Approximating Cumulative Pebbling Cost is Unique Games Hard

Jeremiah Blocki[1], Seunghoon Lee[1], Samson Zhou[2]

[1]Department of Computer Science, Purdue University
[2]School of Computer Science, Carnegie Mellon University

Summary

Motivation.

- Cumulative Pebbling Cost (cc) of a DAG G
- Study of Memory-Hard Functions in cryptography
  - Goal: Design constant indegree G with max $\mathsf{cc}(G)$
  - Practical Constructions: Upper/Lower bounds differ by orders of magnitude
- Computational complexity of $\mathsf{cc}(G)$?

Our Result.

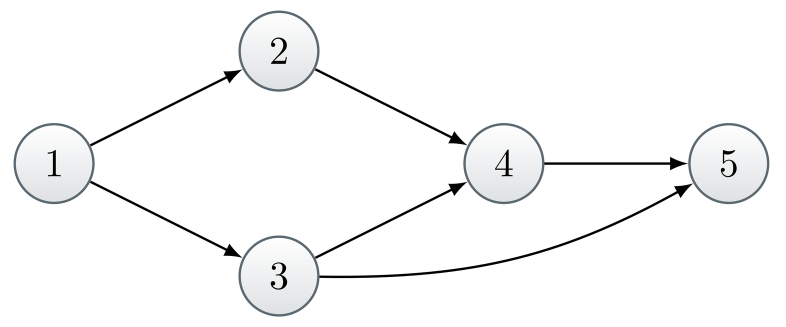
- **Hardness of approximation algorithm for $\mathsf{cc}(G)$!**

Theorem. Given a DAG G with *constant indegree*, it is Unique Games Hard to c-approximate $\mathsf{cc}(G)$ for any constant $c > 1$.

Background

Parallel Pebbling Game and $\mathsf{cc}(G)$.

- Goal: Place pebbles on all sink nodes.
- Pebbling Rules:
  - Initially, the graph is unpebbled.
  - We can add a new pebble only if its parents were all pebbled.
  - We can place multiple pebbles at the same time.
  - We can discard pebbles at any time if not needed.
- $\mathsf{cc}(G) := \min_P \{|P_1| + \cdots + |P_t|\}$.

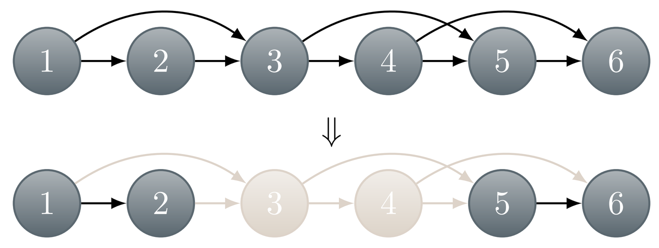


$P_1 = \{1\}, P_2 = \{2,3\}, P_3 = \{3,4\}$, and $P_4 = \{5\}$

$\therefore \mathsf{cc}(G) \le \sum_{i=1}^{4} |P_i| = 1+2+2+1 = 6.$

Depth Robustness of a DAG G.

- A DAG $G = (V,E)$ is (e,d)-*depth robust* if
$$\forall S \subseteq V \text{ s.t. } |S| \le e \;\Rightarrow\; \mathsf{depth}(G - S) \ge d.$$
- G is (e,d)-*reducible* if G is not (e,d)-depth robust.



Previous Work

Relationship between DR and $\mathsf{cc}(G)$.

- [2] If G is (e,d)-depth robust, then $\mathsf{cc}(G) \ge ed$.
- [1] If G is (e,d)-reducible with N nodes, then
$$\mathsf{cc}(G) \le \min_{g \ge d}\left(eN + gN \times \mathsf{indeg}(G) + \frac{N^2 d}{g}\right).$$

Computational Complexity of $\mathsf{cc}(G)$.

- [4] Computing $\mathsf{cc}(G)$ is NP-Hard.
  - did not rule out approximation algorithms for $\mathsf{cc}(G)$

Technical Ingredient 1: Svensson's Result [5]

- Reduction from an instance of Unique Games $\mathcal{U}$ to a DAG $G_{\mathcal{U}}$ on N nodes ($\mathcal{U} \to \hat{G}_{\mathcal{U}} \to G_{\mathcal{U}}$)
- $G_{\mathcal{U}}$ has high indegree $\mathcal{O}(N)$

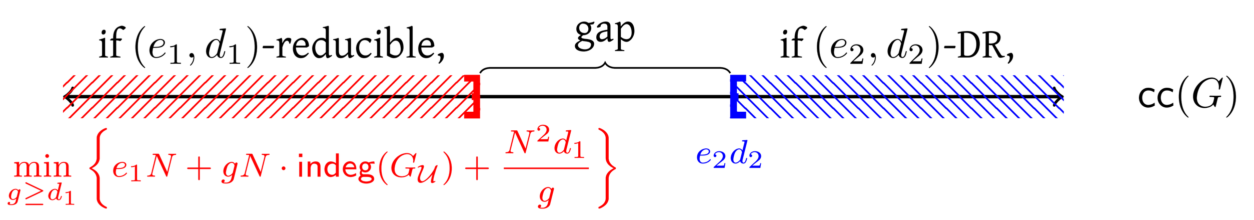
Theorem. [5]

For any integer $k \ge 2$ and constant $\varepsilon > 0$, it is Unique Games Hard to distinguish between

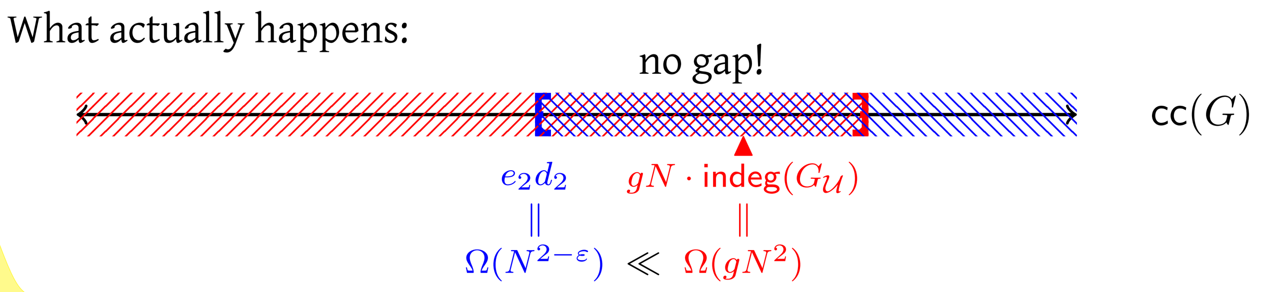
1. G is (e_1,d_1)-reducible with $e_1 = N/k$ and $d_1 = k$, and
2. G is (e_2,d_2)-depth robust with $e_2 = N(1-1/k)$ and $d_2 = \Omega(N^{1-\varepsilon})$.

Large Gap!

What we want:



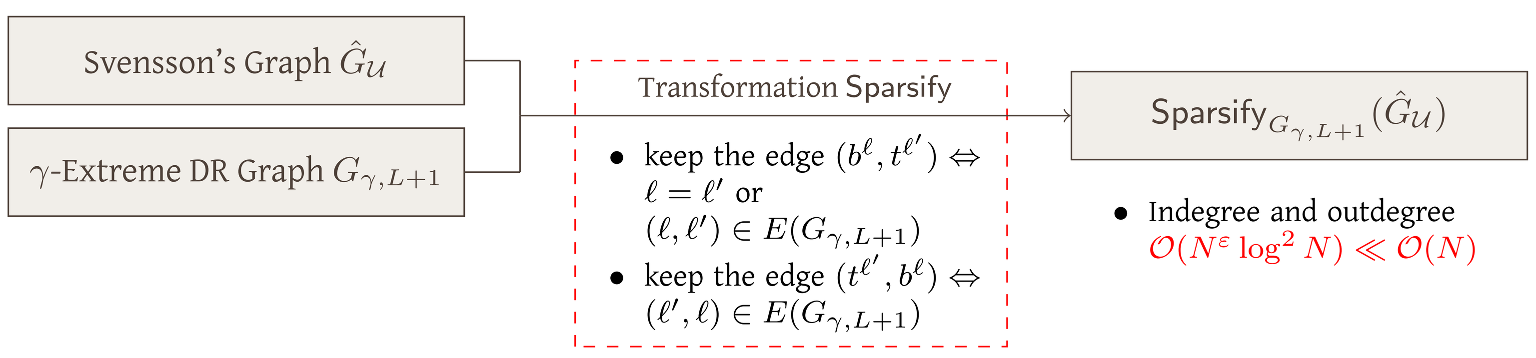
What actually happens:

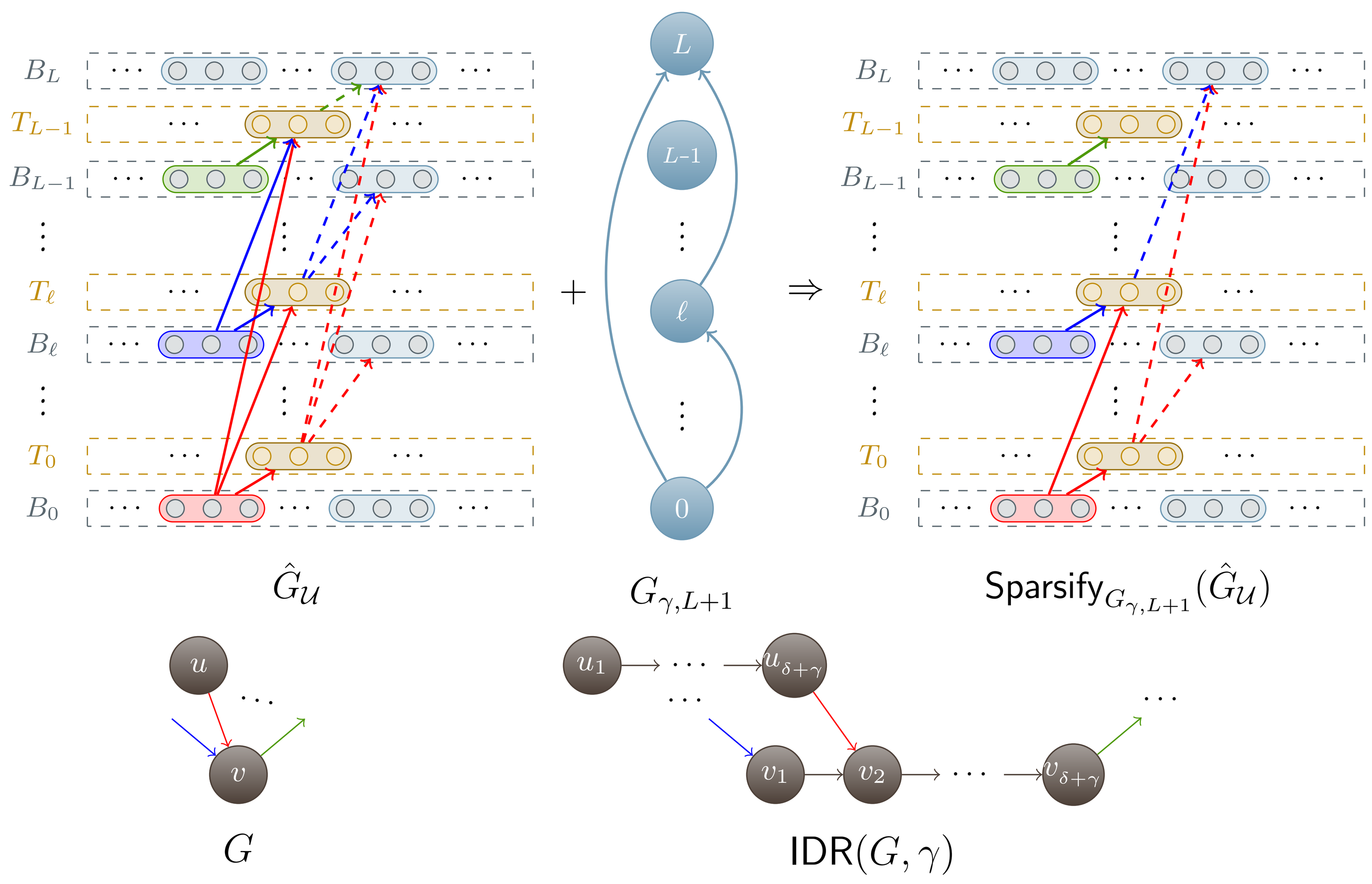


Technical Ingredient 2: Indegree Reduction using a γ-Extreme DR Graph

Definition.

A DAG $G_{\gamma,N}$ on N nodes is said to be γ-*extreme depth-robust* if it is (e,d)-depth robust for any $e,d > 0$ such that $e + d \le (1-\gamma)N$.





Theorem.

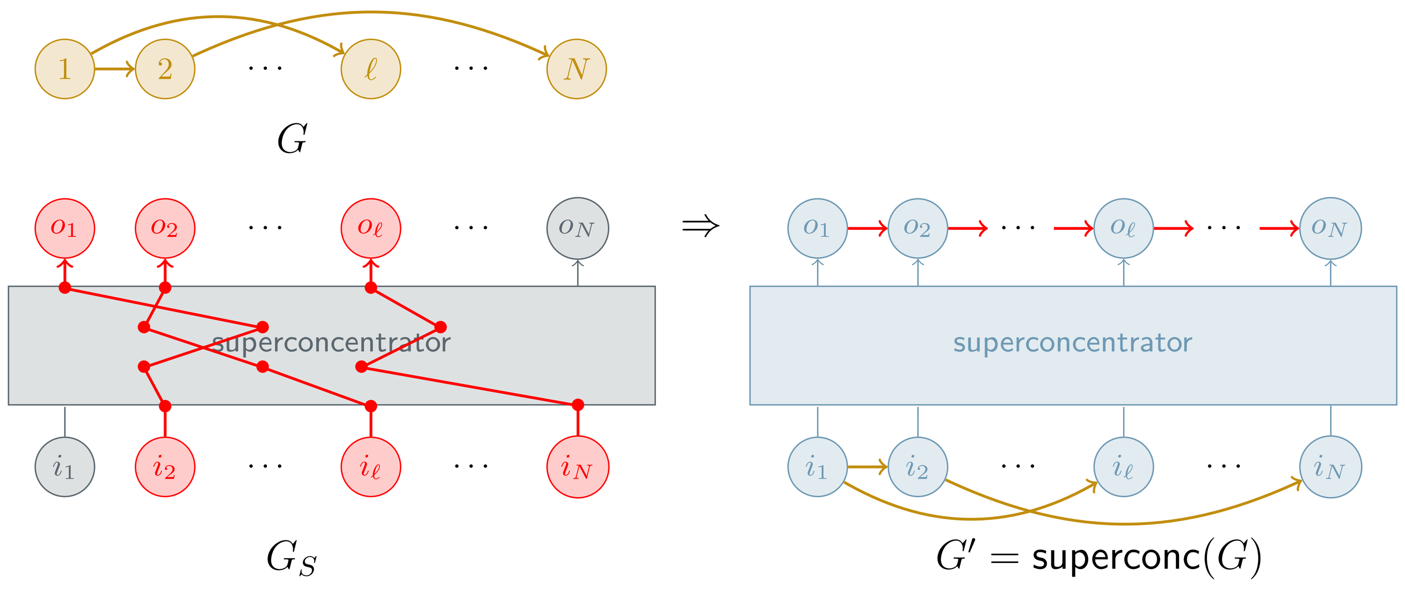
For any integer $k \ge 2$ and constant $\varepsilon > 0$, given a DAG G with N vertices and $\mathsf{indeg}(G) = 2$, it is Unique Games hard to decide whether G is (e_1,d_1)-reducible or (e_2,d_2)-depth robust for

- $e_1 = \frac{1}{k}N^{\frac{1}{1+2\varepsilon}}$, $d_1 = kN^{\frac{2\varepsilon}{1+2\varepsilon}}$, and
- $e_2 = (1-\varepsilon)N^{\frac{1}{1+2\varepsilon}}$, $d_2 = 0.9N^{\frac{1+\varepsilon}{1+2\varepsilon}}$.

$\Downarrow$

Combining with upper/lower bound of $\mathsf{cc}(G)$, **still no gap!**

Technical Ingredient 3: Superconcentrator Overlay



- We have **tighter bounds** for $\mathsf{cc}(\mathsf{superconc}(G))$!
  - If G is (e,d)-depth robust, then [3]
$$\mathsf{cc}(\mathsf{superconc}(G)) \ge \min\left\{\frac{eN}{8}, \frac{dN}{8}\right\},$$
  - If G is (e,d)-reducible, then
$$\mathsf{cc}(\mathsf{superconc}(G)) \le \min_{g\ge d}\left\{2eN + 4gN + \frac{43dN^2}{g} + \frac{24N^2\log(42N)}{g} + 42N\log(42N) + N\right\}.$$

- Recall that $e_1 = \frac{1}{k}N^{\frac{1}{1+2\varepsilon}}$, $d_1 = kN^{\frac{2\varepsilon}{1+2\varepsilon}} \Rightarrow$ for $g = e_1$ and large N, $\mathsf{cc}(\mathsf{superconc}(G)) \le \frac{7}{k}N^{\frac{2+2\varepsilon}{1+2\varepsilon}}$.
- $e_2 = (1-\varepsilon)N^{\frac{1}{1+2\varepsilon}}$, $d_2 = 0.9N^{\frac{1+\varepsilon}{1+2\varepsilon}} \Rightarrow \mathsf{cc}(\mathsf{superconc}(G)) \ge \frac{1-\varepsilon}{8}N^{\frac{2+2\varepsilon}{1+2\varepsilon}}$.
- For any constant $c > 1$, setting $\varepsilon = 0.1$ and $k = \lceil \frac{560}{9}c^2 \rceil$, we have the **gap** $\frac{7}{k}N^{\frac{2+2\varepsilon}{1+2\varepsilon}} \le \frac{9}{80c^2}N^{\frac{2+2\varepsilon}{1+2\varepsilon}} < \frac{9}{80}N^{\frac{2+2\varepsilon}{1+2\varepsilon}} = \frac{1-\varepsilon}{8}N^{\frac{2+2\varepsilon}{1+2\varepsilon}}$.

References

[1] Joël Alwen and Jeremiah Blocki. Efficiently computing data-independent memory-hard functions. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 241–271. Springer, Heidelberg, August 2016.

[2] Joël Alwen, Jeremiah Blocki, and Krzysztof Pietrzak. Depth-robust graphs and their cumulative memory complexity. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part III*, volume 10212 of *LNCS*, pages 3–32. Springer, Heidelberg, April / May 2017.

[3] Jeremiah Blocki, Benjamin Harsha, Siteng Kang, Seunghoon Lee, Lu Xing, and Samson Zhou. Data-independent memory hard functions: New attacks and stronger constructions. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 573–607. Springer, Heidelberg, August 2019.

[4] Jeremiah Blocki and Samson Zhou. On the computational complexity of minimal cumulative cost graph pebbling. *Financial Cryptography and Data Security (FC 2018)*, 2018.

[5] Ola Svensson. Hardness of vertex deletion and project scheduling. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques - 15th International Workshop, APPROX, and 16th International Workshop, RANDOM. Proceedings*, pages 301–312, 2012.

Acknowledgements

- Jeremiah Blocki: Research supported in part by NSF Award #1755708
- Seunghoon Lee: Research supported in part by NSF Award #1755708 and by the Center for Science of Information at Purdue University (NSF CCF-0939370)
- Part of this work was done while Samson Zhou was a post-doctoral fellow at Indiana University.

Further Information