The Open Generalized Mirror Theory Conjecture

Exact Multi-Graph Bounds Beyond the $O(2^{n/4})$ Regime

Status. Statement: AI-written, not yet formalized.

Category. Symmetric-Key Cryptography.

Mirror Theory, initially introduced by Patarin (2003), provides lower bounds on the number of non-degenerate solutions to systems of bivariate linear equations over $\mathbb{F}_2^n$. While recent breakthroughs (e.g., Cogliati et al., 2023) have rigorously established the theory for component sizes up to $\xi_{\max} = O(2^{n/4}/\sqrt{n})$, the fully generalized conjecture for arbitrary dependency graphs up to the information-theoretic limit remains an open problem in theoretical cryptography. This document provides a self-contained statement of the open Generalized Mirror Theory Conjecture.

1 Formal Preliminaries

Let $V = \{p_1, p_2, \ldots, p_q\}$ be a set of variables taking values in $\{0,1\}^n$, where $N = 2^n$. We consider systems of bivariate affine equations over $\mathbb{F}_2^n$ defined on a multi-graph $G = (V, E)$.

Definition 1 (Affine Equation System). Let $G = (V, E)$ be a connected graph with $q = |V|$ vertices and $m = |E|$ edges. Let $\lambda : E \to \{0,1\}^n \setminus \{0^n\}$ be an edge-labeling function assigning non-zero target constants to each edge. The system of equations is given by:

$$\mathcal{E}(G, \lambda) := \left\{ p_i \oplus p_j = \lambda_{i,j} \;\middle|\; e = (p_i, p_j) \in E \right\}. \tag{1}$$

Definition 2 (Non-Degenerate Solutions). A tuple $(P_1, \ldots, P_q) \in (\{0,1\}^n)^q$ is called a **valid (non-degenerate) solution** to $\mathcal{E}(G, \lambda)$ if:

i. $P_i \oplus P_j = \lambda_{i,j}$ for all $(p_i, p_j) \in E$.

ii. $P_i \neq P_j$ for all $i \neq j$ (all variables in V are pairwise distinct).

We denote the set of all non-degenerate solutions by $\mathbf{Sol}(\mathcal{E}(G,\lambda))$ and its cardinality by $h(G,\lambda) := |\mathbf{Sol}(\mathcal{E}(G,\lambda))|$.

Definition 3 (Cycle Consistency and Component Size). A system $\mathcal{E}(G,\lambda)$ is **cycle-consistent** if for every cycle C in G, the XOR sum of labels along the cycle evaluates to 0^n. Let $\xi_{\max}(G)$ denote the maximum size (number of vertices) of any connected component of G, and let $\nu(G) = |E| - |V| + c(G)$ be the circuit rank (cyclomatic number) of G, where $c(G)$ is the number of connected components.

2 The Unconditional Generalized Mirror Theory Conjecture

While localized versions of Mirror Theory have been proven for trees and bounded-degree graphs up to $\xi_{\max} = O(N^{1/4})$, the full asymptotic statement for arbitrary graph topologies up to $O(N^{1/2})$ or higher query limits remains open.

Conjecture 1 (Generalized Mirror Theory Conjecture). *Let $G = (V, E)$ be a graph with $q = |V|$ vertices and $m = |E|$ edges. Let $\mathcal{E}(G,\lambda)$ be a cycle-consistent affine system. Assume that $q \leq o(N^{1/2})$ and that the maximum component size satisfies $\xi_{\max}(G) \leq o(N^{1/2})$. Then, the number of non-degenerate solutions $h(G,\lambda)$ satisfies the tight lower bound:*

$$h(G,\lambda) \geq \frac{(N)_q}{N^m} \cdot \left(1 - O\left(\frac{q \cdot \xi_{\max}(G)}{N}\right)\right), \tag{2}$$

where $(N)_q = N(N-1)\dots(N-q+1)$ denotes the falling factorial. Equivalently, for a collection of c connected tree components $T_1, \dots, T_c$

with $|V(T_k)| = q_k$, $q = \sum q_k$, *and* $m = q - c$:

$$h(G,\lambda) \geq \frac{N^q}{N^{q-c}} \prod_{i=0}^{q-1} \left(1 - \frac{i}{N}\right) \left(1 - \epsilon(q, \xi_{\max}, N)\right), \qquad (3)$$

where $\epsilon(q, \xi_{\max}, N) \to 0$ *as long as* $q \cdot \xi_{\max}(G) = o(N)$.

3 State of the Art and Theoretical Gaps

Reference	**Scope / Topology**	**Max Component ($\xi_{\max}$)**	**Status**
Patarin (2003), Patarin (2005)	Linear Graphs / Trees	$\xi_{\max} = O(1)$	Gaps identified
Cogliati & Seurin (2018)	Circle Graphs ($\nu = 1$)	$\xi_{\max} = O(N^{1/3})$	Proven
Cogliati et al. (2023)	Arbitrary Forest Graphs	$\xi_{\max} = O(N^{1/4}/\sqrt{n})$	Fully Proven
Open Conjecture	**Arbitrary Multi-Graphs**	$\xi_{\max} = \mathbf{o}(\mathbf{N}^{\mathbf{1/2}})$	**OPEN**

Table 1: Evolution of Mirror Theory bounds for system size q and component size $\xi_{\max}$.

Why the Conjecture Remains Open:

1. **High-Order Link Deletions**: Current algebraic techniques (such as link-deletion equations) rely on induction over component sizes. When $\xi_{\max}$ exceeds $O(N^{1/4})$, higher-order dependency intersections generate non-trivial error terms that cannot be absorbed without explicit structural cancellation lemmas.

2. **Multi-Cycle Dependencies**: For graphs with high cyclomatic numbers ($\nu(G) > 1$), handling non-equations ($P_i \neq P_j$) alongside linear constraints requires tracking exact character sums over non-abelian representations, which currently lack tight lower bounds.