$ に対して, $|\Gamma(S)| \geq (d - \lambda_2)/(2d)$.

グラフの隣接行列の第2固有値 λ_2 は, 半正定値であるラプラシアン L の正の最小固有値に対応している. 以上の有限グラフに関する話に対応するスペクトル幾何の話について触れておく. 眉を湿らせて読んでいただきたい.

コンパクトリーマン多様体 M に対して, チェーガー一定数 (Cheeger constant) $h(M)$ が次のように定義される.

$$h(M) = \inf_A \frac{\text{vol}(\partial A)}{\min(\text{vol}(A), \text{vol}(\bar{A}))}.$$

ここで, ∂A は A の境界で, vol は n と $n-1$ 次元の体積で, $\inf$ はすべての開集合 A に関するものである. 多様体 M のラプラシアンの正の最小固有値 λ と h に関してチェーガー型不等式 $\lambda \geq h^2/4$ が成立する.

どうも幾何ではこの不等式を λ の下界を h によって与えるという方向で用いることが多いらしい. 有限グラフの場合は基本的には逆である. どちらかと言えばスペクトルの方が扱いやすい. 境界の拡大を直接示すことが出来るのは, 最近まで確率的手法を用いた場合だけだったように思う. 現在はランダムネス・エクストラクター (extractor) やランダムネス・コンダクター (conductor) に関するかなり複雑な議論によって, 頂点境界の拡大に関して, スペクトラルギャップから導けるパウ

ンドの限界である $d/2$ より大きい拡大が示せるようになっている.

5. エクспанダー上のランダムウォーク

グラフ $G = (V, E)$ を連結な頂点数 n の d -正則無向グラフとし, 隣接行列を A とする. グラフ G 上のランダムウォークの推移行列を $B = 1/d \cdot A$ とする. 頂点集合 V 上の初期分布 q からランダムウォークを k ステップした時の分布は $B^k q$ となる. 確率分布を横ベクトルで表し推移行列を右からかけるやり方もあるがここではそうしていない.

ここで $\alpha < 1$ として, G は α -エクспанダーと仮定して話を進める. 頂点集合 V 上の一様分布を $u = (1/n, 1/n, \dots, 1/n)^t$ で表す. ベクトル u は行列 B の重複度 1 の最大固有値 1 に対応する固有ベクトルである.

ベクトル u と直交する空間は B -不変であり, この空間の任意のベクトルの長さは B により α だけ縮む. 初期分布ベクトル q は $q = u + (q - u)$ と直交分解できる. これらから次が成立することはすぐわかる.

$$\|B^k q - u\|_2 \leq \alpha^k.$$

二つの分布の距離を l_1 ノルムまたは l_∞ ノルムで測る場合は, 一般に成立する関係 $\|v\|_\infty \leq \|v\|_2, \|v\|_1 \leq \sqrt{n}\|v\|_2$, および, l_2 ノルムを指数的に減少させられることによって押さえればよい.

次に, 任意の頂点集合 $S \subseteq V$ を固定して, 以下の確率を考える. 集合 S の大きさを $|S| = \beta n$ とする. 例えば $\beta = 1/2, \alpha = 1/4$ と思うとわかりやすいかもしれない.

ウォークをスタートする頂点はグラフの全頂点の集合 V から一様ランダムに選び, 選んだ頂点から k ステップのウォークをするとしよう. このウォークが最初から最後まで頂点集合 S 内にとどまる確率を $p(S, k)$ とする.

比較のため別のシナリオも考えよう. 頂点を一様ランダムに V から選び, さらに k 回独立に一様ランダムに V から選ぶとする. この場合, $k+1$

回すべて頂点が集合 S から選ばれる確率は β^{k+1} となる。

ランダムウォークの場合は、続けて選ばれる頂点は全く独立ではない。しかし、以下が成立し、 $p(S, k)$ は k に関して指数的に落ちていく。

$$p(S, k) \leq (\alpha + \beta)^k. \quad (2)$$

不等式 (2) を証明するには、 S -対角成分のみ 1 の射影行列を P とし、任意のベクトルの長さが PBP によって $\alpha + \beta$ だけ縮まることを示し、一様分布 u に対して次が成り立つことを示せばよい。

$$\|(PB)^k u\|_2 = \|(PBP)^k u\|_2 \leq (\alpha + \beta)^k \|u\|_2.$$

6. ランダムネスの節約

ランダムアルゴリズム A が次のようにブール関数 f を計算しているとする。任意の x に対して、

$$\begin{aligned} f(x) = 0 &\Rightarrow A(x) = 0 \quad \text{with Prob } 1 \\ f(x) = 1 &\Rightarrow A(x) = 1 \quad \text{with Prob } \geq 1/2. \end{aligned}$$

以上の話における確率はアルゴリズムが用いるランダムビットにのみ関係している。入力 x について何らかの分布を考えているわけではない。

アルゴリズム A は入力 x に対して r 個のランダムビットを用いているとしよう。アルゴリズム A は決定的 (deterministic) アルゴリズム $D(x, q)$ を入力 x とランダムビット列 $q \in \{0, 1\}^r$ に対して実行していると考えられる。

アルゴリズムのエラーを $1/2$ から 2^{-k} に下げたいとする。アルゴリズムを独立に k 回実行し k 回の結果すべて 0 のとき出力を 0 とすればよい。この方法では rk 個のランダムビットを使っている。もっと少ないランダムビットを用いてエラーを 2^{-k} に下げられるだろうか？

次のようにすればよい。アルゴリズム D における r -ビットのランダムビット列全体に対応する 2^r 個の頂点をもつ $1/4$ -エクスパンダーを考え、その上でのランダムウォークを考える。最初のビット列は一様ランダムに選び、その後はランダムウォー

クが各ステップで訪れる頂点に対応する r -ビット列 q をアルゴリズム D に対して、 $D(x, q)$ と用いる。ウォークを $O(k)$ ステップ行えば、前節の (2) のバウンドよりエラーは 2^{-k} 以下となる。

この方法で用いるランダムビット数は $r + O(k)$ となっている。以上のようなシナリオでのランダムネスの節約は **deterministic amplification** と呼ばれ、エクスパンダー上のランダムウォーク以外にいろいろなやり方が知られている。

7. エクスパンダー混合補題

グラフ $G = (V, E)$ を n 頂点 d -正則な α -エクスパンダーとし、任意の頂点集合 $S, T \subseteq V$ について考える。集合 $E(S, T)$ を $E(S, T) = \{(u, v) : u \in S, v \in T\}$ とする。この集合のサイズについて Expander Mixing Lemma として知られる次が成り立つ。

$$\left| \frac{|S| |T|}{n^2} - \frac{|E(S, T)|}{nd} \right| \leq \alpha. \quad (3)$$

実は、左辺は $\alpha \cdot \sqrt{|S| |T|}/n$ で押さえられる。以上の形の方がこの後の話を進めやすい。

ここで $n = 2^r$ であるとして、全頂点の集合 V を r ビット列の集合 $\{0, 1\}^r$ と同一視する。すなわち、各頂点に r -ビットの名前をつける。

一様ランダムに $2r$ ビット列を生成し、前半の r ビット列が S に属し、かつ、後半の r ビット列が T に属する確率は $|S| |T|/n^2$ となる。

一方で次のプロセスを考える。一様ランダムに r ビット列 q_1 を生成し、頂点 q_1 につながっている d 本の辺から一様ランダムに一本選び、選んだ辺のもう一方の端点を q_2 とする。グラフ G の辺集合 E の中から一本の辺を一様ランダムに選び、その両端点を q_1, q_2 としているのと同じことである。このシナリオにおいて $q_1 \in S, q_2 \in T$ となる確率は $|E(S, T)|/(nd)$ となる。

不等式 (3) により、以上の 2 つの確率の差は α 以下となる。ここで、 α は $2/\sqrt{d}$ ぐらいまで小さくできることを思い出すか、または、とにかく α は小さいものとイメージしよう。

8. 疑似ランダムネス生成の雛形

前節の2つの方法が用いるランダムビット数は、それぞれ $2r$ と $m = r + \log_2 d$ である。ここでは、 $\log_2 d \ll r$ と考えよう。後者の方法を以下の関数 G によって表そう。

$$G: \{0, 1\}^m \rightarrow \{0, 1\}^r \times \{0, 1\}^r = \{0, 1\}^{2r}.$$

関数 G は長さ $m = r + \log_2 d$ のビット列を $2r$ ビット列へと移している。長さ m のビット列全体を台としてもつ一様分布 U_m に対して、関数 G は長さ $2r$ のビット列上のある分布を自然に定めている。この $2r$ ビット列上の分布を $G(U_m)$ と表し、分布 U_{2r} とくらべる。

分布 $G(U_m)$ の $\{0, 1\}^{2r}$ の中の台のサイズは高々 2^m である。したがって、 $G(U_m)$ と U_{2r} の差を l_1 ノルムで測るとほぼ 1 となり、 l_1 ノルムに関してこの2つの分布は全く近くない。にもかかわらず、 $q_1 \in S, q_2 \in T$ という事象に関しては、分布 $G(U_m)$ のもとでの確率と分布 U_{2r} のもとでの確率の差が小さい。

このような関数 G の性質は**疑似ランダムネス生成器 (pseudorandom generator)** と呼ばれるものの雛形になっている。一般には、あるクラス $\mathcal{C}$ に属する任意のアルゴリズム D に対して、 $D(q) = 0/1$ となる確率を、 q が一様ランダムに選ばれた場合と q が $G(U_m)$ に従って選ばれた場合について考える。2つの確率の差がクラス $\mathcal{C}$ に属するどのアルゴリズム D に対しても小さいような関数 G で効率的計算可能なものを作ってみせることが問題となる。関数 G がこの性質をもつとき関数 G はクラス $\mathcal{C}$ をだます (fool) という。

9. 1 ビット通信に対する疑似ランダムネス生成

前節の話をもより計算らしい枠組みで言い直し、関数 G が「1 ビット通信計算」のクラスをだましていることを見てみよう。

ボブとアリスが r ビット列 $x, y \in \{0, 1\}^r$ をそれぞれ受け取る。ボブは自分の入力 x に関して 1

ビットの情報をアリスに送る。アリスは送られた 1 ビットと自分の入力 y に基づいて 0 か 1 かを決定し二人の出力とする。ボブとアリスそれぞれについて計算量には何の制限も加えない、すなわち、任意の関数を計算できるとする。

以上の「1 ビット通信計算」は次のように定式化できる。ボブは集合 $\{0, 1\}^r$ のある分割 $\{0, 1\}^r = X_0 \cup X_1$ ($X_0 \cap X_1 = \emptyset$) を決めており、入力 x に対して、 $x \in X_b$ となるビット b をアリスに送っている。アリスは集合 $\{0, 1\}^r$ の2つの分割 $(Y_{00}, Y_{01}), (Y_{10}, Y_{11})$ を決めている。2つの分割はボブから受け取るビットに対応している。アリスは、送られてきたビット b と自分の入力 y に基づき、 $y \in Y_{bc}$ を満たすビット c を出力する。

集合 $R \subseteq \{0, 1\}^{2r}$ が $R = S \times T$, $S, T \subseteq \{0, 1\}^r$ の形に書けると、集合 R を組み合わせ論的長方形 (combinatorial rectangle) と呼ぶ。この後単に長方形と呼ぼう。

以上のボブとアリスの計算では、入力 (x, y) が4つの長方形 $X_0 \times Y_{00}, X_0 \times Y_{01}, X_1 \times Y_{10}, X_1 \times Y_{11}$ のどれに属しているかで出力の 0/1 が決定する。

改めて分布 $G(U_m)$ と分布 U_{2r} の比較をしよう。任意の長方形 $R = S \times T$ に関して、分布 U_{2r} によって選んだ (x, y) が R に属する確率と分布 $G(U_m)$ によって選んだ (x, y) が R に属する確率の差は α 以下で小さい。したがって、二つの分布に従って入力 (x, y) を選んだ時の出力が 0/1 となる確率を考えると二つの確率の差は 4α 以下で小さい。

すなわち、1 ビット通信という制限のもとでは、どのようなやり方によっても、ボブとアリスは自分たちの受け取った (x, y) が分布 U_{2r} に従ったものなのか、分布 $G(U_m)$ に従ったものなのかをほとんど区別できない。

10. グラフのジグザグ積

グラフ G とグラフ H のジグザグ積 $\text{zigzag}(G, H)$ についてインフォーマルに説明する。

グラフ G を n 頂点の 12-正則なグラフ、グラフ H を 12 頂点の 3-正則なグラフとする。

まずグラフ G の各頂点 u に接続している 12 本の辺に任意に 1 から 12 の順番をつける．頂点 u と頂点 v を結ぶ辺 e の u に関する順番と v に関する順番が一致する必要はない．例えば、辺 e が u にとっては 4 番目の辺で v にとっては 1 番目の辺であってもかまわない．

グラフ H は丸い時計で考えよう．1 から 12 の数字が頂点で各数字には 3 本の辺がつながっている．グラフ G の各頂点に時計すなわち H のコピーを置いたとする．全部で $12n$ 個の時計の数字が $\text{zigzag}(G, H)$ の頂点となる．

グラフ G の頂点 u における時計の 12 が時計内の 3 本の辺で 4, 6, 8 につながっているとし、この中で 4 にフォーカスして、12 から 4 にたどり着いた後を説明する．グラフ G において頂点 u の 4 番目の辺 e は u を頂点 v に結ぶもので、また e は v にとっての 1 番目の辺だとする．すると u の時計の 4 からは e をたどって v における時計の 1 にたどりつく．さらにこの 1 から v の時計内でつながっている 3 つの数字へとたどりつく．

以上と同じことを u の時計の 4, 6, 8 すべてに対して考えてたどりつく合計 $3 \times 3 = 9$ 個のところでスタート地点である u の時計の 12 を 9 本の辺で結ぶ．時計内部の辺を 1 本、外部の辺を 1 本、内部の辺を 1 本と『Z』の形にたどっていく様子からジグザグと呼ばれる．

一般には、 n 頂点 m -正則なグラフ G と m 頂点 d -正則なグラフ H に対して $\text{zigzag}(G, H)$ が定義され、ジグザグ積は nm 頂点の d^2 -正則なグラフとなる．

定理 1 (Reingold-Vadhan-Wigderson [5]) グラフ G が α -エクspander、 H が β -エクspander のとき、 $\text{zigzag}(G, H)$ は $\phi(\alpha, \beta)$ -エクspander となる．ここで、 ϕ は次を満たす．

$$\phi(\alpha, \beta) \leq \alpha + \beta.$$

$$\phi(\alpha, \beta) \leq 1 - (1 - \beta^2)(1 - \alpha)/2.$$

10.1 エクspanderの構成

グラフ G のべき乗、例えば G^4 を作ると、スペ

クトラルギャップは大きくなるが次数が同じべき乗の形で増大する．ここで強いエクspanderであるグラフ H とのジグザグ積をとると次数が下がり、スペクトラルギャップはたいして減少しない．以上の原理により、べき乗とジグザグ積を用いて次のようにエクspanderの族を構成できる．

補助グラフ H を頂点数が d^4 で d -正則な $(1/4)$ -エクspander とする．ここで d は定数なので、このようなグラフ H はしらみつぶしに探して見つけることにしてもよい．このようなグラフ H が存在することは確率的手法で証明できる．しらみつぶしより効率的なやり方も知られている．

グラフ G_l を次のように構成する．

$$G_1 = H^2.$$

$$G_{l+1} = \text{zigzag}(G_l^2, H).$$

すると、グラフ G_l は頂点数が d^{4l} で d^2 -正則な $1/2$ -エクspander となる．

10.2 レインゴールドのアルゴリズム

アルゴリズムは次の方針と目標に基づく．

入力グラフ G を次数 $O(1)$ 、頂点数 $\text{poly}(n)$ の $1/2$ -エクspander G' に変換したい．任意の $1/2$ -エクspander に対しては、直径が $O(\log n)$ なのは明らかなので、連結の判定が $O(\log n)$ の記憶容量でできる．すなわち、頂点 s からの長さ $O(\log n)$ のパスをすべてためせばよい．

ただし、変換した G' に関する探索は、あくまで入力 G に基づいて行う．記憶容量の制限からグラフ G' を全部書き下すようなことはできない．しかし、この問題は単に注意深く考えるだけで解決できる．

次のような変換を考える．補助グラフ H を頂点数が d^{16} で d -正則な $1/2$ -エクspander とする．グラフ G を任意の連結な頂点数 n 以下の d -正則無向グラフとしよう．実際は入力グラフの各連結成分に対して同じことを考える．グラフ G は $(1 - \Omega(1/n^2))$ -エクspander であるということをふまえて、グラフ G_l を次のように定義する．

$$G_1 = G.$$

$$G_{l+1} = (\text{zigzag}(G_l, H))^8.$$

グラフ G_l のスペクトルギャップは $\Omega(1/n^2)$ から始まり、 l が 1 増えるごとに倍程度になることが、ジグザグ積のスペクトラルギャップに関する定理 1 の二番目の不等式よりわかる。

したがって、 $l = O(\log n)$ に対してグラフ G_l は $1/2$ -エクスパンダーとなる。グラフ G_l は d^{16l} -正則で頂点数は nd^{16l} となり、 d は定数なので目標が達成できた。

11. 文献注釈, おわりに

ここで触れた以外にもエクスパンダーの応用として、効率的符号の構成 (expander codes)、スーパーコンセンレーター (superconcentrator) の構成、計量的埋め込み (metric embedding) の話などがある。有限の距離空間、例えばグラフ上の最短路距離を歪み最小でユークリッド空間に埋め込むことを考えるとエクスパンダーは埋め込みにくい。

エクスパンダーについては、(1), (2), (3) がよい情報源だと思う。レインゴールドの結果は (4) で、ジグザグ積は (5) で発表された。ランダムネスの節約、除去、抽出というトピックの情報源としては (6) と (7) を挙げておく。文献 (8) は「ランダムネスと計算」を含め現在の計算量理論全体をよく説明している。幅広く強く勧めたい。

本稿の冒頭にあげた出来の悪いコイン問題は、弱いソースからほぼ様なランダムビット列を抽出する問題、ソースの含むランダムネスを出来るだけ無駄なく抽出する問題 (extractor) として定式化される。計算量理論の中で、extractor, disperser, conductor といったものの構成の改良が数年続いて来た。数ヵ月前の STOC という会議で、Zuckerman が強い extractor の構成によりグラフの最大クリークサイズの近似と彩色数の近似について近似の難しさの証拠の強化を発表し、また、Barak らが組合せ論で有名なラムゼイグラフ

の構成問題について Frankl-Wilson の構成のサイズの改良を、2-source disperser によって与えた。この研究の流れは、現在、広く大きなインパクトのある結果がいつでてもおかしくない状態にあるように筆者は思うのだがどうなるであろうか。

参考文献

- 1) Giuliana Davidoff, Peter Sarnak, and Aalin Valette: *Elementary number theory, group theory, and Ramanujan graphs*. volume 55 of London Mathematical Society Student Texts, Cambridge University Press, 2003.
- 2) Fan R. K. Chung: *Spectral Graph Theory*. CBMS Regional Conference Series in Mathematics, number 92, American Math Society, 1997.
- 3) Shlomo Hoory, Nathan Linial, Avi Wigderson: *Expander Graphs and their Applications*, *book draft*, available on the web, 2006.
- 4) Omer Reingold: Undirected st-connectivity in log-space. In: *Proceedings of the 37th ACM Symposium on Theory of Computing*, 376–385, ACM Press, 2005.
- 5) Omer Reingold, Salil Vadhan, and Avi Wigderson: Entropy waves, the zig-zag graph product, and new constant-degree expanders. *Ann. of Math.* (2), 155(1): 157–187, 2002.
- 6) Luca Trevisan: Pseudorandomness and Combinatorial Constructions. To appear in: *Proceedings of the International Congress of Mathematicians*, 2006.
- 7) Russel Impagliazzo: Hardness vs randomness: a survey of universal derandomization. In *Proceedings of the International Congress of Mathematicians*, vol. 3, 659–672, 2002.
- 8) Avi Wigderson: P, NP and Mathematics - a computational complexity perspective. *manuscript*, www.math.ias.edu/~avi, 2006.

(たるい・じゅん, 電気通信大学)