A New Connection Between Node and Edge Depth Robust Graphs

Jeremiah Blocki, Mike Cinkoske

October 22, 2019

Abstract

We create a graph reduction that transforms an \((e, d)\)-edge-depth-robust graph with \(m\) edges into a \((e/4, d)\)-depth-robust graph with \(O(m)\) nodes and constant indegree. An \((e, d)\)-depth robust graph is a directed, acyclic graph with the property that that after removing any \(e\) nodes of the graph there remains a path with length at least \(d\). Similarly, an \((e, d)\)-edge-depth robust graph is a directed, acyclic graph with the property that after removing any \(e\) edges of the graph there remains a path with length at least \(d\). Our reduction relies on constructing graphs with a property we define and analyze called ST-Robustness. We say that a directed, acyclic graph with \(n\) inputs and \(n\) outputs is \((k_1, k_2)\)-ST-Robust if we can remove any \(k_1\) nodes and there exists a subgraph containing at least \(k_2\) inputs and \(k_2\) outputs such that each of the \(k_2\) inputs is connected to all of the \(k_2\) outputs. We use our reduction on a well known edge-depth-robust graph to construct an \(\left\lfloor \frac{n \log \log n}{\log n} \right\rfloor, \frac{n \log \log n}{\log n} (\log \log n)\)-depth-robust graph.

1 Introduction

Given a directed acyclic graph (DAG) \(G = (V, E)\), we say that \(G\) is \((e, d)\)-depth-robust, where \(\text{depth}(G)\) is the length of the longest directed path in \(G\), if for any set \(S \subseteq V\) of nodes with \(|S| \leq e\) we have that \(\text{depth}(G - S) \geq d\). Similarly, we say that \(G\) is \((e, d)\)-edge-depth-robust if for any set \(S \subseteq E\) with \(|S| \leq e\) we have that \(\text{depth}(G - S) \geq d\). Depth robust graphs are used in the construction of proof of sequential work and proof of space schemes \cite{MMV13}, and in the construction of data independent memory hard functions (iMHFs). Highly depth robust graphs are known to be necessary \cite{ABI16} and sufficient \cite{ABP17} to construct iMHF’s with high amortized space time complexity. It has been shown \cite{Val77} that in any DAG
with \( m \) edges and \( n \) nodes, there exists a set \( S_i \) of \( \frac{m_i}{\log n} \) edges that will force \( \text{depth}(G - S_i) \leq \frac{n}{2} \) for all \( i < \log n \). In many contexts, it is required that the depth robust graph have constant indegree. For constant indegree DAG’s, \( m = O(n) \), so an equivalent condition holds for node depth robustness, since a node can be removed by removing all the edges incident to it. In particular, there exists a set \( S_i \) of \( O\left(\frac{n_i}{\log n}\right) \) nodes such that \( \text{depth}(G - S_i) \leq \frac{n}{2^i} \) for all \( i < \log n \).

A general goal of constructing depth-robust graphs is to construct depth robust graphs that match the Valient bound for each \( i \). It is known how to construct an \((c_1 n/\log n, c_2 n)\)-depth-robust graph, for suitable \( c_1, c_2 > 0 \) \cite{ABP17}, and an \((c_3 n, c_4 n^{1-\epsilon})\)-depth-robust graph for small \( \epsilon \) for \cite{Sch83}, however it is currently an open question whether or not there exists maximally depth robust graphs with constant indegree for \( i = \log \log n \).

**Open Question:** Does there exist a constant indegree \((\frac{n \log \log n}{\log n}, \frac{n}{\log n})\)-depth-robust graph?

### 1.1 Results

Our main contribution is introducing a graph reduction that transforms a \((e, d)\)-edge-depth-robust graph with \( m \) edges into a \((e/4, d)\)-depth-robust graph with \( O(m) \) nodes and constant indegree. A previous reduction \cite{ABP17} operated on a \((e, d)\)-node-depth-robust graph with indegree \( f(n) \), transforming into a \((c' e, d \cdot f(n))\)-node-depth-robust graph with \( O(n \cdot f(n)) = O(m) \) nodes and constant indegree.

Our reduction relies on the existence of ST-Robust graphs, a new graph property we introduce. We say that a constant indegree DAG \( G = (V, E) \) is \((k_1, k_2)\)-ST-robust if \( G \) has \( n \) inputs, denoted by set \( I \), and \( n \) outputs, denoted by set \( O \), such that for all \( D \subset V(G) \) with \( |D| \leq k_1 \), there exists subgraph \( H \) of \( G - D \) with \( |I \cap V(H)| \geq k_2 \) and \( |O \cap V(H)| \geq k_2 \) such that for all \( s \in I \cap V(H) \) and \( t \in O \cap V(H) \) there exists a path from \( s \) to \( t \) in \( H \). We say that a graph with \( n \) nodes is \( c_1 \)-maximally ST-robust if there exists a constant \( c_1 \) such that \( G \) is \((k, n - k)\)-ST robust for all \( 0 \leq k \leq c_1 n \). We show that linear size, constant indegree, maximally ST-robust graphs exist for certain parameters, and that the existence of these ST-robust graphs can be used to show the correctness of our reduction.

**Definition 1.1. ST-Robust** Let \( G = (V, E) \) be a DAG with \( n \) inputs, denoted by set \( I \) and \( n \) outputs, denoted by set \( O \). Then \( G \) is \((k_1, k_2)\)-ST-robust if for all \( D \subset V(G) \) with \( |D| \leq k_1 \), there exists subgraph \( H \) of \( G - D \) with \( |I \cap V(H)| \geq k_2 \) and \( |O \cap V(H)| \geq k_2 \) such that for all \( s \in I \cap V(H) \) and
∀t ∈ O ∩ V(H) there exists a path from s to t in H. If ∀s ∈ I ∩ V(H) and ∀t ∈ O ∩ V(H) there exists a path from s to t of length ≥ d then we say that G is (k_1, k_2, d)-ST-robust.

**Definition 1.2. Maximally ST-Robust** Let G = (V, E) be a constant indegree DAG with n inputs and n outputs. Then G is c_1-max ST-robust (resp. c_1 max ST-robust with depth d) if there exists a constant 0 < c_1 ≤ 1 such that G is (k, n − k)-ST-robust (resp. (k, n − k, d)-ST-robust) for all k with 0 ≤ k ≤ c_1n. If c_1 = 1, we just say that G is max ST-Robust.

The reduction can be used with a construction from [Sch83] to construct a (n log log n, n / log log n)-depth-robust graph. We conjecture that the edge-depth-robust graph from [EGS75] is (n log log n, n / log n)-edge-depth-robust where applying the reduction would construct the desired (n log log n, n / log n)-depth-robust graph.

## 2 General Theorem

In this section, we assume the existence of linear sized, constant indegree, maximally ST-robust graphs and use this assumption to construct a transformation of an (e,d)-edge-depth robust graph with m edges into an (e,d)-node-depth robust graph with constant indegree and O(m) nodes.

**Assumption 2.1.** There is a family of graphs \( \mathcal{M} = \{ M_n \}_{n=1}^{\infty} \) with the property that for each \( n \geq 1 \), \( M_n \) has constant indegree, \( O(n) \) nodes, and is maximally ST-Robust.

### 2.1 Reduction Definition

Let \( G = (V, E) \) be a DAG, and let \( \mathcal{M} \) be as in Assumption 2.1. Then we define \( \text{Reduce}(G, \mathcal{M}) \) in construction 2.2 as follows:

**Construction 2.2 (Reduce(G, \mathcal{M})).** Let \( G = (V, E) \) and let \( \mathcal{M} \) be the family of graphs defined above. For each \( M_n \in \mathcal{M} \), we say that \( M_n = (V(M_n), E(M_n)) \), with \( V(M_n) = I(M_n) \cup O(M_n) \cup D(M_n) \), where \( I(M_n) \) are the inputs of \( M_n \), \( O(M_n) \) are the outputs, and \( D(M_n) \) are the internal vertices. For \( v \in V \), let \( \delta(v) = \max \{ \text{indegee}(v), \text{outdegree}(v) \} \). Then we define \( \text{Reduce}(G) = (V_R, E_R) \), where \( V_R = \{ (v, w) | v \in V, w \in V_{\delta(v)} \} \) and \( E_R = E_{\text{internal}} \cup E_{\text{external}} \). We let \( E_{\text{internal}} = \{ ((v, u_{\delta(v)}), (v, w_{\delta(v)})) | v \in V, (u_{\delta(v)}, w_{\delta(v)}) \in E(H_{\delta(v)}) \} \). Then for each \( v \in V \), we define an \( \text{In}(v) = \{ u : (u, v) \in E \} \) and \( \text{Out}(v) = \{ u : (v, u) \in E \} \) and then pick two injective
mappings \( \pi_{in,v} : In(v) \rightarrow I(V_{\delta(v)}) \) and \( \pi_{out,v} : Out(v) \rightarrow O(V_{\delta(v)}) \). We let \( E_{external} = \{(u, \pi_{out,u}(v)), (v, \pi_{in,v}(u)) : (u, v) \in E\} \).

Intuitively, to construct \( \text{Reduce}(G, \mathcal{M}) \) we replace every node of \( G \) with a constant indegree, maximally ST-robust graph, mapping the edges connecting two nodes from the outputs of one ST-robust graph to the inputs of another. Then for every \( e = (u, w) \in E \), add an edge from an output of \( M_{\delta(u)} \) to an input of \( M_{\delta(w)} \) such that the outputs of \( M_{\delta(u)} \) have outdegree at most 1, and the inputs of \( M_{\delta(w)} \) have indegree at most 1. If \( v \in V \) is replaced by \( M_{\delta(v)} \), then we call \( v \) the genesis node and \( M_{\delta(v)} \) its metanode.

\[ v_k \quad v_i \quad v_{i+1} \quad v_{i+2} \quad v_j \quad v_{j+1} \]

\[ \cdots \quad M_k \quad \cdots \quad M_i \quad \cdots \quad M_{i+1} \quad \cdots \quad M_{i+2} \quad \cdots \quad M_j \quad \cdots \quad M_{j+1} \quad \cdots \]

Figure 1: Diagram of the transformation \( \text{Reduce}(G, \mathcal{M}) \)

### 2.2 Proof of Main Theorem

We now prove the main result of this section.

**Theorem 2.3.** Let \( G \) be an \((e, d)\)-edge-depth-robust DAG with \( m \) edges. Let \( \mathcal{M} \) be a family of max ST-Robust graphs with constant indegree. Then \( G' = (V', E') = \text{Reduce}(G, \mathcal{M}) \) is \((e/4, d)\)-depth robust. Furthermore, \( G' \) has maximum indegree \( \max_{v \in V(G)} \{\text{indeg}(M_{\delta(v)})\} \), and its number of nodes is \( \sum_{v \in V(G)} |M_{\delta(v)}| \) where \( \delta(v) = \max\{\text{indeg}(v), \text{outdeg}(v)\} \).

**Proof.** We know that each graph in \( \mathcal{M} \) has constant indegree, and that each node \( v \) in \( G \) will be replaced with a graph in \( \mathcal{M} \) with indegree \( \text{indeg}(M_{\delta(v)}) \). Thus \( G' \) has maximum indegree \( \max_{v \in V(G)} \{\text{indeg}(M_{\delta(v)})\} \). Furthermore,
the metanode corresponding to the node \( v \) has size \( |M_{\delta(v)}| \). Thus \( G' \) has 
\[
\sum_{v \in V(G)} |M_{\delta(v)}| \text{ nodes.}
\]

Let \( S \subset V(G') \) be a set of nodes that we will remove from \( G' \). We say that a node \( v \in V(G) \) is \textit{irrepairable} with respect to \( S \) if \( |S \cap \{v\} \times V_{\delta(v)}| \geq c_1 \delta(v) \). If a node \( v \) is repairable, then because the metanodes are maximally ST-Robust we can find subsets \( I_{v,S} \) and \( O_{v,S} \) such that each \( s \in I_{v,S} \) is connected to every node in \( O_{v,S} \). We say a node \( v \in V(G) \) is \textit{irrepairable} if \( |S \cap \{v\} \times V_{\delta(v)}| \geq c_1 \delta(v) \).

Claim 2.4. Let \( P \) be a path of length \( d \) in \( G - S_{irr} \). Then there exists a path of length \( d \) in \( G' - S \).

\textbf{Proof.} In \( G - S_{irr} \) we have removed all of the irreparable edges, so any path in the graph contains only repairable edges. By definition, if \( (u, v) \) is a repairable edge, both \( u \) and \( v \) will be repairable, and \( (u, \pi_{out,u}(v)) \in O_{u,S} \) and \( (v, \pi_{in,v}(u)) \in I_{v,S} \). Thus the edge corresponding to \( (u, v) \) in \( G' - S \) will connect the metanodes of \( u \) and \( v \), and \( (u, \pi_{out,u}(v)) \) connects to every node in \( I_{u,S} \) and \( (v, \pi_{in,v}(u)) \) connects to every node in \( O_{v,S} \). Thus the edges in \( G' - S \) corresponding to the edges in \( P \) form a path of length \( d \).

\textbf{Claim 2.5.} Let \( S_{irr} \subset E(G) \) be the set of irreparable edges with respect to the removed set \( S \). Then
\[
|S_{irr}| \leq 4|S|.
\]

\textbf{Proof.} When we remove a node from a metanode, we make at most two edges irreparable because the metanodes are maximally ST-robust. But when we remove at least \( \delta(v) \) nodes from the metanode associated to \( v \), we remove the whole metanode and make all of its edges irreparable, which is at most \( 2\delta(v) \) edges. We know that
\[
\sum_{v \text{ irrep.}} \delta(v) \leq |S|
\]

Thus
\[
|S_{irr}| \leq \sum_{v \text{ irrep.}} 2\delta(v) + \sum_{v \text{ rep.}} 2|S \cap \{v\} \times V_{\delta(v)}| 
\]
\[
\leq 2|S| + 2|S| = 4|S|.
\]

\( \square \)
Now suppose that $|S| \leq \frac{\epsilon}{4}$. Then by Claim 2.5 we know that $|S_{irr}| \leq \epsilon$. Since $G$ is $(e,d)$-edges-depth-robust, there exists a path $P$ in $G - S_{irr}$ of length at least $d$. Then by Claim 2.4 the path $P$ corresponds to a path of length at least $d$ in $G' - S$. Thus $G'$ is $(\frac{\epsilon}{4},d)$-depth-robust. \hfill \square

Corollary 2.6. (of Theorem 2.3) If there exists some constants $c_1, c_2$, such that we have a family $\mathcal{M} = \{M_n\}_{n=1}^{\infty}$ of linear sized $|V(M_n)| \leq c_1n$, constant indegree $\operatorname{indeg}(M_n) \leq c_2$, and maximally ST-Robust graphs, then Reduce($G, \mathcal{M}$) has maximum indegree $c_2$ and the number of nodes is at most $2c_1m$.

Corollary 2.7. (of Theorem 2.4) Suppose that there exists a family $\mathcal{M} = \{M_k\}_{k=1}^{\infty}$ of max ST-Robust graphs with depth $d_k$ and constant indegree. Given any $(e,d)$-edge-depth-robust DAG $G$ with $n$ nodes and maximum indegree $\delta$ we can construct a DAG $G'$ with $n \times |M_\delta|$ nodes and constant indegree that is $(e/4,d \cdot d_\delta)$-depth robust.

Proof. (sketch) Instead of replacing each node $v \in G$ with a copy of $M_{\delta(v)}$, we instead replace each node with a copy of $M_{\delta}$, attaching the edges same way as in Construction 2.2. Thus the transformed graph $G'$ has $|V(G)| \times |M_\delta|$ nodes and constant indegree. Let $S \subset V(G')$ be a set of nodes that we will remove from $G'$. By Claim 2.4 there exists a path $P$ in $G' - S$ that passes through $d$ metanodes $M_{\delta,v_1}, \ldots, M_{\delta,v_d}$. Since $M_{\delta}$ is maximally ST-robust with depth $d_\delta$, the sub-path $P_i = P \cap M_{\delta,v_i}$ through each metanode has length $|P_i| \geq d_\delta$. Thus, the total length of the path is at least $\sum |P_i| \geq d \cdot d_\delta$. \hfill \square

Corollary 2.8. (of Theorem 2.3) Let $\epsilon > 0$ be any fixed constant. Given any family $\{G_m\}_{m=1}^{\infty}$ of $(e_m,d_m)$-edge-depth-robust DAGs $G_m$ with $m$ nodes and maximum indegree $\delta_m$ then for some constants $c_1, c_2 > 0$ we can construct a family $\{H_m\}_{m=1}^{\infty}$ of DAGs such that each DAG $H_m$ is $(e_m/4, d_m \cdot \delta_m^{1-\epsilon})$-depth robust, $H_m$ has maximum indegree at most $c_2$ (constant) and at most $|V(H_m)| \leq c_1m\delta_m$ nodes.

Proof. (sketch) This follows immediately from Corollary 2.7 and from our construction of a family $\mathcal{M}_\epsilon = \{M_{k,\epsilon}\}_{k=1}^{\infty}$ of max ST-Robust graphs with depth $d_k > k^{1-\epsilon}$ and constant indegree. \hfill \square

Corollary 2.9. (of Theorem 2.3) Let $\{e_m\}_{m=1}^{\infty}$ and $\{d_m\}_{m=1}^{\infty}$ be any sequence. If there exists a family $\{G_m\}_{m=1}^{\infty}$ of $(e_m,d_m)$-edge-depth-robust graphs, where each DAG $G_m$ has $m$ edges, then there is a corresponding family $\{H_n\}_{n=1}^{\infty}$ of constant indegree DAGs such that each $H_n$ has $n$ nodes and is $(\Omega(e_n), \Omega(d_n))$-depth-robust.
We know that the original Grate’s construction \cite{Sch83}, $G$, has $N = 2^n$ nodes and $m = n2^n$ edges and for any $s \leq n$, and is $(s2^n, \sum_{j=0}^{N} \binom{N}{j})$-edge-depth-robust. Then setting $s = \log \log n$ and applying the indegree reduction from Theorem 2.3, we see that the transformed graph $G'$ has constant indegree, $N' = O(n2^n)$ nodes, and is $(N' \log N', \log N'/(\log N' \log \log N'))$-depth-robust. Blocki et al. \cite{BHK+19} showed that if there exists a node depth robust graph with $e = \Omega(N \log \log N / \log N)$ and $d = \Omega(N \log \log N / \log N)$ then one can obtain another constant indegree graph with pebbling cost $\Omega(N^2 \log \log N / \log N)$ which is optimal for constant indegree graphs. We conjecture that the graphs in \cite{EGS75} are sufficiently edge depth robust to meet these bounds after being transformed by our reduction.

3 ST Robustness

Recall the definition of ST-robust graphs in Definition 1.1. This definition is motivated by previous degree reductions which replaced nodes with other graphs to create metanodes. Previous degree reductions replaced nodes with paths to create metanodes, and removed the entire metanode when one vertex inside it was removed. If ST-robust graphs are used instead, then multiple nodes can be removed from a metanode and the metanode will remain somewhat connected. Note that the set $D$ could consist of only inputs or only outputs, in which case $k_2 \leq n - k_1$. Thus we always have $k_1 + k_2 \leq n$. The key question is whether or not maximally ST-robust graphs with constant indegree exists with a linear number of nodes.

We now introduce other graph properties that will be useful for studying ST-robust graphs. We say that a directed acyclic graph $G = (V, E)$ with $n$ input vertices and $n$ output vertices is an $n$-superconcentrator if for any $r$ inputs and any $r$ outputs, $1 \leq r \leq n$, there are $r$ vertex-disjoint paths in $G$ connecting the set of these $r$ inputs to these $r$ outputs. We note that there exists linear size, constant indegree superconcentrators \cite{Val76,Pip77,GG81} and we use this fact throughout the rest of the paper. For example, Pippenger \cite{Pip77} constructed an $n$-superconcentrator with at most $41n$ vertices and indegree at most 16. Additionally, we say that an $n$-superconcentrator is an $n$-connector if it is possible to specify which input is to be connected to which output by vertex disjoint paths in the subsets of $r$ inputs and $r$ outputs. Connectors and superconcentrators are potential candidates for ST-robust graphs because of their highly connective properties. In fact, we can prove that connectors are maximally ST-robust using their selection property.
Theorem 3.1. If $G$ is an $n$-connector, then $G$ is $(k, n - k)$-ST-robust, for all $1 \leq k \leq n$.

A well known family of constant indegree $n$-connectors, for $n = 2^k$, are the $k$-dimensional butterfly graphs $B_k$, which are formed by connecting two FFT graphs on $n$ inputs back to back. See Figure 3 for an example. We provide a proof showing they are $n$-connectors in the appendix for completeness.

![Figure 2: The butterfly graph $B_3$ is both an 8-superconcentrator and an 8-connector. All edges are directed from left to right.](image)

Theorem 3.2. For $n = 2^k$, the $k$-dimensional butterfly graph $B_k$ is an $n$-connector.

Thus by Theorem 3.1, $B_n$ is a maximally ST-robust graph. Since $B_k$ has $O(n \log n)$ vertices and indegree of 2, a natural question to ask is if there exists $n$-connectors with $O(n)$ vertices and constant indegree. Unfortunately, Shannon [Sha50] studied constant indegree connectors in the context of telephone networks and showed that

Theorem 3.3. (Shannon) An $n$-connector with constant indegree requires at least $\Omega(n \log n)$ vertices.

Thus if we are constructing ST-robust graphs using connectors, $B_k$ is the best we can do up to constant factors.
4 Linear Size ST-robust Graphs

ST-robust graphs have similar connective properties to connectors, so a natural question to ask is whether ST-robust graphs with constant indegree require $\Omega(n \log n)$ vertices. In this section, we show that linear size ST-robust graphs exist by showing that a modified version of the Grates construction [Sch83] is maximally ST-robust for certain parameters.

In the proof of Theorem A in [Sch83], Schnitger constructs a family of DAGs ($H_n | n \in N$) with constant indegree $\delta_H$, where $n$ is the number of nodes and $H_n$ is $(cn, n^{2/3})$-depth-robust, for suitable constant $c > 0$. We construct a similar graph $G_n$ as follows: Let $H^1_n$ and $H^2_n$ be isomorphic copies of $H_n$ with disjoint vertex sets $V_1$ and $V_2$. For each vertex $u \in V_1$, connect $u$ to $\tau$ vertices in $H^1_n$ chosen uniformly and independently at random. Note that Schnitger’s construction makes the connections between $H^1_n$ and $H^2_n$ using random permutations instead of picking the edges uniformly, and this is the only difference between our constructions. Let $S$ be a fixed set of $cn/2$ vertices of $G_n$. For a graph $G = (V, E)$ and a subset $T$ of $V$, we set $G - T$ to be the induced subgraph of $V - T$. We will use the following lemma from the Grates paper. A proof is included for completeness.

**Lemma 4.1.** $H^1_n - S$ contains $k = cn^{1/3}/2$ vertex disjoint paths $A_1, \ldots, A_k$ of length $n^{2/3}$ and $H^2_n - S$ contains $k$ vertex disjoint paths $B_1, \ldots, B_k$ of the same length.

**Proof.** Consider $H^1_n - S$. Since $H^1_n$ is $(cn, n^{2/3})$-depth-robust and $|S| = cn/2$, there must exist a path $A_1 = (v_1, \ldots, v_{n^{2/3}})$ in $H^1_n - S$. Remove all vertices of $A_1$ and repeat to find $A_2, \ldots$. Then we finish with $cn/(2n^{2/3}) = cn^{1/3}/2$ vertex disjoint paths of length $n^{2/3}$. We perform the same process on $H^2_n$ to find the $B_i$.

We now define upper and lower vertices of a path $A_i$. We call $v$ an upper vertex of $A_i$, or in the upper part of $A_i$ if $A_i = (x_1, \ldots, x_{n^{2/3}}/2, \ldots, v, \ldots, x_{n^{2/3}})$. Similarly, we call $v$ a lower vertex of $A_i$ if $A_i = (x_1, \ldots, v, \ldots, x_{n^{2/3}}/2, \ldots, x_{n^{2/3}})$. We define upper and lower vertices analogously for $B_i$. We will now show that with a high probability, the $A_i$’s and $B_j$’s are highly connected.

**Lemma 4.2.** Let $G_n$ be defined as above, with $\tau$ edges added from each vertex in $H^1_n$ to vertices in $H^2_n$ chosen uniformly at random. Then for some constant $c$, with high probability $G_n$ has the property that for all $S \subset V(G_n)$ with $|S| = cn/2$ there exists $A \subseteq V(H^1_n)$ and $B \subseteq V(H^2_n)$ such that for every pair of nodes $u \in A$ and $v \in B$ the graph $G_n - S$ contains a path from $u$ to $v$ and $|A|, |B| \geq cn$.  

9
Proof. By Lemma 4.1, we know that in \( G_n - S \) there exists \( cn^{1/3}/2 \) vertex disjoint paths \( A_1, \ldots, A_{cn^{1/3}/2} \) in \( H_1^n \) of length \( n^{2/3} \) and \( cn^{1/3}/2 \) vertex disjoint paths \( B_1, \ldots, B_{cn^{1/3}/2} \) in \( H_2^n \) of length \( n^{2/3} \). Let \( U_{j,S}^i \) be the upper half of the \( j \)-th path in \( H_1^n \) and \( L_{j,S}^i \) be the lower half, both of which are relative to the fixed removed set \( S \). Consider, for the sake of finding the probabilities, that \( S \) is fixed before all of the random edges are added to \( G_n \).

First we consider the probability that a single upper path, say \( U_{j,S}^1 \), is disconnected from a single lower path, say \( L_{j,S}^2 \). There are \( n^{1/3} \) possible lower parts to connect to, and there are \( n^{2/3}/2 \) nodes in the upper part that can connect to the lower part, and there are \( \tau \) random edges added from each node in the upper part, so we have that

\[
P\left[U_{1,S}^1 \text{ disconnected from } L_{1,S}^2\right] \leq \left(1 - \frac{1}{2n^{1/3}}\right)^{\tau n^{2/3}/2} \leq \left(\frac{1}{e}\right)^{\tau n^{1/3}}.
\]

We now let \( k = cn^{1/3}/2 \) and define the events

\[
BAD_{i,S}^{\text{upper}} := |\{ j : U_{j,S}^1 \text{ disconnected from } L_{i,S}^2 \}| > \frac{k}{10}
\]

\[
BAD_{i,S}^{\text{upper}} := |\{ j : BAD_{j,S}^{\text{upper}} \}| > \frac{k}{10}.
\]

The event \( BAD_{i,S}^{\text{upper}} \) occurs when more than a small fraction of \( U_{j,S}^1 \) are disconnected from \( L_{i,S}^2 \), and \( BAD_{i,S}^{\text{upper}} \) occurs when more than a small fraction of \( BAD_{i,S}^{\text{upper}} \) occur. We will bound these probabilities, then take a union bound over all possible \( S \) to show our desired result. We see that

\[
P\left[BAD_{i,S}^{\text{upper}}\right] \leq \left(\frac{k}{k/10}\right)P\left[U_{1,S}^1 \text{ disc. } L_{i,S}^2, \ldots, U_{k/10,S}^1 \text{ disc. } L_{i,S}^2\right]
\]

\[
= \left(\frac{k}{k/10}\right)\left(1 - \frac{1}{2n^{1/3}}\right)^{\tau n^{2/3}/2 \cdot k/10} \leq \left(\frac{k}{k/10}\right)\left(\frac{1}{e}\right)^{\tau n^{1/3} \cdot k/10},
\]
and that
\[
\mathbb{P}[BAD_{S}^{\text{upper}}] \leq \left( \frac{k}{k/10} \right)^{k/10} \mathbb{P}[BAD_{1,S}^{\text{upper}}, \ldots, BAD_{k/10,S}^{\text{upper}}] \\
\leq \left( \frac{k}{k/10} \right)^{k/10} \mathbb{P}[BAD_{1,S}^{\text{upper}}]^{k/10} \\
\leq \left( \frac{k}{k/10} \right)^{k/10+1} \left( \frac{1}{e} \right)^{\frac{k}{10}n^{1/3}} \\
= \left( \frac{k}{k/10} \right)^{k/10+1} \left( \frac{1}{e} \right)^{\frac{k}{10}n^{1/3}}.
\]

Next we select \( \tau \) such that \( \left( \frac{1}{e} \right)^{k/10} \tau^{n/3} \cdot 2^k \leq 1 \), then we have that \( \left( \frac{k}{k/10} \right)^{k/10} \tau^{n/3} \leq \left( \frac{1}{e} \right)^{k/20} \tau^{n/3} \). Then substituting into the bounds above, we have that
\[
\mathbb{P}[BAD_{S}^{\text{upper}}] \leq \left( \frac{k}{k/10} \right)^{k/10+1} \left( \frac{1}{e} \right)^{\frac{k}{20}n^{1/3}} \\
\leq \left( \frac{k}{k/10} \right)^{k/10+1} \left( \frac{1}{e} \right)^{\gamma}, \text{ for } \gamma = \frac{800}{c^2}.
\]

Finally, we take the union bound over every possible \( S \) to get
\[
\mathbb{P}[\exists S \text{ s.t. } BAD_{S}^{\text{upper}}] \leq 2^n \mathbb{P}[BAD_{S}^{\text{upper}}] \leq 2^n \left( \frac{1}{e} \right)^{10n} \ll 1.
\]

Therefore, with high probability, there exists sets \( A \) in \( H_1^n \) and \( B \) in \( H_2^n \) with \( |A|, |B| \geq \frac{9}{10}k^{2/3} = \frac{9}{20}cn \) such that every node in \( A \) connects to every node in \( B \).

Now that we have proved Lemma 4.2, we can use \( G_n \) to construct linear sized, constant indegree ST-robust graphs.

**Construction 4.3** (\( M_n \)). We construct the family of graphs \( M_n \) as follows: Let the graphs \( SC_1^n \) and \( SC_2^n \) be linear sized \( n \)-superconcentrators with constant indegree \( \delta_{SC} \) [Pip77], and let \( H_1^n \) and \( H_2^n \) be defined and connected as in \( G_n \), where every output of \( SC_1^n \) is connected to a node in \( H_1^n \), every node of \( H_2^n \) is connected to an input of \( SC_2^n \), and every node in \( H_2^n \) connects to \( \tau \) random nodes in \( H_2^n \). Then \( M_n \) has indegree \( \delta = \max\{\tau, \delta_H, \delta_{SC}\} \).
Theorem 4.4. There exists a constant $c' > 0$ such that for all sets $S \subset V(M_n)$ with $|S| \leq c'n$, $M_n$ is $(|S|, n - |S|)$-ST robust, with $n$ inputs and $n$ outputs and constant indegree.

Proof. Let $c' = 9c/40$, where $c$ is the constant from $G_n$. Consider $M_n - S$. Then because $|S \cap (H^1_n \cup H^2_n)| \leq |S| \leq cn$, by Lemma 4.2 with a high probability there exists sets $A$ in $H^1_n$ and $B$ in $H^2_n$ with $|A|, |B| \geq \frac{9}{10}n^{2/3} = \frac{9}{40}cn$, such that every node in $A$ connects to every node in $B$. By the properties of superconcentrators, the size of the bad set of inputs that can’t reach good outputs of $SC^1_n$ is at most $|S|$, so at least $n - |S|$ outputs of $SC^1_n$ are reachable from its inputs. Similarly, at least $n - |S|$ outputs of $SC^2_n$ are reachable from its inputs. Thus at least $n - |S|$ inputs of $M_n$ can reach at least $n - |S|$ outputs of $M_n$. Therefore $M_n$ is $(|S|, n - |S|)$-ST robust. \qed

Corollary 4.5. (of Theorem 4.4) For all $\epsilon > 0$, there exists a family of DAGs $M = \{M^\epsilon_n\}_{n=1}^\infty$, where each $M^\epsilon_n$ is a $c$-maximally ST-robust graphs with $|V(M_n)| \leq c\epsilon n$, indegree $(M_n) \leq c\epsilon$, and depth $d = n^{1-\epsilon}$.

Proof. (sketch) In the proof of Lemma 4.1, we used $(cn, n^{2/3})$-depth robust graphs. When considering the paths $A_i$ and $B_j$, we were considering connecting the upper half of one path to the lower half of another. Thus, after we remove nodes from $M_n$, there exists a path of length at least $n^{2/3}$ that connects any remaining input to any remaining output. Thus $M_n$ is $c$-maximally ST-robust with depth $d = n^{2/3}$. In [Sch83], Schnitger provides a construction that is $(cn, n^{1-\epsilon})$-depth robust for all constant $\epsilon > 0$. By the same arguments we used in this section, we can construct $c$-maximally ST-robust graphs with depth $d = n^{1-\epsilon}$, where the constant $c$ depends on $\epsilon$. \qed

Figure 3: A diagram of the constant indegree, linear sized, ST-robust graph $M_n$. 

12
5 Constructing Maximal ST-Robust Graphs

In this section, we construct maximal ST-robust graphs, which are 1-maximally ST-robust, from $c$-maximally ST-robust graphs. We give the following construction:

Construction 5.1 ($\mathcal{O}(M_n)$). Let $M_n$ be a $c$-maximally ST-robust graph on $O(n)$ nodes. Let $O$ be a set $o_1, o_2, \ldots, o_n$ of $n$ output nodes and let $I$ be a set $i_1, i_2, \ldots, i_n$ of $n$ input nodes. Let $S_j$ for $1 \leq j \leq \lceil \frac{1}{c} \rceil$ be a copy of $M_n$ with outputs $o'_1, o'_2, \ldots, o'_n$ and inputs $i'_1, i'_2, \ldots, i'_n$. Then for all $1 \leq j \leq n$ and for all $1 \leq k \leq n$, add a directed edge from $i_k$ to $i'_k$ and from $o'_k$ to $o_k$.

Because we connect $\lceil \frac{1}{c} \rceil$ copies of $M_n$ to the output nodes, $\mathcal{O}(M_n)$ has indegree $\max\{\delta, \lceil \frac{1}{c} \rceil\}$, where $\delta$ is the indegree of $M_n$. Also, if $M_n$ has $k n$ nodes, then $\mathcal{O}(M_n)$ has $(k \lceil \frac{1}{c} \rceil + 2)n$ nodes. We now show that $\mathcal{O}(M_n)$ is a maximal ST-robust graph.

Theorem 5.2. Let $M_n$ be a $c$-maximally ST-robust graph. Then $\mathcal{O}(M_n)$ is a maximal ST-robust graph.

Proof. Let $R \subset V(\mathcal{O}(M_n))$ with $|R| = k$. Let $R = R_I \cup R_M \cup R_O$, where $R_I = R \cap I$, $R_O = R \cap O$, and $R_M = R \cap (\bigcup_{i=1}^{\lceil \frac{1}{c} \rceil} S_i)$. Consider $\mathcal{O}(M_n) - R$.

We see that $|R_M| \leq k$, so by the Pigeonhole Principal at least one $S_j$ has less than $c n$ nodes removed, say it has $t$ nodes removed for $t \leq c n$. Hence $t \leq |R_M|$. Since $S_j$ is $c$-max ST-robust there exists a subgraph $H$ of $S_j$ containing $n - t$ inputs and $n - t$ outputs such that every input is connected to all of the outputs. Let $H'$ be the subgraph induced by the nodes in $V(H) \cup I' \cup O'$, where $I' = \{(i_o, i'_a) | i'_a \in H\}$ and $O' = \{(o'_a, o_a) | o'_a \in H\}$.

Claim 5.3. The graph $H'$ contains at least $n - k$ inputs and $n - k$ outputs and there is a path between every pair of input and output nodes.

Proof. The set $|I \setminus I'| \leq |I \cap R| + |V(S_j) \cap R| \leq |R| \leq k$. Similarly, $|O \setminus O'| \leq |O \cap R| + |V(S_j) \cap R| \leq |R| \leq k$. Let $v \in I'$ be some input. By the connectivity of $H$, $v$ can reach all of the outputs in $O'$. Thus there is a path between every pair of input and output nodes.

Thus $\mathcal{O}(M_n)$ is $(k, n - k)$-ST-robust for all $1 \leq k \leq n$. Therefore $\mathcal{O}(M_n)$ is a maximal ST-robust graph.

Corollary 5.4. (of Theorem 5.2) For all $\epsilon > 0$, there exists a family $\mathcal{M}^\epsilon = \{M_k^\epsilon\}_{k=1}^{\infty}$ of max ST-robust graphs of depth $d = n^{1-\epsilon}$ such that $|V(M_k^\epsilon)| \leq c n$ and indegree($M_k^\epsilon$) $\leq c \epsilon$.  

13
Proof. Apply Construction 5.1 to the family graphs $M^\epsilon = \{M^\epsilon_k\}_{k=1}^\infty$ from Corollary 4.5. Then by Theorem 5.2 the family of graphs $\{0(M^\epsilon_k)\}_{k=1}^\infty$ is the desired family.

References

[AB16] 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.

[ABP17] 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.

[BHK+19] 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.

[EGS75] Paul Erdős, Ronald L. Graham, and Endre Szemeredi. On sparse graphs with dense long paths., 1975.

[GG81] Ofer Gabber and Zvi Galil. Explicit constructions of linear-sized superconcentrators. Journal of Computer and System Sciences, 22(3):407–420, 1981.

[MMV13] Konstantin Makarychev, Yury Makarychev, and Aravindan Vijayaraghavan. Sorting noisy data with partial information. In Robert D. Kleinberg, editor, ITCS 2013, pages 515–528. ACM, January 2013.

[Pip77] Nicholas Pippenger. Superconcentrators. SIAM J. Comput., 6(2):298–304, 1977.

[Sch83] Georg Schnitger. On depth-reduction and grates. In 24th Annual Symposium on Foundations of Computer Science, Tucson, Arizona, USA, 7-9 November 1983, pages 323–328. IEEE Computer Society, 1983.
Appendix

Proof of Theorem 3.1

Proof. Let $D \subseteq V(G)$ with $|D| = k$. Consider $G - D$. Let $A = \{(s_1, t_1), \ldots, (s_m, t_m)\}$, where the input $s_i \in S$ is disconnected from the output $t_i \in T$ in $G - D$, or $s_i \in D$ or $t_i \in D$. Let $B = \emptyset$.

Perform the following procedure on $A$ and $B$: Pick any pair $(s_p, t_p) \in A$ and add $s_p$ and $t_p$ to $B$. Then remove the pair from $A$ along with any other pair in $A$ that shares either $s_p$ or $t_p$. Continue until $A$ is empty.

If we consider the nodes of $B$ in $G$, then there are $|B|$ vertex-disjoint paths between the pairs in $B$ by the connector property, and in $G - D$ at least one vertex is removed from each path. Thus $|B| \leq k$, or we have a contradiction.

If $(s, t) \in G - (D \cup B)$ are an input to output pair, and $s$ is disconnected from $t$, then by the definition of $A$ and $B$ we would have a contradiction, since $(s, t)$ would still be in $A$. Thus all of the remaining inputs in $G - (D \cup B)$ are connected to all the remaining outputs.

Hence, if we let $H = G - (D \cup B)$, then $H$ is a subgraph of $G$ with at least $n - k$ inputs and $n - k$ outputs, and there is a path going from each input of $H$ to each of its outputs. Therefore, $G$ is $(k, n - k)$-ST-robust for all $1 \leq k \leq n$. \qed

Proof of Theorem 3.2

Proof. We proceed by induction. For $m = 1$, the $B_1$ is just the bipartite graph $K_{2,2}$ with all of the edges directed to the output set. This graph is
clearly a 2-connector.

Assume the $B_{m-1}$ is a $2^{m-1}$-connector. Consider $B_m$. We see the $B_m$ contains two $B_{m-1}$ subgraphs, an upper $B_{m-1}$ and a lower $B_{m-1}$, and that each input of $B_n$ connected to one upper input and one lower input, and each output of $B_n$ is connected to one upper output and one lower output. Note that from the construction of $B_n$, if $i \leq 2^m-1$, then the inputs $i$ and $i + 2^{m-1}$ must be routed through opposite $B_{m-1}$ subgraphs, and similarly for outputs.

We use the following procedure to correctly pick either the upper or lower $B_{m-1}$ for each input and output: Start with a random input and map it through the upper to its destination $i$. Then $i$ corresponds to another output $j$, where $j = i + 2^{m-1}$ if $i \leq 2^m-1$ and $j = i - 2^{m-1}$ otherwise. Map $j$ through the lower to its input $k$. Then input $k$ corresponds to another input $l$, and map $l$ through the upper network. Eventually the next input will correspond to the original input to close the loop. Either the whole graph has been traversed and we are finished, or some inputs and outputs remain, so we pick an input that hasn’t been hit yet and continue the process. Once we have all of the inputs and output assigned to the upper and lower $B_{m-1}$ subgraphs, the result follows from the inductive hypothesis.