Reed-Solomon 符号と擬似ランダム性

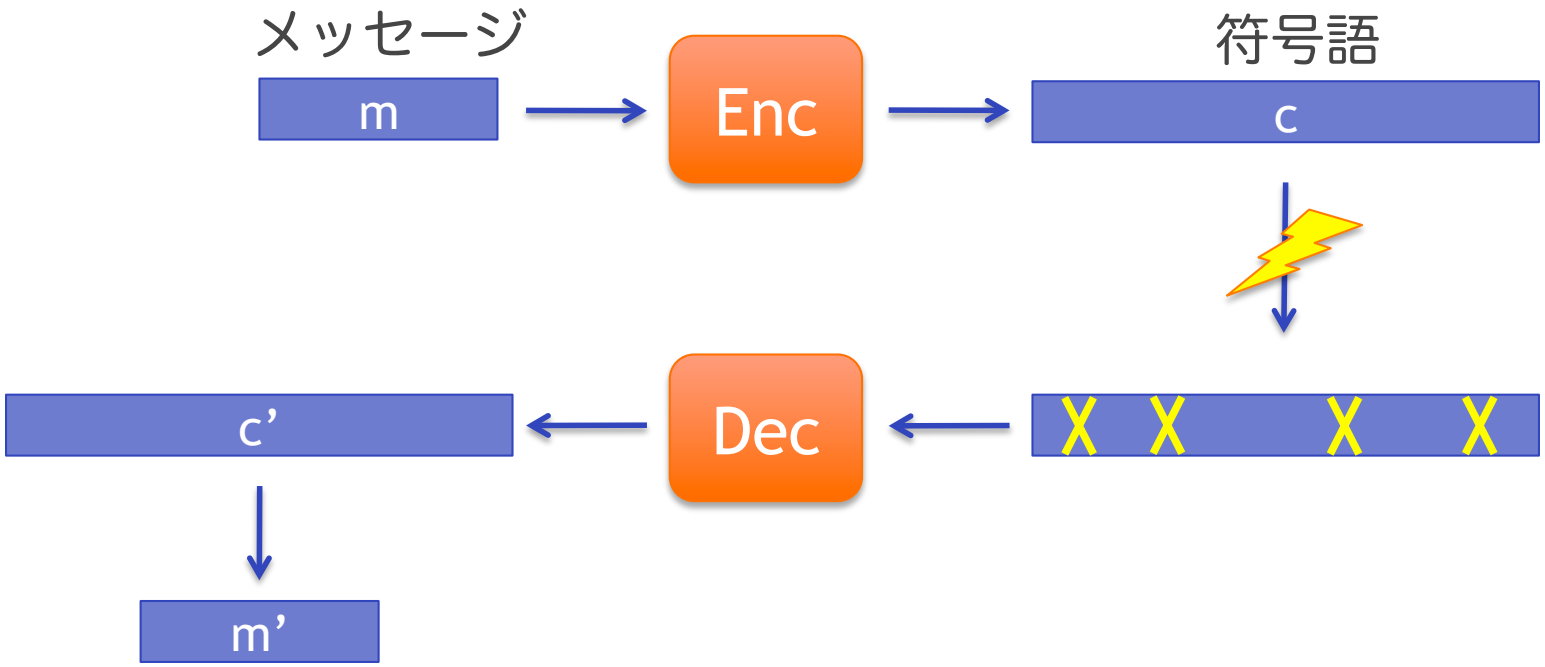
安永憲司

東京工業大学

電子情報通信学会ソサイエティ大会@大阪府立大学
2010年9月16日

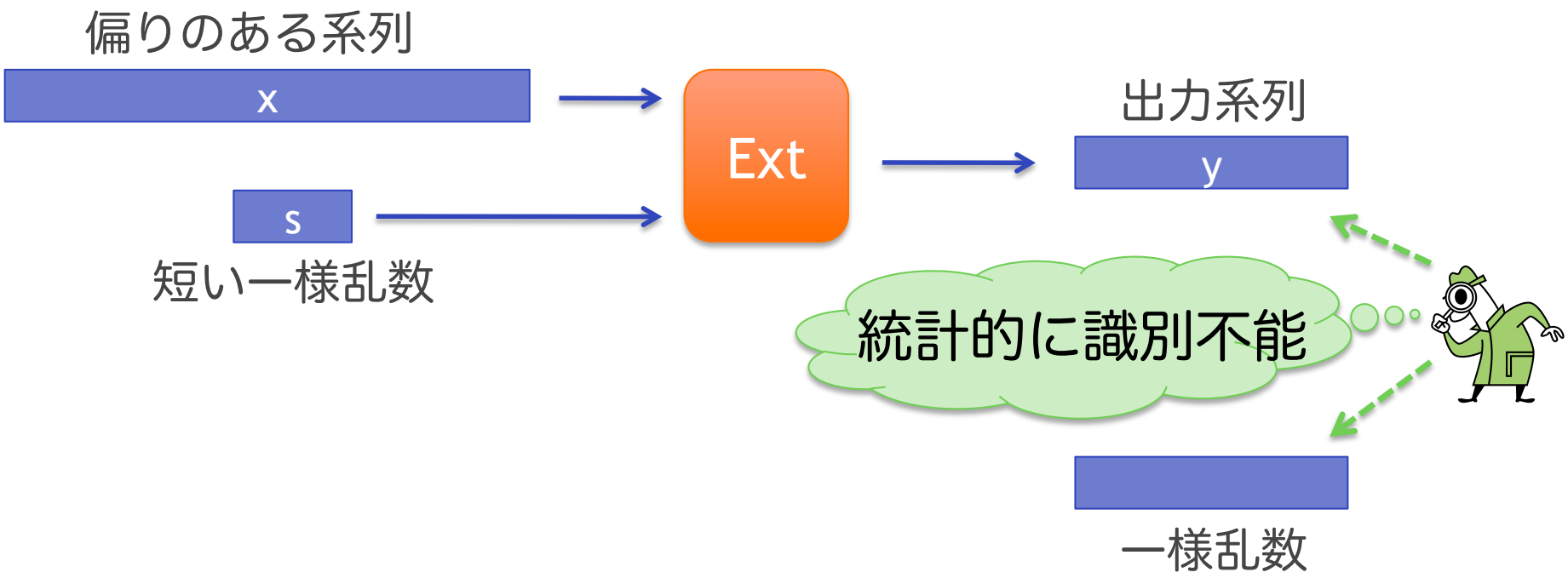
誤り訂正符号

- 誤りが発生しても訂正できるようにする



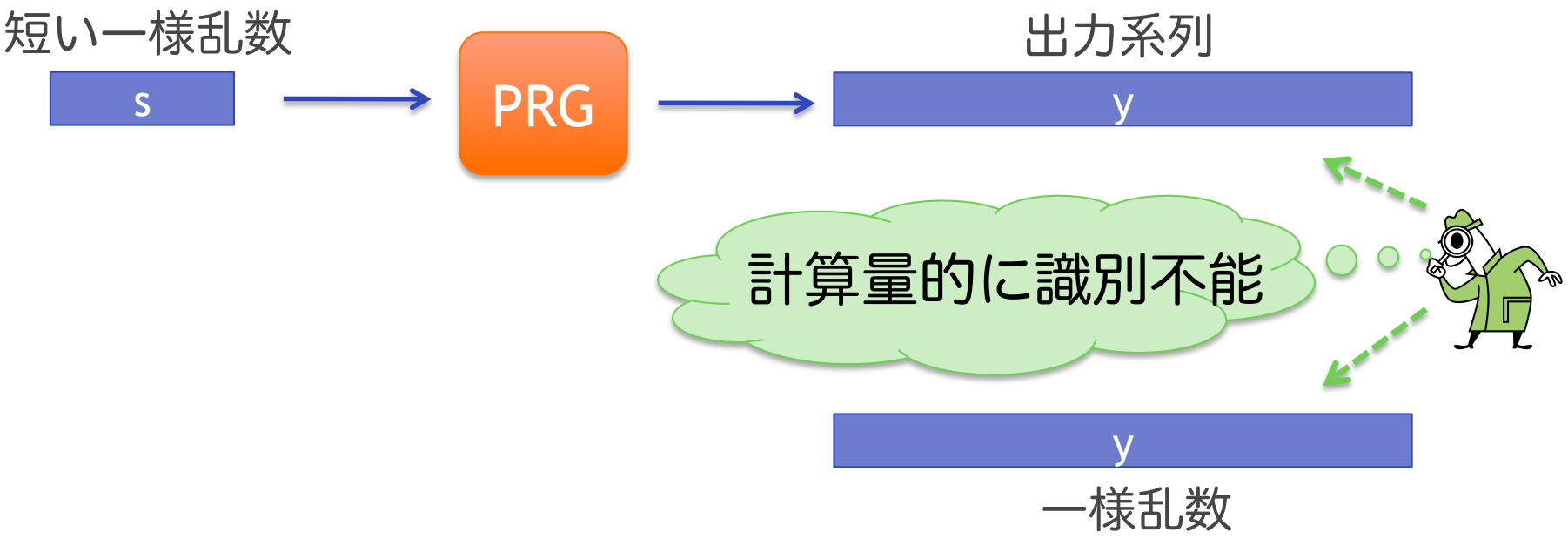
乱数抽出器

- 偏りのある分布から一様分布を取り出す



擬似乱数生成器

- 短い一様乱数から，長い擬似乱数系列を生成



３つの共通点は？

- 誤り訂正符号（符号理論）
- 乱数抽出器（情報理論）
- 擬似乱数生成器（計算量理論）

３つの共通点は？

- 誤り訂正符号（符号理論）
- 乱数抽出器（情報理論）
- 擬似乱数生成器（計算量理論）

➡ 擬似ランダムオブジェクトであること

擬似ランダムオブジェクト

- ランダムに構成すると，
  高い確率で，性能のよいものが得られる
- ランダムネスを（なるべく）使わない，
  明示的構成法を示すことが目標

擬似ランダムオブジェクト

- ランダムに構成すると，
  高い確率で，性能のよいものが得られる
- ランダムネスを（なるべく）使わない，
  明示的構成法を示すことが目標

それだけなのか？

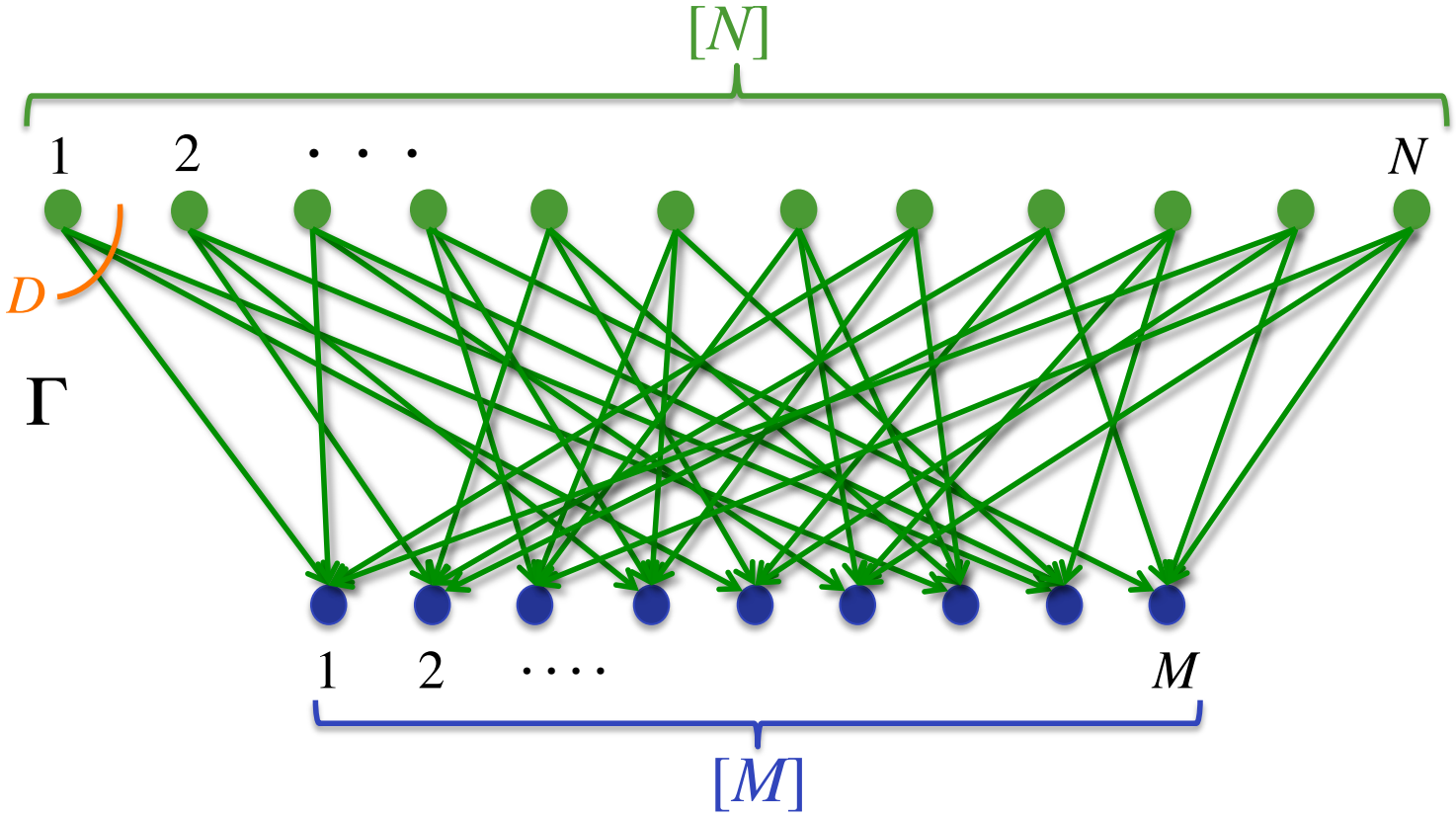
Vadhan の考察

- 擬似ランダムオブジェクトを
  統一的に説明できる枠組みが存在
  - Vadhan,“The unified theory of pseudorandomness”
- 擬似ランダムオブジェクト
  - リスト復号可能符号（符号理論）
  - 乱数抽出器（情報理論）
  - 擬似乱数生成器（計算量理論）
  - エクスパンダグラフ（グラフ理論）
  - 困難性増幅器（計算量理論）

  など

統一的枠組み

関数 $\Gamma : [N] \times [D] \to [M]$　　$[n] = \{1, 2, \ldots, n\}$

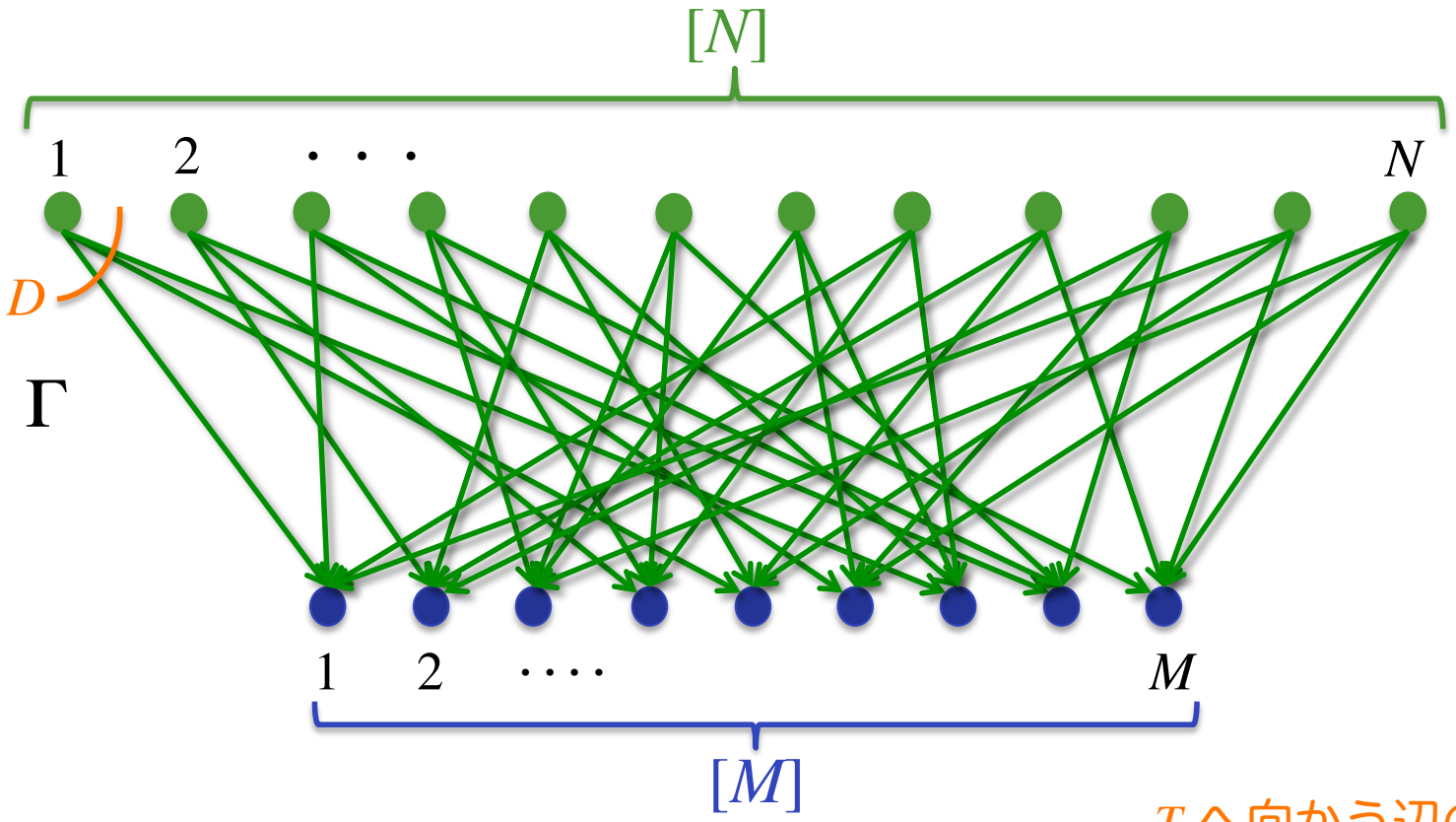


集合 $T \subseteq [M]$ と一致パラメータ $\varepsilon > 0$ に対して,

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

統一的枠組み

関数 $\Gamma : [N] \times [D] \to [M]$　　$[n] = \{1, 2, \ldots, n\}$



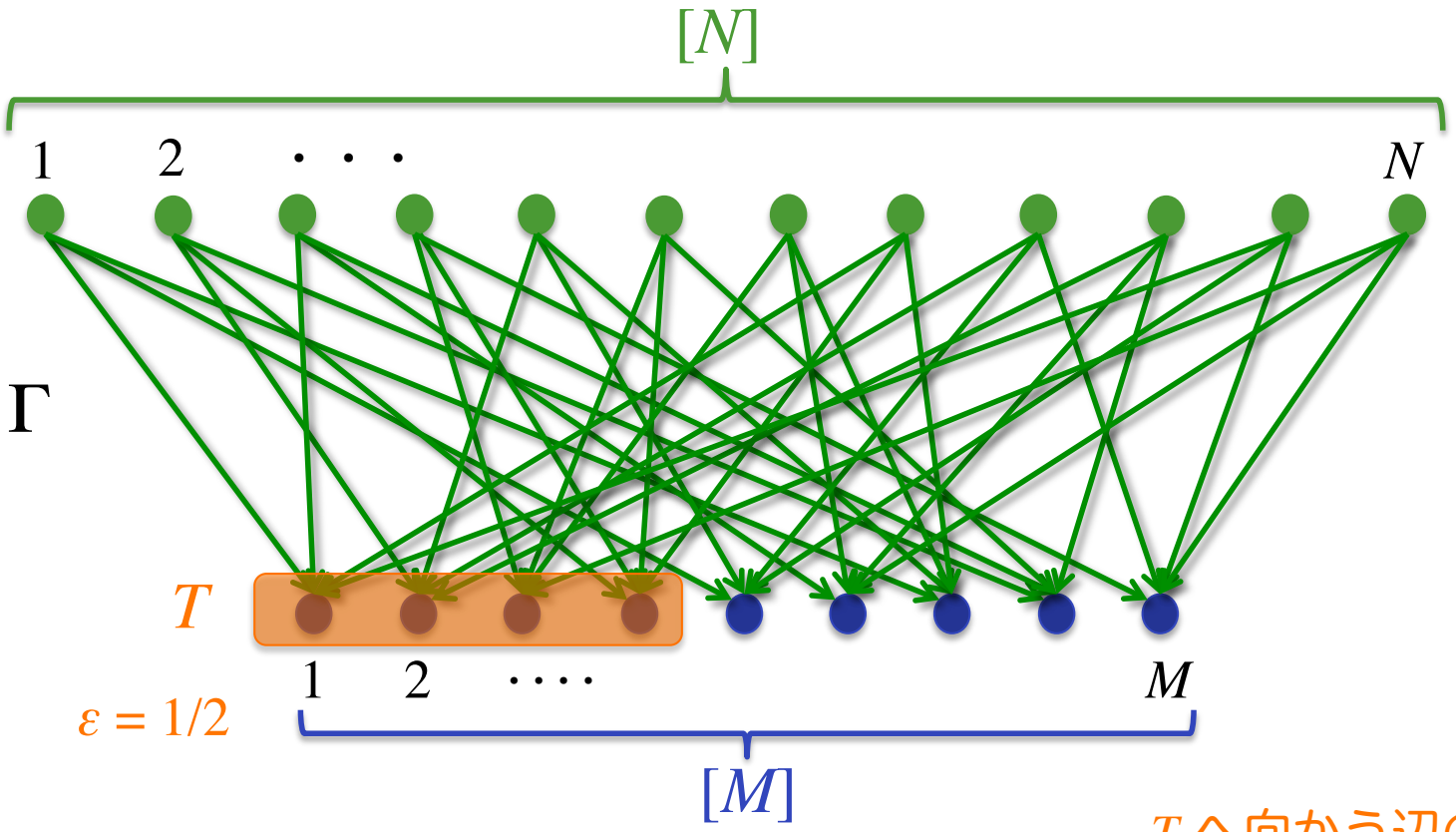
集合 $T \subseteq [M]$ と一致パラメータ $\varepsilon > 0$ に対して,

T へ向かう辺の割合が
ε より大きい x の集合

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

統一的枠組み

関数 $\Gamma : [N] \times [D] \to [M]$　　$[n] = \{1, 2, \ldots, n\}$



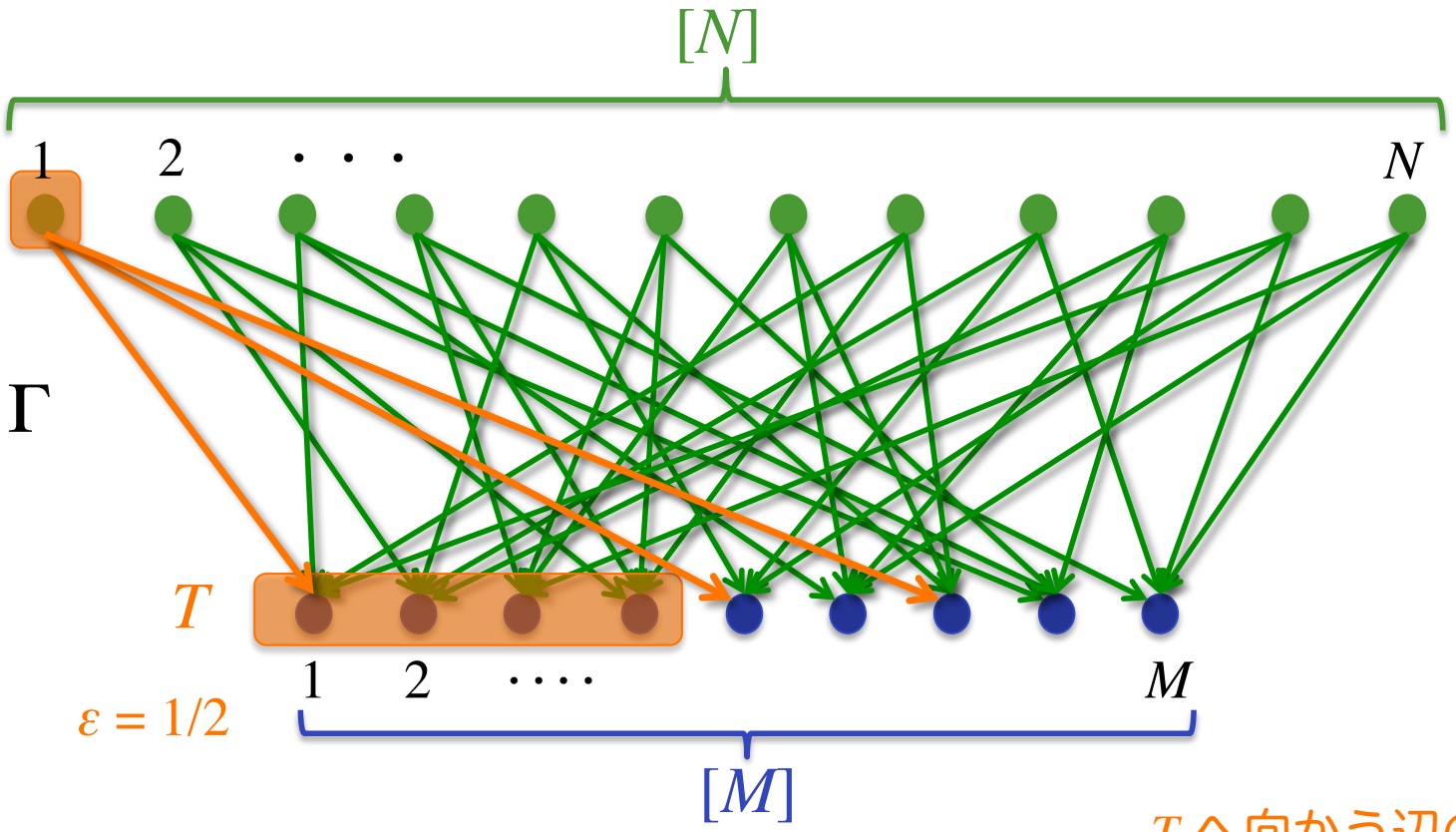
集合 $T \subseteq [M]$ と一致パラメータ $\varepsilon > 0$ に対して,

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

T へ向かう辺の割合が
ε より大きい x の集合

統一的枠組み

関数 $\Gamma : [N] \times [D] \to [M]$　　$[n] = \{1, 2, \ldots, n\}$



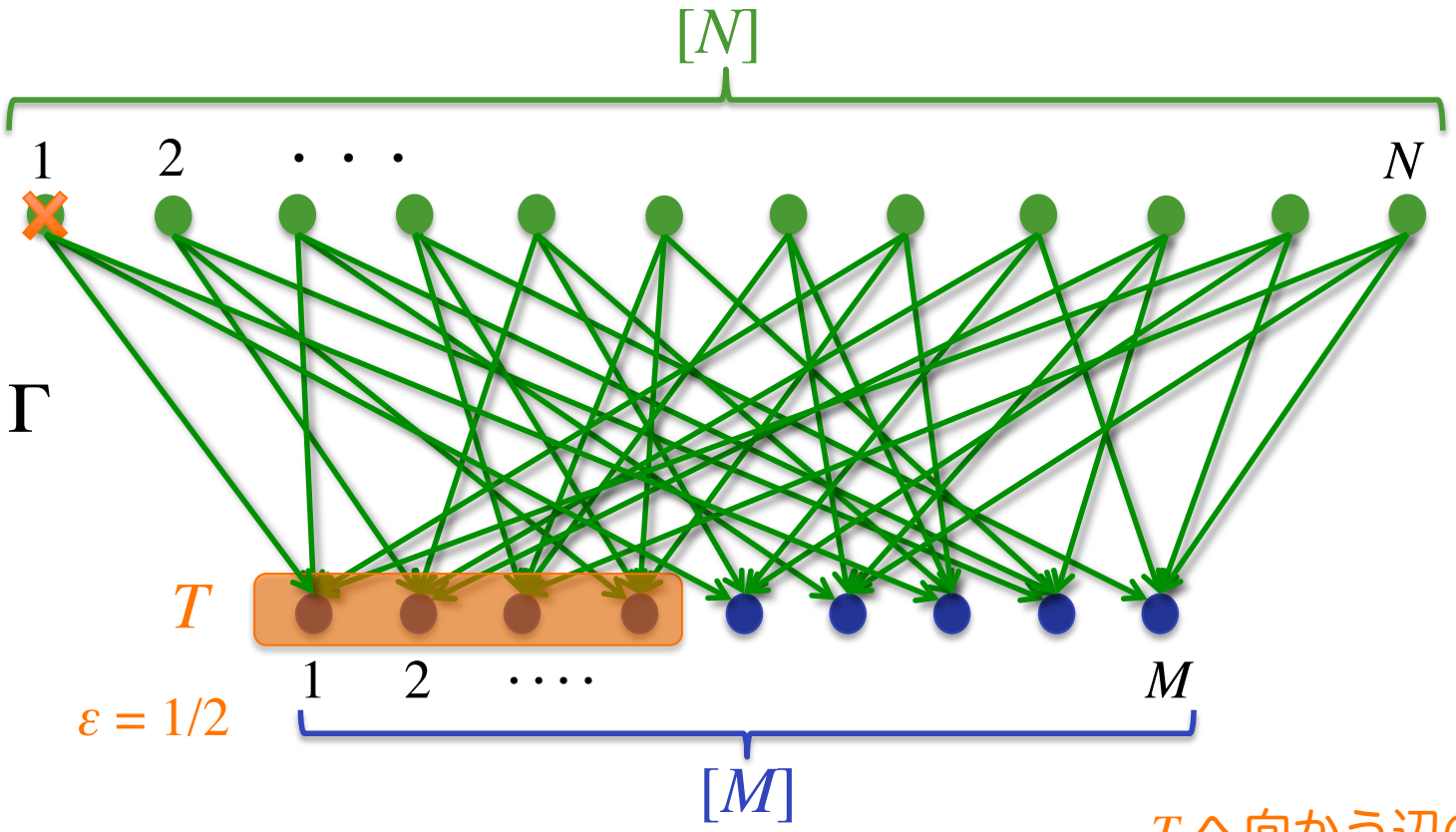
T へ向かう辺の割合が
ε より大きい x の集合

集合 $T \subseteq [M]$ と一致パラメータ $\varepsilon > 0$ に対して,

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

統一的枠組み

関数 $\Gamma : [N] \times [D] \to [M]$　　$[n] = \{1, 2, \ldots, n\}$



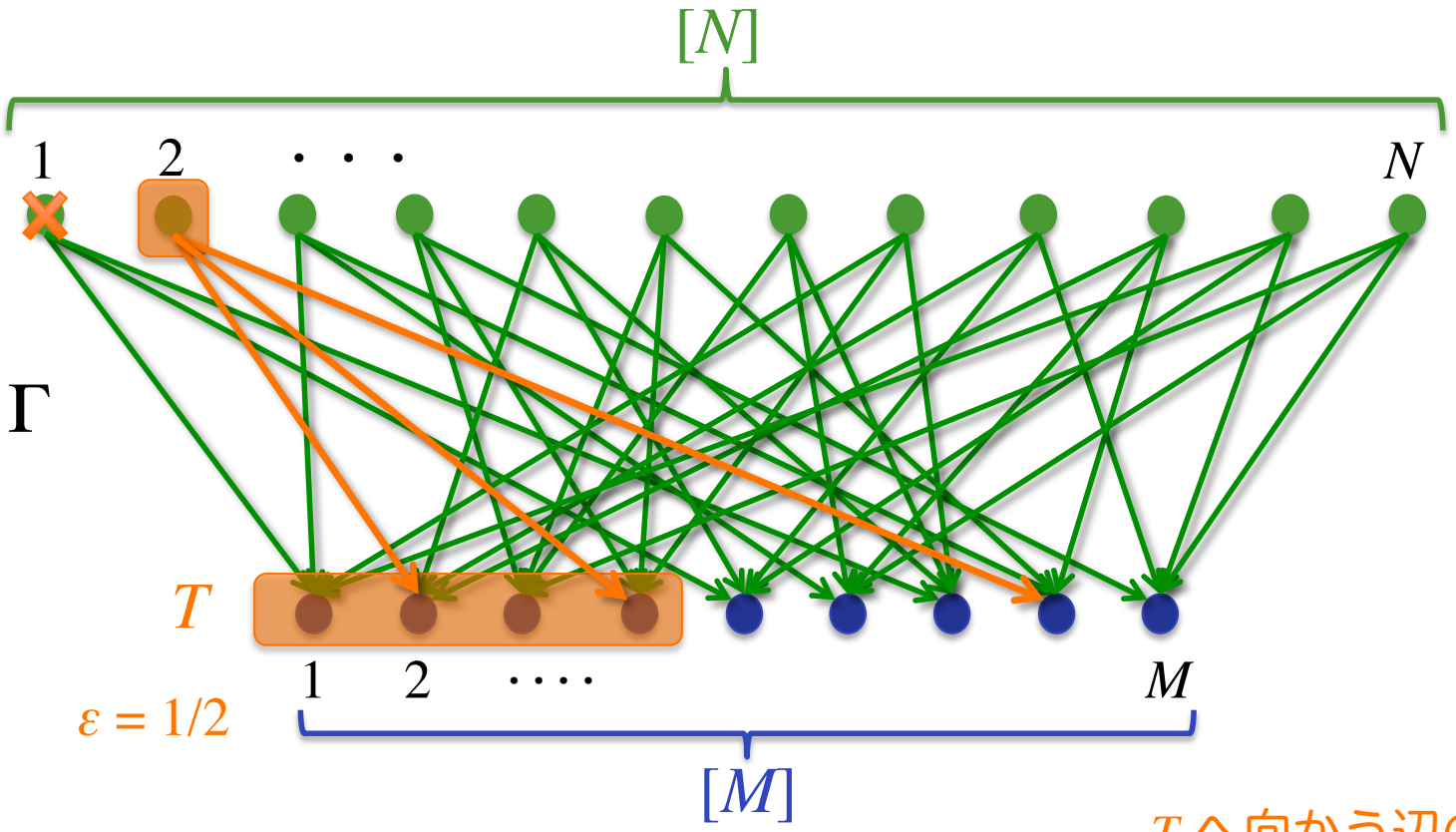
T へ向かう辺の割合が
ε より大きい x の集合

集合 $T \subseteq [M]$ と一致パラメータ $\varepsilon > 0$ に対して,

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

統一的枠組み

関数 $\Gamma : [N] \times [D] \to [M]$　　$[n] = \{1, 2, \ldots, n\}$



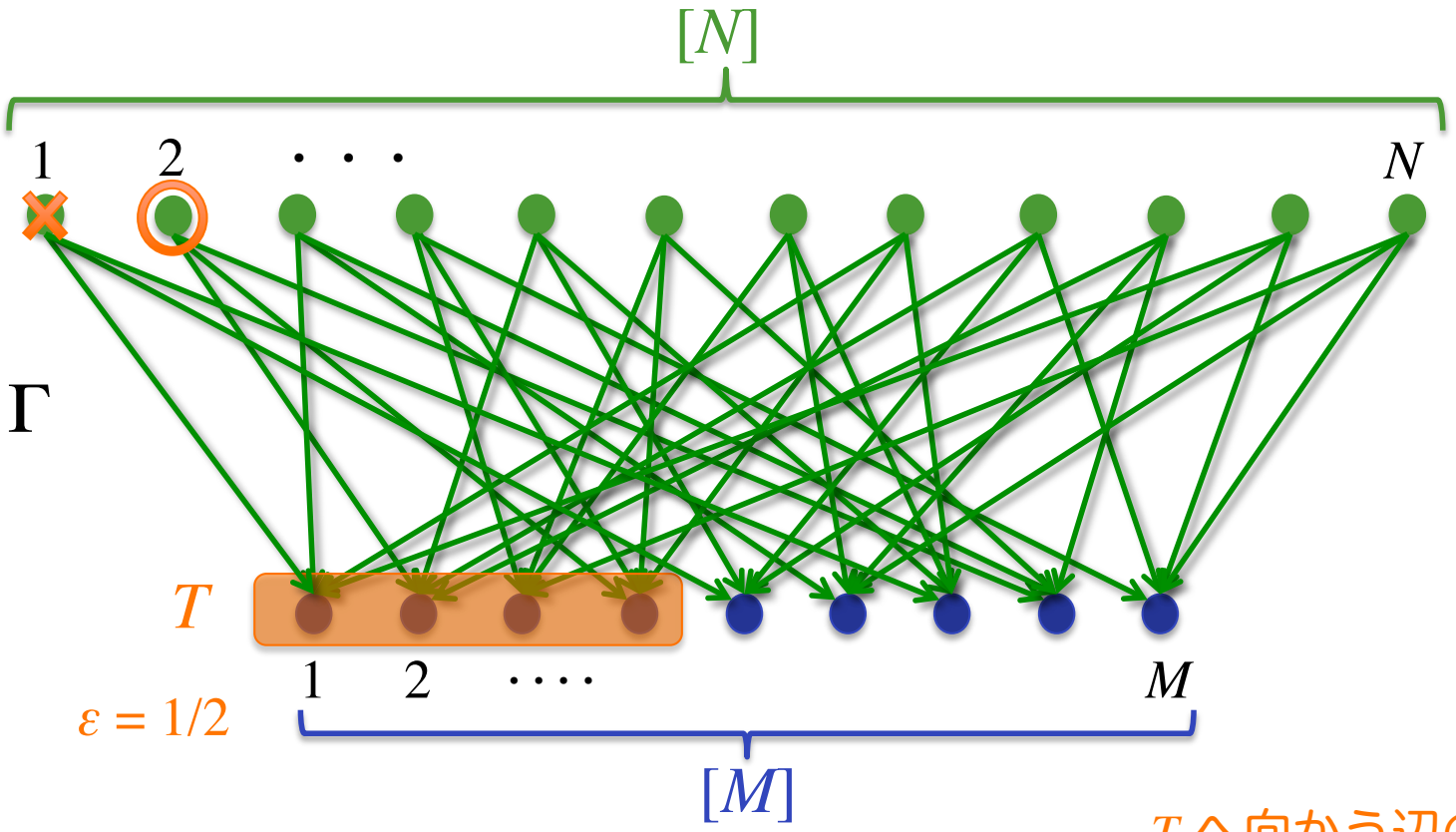
T へ向かう辺の割合が
ε より大きい x の集合

集合 $T \subseteq [M]$ と一致パラメータ $\varepsilon > 0$ に対して,

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

統一的枠組み

関数 $\Gamma : [N] \times [D] \to [M]$　　$[n] = \{1, 2, \ldots, n\}$



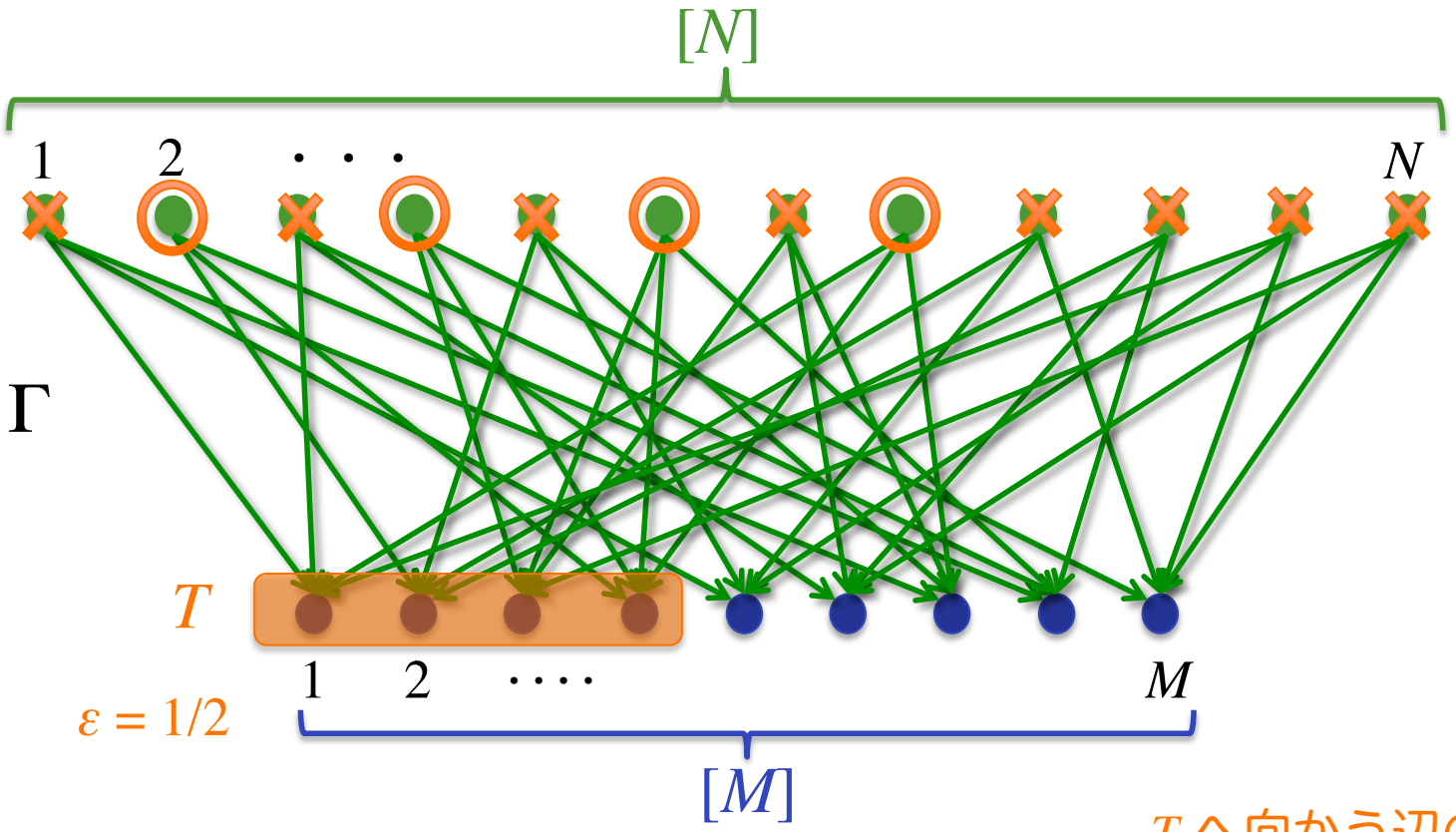
T へ向かう辺の割合が
ε より大きい x の集合

集合 $T \subseteq [M]$ と一致パラメータ $\varepsilon > 0$ に対して,

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

統一的枠組み

関数 $\Gamma : [N] \times [D] \to [M]$　　$[n] = \{1, 2, \ldots, n\}$



集合 $T \subseteq [M]$ と一致パラメータ $\varepsilon > 0$ 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

擬似ランダムオブジェクトの統一的記述

- 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,

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

  という条件によって，オブジェクトを特徴づけ可能

誤り訂正符号の定義

符号 $C \subseteq [q]^D, |C| = N$

$\Leftrightarrow$ 符号化関数 $\mathrm{Enc} : [N] \to [q]^D$

$\Leftrightarrow$ 関数 $\Gamma : [N] \times [D] \to [D] \times [q]$

$$\Gamma(x, y) = (y, \mathrm{Enc}(x)_y)$$

例. $q = 3, D = 3, C = \{111, 222, 333\}$

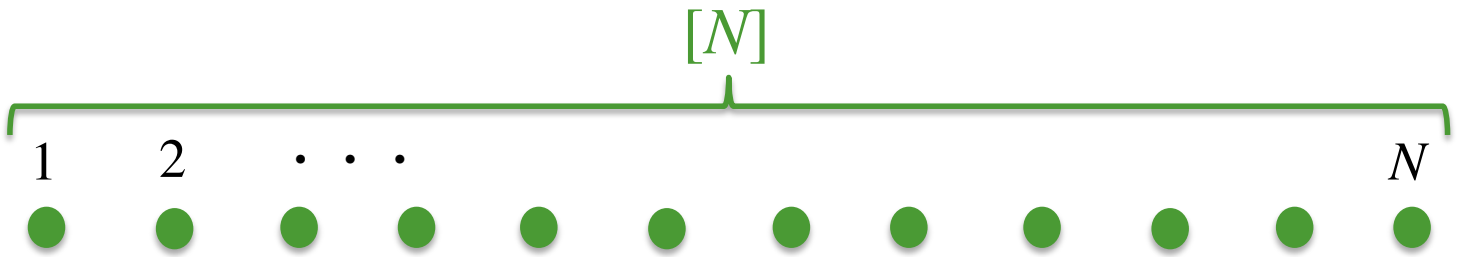
$\Leftrightarrow$ $\mathrm{Enc}(1) = 111, \quad \mathrm{Enc}(2) = 222, \quad \mathrm{Enc}(3) = 333$

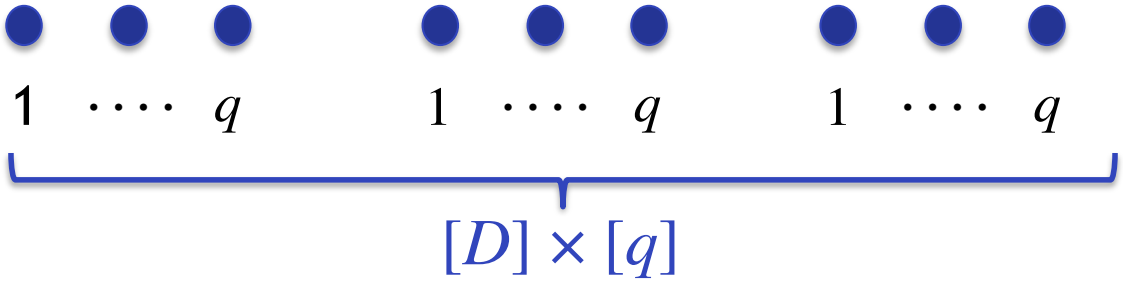
$\Leftrightarrow$ $\Gamma(1,1) = (1,1), \Gamma(1,2) = (2,1), \Gamma(1,3) = (3,1),$

$\Gamma(2,1) = (1,2), \Gamma(2,2) = (2,2), \Gamma(2,3) = (3,2),$

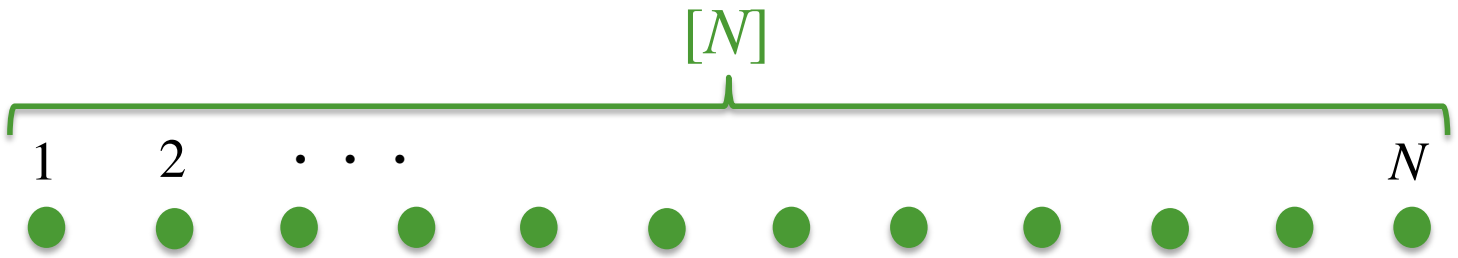
$\Gamma(3,1) = (1,3), \Gamma(3,2) = (2,3), \Gamma(3,3) = (3,3)$

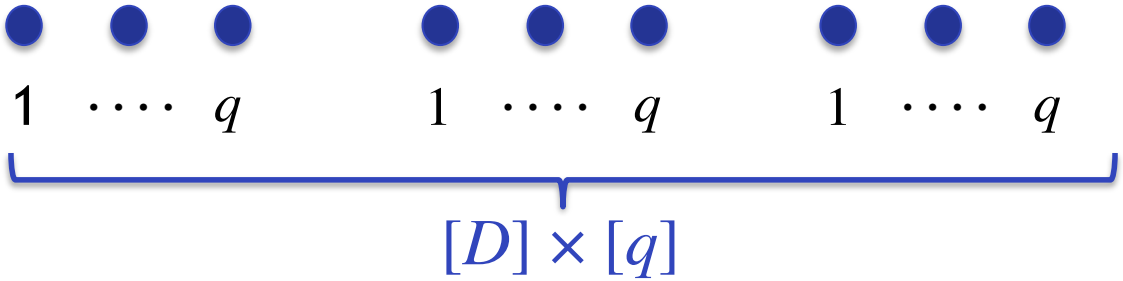
関数 $\Gamma : [N] \times [D] \to [D] \times [q],\ \Gamma(x, y) = (y, \mathrm{Enc}(x)_y)$





関数 $\Gamma : [N] \times [D] \to [D] \times [q],\ \Gamma(x, y) = (y, \mathrm{Enc}(x)_y)$

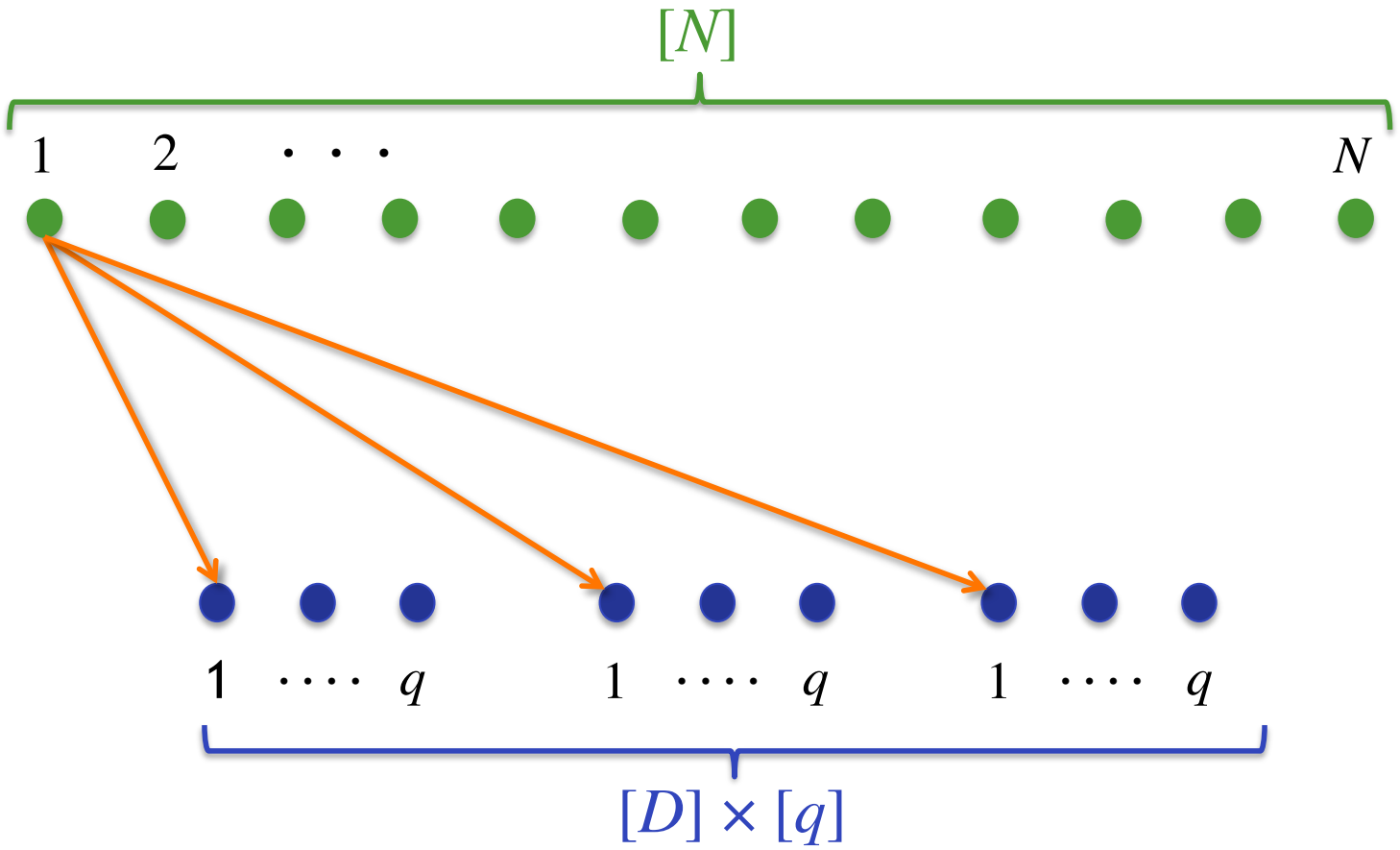




例. $\mathrm{Enc}(1) = 111,\quad \mathrm{Enc}(2) = 222,\quad \mathrm{Enc}(3) = 333$

$\Leftrightarrow$ $\Gamma(1,1) = (1,1), \Gamma(1,2) = (2,1), \Gamma(1,3) = (3,1),$
$\Gamma(2,1) = (1,2), \Gamma(2,2) = (2,2), \Gamma(2,3) = (3,2),$
$\Gamma(3,1) = (1,3), \Gamma(3,2) = (2,3), \Gamma(3,3) = (3,3)$

関数 $\Gamma : [N] \times [D] \to [D] \times [q],\ \Gamma(x, y) = (y, \mathrm{Enc}(x)_y)$



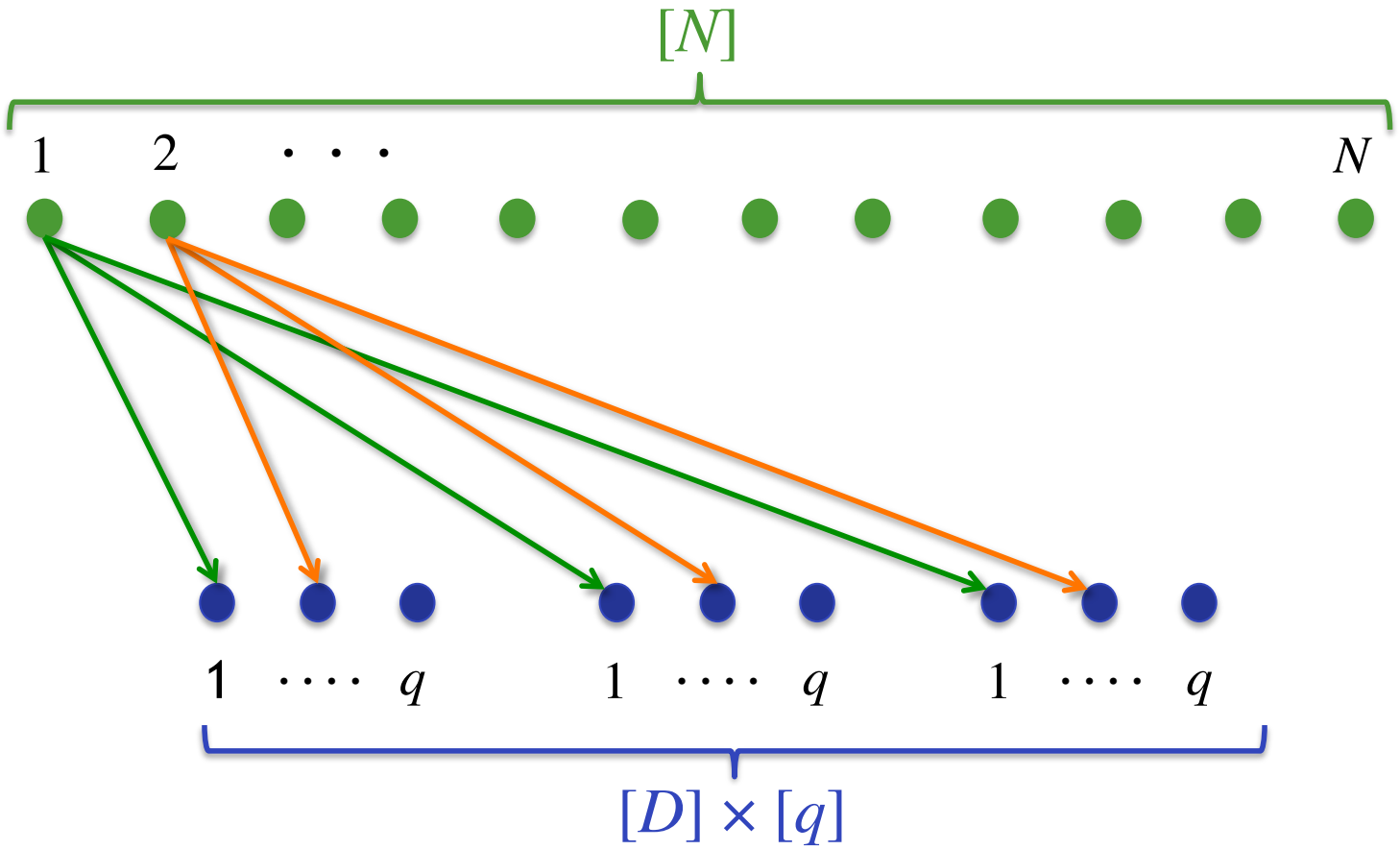
例. $\mathrm{Enc}(1) = 111,\quad \mathrm{Enc}(2) = 222,\quad \mathrm{Enc}(3) = 333$

$\Leftrightarrow$ $\Gamma(1,1) = (1,1), \Gamma(1,2) = (2,1), \Gamma(1,3) = (3,1),$

$\Gamma(2,1) = (1,2), \Gamma(2,2) = (2,2), \Gamma(2,3) = (3,2),$

$\Gamma(3,1) = (1,3), \Gamma(3,2) = (2,3), \Gamma(3,3) = (3,3)$

関数 $\Gamma : [N] \times [D] \to [D] \times [q],\ \Gamma(x, y) = (y, \mathrm{Enc}(x)_y)$



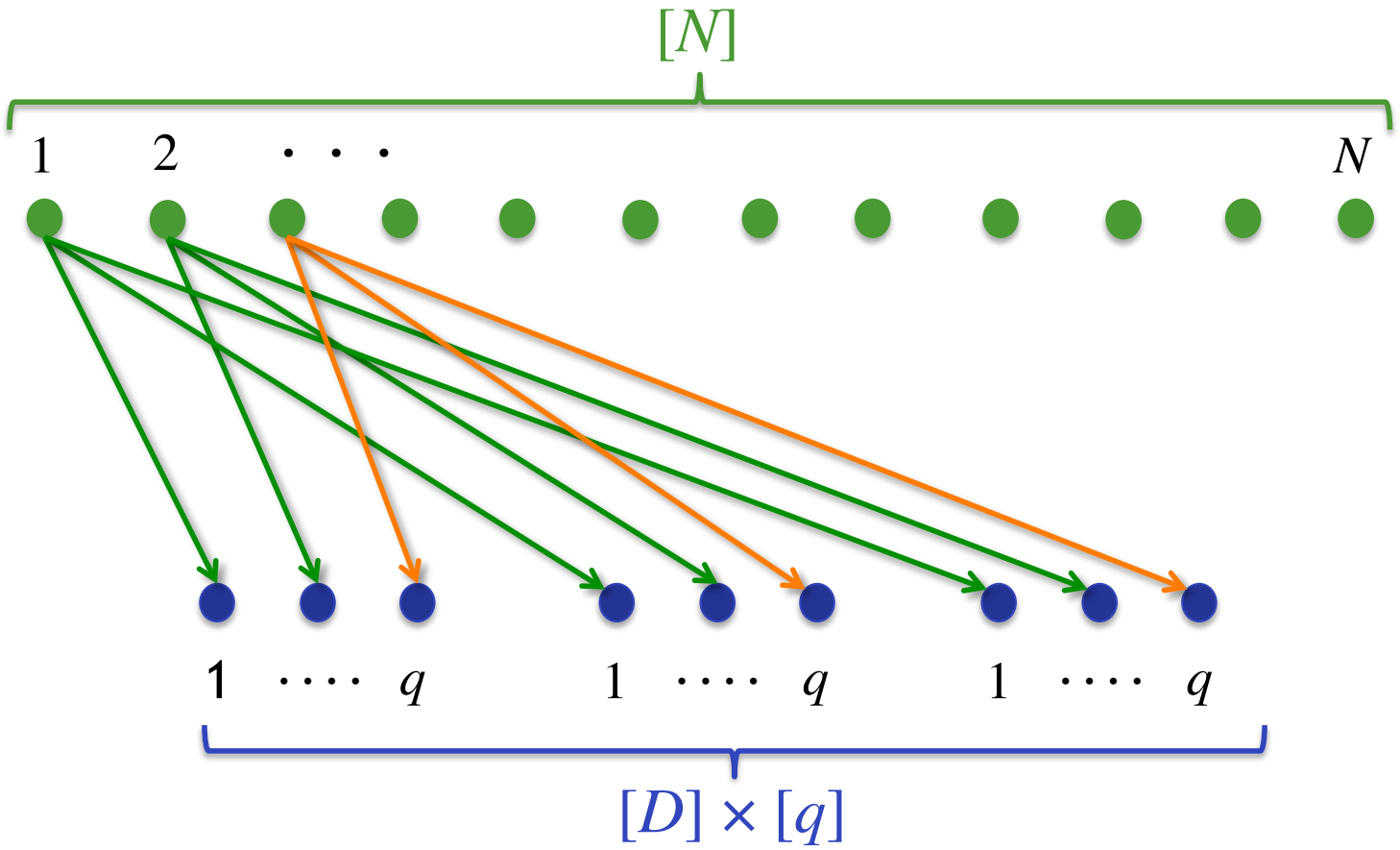
例. $\mathrm{Enc}(1) = 111,\quad \mathrm{Enc}(2) = 222,\quad \mathrm{Enc}(3) = 333$

$\Leftrightarrow$ $\Gamma(1,1) = (1,1), \Gamma(1,2) = (2,1), \Gamma(1,3) = (3,1),$

$\Gamma(2,1) = (1,2), \Gamma(2,2) = (2,2), \Gamma(2,3) = (3,2),$

$\Gamma(3,1) = (1,3), \Gamma(3,2) = (2,3), \Gamma(3,3) = (3,3)$

関数 $\Gamma : [N] \times [D] \to [D] \times [q],\ \Gamma(x, y) = (y, \mathrm{Enc}(x)_y)$



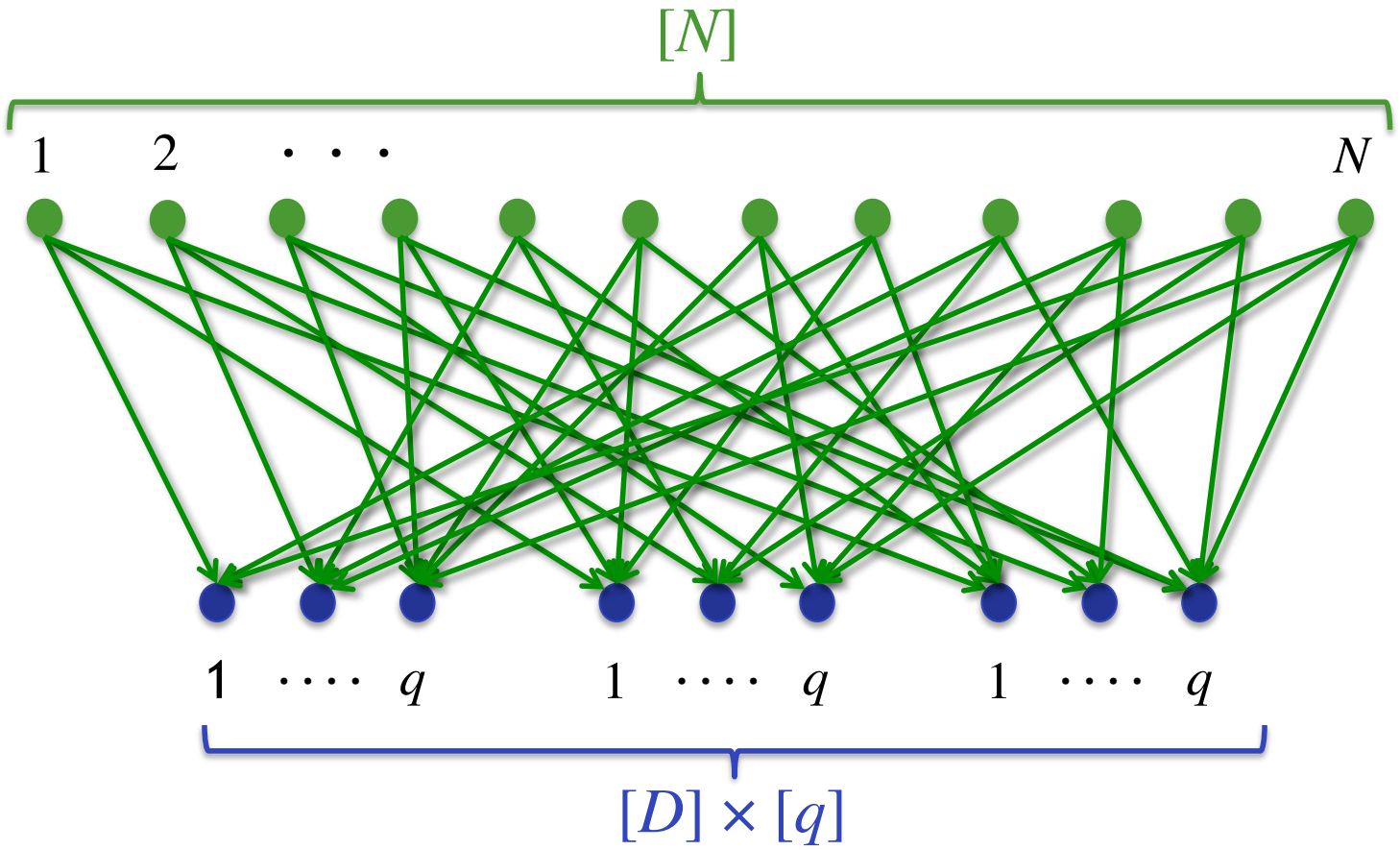
例. $\mathrm{Enc}(1) = 111,\quad \mathrm{Enc}(2) = 222,\quad \mathrm{Enc}(3) = 333$

$\Leftrightarrow$ $\Gamma(1,1) = (1,1), \Gamma(1,2) = (2,1), \Gamma(1,3) = (3,1),$

$\Gamma(2,1) = (1,2), \Gamma(2,2) = (2,2), \Gamma(2,3) = (3,2),$

$\Gamma(3,1) = (1,3), \Gamma(3,2) = (2,3), \Gamma(3,3) = (3,3)$

関数 $\Gamma : [N] \times [D] \to [D] \times [q],\ \Gamma(x, y) = (y, \mathrm{Enc}(x)_y)$



リスト復号可能符号の定義

定義

符号 $\mathrm{Enc}:[N]\to[q]^D$ が (ε, K) リスト復号可能

⟺ 任意の受信語 $r\in[q]^D$ に対して，
r と $1/q+\varepsilon$ 以上の割合が一致するような
$\mathrm{Enc}(x), x\in[N]$ の数が K 以下

目標

- D → 小さく（ $D=\mathrm{O}(n), n=\log N$ ）
- ε → 小さく（ $\varepsilon=\mathrm{O}(1)$ ）
- q → 小さく（ $q=\mathrm{O}(1)$ or $\mathrm{poly}(n)$ ）
- K → 小さく（ $K=\mathrm{poly}(n)$ ）

リスト復号可能符号の統一的記述

命題

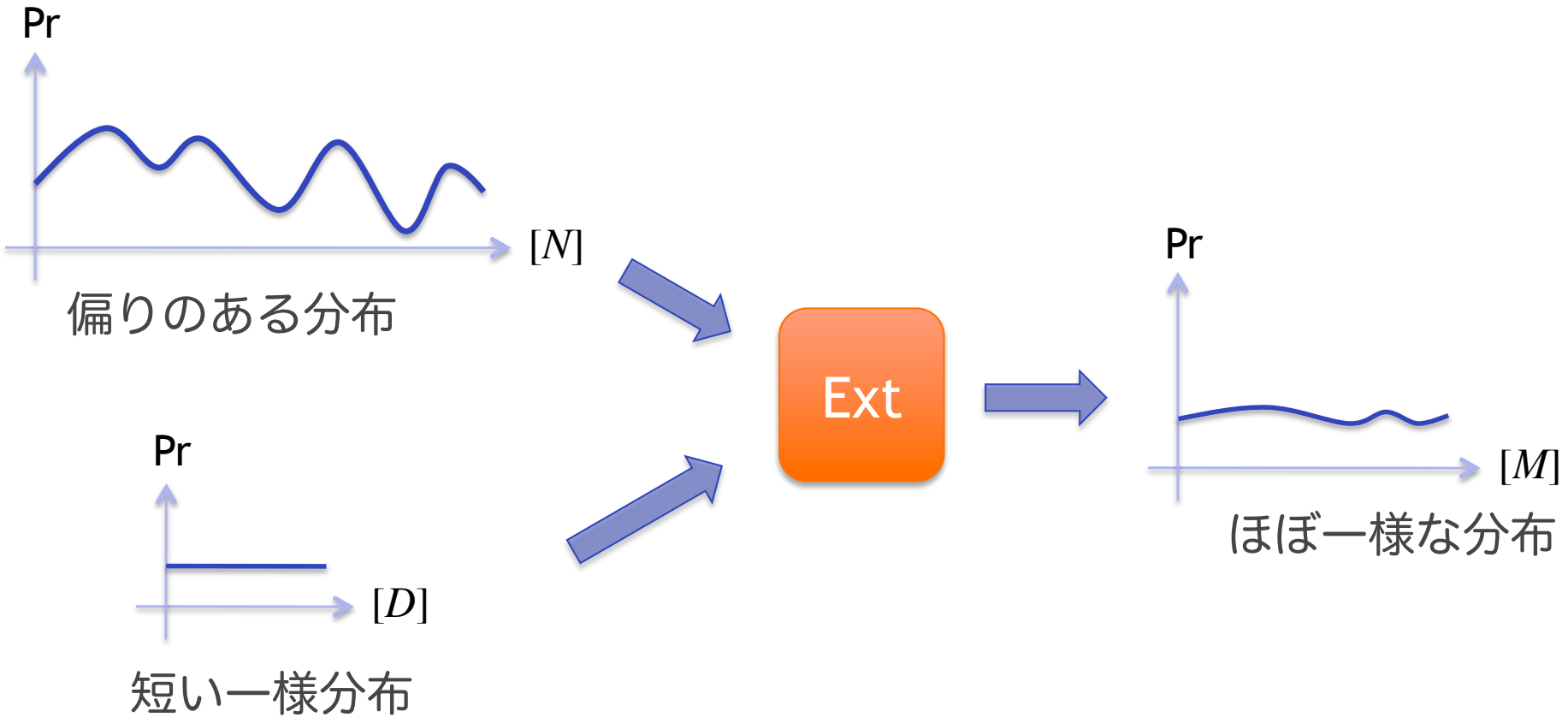
関数 $\Gamma : [N] \times [D] \to [D] \times [q]$ で定義される符号が
(ε, K) リスト復号可能であるための必要十分条件は

$$\forall r \in [q]^D, \quad \left| \mathrm{LIST}_\Gamma(T_r, 1/q + \varepsilon) \right| \leq K$$

ただし，$T_r = \{(y, r_y) : y \in [D]\}$

乱数抽出器

乱数抽出器 $\mathrm{Ext} : [N] \times [D] \to [M]$



乱数抽出器の定義

定義

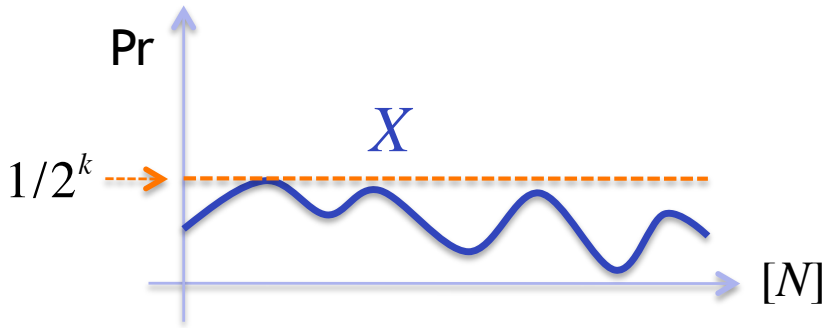
関数 $\mathrm{Ext}:[N]\times[D]\to[M]$ が (k,ε) 乱数抽出器

⇔ 最小エントロピー k 以上の任意の X に対して

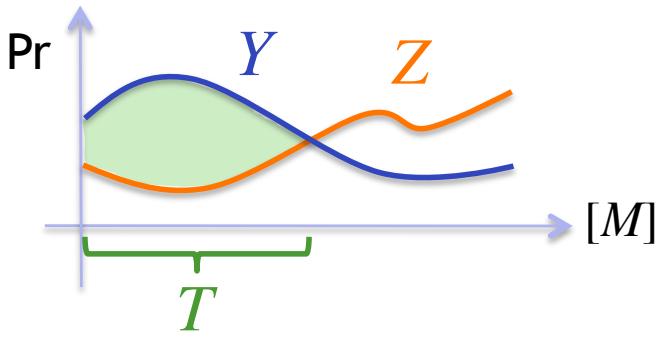
$$\Delta(\mathrm{Ext}(X,U_{[D]}),U_{[M]})\le\varepsilon$$

分布 X の
最小エントロピーが k

⇔



$$\Delta(Y,Z)=\max_{T\subseteq[M]}\left|\Pr[Y\in T]-\Pr[Z\in T]\right|$$



乱数抽出器の定義

定義

関数 $\mathrm{Ext} : [N] \times [D] \to [M]$ が (k, ε) 乱数抽出器

⟷ 最小エントロピー k 以上の任意の X に対して

$$\Delta(\mathrm{Ext}(X, U_{[D]}), U_{[M]}) \leq \varepsilon$$

目標

- $k = \alpha n$ or n^{α} （ $\alpha \in (0, 1)$ ）
- $d = \log D$ → 小さく（ $d = \mathrm{O}(\log n)$ or $\mathrm{polylog}(n)$ ）
- ε → 小さく（ $\varepsilon = \mathrm{O}(1)$ or $\mathrm{o}(1)$ ）
- $m = \log M$ → k（ $m \approx k + d$ が理想， $m = \Omega(k)$ or $k^{\Omega(1)}$ ）

乱数抽出器の統一的記述

命題

関数 $\Gamma = \mathrm{Ext} : [N] \times [D] \to [M]$, $K = 2^k$ とするとき,

1. Ext が (k, ε) 乱数抽出器であれば

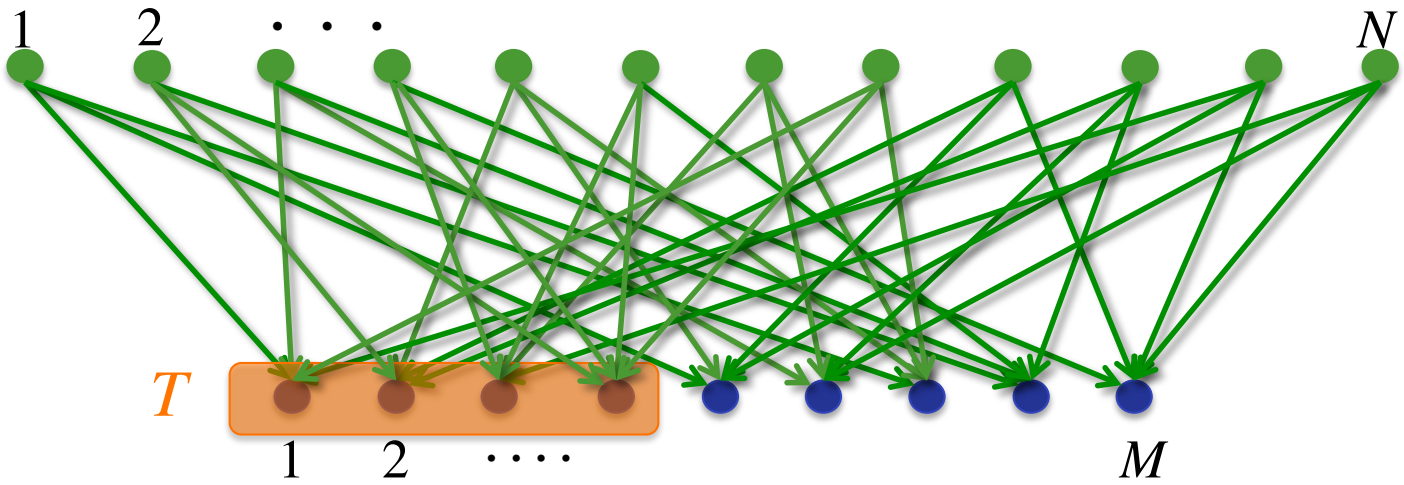
$$\forall T \subseteq [M], \quad \left| \mathrm{LIST}_\Gamma(T, |T|/M + \varepsilon) \right| < K \qquad (1)$$

2. 逆に, (1) が成り立つとき,
   Ext は, $(k + \log(1/\varepsilon), 2\varepsilon)$ 乱数抽出器である

1. Ext が (k,ε) 乱数抽出器であれば

$$\forall T \subseteq [M],\quad \left|\mathrm{LIST}_{\Gamma}(T,|T|/M+\varepsilon)\right| < K \qquad (1)$$

証明:

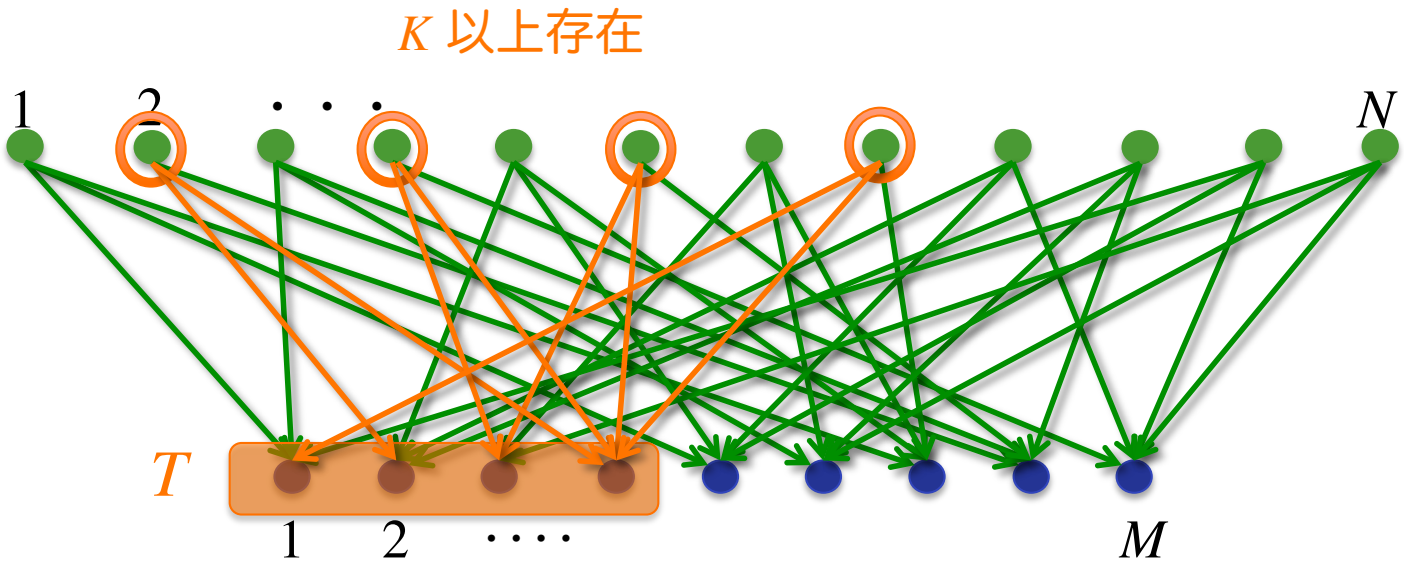


ある T が存在して, $\left|\mathrm{LIST}_{\Gamma}(T,|T|/M+\varepsilon)\right| \geq K$ だとする.

1. Ext が (k,ε) 乱数抽出器であれば

$$\forall T \subseteq [M],\quad \left|\mathrm{LIST}_{\Gamma}(T,|T|/M+\varepsilon)\right| < K \qquad (1)$$

証明:

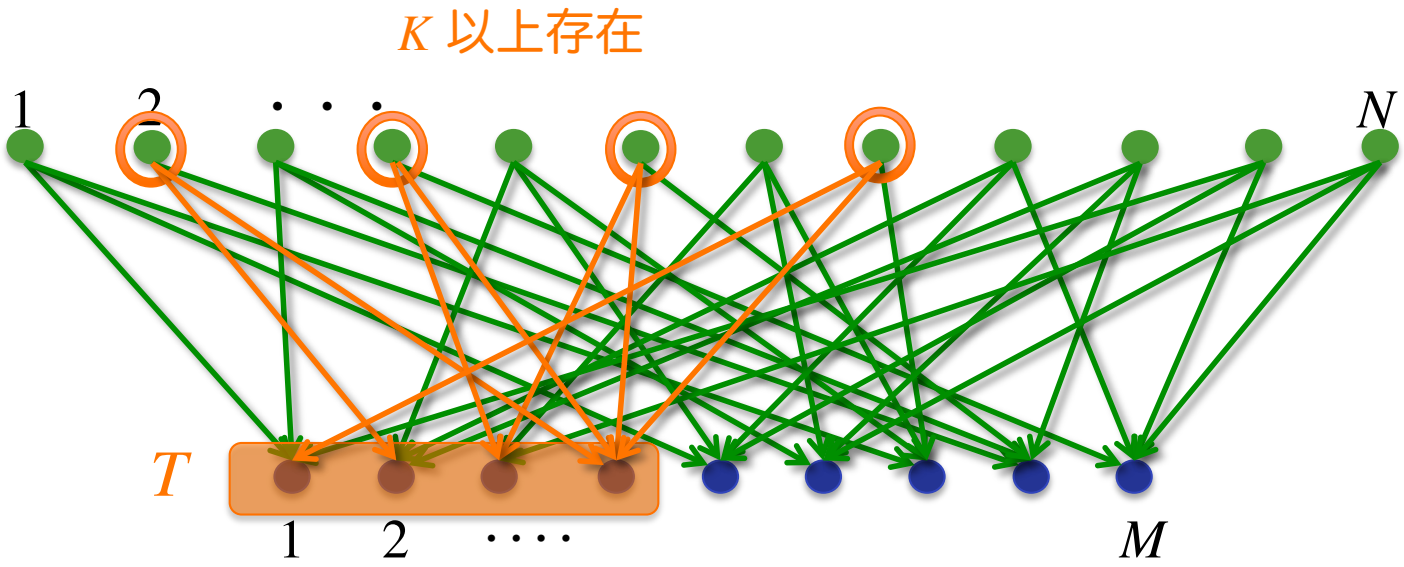


ある T が存在して, $\left|\mathrm{LIST}_{\Gamma}(T,|T|/M+\varepsilon)\right| \geq K$ だとする.

1. Ext が (k,ε) 乱数抽出器であれば

$$\forall T \subseteq [M],\quad \left|\mathrm{LIST}_{\Gamma}(T,|T|/M+\varepsilon)\right| < K \qquad (1)$$

証明:



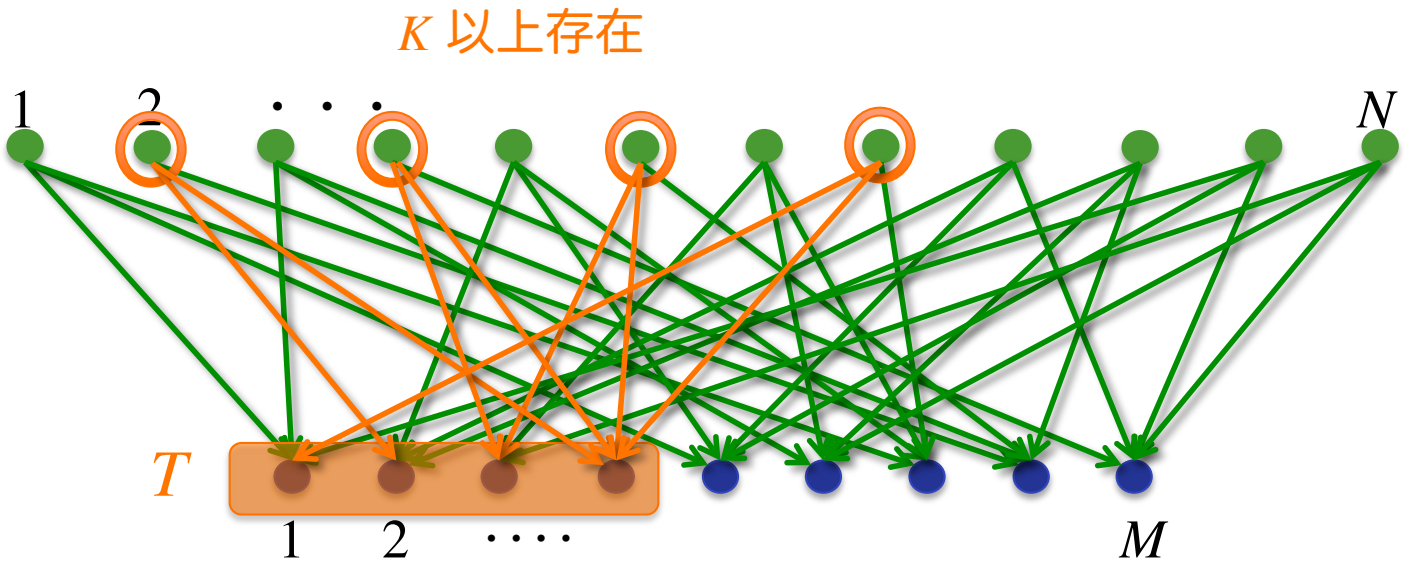
ある T が存在して, $\left|\mathrm{LIST}_{\Gamma}(T,|T|/M+\varepsilon)\right| \geq K$ だとする.

$\mathrm{LIST}_{\Gamma}(T,|T|/M+\varepsilon)$ 上の一様分布 X（ 最小エントロピー $\geq k$ ）を考える.

1. Ext が (k,ε) 乱数抽出器であれば

$$\forall T \subseteq [M],\quad \left|\mathrm{LIST}_{\Gamma}(T,|T|/M+\varepsilon)\right| < K \qquad (1)$$

証明:



ある T が存在して, $\left|\mathrm{LIST}_{\Gamma}(T,|T|/M+\varepsilon)\right| \geq K$ だとする.

$\mathrm{LIST}_{\Gamma}(T,|T|/M+\varepsilon)$ 上の一様分布 X（ 最小エントロピー $\geq k$ ）を考える.

すると，X は T へ，$|T|/M+\varepsilon$ 以上の割合が入ってくるので,
T へ入ってくる割合を見れば，一様分布と ε 以上の確率で識別可能 ■

比較

オブジェクト	リスト復号可能符号	乱数抽出器
関数 Γ	$\Gamma(x,y)=(y,\mathrm{Enc}(x)_y)$	$\Gamma(x,y)=\mathrm{Ext}(x,y)$
条件	$\forall r\in[q]^D$, $\left\|\mathrm{LIST}_\Gamma(T_r,1/q+\varepsilon)\right\|\le K$ $T_r=\{(y,r_y):y\in[D]\}$	$\forall T\subseteq[M]$, $\left\|\mathrm{LIST}_\Gamma(T,\left\|T\right\|/M+\varepsilon)\right\|<K$
パラメータ	$D=\mathrm{O}(n)$ $\varepsilon=\mathrm{O}(1)$ $K=\mathrm{poly}(n)$ $q=\mathrm{O}(1)$ or $\mathrm{poly}(n)$ $M=q\times D$ $=\mathrm{O}(n)$ or $\mathrm{poly}(n)$	$D=\mathrm{poly}(n)$ or $\mathrm{quasipoly}(n)$ $\varepsilon=\mathrm{O}(1)$ or $\mathrm{o}(1)$ $K=2\text{^}(\alpha n)$ or $2\text{^}(n^\alpha)$ $\alpha\in(0,1)$ $m=\Omega(k)$ or $k^{\Omega(1)}$ $M=2\text{^}(\mathrm{O}(n))$ or $2\text{^}(n^{\Omega(1)})$

Parvaresh-Vardy 符号にもとづく乱数抽出器

- Guruswami, Umans, Vadhan 2007
- 統一的記述を利用
- ほぼ最適な乱数抽出器を構成
  - 既存の構成法に比べて格段にシンプル
  - PV 符号は Reed-Solomon 符号の一般化

Guruswami, Umans, Vadhan 2007 の結果

定理

任意の定数 $\alpha, \varepsilon > 0$, 任意の整数 n, k に対し,
(k, ε) 乱数抽出器 $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$
の明示的構成法が存在.
ただし, $d \le \log n + \mathrm{O}(\log(k/\varepsilon)), m \ge (1-\alpha)k$

証明のアイディア

- エントロピーレートが高い場合（ $k/n = \mathrm{O}(1)$ ）,
  単純な構成でほぼ最適な乱数抽出器
  → 任意のエントロピーレートを扱うのが問題
- エントロピーレートを高くするもの → 濃縮器
- 最適な濃縮器を PV 符号から構成

証明の流れ

1. 関数 Γ を PV 符号で定義
   → 無損失エクスパンダグラフ

2. 無損失エクスパンダグラフ ≈ 無損失濃縮器

3. 無損失濃縮器 + 高エントロピーレート用乱数抽出器
   → ほぼ最適な乱数抽出器

証明の流れ

1. 関数 Γ を PV 符号で定義
   → 無損失エクスパンダグラフ

以下で簡単に説明

2. 無損失エクスパンダグラフ ≈ 無損失濃縮器

3. 無損失濃縮器 + 高エントロピーレート用乱数抽出器
   → ほぼ最適な乱数抽出器

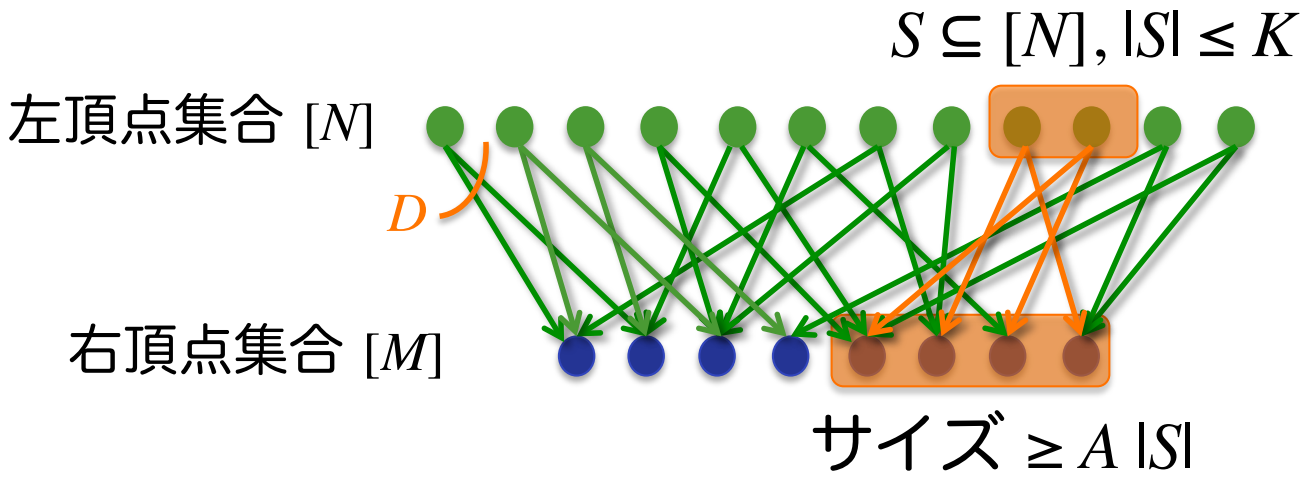
エクスパンダグラフの定義

定義

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

⟷ サイズ K 以下の任意の左頂点集合 $S \subseteq [N]$ は，隣接頂点集合のサイズが $A|S|$ 以上

$A = (1 - \varepsilon) D$ のとき，無損失エクスパンダ



PV 符号と RS 符号

符号	Reed-Solomon	Parvaresh-Vardy
メッセージ	$f \in \mathbf{F}_q[Y]$	$f \in \mathbf{F}_q[Y]$
符号語	$\{f(y)\}_{y \in \mathbf{F}_q}$	$\{f_0(y), f_1(y), \ldots, f_{m-1}(y)\}_{y \in \mathbf{F}_q}$ $\in \mathbf{F}_q^m$ とみなす ただし $f_0 = f$ $f_i(y) = f(Y)^{h^i} \bmod E(y)$ $E(y)$ は n 次既約多項式

リスト復号の証明

r：受信語

$\mathrm{LIST}(r,\varepsilon)$： r とε 以上の割合が一致する符号語集合

符号	Reed-Solomon	Parvaresh-Vardy
Step 1. ある非零多項式が存在	$\exists Q(Y,Z)\neq 0$ $\text{s.t.}\,\forall y\in \mathbf{F}_q, Q(y,r(y))=0$	$\exists Q(Y,Z_0,\cdots,Z_{m-1})\neq 0$ $\text{s.t.}\,\forall y\in \mathbf{F}_q, Q(y,r(y))=0$
理由	$\deg(Q(Y,Z))$ $=(d_Y+1)(d_Z+1)>q$	$\deg(Q(Y,Z_0,\cdots,Z_{m-1}))$ $=d_Y\cdot h^m>q$
Step 2. $f\in\mathrm{LIST}$ が多項式の根	$\forall f\in\mathrm{LIST}(r,\varepsilon),$ $Q(Y,f(Y))=0$	$Q^*(Z)=Q(Y,Z,Z^h,\cdots,Z^{h^{m-1}})\bmod E(y)$ $\forall f\in\mathrm{LIST}(r,\varepsilon),\ Q^*(f(Y))=0$
理由	$\deg(Q(Y,f(Y)))$ $\le d_Y+d_Z<\varepsilon q$	$\deg(Q(Y,f_0(Y),\cdots,f_{m-1}(Y)))$ $\le d_Y+(h-1)dm<\varepsilon q$
Step 3. リストサイズ	$\lvert\mathrm{LIST}(r,\varepsilon)\rvert$ $\le \deg_Z(Q(Y,Z))\le d_Z$	$\lvert\mathrm{LIST}(r,\varepsilon)\rvert\le \deg_Z(Q^*(Z))\le h^m$

リスト復号の証明をエクスパンダの証明へ

- 統一的記述におけるギャップ

オブジェクト	リスト復号可能符号	エクスパンダグラフ
関数 Γ	$\Gamma(x,y)=(y,\mathrm{Enc}(x)_y)$	$\Gamma(x,y)=$ “頂点 x の y 番目の隣接頂点”
条件	$\forall r\in[q]^D,$ $\left\|\mathrm{LIST}_\Gamma(T_r,1/q+\varepsilon)\right\|\le K$ $T_r=\{(y,r_y):y\in[D]\}$	$\forall K'\le K,$ $\forall T\subseteq[M]\ \text{s.t.}\ \left\|T\right\|<AK'$ $\left\|\mathrm{LIST}_\Gamma(T,1)\right\|<K'$

リスト復号の証明をエクスパンダの証明へ

- 統一的記述におけるギャップ

オブジェクト	リスト復号可能符号	エクスパンダグラフ
関数 Γ	$\Gamma(x,y)=(y,\mathrm{Enc}(x)_y)$	$\Gamma(x,y)=$ “頂点 x の y 番目の隣接頂点”
条件	$\forall r\in[q]^D,$ $\left\lvert\mathrm{LIST}_\Gamma(T_r,1/q+\varepsilon)\right\rvert\le K$ $T_r=\{(y,r_y):y\in[D]\}$	$\forall K'\le K,$ $\forall T\subseteq[M]\ \text{s.t.}\ \lvert T\rvert<AK'$ $\left\lvert\mathrm{LIST}_\Gamma(T,1)\right\rvert<K'$
	この形をした T に対して	あるサイズ以下の T に対して

リスト復号の証明をエクスパンダの証明へ

- 統一的記述におけるギャップ

オブジェクト	リスト復号可能符号	エクスパンダグラフ
関数 Γ	$\Gamma(x,y)=(y,\mathrm{Enc}(x)_y)$	$\Gamma(x,y)=$ “頂点 x の y 番目の隣接頂点”
条件	$\forall r\in[q]^D,$ $\left\lvert \mathrm{LIST}_\Gamma(T_r,1/q+\varepsilon)\right\rvert \le K$ $T_r=\{(y,r_y):y\in[D]\}$	$\forall K'\le K,$ $\forall T\subseteq[M]\ \text{s.t.}\ \lvert T\rvert < AK'$ $\left\lvert \mathrm{LIST}_\Gamma(T,1)\right\rvert < K'$
	この形をした T に対して	あるサイズ以下の T に対して

➡ PV 符号はエクスパンダグラフの条件も同様に証明可能

まとめ

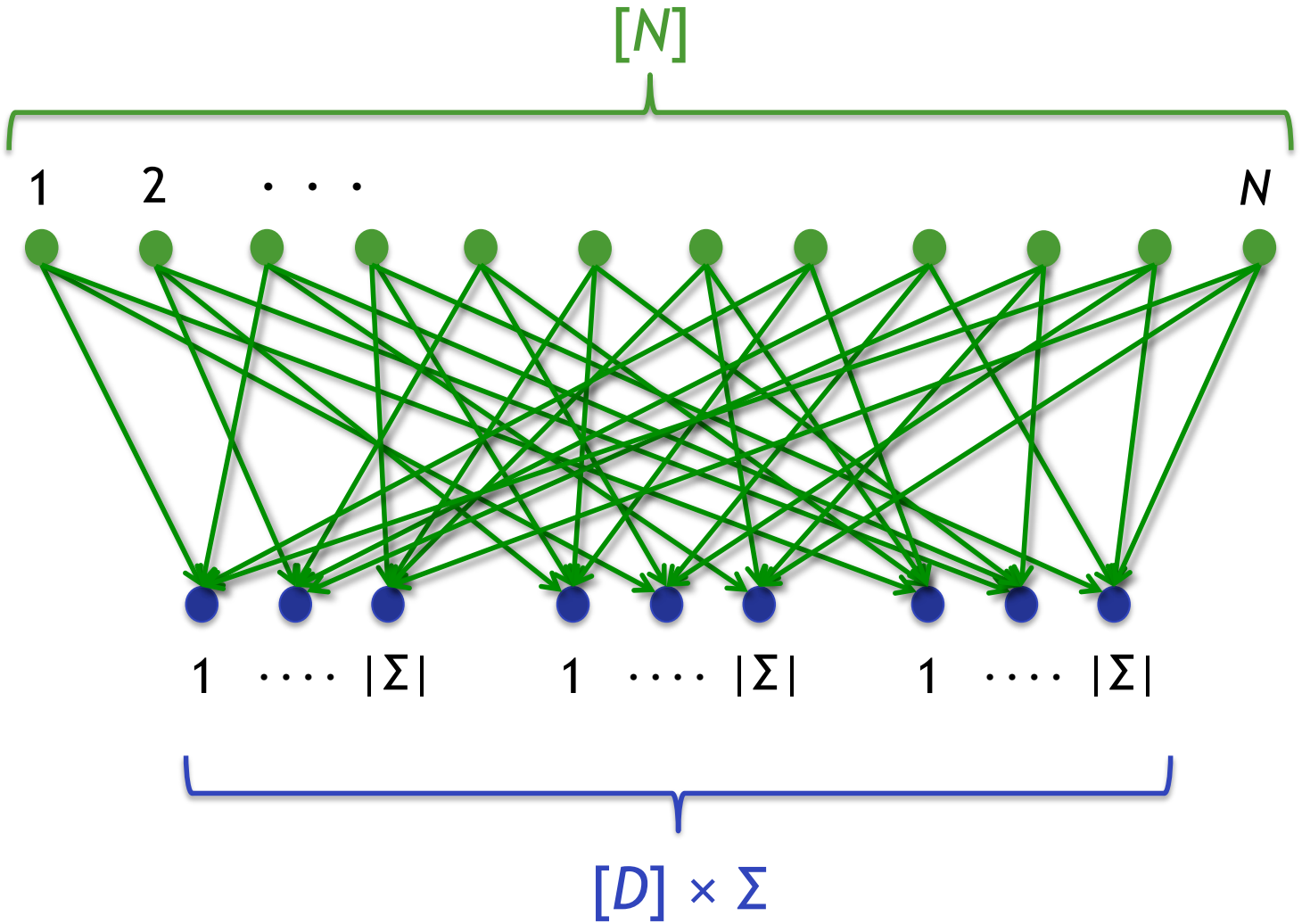
- 擬似ランダムオブジェクトに対する統一的記述
  - Vdhan による考察
  - リスト復号可能符号，乱数抽出器，擬似乱数生成器，エクスパンダグラフ，困難性増幅器，など
  - 共通点が見つかることで相違点も明らかに
- Parvaresh-Vardy 符号にもとづく乱数抽出器
  - Guruswami, Umans, Vadhan 2007
  - PV 符号 → 無損失エクスパンダ → 無損失濃縮器
  - PV 符号の代数的性質によって，
    ほぼ最適な乱数抽出器をシンプルに構成

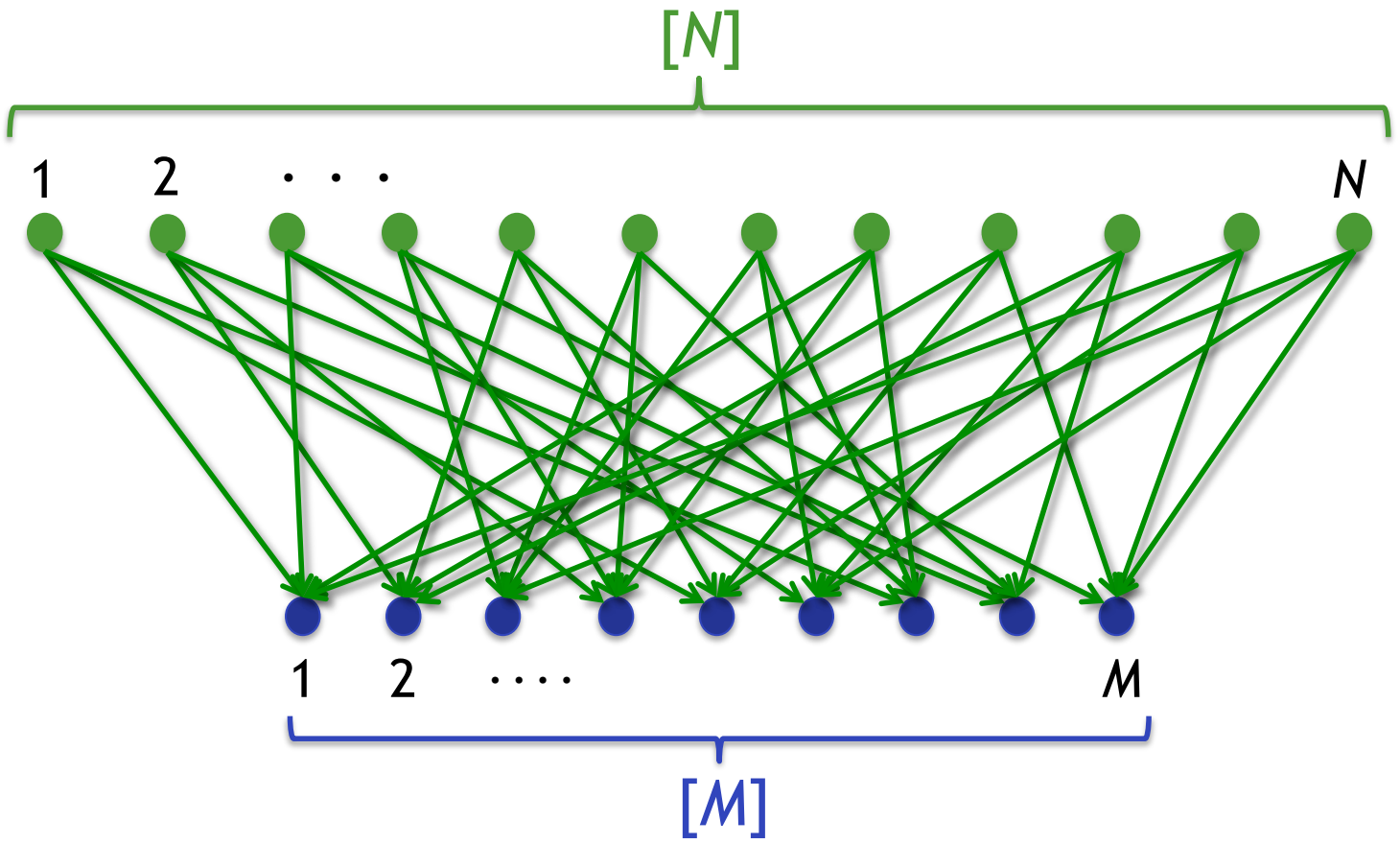
    → 代数的構造が強力な道具であることを証明！

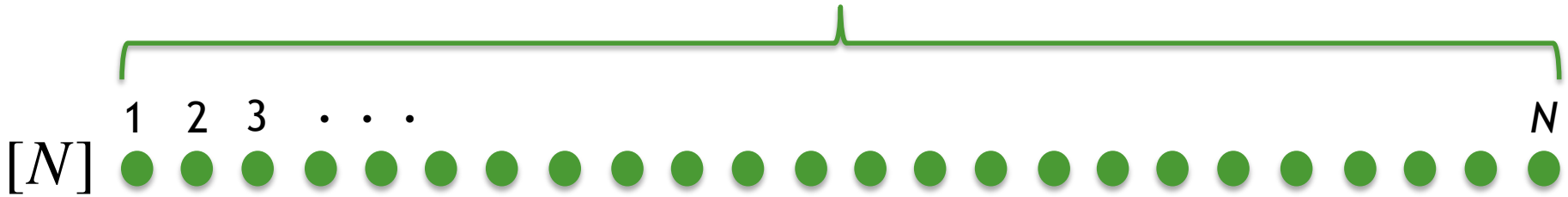
今後の研究

- 統一的枠組みを，
  他の擬似ランダムオブジェクトに拡張可能か？
  - 複数情報源の乱数抽出器
  - 暗号論的擬似乱数生成器

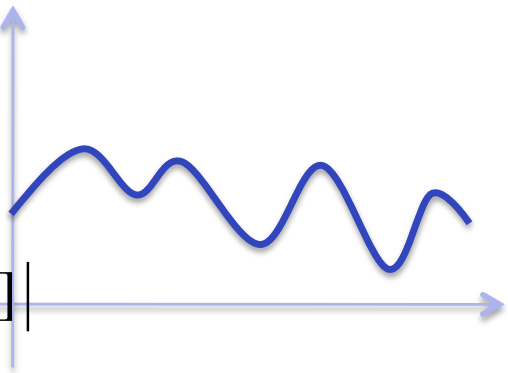
  - Cheraghchi, “Capacity achieving codes from randomness conductors” (ISIT 2009)
    - 乱数抽出器から BSC, BEC で 通信路容量を達成する符号アンサンブル（quasipoly size）を構成


[N]
1
2
N
1 ···· |Σ|
1 ···· |Σ|
1 ···· |Σ|
[D] × Σ


[N]
1
2
N
1
2
M
[M]



$$\Delta(Y,Z) = \frac{1}{2}\sum_{a\in[M]}\left|\Pr[Y=a]-\Pr[Z=a]\right|$$



$$\Pr_{i\in[D]}\left[r_i = \mathrm{Enc}(x)_i\right] \geq \frac{1}{|\Sigma|} + \varepsilon$$