Resource Bounded Kučera–Gács Theorems and Polynomial-time Dimension

Satyadev Nandakumar, Akhil S, Chandrasekhar Tiwari

IIT Kanpur

June 17, 2025

Outline

Outline

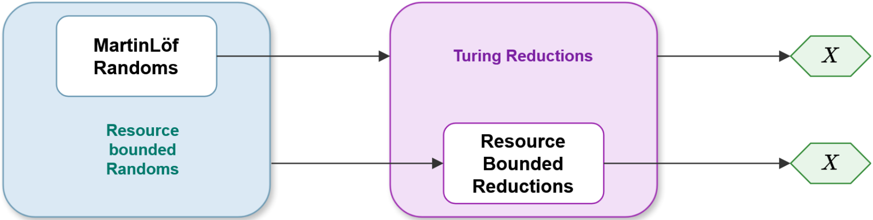
Kučera–Gács Theorem

Theorem

For every $X \in \{0,1\}^\infty$, *there exists a Martin-Löf random* R *such that*

$$X \leq_T R.$$

Resource Bounded Kučera–Gács



Overview

- Proof of Classical Kučera–Gács.

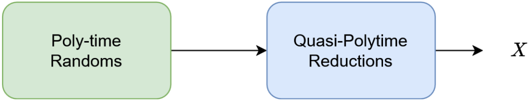
Overview

- Proof of Classical Kučera–Gács.
- (Quasi) Polynomial-time Kučera–Gács.
  - Optimisation: Number of Oracle queries used.

Quasi-Polynomial Kučera–Gács

Theorem

For any $X \in \Sigma^{\infty}$*, and* $t \in \omega(poly)$*, there exits a polynomial-time random* $R \in \Sigma^{\infty}$ *such that* $X \leq_{t'(n)} R$*, where* $t'(n) = O(n \cdot t(n + \sqrt{n}\log n))$*.*



Moreover, $X[1 \ldots n]$ can be computed using $R[1 \ldots n + \sqrt{n}\log n]$.

Overview

- Proof of Classical Kučera–Gács.
- (Quasi) Polynomial-time Kučera–Gács.
  - Optimisation: Number of Oracle queries used.
- Polytime Dimension and (quasi) Polytime Kučera–Gács Reductions.

Poly-time Dimension and Reductions

Theorem

For all $X \in \Sigma^\infty$, there exists a Polynomial-time Random $R \in \Sigma^\infty$ such that $X \leq_{t(n)} R$ via M with oracle use u_n such that

$$\mathcal{K}_{\text{poly}}(X) = \liminf \frac{u_n}{n}.$$

where $t(n) = (n \cdot t'(n + \sqrt{n} \log n))$ and $t'(n) \in \omega(poly)$.

Overview

- Proof of Classical Kučera–Gács.
- (Quasi) Polynomial-time Kučera–Gács.
  - Optimisation: Number of Oracle queries used.
- Polytime Dimension and (quasi) Polytime Kučera–Gács Reductions.
- Finite-state Analogue of Kučera–Gács.

Outline

Kučera–Gács Theorem

Theorem (Kučera–Gács)

For every $X \in \{0,1\}^\omega$, there exists a Martin-Löf random R such that

$$X \leq_T R.$$

Kučera–Gács Theorem

Theorem (Kučera–Gács)

For every $X \in \{0,1\}^\omega$, *there exists a Martin-Löf random* R *such that*

$$X \leq_T R.$$

$\xrightarrow{M}$

Definition

A function $d : \Sigma^* \to [0, \infty)$ is called a martingale if for all $w \in \Sigma^*$,

$$d(w0) + d(w1) = 2 \cdot d(w).$$

Martingales and Martin-Löf Randomness

Definition

A function $d : \Sigma^* \to [0, \infty)$ is called a martingale if for all $w \in \Sigma^*$,

$$d(w0) + d(w1) = 2 \cdot d(w).$$

Definition

A function $d : \Sigma^* \to [0, \infty)$ is c.e or lower-semi computable if there exists a computable $\tilde{d} : \Sigma^* \times \mathbb{N} \to [0, \infty) \cap \mathbb{Q}$ such that

- $\forall t \; \tilde{d}(w, t) <= \tilde{d}(w, t + 1)$
- $\lim_t \tilde{d}(w, t) = d(w)$.

Martingales and Martin-Löf Randomness

Theorem

A sequence $R \in \Sigma^\infty$ *is Martin-Löf random iff for the universal c.e martingale* $d : \Sigma^* \to [0, \infty)$,

$$\limsup_n (d(R \upharpoonright n)) < \infty.^1$$

Martingales and Martin-Löf Randomness

Theorem

A sequence $R \in \Sigma^\infty$ is Martin-Löf random iff for the universal c.e martingale $d : \Sigma^* \to [0, \infty)$,

$$\limsup_n (d(R \upharpoonright n)) < \infty.^{1}$$

(1) $\liminf_n (d(R \upharpoonright n)) < \infty$ also works.

Proof Strategy

[Merkle Mihalovic 2004] Given $X \in \Sigma^\infty$,

Proof Strategy

[Merkle Mihalovic 2004] Given $X \in \Sigma^\infty$,

1. Take the *universal* c.e Martingale $d : \Sigma^* \to [0, \infty)$.

Proof Strategy

[Merkle Mihalovic 2004] Given $X \in \Sigma^\infty$,

1. Take the *universal* c.e Martingale $d : \Sigma^* \to [0, \infty)$.
2. Construct a ML-random sequence R by encoding X.
   - Randomness: Diagonalizing against d.
   - Recoverability: Use bits of X to choose among possibilities for R.

Proof Strategy

[Merkle Mihalovic 2004] Given $X \in \Sigma^\infty$,

1. Take the *universal* c.e Martingale $d : \Sigma^* \to [0, \infty)$.
2. Construct a ML-random sequence R by encoding X.
   - Randomness: Diagonalizing against d.
   - Recoverability: Use bits of X to choose among possibilities for R.
3. Decode X from R via a computable function.

Proof Strategy

Given $X \in \Sigma^\infty$, Diagonalize against d.

- Stage i : Extend R_{i-1} to R_i using $X[i]$.

Proof Strategy

Given $X \in \Sigma^\infty$, Diagonalize against d.

- Stage i : Extend R_{i-1} to R_i using $X[i]$.
- Choose an R_i such that

$$d(R_i) \leq d(R_{i-1})(1 + \delta_i).$$

Proof Strategy

Given $X \in \Sigma^\infty$, Diagonalize against d.

- Stage i : Extend R_{i-1} to R_i using $X[i]$.
- Choose an R_i such that

$$d(R_i) \leq d(R_{i-1})(1 + \delta_i).$$

- Take $\delta_i = i^{-2}$, then $\prod_i (1 + \delta_i) < \infty$.

Proof Strategy

Given $X \in \Sigma^\infty$, Diagonalize against d.

- Stage i : Extend R_{i-1} to R_i using $X[i]$.
- Choose an R_i such that

$$d(R_i) \leq d(R_{i-1})(1 + \delta_i).$$

- Take $\delta_i = i^{-2}$, then $\prod_i (1 + \delta_i) < \infty$.
- $\liminf_n d(R \upharpoonright n) < \infty \implies R$ is MLR.

Proof Strategy

Encoding X into R.

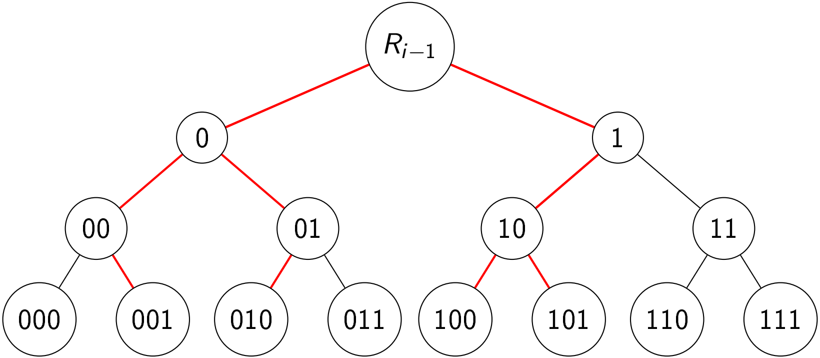
- At stage i, extend R_{i-1} by enough bits (ℓ_i) so that there are atleast 2 candidates for R_i.
  - ℓ_i can be computed from δ_i.

Proof Strategy

Encoding X into R.

- At stage i, extend R_{i-1} by enough bits (ℓ_i) so that there are atleast 2 candidates for R_i.
    - ℓ_i can be computed from δ_i.
- If $X_i = 0$, pick leftmost feasible R_i.
- If $X_i = 1$, pick the rightmost feasible R_i.

Picking R_i



$$d(R_i) < d(R_{i-1})(1 + \delta_i).$$

Proof Strategy

Decoding X from R.

- At stage i, calculate R_{i-1} and R_i from R.
- Run two processes parallely. Check among $x \in R_{i-1}.\Sigma^{\ell_i}$.
  - Check if forall $x \preccurlyeq R_i$, $d(x) \leq d(R_{i-1})(1 + \delta_i)$. $X[i] = 0$.
  - Check if forall $R_i \preccurlyeq x$ $d(x) \leq d(R_{i-1})(1 + \delta_i)$. $X[i] = 1$.

Theorem (Kučera–Gács)

For every $X \in \{0,1\}^\omega$, there exists a Martin-Löf random R such that X is Turing reducible to R, i.e.

$$X \leq_T R.$$

$$\xrightarrow{M}$$

Outline

Polynomial-time Martingale

Definition

A function $d : \Sigma^* \to [0, \infty)$ is called a martingale iff for all $w \in \Sigma^*$,

$$d(w0) + d(w1) = 2 \cdot d(w).$$

Definition

A function $d : \Sigma^* \to [0, \infty) \cap \mathbb{Q}$ is poly-time computable if there is a turing machine that on input $x \in \Sigma^n$ outputs $d(x)$ in time $O(n^k)$.

Polynomial-time Randoms

Definition

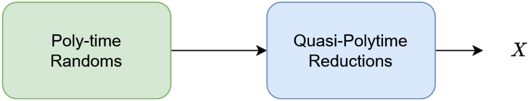
A sequence $R \in \Sigma^\infty$ is polytime random iff for all poly-time computable martingale $d : \Sigma^* \to [0, \infty)$,

$$\limsup_n (d(R \restriction n)) < \infty.$$

Quasi-Polynomial Kučera–Gács

Theorem

For any $X \in \Sigma^\infty$, and $t \in \omega(poly)$, there exits a polynomial-time random $R \in \Sigma^\infty$ such that $X \leq_{t'(n)} R$, where $t'(n) = O(n \cdot t(n + \sqrt{n} \log n))$.



Moreover, $X[1 \ldots n]$ can be computed using $R[1 \ldots n + \sqrt{n} \log n]$.

Proof Strategy

1. Take the *universal* poly-time Martingale $d : \Sigma^* \to [0, \infty)$.
2. Construct a polytime-random sequence R by ensuring
   - Randomness: Diagonalizing against d.
   - Recoverability: Use bits of X to choose among possibilities for R.
3. Decode X from R via a quasi poly-time computable function.

Universal poly-time Martingale

Theorem

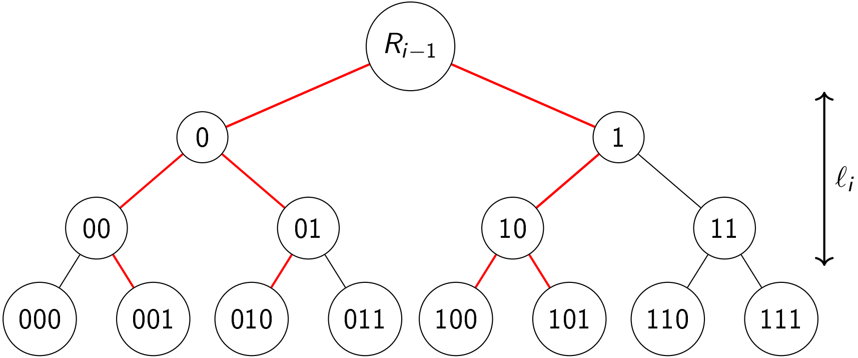
For any $t \in \omega(poly)$, there exits a $t(n) \cdot n \cdot \log n$-time Martingale that is universal over all polynomial-time martingales.

d_1	d_2	d_3	d_4	d_5	d_6	d_7	$\ldots$

$X[0]$	d_1			
$X[1]$	d_1	d_2		
$X[2]$	d_1	d_2	d_3	
$X[2]$	d_1	d_2	d_3	d_4

$\ldots$

Encoding



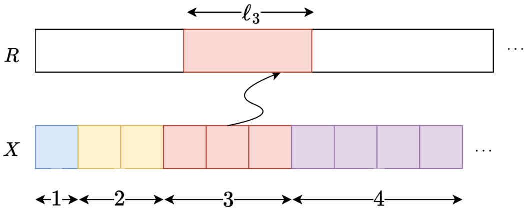
$$d(R_i) < d(R_{i-1})(1 + \delta_i).$$

New Encoding

- At stage i, $\ell_i = 2 + 2 \cdot \log i$.
- Encoding n bits of X requires $\Omega(n \log n)$ bits of R !
- Modify: n bits of X requires only $n + O(\sqrt{n} \log n)$ bits of R.

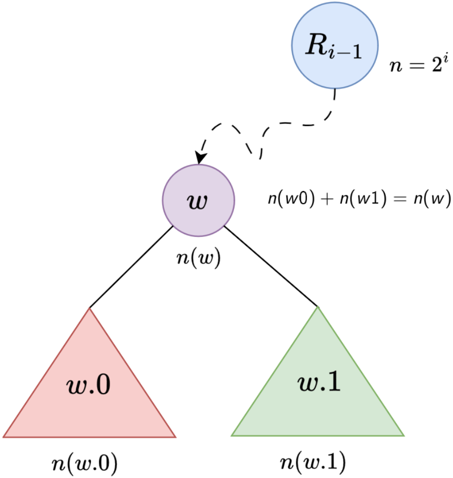
Block Encoding

- At stage i, encode next i bits of X into R.



- Taking $\delta_i = i^{-2}$, $\ell_i = i + 2\log i$.
- Only need $n + \sqrt{n}\log n$ bits of R to get $X[1\ldots n]$.

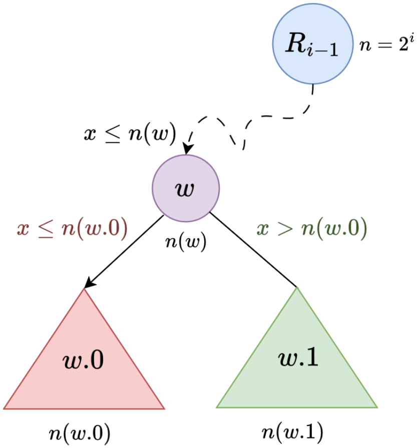
Encoding



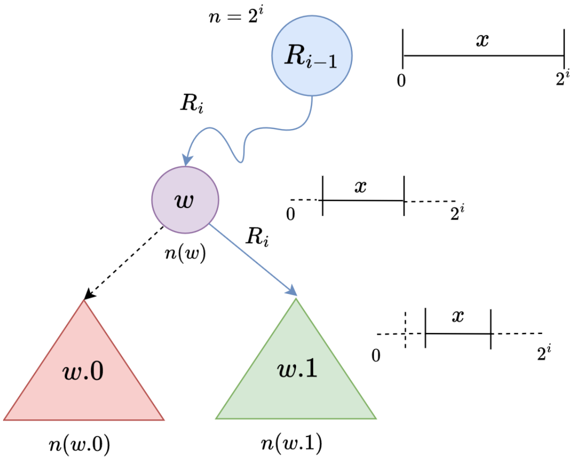
$$n(w) = \frac{2_i^{\ell}}{2^{|w|}}\left(1 - \frac{d(R_{i-1}.w)}{d(R_{i-1})} \cdot \frac{i^2}{1+i^2}\right).$$

$$n(w) \leq \#\{x \in \Sigma^{\ell_i - |w|} : d(R_{i-1}.w.x) < d(R_{i-1}) \cdot (1 + i^{-2}).\}$$

Encoding



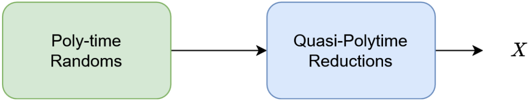
Decoding



Quasi-Polynomial Kučera–Gács

Theorem

For any $X \in \Sigma^\infty$, and $t \in \omega(poly)$, there exits a polynomial-time random $R \in \Sigma^\infty$ such that $X \leq_{t'(n)} R$, where $t'(n) = O(n \cdot t(n + \sqrt{n} \log n))$.



Moreover, $X[1 \ldots n]$ can be computed using $R[1 \ldots n + \sqrt{n} \log n]$.

Outline

Constructive Dimension

- Measures Density of Information in an infinite sequence.

Theorem (Lutz, Mayordomo)

For $X \in \Sigma^\infty$,

$$\mathrm{cdim}(X) = \liminf_n \frac{K(X \upharpoonright n)}{n}.$$

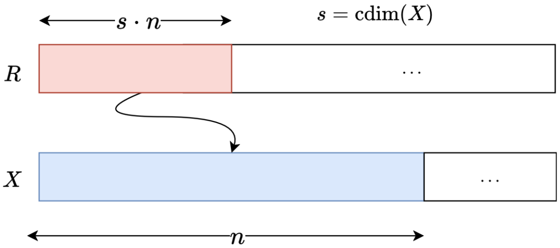
- $K(x)$: Algorithmic Information content in a string.

$$K(x) = \min_{\pi \in \mathcal{P}} \{U(\pi) = x\}.$$

Theorem (Doty (2006))

For all $X \in \Sigma^\infty$, there exists a Martin-Löf Random $R \in \Sigma^\infty$ such that $X \leq_T R$ via M with oracle use u_n such that

$$\mathrm{cdim}(X) = \liminf \frac{u_n}{n}.$$



Poly-time Dimension

- Density of Information in an infinite sequence measured using Polynomial-time algorithms.

Definition

For $X \in \Sigma^\infty$,

$$\mathcal{K}_{\text{poly}}(X) = \inf_{t \in \text{poly}} \liminf_{n} \frac{K_t(X \upharpoonright n)}{n}.$$

- $K_t(x)$: t-time bounded Algorithmic Information content in a string.

$$K_t(x) = \min_{\pi \in \mathcal{P}} \{U^{t(|x|)}(\pi) = x\}.$$

Poly-time Dimension and Reductions

Definition

For two sequences $X, Y \in \Sigma^\infty$, we say

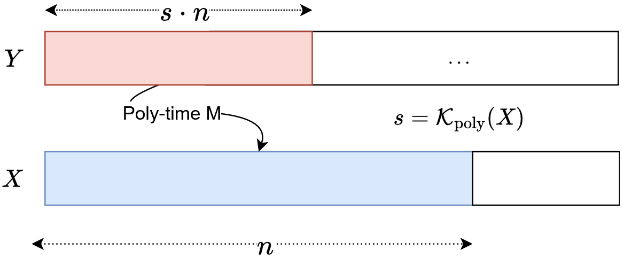
$$X \leq_P Y \iff \exists \text{ poly-time T.M s.t } \forall n\; M^Y(1^n) = X \restriction n.$$

Theorem

$$\mathcal{K}_{\text{poly}}(X) = \inf_{\substack{Y \in \Sigma^\infty \\ M \in OTM}} \left\{ \liminf \frac{u_n}{n} \;\middle|\; X \leq_P Y \textit{ via } M \right\}.$$

u_n : Oracle use of Y by M to produce $X[1 \ldots n]$.

Poly-time Dimension and Reductions



Proof Outline

$$\mathcal{K}_{\text{poly}}(X) \leq \inf_{\substack{Y \in \Sigma^\infty \\ M \in \text{OTM}}} \left\{ \liminf \frac{u_n}{n} \,\middle|\, X \leq_P Y \text{ via } M \right\}.(*)$$

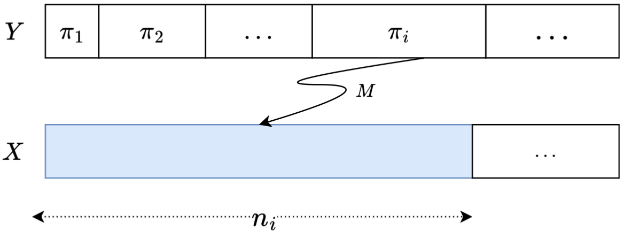
- $s > *$ via
  - Machine M ($t(n)$ time), Oracle Y, Indices $\{n_i\}$.
- $K_t(X \upharpoonright n_i) \leq |u_n(Y)| \leq sn_i$.

Proof Outline

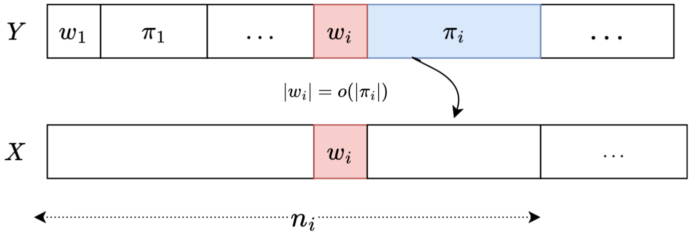
$$\mathcal{K}_{\text{poly}}(X) \geq \inf_{\substack{Y \in \Sigma^\infty \\ M \in \text{OTM}}} \left\{ \liminf \frac{u_n}{n} \,\middle|\, X \leq_P Y \text{ via } M \right\}.(*)$$

- $s > \mathcal{K}_{\text{poly}}$
  - For indices $\{n_i\}$, $K_t(X \upharpoonright n_i) < s \cdot n_i$, say via π_i.
  - Take $n_i = o(n_1 + \ldots n_{i-1})$.
- Attempt 1 : $Y = \pi_1.\pi_2 \ldots \pi_i \ldots$

Proof Outline



Proof Outline



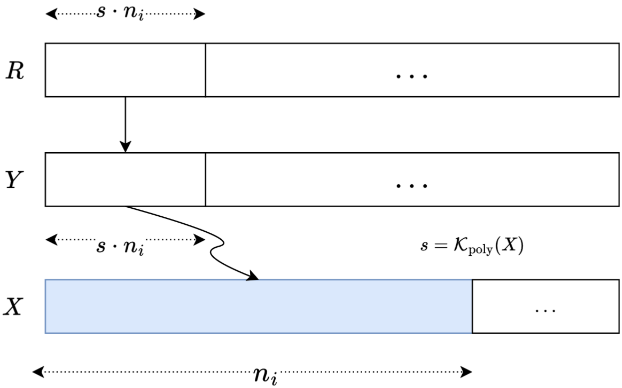
Poly-time Dimension and Reductions

Theorem

$$\mathcal{K}_{\mathrm{poly}}(X) = \inf_{\substack{Y \in \Sigma^\infty \\ M \in OTM}} \left\{ \liminf \frac{u_n}{n} \;\middle|\; X \leq_P Y \textit{ via } M \right\}.$$

u_n : Oracle use of Y by M to produce $X[1 \ldots n]$.

Putting things together



Theorem

For all $X \in \Sigma^\infty$, there exists a Polynomial-time Random $R \in \Sigma^\infty$ such that $X \leq_{t(n)} R$ via M with oracle use u_n such that

$$\mathcal{K}_{\mathrm{poly}}(X) = \liminf \frac{u_n}{n}.$$

where $t(n) = (n \cdot t'(n + \sqrt{n}\log n))$ and $t'(n) \in \omega(poly)$.

Outline

Finite-state Kučera–Gács

- Finite-State Randoms and Finite-State Reductions.

Theorem (Schnorr, Stimm 1972)

For any sequence $X \in \Sigma^\infty$

$$X \text{ is Finite-State Random} \iff X \text{ is Normal}$$

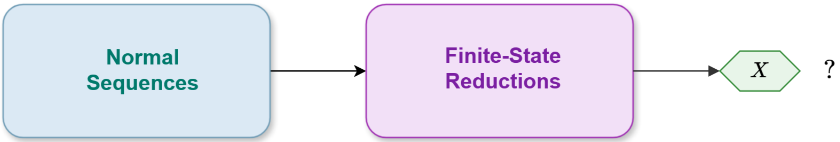
Finite-state Kučera–Gács

- Finite-State Randoms and Finite-State Reductions.

Theorem (Schnorr, Stimm 1972)

For any sequence $X \in \Sigma^\infty$

$$X \text{ is Finite-State Random} \iff X \text{ is Normal}$$

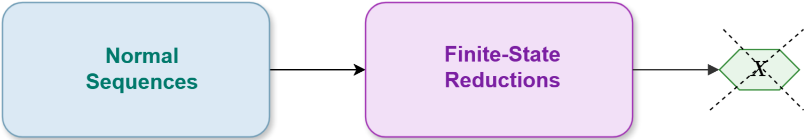


No Kučera–Gács for Normality

Theorem

There exists an $X \in \Sigma^\infty$ such that for all Normal $N \in \Sigma^\infty$ and finite state reductions $T : \Sigma^\infty \to \Sigma^\infty$,

$$T(N) \neq X.$$



Proof overview

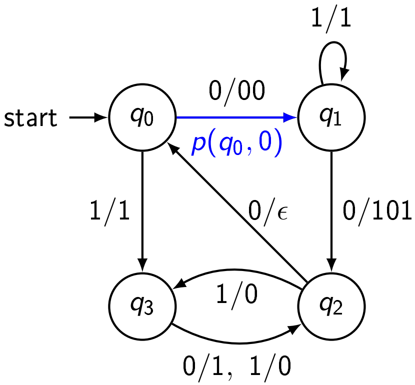
- If $N \in \Sigma^\infty$ is normal, N induces a stationary distribution on the transitions of G.

Theorem (Schnorr, Stimm)

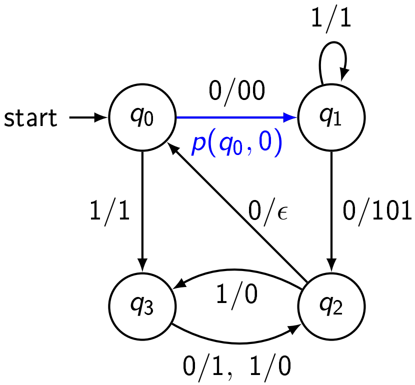
For any normal $N \in \Sigma^\infty$ and finite state transducer $G = (Q, \Sigma, q_0, \delta, \tau)$, there exists a probaility distribution $P : Q \times \Sigma \to [0,1]$ such that

$$\lim_n \frac{\#((q,a), X \upharpoonright n)}{n} = P(q,a)$$

Proof overview



Proof overview



Therefore $P(0)$ and $P(1)$ in $T(X)$ must converge !

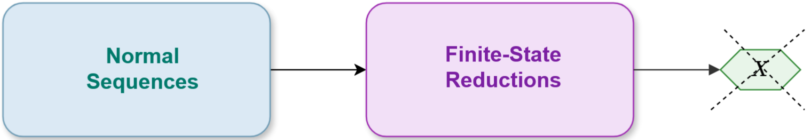
Proof overview

- Consider any $X \in \{0,1\}^\infty$ such that $P(0)$ and $P(1)$ in X does not converge.

Theorem

*There **does not** exist a Normal $N \in \Sigma^\infty$ and finite state reduction $T : \Sigma^\infty \to \Sigma^\infty$ such that*

$$T(N) = X.$$



Outline

Conclusion

- Kučera–Gács : For every sequence, there is a random sequence from which it is constructively recoverable.
- (Quasi) Polynomial-time analogue of Kučera–Gács.
  - Using $\sqrt{n} \log n$ extra bits.
- $\mathcal{K}_{\text{poly}}$ dimension can be characterised using poly-time reductions.
  - Quasi poly-time reductions from poly-time randoms.
- Finite-state analogue of Kučera–Gács does not hold.

Open Questions

- Can we get an actual polynomial-time Kucera Gacs theorem ?
- Can we characterize $\mathcal{K}^{str}_{\mathrm{poly}}$ using poly-time reductions ?

References

- Merkle, Wolfgang, and Nenad Mihailović. "On the construction of effectively random sets." The Journal of Symbolic Logic 69.3 (2004): 862-878.
- Doty, David. "Dimension extractors and optimal decompression." Theory of Computing Systems 43.3 (2008): 425-463.
- Schnorr, Claus-Peter, and Hermann Stimm. "Endliche automaten und zufallsfolgen." Acta Informatica 1 (1972): 345-359.