Proof of Mirror Theory for $\xi_{\max} = 2$

Avijit Dutta[1], Mridul Nandi[2], Abishanka Saha[2]

Indian Institute of Technology, Kharagpur
Indian Statistical Instiute, Kolkata

Abstract. In ICISC-05, ePrint-10 and patarin-book, Patarin proved that the number of solutions of $(P_1, \ldots, P_{2q})$ with distinct $P_1, P_2, \ldots, P_{2q}$ from $\{0,1\}^n$ satisfying $P_{2i-1} \oplus P_{2i} = \lambda_i$ $(\neq 0)$, $1 \leq i \leq q$ is at least

$$\frac{(2^n)_{2q}}{2^{nq}} \text{ for all } q \leq \frac{2^n}{134}$$

where $(2^n)_{2q} := 2^n(2^n-1)\cdots(2^n-2q+1)$. This result is known as *Mirror Theory*. Mirror theory stands out to be a powerful tool to provide a high security guarrantee for many block cipher (or even an ideal permutation) based designs. Unfortunately, the proof of mirror theory contains some unverifiable gaps and several mistakes. In this paper, we revisit the proof strategy of ePrint-10 and *provide a detailed proof of the mirror theory by correcting the mistakes and filling up gaps*. In particular, we prove the mirror theory for all $q \leq 2^n/33.1$ (a wider range than what was originally claimed by Patarin). As an application, we show that the maximum PRF-advantage of sum of domain separated random permutation is **exactly** $1-(1-2^{-n})^q$, $\forall q \leq 2^n/33.1$. Using similar proof strategy, we also prove the following mirror theory for sum of two independent permutations: the number of solutions of $(P_1, Q_1, \ldots, P_q, Q_q)$ with distinct $P_1, P_2, \ldots, P_q$ and distinct $Q_1, \ldots, Q_q$ satisfying $P_i \oplus Q_i = \lambda_i$ for any fixed $\lambda_i \in \{0,1\}^n$, $1 \leq i \leq q$ is at least

$$\frac{(2^n)_q \times (2^n)_q}{2^{nq}} \times \left(1 - \frac{1.2q^2}{2^{2n}} - \frac{108n^3}{2^{2n}}\right), \text{ for all } q \leq \frac{2^n}{13}.$$

Keywords: Mirror Theory, Sum of Permutation, PRP, PRF, H-Technique.

1 Introduction

Block ciphers, the workhorses of symmetric-key cryptography, are used in different modes of operations to provide solutions for data confidentiality, data integrity and authenticity etc. However, most of the modes of operation do not exploit the invertible property of the block cipher [2,5,20,34] and hence block cipher seems to be an over-engineered primitive for such cases. Instead of block ciphers, pseudorandom functions (PRF) could be a more natural choice in such modes of operation. But unlike block ciphers, which are available in plenty, practical candidates of PRF are rarely available. Although, a block cipher itself is a good PRF, but it gives security only upto the birthday bound of its block size due to the standard PRP-PRF result [4,35,6]. Hence, one can safely consider a

block cipher as a PRF in a mode of operation when the block size is moderate enough (e.g., block size is 128 bits). However, the solution is inadequate when the block size is small (e.g., 64 bits), a scenario quite common in lightweight applications [26]. This led to the search for a PRF which can be designed out of block ciphers and also gives security higher than the usual birthday bound.

LUBY-RACKOFF BACKWARDS: To ponder this problem, Bellare et al. [3] studied in designing PRFs out of block ciphers in the name of *Luby-Rackoff backwards* that addressed the problem of converting a pseudorandom permutations (PRP) into a PRF. Among many alternatives, xoring the outputs of two independent n-bit block ciphers, denoted as XOR_2, is one of them. However, the security analysis of XOR_2 was open till then. The importance of this construction and its domain separated single permutation variant construction XOR_1 (i.e. $\pi(0\|\cdot) \oplus \pi(1\|\cdot)$) [1] have gained attentions in the cryptographic community over the last few years and the study of their security analysis remained the most challenging problem[2] until [7], in which Dai et al. proved both the constructions are optimally secure PRF.

HISTORY OF XOR FUNCTION. In 2000, Lucks [19] proved that XOR_2 achieves $2n/3$ bit PRF security. Concurrent to this, Patarin, in 2008, gave an improved security bound $O(2^n)$ on XOR_2 construction using H_σ-technique [30]. Later, in 2013, he proved the similar bound for XOR_2 construction using standard H-technique [33]. Patarin [32], in 2010, gave 2^n bit security of XOR_1 construction. The entire security analysis of this construction stands on the following result which informally says that

"For a given system of bi-variate affine equations over a finite group with non-equalities among the variables, the number of distinct solutions is always greater than the average number of solutions.".

Patarin named this notion as *Theorem* $P_i \oplus P_j$ in [28] (and later in [32] renamed to *Mirror Theory*). This theorem was stated as a conjecture in [27] and proved in [28]. For proving the optimal security of XOR_1 construction, *Theorem* $P_i \oplus P_j$ *for* $\xi_{\max} = 2$ is required, which has been acknowledged in the community as a potential and strong approach to establish higher security of the construction. Despite the strength of the approach, the proof of the theorem is very involved and contains many unverifiable gaps. In fact, the authors of [7] stated that

"Patarin's tight proof is very involved, using an approach he refers to as "mirror theory" with some claims remaining open or unproved".

Apart from the own standalone value of XOR_2 or XOR_1 function (generically we call them as **sum function**), they are used as a major component in many important block cipher based designs [36,37,38,25,9,8,16,18,13,12,15] and tweakable

[1] Here, π is an n-bit random permutation and throughout the paper, we use the ideal primitive π instead of its computational counterpart E_k.

[2] Bellare et al. in an unpublished work [1] first showed that XOR_1 is a secure PRF up to $2^{1.5n}/n$ queries. However, their analysis is sketchy and hard to verify.

block cipher based designs [24,17]. However, the security proof of most of these designs require to degenerate the final outputs to get rid of adaptiveness nature of adversary. Hence the proof cannot use the fact that the sum function is a PRF. Instead of that, these security proofs require (by applying the H-Coefficient technique [29]) a good lower bound on the number of distinct solutions to a system of bi-variate affine equations and there comes the role of the mirror theory. However, the correctness of the proof of the mirror theory [28,32] is still a subject of debate in the community. Despite of this, several authors have used this precarious result to derive an optimal bound of some constructions [14,21,39]. This triggers the need for a correct and verifiable proof of mirror theory, which eventually helps to correctly establish the security proof of the above constructions and possibly can improve their security.

Mirror Theory Statements for $\xi_{\max} = 2$. We write $(x)_a \stackrel{\text{def}}{=} x(x-1)\cdots(x-a+1)$ for positive integers x and a. Patarin stated and proved the following result [32]

1. Mirror Theory for a single permutation with $((\xi_{\max}, \theta) = (2, 134))$ ([32]). The number of $(P_1, \ldots, P_{2q})$ with distinct $P_1, P_2, \ldots, P_{2q}$ from $\{0,1\}^n$ satisfying $P_{2i-1} \oplus P_{2i} = \lambda_i$ $(\neq 0)$, $1 \leq i \leq q$ is at least $\frac{(2^n)_{2q}}{2^{nq}}$ for all $q \leq \frac{2^n}{134}$.

In [30], Patarin proved a similar result involving $q \ll 2^n$ equations for the case of independent random permutations:

2. Mirror Theory for a pair of permutations with $\xi_{\max} = 2$. ([30,33]). There exists a set $G \subseteq (\{0,1\}^n)^q$ with size at most $2^{nq} \times (1 - O(\frac{q}{2^n}))$ such that for all $(\lambda_1, \ldots, \lambda_q) \in G$ the number of $(P_1, Q_1, \ldots, P_q, Q_q)$ with distinct $P_1, P_2, \ldots, P_q$ and distinct $Q_1, \ldots, Q_q$ from $\{0,1\}^n$ satisfying $P_i \oplus Q_i = \lambda_i$, $1 \leq i \leq q$ is at least

$$\frac{(2^n)_q \times (2^n)_q}{2^{nq}} \times (1 - O(\frac{q}{2^n})).$$

As applications of the above results, one can immediately see that the XOR_1 and XOR_2 functions behave almost like a random function.

Applications of Mirror Theory for any $\xi_{\max}$ in Cryptography. Note that, $\xi_{\max} = 2$ means that each variable in the system of equations are distinct. For a general $\xi_{\max}$, a variable is used at most $\xi_{\max} - 1$ times. He claimed a similar result that for a given system of q many bi-varite affine equations, the number of distinct solutions is always larger than the average number of solutions provided $q \leq 2^n/67.(\xi_{\max} - 1)$. This result in fact was stated as a conjecture (Conjecture 8.1) in [27] and proved in [28,23]. However, the proof is very sketchy with most of the details missing (in fact, later we address several major issues present even in the simpler case when $\xi_{\max} = 2$).

Over the years, mirror theory has been proven to be an extremely important tool in the context of analysing the security bound of numerous cryptographic designs. Mennink et al. [21] have shown the optimal security bound of EWCDM using mirror theory as the underlying tool. Iwata et al. [14] used mirror theory to shown the optimal security bound of CENC. Mirror theory has been used in proving the beyond birthday bound security of many nonce based MACs [10,11,12,22].

However, the proof for all such construction requires the mirror theory result with an arbitrary $\xi_{\max}$ value and according to the current status, proof of this result is still unverifiable.

DISCLAIMER. From now onwards we use the term "**Mirror Theory**" throughout the paper to refer to the *Mirror Theory with* $\xi_{\max} = 2$ for a single or a pair of permutation (as will be clear from the context).

1.1 Issues in the Proof of Mirror Theory [32,28,31,33]

PROOF APPROACH DUE TO PATARIN. Let h_α denote the number of distinct solutions $(P_1, \ldots, P_{2\alpha})$ such that $P_1 \oplus P_2 = \lambda_1, \ldots, P_{2\alpha-1} \oplus P_{2\alpha} = \lambda_\alpha$ where λ_i's are non-zero n-bit binary strings. We write $H_{2\alpha} = 2^{n\alpha} \cdot h_\alpha$ and $J_{2\alpha} = (2^n)_{2\alpha}$. Obviously, $H_2 \geq J_2$. It is sufficient to show that $\frac{H_{2\alpha+2}}{J_{2\alpha+2}} \geq \frac{H_{2\alpha}}{J_{2\alpha}}$ for all $1 \leq \alpha \leq 2^n/\theta$ for suitably small constant $\theta \geq 1$ (smaller is better). In other words,

$$h_{\alpha+1} \geq \frac{(2^n - 2\alpha)_2}{2^n} h_\alpha = (2^n - 4\alpha)h_\alpha + \frac{\Theta(\alpha^2)}{2^n} \cdot h_\alpha. \tag{1}$$

To reach the lower bound as stated in Eqn. (1), Patarin begins with an useful equation, called *Orange equation* [Theorem 5, [32]], as follows:

$$h_{\alpha+1} = (2^n - 4\alpha + 2\delta)h_\alpha + \sum_{(k,l)\in M} h'_\alpha(k,l),$$

where $\delta = \#\{i : 1 \leq i \leq \alpha \text{ such that } \lambda_i = \lambda_{\alpha+1}\}$ and $M = \{(i,j) \mid i \neq j \in [\alpha], \lambda_i \neq \lambda_{\alpha+1}, \lambda_j \neq \lambda_{\alpha+1}, \lambda_i \oplus \lambda_j \neq \lambda_{\alpha+1}\}$, and $h'_\alpha(k,l)$ represents the number of 'appropriate' h_α solutions with one added equation $P_k \oplus P_l = \lambda_{\alpha+1}$. It can be easily shown that $|M| = \Theta(\alpha^2)$. Hence, for every $(k,l) \in M$, it is sufficient to show the following :

$$h'_\alpha(k,l) \geq \frac{h_\alpha}{2^n}\left(1 - \frac{A}{2^n} - \frac{B\alpha}{2^{2n}} - \frac{C\Delta\alpha}{2^{2n}}\right), \tag{2}$$

for some constants A, B and C. We call Eqn. (2) the h'_α*-property* [Sect B.3, [32]]. Note that the security strength θ would depend on these values of A, B and C. A simple algebra on the orange equation followed by applying h'_α-property, leads to our target inequation as stated in Eqn. 1. Therefore, we can now focus to prove the h'_α-property for all α and for all nonzero $\lambda_1, \cdots, \lambda_\alpha$. To prove this property, Patarin derived the following equation [Theorem 15, [32]], called *Purple equation* as follows:

$$h'_{\alpha+1} = h_\alpha + (-4\alpha + T)h'_\alpha + \sum_{(i,j)\in M'} h''_\alpha(i,j), \tag{3}$$

where $0 \leq T \leq 10\Delta+14$, Δ being the maximum number of multicollisions among $\lambda_1, \cdots, \lambda_{\alpha+1}$. Here, h''_α (in general $h^{[\mu]}_\alpha$, $\mu \geq 0$) represents the number of injective solutions of a system of equations, where there are α many *"base"* equations (i.e. the original equations) and 2 (resp. μ) additional equations (called linking

equations) between $P_1, \cdots, P_{2\alpha}$. Note that, $h_\alpha^{[0]} = h_\alpha$ and $h'_\alpha = h_\alpha^{[1]}$. Similar to Eqn. (3), one can write $h_\alpha^{[\mu]}$ in terms of $h_\alpha^{[\mu-1]}$, $h_\alpha^{[\mu]}$ and $h_\alpha^{[\mu+1]}$. This is called the *μ-th order purple equation*. Thus, Eqn. (3) is called the "first order purple equation". Now, we discuss the issues in Patarin's proof approach while proving the h'_α-property.

Issue-1: Label Dependency. First of all, note that all the h-terms in the orange and the purple equations depend on two factors: (i) $\alpha+1$ many constant values $\lambda_1, \cdots, \lambda_{\alpha+1}$ and (ii) the additional equations, which we call the *linking equations*, that we consider. *Although Patarin cautioned about this dependency, he unified these terms and expressed these two equations without providing any justification.*

Once the orange and the purple equations are derived, the main strategy of Patarin's proof is to show that all the A-terms are negligible, where the μ-th order A-term is defined as follows:

$$A_\alpha^{[\mu]} \stackrel{\text{def}}{=} \left| h_\alpha^{[\mu]} - \frac{h_\alpha^{[\mu-1]}}{2^n} \right|, \quad \mu \geq 1.$$

An upper bound on $A^{[1]}$-term can be obtained by subtracting the orange equation (after multiplying it by $1/2^n$) from the first order purple equation. To get similar upper bounds for μ-th order A-terms, Patarin used μ-th order and $(\mu-1)$-th order purple equations. This would lead to a recurrence relation on an upper bound of A-terms. In this way, Patarin derived a general upper bound on A-terms, which he called the *central theorem. However, Patarin did not state the higher order purple equations.*

Issue-2: Higher Order Central Theorem. First of all, the previous issue of label dependency remains for the A-terms as well. We have also observed that the first order A-term, i.e., $A^{[1]}$-term, which we call the *first order central theorem* [Theorem 16, [32]], is not written correctly. A more serious issue lies in the expression of the higher order A-terms, i.e., $A^{[\mu]}$ for $\mu \geq 2$, that we call the *general version of the central theorem*. It states the following [Theorem 17, [32]]:

$$\left| h_{\alpha+1}^{[\mu]} - \frac{h_{\alpha+1}^{[\mu-1]}}{2^n} \right| \leq 4\alpha \left| h_\alpha^{[\mu]} - \frac{h_\alpha^{[\mu-1]}}{2^n} \right| + 4\alpha^2 \left| h_\alpha[\mu+1] + \frac{h_\alpha^{[\mu]}}{2^n} \right| + \frac{26\Delta + 30}{2^{2n}} h_{\alpha+1},$$

where $\Delta = \sup_{0 \leq i \leq \alpha+1}[\#j, 0 \leq j \leq \alpha+1, j \neq i, : \lambda_j = \lambda_i]$. Patarin stated the general version of the central theorem as a generalization of the first order central theorem without giving any formal explanation in support of this. Nevertheless, *we have found that the expression is incorrect as there is no way to obtain the $h_{\alpha+1}$-term on the right hand side of the inequality.*

Issue-3: Missing Proof. *Finally, Patarin claimed, almost magically, the following result [Theorem 18 of [32]] from the general version of the central theorem without any justification for it.*

$$\left| h'_\alpha - \frac{h_\alpha}{2^n} \right| \leq h_\alpha \left(\frac{2^{3k}\alpha^k}{(2^n - 4\alpha)^{k+1}\left(1 - \frac{4\alpha}{2^n} - \frac{4\alpha^2}{2^{2n}}\right)} + \frac{26\Delta + 30}{2^{2n}\left(1 - \frac{4\alpha}{2^n} - \frac{4\alpha^2}{2^{2n}}\right)} \right).$$

Note that, this result actually leads to proving the h'_α-property.

Issue-4: Issue in ICISC-05 paper [28]. Patarin proved χ-bound in Theorem 9 of [28], where he defined $\chi \stackrel{\text{def}}{=} O(\frac{2\alpha}{2^{2n}})h_{2\alpha-4}$. However, the proof assumed a result which essentially boils down to proving the h'_α-property (the core part of the mirror theory) and this result has not been backed up by a verifiable proof anywhere in the literature.

Issue-5: Missing Proof in [33]. Issues in the proof of Mirror theory for a pair of independent permutations are somewhat similar to the issues that we have pointed out for single permutation case. Patarin first proved this result using H_σ technique in [30,31] to derive $O(q/2^n)$ bound and later used H-cofficient technique [33] to derive the similar bound. Here, we point out the non-trivial issues of the proof presented in all these papers[3]. To estimate the number of solutions, Patarin started with orange equation, by which he showed only $2n/3$ bound. Then, with a simple approximation of h'_α, he slightly improved the bound to $3n/4$. In section 6, he derived an induction formula on h'_α in which he only proved first order purple theorem and given a bound on set $\mathscr{N}$. These results do not immediately give any generalized result that helps to prove 2^n bound. However, in Appendix C of [33], author chalked out a general proof strategy, but again that is too less informative to derive a generic proof out of it. Therefore, although the author claims that he has proved optimal security bound for mirror theory with a pair of permutations, the paper lacks of a complete and generalized proof.

Remark 1. We would like to mention here that chapter 15 of [23] deals with mirror theory for $\xi_{\max} = 2$ using a slightly different approach than that of [32]. Authors have used *Maximal Regression from the Mean value* method (Theorem 15.7 and 15.8, pg 234 of [23]) to prove mirror theory. Although the proof is incomplete and requires a proper repairing, we feel that this approach has a potentiality to establish a correct proof of mirror theory for $\xi_{\max} = 2$ if one carefully fills up the non-trivial gaps present in the proof.

In this paper we have mainly followed the proof approach of [32]. It enables us to fill up the non-trivial gaps present in the proof of [32], for which we have been able to establish a correct security proof of mirror theory for $\xi_{\max} = 2$. Although there are several proofs of mirror theory present in the literature, but as we have mentioned that all of them are either erroneous or incomplete. At this point, we feel that instead of having several incomplete and erroneous proofs of an important result, it is always worthy to have its one concrete and correct security proof.

[3] The paper [31] is an extended version of [30] and analysis of most of the proofs of [30] are given in the extended version. Thus, we discuss the issues of the proofs presented in [31].

1.2 Our Contribution

The sole contribution of this paper is to prove the following two theorems. The first one is the mirror theory result for a single permutation and the later one is the mirror theory result for a pair of permutations.

Theorem 1 (Mirror Theory $(\xi_{\max}, \theta) = (2, 33.1)$ for Single Permutation). *Let $n \geq 8$, $q \leq 2^n/\theta$ and $\lambda_1, \ldots, \lambda_{q+1}$ are nonzero n-bit strings. The number of pairwise distinct solutions $(P_1, \ldots, P_{2q+2}) \in (\{0,1\}^n)^{2q+2}$ to the following system of equations*

$$\mathscr{E} = \{P_1 \oplus P_2 = \lambda_1, P_3 \oplus P_4 = \lambda_2, \cdots, P_{2q+1} \oplus P_{2q+2} = \lambda_{q+1}\}$$

is at least

$$\frac{2^n(2^n-1)\cdots(2^n-2q-1)}{2^{n(q+1)}}.$$

We note that our statement holds for a more wide range of number of queries q than the original claim made by Patarin [32]. As an application of our theorem, we state the following corollary, which gives a tight PRF bound [4] $1-(1-2^{-n})^q$ of XOR_1 construction, for all $q \leq 2^n/33.1$. Proof of the corollary is deferred in Appendix E.

Corollary 1. *Let π be an n-bit random permutation and A be a distinguisher that makes q distinct queries to either XOR_1 or an $(n-1)$-bit to n-bit random function RF, where each query $x \in \{0,1\}^{n-1}$. Then for all $q \leq 2^n/33.1$, we have*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XOR}_1}(\mathsf{A}) \leq 1 - \left(1 - \frac{1}{2^n}\right)^q.$$

As the second contribution of the paper, we state the mirror theory result for a pair of indepenent permutations as follows:

Theorem 2 (Mirror Theory $(\xi_{\max}, \theta) = (2, 13)$ for a Pair of Permutations). *Let $n \geq 5$, $q \leq 2^n/\theta$ and $\lambda_1, \ldots, \lambda_{q+1}$ are n-bit strings. The number of solutions $((P_1, \ldots, P_{q+1}), (Q_1, \ldots, Q_{q+1})) \in (\{0,1\}^n)^{q+1} \times (\{0,1\}^n)^{q+1}$ to the following system of equations*

$$\mathscr{E} = \{P_1 \oplus Q_1 = \lambda_1, P_2 \oplus Q_2 = \lambda_2, \cdots, P_{q+1} \oplus Q_{q+1} = \lambda_{q+1}\},$$

such that all P_i's are pairwise distinct and all Q_i's are pairwise distinct, is at least

$$\frac{(2^n(2^n-1)\cdots(2^n-q))^2}{2^{n(q+1)}} \cdot \left(1 - \frac{1.2q^2}{2^{2n}} - \frac{108n^3}{2^{2n}}\right).$$

As an application of Theorem 2, we state the following corollary, which shows that the PRF advantage of XOR_2 construction is at most $1.2(q/2^n)^2 + 108n^3/2^{2n}$, for all $q \leq 2^n/13$. Proof of the result is deferred in Appendix E.

[4] A simple distinguisher returns 1 whenever it observes 0^n output. In case of random function it returns 1 with probability exactly $1-(1-2^{-n})^q$, whereas it returns 0 with probability zero for the XOR_1 construction as it never returns zero.

Corollary 2. *Let π_1, π_2 be a pair of n-bit random permutations and A be a distinguisher that makes q distinct queries to either XOR_2 or an n-bit to n-bit random function RF. Then for all $q \leq 2^n/13$, we have*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XOR}_2}(\mathsf{A}) \leq \frac{1.2q^2}{2^{2n}} + \frac{108n^3}{2^{2n}}. \tag{4}$$

This bound is better than the bound established in [30,33]. In fact, our bound also supersedes the bound $(q/2^n)^{1.5}$ for $q \leq 2^n/16$ by Dai et al. [7]. However our bound is not yet proven to be tight because there is no known attack against XOR_2 which uses less than 2^n queries.[5]
It is needless to say that the application of these results are limited only in proving the optimal PRF security of the sum function. But, we believe that this would be the first stepping stone in making any further progress on different variants of mirror theory.

Roadmap of the paper: We set up the neccessary background in Sect. 2. In Sect. 3, we derive the orange and the purple equations - the two most basic equations for the proof of mirror theory for same permuation and a pair of independent permutations case. Followed by this, we quickly settle the proof of Theorem 1 in Sect. 4 modulo the proof of the h'_α property, the fundamental lemma of the analysis. We devote Sect. 5 for proving the h'_α property on top of another two results, called derived inequality lemma and general order central lemma. We prove these two results in Sect. 6. We devote Sect. 7 for proving Theorem 2.

2 System of Bi-Variate Equations

In this section we give a graphical view of a system of bi-variate affine equations for same permutation and a pair of independent permutations case. This equivalent view of a system of equations stands out to be crucial for the understanding of the rest of the paper.

2.1 System of Bi-variate Equations for Same Permutation

Labelled Acyclic Graph. Let $\mathscr{V}$ be a set integers $\{1, 2, \ldots, v\}$ of size v. We denote the set of all doubleton sets of $\mathscr{V}$ as $\mathscr{V}^{(2)}$ which represents the set of all possible edges (undirected) over the vertex set $\mathscr{V}$. Let $G = (\mathscr{V}, \mathscr{E}, \lambda)$ be a simple acyclic undirected edge-labelled graph, where $\mathscr{E} \subseteq \mathscr{V}^{(2)}$ is the edge set of G and $\lambda : \mathscr{E} \to \{0,1\}^n$ is an edge labelling function that assigns an n-bit binary string to all edges of $\mathscr{E}$.

Injective Solution of Equations. The system of equations induced by such a simple acylic undirected edge-labelled graph G is denoted $\mathbb{E}_G$, which is defined

[5] A simple distinguisher for XOR_2 (that makes 2^n distinct queries) returns 0 whenever it observes that the xor of the replies to its 2^n distinct queries is 0^n, and returns 1 otherwise.

as $\mathbb{E}_G = \{Y_i \oplus Y_j = \lambda_{\{i,j\}} \stackrel{\text{def}}{=} \lambda(\{i,j\}) \mid \{i,j\} \in \mathscr{E}\}$, where each vertices of G correspond to a variable in the system of equations (i.e., vertex i corresponds to the variable Y_i) and each edges of G correspond to an equation in $\mathbb{E}_G$ (i.e., edge $\{i,j\}$ corresponds to the equation $Y_i \oplus Y_j = \lambda_{\{i,j\}}$). Note that a cycle in the graph G implies the system of equations $\mathbb{E}_G$ are not linearly independent. As a linearly dependent equation may lead to an inconsistent system of affine equations, we avoid cycles in the graph G and hence G is restricted to be acylic. An injective function $P : \mathscr{V} \to \{0,1\}^n$ is said to be a an *injective solution* if $P_i \oplus P_j = \lambda_{\{i,j\}}$ for all $\{i,j\} \in \mathscr{E}$, where P_a denotes $P(a)$.

ℓ-LINKED GRAPH: In this paper we are mostly interested in a special class of simple acyclic undirected graphs called *ℓ-linked graph*. For a positive integer ℓ, a graph is called *ℓ-linked*, if it contains exactly one component P which is a path of size $2\ell+1$ (i.e the number of edges is $2\ell+1$) and all other components are path of length one. A *zero linked* graph (also called **base graph**) is simply the graph of disjoint paths of length one. For $\ell \geq 0$, an ℓ-linked graph G with 2α vertices, for some $\alpha > \ell$, contains exactly (i) $\alpha - \ell$ many components which are path of length one and (ii) total $\alpha + \ell$ many edges. Let $\mathsf{P} = (e_1, e_2, \ldots, e_{2\ell+1})$ be the path for an ℓ-linked graph, where $\ell \geq 1$. Then, alternating even positioned edges of P, namely $e_2, e_4, \ldots, e_{2\ell}$, are called the **linking edges**, alternating odd positioned edges of P, namely $e_1, e_3, \ldots, e_{2\ell+1}$ are called *linked-base* edges and all the other remaining edges are called *unlinked-based* edges. A **base edge** is either a linked-base edge or an unlinked-base edge. Fig. 2.1 depicts an example of an ℓ-linked graph.

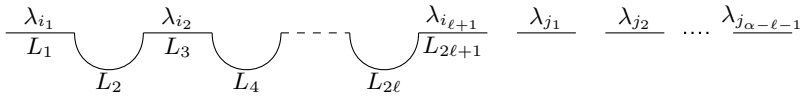

Fig. 2.1: An ℓ-linked graph with ℓ-linked label $\tau = (\mathscr{B}_\alpha, L^{[2\ell+1]})$, where $\mathscr{B}_\alpha = \{\lambda_{i_1}, \lambda_{i_2}, \ldots, \lambda_{i_{\ell+1}}, \lambda_{j_1}, \cdots, \lambda_{j_{\alpha-\ell-1}}\}$. Here, $L_1 = \lambda_{i_1}, L_3 = \lambda_{i_2}, \cdots, L_{2\ell+1} = \lambda_{i_{\ell+1}}$.

LABELS OF LINKED GRAPHS: Let G_1 and G_2 be two simple acylic undirected edge-labelled graphs such that they are label isomporphic. Then, it is easy to verify that the number of injective solutions of $\mathbb{E}_{G_1}$ and $\mathbb{E}_{G_2}$ are same. In other words, the number of injective solutions is invariant under label isomorphism (an isomorphism which preserves the labels). This result allows us to provide a signature which uniquely associates all label isomorphic graphs.

Definition 1 (ℓ-linked label). *Let $\ell \geq 1$, $\mathscr{B}_\alpha \stackrel{\text{def}}{=} \{\lambda_1, \ldots, \lambda_\alpha\}$ be a multiset, where each $\lambda_i \in \{0,1\}^n$ (called* base labels*) and $L^{[2\ell+1]} = (L_1, L_2, \ldots, L_{2\ell+1})$, also denoted as $(L_1 \cdot L_2 \cdot \ldots \cdot L_{2\ell+1})$, be an ordered tuple, where each $L_i \in \{0,1\}^n$. We call the pair $\tau \stackrel{\text{def}}{=} (\mathscr{B}_\alpha, L^{[2\ell+1]})$ ℓ-linked label if there exists distinct $i_1, \ldots, i_{\ell+1}$ with*

$$L_1 = \lambda_{i_1}, L_3 = \lambda_{i_2}, \ldots, L_{2\ell+1} = \lambda_{i_{\ell+1}}.$$

We call $L_2, L_4, \ldots, L_{2\ell}$ linking labels which connect the base labels $\lambda_{i_1}, \lambda_{i_2}, \lambda_{i_{\ell+1}}$. We call these base labels linked-based labels and all other base labels unlinked-base labels. In particular, a 0-linked label is simply the multiset $\mathscr{B}_\alpha$.

Labeling ℓ-linked graph. Given a $\ell(\geq 1)$-linked labels τ as defined above and an ℓ-linked graph $G = (\mathscr{V}, \mathscr{E})$ with $|\mathscr{E}| = \alpha + \ell$, we define a label function $\lambda \stackrel{\text{def}}{=} \lambda_\tau$ over $\mathscr{E}$ as follows: let $\mathsf{P} = (e_1, e_2, \ldots, e_{2\ell+1})$ be the $(2\ell+1)$-sized path. We define $\lambda(e_i) = L_i$, $1 \leq i \leq 2\ell+1$ and for all other $\alpha - \ell - 1$ edges (if any), we assign elements from the multiset $\mathscr{B}_\alpha \setminus \{\lambda_{i_1}, \ldots, \lambda_{i_{\ell+1}}\}$ (of size $\alpha - \ell - 1$) arbitrarily as their labels such that each element is being assigned exactly once. Note that the label function is not unique as we can choose the order of the path in two directions and the assignment of the remaining edges are arbitrary. Clearly, all such labeling functions are label isomorphic and so the number of solutions of the system of equations based on $G = (\mathscr{V}, \mathscr{E}, \lambda)$ are same. Therefore, the number of injective solutions is uniquely determined by the label τ.
In case of a zero-linked label $\mathscr{B}_\alpha$ and a zero-linked graph G, there is no path in G with more than one edge and thus we simply assign all elements from $\mathscr{B}_\alpha$ to edges of G.

Valid Labels. Let G be an ℓ-linked graph and $\tau = (\mathscr{B}_\alpha, L^{[2\ell+1]})$ be its label. Then, we denote the set of all injective solutions of G as $\mathscr{H}(\tau)$ and the number of its injective solutions as $h(\tau)$.[6] However, $\mathscr{H}(\tau)$ and $h(\tau)$ depends on the exact choice of labelling function λ_τ. Now, an injective solution exists for a zero-linked system (also called *base system*) with label $\tau = \mathscr{B}_\alpha$, provided elements of $\mathscr{B}_\alpha$ are non-zero elements of s^n. Similarly, necessary conditions for existence of an injective solution for a ℓ-linked graph G with label $\tau = (\mathscr{B}_\alpha, L^{[2\ell+1]})$ are the following: (i) the elements of $\mathscr{B}_\alpha$ and L are non-zero elements of $\{0,1\}^n$ and (ii) for all $1 \leq i < j \leq 2\ell+1$, $L_i \oplus L_{i+1} \oplus \cdots \oplus L_j \neq 0^n$. Any such label τ is called **valid**. The set of all valid ℓ-linked labels is denoted as V_ℓ and the set of all $L^{[2\ell+1]}$ such that each element of $L^{[2\ell+1]}$ is non-zero elements of $\{0,1\}^n$ and $L^{[2\ell+1]}$ satisfying (ii), is denoted as V'_ℓ.

2.2 System of Bi-variate Equations for a Pair of Independent Permutations

We required a simple undirected acyclic edge-labelled graph for same permutation case, but to give a graphical view of a system of bi-variate affine equations for a pair of independent permutations, we need a simple undirected acylic edge-labelled bipartite graph $G = (\mathscr{V}, \mathscr{E}, \lambda)$ whose vertex set $\mathscr{V}$ is partitioned into two disjoint sets $\mathscr{X} = \{x_1, \cdots, x_v\}$, whose vertices are called *x-nodes*, and $\mathscr{Z} = \{z_1, \cdots, z_v\}$, whose vertices are called *z-nodes*. As before, we consider G to be acyclic, otherwise a dependent equation may lead to an inconsistent system of equations. For such a acylic edge-labelled bipartite graph G, we denote its induced system of equations as $\mathbb{E}_G = \{X_i \oplus Z_j = \lambda_{\{x_i,z_j\}} \stackrel{\text{def}}{=} \lambda(\{x_i, z_j\}) \mid \{x_i, z_j\} \in \mathscr{E}\}$. Note that node $x_i \in \mathscr{X}$ corresponds to the variable X_i and node $z_i \in \mathscr{Z}$

[6] Convention. For $\ell = 0$, we simply write $h(\mathscr{B}_\alpha, L^{[1]}) \stackrel{\text{def}}{=} h(\mathscr{B}_\alpha)$.

corresponds to the variable Z_i and an edge $\{x_i, z_j\}$ corresponds to the equation $X_i \oplus Z_j = \lambda_{\{x_i,z_j\}}$. The pair of injective functions $P : \mathscr{X} \to \{0,1\}^n$ and $Q : \mathscr{Z} \to \{0,1\}^n$ is said to be a an *injective solution* if $P_i \oplus Q_j = \lambda_{\{x_i,z_j\}}$ for all $\{x_i, z_j\} \in \mathscr{E}$, where P_a, Q_b denotes $P(x_a), Q(z_b)$ respectively. Definition for linked graph and labels of a linked graph for acyclic labelled bipartite graph is exactly same as defined for single permutation case. However, the criterion for valid label is somewhat different, which says that, for $\ell \geq 1$, necessary conditions for existence of an injective solution for an l-linked labelled bipartite graph with label $\tau = (\mathscr{B}_\alpha, L^{[2\ell+1]})$ is the following: for all $1 \leq i < j \leq 2\ell + 1$, with $j - i$ being an odd number, $L_i \oplus L_{i+1} \oplus \cdots \oplus L_j \neq 0^n$. Any such label τ is called **valid**. The set of all valid ℓ-linked labels is denoted by U_ℓ and the set of all $L^{[2\ell+1]}$ satisfying the above condition is denote by U'_ℓ.

Remark 2. We note that the validity conditions here are quite different than the same permutation case, because here P_i's have to be mutually distinct and so should be the Q_j's, but there can collision between P_i and Q_j, $i, j \in [v]$.

3 Orange, Purple and Combinatorial Lemmas

We begin this section by stating two useful equations called orange and purple equations, which are the starting point of the analysis for both the same permutation and the independent permutation cases. In this section, we first state the orange equation and the higher order purple equations for both the same permutation and a pair of independent permutations followed by stating a combinatorial result which we will use in our future analysis.

3.1 Orange and Purple Equations for Same Permutation

NOTATION. Let $\mathscr{B}_{\alpha+1} = \{\lambda_1, \ldots, \lambda_{\alpha+1}\}$, where each $\lambda_i \in \{0,1\}^n$, be a multiset of valid 0-linked label of size $\alpha + 1$ and for $\ell \geq 1$, $\tau = (\mathscr{B}_{\alpha+1}, L^{[2\ell+1]}) \in V_\ell$ be a valid ℓ-linked label, where each element of $L^{[2\ell+1]}$ is an element of $\{0,1\}^n$ and $\lambda_{\alpha+1} = L_1, \lambda_\alpha = L_3, \ldots, \lambda_{\alpha-\ell+1} = L_{2\ell+1}$. Moreover, $\mathscr{B}_\alpha = \mathscr{B}_{\alpha+1} \setminus \{\lambda_{\alpha+1}\}$ is a multiset and $L^{[3,2\ell+1]} = (L_3, \ldots, L_{2\ell+1})$ is an ordered tuple. For $\ell \geq 0$, we denote $\delta_{\mathscr{B}_{\alpha-\ell}}(\lambda_{\alpha+1})$ as the number of $i \in [\alpha - \ell]$ such that $\lambda_i = \lambda_{\alpha+1}$ and Δ to be the maximum of such $\delta_{\mathscr{B}_\alpha}(\lambda)$ where the maximum is taken over all λ.

ORANGE EQUATION. To derive the orange equation, we want to estimate $h(\mathscr{B}_{\alpha+1})$ in terms of $h(\mathscr{B}_\alpha)$. For this, we state the following lemma, which we call the "*orange lemma*" as follows:

Lemma 1 (Orange Lemma). *With the notations as defined above, we have*

$$h(\mathscr{B}_{\alpha+1}) = (2^n - 4\alpha + 2\delta_{\mathscr{B}_\alpha}(\lambda_{\alpha+1})) \cdot h(\mathscr{B}_\alpha) + \sum_{L^{[3]} \in \mathscr{M}_3} h(\mathscr{B}_\alpha, L^{[3]}), \qquad (5)$$

where $\mathscr{M}_3 \stackrel{\text{def}}{=} \mathscr{M}_3(\mathscr{B}_{\alpha+1}) = \{\lambda_a \cdot x \cdot \lambda_b \in V'_1 \mid a \neq b \in [\alpha],\ x \in \lambda_{\alpha+1} \oplus \langle \lambda_a, \lambda_b \rangle\}$.

We call Eqn. (5) the "*Orange Equation*".

PURPLE EQUATIONS OF ORDER ℓ. To derive the purple equation of order $\ell \geq 1$, we want to estimate $h(\mathscr{B}_{\alpha+1}, L^{[2\ell+1]})$ in terms of $h(\mathscr{B}_\alpha, L^{[3,2\ell+1]})$. For this, we state the following lemma, which we call the "*purple lemma*" as follows:

Lemma 2 (Purple Lemma). *With the notations as defined above, we have*

$$h(\mathscr{B}_{\alpha+1}, L^{[2\ell+1]}) = h(\mathscr{B}_\alpha, L^{[3,2\ell+1]}) - \sum_{\substack{K^{[2\ell+1]} \\ \in \mathscr{N}_{2\ell+1}}} h(\mathscr{B}_\alpha, K^{[2\ell+1]}) + 2\delta_{\mathscr{B}_{\alpha-\ell}}(\lambda_{\alpha+1}) h(\mathscr{B}_\alpha, L^{[2\ell+1]}) + \sum_{\substack{K^{[2\ell+3]} \\ \in \mathscr{M}_{2\ell+3}}} h(\mathscr{B}_\alpha, K^{[2\ell+3]}), \quad (6)$$

where $\mathscr{N}_{2\ell+1} \stackrel{\text{def}}{=} \mathscr{N}_{2\ell+1}(\tau) = \{\lambda_a \cdot x \cdot L^{[3,2\ell+1]} \in V'_\ell \mid a \in [\alpha-\ell],\, x \in L_2 \oplus \langle L_1 \oplus \lambda_i \rangle\}$ *and* $\mathscr{M}_{2\ell+3} \stackrel{\text{def}}{=} \mathscr{M}_{2\ell+3}(\tau) = \{\lambda_b \cdot x \cdot \lambda_a \cdot y \cdot L^{[3,2\ell+1]} \in V'_{\ell+1} \mid a \neq b \in [\alpha-\ell],\, x \in L_1 \oplus \langle \lambda_a, \lambda_b \rangle, y \in L_2 \oplus \lambda_a\}$.

We call Eqn. (6) the "*Purple Equation of order ℓ*". Proof of the orange and the purple lemma is deferred to Appendix A. We also estimate an upper and a lower bound on the size of $\mathscr{M}_3, \mathscr{N}_{2\ell+1}$ and $\mathscr{M}_{2\ell+3}$ in the following lemma, called "*size lemma*", whose proof is deferred in Appendix B.

Lemma 3 (Size Lemma). *For any valid label $\tau = \mathscr{B}_{\alpha+1}$, $\tau_1 = (\mathscr{B}_{\alpha+1}, L^{[2\ell+1]})$ and $\tau_2 = (\mathscr{B}_{\alpha+1}, L^{[2\ell+3]})$ we have*

(a) $4\alpha(\alpha-1) - 12\alpha\Delta \leq |\mathscr{M}_3(\mathscr{B}_{\alpha+1})| \leq 4\alpha(\alpha-1)$
(b) $4(\alpha-1) - 4\Delta \leq |\mathscr{N}_3(\tau)| \leq 4(\alpha-1)$
(c) $|\mathscr{N}_{2\ell+1}(\tau_1)| - 4 - 4\Delta \leq |\mathscr{N}_{2\ell+3}(\tau_2)| \leq 4(\alpha-1)$
(d) $|\mathscr{M}_{2\ell+3}(\tau_1)| - 8(\alpha-\ell-1) + 4\Delta - 16\Delta(\alpha-\ell-2) \leq |\mathscr{M}_{2\ell+5}(\tau_2)|$
(e) $|\mathscr{M}_{2\ell+5}(\tau_2)| \leq 4(\alpha-\ell-1)(\alpha-\ell-2)$.

3.2 Orange and Purple Equations for a Pair of Independent Permutations

In this section, we state the orange and purple equation for a pair of independent permutations. Notations which are required for stating the equations are almost same as defined in Subsect. 3.1, except the notion of valid label $\tau = (\mathscr{B}_{\alpha+1}, L^{[2\ell+1]}) \in U'_\ell$. As before, to derive the orange equation, we estimate $h(\mathscr{B}_{\alpha+1})$ in terms of $h(\mathscr{B}_\alpha)$, which we state in the form of the following lemma:

Lemma 4 (Orange Lemma for Independent Permutations). *With the similar notations as introduced in Subsect 3.1, we have*

$$h(\mathscr{B}_{\alpha+1}) = (2^n - 2\alpha + \delta_{\mathscr{B}_\alpha}(\lambda_{\alpha+1})) \cdot h(\mathscr{B}_\alpha) + \sum_{L^{[3]} \in \mathscr{M}'_3} h(\mathscr{B}_\alpha, L^{[3]}), \quad (7)$$

where $\mathscr{M}'_3 \stackrel{\text{def}}{=} \mathscr{M}'_3(\mathscr{B}_{\alpha+1}) = \{\lambda_i.\lambda_{\alpha+1}.\lambda_j \in U'_3 \mid i \neq j \in [\alpha]\}$.

Note that, the set $\mathscr{M}_3$ defined in the context of same permutation is significantly different from the set $\mathscr{M}'_3$ defined here. We call Eqn. (7) as "*Orange Equation for a Pair of Independent Permutations*". To derive the purple equation of order $\ell \geq 1$, we estimate $h(\mathscr{B}_{\alpha+1}, L^{[2\ell+1]})$ in terms of $h(\mathscr{B}_\alpha, L^{[3,2\ell+1]})$, which, we state in the form of the following lemma:

Lemma 5 (Purple Lemma for Independent Permutations). *With the similar notations as introduced in Subsect 3.1, we have*

$$h(\mathscr{B}_{\alpha+1}, L^{[2\ell+1]}) = h(\mathscr{B}_\alpha, L^{[3,2\ell+1]}) - \sum_{\substack{K^{[2\ell+1]} \\ \in \mathscr{N}'_{2\ell+1}}} h(\mathscr{B}_\alpha, K^{[2\ell+1]}) + \delta_{\mathscr{B}_{\alpha-\ell}}(\lambda_{\alpha+1}) h(\mathscr{B}_\alpha, L^{[2\ell+1]}) + \sum_{\substack{K^{[2\ell+3]} \\ \in \mathscr{M}'_{2\ell+3}}} h(\mathscr{B}_\alpha, K^{[2\ell+3]}), \quad (8)$$

where $\mathscr{N}'_{2\ell+1} \stackrel{\text{def}}{=} \mathscr{N}'_{2\ell+1}(\tau) = \{\lambda_i.(\lambda_i \oplus L_2 \oplus L_1).L^{[3,2\ell+1]} \in U'_\ell \mid i \in [\alpha - \ell]\} \cup \{\lambda_i.L_2.L^{[3,2\ell+1]} \mid i \in [\alpha - \ell]\}$ *and* $\mathscr{M}'_{2\ell+3} \stackrel{\text{def}}{=} \mathscr{M}'_{2\ell+3}(\tau) = \{\lambda_j.\lambda_{\alpha+1}.\lambda_i.(\lambda_i \oplus L_1 \oplus L_2).L^{[3,2\ell+1]} \in U'_{\ell+1} \mid i \neq j \in [\alpha - \ell]\}$.

Again, note that the set $\mathscr{N}_{2\ell+1}$ and $\mathscr{M}_{2\ell+3}$ defined in the context of same permutation is significantly different from the set $\mathscr{N}'_{2\ell+1}$ and $\mathscr{M}'_{2\ell+3}$ respectively. We call Eqn. (8) as "*Purple Equation of order ℓ for a Pair of Independent Permutations*". We postpone the proof of Lemma 4 and Lemma 5 in Appendix A. As before, we also estimate an upper and a lower bound on the size of $\mathscr{M}'_3, \mathscr{N}'_{2\ell+1}$ and $\mathscr{M}'_{2\ell+3}$ in the following lemma, proof of which is deferred in Appendix C.

Lemma 6 (Size Lemma for Independent Permutations). *For any valid label $\tau = \mathscr{B}_{\alpha+1}$, $\tau_1 = (\mathscr{B}_{\alpha+1}, L^{[2\ell+1]})$ and $\tau_2 = (\mathscr{B}_{\alpha+1}, L^{[2\ell+3]})$ we have*

(a) $|\mathscr{M}'_3(\tau)| = (\alpha - \delta_{\mathscr{B}_\alpha}(\lambda_{\alpha+1}))(\alpha - \delta_{\mathscr{B}_\alpha}(\lambda_{\alpha+1}) - 1)$
(b) $2(\alpha - 1 - \Delta) \leq |\mathscr{N}'_3(\tau)| \leq 2(\alpha - 1)$
(c) $|\mathscr{N}'_{2\ell+1}(\tau_1)| - 2 - 2\Delta \leq |\mathscr{N}'_{2\ell+3}(\tau_2)| \leq 2(\alpha - \ell - 1)$
(d) $|\mathscr{M}'_{2\ell+3}(\tau_1)| - 2(\alpha - \ell - 1) + 2\Delta - \Delta(\alpha - \ell - 2) \leq |\mathscr{M}'_{2\ell+5}(\tau_2)|$
(e) $|\mathscr{M}'_{2\ell+5}(\tau_2)| \leq (\alpha - \ell - 1)(\alpha - \ell - 2)$.

3.3 A Combinatorial Lemma

In this section we state a combinatorial lemma, which would be useful in the final analysis while proving both of our main theorems.

Lemma 7 (Combinatorial Lemma). *Fix integers r, T. We define the double sequence $\{a^k_m\}_{m,k}$ of non-negative rationals, for $1 \leq m \leq T$, as follows:*

- $a^k_m = 0$ *for* $k < 0$.
- *For* $k = 0, \cdots, m-1$,

- $\{a_m^k\}_{m,k}$ *satisfies the recurrence relation,*

$$a_{m+1}^k \le a_m^{k-1} + 2\beta T a_m^k + \beta^2 T^2 a_m^{k+1} + \frac{E\xi}{2^n(2^n-\gamma T)^{T-m+k}} \tag{9}$$

for some constants $\beta, \gamma, E, \xi > 0$.
- $\{a_m^k\}_{m,k}$ *satisfies the inequality*

$$a_m^k \le \frac{2\xi}{(2^n-\gamma T)^{T-m+k+1}} \tag{10}$$

Let $C_r = 2e\beta \cdot 2^{1/r} + \gamma$. *Then for* $rn < T < \frac{2^n}{C_r}$, *the following inequality holds,*

$$\boxed{a_T^0 < \frac{\xi}{2^n(2^n-\gamma T)} \cdot \frac{2^{1/r}}{2^{1/r}-1}\left(2 + \frac{2^{1/r}\cdot E}{2^{1/r}-1}\right)} \tag{11}$$

Interpretation of the Lemma. It is easy to see that from Eqn. (10), one can easily obtains a crude estimation of a_T^0, which is $O(\frac{\xi}{2^n})$. Now, the essence of the lemma is that one can iterate the binomial-type recurrence relation (9) several times (refer Fig. D.1) followed by applying Eqn. (10) to the last level of the iteration to get a much better estimation of a_T^0 in (11), i.e. $O(\xi/2^{2n})$.

Proof. We write $E' = 2^n \cdot E$. To prove the lemma, we first state the following claim:

Claim 1. Let $D = \beta T$. Then, for every $1 \le d \le T-1$,

$$a_T^0 \le \sum_{j=d}^{2d} \binom{2d}{j} D^j a_{T-d}^{j-d} + \sum_{t=0}^{d-1}\sum_{j=t}^{2t} \binom{2t}{j} D^j \frac{E'\cdot\xi}{(2^n-\gamma T)^{j+1}}.$$

Proof of the claim is deferred in Appendix D.

Resuming the proof. Using $d = rn$ in Claim 1 (as $rn \le T-1$), we get,

$$a_T^0 \le \sum_{j=rn}^{2rn} \binom{2rn}{j} D^j a_{T-rn}^{j-rn} + \sum_{t=0}^{rn-1}\sum_{j=t}^{2t} \binom{2t}{j} D^j \frac{E'\cdot\xi}{(2^n-\gamma T)^{j+1}}. \tag{12}$$

Using Eqn. (10), we have

$$\begin{aligned}
\sum_{j=rn}^{2rn} \binom{2rn}{j} D^j a_{T-rn}^{j-rn} &= \sum_{j=rn}^{2rn} \binom{2rn}{j} D^j \frac{2\xi}{(2^n-\gamma T)^{j+1}} \\
&= \frac{2\xi}{2^n-\gamma T} \sum_{j=rn}^{2rn} \binom{2rn}{j} \left(\frac{D}{2^n-\gamma T}\right)^j \\
&\overset{(\star)}{\le} \frac{2\xi}{2^n-\gamma T} \sum_{j=rn}^{2rn} \left(\frac{2eD}{2^n-\gamma T}\right)^j,
\end{aligned} \tag{13}$$

where $(\star)$ follows from the inequality $\binom{n}{k} \leq \left(\frac{en}{k}\right)^k$, since that implies $\binom{2rn}{j} \leq \left(\frac{2rne}{j}\right)^j \leq (2e)^j$ as $j \geq rn$. As, $T < \frac{2^n}{2\beta \cdot 2^{1/r}e+\gamma}$, we have $2 \cdot 2^{1/r}eD + \gamma T = (2\beta \cdot 2^{1/r}e + \gamma)T < 2^n$, which implies $\frac{2eD}{2^n - \gamma T} < \frac{1}{2^{1/r}}$. Therefore,

$$\sum_{j=rn}^{2rn} \left(\frac{2eD}{2^n - \gamma T}\right)^j < \left(\frac{1}{2^{1/r}}\right)^{rn} \sum_{j=0}^{\infty} 2^{-j/r} = \frac{1}{2^n} \cdot \frac{2^{1/r}}{2^{1/r} - 1}. \tag{14}$$

Using Eqn. (13) and Eqn. (14), we have

$$\sum_{j=rn}^{2rn} \binom{2rn}{j} D^j a_{T-rn}^{j-rn} < \frac{2 \cdot 2^{1/r} \cdot \xi}{2^n(2^n - \gamma T)(2^{1/r} - 1)}. \tag{15}$$

Similarly, we have

$$\begin{aligned} \sum_{t=0}^{rn-1} \sum_{j=t}^{2t} \binom{2t}{j} D^j \frac{E' \cdot \xi}{(2^n - \gamma T)^{j+1}} &< \frac{E' \cdot \xi}{2^n - \gamma T} \cdot \sum_{t=0}^{rn-1} \frac{2^{1/r}}{2^{t/r}(2^{1/r} - 1)} \\ &< \frac{E' \cdot \xi}{2^n - \gamma T} \cdot \left(\frac{2^{1/r}}{2^{1/r} - 1}\right)^2. \end{aligned} \tag{16}$$

Thus, from (12), (15) and (16), we get

$$a_T^0 < \frac{2^{1/r} \cdot \xi}{(2^n - \gamma T)(2^{1/r} - 1)} \left(\frac{1}{2^{n-1}} + \frac{2^{1/r} \cdot E'}{2^{1/r} - 1}\right),$$

which proves the result of Lemma 7. □

4 Proof of Theorem 1: Mirror Theory with $(\xi_{\max}, \theta) = (2, 33.1)$

NOTATION. For the simplicity of the notation, we use δ to denote $\delta_{\mathscr{B}_q}(\lambda_{q+1})$, for a fixed $\lambda_{q+1} \in \{0,1\}^n$ and Δ to denote the maximum of $\delta_{\mathscr{B}_q}(\lambda)$, where the maximum is taken over all $\lambda \in \{0,1\}^n$. It is to be noted that the labels of the base edges of a zero-linked graph G can be re-ordered without changing the number of solutions. This is because any such re-ordering would generate another zero-linked graph G' which is label isomorphic to G, and due to the Defn. 1, we can uniquely associate all such label isomorphic graphs. This justification essentially allows us to reorder λ values of $\mathscr{B}_{q+1}$ so that $\delta + 1 = \Delta$ [7]. In the foregoing discussion, we will use the shorthand notation h_α to denote $h(\mathscr{B}_\alpha)$.

[7] Suppose $\lambda \in \{0,1\}^n$ is the value with maximum number of multicollisions among the base labels $\lambda_1, \cdots, \lambda_{\alpha+1}$. Set $\lambda_{\alpha+1} = \lambda$. Then $\delta + 1 =$ #multicollisions of $\lambda_{\alpha+1}$ among base labels $= \Delta$. We would like to note here, that, Patarin used an incorrect assumption in [32], where it was stated that labels can be reordered so that $\delta = \Delta$, which is not possible.

We define $H_{2q} = 2^{nq} h_q$ and $J_{2q} = (2^n)_{2q}$. These notations allows us to reformulate the theorem statement $h_{q+1} \geq \frac{(2^n)_{2q+2}}{2^{n(q+1)}}$, as

$$H_{2q+2} \geq J_{2q+2}. \tag{17}$$

It is obvious to see that Eqn. (17) holds true for $q = 0$, as $H_2 = 2^{2n} > (2^n)_2 = J_2$. To prove Eqn. (17) via induction, we show the following:

$$\frac{H_{2q+2}}{J_{2q+2}} \geq \frac{H_{2q}}{J_{2q}},\ 1 \leq q \leq 2^n/33.1. \tag{18}$$

Moreover, Eqn. (18) also holds true for all q such that $2q(2q+1) \leq 2^n$ [28]. Therefore, we assume that $2^{n/2-1} - 1 < q \leq 2^n/33.1$.[8] If $n \geq 12$, we have $2^{n/2-1} - 1 \geq 2n$, and hence $q > 2n$. Therefore, we just need to show that Eqn. (18) holds true for $2n \leq q \leq 2^n/33.1$. To prove this, we need an important result called "h'_α **property**", suggested by Patarin [32], which is the central result of this paper. In the following lemma, we state the h'_α property, proof of which is deferred in Sect. 5.

Lemma 8 (h'_α property). *If $2n < q < \frac{2^n}{6\sqrt{2}e+4} \approx \frac{2^n}{27.1}$, then for any $L^{[3]} \in \mathscr{M}_3(\mathscr{B}_q)$, where $\mathscr{M}_3(\cdot)$ is defined in Lemma 1 of Sect. 3.1, we have*

$$h(\mathscr{B}_q, L^{[3]}) \geq \frac{h_q}{2^n}\left(1 - \frac{C_1\Delta}{2^n\left(1-\frac{4q}{2^n}\right)} - \frac{C_2 q\Delta}{2^{2n}\left(1-\frac{4q}{2^n}\right)^2}\right), \tag{19}$$

where $C_1 = 2\frac{\sqrt{2}}{\sqrt{2}-1} + 8\left(\frac{\sqrt{2}}{\sqrt{2}-1}\right)^2$ and $C_2 = 24\left(\frac{\sqrt{2}}{\sqrt{2}-1}\right)^2$.

Resuming Proof of Theorem 1. We have assumed that $2n < q < \frac{2^n}{33.1}$, and hence q satisfies the bounds given in Lemma 8 (i.e. $2n < q < \frac{2^n}{6\sqrt{2}e+4}$). Therefore, we can apply the lemma to the orange equation (i.e., Eqn. (5)) and get,

$$\begin{aligned}\frac{h_{q+1}}{2^n} &= h_q\left(1 - \frac{4q}{2^n} + \frac{2\delta}{2^n}\right) + \frac{1}{2^n}\sum_{L^{[3]}\in\mathscr{M}_3} h(\mathscr{B}_q, L^{[3]}) \\ &\overset{(1)}{\geq} h_q\left(1 - \frac{4q}{2^n} + \frac{2\delta}{2^n} + \frac{|\mathscr{M}_3|}{2^{2n}}\left(1 - \frac{C_1\Delta}{2^n\left(1-\frac{4q}{2^n}\right)} - \frac{C_2 q\Delta}{2^{2n}\left(1-\frac{4q}{2^n}\right)^2}\right)\right)\end{aligned} \tag{20}$$

where (1) follows from Lemma 8. Note that,

$$\frac{H_{2q+2}}{H_{2q}} = 2^n\frac{h_{q+1}}{h_q},\quad \frac{J_{2q+2}}{J_{2q}} = (2^n - (2q+1))(2^n - 2q). \tag{21}$$

[8] As $2q+1 \leq 2^{n/2} - 1 \Rightarrow 2q(2q+1) \leq 2^n$

From Eqn. (20), Eqn. (21) and by plug-in $|\mathscr{M}_3| \leq 4q(q-1) - 12q\Delta$ (follows from part (a) of Lemma 3) into Eqn. (20), we have

$$\frac{H_{2q+2}}{J_{2q+2}} \geq \frac{1 - \frac{4q}{2^n} + \frac{2\delta}{2^n} + \frac{4q(q-1)-12q\Delta}{2^{2n}} \left(1 - \frac{C_1\Delta}{2^n\left(1-\frac{4q}{2^n}\right)} - \frac{C_2 q\Delta}{2^{2n}\left(1-\frac{4q}{2^n}\right)^2}\right)}{1 - \frac{4q+1}{2^n} + \frac{2q(2q+1)}{2^{2n}}} \frac{H_{2q}}{J_{2q}}$$

$$\overset{(2)}{=} \left(1 + \frac{\frac{1}{2^n} + \frac{2\delta}{2^n} + \frac{-6q-12q(\delta+1)}{2^{2n}} - \frac{4C_1(\delta+1)q^2}{2^{3n}\left(1-\frac{4q}{2^n}\right)} - \frac{4C_2(\delta+1)q^3}{2^{4n}\left(1-\frac{4q}{2^n}\right)^2}}{1 - \frac{4q+1}{2^n} + \frac{2q(2q+1)}{2^{2n}}}\right) \frac{H_{2q}}{J_{2q}}$$

where (2) follows from the fact that $(4q(q-1) - 12q\Delta) < 4q^2$ and the indices can be reordered so that $\Delta = \delta + 1$. Let A denotes the numerator of (2). Then, we have,

$$\mathsf{A} = \frac{2\delta}{2^n}\left(1 - \frac{6q}{2^n} - \frac{2C_1q^2}{2^{2n}\left(1-\frac{4q}{2^n}\right)} - \frac{2C_2q^3}{2^{3n}\left(1-\frac{4q}{2^n}\right)^2}\right) + \frac{1}{2^n}\left(1 - \frac{18q}{2^n} - \frac{4C_1q^2}{2^{2n}\left(1-\frac{4q}{2^n}\right)} - \frac{4C_2q^3}{2^{3n}\left(1-\frac{4q}{2^n}\right)^2}\right).$$

Note that, $\mathsf{A} > 0$ for $q < \frac{2^n}{33.1}$, as the functions $f(x) = 1 - 6x - 2C_1\frac{x^2}{1-4x} - 2C_2\frac{x^3}{(1-4x)^2} \geq 0$ and $g(x) = 1 - 18x - 4C_1\frac{x^2}{1-4x} - 4C_2\frac{x^3}{(1-4x)^2} \geq 0$, $\forall 0 \leq x \leq \frac{1}{33.1}$. Therefore, we have proved that Eqn. (18) holds for $2n \leq q \leq \frac{2^n}{33.1}$. □

5 Proof of Lemma 8 : h'_α-property

Before we begin the proof, we first introduce the notion of a *derived multiset* for a given multiset $\mathscr{B}_q = \{\lambda_1, \ldots, \lambda_q\}$, where $\lambda_i \in \{0,1\}^n \setminus \{0^n\}$.

Derived ℓ-linked Graph: Given a zero-linked graph with q base edges, we derive a collection of ℓ-linked graph with $\alpha(\leq q)$ base edges by removing some $q - \alpha$ base edges followed by adding ℓ many linking edges connecting $\ell + 1$ base edges (which turns out to be linked base edges). We define derived labels corresponding to the derived graphs as follows:

Definition 2. *We call the tuple $(\mathscr{B}_\alpha, L^{[2\ell+1]})$ is (ℓ, d)-derived from a base label $\mathscr{B}_q$ if $\mathscr{B}_\alpha \subseteq \mathscr{B}_q$ with $\alpha = q - d, \ell \leq \alpha - 1$, and $(\mathscr{B}_\alpha, L^{[2\ell+1]})$, a valid linked label.*

With this ammunition, we define the A-term. Let $(\mathscr{B}_\alpha, L^{[2\ell+1]}) \in V_\ell$ be a valid label. Then we define the ℓ-th order A term as follows:

$$A(\mathscr{B}_\alpha, L^{[2\ell+1]}) \overset{\text{def}}{=} \left| h(\mathscr{B}_\alpha, L^{[2\ell+1]}) - \frac{h(\mathscr{B}_\alpha, L^{[2\ell-1]})}{2^n} \right|. \tag{22}$$

According to our convention, we note that the 1st order A term (i.e. for $\ell = 1$) turns out to be:

$$A(\mathscr{B}_\alpha, L^{[3]}) \overset{\text{def}}{=} \left| h(\mathscr{B}_\alpha, L^{[3]}) - \frac{h(\mathscr{B}_\alpha)}{2^n} \right|. \tag{23}$$

Having defined the first order and the ℓ-th order A term, let us define the following: for $\ell \geq 1$, we define

$$A_{\alpha}^{[\ell-1]} \stackrel{\text{def}}{=} \max\{A(\mathscr{B}_{\alpha}, L^{[2\ell+1]}) \text{ such that } (\mathscr{B}_{\alpha}, L^{[2\ell+1]}) \text{ is } (q-\alpha,\ell)\text{-derived from } \mathscr{B}_q\}.$$

Recipe of the proof. Now, we give a brief outline of the proof of Lemma 8. We carry out the proof in a modular way. We first state a derived inequality lemma (i.e., Lemma 9) which gives an upper bound on $A_{\alpha}^{[\ell-1]}$ followed by stating a general order central lemma (i.e., Lemma 10) which gives a recurrence relation on A values. We combine this recurrence relation with the combinatorial lemma to get an upper bound on $A_q^{[0]}$. This upper bound is sufficient to prove Lemma‘8. In the following, we first state the derived inequality lemma, proof of which is deferred in Sect. 6.

Lemma 9 (Derived Inequality Lemma). *Let $\alpha \stackrel{\text{def}}{=} q - d$ for two positive integers q, d such that $d < q$. If $(\mathscr{B}_{\alpha}, L^{[2\ell+1]})$ is (ℓ, d)-derived from a base label $\mathscr{B}_q$, then we have,*

$$(a)\ h(\mathscr{B}_{\alpha}, L^{[2\ell+1]}) \leq \frac{h_q}{(2^n-4q)^{d+\ell}}, \quad (b)\ A(\mathscr{B}_{\alpha}, L^{[2\ell+1]}) \leq \frac{2h_q}{(2^n-4q)^{d+\ell}}.$$

Note that, these inequalities are applicable for $(\mathscr{B}_{\alpha}, L^{[2\ell+1]})$ only when it is (ℓ, d)-derived from the base label $\mathscr{B}_q$. As $A(\mathscr{B}_{\alpha}, L^{[2\ell+1]})$ follows inequality (b) of Lemma 9, for all $(\mathscr{B}_{\alpha}, L^{[2\ell+1]})$ that is (ℓ, d)-derived from $\mathscr{B}_q$, we get

$$A_{\alpha}^{[\ell-1]} \leq \frac{2h_q}{(2^n-4q)^{q-\alpha+\ell}}. \quad (\text{ by putting } d = q-\alpha) \tag{24}$$

Now, it is to be noted that $A(\mathscr{B}_q, L^{[3]}) \stackrel{(\dagger)}{\leq} A_q^{[0]}$ and we would like to establish the following inequality:

$$A_q^{[0]} \leq \frac{h_q}{2^n}\left(\frac{C_1\Delta}{2^n\left(1-\frac{4q}{2^n}\right)} + \frac{C_2 q\Delta}{2^{2n}\left(1-\frac{4q}{2^n}\right)^2}\right). \tag{25}$$

For the time being if we assume that the Eqn. (25) is correct, then from Eqn. (23), Eqn. (25) and from (†), we have

$$h(\mathscr{B}_{\alpha}, L^{[3]}) - \frac{h(\mathscr{B}_{\alpha})}{2^n} \geq -\frac{h_q}{2^n}\left(\frac{C_1\Delta}{2^n\left(1-\frac{4q}{2^n}\right)} + \frac{C_2 q\Delta}{2^{2n}\left(1-\frac{4q}{2^n}\right)^2}\right),$$

which proves the h'_{α} property lemma. Thus, our focus is now shifted to prove the inequality stated in Eqn. (25). For proving this, we use the following lemma, which we call the *general order central lemma*, proof of which is deferred in Sect. 6.

Lemma 10 (General Order Central Lemma). *With the notation $A_{\alpha}^{[\ell-1]}$ for $\ell \geq 1$, as defined above, we have the following recurrence relation:*

$$A_{\alpha+1}^{[\ell]} \leq A_{\alpha}^{[\ell-1]} + 6qA_{\alpha}^{[\ell]} + 9q^2A_{\alpha}^{[\ell+1]} + \frac{h_q}{(2^n-4q)^{q-\alpha+\ell}}\left(\frac{8\Delta}{2^n} + \frac{24q\Delta}{2^n(2^n-4q)}\right).$$

Resuming Proof of Lemma 8. Now, we recognize that $\{A_\alpha^{[\ell]}\}_{\alpha \le q, \ell \le \alpha-1}$ satisfies the conditions for a double sequence as stated in the combinatorial lemma (i.e. Lemma 7), with $r = 2$, $T = q$, $\beta = 3$, $\gamma = 4$, $\xi = h_q$ and $E = 8\Delta + \frac{24q\Delta}{(2^n - 4q)}$. Thus, we can directly apply Eqn. (11) to get the following

$$A_q^{[0]} < \frac{h_q}{2^n}\left(\frac{2\frac{\sqrt{2}}{\sqrt{2}-1}}{2^n\left(1-\frac{4q}{2^n}\right)} + \left(\frac{\sqrt{2}}{\sqrt{2}-1}\right)^2 \frac{8\Delta}{2^n\left(1-\frac{4q}{2^n}\right)} + \left(\frac{\sqrt{2}}{\sqrt{2}-1}\right)^2 \frac{24q\Delta}{2^{2n}\left(1-\frac{4q}{2^n}\right)^2}\right)$$

$$\overset{(\star)}{\le} \frac{h_q}{2^n}\left(\underbrace{\left(2\frac{\sqrt{2}}{\sqrt{2}-1} + 8\left(\frac{\sqrt{2}}{\sqrt{2}-1}\right)^2\right)}_{C_1} \frac{\Delta}{2^n\left(1-\frac{4q}{2^n}\right)} + \underbrace{24\left(\frac{\sqrt{2}}{\sqrt{2}-1}\right)^2}_{C_2} \frac{q\Delta}{2^{2n}\left(1-\frac{4q}{2^n}\right)^2}\right),$$

for $q < \frac{2^n}{6\sqrt{2}e+4}$, where $(\star)$ follows from the fact that $\Delta \ge 1$. This completes the proof. □

6 Proof of Lemma 9 and Lemma 10

6.1 Proof of Derived Inequality Lemma

As the order of coefficients does not matter, without loss of generality, we assume that $\mathscr{B}_\alpha = \{\lambda_1, \cdots, \lambda_\alpha\}$ where $\mathscr{B}_q = \{\lambda_1, \cdots, \lambda_q\}$. Let us represent a solution, $(P_1, \cdots, P_{2\alpha})$ of $\mathbb{E}_G$ where G is an ℓ -linked graph labeled by a valid label $\tau = (\mathscr{B}_\alpha, L^{[2\ell+1]})$, by a graph E_G which is isomorphic to G, except that, the node in G corresponding to the variable $Y_i,\ i \in [2\alpha]$, is replaced by a node having the value $P_i,\ i \in [2\alpha]$ in E_G.

Let E_{G_1} be the representation of a solution of $\mathbb{E}_{G_1}$ where G_1 is an zero-linked graph with labelling $\tau = \mathscr{B}_\alpha$. We recursively add d disjoint edges to E_{G_1}. When we add the i^{th} edge, $i = 1, \cdots, d$, we assign any one of $2^n - 4\alpha + 2\delta_{\mathscr{B}_{\alpha+i-1}}(\lambda_{\alpha+i})$ values $\big($size of $\{0,1\}^n \setminus \big(\{P_1, \cdots, P_{2\alpha+i-1}\} \cup \{P_1 \oplus \lambda_{\alpha+i}, \cdots, P_{2\alpha} \oplus \lambda_{\alpha+i}\}\big)\big)$ to one of the two nodes of the edge, and assign the value $\lambda_{\alpha+i}$ to that edge (See Fig. 6.1).

Thus we get representations of $\prod_{i=0}^{d-1}(2^n - 4(\alpha'+i) + 2\delta_{\mathscr{B}_{\alpha+i}}(\lambda_{\alpha+i+1})) > (2^n - 4q)^d$ solutions to $\mathbb{E}_G$, where G is the zero-linked graph with labelling $\tau = \mathscr{B}_q$. Hence,

$$h(\mathscr{B}_\alpha) \le \frac{h_q}{(2^n - 4q)^d}.$$

Now, let E_{G_2} be the representation of a solution of $\mathbb{E}_{G_2}$ where G_2 is an ℓ-linked graph with labelling $\tau = (\mathscr{B}_\alpha, L^{[2\ell+1]})$. Let us reorder the indices such that $L_1 = \lambda_1, \cdots, L_{2\ell+1} = \lambda_{\ell+1}$. We recursively remove the ℓ links from E_{G_2}. When we remove the i^{th} link from the last, $L_{2(\ell-i+1)}$, from E_{G_2}, we put one of the $2^n - 4(\alpha - 1) + 2\delta_{\mathscr{B}_{\ell-i+1}}(\lambda_{\ell-i+2})$ values of $\{0,1\}^n \setminus \big(\{P_1, \cdots, P_{2(\ell-i+1)}, P_{2(\ell-i+2)+1}, \cdots, P_{2\alpha}\} \cup \{P_1 \oplus \lambda_{\ell-i+2}, \cdots, P_{2(\ell-i+1)} \oplus \lambda_{\ell-i+2}, P_{2(\ell-i+2)+1} \oplus \lambda_{\ell-i+2}, \cdots, P_{2\alpha} \oplus \lambda_{\ell-i+2}\}\big)$

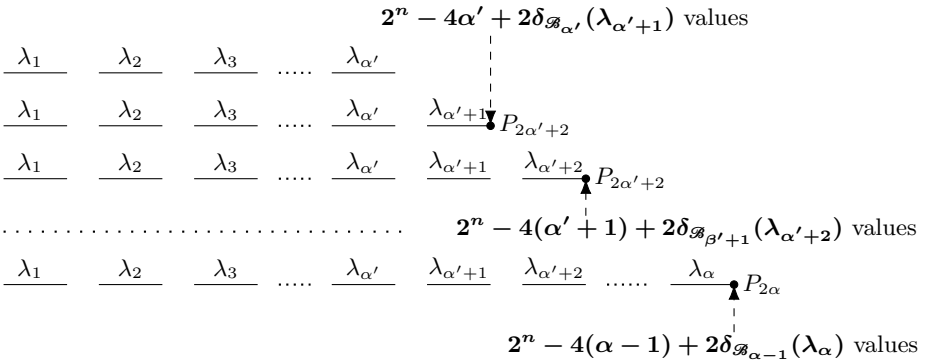

Fig. 6.1: Adding d edges to the graph E_{G_1} resulting in $\prod_{i=0}^{d-1}(2^n - 4(\alpha' + i) + 2\delta_{\mathscr{B}_{\alpha'+i}}(\lambda_{\alpha'+i+1}))$ solutions of $\mathbb{E}_G$

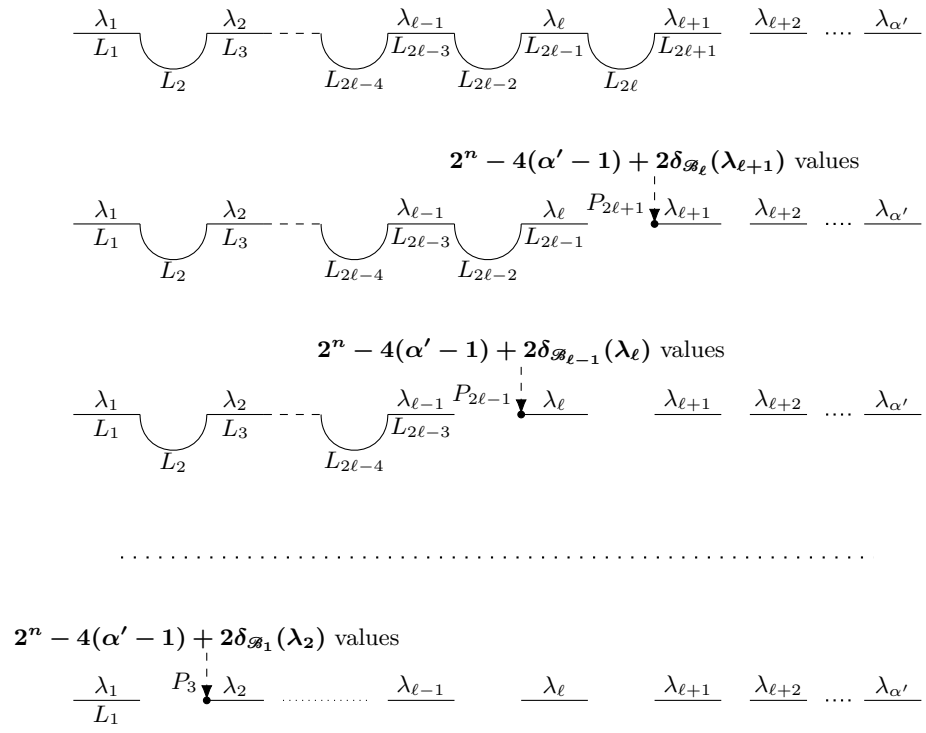

Fig. 6.2: Removing ℓ links from E_{G_2} to get $\prod_{i=1}^{\ell}(2^n - 4(\alpha' - 1) + 2\delta_{\mathscr{B}_i}(\lambda_{i+1}))$ solutions to $\mathbb{E}_{G_1}$

as the value of one of the nodes of the edge that got disjoint from the linked system (See Fig. 6.2).

Thus, we get $\prod_{i=1}^{\mu}(2^n - 4(\alpha' - 1) + 2\delta_{\mathscr{B}_i}(\lambda_{i+1})) > (2^n - 4q)^\ell$ solutions to $\mathbb{E}_{G_1}$ from one solution of $\mathbb{E}_{G_2}$. Hence, we get

$$h(\mathscr{B}_\alpha, L^{[2\ell+1]}) \leq \frac{h_\alpha}{(2^n - 4q)^\ell} \leq \frac{h_q}{(2^n - 4q)^{d+\ell}},$$

which completes part (a) of the lemma. □

Now, for part (b) we have

$$\begin{aligned} A(\mathscr{B}_\alpha, L^{[2\ell+1]}) &\leq \left| h(\mathscr{B}_q, L^{[2\ell+1]}) - \frac{h(\mathscr{B}_q, L^{[2\ell-1]})}{2^n} \right| \\ &\leq \frac{h_q}{(2^n - 4q)^{d+\ell}} + \frac{h_q}{2^n(2^n - 4q)^{d+\ell-1}} \\ &\leq \frac{2h_q)}{(2^n - 4q)^{d+\ell}}. \qquad \square \end{aligned}$$

6.2 Proof of General Order Central Lemma

NOTATION. We write $\delta^{(\ell)}$ to denote $\delta_{\mathscr{B}_{\alpha-\ell}}(\lambda_{\alpha+1})$. We also use the shorthand notation $h_a(L^{[2\mu+1]})$ to represent $h(\mathscr{B}_a, L^{[2\mu+1]})$.

We prove the general order central lemma in two parts: in the first part we prove central lemma of $\ell + 1$-th order, $\ell \geq 1$, and in the second part we prove central lemma of first order.

6.2.1 Central Lemma of $\ell + 1$-th order ($\ell \geq 1$). Let us consider the purple equation with ℓ links and $\ell + 1$ links respectively.

PURPLE EQUATION WITH ℓ-LINKS

$$\begin{aligned} h_{\alpha+1}(L^{[2\ell+1]}) = h_\alpha(L^{[3,2\ell+1]}) &- \sum_{\substack{K^{[2\ell+1]} \\ \in \mathscr{N}_{2\ell+1}}} h_\alpha(K^{[2\ell+1]}) \\ &+ 2\delta^{(\ell)} h_\alpha(L^{[2\ell+1]}) + \sum_{\substack{K^{[2\ell+3]} \\ \in \mathscr{M}_{2\ell+3}}} h_\alpha(K^{[2\ell+3]}). \end{aligned} \tag{26}$$

PURPLE EQUATION WITH $\ell + 1$-LINKS

$$\begin{aligned} h_{\alpha+1}(L^{[2\ell+3]}) = h_\alpha(L^{[3,2\ell+3]}) &- \sum_{\substack{K^{[2\ell+3]} \\ \in \mathscr{N}_{2\ell+3}}} h_\alpha(K^{[2\ell+3]}) \\ &+ 2\delta^{(\ell+1)} h_\alpha(L^{[2\ell+3]}) + \sum_{\substack{K^{[2\ell+5]} \\ \in \mathscr{M}_{2\ell+5}}} h_\alpha(K^{[2\ell+5]}). \end{aligned} \tag{27}$$

By subtracting Eqn. (26) $\times \frac{1}{2^n}$ from Eqn. (27) and using the inequality $\delta^{(\ell+1)} \leq \delta^{(\ell)}$, we get

$$h_{\alpha+1}(L^{[2\ell+3]}) - \frac{h_{\alpha+1}(L^{[2\ell+1]})}{2^n} \leq h_\alpha(L^{[3,2\ell+3]}) - \frac{h_\alpha(L^{[3,2\ell+1]})}{2^n} + \sum\nolimits_\ell + \sum\nolimits^\star + \sum\nolimits^{\star\star} + \mathsf{LO}, \tag{28}$$

where,

$$\sum\nolimits_\ell = 2\delta^{(\ell)}\left(h_\alpha(L^{[2\ell+3]}) - \frac{h_\alpha(L^{[2\ell+1]})}{2^n}\right), \ell = 0, \ldots, \alpha-1.$$

$$\sum\nolimits^\star = \sum_{K^{[2\ell+3]} \in \mathcal{N}_{2\ell+3}} \left(h_\alpha(K^{[2\ell+3]}) - \frac{h_\alpha(K^{[2\ell+1]})}{2^n}\right).$$

$$\sum\nolimits^{\star\star} = \sum_{K^{[2\ell+5]} \in \mathscr{M}_{2\ell+5}} \left(h_\alpha(K^{[2\ell+5]}) - \frac{h_\alpha(K^{[2\ell+3]})}{2^n}\right).$$

$$\mathsf{LO} = \frac{1}{2^n} \sum_{\substack{K^{[2\ell+1]} \in \mathcal{N}_{2\ell+1} \\ \ni K^{[2\ell+3]} \notin \mathcal{N}_{2\ell+3}}} h_\alpha(K^{[2\ell+1]}) + \frac{1}{2^n} \sum_{\substack{K^{[2\ell+3]} \in \mathscr{M}_{2\ell+3} \\ \ni K^{[2\ell+5]} \notin \mathscr{M}_{2\ell+5}}} h_\alpha(K^{[2\ell+3]}).$$

Now we bound each term on the right hand side of Eqn. (28).

$$\left|\sum\nolimits_\ell\right| = 2\delta^{(\ell)}\left|h_\alpha(L^{[2\ell+3]}) - \frac{h_\alpha(L^{[2\ell+1]})}{2^n}\right| \overset{(1)}{\leq} 2\Delta A_\alpha^{[\ell]}. \tag{29}$$

$$\left|\sum\nolimits^\star\right| \leq \sum_{K^{[2\ell+3]} \in \mathcal{N}_{2\ell+3}} A(\mathscr{B}_\alpha, K^{[2\ell+3]}) \leq |\mathcal{N}_{2\ell+3}| A_\alpha^{[\ell]} \overset{(2)}{\leq} 4q A_\alpha^{[\ell]}. \tag{30}$$

$$\left|\sum\nolimits^{\star\star}\right| \leq \sum_{K^{[2\ell+5]} \in \mathscr{M}_{2\ell+5}} A(\mathscr{B}_\alpha, K^{[2\ell+5]}) \leq |\mathscr{M}_{2\ell+5}| A_\alpha^{[\ell+1]} \overset{(3)}{\leq} 4q^2 A_\alpha^{[\ell+1]}. \tag{31}$$

$$\mathsf{LO} = \frac{|\mathcal{N}_{2\ell+1} \setminus \mathcal{N}_{2\ell+3}|}{2^n} \frac{h_q}{(2^n-4q)^{q-\alpha+\ell}} + \frac{|\mathscr{M}_{2\ell+3} \setminus \mathscr{M}_{2\ell+5}|}{2^n} \frac{h_q}{(2^n-4q)^{q-\alpha+\ell+1}}$$
$$\overset{(4)}{\leq} \frac{8\Delta}{2^n} \frac{h_q}{(2^n-4q)^{q-\alpha+\ell}} + \frac{24q\Delta}{2^n} \frac{h_q}{(2^n-4q)^{q-\alpha+\ell+1}} = \frac{h_q \cdot \Delta'}{(2^n-4q)^{q-\alpha+\ell}}. \tag{32}$$

where $\Delta' = \left(\frac{8\Delta}{2^n} + \frac{24q\Delta}{2^n(2^n-4q)}\right)$. Note that (1) follows as $\delta^{(\ell)} \leq \Delta$ and due to the definition of $A_\alpha^{[\ell]}$. Moreover, (2), (3) and (4) follows from Lemma 3 as $|\mathcal{N}_{2\ell+2}| \leq 4(\alpha-1) \leq 4q$, $\mathscr{M}_{2\ell+5} \leq 4(\alpha-\ell-1)(\alpha-\ell-2) \leq 4q^2$, $|\mathcal{N}_{2\ell+1} \setminus \mathcal{N}_{2\ell+3}| \leq 4+4\Delta \leq 8\Delta$ (as $\Delta \geq 1$) and $|\mathscr{M}_{2\ell+3} \setminus \mathscr{M}_{2\ell+5}| \leq 8(\alpha-\ell-1) - 4\Delta + 16\Delta(\alpha-\ell-2) \leq 24\alpha\Delta \leq 24q\Delta$.[9] Now, by taking the absolute value of the both side of Eqn. (28), and

[9] Here we make the abuse of notation by denoting the set of all $K^{[2\ell+3]} \in \mathscr{M}_{2\ell+3}$ such that $K^{[2\ell+5]} \notin \mathscr{M}_{2\ell+5}$ as $\mathscr{M}_{2\ell+3} \setminus \mathscr{M}_{2\ell+5}$. Similarly we denote the set of all $K^{[2\ell+1]} \in \mathcal{N}_{2\ell+1}$ such that $K^{[2\ell+3]} \notin \mathcal{N}_{2\ell+3}$ as $\mathcal{N}_{2\ell+1} \setminus \mathcal{N}_{2\ell+3}$.

using Eqn. (29)-Eqn. (32), we have

$$A(\mathscr{B}_{\alpha+1}, L^{[2\ell+3]}) \leq A(\mathscr{B}_{\alpha}, L^{[3,2\ell+3]}) + (4q+2\Delta)A_{\alpha}^{[\ell]} + 4q^2 A_{\alpha}^{[\ell+1]} + \frac{h_q \cdot \Delta'}{(2^n-4q)^{q-\alpha+\ell}}$$
$$\leq \underbrace{A_{\alpha}^{[\ell-1]}}_{(4)} + \underbrace{6q}_{(5)} A_{\alpha}^{[\ell]} + \underbrace{9q^2}_{(6)} A_{\alpha}^{[\ell+1]} + \frac{h_q \cdot \Delta'}{(2^n-4q)^{q-\alpha+\ell}}, \tag{33}$$

where (4) follows from the fact that $(\mathscr{B}_{\alpha}, L^{[3,2\ell+3]})$ is derived from $\mathscr{B}_q$, (5) follows from the fact that $\Delta \leq q$ and for (6) we just used $9q^2 > 4q^2$. Taking maximum of the left hand side of Eqn. (33) over all $(\mathscr{B}_{\alpha+1}, L^{[2\ell+3]})$ derived from $\mathscr{B}_q$, we get the *purple-purple equation* or the *central lemma of* $(\ell+1)$*-th order* as follows:

$$\boxed{A_{\alpha+1}^{[\ell]} \leq A_{\alpha}^{[\ell-1]} + 6qA_{\alpha}^{[\ell]} + 9q^2 A_{\alpha}^{[\ell+1]} + \frac{h_q}{(2^n-4q)^{q-\alpha+\ell}}\left(\frac{8\Delta}{2^n} + \frac{24q\Delta}{2^n(2^n-4q)}\right).} \tag{34}$$

6.2.2 Central Lemma of first order. By subtracting the (orange equation)$\times \frac{1}{2^n}$ from the first order purple equation, and using Lemma 3 by setting $\ell = 1$ and the inequality $\delta^{(1)} \leq \delta^{(0)} (= \delta)$, we get

$$h_{\alpha+1}(L^{[3]}) - \frac{h_{\alpha+1}}{2^n} \leq \sum\nolimits_0 - \sum\nolimits_{\star} + \sum\nolimits_{\star\star} + \mathsf{LO}, \tag{35}$$

where,

$$\sum\nolimits_{\star} = \sum_{K^{[3]} \in \mathscr{N}_3} \left(h_{\alpha}(K^{[3]}) - \frac{h_{\alpha}}{2^n}\right) \quad \sum\nolimits_{\star\star} = \sum_{K^{[5]} \in \mathscr{M}_5} \left(h_{\alpha}(K^{[5]}) - \frac{h_{\alpha}(K^{[3]})}{2^n}\right)$$
$$\mathsf{LO} = \underbrace{x\frac{h_{\alpha}}{2^n}}_{x \leq 4\Delta+4} - \frac{1}{2^n} \sum_{K^3 \in \mathscr{M}_3 \setminus \mathscr{M}_5} h_{\alpha}(K^{[3]}).$$

Now, we bound each term of the right hand side of Eqn. (35) as before using Lemma 3 and Lemma 9, we get

$$\boxed{A(\mathscr{B}_{\alpha+1}, L^{[3]}) \leq 6qA_{\alpha}^{[0]} + 9q^2 A_{\alpha}^{[1]} + \frac{h_q}{(2^n-4q)^{q-\alpha}}\left(\frac{8\Delta}{2^n} + \frac{24q\Delta}{2^n(2^n-4q)}\right).} \tag{36}$$

Assuming the convention that $A_{\alpha}^{[\ell]} = 0$ for $\ell < 0$, we combine Eqn. (34) and Eqn. (36) to obtain the desired result. □

7 Proof of Theorem 2 : Mirror Theory with $(\xi_{\max}, \theta) = (2, 13)$ for a Pair of Independent Permutations

In this section, we prove Theorem 2, namely the mirror theory for a pair of independent permutations. However, as most of the analysis carried out in this

section will be similar to that of Theorem 1, we will skip unnecessary details of the proof. We basically follow the similar proof plan that we had taken for proving Theorem 1. We recall the notations that δ is used to denote $\delta_{\mathscr{B}_q}(\lambda_{q+1})$ for a fixed $\lambda_{q+1} \in \{0,1\}^n$ and Δ is the maximum of $\delta_{\mathscr{B}_q}(\lambda)$, where the maximum is taken over all $\lambda \in \{0,1\}^n$. As before, we use the shorthand notation h_α to denote $h(\mathscr{B}_\alpha)$ and with a slight abuse of notation, we write H_{2q} to denote $2^{nq}h_q$ and $J_{2q} = (2^n)_q^2$. As we did in proving Theorem 1, we begin the proof by first stating the corresponding h'_α-property for a pair of independent permutations case as follows:

Lemma 11 (h'_α property for a pair of independent permutations). *If $3n < q < \frac{2^n}{3\sqrt[3]{2}e+2} \approx \frac{2^n}{12.27}$, then for any $L^{[3]} \in \mathscr{M}'_3(\mathscr{B}_q)$, where $\mathscr{M}'_3(\cdot)$ is defined in Lemma 4 of Sect. 3.2, we have*

$$h(\mathscr{B}_q, L^{[3]}) \geq \frac{h_q}{2^n}\left(1 - \frac{C_1\Delta}{2^n(1-\frac{2q}{2^n})} - \frac{C_2 q\Delta}{2^{2n}(1-\frac{2q}{2^n})^2}\right),$$

where $C_1 = 2\frac{\sqrt[3]{2}}{\sqrt[3]{2}-1} + 4\left(\frac{\sqrt[3]{2}}{\sqrt[3]{2}-1}\right)^2$ and $C_2 = 3\left(\frac{\sqrt[3]{2}}{\sqrt[3]{2}-1}\right)^2$.

Resuming the proof. We have assumed that $3n < q \leq \frac{2^n}{13}$, and hence q satisfies the bound given in Lemma 11. Therefore, we apply Lemma 11 to the orange equation for independent permutations (i.e., Eqn. (7)) to get

$$\begin{aligned}\frac{h_{q+1}}{2^n} &= h_q\left(1 - \frac{2q}{2^n} + \frac{\delta}{2^n}\right) + \frac{1}{2^n}\sum_{L^{[3]}\in\mathscr{M}'_3} h(\mathscr{B}_q, L^{[3]}) \\ &\overset{(1)}{\geq} h_q\left(1 - \frac{2q}{2^n} + \frac{\delta}{2^n} + \frac{q(q-1)-2q\delta}{2^{2n}}\cdot \mathsf{X}\right), \end{aligned} \tag{37}$$

where (1) follows from the fact that $|\mathscr{M}'_3| = (q-\delta)(q-\delta-1) = q(q-1) - \delta(2q-\delta-1) \geq q(q-1) - 2q\delta$ and X denotes $\left(1 - \frac{C_1\Delta}{2^n(1-\frac{2q}{2^n})} - \frac{C_2 q\Delta}{2^{2n}(1-\frac{2q}{2^n})^2}\right)$. Moreover, we have

$$\frac{H_{2q+2}}{H_{2q}} = 2^n\frac{h_{q+1}}{h_q}, \quad \frac{J_{2q+2}}{J_{2q}} = (2^n - q)^2. \tag{38}$$

Now, from Eqn. (37), Eqn. (38) and by plug-in the value of X in Eqn. (37), we have

$$\begin{aligned}
\frac{H_{2q+2}}{J_{2q+2}} &\geq \frac{1 - \frac{2q}{2^n} + \frac{\delta}{2^n} + \frac{q(q-1)-2q\delta}{2^{2n}} \left(1 - \frac{C_1\Delta}{2^n(1-\frac{2q}{2^n})} - \frac{C_2 q\Delta}{2^{2n}(1-\frac{2q}{2^n})^2}\right)}{1 - \frac{2q}{2^n} + \frac{q^2}{2^{2n}}} \frac{H_{2q}}{J_{2q}} \\
&\overset{(2)}{\geq} \frac{\left(1 - \frac{2q}{2^n} + \frac{q^2}{2^{2n}}\right) + \frac{\delta}{2^n} - \frac{q+2q\delta}{2^{2n}} - \frac{q^2}{2^{2n}} \left(\frac{C_1\Delta}{2^n(1-\frac{2q}{2^n})} + \frac{C_2 q\Delta}{2^{2n}(1-\frac{2q}{2^n})^2}\right)}{1 - \frac{2q}{2^n} + \frac{q^2}{2^{2n}}} \frac{H_{2q}}{J_{2q}} \\
&= \left(1 + \frac{\frac{\delta}{2^n} - \frac{q+2q\delta}{2^{2n}} - \frac{q^2}{2^{2n}} \left(\frac{C_1\Delta}{2^n(1-\frac{2q}{2^n})} + \frac{C_2 q\Delta}{2^{2n}(1-\frac{2q}{2^n})^2}\right)}{1 - \frac{2q}{2^n} + \frac{q^2}{2^{2n}}}\right) \frac{H_{2q}}{J_{2q}} \\
&\overset{(3)}{=} \left(1 + \frac{\frac{\delta}{2^n} - \frac{q+2q\delta}{2^{2n}} - \frac{q^2}{2^{2n}} \left(\frac{C_1(\delta+1)}{2^n(1-\frac{2q}{2^n})} + \frac{C_2 q(\delta+1)}{2^{2n}(1-\frac{2q}{2^n})^2}\right)}{1 - \frac{2q}{2^n} + \frac{q^2}{2^{2n}}}\right) \frac{H_{2q}}{J_{2q}},
\end{aligned}$$

where (2) follows from the fact that $q(q-1) - 2q\delta < q^2$ and (3) follows from the fact that the base labels can be re-ordered so that $\Delta = \delta + 1$ [10]. We have,

$$\begin{aligned}
&\frac{\delta}{2^n} - \frac{2q\delta}{2^{2n}} - \frac{C_1\delta q^2}{2^{3n}(1-\frac{2q}{2^n})} - \frac{C_2\delta q^3}{2^{4n}(1-\frac{2q}{2^n})^2} \\
&\qquad = \frac{\delta}{2^n}\left(1 - \frac{2q}{2^n} - \frac{C_1 q^2}{2^{2n}(1-\frac{2q}{2^n})} - \frac{C_2 q^3}{2^{3n}(1-\frac{2q}{2^n})^2}\right) > 0
\end{aligned}$$

for $q < \frac{2^n}{13}$, as the function $f(x) = 1 - 2x - \frac{C_1 x^2}{1-2x} - \frac{C_2 x^3}{(1-2x)^2} > 0,\ \forall\ 0 \leq x \leq \frac{1}{13}$. Thus, for $3n < q < \frac{2^n}{13}$ we get

$$\frac{H_{2q+2}}{J_{2q+2}} \geq \left(1 - \frac{\frac{q}{2^{2n}} - \frac{C_1 q^2}{2^{3n}(1-\frac{2q}{2^n})} - \frac{C_2 q^3}{2^{4n}(1-\frac{2q}{2^n})^2}}{1 - \frac{2q}{2^n} + \frac{q^2}{2^{2n}}}\right) \frac{H_{2q}}{J_{2q}} \geq (1 - \epsilon(q))\, \frac{H_{2q}}{J_{2q}},$$

where $\epsilon(q) = \frac{\frac{q}{2^{2n}}}{1 - \frac{2q}{2^n} + \frac{q^2}{2^{2n}}}$. Therefore, by inducting on q, we have

$$\begin{aligned}
\frac{H_{2q+2}}{J_{2q+2}} &\geq (1-\epsilon(q))(1-\epsilon(q-1)) \cdots (1-\epsilon(3n)) \frac{H_{6n}}{J_{6n}} \overset{(4)}{\geq} (1-\epsilon(q))^{q-3n} \frac{H_{6n}}{J_{6n}} \\
&\geq (1-\epsilon(q))^q \frac{H_{6n}}{J_{6n}} \overset{(5)}{\geq} \left(1 - \frac{\frac{q^2}{2^{2n}}}{1 - \frac{2q}{2^n} + \frac{q^2}{2^{2n}}}\right) \frac{H_{6n}}{J_{6n}}, \quad (39)
\end{aligned}$$

where (4) follows from the fact that $\epsilon(q)$ is increasing in q as the function $g(x) = \frac{x}{(1-x)^2}$ is increasing for $0 \leq x < 1$, and (5) follows from binomial theorem. Now, we are left to bound H_{6n}/J_{6n}.

[10] The base labels can be re-ordered in a similar way that we have applied for the same permutation case. Due to the label isomorphism, the number of solutions remain invariant.

BOUNDING H_{6n}/J_{6n}: From the orange equation for a pair of independent permutations, we can see that

$$h(\mathscr{B}_{\alpha+1}) \geq h(\mathscr{B}_{\alpha})(2^n - 2\alpha). \tag{40}$$

Now, by doing the similar calculations as above on Eqn. (40), we derive the following:

$$\frac{H_{2\alpha+2}}{J_{2\alpha+2}} \geq \left(1 - \frac{\frac{\alpha^2}{2^{2n}}}{1 - \frac{2\alpha}{2^n} + \frac{\alpha^2}{2^{2n}}}\right) \frac{H_{2\alpha}}{J_{2\alpha}},$$

for all $1 \leq \alpha < 2^n$. Iterating the inequality and using the fact that the function $\frac{x^2}{(1-x)^2}$ is increasing for $0 \leq x < 1$, we get

$$\frac{H_{2\alpha+2}}{J_{2\alpha+2}} \geq \left(1 - \frac{\frac{\alpha^3}{2^{2n}}}{1 - \frac{2\alpha}{2^n} + \frac{\alpha^2}{2^{2n}}}\right) \frac{H_2}{J_2} \overset{(6)}{=} \left(1 - \frac{\frac{\alpha^3}{2^{2n}}}{1 - \frac{2\alpha}{2^n} + \frac{\alpha^2}{2^{2n}}}\right), \tag{41}$$

where (6) follows due to $H_2 = J_2 = 2^{2n}$. Hence, by substituting $\alpha = 3n - 1$ in Eqn. (41), we get

$$\frac{H_{6n}}{J_{6n}} \geq \left(1 - \frac{\frac{(3n-1)^3}{2^{2n}}}{1 - \frac{2(3n-1)}{2^n} + \frac{(3n-1)^2}{2^{2n}}}\right). \tag{42}$$

By substituting Eqn. (42) in Eqn. (39), we get the following which holds true for all $q \leq \frac{2^n}{13}$.

$$\begin{aligned} H_{2q+2} &\geq \left(1 - \frac{\frac{q^2}{2^{2n}}}{1 - \frac{2q}{2^n} + \frac{q^2}{2^{2n}}}\right)\left(1 - \frac{(3n-1)^3}{(2^n - (3n-1))^2}\right) J_{2q+2} \\ &\overset{(7)}{\geq} \left(1 - \frac{1.2q^2}{2^{2n}}\right)\left(1 - \frac{108n^3}{2^{2n}}\right) J_{2q+2} \geq \left(1 - \frac{1.2q^2}{2^{2n}} - \frac{108n^3}{2^{2n}}\right) J_{2q+2}, \end{aligned}$$

where (7) follows from the fact that for all $q \leq \frac{2^n}{13}$, $1 - \frac{2q}{2^n} + \frac{q^2}{2^{2n}} > 1.2$ and that for $n \geq 5$, $1 - \frac{(3n-1)^3}{(2^n-(3n-1))^2} \geq 1 - \frac{108n^3}{2^{2n}}$.[11] □

7.1 Proof Outline of Lemma 11 : h'_{α}-property

We prove Lemma 11 in a similar way as we proved Lemma 8. We first define derived ℓ-linked graph and derived (ℓ, d)-labels which are derived from base label $\mathscr{B}_q = \{\lambda_1, \cdots, \lambda_q\}$. Then, we analogously define the ℓ-th order A-term as,

$$A(\mathscr{B}_{\alpha}, L^{[2\ell+1]}) = \left| h(\mathscr{B}_{\alpha}, L^{[2\ell+1]}) - \frac{h(\mathscr{B}_{\alpha}, L^{[2\ell-1]})}{2^n} \right|.$$

[11] This $1 - O(n^3/2^{2n})$-bound can be further improved by using better bounding techniques than (40)

In addition to this, we also define the 1st order A term (for which one of the two terms is from the base equations) as follows:

$$A(\mathscr{B}_\alpha, L^{[3]}) \stackrel{\text{def}}{=} \left| h(\mathscr{B}_\alpha, L^{[3]}) - \frac{h(\mathscr{B}_\alpha)}{2^n} \right|.$$

Having defined the first order and the ℓ-th order A term, let us define the following: for $\ell \geq 1$, we define

$$A_\alpha^{[\ell-1]} = \max\{A(\mathscr{B}_\alpha, L^{[2\ell+1]}) \mid (\mathscr{B}_\alpha, L^{[2\ell+1]}) \text{ is } (\ell, q-\alpha)\text{-derived from } \mathscr{B}_q\}.$$

Now, we state the derived inequality lemma for pair of independent permutations as follows:

Lemma 12 (Derived Inequality Lemma for Independent Permutations). *Let $\alpha \stackrel{\text{def}}{=} q - d$ for two positive integers q, d such that $d < q$. If $(\mathscr{B}_\alpha, L^{[2\ell+1]})$ is (ℓ, d) derived from a base label $\mathscr{B}_q$, then we have,*

$$(a) h(\mathscr{B}_\alpha, L^{[2\ell+1]}) \leq \frac{h_q}{(2^n - 2q)^{d+\ell}}, \qquad (b) A(\mathscr{B}_\alpha, L^{[2\ell+1]}) \leq \frac{2h_q}{(2^n - 2q)^{d+\ell}}.$$

Proof of the lemma is no different than that of Lemma 9 and hence we skip its proof. By algebraically manipulating the orange and purple equations for independent permutations, using the size lemma for independent permutations (i.e., Lemma 6) and the derived inequality lemma for independent permutations (i.e., Lemma 12), we derive the *general order central lemma for a pair of independent permutations* as we did for deriving Lemma 10:

Lemma 13 (General Order Central Lemma for Independent Permutations). *For $\ell = 0, \cdots, \alpha - 1$,*

$$A_{\alpha+1}^{[\ell]} \leq A_\alpha^{[\ell-1]} + 3qA_\alpha^{[\ell]} + \frac{9}{4}q^2 A_\alpha^{[\ell+1]} + \frac{h_q}{(2^n - 2q)^{q-\alpha+\ell}} \left(\frac{4\Delta}{2^n} + \frac{3q\Delta}{2^n(2^n - 2q)} \right)$$

Resuming the proof. Now, we use the combinatorial lemma by recognizing the fact that $\{A_\alpha^{[l]}\}_{\alpha \leq q, l \leq \alpha - 1}$ satisfies the conditions for a double sequence as in Lemma 7, with $r = 3, T = q, \beta = \frac{3}{2}, \gamma = 2, \xi = h_q$ and $E = 4\Delta + \frac{3q\Delta}{(2^n - 2q)}$, to get

$$\begin{aligned} A_q^{[0]} &< \frac{h_q}{2^n} \left(\frac{2\frac{\sqrt[3]{2}}{\sqrt[3]{2}-1}}{2^n(1 - \frac{2q}{2^n})} + \left(\frac{\sqrt[3]{2}}{\sqrt[3]{2} - 1} \right)^2 \frac{4\Delta}{2^n(1 - \frac{2q}{2^n})} + \left(\frac{\sqrt[3]{2}}{\sqrt[3]{2} - 1} \right)^2 \frac{3q\Delta}{2^{2n}(1 - \frac{2q}{2^n})^2} \right) \\ &\stackrel{(*)}{\leq} \frac{h_q}{2^n} \left(\left(2\frac{\sqrt[3]{2}}{\sqrt[3]{2} - 1} + 4\left(\frac{\sqrt[3]{2}}{\sqrt[3]{2} - 1} \right)^2 \right) \frac{\Delta}{2^n(1 - \frac{2q}{2^n})} + \left(\frac{\sqrt[3]{2}}{\sqrt[3]{2} - 1} \right)^2 \frac{3q\Delta}{2^{2n}(1 - \frac{2q}{2^n})^2} \right) \end{aligned}$$

for $q < \frac{2^n}{3\sqrt[3]{2}e+2}$, where $(*)$ follows from the fact that $\Delta \geq 1$. As $\left| h(\mathscr{B}_q, L^{[3]}) - \frac{h_q}{2^n} \right| = A(\mathscr{B}_q, L^{[3]}) \leq A_q^{[0]}$ for all $(\mathscr{B}_q, L^{[3]})$ derived from $\mathscr{B}_q$, we get

$$h(\mathscr{B}_q, L^{[3]}) \geq \frac{h_q}{2^n} \left(1 - \frac{C_1\Delta}{2^n(1 - \frac{2q}{2^n})} - \frac{C_2 q\Delta}{2^{2n}(1 - \frac{2q}{2^n})^2} \right), \tag{43}$$

where $C_1 = 2\frac{\sqrt[3]{2}}{\sqrt[3]{2}-1} + 4\left(\frac{\sqrt[3]{2}}{\sqrt[3]{2}-1}\right)^2$ and $C_2 = 3\left(\frac{\sqrt[3]{2}}{\sqrt[3]{2}-1}\right)^2$, which completes the proof. □

8 Conclusion and Future Works

In this paper, we provide a complete and verifiable proof of mirror theory for single permutation case and a pair of independent permutations case. Our result on mirror theory for single permutation case directly gives an optimal and tight PRF security on XOR_1 construction, whereas our result on mirror theory for a pair of independent permutations give security bound of $O(q^2/2^{2n})$ for XOR_2 construction. However, our bound for XOR_2 construction is not known to be tight and hence it leaves the room for the bound to be improved. Also, our result is applicable only for $\xi_{\max} = 2$ whereas Patarin[Theorem 6, [32]] claimed that the same result holds for a general $\xi_{\max} > 2$ with $\theta = 134$, and $\alpha \leq \frac{2^n}{(\xi_{\max}-1)\cdot\theta}$. Unfortunately, there is no proof available in support of this claim (only a very high-level sketchy proof can be found in [32]). One can inevitably notice from our proof that the analysis of the same for general $\xi_{\max}$ is much more complicated. Nevertheless, this is an interesting problem to address. In fact, coming up with a concrete security proof for general $\xi_{\max}$ result eventually helps to correctly establish the improved security bound of many cryptographic constructions.

References

1. Mihir Bellare and Russell Impagliazzo. A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion. *IACR Cryptology ePrint Archive*, 1999:24, 1999.
2. Mihir Bellare, Joe Kilian, and Phillip Rogaway. The security of the cipher block chaining message authentication code. *J. Comput. Syst. Sci.*, 61(3):362–399, 2000.
3. Mihir Bellare, Ted Krovetz, and Phillip Rogaway. Luby-rackoff backwards: Increasing security by making block ciphers non-invertible. In *Advances in Cryptology - EUROCRYPT '98, International Conference on the Theory and Application of Cryptographic Techniques, Espoo, Finland, May 31 - June 4, 1998, Proceeding*, pages 266–280, 1998.
4. Mihir Bellare and Phillip Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, pages 409–426, 2006.
5. John Black and Phillip Rogaway. A block-cipher mode of operation for parallelizable message authentication. In *EUROCRYPT 2002*, pages 384–397, 2002.
6. Donghoon Chang and Mridul Nandi. A short proof of the PRP/PRF switching lemma. *IACR Cryptology ePrint Archive*, 2008:78, 2008.
7. Wei Dai, Viet Tung Hoang, and Stefano Tessaro. Information-theoretic indistinguishability via the chi-squared method. In *Advances in Cryptology - CRYPTO 2017. Proceedings, Part III*, pages 497–523, 2017.

8. Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Goutam Paul. Double-block hash-then-sum: A paradigm for constructing bbb secure prf. *IACR Trans. Symmetric Cryptol.*, 2018(3):36–92, 2018.
9. Nilanjan Datta, Avijit Dutta, Mridul Nandi, Goutam Paul, and Liting Zhang. Single key variant of pmac_plus. *IACR Trans. Symmetric Cryptol.*, 2017(4):268–305, 2017.
10. Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Kan Yasuda. Encrypt or decrypt? to make a single-key beyond birthday secure nonce-based MAC. In *Advances in Cryptology - CRYPTO 2018. Proceedings, Part I*, pages 631–661, 2018.
11. Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Kan Yasuda. sfdwcdm+: A BBB secure nonce based MAC. *Adv. in Math. of Comm.*, 13(4):705–732, 2019.
12. Avijit Dutta, Mridul Nandi, and Suprita Talnikar. Beyond birthday bound secure MAC in faulty nonce model. In *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part I*, pages 437–466, 2019.
13. Tetsu Iwata. New blockcipher modes of operation with beyond the birthday bound security. In *Fast Software Encryption, 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers*, pages 310–327, 2006.
14. Tetsu Iwata, Bart Mennink, and Damian Vizár. CENC is optimally secure. *IACR Cryptology ePrint Archive*, 2016:1087, 2016.
15. Tetsu Iwata and Kazuhiko Minematsu. Stronger security variants of GCM-SIV. *IACR Trans. Symmetric Cryptol.*, 2016(1):134–157, 2016.
16. Tetsu Iwata, Kazuhiko Minematsu, Thomas Peyrin, and Yannick Seurin. ZMAC: A fast tweakable block cipher mode for highly secure message authentication. In *Advances in Cryptology - CRYPTO 2017. Proceedings, Part III*, pages 34–65, 2017.
17. Eik List and Mridul Nandi. Revisiting full-prf-secure PMAC and using it for beyond-birthday authenticated encryption. In *Topics in Cryptology - CT-RSA 2017 - The Cryptographers' Track at the RSA Conference 2017, San Francisco, CA, USA, February 14-17, 2017, Proceedings*, pages 258–274, 2017.
18. Eik List and Mridul Nandi. ZMAC+ - an efficient variable-output-length variant of ZMAC. *IACR Trans. Symmetric Cryptol.*, 2017(4):306–325, 2017.
19. Stefan Lucks. The sum of prps is a secure PRF. In *EUROCRYPT 2000*, pages 470–484, 2000.
20. David A. McGrew and John Viega. The security and performance of the galois/counter mode (GCM) of operation. In *Progress in Cryptology - INDOCRYPT 2004, 5th International Conference on Cryptology in India, Chennai, India, December 20-22, 2004, Proceedings*, pages 343–355, 2004.
21. Bart Mennink and Samuel Neves. Encrypted davies-meyer and its dual: Towards optimal security using mirror theory. In *Advances in Cryptology - CRYPTO 2017. Proceedings, Part III*, pages 556–583, 2017.
22. Alexander Moch and Eik List. Parallelizable macs based on the sum of prps with security beyond the birthday bound. In *Applied Cryptography and Network Security - 17th International Conference, ACNS 2019, Bogota, Colombia, June 5-7, 2019, Proceedings*, pages 131–151, 2019.
23. Valérie Nachef, Jacques Patarin, and Emmanuel Volte. *Feistel Ciphers - Security Proofs and Cryptanalysis*. Springer, 2017.
24. Yusuke Naito. Full prf-secure message authentication code based on tweakable block cipher. In *Provable Security - 9th International Conference, ProvSec 2015, Kanazawa, Japan, November 24-26, 2015, Proceedings*, pages 167–182, 2015.

25. Yusuke Naito. Blockcipher-based macs: Beyond the birthday bound without message length. In *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part III*, pages 446–470, 2017.
26. NIST. Lightweight cryptography, 2018. Online: `https://csrc.nist.gov/Projects/Lightweight-Cryptography`. Accessed: August 01, 2019.
27. Jacques Patarin. Luby-rackoff: 7 rounds are enough for $2^{n(1\text{-epsilon})}$security. In *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, pages 513–529, 2003.
28. Jacques Patarin. On linear systems of equations with distinct variables and small block size. In *Information Security and Cryptology - ICISC 2005, 8th International Conference, Seoul, Korea, December 1-2, 2005, Revised Selected Papers*, pages 299–321, 2005.
29. Jacques Patarin. The "coefficients H" technique. In *Selected Areas in Cryptography - SAC 2008. Revised Selected Papers*, pages 328–345, 2008.
30. Jacques Patarin. A proof of security in o(2n) for the xor of two random permutations. In *Information Theoretic Security, Third International Conference, ICITS 2008, Calgary, Canada, August 10-13, 2008, Proceedings*, pages 232–248, 2008.
31. Jacques Patarin. A proof of security in $o(2^n)$ for the xor of two random permutations
– proof with the "h_σ technique"–. Cryptology ePrint Archive, Report 2008/010, 2008. `https://eprint.iacr.org/2008/010`.
32. Jacques Patarin. Introduction to mirror theory: Analysis of systems of linear equalities and linear non equalities for cryptography. *IACR Cryptology ePrint Archive*, 2010:287, 2010.
33. Jacques Patarin. Security in $o(2^n)$ for the xor of two random permutations \\ - proof with the standard H technique -. *IACR Cryptology ePrint Archive*, 2013:368, 2013.
34. Phillip Rogaway and Thomas Shrimpton. A provable-security treatment of the key-wrap problem. In *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, pages 373–390, 2006.
35. Victor Shoup. Sequences of games: a tool for taming complexity in security proofs. *IACR Cryptology ePrint Archive*, 2004:332, 2004.
36. Kan Yasuda. The sum of CBC macs is a secure PRF. In *CT-RSA 2010*, pages 366–381, 2010.
37. Kan Yasuda. A new variant of PMAC: beyond the birthday bound. In *Advances in Cryptology - CRYPTO 2011. Proceedings*, pages 596–609, 2011.
38. Liting Zhang, Wenling Wu, Han Sui, and Peng Wang. 3kf9: Enhancing 3gpp-mac beyond the birthday bound. In *ASIACRYPT 2012*, pages 296–312, 2012.
39. Ping Zhang, Honggang Hu, and Qian Yuan. Close to optimally secure variants of GCM. *Security and Communication Networks*, 2018:9715947:1–9715947:12, 2018.

Supplementary Materials

A Proof of Orange Lemma and Purple Lemma

In this section, we prove orange lemma and purple lemma for both the single permutation case (i.e., Lemma 1 and 2) and the pair of independent permutations case (i.e., Lemma 4 and 5). We prove orange and purple lemma for single permutation in the first two subsections and the later two subsections include the proof of purple lemma for a pair of independent permutations.

A.1 Proof of Lemma 1

To prove the lemma, we first begin with a system of base equations of size α:

$$Y_1 \oplus Y_2 = \lambda_1, Y_3 \oplus Y_4 = \lambda_2, \ldots, Y_{2\alpha-1} \oplus Y_{2\alpha} = \lambda_\alpha.$$

An injective solution in $\mathscr{H}(\mathscr{B}_\alpha)$ means a tuple of distinct values $(P_1, P_2, \ldots, P_{2\alpha})$ which satisfies the above system of equation. In order to extend this to a solution of $\mathscr{H}(\mathscr{B}_{\alpha+1})$, it is necessary and sufficient to choose

$$P_{2\alpha+1} \notin \underbrace{\{P_1, P_2, \ldots, P_{2\alpha}\}}_{\mathcal{S}_1} \cup \underbrace{\{\lambda_{\alpha+1} \oplus P_1, \lambda_{\alpha+1} \oplus P_2, \ldots, \lambda_{\alpha+1} \oplus P_{2\alpha}\}}_{\mathcal{S}_2}$$

and set $P_{2\alpha+2} \stackrel{\text{def}}{=} P_{2\alpha+1} \oplus \lambda_{\alpha+1}$. So the number of possible values of $P_{2\alpha+1}$ is exactly $2^n - |\mathcal{S}_1| - |\mathcal{S}_2| + |\mathcal{S}_1 \cap \mathcal{S}_2| = 2^n - 4\alpha + |\mathcal{S}_1 \cap \mathcal{S}_2|$. A collision between $\mathcal{S}_1$ and $\mathcal{S}_2$ essentially means that for some $i \neq j$ (as equality cannot happen), $P_i = \lambda_{\alpha+1} \oplus P_j$. So we can write

$$\begin{aligned} h(\mathscr{B}_{\alpha+1}) &= \sum_{P^{2\alpha} \in \mathscr{H}(\mathscr{B}_\alpha)} (2^n - 4\alpha + |\mathcal{S}_1 \cap \mathcal{S}_2|) \\ &= (2^n - 4\alpha) \cdot h(\mathscr{B}_\alpha) + \sum_{P^{2\alpha} \in \mathscr{H}(\mathscr{B}_\alpha)} \sum_{i \neq j} \chi(P_i \oplus P_j = \lambda_{\alpha+1}), \end{aligned} \tag{44}$$

where, $\chi(E)$ is 1 if the statement E is true, 0 otherwise. Now we fix any $P^{2\alpha} \in \mathscr{H}(\mathscr{B}_\alpha)$. There are three possibilities for the pair (i, j) in the view of $\chi(P_i \oplus P_j = \lambda_{\alpha+1})$.

- Case-1: P_i and P_j are in the same block (i.e. $e \stackrel{\text{def}}{=} \{i, j\}$ is an edge). In this case, $P_i \oplus P_j = \lambda_{\alpha+1}$ is a consequence of the relations induced by $\mathscr{B}_\alpha$.
  1. Case-1.1: If $\lambda_{\alpha+1} \neq \lambda_e$ then χ takes value zero always.
  2. Case-1.2: If $\lambda_{\alpha+1} = \lambda_e$ then χ takes value one always. Note that the number of (i, j) from the same block under this case is exactly 2δ.

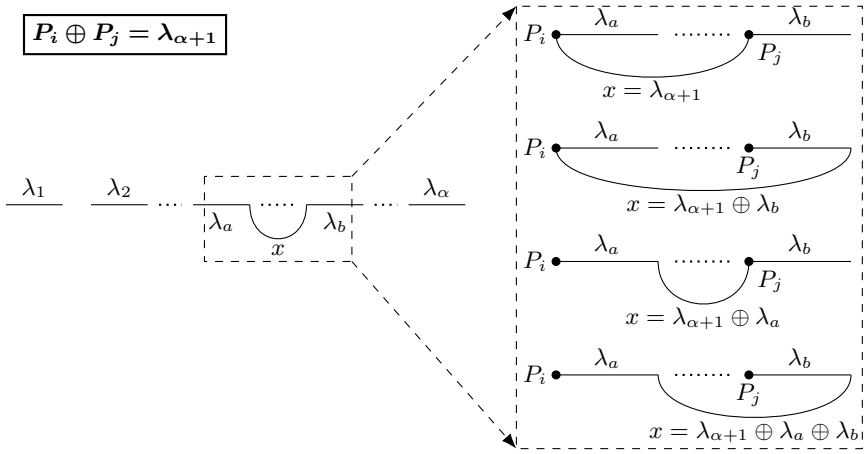

Fig. A.1: The four cases for which the link between λ_a and λ_b takes the four values $x = \lambda_{\alpha+1} \oplus \langle \lambda_a, \lambda_b \rangle$, when $P_{2\alpha+1} = P_i$, $P_{2\alpha+2} = P_j$ and P_i and P_j are not in the same block.

– Case-2: P_i and P_j are in different blocks. This case yields the scenario where there are α base equations, and a linking equation between P_i and P_j. Let λ_a and λ_b denote the labels of edges containing i and j respectively. Then,

$$\lambda_{\alpha+1} \neq \lambda_a, \lambda_{\alpha+1} \neq \lambda_b \text{ and } \lambda_{\alpha+1} \neq \lambda_a \oplus \lambda_b \tag{45}$$

must hold to have an injective solution. So we rewrite the sum

$$\sum_{P^{2\alpha} \in \mathscr{K}(\mathscr{B}_\alpha)} \sum_{i \neq j} \chi(P_i \oplus P_j = \lambda_{\alpha+1})$$

in terms of (a, b) instead of (i, j). For any such i and j satisfying above we have four possibilities of linking between λ_a and λ_b (See Fig A.1). Depending on the vertices of the edges which are linked, one can show that

$$\sum_{P^{2\alpha} \in \mathscr{K}(\mathscr{B}_\alpha)} \sum_{i \neq j} \chi(P_i \oplus P_j = \lambda_{\alpha+1}) = \sum_{\lambda_a . x . \lambda_b \in \mathscr{M}_3} h(\mathscr{B}_\alpha,\ \lambda_a \cdot x \cdot \lambda_b), \tag{46}$$

where recall that, $\mathscr{M}_3(\mathscr{B}_{\alpha+1}) = \{\lambda_a \cdot x \cdot \lambda_b \in V_1' \mid a \neq b \in [\alpha],\ x \in \lambda_{\alpha+1} \oplus \langle \lambda_a, \lambda_b \rangle\}$.

Thus, from Eqn. (44) and Eqn. (46), we obtain the result.

A.2 Proof of Lemma 2

From the definition of the system of equations, $h(\mathscr{B}_{\alpha+1}, L^{[2\ell+1]})$ contains two extra equations (namely $Y_{2\alpha+1} \oplus Y_{2\alpha+2} = \lambda_{\alpha+1} \stackrel{\text{def}}{=} L_1$ and $Y_{2\alpha} \oplus Y_{2\alpha+1} = L_2$)

in addition of those of $h(\mathscr{B}_\alpha, L^{[3,2\ell+1]})$. Now, we begin with $h(\mathscr{B}_\alpha, L^{[3,2\ell+1]})$ which contains following system of α many base equations and $\ell - 1$ many link equations:

$$\begin{cases} Y_1 \oplus Y_2 = \lambda_1, Y_3 \oplus Y_4 = \lambda_2, \ldots, Y_{2\alpha-1} \oplus Y_{2\alpha} = \lambda_\alpha. \\ Y_2 \oplus Y_3 = L_4, Y_4 \oplus Y_5 = L_6, \ldots, Y_{2\alpha-2} \oplus Y_{2\alpha-1} = L_{2\ell}. \end{cases}$$

We fix an injective solution $P^{2\alpha} \stackrel{\text{def}}{=} (P_1, \ldots, P_{2\alpha}) \in \mathscr{H}(\mathscr{B}_\alpha, L^{[3,2\ell+1]})$ and define $P_{2\alpha+1} = P_{2\alpha} \oplus L_2$ and $P_{2\alpha+2} = P_{2\alpha} \oplus L_1 \oplus L_2$. We call a solution $P^{2\alpha}$ invalid if either $P_{2\alpha+1} = P_i$ or $P_{2\alpha+2} = P_i$ holds for $i \in [2\alpha]$. The number of solutions in $\mathscr{H}(\mathscr{B}_{\alpha+1}, L^{[2\ell+1]})$ is the number of valid (i.e. not invalid) solutions of $\mathscr{H}(\mathscr{B}_\alpha, L^{[3,2\ell+1]})$. In other words, we must choose $P_{2\alpha}$ such that (see Fig A.2)

$$P_{2\alpha} \notin \underbrace{\{L_2 \oplus P_1, \ldots, L_2 \oplus P_{2\alpha}\}}_{\mathcal{S}_1'} \cup \underbrace{\{L_2 \oplus L_1 \oplus P_1, \ldots, L_2 \oplus L_1 \oplus P_{2\alpha}\}}_{\mathcal{S}_2'}.$$

Therefore, by using principle of inclusion and exclusion,

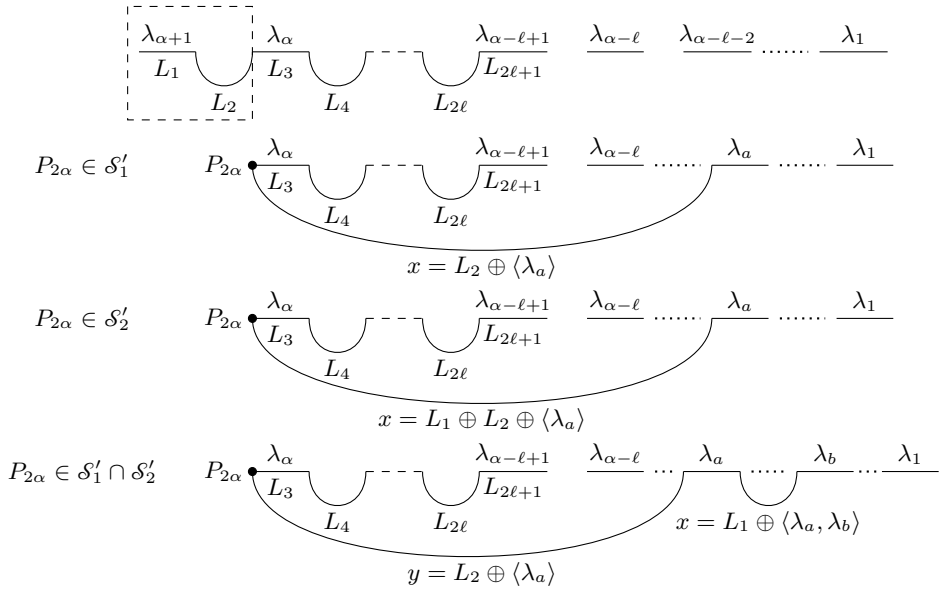

Fig. A.2: The cases when a solution of $h(\mathscr{B}_\alpha, L^{[3,2\ell+1]})$ is not valid for $h(\mathscr{B}_{\alpha+1}, L^{[2\ell+1]})$.

$$h(\mathscr{B}_{\alpha+1}, L^{[2\ell+1]}) = \sum_{P^{2\alpha}} (1 - \chi(P^{2\alpha} \in \mathcal{S}_1') - \chi(P^{2\alpha} \in \mathcal{S}_2') + \chi(P^{2\alpha} \in \mathcal{S}_1' \cap \mathcal{S}_2')) \tag{47}$$

where, the sum is taken over all $P^{2\alpha} \in \mathscr{H}(\mathscr{B}_\alpha, L^{[3,2\ell+1]})$. Now, suppose $P_{2\alpha} \in \mathcal{S}'_1$, i.e., $P_{2\alpha} = P_i \oplus L_2$ for some $i \in [2\alpha]$. This restriction yields a scenario where there are α base equations, $\ell - 1$ linking equations from before, and a new linking equation in between $P_{2\alpha}$ and P_i. (Note that, here $i \not\geq 2(\alpha - \ell)$, because, for $i > 2(\alpha - \ell)$, $P_{2\alpha}$ is already connected to P_i via links and edges and another link between $P_{2\alpha}$ and P_i would introduce a cycle in the graph which leads no solution due to valid label). Let λ_a be the label of the edge containing vertex P_i. Therefore, the label of the linking edge $(2\alpha, i)$ is either L_2 or $L_2 \oplus \lambda_a$ (depending on which vertex of the edge labeled λ_a is connected to $P_{2\alpha}$ by the link). Thus the subset of solutions $P^\alpha \in \mathscr{H}(\mathscr{B}_\alpha, L^{[3,2\ell+1]})$, that satisfies the condition $P_{2\alpha} \in \mathcal{S}'_1$, forms the set of solutions, $\mathscr{H}(\mathscr{B}_\alpha, K^{[2\ell+1]})$ where $K^{[2\ell+1]} = \lambda_a \cdot x \cdot L^{[3,2\ell+1]}$, $a \in [\alpha - \ell]$ and $x = L_2$ or $L_2 \oplus \lambda_a$ (See Figure A.3).

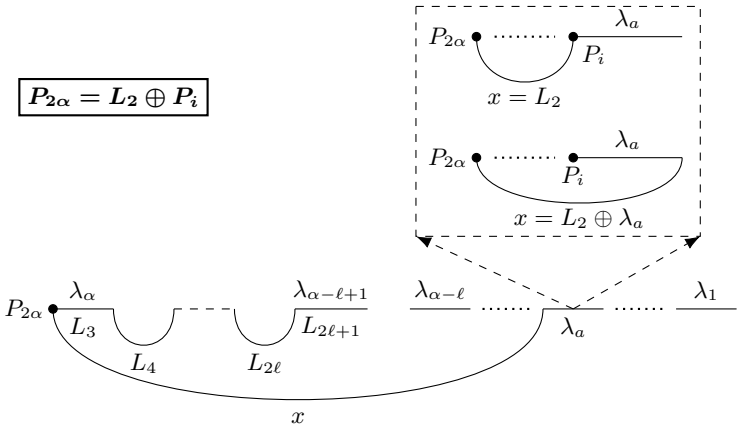

Fig. A.3: The two cases for which the link between $P_{2\alpha}$ and λ_a takes the two values $x = L_2 \oplus \langle \lambda_a \rangle$, when $P_{2\alpha} \in V'_1$.

Similarly, the subset of solutions $P^\alpha \in \mathscr{H}(\mathscr{B}_\alpha, L^{[3,2\ell+1]})$, that satisfies the condition $P_{2\alpha} \in \mathcal{S}'_2$, forms the set of solutions, $\mathscr{H}(\mathscr{B}_\alpha, K^{[2\ell+1]})$ where $K^{[2\ell+1]} = \lambda_a \cdot x \cdot L^{[3,2\ell+1]}$, $a \in [\alpha - \ell]$ and $x = L_1 \oplus L_2$ or $L_1 \oplus L_2 \oplus \lambda_a$, given the edge containing P_i. Therefore,

$$\sum_{P^{2\alpha}} (\chi(P^{2\alpha} \in \mathcal{S}'_1) + \chi(P^{2\alpha} \in \mathcal{S}'_2)) = \sum_{K^{2\ell+1} \in \mathcal{N}_{2\ell+1}} h(\mathscr{B}_\alpha, K^{2\ell+1}), \tag{48}$$

where the L.H.S. sum is taken over $\mathscr{H}(\mathscr{B}_\alpha, L^{[3,2\ell+1]})$, and recall that $\mathcal{N}_{2\ell+1} = \{\lambda_a \cdot x \cdot L^{[3,2\ell+1]} \in V'_\ell \,|\, a \in [\alpha - \ell], x \in L_2 \oplus \langle L_1 \oplus \lambda_i \rangle\}$, where $\tau = (\mathscr{B}_{\alpha+1}, L^{[2\ell+1]})$. Now suppose $P^{2\alpha} \in \mathcal{S}'_1 \cap \mathcal{S}'_2$. Then there exist $i \neq j \in [2(\alpha - \ell)]$, such that $P_{2\alpha} = L_2 \oplus P_i$ and $P_{2\alpha} = L_2 \oplus L_1 \oplus P_j$. These two constraints essentially implies an equation of the form: $P_i \oplus P_j = L_1$. There are three possibilities for the pair (i, j).

– Case-1: P_i and P_j are in the same block (i.e. $e \stackrel{\text{def}}{=} \{i, j\}$ is an edge). In this case, $P_i \oplus P_j = L_1$ is a consequence of the relations induced by $(\mathscr{B}_\alpha, L^{[3,2\ell+1]})$.

  1. Case-1.1: If $L_1 \neq \lambda_e$ then χ takes value zero always.
  2. Case-1.2: If $L_1 = \lambda_e$ then χ takes value one always. In this scenario there are α base equations, $\ell - 1$ links from before (namely $L_4, \cdots, L_{2\ell}$), and a new link L_2 between edges labeled $\lambda_{2\alpha}$ and $\lambda_e = L_1$. Hence in this case we get $h(\mathscr{B}_\alpha, L^{[2\ell+1]})$ solutions. Note that the number of (i, j) from the same base edge under this case is exactly $2\delta_{\mathscr{B}_{\alpha-\ell}}(\lambda_{\alpha+1})$.

– Case-2: P_i and P_j are in different blocks. In this case, it can be viewed as the introduction of two linking equations $P_{2\alpha} \oplus P_i = L_2$ and $P_i \oplus P_j = L_1$, i.e. introduction of two new links, one from vertex 2α to the edge e_i containing the vertex i with edge label λ_a, and another link from the vertices of e_i to the vertices of the edge e_j containing the vertex j with edge label λ_b. The label of the link from λ_a to λ_b can take four possible values, as it does in the case of the Orange equation depending on the vertices to connect, i.e., $L_1 \oplus \langle \lambda_a, \lambda_b \rangle$. For the link from the vertex 2α to vertex i, the possible labels of the link are L_2 and $L_2 \oplus \lambda_a$. Hence this gives rise to $h(\mathscr{B}_\alpha, K^{[2\ell+3]})$ solutions, where $K^{[2\ell+3]} = \lambda_b \cdot x \cdot \lambda_a \cdot y \cdot L^{[3,2\ell+1]}$, where $a \neq b \in [\alpha - \ell]$, $x \in L_1 \oplus \langle \lambda_a, \lambda_b \rangle$ and y is uniquely determined by x (See Figure A.4).

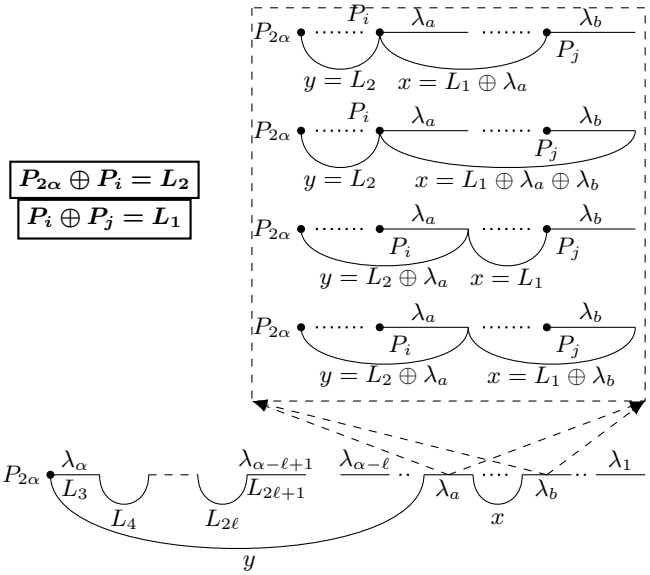

Fig. A.4: The four cases for which the link between λ_a and λ_b takes the four values $x = L_1 \oplus \langle \lambda_a, \lambda_b \rangle$, when $P_{2\alpha} = L_2 \oplus P_i$, $P_{2\alpha} = L_1 \oplus L_2 \oplus P_j$ and P_i, P_j are not in the same block.

Hence, we have

$$\sum_{P^{2\alpha}} \chi(P^{2\alpha} \in \mathcal{S}_1' \cap \mathcal{S}_2') = 2\delta_{\mathscr{B}_{\alpha-\ell}}(\lambda_{\alpha+1}) h_\alpha^{[2\ell+1]} + \sum_{K^{2\ell+3} \in \mathscr{M}_{2\ell+3}} h(\mathscr{B}_\alpha, K^{2\ell+1}), \quad (49)$$

where the sum on LHS is taken over $\mathscr{H}(\mathscr{B}_\alpha, L^{[3,2\ell+1]})$, and recall that $\mathscr{M}_{2\ell+3} = \{\lambda_b \cdot x \cdot \lambda_a \cdot y \cdot L^{[3,2\ell+1]} \in V'_{\ell+1} \mid a \neq b \in [\alpha - \ell], x \in L_1 \oplus \langle \lambda_a, \lambda_b \rangle, y \in L_2 \oplus \lambda_a\}$. By considering all the above cases and from Eqn. (47), Eqn. (48) and Eqn. (49), we obtain the result.

A.3 Proof of Lemma 4

Let $\mathscr{B}_{\alpha+1} = \{\lambda_1, \cdots, \lambda_{\alpha+1}\}$ be a multiset of size $\alpha + 1$. Let us suppose consider that $(P_1, \cdots, P_\alpha, Q_1, \cdots, Q_\alpha)$ be an injective solution in $\mathscr{H}(\mathscr{B}_\alpha)$. This solution can be extended to a solution in $\mathscr{H}(\mathscr{B}_{\alpha+1})$ by choosing

$$P_{\alpha+1} \notin \{P_1, \cdots, P_\alpha\} \cup \{Q_1 \oplus \lambda_{\alpha+1}, \cdots, Q_\alpha \oplus \lambda_{\alpha+1}\}$$

and setting $Q_{\alpha+1} = P_{\alpha+1} \oplus \lambda_{\alpha+1}$. By doing almost similar calculations as in the single permutation case (see Subsect. A.1), we prove the result. □

A.4 Proof of Lemma 5

Let $\mathscr{B}_{\alpha+1} = \{\lambda_1, \cdots, \lambda_{\alpha+1}\}$ be a multiset of size $\alpha + 1$ and $(\mathscr{B}_{\alpha+1}, L^{[2\ell+1]}) \in U'_\ell$ be a valid ℓ-linked labels, where $\lambda_{\alpha+1} = L_1, \lambda_\alpha = L_3, \cdots, \lambda_{\alpha-\ell+1} = L_{2\ell+1}$. Now we want to estimate $h(\mathscr{B}_{\alpha+1}, L^{[2\ell+1]})$ in terms of $h(\mathscr{B}_\alpha, L^{[2,2\ell+1]})$, where $\mathscr{B}_\alpha = \{\lambda_1, \cdots, \lambda_\alpha\}$ is a multiset and $L^{[3,2\ell+1]} = (L_3, \cdots, L_{2\ell+1})$ is an ordered tuple. $h(\mathscr{B}_\alpha, L^{[2\ell+1]})$ contains two extra equations (namely $P_{\alpha+1} \oplus Q_{\alpha+1} = \lambda_{\alpha+1}, Q_{\alpha+1} \oplus P_\alpha = L_2$) in addition to those of $h(\mathscr{B}_\alpha, L^{[3,2\ell+1]})$. Now we begin with $h(\mathscr{B}_\alpha, L^{[3,2\ell+1]})$ which contains the following system of α many base equations and $\ell - 1$ many link equations:

$$P_1 \oplus Q_1 = \lambda_1, \cdots, P_\alpha \oplus Q_\alpha = \lambda_\alpha$$
$$P_{\alpha-\ell+1} \oplus Q_{\alpha-\ell+2} = L_{2\ell}, \cdots, P_{\alpha-1} \oplus Q_\alpha = L_4$$

We fix an injective solution $(P^\alpha, Q^\alpha) \in \mathscr{H}(\mathscr{B}_\alpha, L^{[3,2\ell+1]})$ and define $Q_{\alpha+1} = P_\alpha \oplus L_2$ and $P_{\alpha+1} = P_\alpha \oplus L_2 \oplus L_1$.We call a solution (P^α, Q^α) invalid if either $P_{\alpha+1} = P_i$ or $Q_{\alpha+1} = Q_i$ holds for $i \in [\alpha]$. The number of valid solutions of $\mathscr{H}(\mathscr{B}_{\alpha+1}, L^{[2\ell+1]})$ is the number of valid solutions of $\mathscr{H}(\mathscr{B}_\alpha, L^{[3,2\ell+1]})$. In other words we must choose P_α such that

$$P_\alpha \notin \{P_1 \oplus L_2 \oplus L_1, \cdots, P_\alpha \oplus L_2 \oplus L_1\} \cup \{Q_1 \oplus L_2, \cdots, Q_\alpha \oplus L_2\}$$

Again, by doing almost identical calculations as in the single permutation case (see Subsect. A.2), we prove the result. □

B Proof of Lemma 3 : Size Lemma

In this section, we prove each part of Lemma 3 in separate sections.

B.1 Proof of Part (a) of Size Lemma

Recall that, for $\tau = \mathscr{B}_{\alpha+1}$, we have $\mathscr{M}_3(\tau) = \{\lambda_b \cdot x \cdot \lambda_a \in V_1' \mid a \neq b \in [\alpha], x \in \lambda_{\alpha+1} \oplus \langle \lambda_a, \lambda_b \rangle\}$. Now, we can choose (λ_a, λ_b) in $\alpha(\alpha-1)$ ways since $a \neq b$, and for fixed values of λ_a and λ_b, x can take 4 values. But again, not all the $4\alpha(\alpha-1)$ tuples $\lambda_b \cdot x \cdot \lambda_a$ are valid. We can calculate the number of such invalid tuples by considering the invalidity conditions.

$\boldsymbol{x}$	$\boldsymbol{x = 0}$	$\boldsymbol{x = \lambda_a}$	$\boldsymbol{x = \lambda_b}$	$\boldsymbol{x = \lambda_a \oplus \lambda_b}$
$\lambda_{\alpha+1}$	$\lambda_{\alpha+1} = 0$	$\lambda_{\alpha+1} = \lambda_a$	$\lambda_{\alpha+1} = \lambda_b$	$\lambda_{\alpha+1} \overset{(*)}{=} \lambda_a \oplus \lambda_b$
$\lambda_{\alpha+1} \oplus \lambda_a$	$\lambda_{\alpha+1} = \lambda_a$	$\lambda_{\alpha+1} = 0$	$\lambda_{\alpha+1} \overset{(*)}{=} \lambda_a \oplus \lambda_b$	$\lambda_{\alpha+1} = \lambda_b$
$\lambda_{\alpha+1} \oplus \lambda_b$	$\lambda_{\alpha+1} = \lambda_b$	$\lambda_{\alpha+1} \overset{(*)}{=} \lambda_a \oplus \lambda_b$	$\lambda_{\alpha+1} = 0$	$\lambda_{\alpha+1} = \lambda_a$
$\lambda_{\alpha+1} \oplus \lambda_a \oplus \lambda_b$	$\lambda_{\alpha+1} \overset{(*)}{=} \lambda_a \oplus \lambda_b$	$\lambda_{\alpha+1} = \lambda_b$	$\lambda_{\alpha+1} = \lambda_a$	$\lambda_{\alpha+1} = 0$

The gray equations cannot hold tirvially. Each of the unmarked equations can happen in at most Δ ways. The unmarked conditions fix either of λ_a or λ_b so that the other one can take $\alpha-1$ of the remaining values. Each of the $(*)$-marked equations can happen in at most Δ_2 ways, which is $\leq (\alpha+1)\Delta$. Hence

$$4\alpha(\alpha-1) - 8\Delta(\alpha-1) - 4(\alpha+1)\Delta < |\mathscr{M}_3(\tau)| \leq 4\alpha(\alpha-1)$$

Now, it is easy to see that $8\Delta(\alpha-1) + 4(\alpha+1)\Delta = 12\alpha\Delta - 4\Delta \leq 12\alpha\Delta$, which proves part (a) of the lemma. □

B.2 Proof of Part (b) of Size Lemma

Recall that, for any valid label $\tau = \mathscr{B}_{\alpha+1}$, we have $\mathscr{N}_3(\tau) = \{\lambda_a \cdot x \cdot \lambda_\alpha \in V_1' \mid a \in [\alpha-1], x \in L_2 \oplus \langle \lambda_{\alpha+1}, \lambda_a \rangle\}$. For each value of $\lambda_a, a \in [\alpha-1]$, x can have 4 different values, namely, $L_2, L_2 \oplus \lambda_{\alpha+1}, L_2 \oplus \lambda_a, L_2 \oplus \lambda_{\alpha+1} \oplus \lambda_a$, leading to $4(\alpha-1)$ such tuples, $\lambda_a \cdot x \cdot \lambda_\alpha$. However tuples for which either $\lambda_\alpha = x$ or $\lambda_a = x$ or $\lambda_a = x \oplus \lambda_\alpha$ are invalid and not in V. So we calculate the number of invalid tuples.

$\boldsymbol{x}$	$\boldsymbol{\lambda_\alpha = x}$	$\boldsymbol{\lambda_a = x}$	$\boldsymbol{\lambda_i = x \oplus \lambda_\alpha}$
L_2	$\lambda_\alpha = L_2$	$\lambda_a = L_2$	$\lambda_a = \lambda_\alpha \oplus L_2$
$L_2 \oplus \lambda_{\alpha+1}$	$\lambda_\alpha \oplus L_2 \oplus \lambda_{\alpha+1} = 0$	$\lambda_a = L_2 \oplus \lambda_{\alpha+1}$	$\lambda_a = \lambda_\alpha \oplus L_2 \oplus \lambda_{\alpha+1}$
$L_2 \oplus \lambda_a$	$\lambda_a = L_2 \oplus \lambda_\alpha$	$L_2 = 0$	$L_2 \oplus \lambda_\alpha = 0$
$\lambda_a \oplus L_2 \oplus \lambda_{\alpha+1}$	$\lambda_a = \lambda_\alpha \oplus L_2 \oplus \lambda_{\alpha+1}$	$L_2 \oplus \lambda_{\alpha+1} = 0$	$\lambda_\alpha \oplus L_2 \oplus \lambda_{\alpha+1} = 0$

The gray equations cannot hold because $\lambda_\alpha \cdot L_2 \cdot \lambda_{\alpha+1}$ form a valid tuple. Otherwise, the tuple $\lambda_a \cdot x \cdot \lambda_\alpha$ will not be a valid tuple in either of the four cases, when

1. $\lambda_a = L_2$

2. $\lambda_a = L_2 \oplus \lambda_\alpha$
3. $\lambda_a = L_2 \oplus \lambda_{\alpha+1}$
4. $\lambda_a = \lambda_\alpha \oplus L_2 \oplus \lambda_{\alpha+1}$

where each case can happen at most Δ times, which proves part (b) of the lemma. □

B.3 Proof of Part (c) of Size Lemma

Recall that, for any valid label $\tau_1 = (\mathscr{B}_{\alpha+1}, L^{[2\ell+1]})$ and $\tau_2 = (\mathscr{B}_{\alpha+1}, L^{[2\ell+3]})$,

$$\mathscr{N}_{2\ell+1}(\tau_1) = \{\lambda_a \cdot x \cdot L^{[3,2\ell+1]} \in V'_\ell \mid a \in [\alpha-\ell], x \in L_2 \oplus \langle L_1, \lambda_a \rangle\}$$

$$\mathscr{N}_{2\ell+3}(\tau_2) = \{\lambda_a \cdot x \cdot L^{[3,2\ell+1]} \cdot L_{2\ell+2} \cdot L_{2\ell+3} \in V'_{\ell+1} \mid a \in [\alpha-\ell-1], x \in L_2 \oplus \langle L_1, \lambda_a \rangle\}$$

There are 4 tuples of the form, $\lambda_{\alpha-\ell} \cdot x \cdot L^{[3,2\ell+1]}$, in $\mathscr{N}_{2\ell+1}(\tau_1)$ that are not in $\mathscr{N}_{2\ell+3}(\tau_2)$. The tuples of the form $\lambda_a \cdot x \cdot L^{[3,2\ell+1]} \cdot L_{2\ell+2} \cdot L_{2\ell+3}$ that are not valid, are the ones that satisfy either of the following conditions :

$$\begin{aligned}
&\lambda_a = x \\
&\lambda_a = x \oplus L_3 \\
&\lambda_a = x \oplus L_3 \oplus L_4 \\
&\cdots \\
&\lambda_a = x \oplus \bigoplus_{i=3}^{2\ell+1} L_i \\
&\lambda_a = x \oplus \bigoplus_{i=3}^{2\ell+1} L_i \oplus L_{2\ell+2} \\
&\lambda_a = x \oplus \bigoplus_{i=3}^{2\ell+1} L_i \oplus L_{2\ell+2} \oplus L_{2\ell+3}.
\end{aligned}$$

The gray equations cannot hold because because $\lambda_a \cdot x \cdot L^{[2\ell+1,3]}$ is a valid tuple belonging to $\mathscr{N}_{2\ell+1}$. To check the other invalidity conditions we check the following table (where $Z = \bigoplus_{i=3}^{2\ell+2} L_i$)

$\boldsymbol{x}$	$\boldsymbol{\lambda_a = x \oplus Z}$	$\boldsymbol{\lambda_a = x \oplus Z \oplus L_{2\ell+3}}$
L_2	$\lambda_a = L_2 \oplus Z$	$\lambda_a = L_2 \oplus Z \oplus L_{2\ell+3}$
$L_2 \oplus \lambda_{\alpha+1}$	$\lambda_a = \lambda_{\alpha+1} \oplus L_2 \oplus Z$	$\lambda_a = \lambda_{\alpha+1} \oplus L_2 \oplus Z \oplus L_{2\ell+3}$
$L_2 \oplus \lambda_a$	$L_2 \oplus Z = 0$	$L_2 \oplus Z \oplus L_{2\ell+3} = 0$
$L_2 \oplus \lambda_a \oplus \lambda_{\alpha+1}$	$\lambda_{\alpha+1} \oplus L_2 \oplus Z = 0$	$\lambda_{\alpha+1} \oplus L_2 \oplus Z \oplus L_{2\ell+3} = 0$

Again, the gray equations cannot hold because we have assumed $L^{[2\ell+1]}$ is a valid tuple. So the tuple $\lambda_a \cdot x \cdot L^{[3,2\ell+3]}$ is not valid in the four cases corresponding to the dark equations of the above table, and each case can happen at most Δ times. Hence, we have

$$|\mathscr{N}_{2\ell+1}| - 4 - 4\Delta \le |\mathscr{N}_{2\ell+3}| \le |\mathscr{N}_{2\ell+1}| - 4 \le \cdots \le |\mathscr{N}_3| - 4\ell \le 4(\alpha-1). \quad \square$$

B.4 Proof of Part (d) and Part (e) of Size Lemma

We prove this result in two parts: in the first part we prove the result for $\ell = 0$ and in the second part, we prove the result for $\ell \geq 1$.

B.4.1 First Part: $|\mathscr{M}_5|$ in terms of $|\mathscr{M}_3|$: For any valid label $\tau_1 = (\mathscr{B}_{\alpha+1}, L^{[3]})$

$$\mathscr{M}_5(\tau_2) = \{\lambda_b{\cdot}x{\cdot}\lambda_a{\cdot}y{\cdot}\lambda_{\alpha+1} \in V'_{\ell+1} \mid a \neq b \in [\alpha{-}1], y \in L_2{\oplus}\langle\lambda_a\rangle, x \in \lambda_{\alpha+1}{\oplus}\langle\lambda_a, \lambda_b\rangle\}$$

There are $4(\alpha-1)$ tuples of the form, $\lambda_b \cdot x \cdot \lambda_\alpha, \quad b \in [\alpha-1]$, as for each b, x can take 4 values, and for each such x, y can take one value, and $4(\alpha-1)$ tuples of the form, $\lambda_\alpha \cdot x \cdot \lambda_a, \quad a \in [\alpha-1]$, that might be in $\mathscr{M}_3(\tau)$ ($\tau = \mathscr{B}_{\alpha+1}$), but are definitely not in $\mathscr{M}_5(\tau_1)$.

Now, $\lambda_b \cdot x \cdot \lambda_\alpha$ will not be a valid tuple belonging to $\mathscr{M}_3(\tau)$, if and only if, for some value of λ_b, $x = 0$, which happens when either either $\lambda_b = \lambda_{\alpha+1}$ or $\lambda_b = \lambda_{\alpha+1} \oplus \lambda_\alpha$. Either of the cases can happen in atmost Δ ways giving us at least $(4(\alpha-1) - 2\Delta)$ tuples of the form $\lambda_b \cdot x \cdot \lambda_\alpha$ that are in $\mathscr{M}_3(\tau)$ but not in $\mathscr{M}_5(\tau_1)$.

Similarly, there are at least $(4(\alpha-1) - 2\Delta)$ tuples of the form $\lambda_\alpha \cdot x \cdot \lambda_i$ that are in $\mathscr{M}_3(\tau)$ but not in $\mathscr{M}_5(\tau_1)$. The tuples of the form $\lambda_b \cdot x \cdot \lambda_a \cdot y \cdot \lambda_{\alpha+1}$ that are not valid, are the ones that satisfy either of the following conditions :

$$\begin{aligned} y &= 0 & y &= \lambda_\alpha \\ y &= \lambda_a & y &= \lambda_a \oplus \lambda_\alpha \\ y &= \lambda_a \oplus x & y &= \lambda_a \oplus x \oplus \lambda_\alpha \\ y &= \lambda_a \oplus x \oplus \lambda_b & y &= \lambda_a \oplus x \oplus \lambda_b \oplus \lambda_\alpha \end{aligned}$$

$\boldsymbol{x}$	$\boldsymbol{y}$	$\boldsymbol{y = 0}$	$\boldsymbol{y = \lambda_a}$
$\lambda_{\alpha+1}$	$L_2 \oplus \lambda_a$	$\lambda_a = L_2$	$L_2 = 0$
$\lambda_{\alpha+1} \oplus \lambda_a$	L_2	$L_2 = 0$	$\lambda_a = L_2$
$\lambda_{\alpha+1} \oplus \lambda_b$	$L_2 \oplus \lambda_a$	$\lambda_a = L_2$	$L_2 = 0$
$\lambda_{\alpha+1} \oplus \lambda_a \oplus \lambda_b$	L_2	$L_2 = 0$	$\lambda_a = L_2$

$\boldsymbol{x}$	$\boldsymbol{y}$	$\boldsymbol{y = \lambda_a \oplus x}$	$\boldsymbol{y = \lambda_a \oplus x \oplus \lambda_b}$
$\lambda_{\alpha+1}$	$L_2 \oplus \lambda_a$	$L_2 = \lambda_{\alpha+1}$	$\lambda_b = \lambda_{\alpha+1} \oplus L_2$
$\lambda_{\alpha+1} \oplus \lambda_a$	L_2	$L_2 = \lambda_{\alpha+1}$	$\lambda_b = \lambda_{\alpha+1} \oplus L_2$
$\lambda_{\alpha+1} \oplus \lambda_b$	$L_2 \oplus \lambda_a$	$\lambda_b = \lambda_{\alpha+1} \oplus L_2$	$L_2 = \lambda_{\alpha+1}$
$\lambda_{\alpha+1} \oplus \lambda_a \oplus \lambda_b$	L_2	$\lambda_b = \lambda_{\alpha+1} \oplus L_2$	$L_2 = \lambda_{\alpha+1}$

$\boldsymbol{x}$	$\boldsymbol{y}$	$\boldsymbol{y = \lambda_\alpha}$	$\boldsymbol{y = \lambda_a \oplus \lambda_\alpha}$
$\lambda_{\alpha+1}$	$L_2 \oplus \lambda_a$	$\lambda_a = L_2 \oplus \lambda_\alpha$	$L_2 \oplus \lambda_\alpha = 0$
$\lambda_{\alpha+1} \oplus \lambda_a$	L_2	$L_2 = \lambda_\alpha$	$\lambda_a = L_2 \oplus \lambda_\alpha$
$\lambda_{\alpha+1} \oplus \lambda_b$	$L_2 \oplus \lambda_a$	$\lambda_a = L_2 \oplus \lambda_\alpha$	$L_2 = \lambda_\alpha$
$\lambda_{\alpha+1} \oplus \lambda_a \oplus \lambda_b$	L_2	$L_2 = \lambda_\alpha$	$\lambda_a = L_2 \oplus \lambda_\alpha$

$\boldsymbol{x}$	$\boldsymbol{y}$	$\boldsymbol{y = \lambda_a \oplus x \oplus \lambda_\alpha}$	$\boldsymbol{y = \lambda_a \oplus x \oplus \lambda_b \oplus \lambda_\alpha}$
$\lambda_{\alpha+1}$	$L_2 \oplus \lambda_a$	$\lambda_{\alpha+1} = L_2 \oplus \lambda_\alpha$	$\lambda_{\alpha+1} = \lambda_b \oplus L_2 \oplus \lambda_{\alpha+1}$
$\lambda_{\alpha+1} \oplus \lambda_a$	L_2	$\lambda_{\alpha+1} = L_2 \oplus \lambda_\alpha$	$\lambda_{\alpha+1} = \lambda_b \oplus L_2 \oplus \lambda_\alpha$
$\lambda_{\alpha+1} \oplus \lambda_b$	$L_2 \oplus \lambda_a$	$\lambda_{\alpha+1} = \lambda_b \oplus L_2 \oplus \lambda_\alpha$	$\lambda_{\alpha+1} = L_2 \oplus \lambda_\alpha$
$\lambda_{\alpha+1} \oplus \lambda_a \oplus \lambda_b$	L_2	$\lambda_{\alpha+1} = \lambda_b \oplus L_2 \oplus \lambda_\alpha$	$\lambda_{\alpha+1} = L_2 \oplus \lambda_\alpha$

The gray equations listed in the above four tables cannot hold because $\lambda_\alpha \cdot L_2 \cdot \lambda_{\alpha+1}$ is a valid tuple. Number of tuples of the form $\lambda_b \cdot x \cdot \lambda_a \cdot y \cdot \lambda_{\alpha+1}$ such that λ_a satisfies one of the 8 invalidity conditions given in the first and third tables is at most $\Delta(\alpha-2)$, because there can be $\alpha-2$ choices for λ_b. Similarly, number of tuples of the form $\lambda_b \cdot x \cdot \lambda_a \cdot y \cdot \lambda_{\alpha+1}$ such that λ_b satisfies one of the 8 invalidity conditions given in the second and fourth tables is at most $\Delta(\alpha-2)$. Hence, we have

$$|\mathscr{M}_3(\tau)| - 8(\alpha-1) + 4\Delta - 16\Delta(\alpha-2) \le |\mathscr{M}_5(\tau_1)| \le 4(\alpha-1)(\alpha-2). \quad (50)$$

B.4.2 Second Part: $|\mathscr{M}_{2\ell+5}|$ in terms of $|\mathscr{M}_{2\ell+3}|$ Recall that, for any valid label $\tau_1 = (\mathscr{B}_{\alpha+1}, L^{[2\ell+1]})$ and $\tau_2 = (\mathscr{B}_{\alpha+1}, L^{[2\ell+3]})$

$$\mathscr{M}_{2\ell+3}(\tau_1) = \{\lambda_b \cdot x \cdot \lambda_a \cdot y \cdot L^{[3,2\ell+1]} \in V'_{\ell+1} \mid a \neq b \in [\alpha-\ell], y \in L_2 \oplus \langle\lambda_a\rangle, x \in \lambda_{\alpha+1} \oplus \langle\lambda_a, \lambda_b\rangle\}$$

$$\mathscr{M}_{2\ell+5}(\tau_2) = \{\lambda_b \cdot x \cdot \lambda_a \cdot y \cdot L^{[3,2\ell+1]} \cdot L_{2\ell+2} \cdot L_{2\ell+3} \in V'_{\ell+2} \mid a \neq b \in [\alpha-\ell-1], y \in L_2 \oplus \langle\lambda_a\rangle, x \in \lambda_{\alpha+1} \oplus \langle\lambda_a, \lambda_b\rangle\}$$

There are $4(\alpha-\ell-1)$ tuples of the form, $\lambda_b \cdot x \cdot \lambda_{\alpha-\ell} \cdot y \cdot L^{[3,2\ell+1]}$, $b \in [\alpha-\ell-1]$ (because for each b, x can take 4 values, and for each such x, y can take one value), and $4(\alpha-\ell-1)$ tuples of the form, $\lambda_{\alpha-\ell} \cdot x \cdot \lambda_a \cdot y \cdot L^{[3,2\ell+1]}$, $a \in [\alpha-\ell-1]$, that might be in $\mathscr{M}_{2\ell+3}(\tau_1)$, but are definitely not in $\mathscr{M}_{2\ell+5}(\tau_2)$. $\lambda_b \cdot x \cdot \lambda_{\alpha-\ell} \cdot y \cdot L^{[3,2\ell+1]}$ will not be a valid tuple belonging to $\mathscr{M}_{2\ell+3}(\tau_1)$ if and only if for some value of λ_b, $x = 0$, which happens when either of the following holds:

- $\bullet$ $\lambda_b = \lambda_{\alpha+1}$
- $\bullet$ $\lambda_b = \lambda_{\alpha+1} \oplus \lambda_{\alpha-\ell}$

as $L^{[3,2\ell+1]}$ is already a valid tuple.

Now either of the cases can happen in atmost Δ ways giving us at least $(4(\alpha-\ell-1)-2\Delta)$ tuples of the form $\lambda_b \cdot x \cdot \lambda_{\alpha-\ell} \cdot y \cdot L^{[3,2\ell+1]}$ that are in $\mathscr{M}_{2\ell+3}(\tau_1)$ but not in $\mathscr{M}_{2\ell+5}(\tau_2)$.

Similarly there are at least $(4(\alpha-\ell-1)-2\Delta)$ tuples of the form $\lambda_{\alpha-\ell} \cdot x \cdot \lambda_a \cdot y \cdot L^{[3,2\ell+1]}$ that are in $\mathscr{M}_{2\ell+3}(\tau_1)$ but not in $\mathscr{M}_{2\ell+5}(\tau_2)$. The tuples of the form $\lambda_b \cdot x \cdot \lambda_a \cdot y \cdot L^{[3,2\ell+1]} \cdot L_{2\ell+2} \cdot L_{2\ell+3}$ that are not valid, are the ones that satisfy either of the following conditions :

$$y = 0 \qquad y = L_3 \qquad \cdots\cdots \qquad y = \bigoplus_{i=3}^{2\ell+1} L_i$$
$$y = \lambda_a \qquad y = \lambda_a \oplus L_3 \qquad y = \lambda_a \oplus \bigoplus_{i=3}^{2\ell+1} L_i$$
$$y = \lambda_a \oplus x \qquad y = \lambda_a \oplus x \oplus L_3 \qquad y = \lambda_a \oplus x \oplus \bigoplus_{i=3}^{2\ell+1} L_i$$
$$y = \lambda_a \oplus x \oplus \lambda_b \qquad y = \lambda_a \oplus x \oplus \lambda_b \oplus L_3 \qquad y = \lambda_a \oplus x \oplus \lambda_b \oplus \bigoplus_{i=3}^{2\ell+1} L_i$$

$$y = \bigoplus_{i=3}^{2\ell+2} L_i \qquad y = \bigoplus_{i=3}^{2\ell+3} L_i$$
$$y = \lambda_a \oplus \bigoplus_{i=3}^{2\ell+2} L_i \qquad y = \lambda_a \oplus \bigoplus_{i=3}^{2\ell+3} L_i$$
$$y = \lambda_a \oplus x \oplus \bigoplus_{i=3}^{2\ell+2} L_i \qquad y = \lambda_a \oplus x \oplus \bigoplus_{i=3}^{2\ell+3} L_i$$
$$y = \lambda_a \oplus x \oplus \lambda_b \oplus \bigoplus_{i=3}^{2\ell+2} L_i \qquad y = \lambda_a \oplus x \oplus \lambda_b \oplus \bigoplus_{i=3}^{2\ell+3} L_i$$

The gray equations listed above cannot hold because because $\lambda_b \cdot x \cdot \lambda_a \cdot y \cdot L^{[3,2\ell+1]}$ is a valid tuple belonging to $\mathscr{M}_{2\ell+3}(\tau_1)$. To check the other invalidity conditions we check the following tables (where $Z = \bigoplus_{i=3}^{2m+2} L_i$)

$\boldsymbol{x}$	$\boldsymbol{y}$	$\boldsymbol{y = Z}$	$\boldsymbol{y = Z \oplus \lambda_a}$
$\lambda_{\alpha+1}$	$L_2 \oplus \lambda_a$	$\lambda_a = L_2 \oplus Z$	$L_2 \oplus Z = 0$
$\lambda_{\alpha+1} \oplus \lambda_a$	L_2	$L_2 \oplus Z = 0$	$\lambda_a = L_2 \oplus Z$
$\lambda_{\alpha+1} \oplus \lambda_b$	$L_2 \oplus \lambda_a$	$\lambda_a = L_2 \oplus Z$	$L_2 \oplus Z = 0$
$\lambda_{\alpha+1} \oplus \lambda_a \oplus \lambda_b$	L_2	$L_2 \oplus Z = 0$	$\lambda_a = L_2 \oplus Z$

$\boldsymbol{x}$	$\boldsymbol{y}$	$\boldsymbol{y = Z \oplus \lambda_a \oplus x}$	$\boldsymbol{y = Z \oplus \lambda_a \oplus x \oplus \lambda_b}$
$\lambda_{\alpha+1}$	$L_2 \oplus \lambda_a$	$\lambda_{\alpha+1} \oplus L_2 \oplus Z = 0$	$\lambda_b = \lambda_{\alpha+1} \oplus L_2 \oplus Z$
$\lambda_{\alpha+1} \oplus \lambda_a$	L_2	$\lambda_{\alpha+1} \oplus L_2 \oplus Z = 0$	$\lambda_b = \lambda_{\alpha+1} \oplus L_2 \oplus Z$
$\lambda_{\alpha+1} \oplus \lambda_b$	$L_2 \oplus \lambda_a$	$\lambda_b = \lambda_{\alpha+1} \oplus L_2 \oplus Z$	$\lambda_{\alpha+1} \oplus L_2 \oplus Z = 0$
$\lambda_{\alpha+1} \oplus \lambda_a \oplus \lambda_b$	L_2	$\lambda_b = \lambda_{\alpha+1} \oplus L_2 \oplus Z$	$\lambda_{\alpha+1} \oplus L_2 \oplus Z = 0$

$\boldsymbol{x}$	$\boldsymbol{y}$	$\boldsymbol{y = Z \oplus L_{2\ell+3}}$	$\boldsymbol{y = Z \oplus L_{2\ell+3} \oplus \lambda_i}$
$\lambda_{\alpha+1}$	$L_2 \oplus \lambda_a$	$\lambda_a = L_2 \oplus Z \oplus L_{2\ell+3}$	$L_2 \oplus Z \oplus L_{2\ell+3} = 0$
$\lambda_{\alpha+1} \oplus \lambda_a$	L_2	$L_2 \oplus Z \oplus L_{2\ell+3} = 0$	$\lambda_a = L_2 \oplus Z \oplus L_{2\ell+3}$
$\lambda_{\alpha+1} \oplus \lambda_b$	$L_2 \oplus \lambda_a$	$\lambda_a = L_2 \oplus Z \oplus L_{2\ell+3}$	$L_2 \oplus Z \oplus L_{2\ell+3} = 0$
$\lambda_{\alpha+1} \oplus \lambda_a \oplus \lambda_b$	L_2	$L_2 \oplus Z \oplus L_{2\ell+3} = 0$	$\lambda_a = L_2 \oplus Z \oplus L_{2\ell+3}$

$\boldsymbol{x}$	$\boldsymbol{y}$	$\boldsymbol{y = Z \oplus L_{2\ell+3} \oplus \lambda_a \oplus x}$	$\boldsymbol{y = Z \oplus L_{2\ell+3} \oplus \lambda_a \oplus x \oplus \lambda_b}$
$\lambda_{\alpha+1}$	$L_2 \oplus \lambda_i = a$	$\lambda_{\alpha+1} \oplus L_2 \oplus Z \oplus L_{2\ell+3} = 0$	$\lambda_b = \lambda_{\alpha+1} \oplus L_2 \oplus Z \oplus L_{2\ell+3}$
$\lambda_{\alpha+1} \oplus \lambda_a$	L_2	$\lambda_{\alpha+1} \oplus L_2 \oplus Z \oplus L_{2\ell+3} = 0$	$\lambda_b = \lambda_{\alpha+1} \oplus L_2 \oplus Z \oplus L_{2\ell+3}$
$\lambda_{\alpha+1} \oplus \lambda_b$	$L_2 \oplus \lambda_a$	$\lambda_b = \lambda_{\alpha+1} \oplus L_2 \oplus Z \oplus L_{2\ell+3}$	$\lambda_{\alpha+1} \oplus L_2 \oplus Z \oplus L_{2\ell+3} = 0$
$\lambda_{\alpha+1} \oplus \lambda_a \oplus \lambda_b$	L_2	$\lambda_b = \lambda_{\alpha+1} \oplus L_2 \oplus Z \oplus L_{2\ell+3}$	$\lambda_{\alpha+1} \oplus L_2 \oplus Z \oplus L_{2\ell+3} = 0$

Again, the gray equations listed in the above four tables cannot hold because we have assumed $L^{[2,2\ell+3]}$ is a valid tuple. Number of tuples of the form $\lambda_b \cdot x \cdot \lambda_a \cdot y \cdot L^{[3,2\ell+3]}$ such that λ_a satisfies one of the 8 invalidity conditions given in the first and third tables is at most $\Delta(\alpha-\ell-2)$, because there can be $\alpha-\ell-2$ choices for λ_b. Similarly, number of tuples of the form $\lambda_b \cdot x \cdot \lambda_a \cdot y \cdot L^{[3,2\ell+3]}$ such that λ_b satisfies one of the 8 invalidity conditions given in the second and fourth tables is at most $\Delta(\alpha-\ell-2)$. Hence for $\ell \geq 1$,

$$|\mathscr{M}_{2\ell+3}(\tau_1)| - 8(\alpha-\ell-1) + 4\Delta - 16\Delta(\alpha-\ell-2) \leq |\mathscr{M}_{2\ell+5}(\tau_2)| \leq 4(\alpha-\ell-1)(\alpha-\ell-2). \tag{51}$$

Now, by combining Eqn. (50) and Eqn. (51), we get the result for all $\ell \geq 0$. □

C Proof of Lemma 6 : Size Lemma for Independent Permutations

In this section, we prove each part of Lemma 6 in separate sections.

C.1 Proof of Part (a) of the Lemma

For $\tau = \mathscr{B}_{\alpha+1}$, we have $\mathscr{M}'_3(\tau) = \{\lambda_i \cdot \lambda_{\alpha+1} \cdot \lambda_j \in U'_3 \mid i \neq j \in [\alpha]\}$. Now for a tuple $\lambda_i \cdot \lambda_{\alpha+1} \cdot \lambda_j$ to be valid, the two conditions must hold, $\lambda_i \neq \lambda_{\alpha+1}$ and $\lambda_j \neq \lambda_{\alpha+1}$. There are exactly $(\alpha-\delta)$ many labels from which we can choose λ_i and λ_j. As $i \neq j$, we get $|\mathscr{M}'_3(\tau)| = (\alpha-\delta)(\alpha-\delta-1)$. □

C.2 Proof of Part (b) of the Lemma

Recall that, for any valid label $\tau = \mathscr{B}_{\alpha+1}$, we have $\mathscr{N}'_3(\tau) = \{\lambda_i \cdot (\lambda_i \oplus L_1 \oplus L_2) \cdot \lambda_\alpha \in U'_3 \mid i \in [\alpha-1]\} \cup \{\lambda_i \cdot L_2 \cdot \lambda_\alpha \in U'_3 \mid i \in [\alpha-1]\}$. The tuple $\lambda_i \cdot (\lambda_i \oplus L_1 \oplus L_2) \cdot \lambda_\alpha$ is valid only under the condition that $\lambda_i \neq \lambda_\alpha \oplus L_1 \oplus L_2$, which can happen in at least $\alpha - 1 - \Delta$ ways, so $\alpha - 1 - \Delta \leq |\{\lambda_i \cdot (\lambda_i \oplus L_1 \oplus L_2) \cdot \lambda_\alpha \in U'_3 \mid i \in [\alpha-1]\}| \leq \alpha - 1$. Similarly, $\lambda_i \cdot L_2 \cdot \lambda_\alpha$ is valid if and only if $\lambda_i \neq L_2$, so $\alpha - 1 - \Delta \leq |\{\lambda_i \cdot L_2 \cdot \lambda_\alpha \in U'_3 \mid i \in [\alpha-1]\}| \leq \alpha - 1$. □

C.3 Proof of Part (c) of the Lemma

Recall that, for any valid label $\tau_1 = (\mathscr{B}_{\alpha+1}, L^{[2\ell+1]})$ and $\tau_2 = (\mathscr{B}_{\alpha+1}, L^{[2\ell+3]})$, we have

$$\mathscr{N}'_{2\ell+1}(\tau_1) = \{\lambda_i.(\lambda_i \oplus L_2 \oplus L_1).L^{[3,2\ell+1]} \in U'_\ell \mid i \in [\alpha-\ell]\} \cup \{\lambda_i.L_2.L^{[3,2\ell+1]} \in U'_\ell \mid i \in [\alpha-\ell]\}$$

$$\mathscr{N}'_{2\ell+3}(\tau_2) = \{\lambda_i.(\lambda_i \oplus L_2 \oplus L_1).L^{[3,2\ell+3]} \in U'_{\ell+1} \mid i \in [\alpha-\ell-1]\} \cup \{\lambda_i.L_2.L^{[3,2\ell+3]} \in U'_{\ell+1} \mid i \in [\alpha-\ell-1]\}$$

Firstly, $\lambda_{\alpha-\ell}.(\lambda_{\alpha-\ell} \oplus L_2 \oplus L_1).L^{[3,2\ell+1]}$ and $\lambda_{\alpha-\ell}.L_2.L^{[3,2\ell+1]} \in \mathcal{N}'_{2\ell+1}$ but does not belong to $\mathcal{N}'_{2\ell+3}$.
Any other valid ℓ-linked label, $\lambda_i.(\lambda_i \oplus L_2 \oplus L_1).L^{[3,2\ell+1]}$ in $\mathcal{N}'_{2\ell+1}$, such that $\lambda_i.(\lambda_i \oplus L_2 \oplus L_1).L^{[3,2\ell+3]} \notin \mathcal{N}'_{2\ell+1}$ must satisfy the equality:

$$\lambda_i = L_1 \oplus L_2 \oplus \cdots \oplus L_{2\ell+3}.$$

This equality can hold in atmost Δ ways, hence,

$$\begin{aligned}&|\{\lambda_i.(\lambda_i \oplus L_2 \oplus L_1).L^{[3,2\ell+1]} \in U'_\ell \mid i \in [\alpha-\ell]\}| - 1 - \Delta \\ &\quad \le |\{\lambda_i.(\lambda_i \oplus L_2 \oplus L_1).L^{[3,2\ell+3]} \in U'_{\ell+1} \mid i \in [\alpha-\ell-1]\}| \le \alpha-\ell-1.\end{aligned}$$

Similarly, any other $\lambda_i.L_2.L^{[3,2\ell+1]}$ in $\mathcal{N}'_{2\ell+1}$, such that $\lambda_i.L_2.L^{[3,2\ell+3]} \notin \mathcal{N}'_{2\ell+3}$, must satisfy the equality

$$\lambda_i = L_2 \oplus L_3 \oplus \cdots \oplus L_{2\ell+2},$$

which can happen in at most Δ ways. Hence

$$\begin{aligned}&|\{\lambda_i.L_2.L^{[3,2\ell+1]} \in U'_\ell \mid i \in [\alpha-\ell]\}| - 1 - \Delta \\ &\quad \le |\{\lambda_i.L_2.L^{[3,2\ell+3]} \in U'_{\ell+1} \mid i \in [\alpha-\ell-1]\}| \le \alpha-\ell-1.\end{aligned}$$

□

C.4 Proof of Part (d) and (e) of the Lemma 6

Recall that, for any valid label $\tau_1 = (\mathscr{B}_{\alpha+1}, L^{[2\ell+1]})$ and $\tau_2 = (\mathscr{B}_{\alpha+1}, L^{[2\ell+3]})$, we have

$$\mathscr{M}'_{2\ell+3}(\tau) = \{\lambda_j.\lambda_{\alpha+1}.\lambda_i.(\lambda_i \oplus L_1 \oplus L_2).L^{[3,2\ell+1]} \in U'_{\ell+1} \mid i \ne j \in [\alpha-\ell]\}$$

$$\mathscr{M}'_{2\ell+5}(\tau) = \{\lambda_j.\lambda_{\alpha+1}.\lambda_i.(\lambda_i \oplus L_1 \oplus L_2).L^{[3,2\ell+3]} \in U'_{\ell+2} \mid i \ne j \in [\alpha-\ell-1]\}$$

Firstly, if $\lambda_{\alpha-\ell} \ne \lambda_{\alpha+1}$, there are $(\alpha-\ell-1-\Delta)$ many tuples of the form $\lambda_{\alpha-\ell}.\lambda_{\alpha+1}.\lambda_i.(\lambda_i \oplus L_1 \oplus L_2).L^{[3,2\ell+1]}$ in $\mathscr{M}'_{2\ell+3}$, but $\lambda_{\alpha-\ell}.\lambda_{\alpha+1}.\lambda_i.(\lambda_i \oplus L_1 \oplus L_2).L^{[3,2\ell+3]} \notin \mathscr{M}'_{2\ell+5}$. This is because $\lambda_{\alpha-\ell}.\lambda_{\alpha+1}.\lambda_i.(\lambda_i \oplus L_1 \oplus L_2).L^{[3,2\ell+1]}$ will not be a valid tuple if

$$\lambda_i = \lambda_{\alpha+1},$$

which can happen in at most Δ ways. Similarly, if $\lambda_{\alpha-\ell} \ne \lambda_{\alpha+1}$, there are $(\alpha-\ell-1-\Delta)$ many tuples of the form $\lambda_j.\lambda_{\alpha+1}.\lambda_{\alpha-\ell}.(\lambda_{\alpha-\ell} \oplus L_1 \oplus L_2).L^{[3,2\ell+1]}$ in $\mathscr{M}'_{2\ell+3}$, but $\lambda_j.\lambda_{\alpha+1}.\lambda_{\alpha-\ell}.(\lambda_{\alpha-\ell} \oplus L_1 \oplus L_2).L^{[3,2\ell+3]} \notin \mathscr{M}'_{2\ell+5}$.
For any other $\lambda_j.\lambda_{\alpha+1}.\lambda_{\alpha-\ell}.(\lambda_{\alpha-\ell} \oplus L_1 \oplus L_2).L^{[3,2\ell+1]} \in \mathscr{M}'_{2\ell+3}$, such that $\lambda_j.\lambda_{\alpha+1}.\lambda_{\alpha-\ell}.(\lambda_{\alpha-\ell} \oplus L_1 \oplus L_2).L^{[3,2\ell+3]} \notin \mathscr{M}'_{2\ell+5}$, it must satisfy

$$\lambda_j = L_2 \oplus L_3 \oplus L_{2\ell+2},$$

which can happen in atmost Δ, which gives us at most $\Delta(\alpha-\ell-1)$ such tuples (as λ_i can be chosen in $\alpha-\ell-2$ ways). Hence

$$|\mathscr{M}'_{2\ell+3}(\tau_1)| - 2(\alpha-\ell-1) + 2\Delta - \Delta(\alpha-\ell-2) \le |\mathscr{M}'_{2\ell+5}(\tau_2)| \overset{(\star)}{\le} (\alpha-\ell-1)(\alpha-\ell-2)$$

where $(\star)$ follows from the fact that $i \ne j \in [\alpha-\ell-1]$. □

D Proof of Claim 1

As $a^k_{m+1} = 0$ for $k < 0$, we have the following inequality for $k < 0$:

$$a^k_{m+1} \le a^{k-1}_m + 2Da^k_m + D^2 a^{k+1}_m, \tag{52}$$

as all the terms $a^{k-1}_m, a^k_m, a^{k+1}_m$ are non-negative. We use this truncated recurrence relation for a^k_m when $k < 0$. Our claim holds for $d = 1$ as is evident if we put $m + 1 = T$ and $k = 0$ in (9). For $d = 2$, we see,

$$\begin{aligned}
a^0_T &= a^{-1}_{T-1} + 2Da^0_{T-1} + D^2 a^1_{T-1} + \frac{E' \cdot \xi}{2^n - \gamma T} \\
&\le a^{-2}_{T-2} + 2Da^{-1}_{T-2} + D^2 a^0_{T-2} \qquad (\star) \\
&\quad +2D\left(a^{-1}_{T-2} + 2Da^0_{T-2} + D^2 a^1_{T-2} + \frac{E' \cdot \xi}{(2^n - \gamma T)^2}\right) \\
&\quad +D^2\left(a^0_{T-2} + 2Da^1_{T-2} + D^2 a^2_{T-2} + \frac{E' \cdot \xi}{(2^n - \gamma T)^3}\right) \\
&\quad +\frac{E' \cdot \xi}{2^n - \gamma T} \\
&= 6D^2 a^0_{T-2} + 4D^3 a^1_{T-2} + a^2_{T-2} \\
&\quad +\frac{E' \cdot \xi}{2^n - \gamma T} + 2D \cdot \frac{E' \cdot \xi}{(2^n - \gamma T)^2} + D^2 \cdot \frac{E' \cdot \xi}{(2^n - \gamma T)^3},
\end{aligned}$$

where $(\star)$ follows from (52). Hence our claim is true for $d = 2$. We make the inductive hypothesis that it holds for some $p > 1$ and prove that it holds for $p+1$ as well. We check the terms in $\sum_{j=0}^{2p} \binom{2p}{j} D^j a^{j-p}_{T-p}$ which gives rise to the term a^{j-p-1}_{T-p-1} when (9) or (52) is applied. We see those terms are $a^{j-p-2}_{T-p}, a^{j-p-1}_{T-p}, a^{j-p}_{T-p}$, and they contribute $D^2 a^{j-p-1}_{T-p-1}$, $2Da^{j-p-1}_{T-p-1}$, a^{j-p-1}_{T-p-1}, respectively (See Fig. D.1).

Hence the coefficient of a^{j-p-1}_{T-p-1} in this $(p+1)^{th}$ level of iteration would be

$$\left(\binom{2p}{j-2} + 2\binom{2p}{j-1} + \binom{2p}{j}\right) D^j = \binom{2p+2}{j} D^j.$$

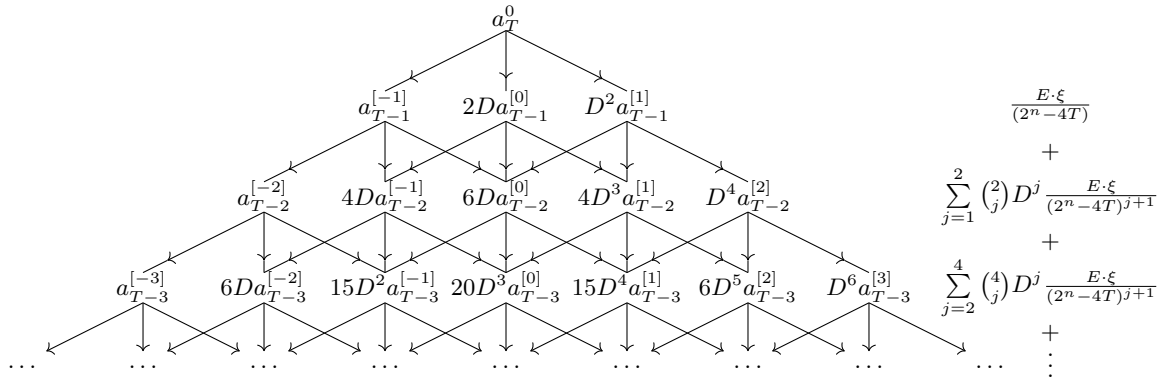

Fig. D.1: How the terms of a_m^k add up at every iteration of the recurrence relation

Also each of the a_{T-p}^{j-p}, for $j \geq p$, would add $\frac{E\cdot\xi}{(2^n-\gamma T)^{j+1}}$ to the $(p+1)^{th}$ level of iteration. Hence from our inductive hypothesis,

$$\begin{aligned}
a_T^0 &\leq \sum_{j=p}^{2p}\binom{2d}{j}D^j a_{T-p}^{j-p} + \sum_{t=0}^{p-1}\sum_{t=r}^{2t}\binom{2t}{j}D^j\frac{E'\cdot\xi}{(2^n-\gamma T)^{j+1}} \\
&= \sum_{j=0}^{2p}\binom{2p}{j}D^j a_{T-p}^{j-p} + \sum_{t=0}^{p-1}\sum_{j=t}^{2t}\binom{2t}{j}D^j\frac{E'\cdot\xi}{(2^n-\gamma T)^{j+1}} \\
&\leq \sum_{j=0}^{2(p+1)}\binom{2p+2}{j}D^j a_{T-p-1}^{j-p-1} + \sum_{t=0}^{p-1}\sum_{j=t}^{2t}\binom{2t}{j}D^j\frac{E'\cdot\xi}{(2^n-\gamma T)^{j+1}} \\
&\quad + \sum_{j=p}^{2p}\binom{2p}{j}D^j\frac{E'\cdot\xi}{(2^n-\gamma T)^{j+1}} \\
&\leq \sum_{j=p+1}^{2(p+1)}\binom{2p+2}{j}D^j a_{T-p-1}^{j-p-1} + \sum_{t=0}^{p}\sum_{j=t}^{2t}\binom{2t}{j}D^j\frac{E'\cdot\xi}{(2^n-\gamma T)^{j+1}}.
\end{aligned}$$

Hence our claim holds for $p+1$ whenever it holds for p. Hence our claim holds for every $d > 1$. □

E Proof of Corollary 1 and Corollary 2

E.1 Proof of Corollary 1

Let $\tau = \{(x_1, y_1), (x_2, y_2), \ldots, (x_q, y_q)\}$ be the transcript that result from the interaction between A and the corresponding oracle, where $x_i \in \{0,1\}^{n-1}$ is the i-th query of A and y_i be its corresponding response. We call τ to be a *bad transcript* if there exists at least one $i \in [q]$ such that $y_i = 0^n$. Otherwise, τ is said to be a *good transcript*.

According to the H-Coefficient technique, we bound the probability of the occurence of bad transcripts in the ideal world. Let D_{re} (resp. D_{id}) be the random variable that takes the transcript induced by the real world (resp. ideal world) distribution. Let Θ_{good} (resp. Θ_{bad}) denotes the set of all good (resp. bad transcripts). Then, we have

$$\begin{aligned}\Pr[\mathsf{D}_{\mathrm{id}} \in \Theta_{\mathrm{bad}}] &= \Pr[\exists i \text{ such that } y_i = 0^n] \\ &= 1 - \Pr[\forall i \text{ such that } y_i \neq 0^n] \\ &\overset{(1)}{=} 1 - (1 - 2^{-n})^q, \end{aligned} \tag{53}$$

where (1) follows as the y_i's are independently and uniformly sampled in the ideal world. Therefore, for a good transcript τ, each y_i is a non-zero n-bit string. Therefore, for a good transcript $\tau = \{(x_1, y_1), (x_2, y_2), \ldots, (x_q, y_q)\}$, which is realized in the real world, we can write

$$\mathscr{E} = \begin{cases} \pi(0\|x_1) \oplus \pi(1\|x_1) = y_1 \\ \pi(0\|x_2) \oplus \pi(1\|x_2) = y_2 \\ \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\ \pi(0\|x_q) \oplus \pi(1\|x_q) = y_q. \end{cases}$$

Computing the real interpolation probability for a good transcript τ, i.e., computing $\Pr[\mathsf{D}_{\mathrm{re}} = \tau]$, is equivalent to count the number of permutations π satisfying $\mathscr{E}$. Note that, as τ is a good transcript, this count is essentially $(2^n)_{2q}/2^{nq}$ that follows from our main theorem of the paper as we are dealing with $\xi_{\max} = 2$. Therefore,

$$\Pr[\mathsf{D}_{\mathrm{re}} = \tau] \geq \frac{1}{2^{nq}} = \Pr[\mathsf{D}_{\mathrm{id}} = \tau](\text{ the ideal interpolation probability of } \tau).$$

Thus, the ratio of real to ideal interpolation probability becomes at least 1. Hence, by the result of H-Coefficient technique,

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XOR}_1}(\mathsf{A}) \leq 1 - (1 - 2^{-n})^q,$$

which proves the result.

E.2 Proof of Corollary 2

In this proof, there is no bad transcript. Therefore, for any transcript τ, probability of realizing it in the real worls is equivalent to count the number of distinct solutions to the following system of equations: $\mathscr{E} = \{\pi_1(x_1) \oplus \pi_2(x_1) = y_1, \pi_1(x_2) \oplus \pi_2(x_2) = y_2, \ldots, \pi_1(x_q) \oplus \pi_2(x_q) = y_q\}$, which is $(2^n)_q \cdot (2^n)_q / 2^{nq} \cdot (1 - \epsilon)$, where $\epsilon = 1.2q^2/2^{2n} + \frac{108n^3}{2^{2n}}$ that follows from our main theorem of the paper as we are dealing with $\xi_{\max} = 2$. Therefore,

$$\Pr[\mathsf{D}_{\mathrm{re}} = \tau] \geq \frac{1}{2^{nq}} \cdot \left(1 - \frac{1.2q^2}{2^{2n}} - \frac{108n^3}{2^{2n}}\right).$$

Hence, by the result of H-Coefficient technique, our result follows.