Approximating Cumulative Pebbling Cost is Unique Games Hard

Jeremiah Blocki¹, Seunghoon Lee¹, Samson Zhou²

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

January 12, 2020
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 $\gamma$-extreme depth robust graphs
- Superconcentrator overlay
Overview

(Parallel) Graph Pebbling and Cumulative Pebbling Cost $\text{cc}(G)$

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

Significance of $\text{cc}(G)$.
- Analysis of data-independent memory-hard functions
- Amortization / Parallelism

Results.
- Unique Games Hard to approximate $\text{cc}(G)$ for any constant factor

Technical Ingredients.
- Indegree reduction using $\gamma$-extreme depth robust graphs
- Superconcentrator overlay

(Parallel) Pebbling Example.

\[ P_1 = \{1\} \]
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 $\gamma$-extreme depth robust graphs
- Superconcentrator overlay

(Parallel) Pebbling Example.

$$P_1 = \{1\}, P_2 = \{2, 3\}$$
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 $\gamma$-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 \( \gamma \)-extreme depth robust graphs
- Superconcentrator overlay

(Parallel) Pebbling Example.

\[
P_1 = \{1\}, P_2 = \{2, 3\}, P_3 = \{3, 4\}, P_4 = \{5\}
\]
Overview

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

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 $\gamma$-extreme depth robust graphs
- Superconcentrator overlay

(Parallel) Pebbling Example.

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

$$cc(G) := \min_P \{|P_1| + \cdots + |P_4|\}$$
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 $\gamma$-extreme depth robust graphs
- Superconcentrator overlay

(Parallel) Pebbling Example.

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

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

$$\therefore \text{cc}(G) \leq \sum_{i=1}^{t} |P_i| = 1$$
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 $\gamma$-extreme depth robust graphs
  - Superconcentrator overlay

(Parallel) Pebbling Example.

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

\[ cc(G) := \min_P \left\{ |P_1| + \cdots + |P_t| \right\} \]

\[ \therefore cc(G) \leq \sum_{i=1}^{t} |P_i| = 1 + 2 \]
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 $\gamma$-extreme depth robust graphs
- Superconcentrator overlay

(Parallel) Pebbling Example.

```
\begin{align*}
P_1 &= \{1\}, P_2 = \{2, 3\}, P_3 = \{3, 4\}, P_4 = \{5\} \\
cc(G) &= \min_{P} \{|P_1| + \cdots + |P_t|\} \\
\therefore cc(G) &\leq \sum_{i=1}^{t} |P_i| = 1 + 2 + 2
\end{align*}
```
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 $\gamma$-extreme depth robust graphs
- Superconcentrator overlay

(Parallel) Pebbling Example.

![Graph Diagram]

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

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

$\therefore cc(G) \leq \sum_{i=1}^{t} |P_i| = 1 + 2 + 2 + 1 = 6.$
Significance of \( cc(G) \) and a Challenging Problem

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 \( \gamma \)-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 (\( cc(G^n) = n \times cc(G) \))

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

\[
\frac{10^{-6} \cdot N^2}{\log N} \leq cc(DRSample) \leq \frac{1}{\log N} \cdot N^2.
\]
Our Main Result: Hardness of Approximating $\text{cc}(G)$

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 $\text{cc}(G)$.
- Analysis of data-independent memory-hard functions
- Amortization / Parallelism

We Are Here

Results.
- Unique Games Hard to approximate $\text{cc}(G)$ for any constant factor

Technical Ingredients.
- Indegree reduction using $\gamma$-extreme depth robust graphs
- Superconcentrator overlay

Our Result.
- [BZ18] proved that computing $\text{cc}(G)$ is NP-Hard
- This did not rule out the existence of a constant-factor approximation algorithm for $\text{cc}(G)$
- 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 $\text{cc}(G)$ 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 $\gamma$-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!
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 $\gamma$-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 doesn’t work for constant indegree graphs
  - Challenge 2: Connection between Depth-Robustness and $cc(G)$ is not tight

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

Superconcentrator Overlay.
References

