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

November 21, 2019

(Parallel) Graph Pebbling and Cumulative Pebbling Cost cc(G)

Overview

We Are Here

(Parallel) Graph Pebbling.

- Pebbling example
- Cumulative Pebbling Cost of G

Problem Statement.

- Given a DAG G find the (approx.) minimum cost pebbling

Significance of cc(G)**.**

- Analysis of data-independent memory-hard functions
- Amortization / Parallelism

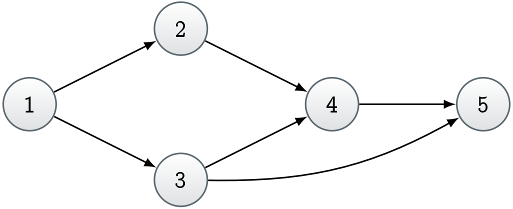
Results.

- Unique Games Hard to approximate cc(G) for any constant factor

Technical Ingredients.

- Indegree reduction using γ-extreme depth robust graphs
- Superconcentrator overlay

(Parallel) Pebbling Example.



(Parallel) Graph Pebbling and Cumulative Pebbling Cost cc(G)

Overview

We Are Here

(Parallel) Graph Pebbling.

- Pebbling example
- Cumulative Pebbling Cost of G

Problem Statement.

- Given a DAG G find the (approx.) minimum cost pebbling

Significance of cc(G)**.**

- Analysis of data-independent memory-hard functions
- Amortization / Parallelism

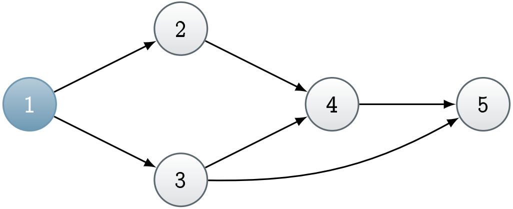
Results.

- Unique Games Hard to approximate cc(G) for any constant factor

Technical Ingredients.

- Indegree reduction using γ-extreme depth robust graphs
- Superconcentrator overlay

(Parallel) Pebbling Example.



$$P_1 = \{1\}$$

(Parallel) Graph Pebbling and Cumulative Pebbling Cost cc(G)

Overview

We Are Here

(Parallel) Graph Pebbling.

- Pebbling example
- Cumulative Pebbling Cost of G

Problem Statement.

- Given a DAG G find the (approx.) minimum cost pebbling

Significance of cc(G)**.**

- Analysis of data-independent memory-hard functions
- Amortization / Parallelism

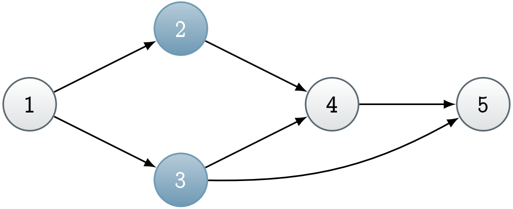
Results.

- Unique Games Hard to approximate cc(G) for any constant factor

Technical Ingredients.

- Indegree reduction using γ-extreme depth robust graphs
- Superconcentrator overlay

(Parallel) Pebbling Example.



$$P_1 = \{1\}, P_2 = \{2, 3\}$$

(Parallel) Graph Pebbling and Cumulative Pebbling Cost cc(G)

Overview

We Are Here

(Parallel) Graph Pebbling.

- Pebbling example
- Cumulative Pebbling Cost of G

Problem Statement.

- Given a DAG G find the (approx.) minimum cost pebbling

Significance of cc(G).

- Analysis of data-independent memory-hard functions
- Amortization / Parallelism

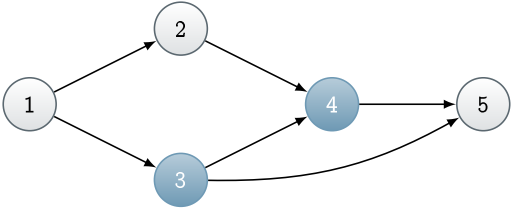
Results.

- Unique Games Hard to approximate cc(G) for any constant factor

Technical Ingredients.

- Indegree reduction using γ-extreme depth robust graphs
- Superconcentrator overlay

(Parallel) Pebbling Example.



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

(Parallel) Graph Pebbling and Cumulative Pebbling Cost cc(G)

Overview

We Are Here

(Parallel) Graph Pebbling.

- Pebbling example
- Cumulative Pebbling Cost of G

Problem Statement.

- Given a DAG G find the (approx.) minimum cost pebbling

Significance of cc(G).

- Analysis of data-independent memory-hard functions
- Amortization / Parallelism

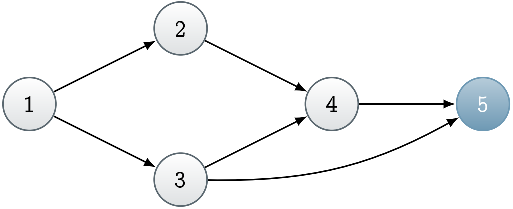
Results.

- Unique Games Hard to approximate cc(G) for any constant factor

Technical Ingredients.

- Indegree reduction using γ-extreme depth robust graphs
- Superconcentrator overlay

(Parallel) Pebbling Example.



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

Overview

We Are Here

(Parallel) Graph Pebbling.

- Pebbling example
- Cumulative Pebbling Cost of G

Problem Statement.

- Given a DAG G find the (approx.) minimum cost pebbling

Significance of cc(G).

- Analysis of data-independent memory-hard functions
- Amortization / Parallelism

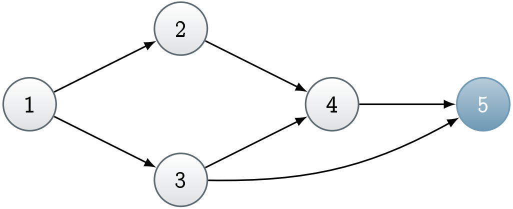
Results.

- Unique Games Hard to approximate cc(G) for any constant factor

Technical Ingredients.

- Indegree reduction using γ-extreme depth robust graphs
- Superconcentrator overlay

(Parallel) Pebbling Example.



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

$$\mathrm{cc}(G) := \min_{P}\{|P_1| + \cdots + |P_t|\}$$

Overview

We Are Here

(Parallel) Graph Pebbling.

- Pebbling example
- Cumulative Pebbling Cost of G

Problem Statement.

- Given a DAG G find the (approx.) minimum cost pebbling

Significance of cc(G)**.**

- Analysis of data-independent memory-hard functions
- Amortization / Parallelism

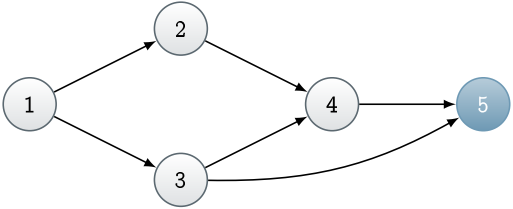
Results.

- Unique Games Hard to approximate cc(G) for any constant factor

Technical Ingredients.

- Indegree reduction using γ-extreme depth robust graphs
- Superconcentrator overlay

(Parallel) Pebbling Example.



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

$$\text{cc}(G) := \min_P \{|P_1| + \cdots + |P_t|\}$$

$$\therefore \text{cc}(G) \le \sum_{i=1}^{t} |P_i| = 1$$

(Parallel) Graph Pebbling and Cumulative Pebbling Cost cc(G)

Overview

We Are Here

(Parallel) Graph Pebbling.

- Pebbling example
- Cumulative Pebbling Cost of G

Problem Statement.

- Given a DAG G find the (approx.) minimum cost pebbling

Significance of cc(G).

- Analysis of data-independent memory-hard functions
- Amortization / Parallelism

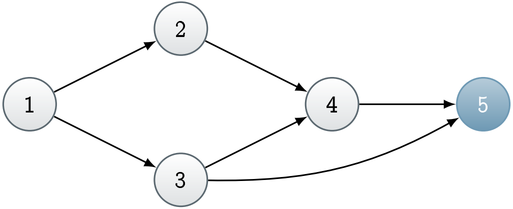
Results.

- Unique Games Hard to approximate cc(G) for any constant factor

Technical Ingredients.

- Indegree reduction using γ-extreme depth robust graphs
- Superconcentrator overlay

(Parallel) Pebbling Example.



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

$$\mathrm{cc}(G) := \min_P \{|P_1| + \cdots + |P_t|\}$$

$$\therefore \mathrm{cc}(G) \le \sum_{i=1}^{t} |P_i| = 1 + 2$$

Overview

We Are Here

(Parallel) Graph Pebbling.

- Pebbling example
- Cumulative Pebbling Cost of G

Problem Statement.

- Given a DAG G find the (approx.) minimum cost pebbling

Significance of cc(G)**.**

- Analysis of data-independent memory-hard functions
- Amortization / Parallelism

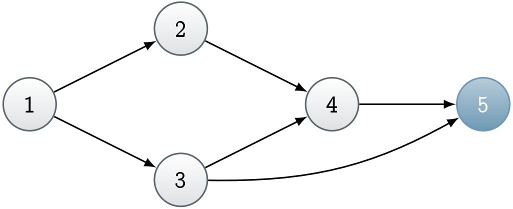
Results.

- Unique Games Hard to approximate cc(G) for any constant factor

Technical Ingredients.

- Indegree reduction using γ-extreme depth robust graphs
- Superconcentrator overlay

(Parallel) Pebbling Example.



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

$$\mathrm{cc}(G) := \min_P \{|P_1| + \cdots + |P_t|\}$$

$$\therefore \mathrm{cc}(G) \le \sum_{i=1}^{t} |P_i| = 1 + 2 + 2$$

Overview

We Are Here

(Parallel) Graph Pebbling.

- Pebbling example
- Cumulative Pebbling Cost of G

Problem Statement.

- Given a DAG G find the (approx.) minimum cost pebbling

Significance of cc(G)**.**

- Analysis of data-independent memory-hard functions
- Amortization / Parallelism

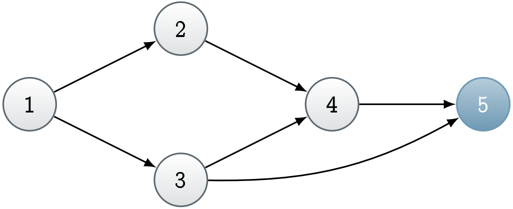
Results.

- Unique Games Hard to approximate cc(G) for any constant factor

Technical Ingredients.

- Indegree reduction using γ-extreme depth robust graphs
- Superconcentrator overlay

(Parallel) Pebbling Example.



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

$$\mathrm{cc}(G) := \min_P \{|P_1| + \cdots + |P_t|\}$$

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

Overview

(Parallel) Graph Pebbling.

- Pebbling example
- Cumulative Pebbling Cost of G

We Are Here

Problem Statement.

- Given a DAG G find the (approx.) minimum cost pebbling

Significance of cc(G)**.**

- Analysis of data-independent memory-hard functions
- Amortization / Parallelism

Results.

- Unique Games Hard to approximate cc(G) for any constant factor

Technical Ingredients.

- Indegree reduction using γ-extreme depth robust graphs
- Superconcentrator overlay

Challenging Problem.

- Given a DAG G, find the (approximately) minimum cost pebbling

Why We Care About cc(G)?

- Analysis of data-independent Memory-Hard Functions (iMHFs)
- [AS15] For a secure iMHF, it suffices to find a DAG G with *constant indegree* and *maximum* cc(G)
- Amortization / Parallelism ($\mathrm{cc}(G^{\times n}) = n \times \mathrm{cc}(G)$)

Challenges.

- We don't know how to compute cc(G) exactly for any given G
- Large gaps between upper/lower bounds for known constructions

Example

DRSample: one practical instantiation of an iMHF

$$\frac{10^{-6} \cdot N^2}{\log N} \le \mathrm{cc}(\mathrm{DRSample}) \le \frac{1 \cdot N^2}{\log N}.$$

Our Main Result: Hardness of Approximating cc(G)

Overview

(Parallel) Graph Pebbling.

- Pebbling example
- Cumulative Pebbling Cost of G

Problem Statement.

- Given a DAG G find the (approx.) minimum cost pebbling

Significance of cc(G)**.**

- Analysis of data-independent memory-hard functions
- Amortization / Parallelism

We Are Here

Results.

- Unique Games Hard to approximate cc(G) for any constant factor

Technical Ingredients.

- Indegree reduction using γ-extreme depth robust graphs
- Superconcentrator overlay

Our Result.

- [BZ18] proved that computing cc(G) is NP-Hard
- This did not rule out the existence of a constant-factor approximation algorithm for cc(G)
- Our result is the hardness of any constant factor approximation to the cost of graph pebbling even for DAGs with constant indegree.

Theorem

Given a DAG G with constant indegree, it is Unique Games hard to approximate cc(G) *within any constant factor.*

Our Main Result: Hardness of Approximating cc(G)

Overview

(Parallel) Graph Pebbling.

- Pebbling example
- Cumulative Pebbling Cost of G

Problem Statement.

- Given a DAG G find the (approx.) minimum cost pebbling

Significance of cc(G).

- Analysis of data-independent memory-hard functions
- Amortization / Parallelism

We Are Here

Results.

- Unique Games Hard to approximate cc(G) for any constant factor

Technical Ingredients.

- Indegree reduction using γ-extreme depth robust graphs
- Superconcentrator overlay

Our Result.

- [BZ18] proved that computing cc(G) is NP-Hard
- This did not rule out the existence of a constant-factor approximation algorithm for cc(G)
- Our result is the hardness of any constant factor approximation to the cost of graph pebbling even for DAGs with constant indegree.

Theorem

Given a DAG G with constant indegree, it is Unique Games hard to approximate cc(G) *within any constant factor.*

Implication.

- Cryptanalysis of iMHFs is Hard!

Technical Ingredients

Overview

(Parallel) Graph Pebbling.

- Pebbling example
- Cumulative Pebbling Cost of G

Problem Statement.

- Given a DAG G find the (approx.) minimum cost pebbling

Significance of cc(G).

- Analysis of data-independent memory-hard functions
- Amortization / Parallelism

Results.

- Unique Games Hard to approximate cc(G) for any constant factor

We Are Here

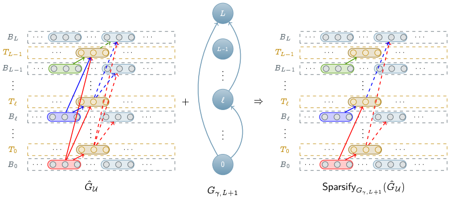
Technical Ingredients.

- Indegree reduction using γ-extreme depth robust graphs
- Superconcentrator overlay

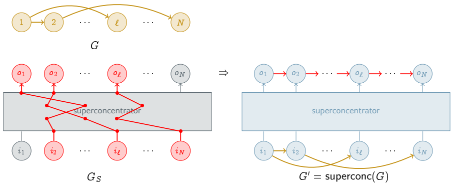
Svensson's Result [Sve12].

- cc(G) is related to the combinatorial property called Depth-Robustness
- Unique Games Hard to approximately test DAGs for Depth-Robustness
  - Challenge 1: Svensson's reduction dœsn't work for constant indegree graphs
  - Challenge 2: Connection between Depth-Robustness and cc(G) is not tight

Indegree Reduction Procedure using γ-Extreme DR Graph $G_{\gamma,L+1}$.



Superconcentrator Overlay.

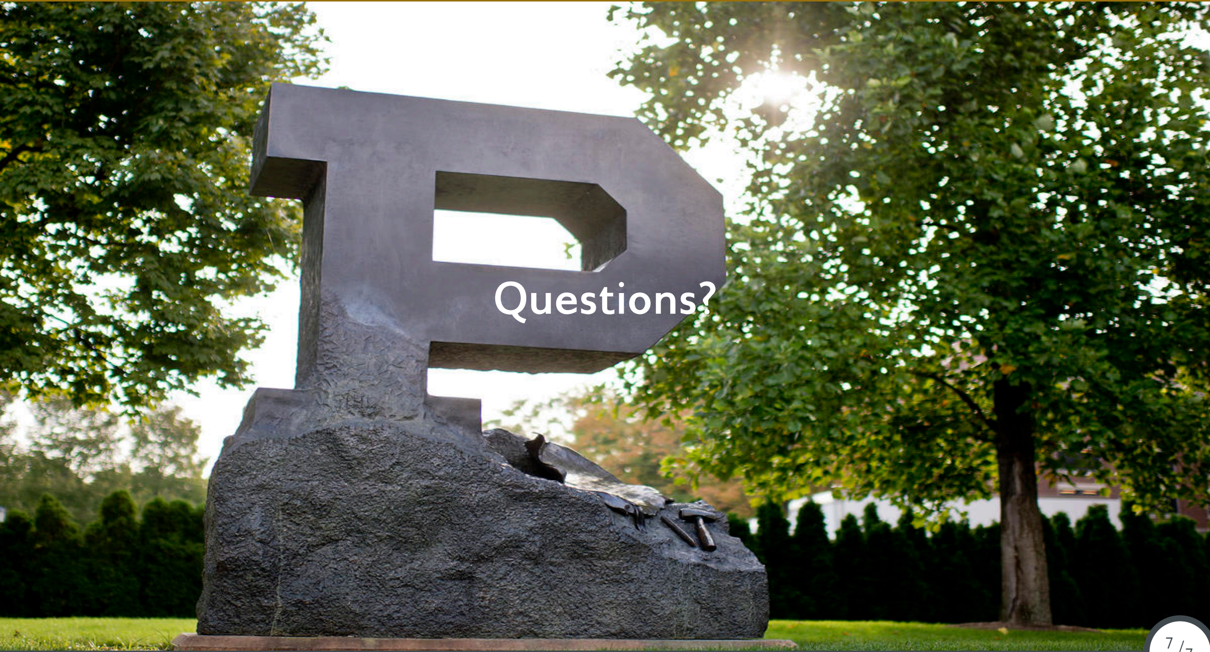


References I

Joël Alwen and Vladimir Serbinenko, *High parallel complexity graphs and memory-hard functions*, 47th ACM STOC (Rocco A. Servedio and Ronitt Rubinfeld, eds.), ACM Press, June 2015, pp. 595–603.

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

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



Questions?