明示的構成の計算量と値域回避問題

Complexity of Explicit Constructions and Range Avoidance Problems

安永 憲司

東京工業大学

2022年8月25日

エクスパンダーグラフの構成手法の確立とその応用@九州大学

講演の流れ

値域回避問題と明示的構成問題

値域回避問題に関する最近の研究

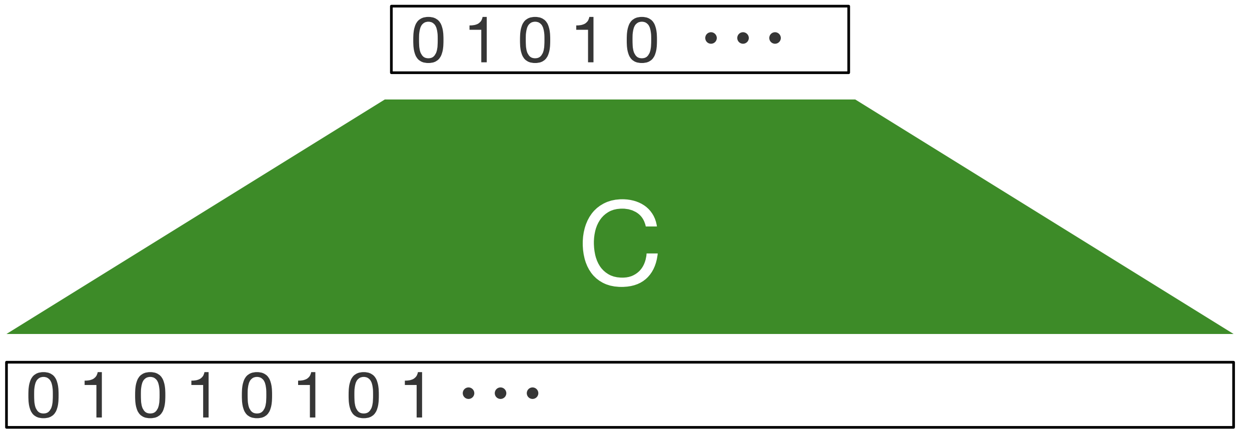
誤り訂正符号の明示的構成と値域回避問題

リスト復号可能な符号とエクスパンダーグラフ

値域回避問題 (Range Avoidance Problem / AVOID)

入力：回路 $C : \{0,1\}^n \rightarrow \{0,1\}^m$ ($n < m$)

出力：$y \notin \mathrm{Range}(C)$ ($y \in \{0,1\}^m$ s.t. $\forall x \in \{0,1\}^n, C(x) \neq y$)



問題のインスタンスを, 多項式時間で AVOID のインスタンスに変換することで解ける

Korten (FOCS'21)

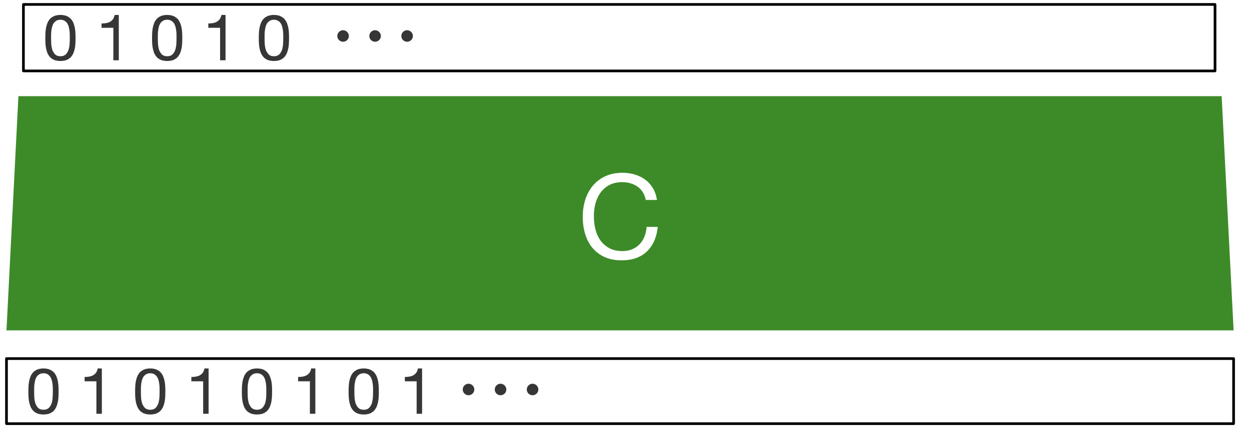
- 計算量クラス APEPP : AVOID に多項式時間帰着できる問題
- 様々な明示的構成法問題が APEPP に入る

計算量クラス PEPP

Kleinberg, Korten, Mitropolsky, Papadimitriou (ITCS'21) が導入

EMPTY に多項式時間帰着できる問題

- EMPTY：入力は回路 C : [N-1] → [N]，出力は $y \notin \mathrm{Range}(C)$



[N] = { 1, 2, …, N }

適切な $\eta : \{0,1\}^{\log N} \to [N]$ が存在

定理１ [KKMP'21]： FNP $\subseteq$ PEPP

FNP : 計算量クラス NP の探索版

L $\in$ NP ⇔ 多項式時間計算可能な二項関係 R が存在して,
x $\in$ L $\subseteq$ $\{0,1\}^*$ ⇔ $\exists y$ s.t. $|y| = \mathrm{poly}(|x|)$, $(x, y) \in R$

FNP の問題：多項式時間計算可能な R が存在して，入力 x に対し,
$|y| = \mathrm{poly}(|x|)$ かつ $(x, y) \in R$ を満たす y があればそれを出力.
それ以外は No を出力

SAT は FNP 完全 : 任意の FNP 問題は SAT に帰着できる

定理 1 [KKMP'21]： FNP $\subseteq$ PEPP

証明

- SAT が EMPTY に帰着できることを示せばよい
- 入力論理式 ϕ は，$\phi(1111\cdots1) = 0$ と仮定
- Φ に対し，以下を満たす回路 $C : [2^n - 1] \rightarrow [2^n]$ を準備
    - $\Phi(y) = 1$ のとき $C(y) = 1^n$, $\Phi(y) = 0$ のとき $C(y) = y$

割り当て y	$\Phi(y)$	$C(y)$
0000000	1	1111111
⋮		
1110000	0	1110000
1110001	1	1111111
⋮		
1111111	0	NA

$y \notin \mathrm{Range}(C)$ を出力

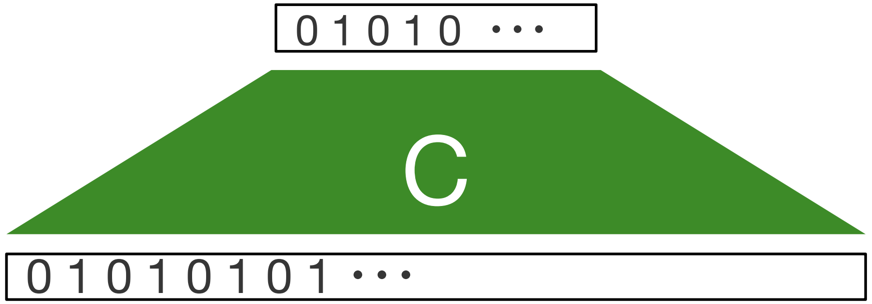
$\Leftrightarrow$ $\Phi(y) = 1$ を満たす y を出力

AVOID vs. EMPTY

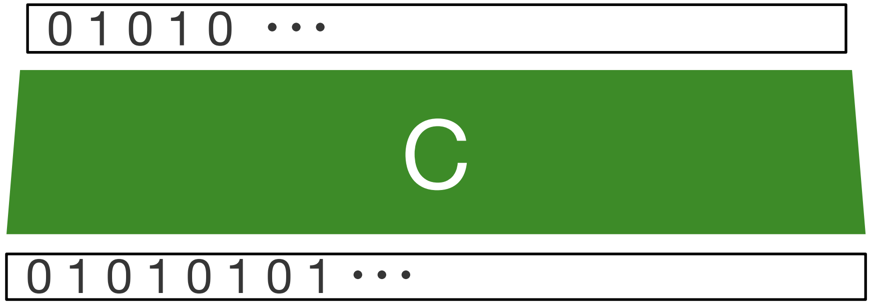
AVOID の方が簡単（ $y \notin \mathrm{Range}(C)$ である y が多い）

- ランダムに y を選べば確率 ≥ 1/2 で正しい y が見つかる

EMPTY を使えば NP 問題を解ける（FNP ⊆ PEPP）が,
AVOID も同様にできるか（FNP ⊆ APEPP ?）は不明



AVOID



EMPTY

APEPP の特徴づけ [Korten'21]

APEPP は様々な明示的構成問題を含む

- 回路計算量 $2^n/2n$・長さ 2^n の真理値表の構成
- 擬似乱数生成器の構成
- 二情報源 (two-source) 乱数抽出器の構成
- ridigity の高い行列の構成
- 時間制約 Kolmogorov 計算量 n-1・長さ n の文字列の構成

共通の証明方針：
n ビット文字列が性質 π をもたない
→ n ビットより短く表現できる

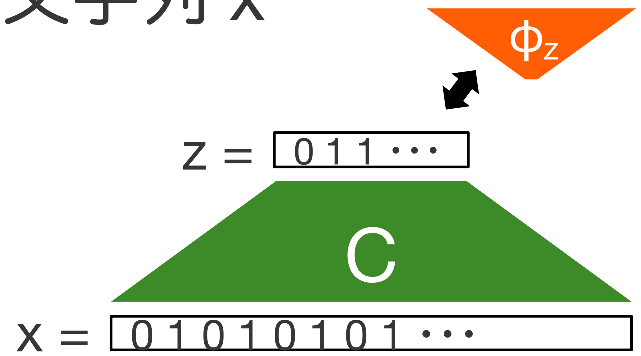
回路計算量 $2^{\varepsilon n}$・長さ 2^n の真理値表構成は APEPP 完全

- ただし，P^{NP} 帰着
- 「AVOID が P^{NP} で解ける ⇔ E^{NP} に回路計算量 $2^{\Omega(n)}$ の言語が存在」

回路計算量の大きな真理値表の構成

Hard Truth Table (HTT)

- 入力：1^N
- 出力：サイズ N/2log(N) の回路で計算できない長さ N の文字列 x
  - 回路で計算できる：$\exists C$ s.t. $C(i) = x_i$ for $\forall i \in [N]$



定理２． HTT は AVOID に多項式時間帰着できる

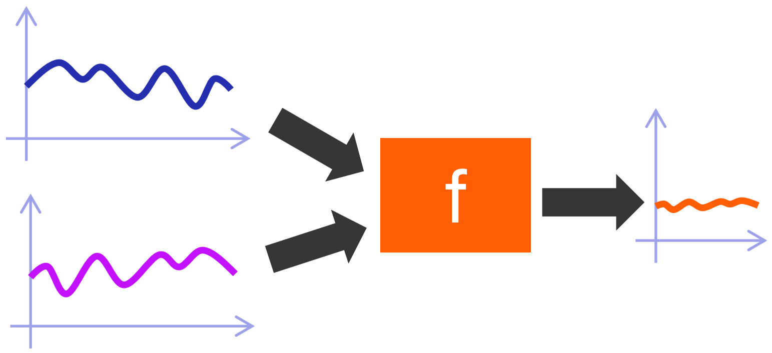
<u>証明</u>

- AVOID への入力回路 C は，C への入力 z を回路 $\phi_z : \{0,1\}^{\log(N)} \to \{0,1\}$ とみなし，N 通りの出力結果を長さ N の真理値表 x として出力
- サイズ s の回路は 2s log(s) + O(s) ビットで記述可能
- $s \leq N/2\log(N)$ であれば，ϕ_z は N より小さいビット数で記述可能
- $\forall x \notin \mathrm{Range}(C)$ は回路計算量が N/2log(N) より大きい （証明終）

乱数抽出器の構成

(k, ε)-二情報源 (two-source) 乱数抽出器 $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$

⇔ $\forall X, Y \subseteq \{0,1\}^n, |X| = |Y| = 2^k, b \in \{0,1\}$ s.t. $|\ \Pr[\ f(U_X, U_Y) = b] - 1/2\ | \leq \varepsilon$



(k, 1/2)-二情報源乱数抽出器が存在

➔ 頂点数 2^n の 2^{k-1}-Ramsey グラフが存在

- K-Ramsey グラフ
  ⇔ サイズ K のクリークや独立集合をもたないグラフ

(k, ε)-EXTRACTOR

- 入力：1^n
- 出力：(k(n), ε(n))-二情報源乱数抽出器である回路 f

定理３． $1/n^c < \varepsilon < 1/2$ に対し，$(\log(n)+2\log(1/\varepsilon)+3, \varepsilon)$-EXTRACTOR は AVOID に多項式時間帰着できる

証明

AVOID への入力回路 $C : \{0,1\}^{<2nD} \to \{0,1\}^{2nD}$

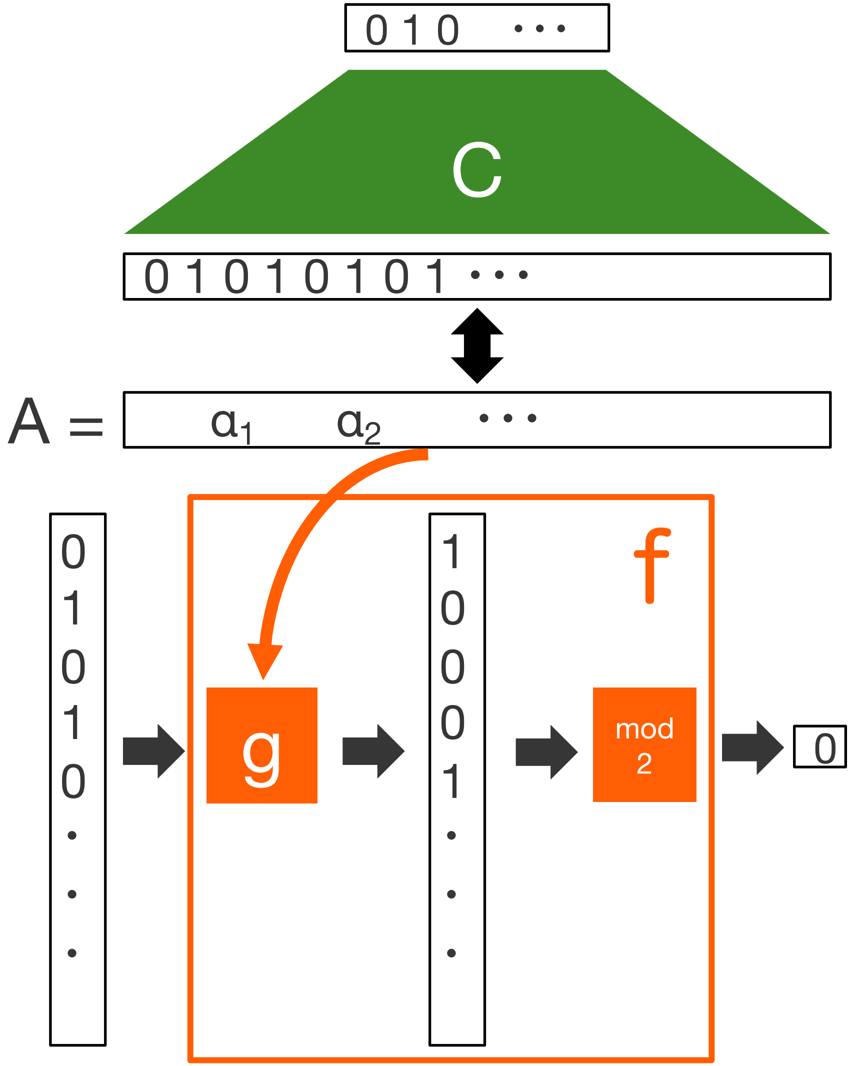
出力の 2nD ビットを $A = (a_1, \ldots, a_D) \in \mathbf{F}_q{}^D$ に対応

- $q = 2^{2n}$, $D = d^2n^2$, $d = 4/\varepsilon^2$

$g : \{0,1\}^{2n} \to \{0,1\}^{2n}$ と $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ を

$$g(x) = \Sigma_{i=1,..,D}\, a_i x^{i-1}, \quad f(x) = \Sigma_{i=1,\ldots,2n}\, g(x)_i \bmod 2$$

と定める．二情報源乱数抽出器 f が A から定まる．



証明の続き

回路 C として，f が (log(dn), ε)-乱数抽出器でないような A をすべて Range(C) に含むものを示せばよい（➔ $\forall A \notin$ Range(C) は所望の抽出器）

f が (log(dn), ε)-乱数抽出器でない

⇔ $\exists X, Y \subseteq \{0,1\}^n$, $|X| = |Y| = dn$, $b \in \{0,1\}$ s.t. $\Pr_{x\sim U(X), y\sim U(Y)}[\, f(xy) = b\,] > 1/2 + \varepsilon$

$R := \{\, xy \mid x \in X, y \in Y \,\} \subseteq \{0,1\}^{2n}$, $|R| = |X||Y| = d^2n^2 = D$

$R' := (r_1, \ldots, r_D) \in \mathbf{F}_q^{\,D}$: R の各要素を辞書順に $\mathbf{F}_q$ の要素に対応させたもの

$\exists S \subseteq \{1, \ldots, D\}$ s.t. $|S|/D \geq 1/2 + \varepsilon$, $\forall i \in S$, $f(r_i) = b$

β_i := ($g(r_i)$ の先頭 2n – 1 ビット) のとき，$i \in S$ ➔ (β_i, b) から $g(r_i)$ を復元できる

➔ (X, Y, b, S, $\{\beta_i\}_{i\in S}$) から $\{ g(r_i) \}_{i \in S}$ を復元できる

➔ g(x) は次数 D – 1 なので係数 $a_1, \ldots, a_D$ も復元できる

つまり，(X, Y, b, S, $\{\beta_i\}_{i\in S}$) から A を復元できる（この計算を回路 C で行う）

2nD ビットよりも短ければ OK

値域回避問題に関する最近の研究

値域回避問題に関する最近の研究

Kleinberg, Korten, Mitropolsky, Papadimitriou (ITCS’21) Total Functions in the Polynomial Hierarchy

- PEPP に関する研究

Korten (FOCS’21) The Hardest Explicit Construction

- APEPP に関する研究

Ren, Santhanam, Wang (FOCS’22) On the Range Avoidance Problem for Circuits

- 回路を限定した値域回避問題 (AVOID) に関する研究と計算量理論とのつながり

Guruswami, Lyu, Wang (RANDOM’22) Range Avoidance for Low-depth Circuits and Connections to Pseudorandomness

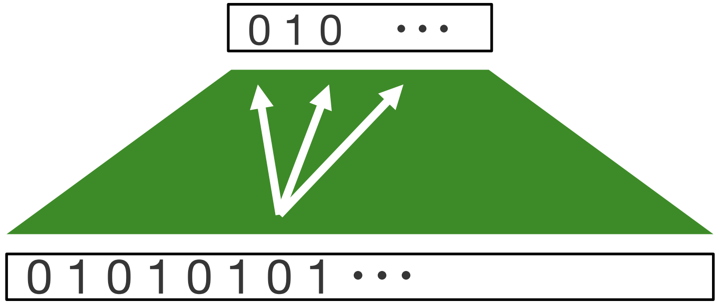
- 回路を限定した AVOID に関する研究（特に定数段回路）

回路を限定した AVOID

D-AVOID （回路クラス D に対する AVOID）

- 入力：回路 $C : \{0,1\}^n \rightarrow \{0,1\}^m$ ($n < m$) s.t. $C \in D$
- 出力：$y \notin \mathrm{Range}(C)$

m：ストレッチ



NC^0_3 回路

<u>D の候補</u>

- 多項式サイズ回路：これまで考えてきたもの
- AC^0 回路：定数段の多項式サイズ回路
- NC^i 回路：$O(\log(n)^i)$ 段の多項式サイズ回路で，各素子の fan-in が 2
- NC^0_k：定数段の多項式サイズ回路で，各出力が入力 k 個に依存
- Formula（論理式）：各素子の fan-out が 1 の回路

Ren, Santhanam, Wang (FOCS'22) の結果

結果１：D-AVOID に FP^{NP} アルゴリズムが存在するための十分条件

- 十分条件：ある D' に対し，あるデータ構造が存在すること
- 結果として，E^{NP} に対する回路下界の新しい特徴づけ

結果２：D-AVOID に対するアルゴリズムが新しい回路下界を与える

- m = quasi-poly(n) の AC^0-AVOID が FP^{NP} ➔ $E^{NP} \not\subseteq NC^1$
- $m = n + n^{o(1)}$ の NC^0_4-AVOID が FP^{NP} ➔ $E^{NP} \not\subseteq$ Formula[$2^{o(n)}$]

結果３：AVOID が FNP であることと，ある命題証明系が存在することの等価性

- その中で，時間制約 Kolmogorov 計算量に関する問題が AVOID の完全問題

Guruswami, Lyu, Wang (RANDOM'22) の結果

結果１：NC^1-AVOID に多項式時間帰着できる明示的構成問題

- Gilbert-Varshamov 限界を達成する線形符号の構成
- 最適なリスト復号性能を達成する線形符号の構成
- rigidity の高い行列の構成

さらに，[RSW22] の結果と組み合わせると，

NC^0_4-AVOID に対する FP (FP^{NP}) アルゴリズムが存在

➔ 上記の構成問題に対する FP (FP^{NP}) アルゴリズムが存在

結果２：NC^0_2-AVOID に対する多項式時間アルゴリズム

誤り訂正符号の明示的構成と値域回避問題

誤り訂正符号の用語

符号 $C \subseteq \{0,1\}^n$ の最小ハミング距離 $d = \min_{x \neq y \in C} d_H(x,y)$

線形符号 $C \subseteq \{0,1\}^n$

$\Leftrightarrow$ ∃生成行列 $G \in \{0,1\}^{k \times n}$ s.t. $C = \{ xG : x \in \{0,1\}^k \}$, $\mathrm{rank}(G) = k$

符号 C として，符号化率 k/n と相対最小距離 d/n は大きくしたい

(r, p)-線形符号：符号化率 $r = k/n$, 相対最小距離 $\geq p$ の線形符号

Gilbert-Varshamov 限界

定理４． ∀ r, p ∈ (0,1) s.t. r < 1 – H(p)，(r, p)-線形符号 C ⊆ $\{0,1\}^n$ が存在.
ただし， H(x) = – x $\log_2$(x) – (1 – x) $\log_2$(1 – x)

証明

∀ε >0, r = k/n = 1 – H(p) – ε に対し (r, p)-線形符号の存在を示す.
生成行列 G ∈ $\{0,1\}^{k\times n}$ をランダムに選ぶと

$$\forall x \in \{0,1\}^k \setminus \{\mathbf{0}\},$$

$$\Pr_G[w_{\mathrm{H}}(xG) < pn] = \frac{\mathrm{Vol}(pn-1,n)}{2^n} \leq \frac{2^{nH(p)}}{2^n} = \frac{2^{n(1-r-\varepsilon)}}{2^n} = 2^{-(k+\varepsilon n)}$$

- ここで， $\mathrm{Vol}(pn-1,n) = \sum_{i=0}^{pn-1}\binom{n}{i} \approx 2^{nH(p)}$

➔ $\Pr_G[\exists x \in \{0,1\}^k \setminus \{\mathbf{0}\},\ \mathrm{s.t.}\ d_w(xG) < pn\,] \leq \left(2^k - 1\right)\cdot 2^{-(k+\varepsilon n)} \leq 2^{-\varepsilon n}$

➔ 確率 1 – $2^{-\varepsilon n}$ 以上で (1 – H(p) – ε, p)-線形符号 （証明終）

(r, p)-Linear Code 問題

- 入力：1^n
- 出力：(r, p)-線形符号の生成行列 $G \in \{0,1\}^{rn \times n}$

定理５．$\forall$ r, p $\in$ (0,1) s.t. $r < 1 - H(p)$，(r, p)-Linear Code 問題は NC^1-AVOID に多項式時間帰着できる

証明で使う「簡素な」データ構造 [Patrascu(FOCS'08)]

- Σ 上の n 要素を格納する配列が与えられたとき，その配列を

$$O(\,|\Sigma|\log(n)\,) + O(\,n/\log^2(n)\,) + \Sigma_\sigma f_\sigma \log_2(n/f_\sigma)$$

配列のエントロピーに相当

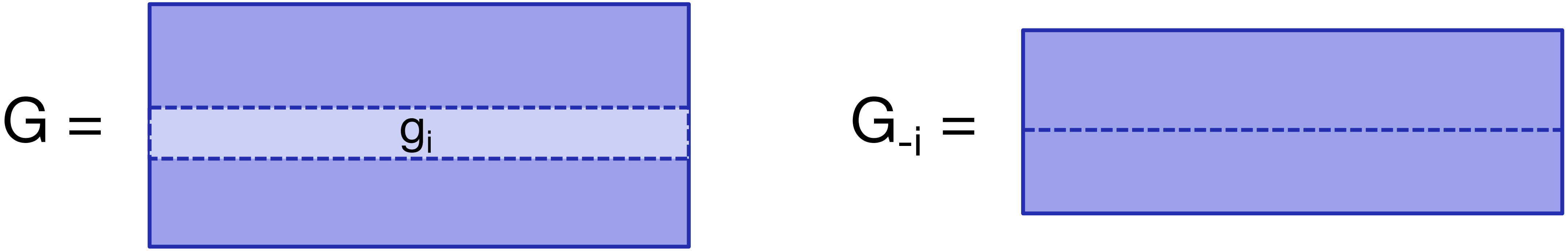
  ビットのメモリで保管するデータ構造が存在．f_σ = (σ が登場する回数)
- さらに，$i \in [n]$ に対し，O(log(n)) ビットのデータにクエリすることで i 番目の要素を取り出せる．

定理５（再掲）． $\forall r, p \in (0,1)$ s.t. $r < 1 - H(p)$，(r, p)-Linear Code 問題は NC^1-AVOID に多項式時間帰着できる

証明

$G \in \{0,1\}^{k \times n}$ が (r, p)-線形符号の生成行列でない（ $k = rn$ とおく）

$\Leftrightarrow$ $\exists z \in \{0,1\}^k \setminus \{\mathbf{0}\}$ s.t. $w_H(zG) < pn$ （ $z_i = 1$ とする ）



考察：(G_{-i}, $s = zG$, z_{-i}, i) から G を復元できる

- $g_i = s - z_{-i}\, G_{-i}$ と計算すればよい

証明の続き

考察：(G_{-i}, $s = zG$, z_{-i}, i) から G を（多項式時間で）復元できる

AVOID への入力回路 C：入力は (G_{-i}, $s = zG$, z_{-i}, i), 出力は G

- $G_{-i} \in \{0,1\}^{(k-1)\times n}$ ➔ $(k-1)n$ ビット
- $s = zG \in \{0,1\}^n$ s.t. $w_H(s) < pn$ ➔ $H(p)n + O(n/\log^2(n))$ ビット
- $z_{-i} \in \{0,1\}^{k-1}$ ➔ $k-1$ ビット
- $i \in [k]$ ➔ $\log(k)$ ビット

入力の長さ $= kn - n + (k-1) + H(p)n + O(n/\log^2(n))$

$$= kn - n(1 + k/n + H(p) + O(1/\log^2(n)) - 1/n) < kn$$

- $k/n = r < 1 - H(p) - O(1/\log^2(n))$ で，n が十分大きいとき

以上より，任意の $G' \notin \mathrm{Range}(C)$ は (r, p)-線形符号 （証明終）

(r, p, L)-List Decodable 問題

- 入力：1^n
- 出力： (p, L)-リスト復号可能な線形符号の生成行列 $G \in \{0,1\}^{rn \times n}$
  - 符号 $C \subseteq \{0,1\}^n$ が (p, L)-リスト復号可能

$\Leftrightarrow \forall z \in \{0,1\}^n, |\{ c \in C : d_H(z, c) \le pn \}| \le L$

$\Leftrightarrow \forall z \in \{0,1\}^n, |\{ x \in \{0,1\}^{rn} : w_H(xG - z) \le pn \}| \le L$

定理６． $\forall r, p, L$ s.t. $r < 1 - H(p) - 2/\log_2(L)$, (r, p, L)-List Decodable 問題は NC^1-AVOID に多項式時間帰着できる

定理６（再掲）．$\forall r, p, L$ s.t. $r < 1 - H(p) - 2/\log_2(L)$,
(r, p, L)-List Decodable 問題は NC^1-AVOID に多項式時間帰着できる

証明

$G \in \{0,1\}^{k\times n}$ が (p,L)-リスト復号可能な符号の生成行列でない（ $k = rn$ ）
$\Leftrightarrow \exists z \in \{0,1\}^n$ s.t. $|\{ x \in \{0,1\}^k : w_H(xG - z) \le pn \}| \ge L+1$

リストから線形独立な符号語 $t = \log_2(L)$ 個 → $\{ y_1+z, y_2+z, \ldots, y_t+z \}$
➔ $\exists g_1,\ldots, g_{k-t} \in$ {Gの行} s.t. $\{g_1, \ldots, g_{k-t}, y_1+z, y_2+z, \ldots, y_t+z\}$ が線形独立

生成行列の残り t 行は線形組合せの係数 $a_1, \ldots, a_t \in \{0,1\}^k$ で表現

考察：$(z, y_1, \ldots, y_t, s, g_1, \ldots, g_{k-t}, a_1, .., a_t)$ から G を復元できる
- $s \in \{0,1\}^k$ は G における $g_1, \ldots, g_{k-t}$ を表す重み k-t の文字列
- $y_1, \ldots, y_t$ と s はデータ構造を用いて計算 ➔ NC^1 回路で G を計算可能

証明の続き

考察： $(z, y_1, \dots, y_t, s, g_1, \dots, g_{k-t}, a_1, .., a_t)$ から G を復元できる

AVOID への入力回路 C：入力は上記文字列, 出力は G

- $z \in \{0,1\}^n$ ➔ n ビット
- $y_1, \dots, y_t \in \{0,1\}^n$ s.t. $w_H(y_i) \le pn$ ➔ $t(H(p)n + O(n/\log^2(n)))$ ビット
- $s \in \{0,1\}^k$ ➔ k ビット
- $g_1, \dots, g_{k-t} \in \{0,1\}^n$ ➔ $(k - t)n$ ビット
- $a_1, .., a_t \in \{0,1\}^k$ ➔ kt ビット

入力の長さ $= n + t(H(p)n + O(n/\log_2(n))) + k + (k - t)n + kt$
$< tn(\ 1/t + H(p) + O(1/\log_2(n)) + r/t - 1 + r\ ) + kn$
$\le tn(\ r - (1 - H(p) - 2/t) + O(1/\log_2(n))\ ) + kn \quad < \quad kn$

- $r < 1 - H(p) - 2/\log_2(L)$ で，n が十分大きいとき

以上より，任意の $G' \notin \mathrm{Range}(C)$ は (p, L)-リスト復号可能 （証明終）

リスト復号可能な符号とエクスパンダーグラフ

擬似ランダムオブジェクトの統一理論

Vadhan (ICM2010). The Unified Theory of Pseudorandomness

Vadhan. Pseudorandomness. Foundations and Trends in Theoretical Computer Science, 2012

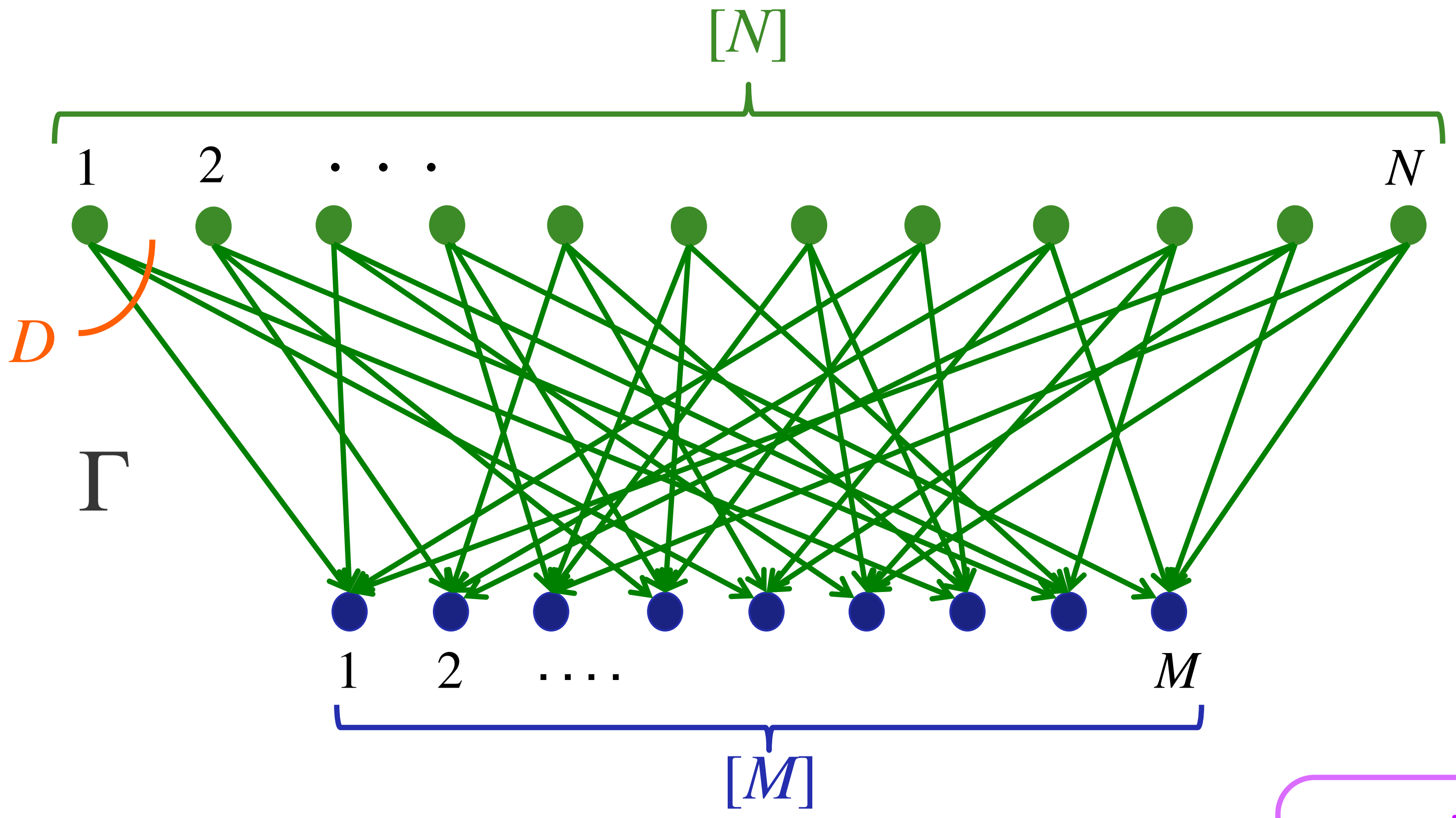
様々な擬似ランダムオブジェクトを統一的に記述可能

- 擬似乱数生成器
- エクスパンダーグラフ
- リスト復号可能符号
- 平均化標本器
- 困難性増幅器

どれもリスト復号っぽい性質

統一的な枠組み

関数 $\Gamma : [N] \times [D] \to [M]$



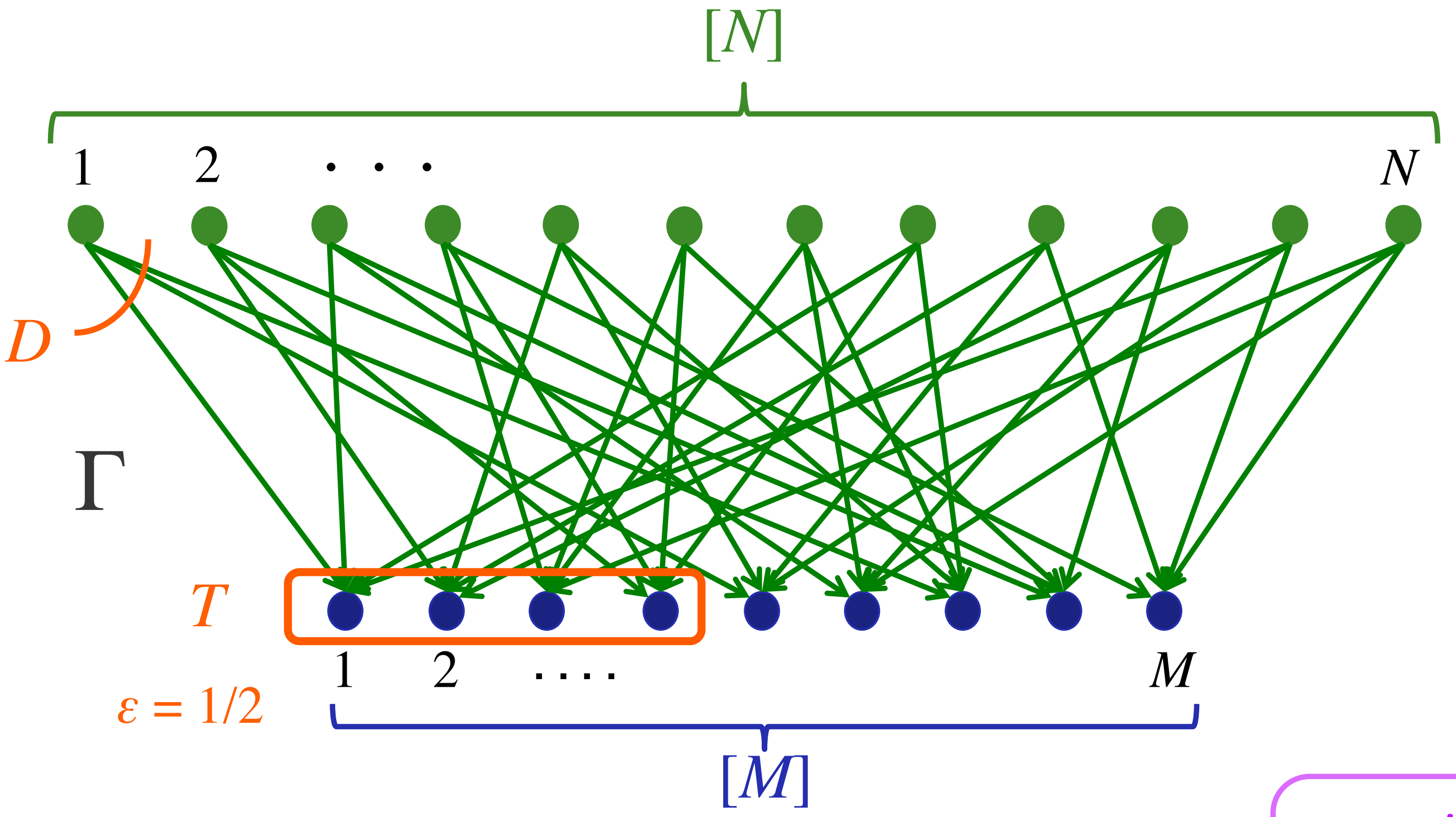
集合 $T \subseteq [M]$ と一致パラメータ ε に対して,

$$\mathrm{LIST}_\Gamma(T, \varepsilon) = \{\, x \in [N] : \Pr[\, \Gamma(x, U_{[D]}) \in T] > \varepsilon \,\}$$

T へ向かう辺の割合が
ε より大きい x の集合

統一的な枠組み

関数 $\Gamma : [N] \times [D] \to [M]$



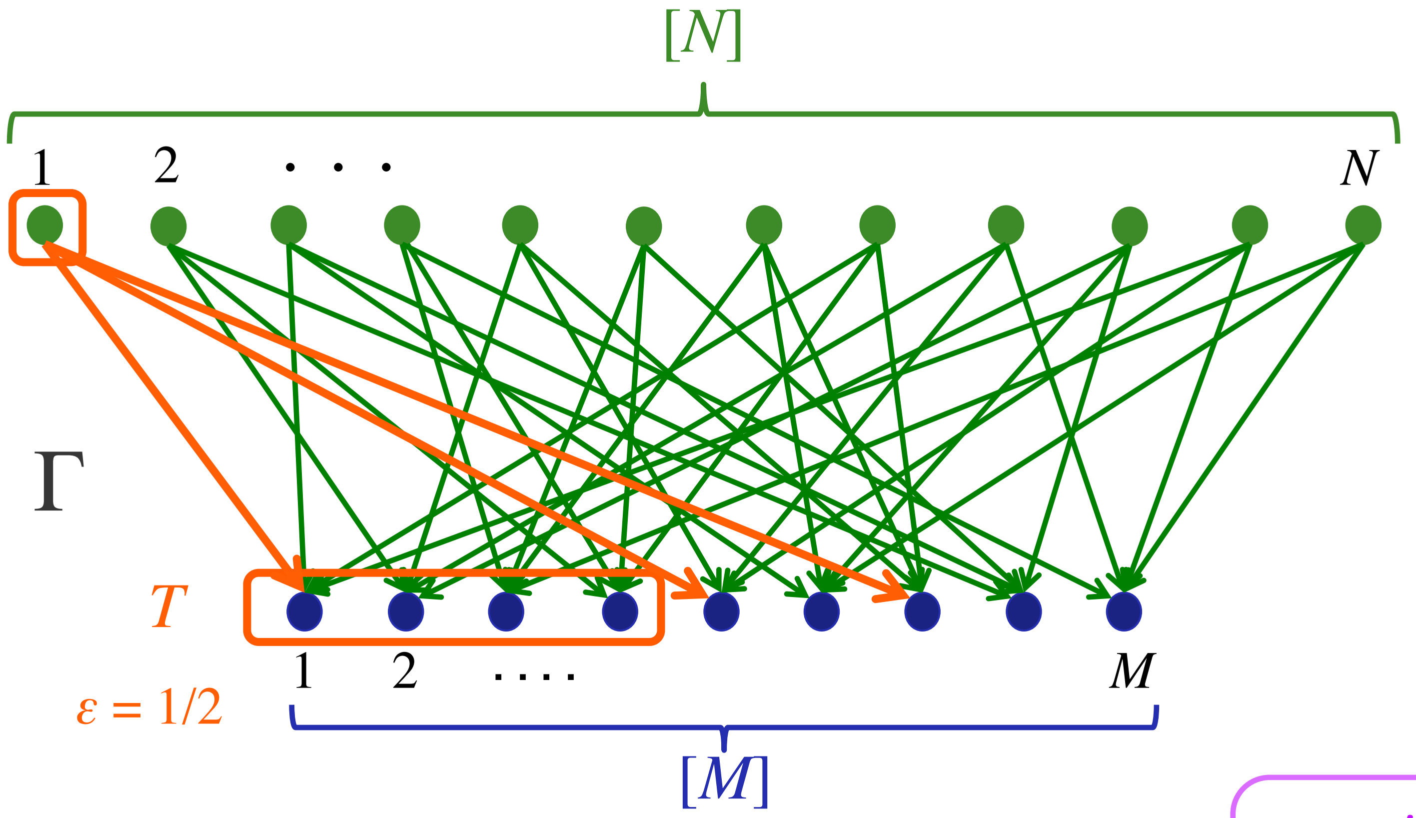
集合 $T \subseteq [M]$ と一致パラメータ ε に対して,

T へ向かう辺の割合が
ε より大きい x の集合

$$\mathrm{LIST}_\Gamma(T, \varepsilon) = \{\, x \in [N] : \Pr[\, \Gamma(x, U_{[D]}) \in T] > \varepsilon \,\}$$

統一的な枠組み

関数 $\Gamma : [N] \times [D] \to [M]$



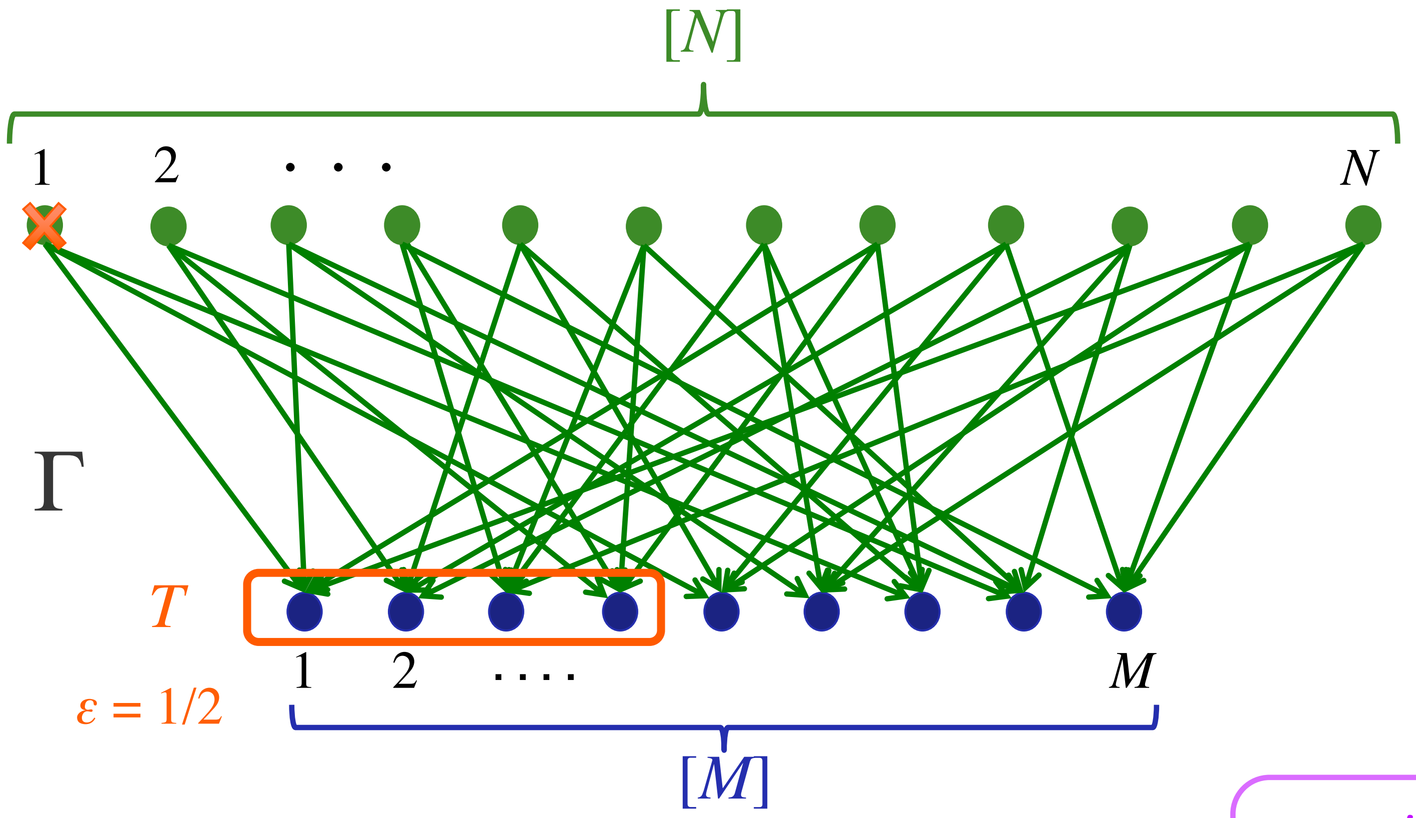
集合 $T \subseteq [M]$ と一致パラメータ ε に対して,

$$\mathrm{LIST}_\Gamma(T, \varepsilon) = \{\, x \in [N] : \Pr[\,\Gamma(x, U_{[D]}) \in T] > \varepsilon \,\}$$

T へ向かう辺の割合が
ε より大きい x の集合

統一的な枠組み

関数 $\Gamma : [N] \times [D] \to [M]$



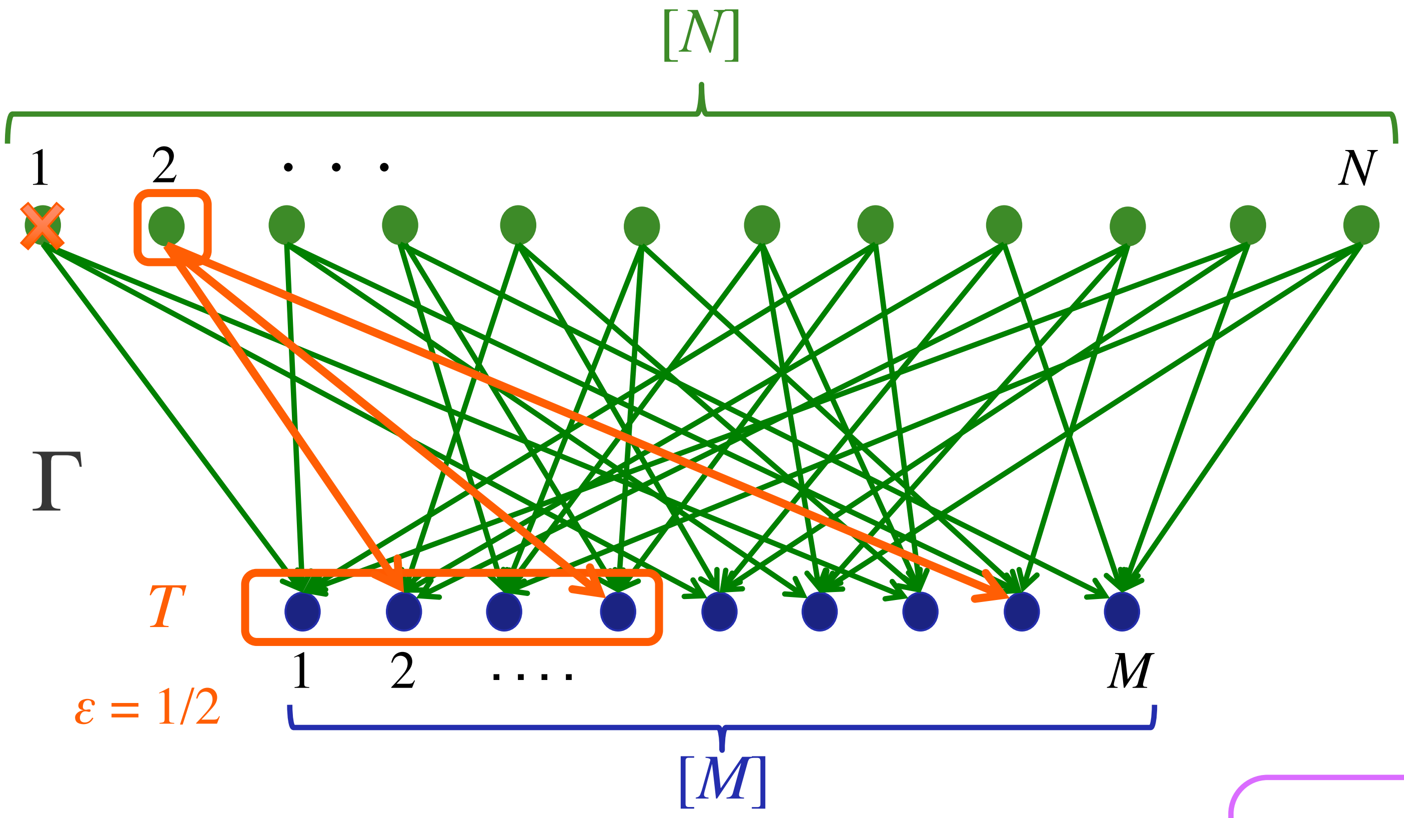
集合 $T \subseteq [M]$ と一致パラメータ ε に対して,

T へ向かう辺の割合が
ε より大きい x の集合

$$\mathrm{LIST}_\Gamma(T, \varepsilon) = \{\, x \in [N] : \Pr[\, \Gamma(x, U_{[D]}) \in T] > \varepsilon \,\}$$

統一的な枠組み

関数 $\Gamma : [N] \times [D] \to [M]$



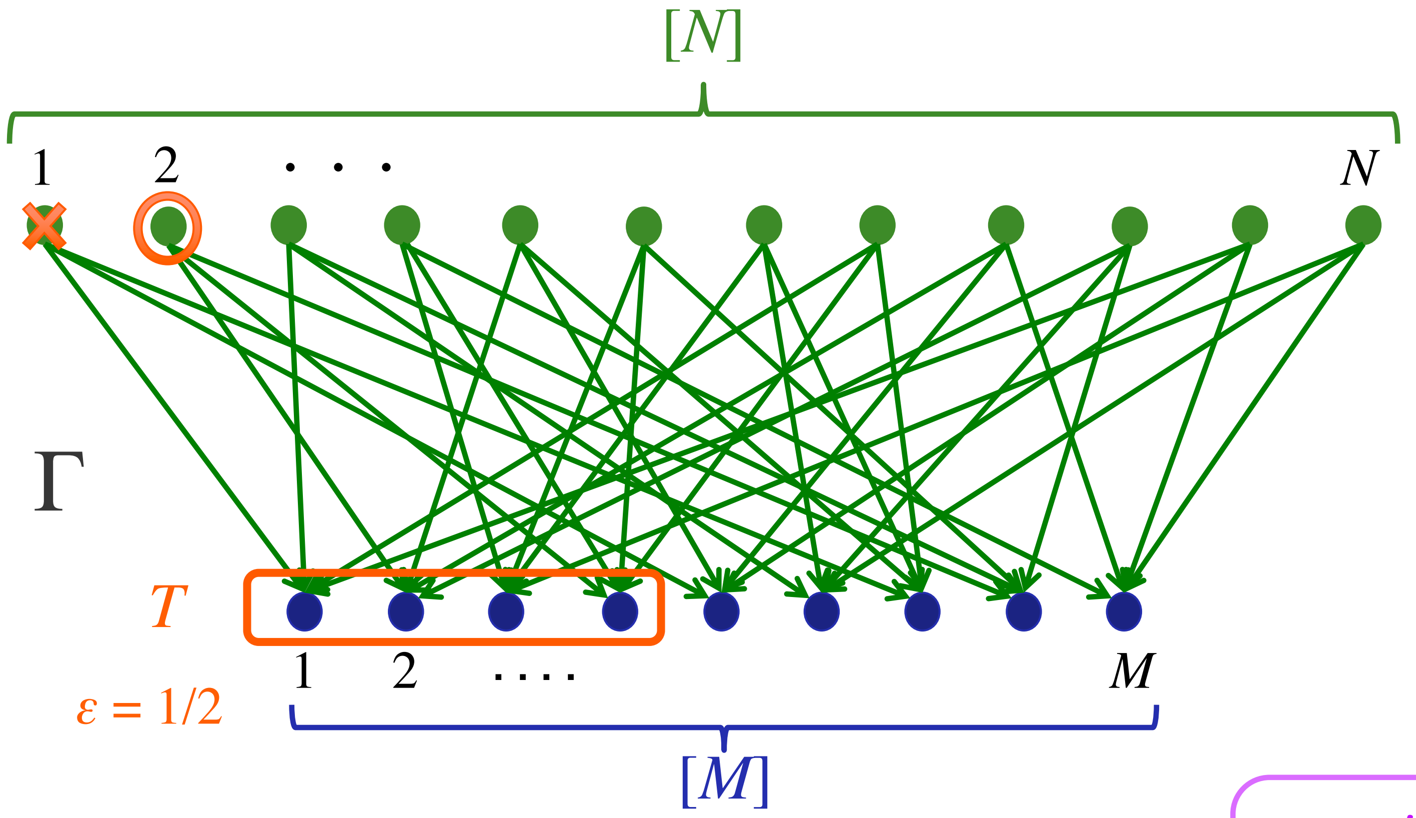
集合 $T \subseteq [M]$ と一致パラメータ ε に対して,

$$\mathrm{LIST}_\Gamma(T, \varepsilon) = \{\, x \in [N] : \Pr[\, \Gamma(x, U_{[D]}) \in T] > \varepsilon \,\}$$

T へ向かう辺の割合が ε より大きい x の集合

統一的な枠組み

関数 $\Gamma : [N] \times [D] \to [M]$



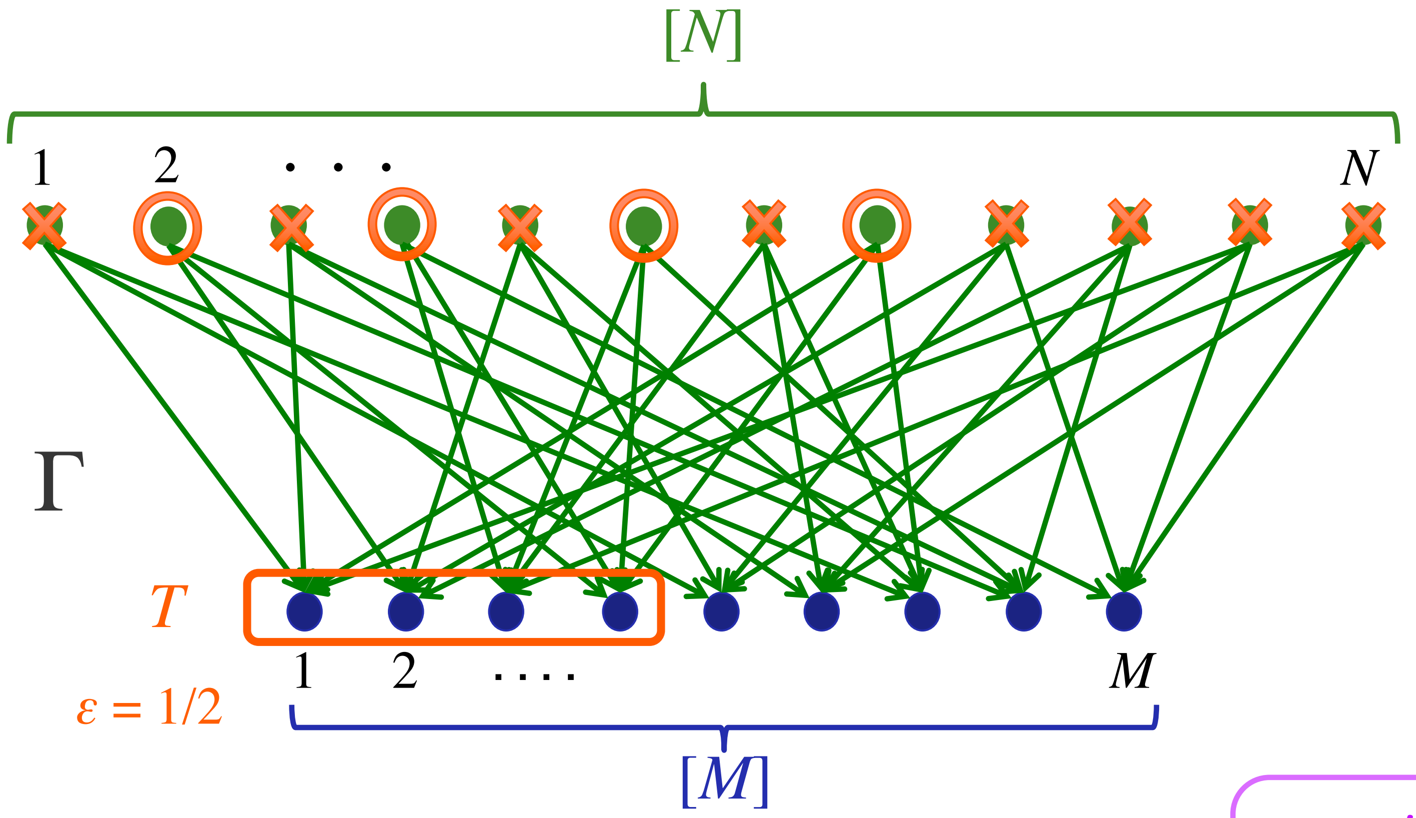
集合 $T \subseteq [M]$ と一致パラメータ ε に対して,

$$\mathrm{LIST}_\Gamma(T, \varepsilon) = \{\, x \in [N] : \Pr[\, \Gamma(x, U_{[D]}) \in T] > \varepsilon \,\}$$

T へ向かう辺の割合が
ε より大きい x の集合

統一的な枠組み

関数 $\Gamma : [N] \times [D] \to [M]$



集合 $T \subseteq [M]$ と一致パラメータ ε に対して,

T へ向かう辺の割合が
ε より大きい x の集合

$$\mathrm{LIST}_{\Gamma}(T, \varepsilon) = \{\, x \in [N] : \Pr[\, \Gamma(x, U_{[D]}) \in T] > \varepsilon \,\}$$

統一的な枠組み

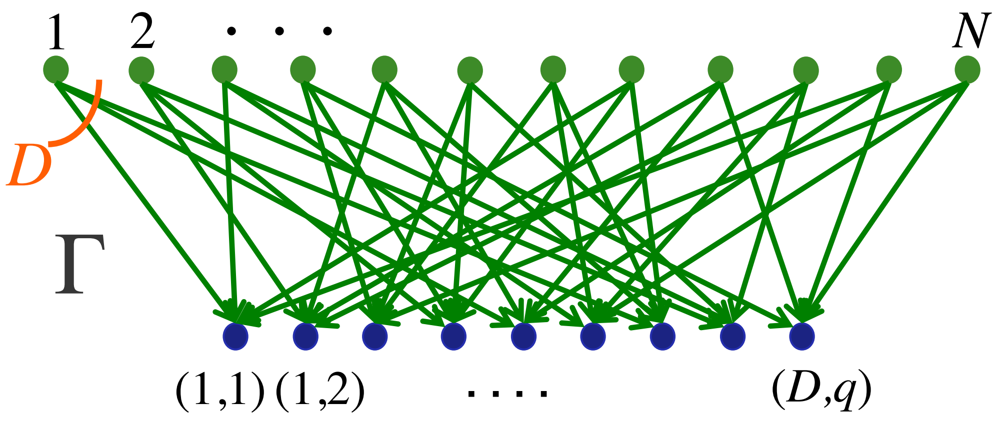
各オブジェクトに対して，
適切に関数 $\Gamma : [N] \times [D] \to [M]$ を定義したとき，

$$\forall T \in C, \quad |\mathrm{LIST}_\Gamma(T, \varepsilon)| \le K$$

という条件によって，オブジェクトを特徴づけ可能

リスト復号可能な符号の統一的記述

符号 $C \subseteq \{0,1\}^n$ が (p, L)-リスト復号可能
$\Leftrightarrow \forall z \in \{0,1\}^n, |\{ c \in C : d_{\mathrm{H}}(z, c) \leq pn \}| \leq L$



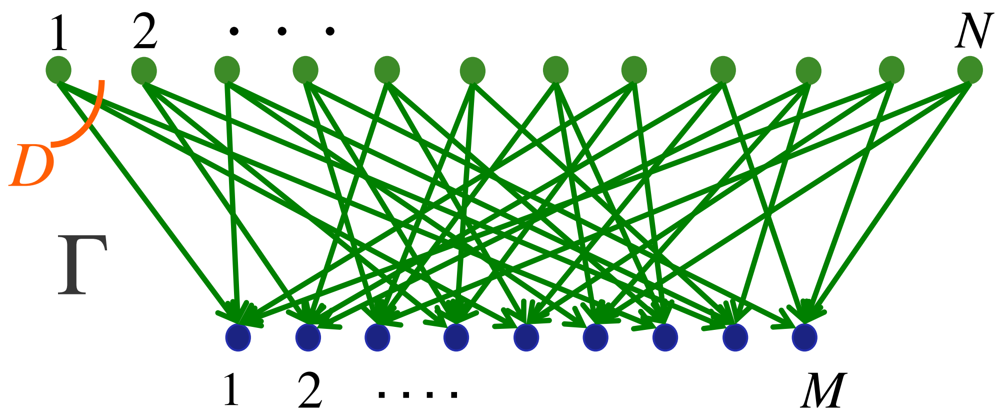
命題. 符号 $\mathrm{Enc} : [N] \to [q]^D$ が (p, L)-リスト復号可能であるための必要十分条件は，$\Gamma(x, y) = (y, \mathrm{Enc}(x)_y)$ と定めたとき，

$$\forall r \in [q]^D, \quad |\mathrm{LIST}_\Gamma(T_r, 1-p)| \leq L$$

ただし，$T_r = \{(y, r_y) : y \in [D]\}$

エクスパンダーグラフの統一的記述

G : 左頂点集合 $[N]$, 右頂点集合 $[M]$,
左頂点次数 D の二部グラフ



G が $(=K, A)$-エクスパンダー
$\Leftrightarrow \forall S \subseteq [N],\ |S| \geq K \rightarrow |\mathrm{Neigh}(S)| \geq A \cdot K$

G が (K, A)-エクスパンダー
$\Leftrightarrow \forall K' \leq K, (=K', A)$-エクスパンダー

命題. G が $(=K, A)$-エクスパンダーであるための必要十分条件は
$\Gamma(x, y) = (x$ の y 番目の隣接頂点) と定めたとき,

$$\forall T \in [M] \text{ s.t. } |T| < AK, \quad |\mathrm{LIST}_\Gamma(T, 1)| < K$$

まとめ

- 様々な明示的構成問題は値域回避問題 (AVOID) に帰着できる
- 完全問題もある（計算量の大きい文字列構成）
- 誤り訂正符号の明示的構成と値域回避問題
- GV 限界を達成する符号は NC^1-AVOID に多項式時間帰着できる
- リスト復号可能な符号とエクスパンダーグラフ

今後の展望

- 符号構成問題は完全問題になるか？（➔ 構成の難しさを納得）
- 構成問題同士の関係は？
- GV 符号・リスト復号可能符号・乱数抽出器・エクスパンダーグラフ
- 構造を入れた構成問題（とそのときのパラメータ）
- 連接符号・LDPC 符号・エクスパンダー符号