Building PRFs from TPRPs: Beyond the Block and the Tweak Length Bounds

Wonseok Choi, Jooyoung Lee, and Yeongmin Lee

{krwioh,hicalf,dudals4780}@kaist.ac.kr

KAIST, Korea

Abstract. A secure n-bit tweakable block cipher (TBC) using t-bit tweaks can be modeled as a tweakable uniform random permutation, where each tweak defines an independent random n-bit permutation. When an input to this tweakable permutation is fixed, it can be viewed as a perfectly secure t-bit random function. On the other hand, when a tweak is fixed, it can be viewed as a perfectly secure n-bit random permutation, and it is well known that the sum of two random permutations is pseudorandom up to 2^n queries.

A natural question is whether one can construct a pseudorandom function (PRF) beyond the block and the tweak length bounds using a small number of calls to the underlying tweakable permutations. As a positive answer to this question, we propose two PRF constructions based on tweakable permutations, dubbed $\mathsf{XoTP1}_c$ and $\mathsf{XoTP2}_c$, respectively. Both constructions are parameterized by c, giving a $(t+n-c)$-to-n bit PRF.

When $t < 2n$, $\mathsf{XoTP1}_{\frac{t}{2}}$ becomes an $(n+\frac{t}{2})$-to-n bit pseudorandom function, which is secure up to $2^{n+\frac{t}{2}}$ queries. $\mathsf{XoTP2}_{\frac{t}{3}}$ is even better, giving an $(n+\frac{2t}{3})$-to-n bit pseudorandom function, which is secure up to $2^{n+\frac{2t}{3}}$ queries, when $t < 3n$. These PRFs provide security beyond the block and the tweak length bounds, making two calls to the underlying tweakable permutations.

In order to prove the security of $\mathsf{XoTP1}$ and $\mathsf{XoTP2}$, we firstly extend Mirror theory to $q \gg 2^n$, where q is the number of equations. From a practical point of view, our constructions can be used to construct TBC-based MAC finalization functions and CTR-type encryption modes with stronger provable security compared to existing schemes.

Keywords: Mirror theory, pseudorandom function, tweakable block cipher, sum of permutations

1 Introduction

Constructing PRFs from PRPs. A block cipher is typically modeled as a pseudorandom permutation (PRP) in a provable security setting: any adversary

should not be able to distinguish the block cipher from a truly random permutation by making a certain number of encryption and decryption queries in a black-box manner. However, for some modes of operation, one might want the block cipher to behave like a pseudorandom function (PRF). For example, a counter mode generates a keystream

$$\mathsf{E}_K(N \,\|\, 0), \mathsf{E}_K(N \,\|\, 1), \mathsf{E}_K(N \,\|\, 2), \ldots$$

using a block cipher E with a secret key K and a nonce N. In this mode of operation, all the blocks are pairwise distinct, allowing an adversary to distinguish it from a truly random keystream. For this reason, the counter mode is proved to be secure only up to the birthday bound (in the assumption that E is a pseudorandom permutation). This observation motivates the problem of constructing a pseudorandom function from pseudorandom permutations. Sometimes this problem is called "Luby-Rackoff backward" [3]: the Feistel network transforms a set of (not necessarily one-to-one) functions into a permutation, and this problem considers its opposite direction.

A natural way of building a PRF by using PRPs is to xor two independent pseudorandom permutations. Given two n-bit (keyed) PRPs P and P', their sum, denoted XoP, maps $X \in \{0,1\}^n$ to

$$\mathsf{XoP}(X) \stackrel{\text{def}}{=} \mathsf{P}(X) \oplus \mathsf{P}'(X).$$

Alternatively, one can simply truncate outputs from a single permutation. This construction, denoted TRP, maps $X \in \{0,1\}^n$ to

$$\mathsf{TRP}_m(X) \stackrel{\text{def}}{=} \mathsf{Tr}_m\left(\mathsf{P}(X)\right)$$

where m is a positive integer such that $m < n$, and Tr_m is a truncation function that takes an n-bit string and returns leftmost m bits of the input. There has been a significant amount of research on these constructions [2, 3, 4, 5, 9, 14, 15, 16, 24, 32, 33].

Tweakable Block Ciphers. Tweakable block ciphers (TBC), first introduced in [25], are a generalization of standard block ciphers that accept extra inputs called *tweaks*. The tweak, providing inherent variability to the block cipher, makes it easy to design various higher level cryptographic schemes such as message authentication codes and modes of operation.

Tweakable block ciphers can either be designed from scratch [8, 13, 35], or be built upon off-the-shelf cryptographic primitives such as block ciphers and (public) permutations [6, 23, 27, 30]. Recently, a unified vision for the tweak and key inputs has been proposed within the TWEAKEY framework [19]. Skinny [1] and deoxys-BC [20] follow this framework. Theoretically, a secure TBC is modeled as a tweakable pseudorandom permutation (TPRP); when a key is chosen uniformly at random and kept secret, the keyed TBC should behave like an independent random permutation for each tweak. The ideal counterpart of a TPRP is called a *tweakable uniform random permutation* (TURP).

1.1 Our Contribution

Building PRFs from TPRPs. As tweakable block ciphers are widely used and studied, it is natural to ask how one can efficiently construct a PRF on top of a tweakable block cipher. The underlying tweakable block cipher being modeled as an n-bit TURP using t-bit tweaks, denoted $\widetilde{\mathsf{P}}$, a straightforward construction is to fix a message input to $\widetilde{\mathsf{P}}$, obtaining a t-to-n bit function. Then such a construction is perfectly secure for every possible query; it is secure up to 2^t queries. On the other hand, one can obtain a perfectly random n-bit permutation by fixing a tweak input to $\widetilde{\mathsf{P}}$. This construction is secure only up to the birthday bound. By summing two distinct permutations (using different tweaks), one can obtain a pseudorandom function that is secure up to 2^n queries [32].

The goal of this paper is to construct pseudorandom functions that make a small number of calls to the underlying TPRPs, providing security beyond the block and the tweak length bounds. We note that a TBC-based Feistel cipher provides such a strong security bound with at least 10 rounds, using that many tweakable block cipher calls [36].

In this work, we propose two PRF constructions using only two calls to the underlying TPRPs

$$\widetilde{\mathsf{P}} : \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n,$$
$$\widetilde{\mathsf{Q}} : \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n,$$

where $\widetilde{\mathsf{P}}$ and $\widetilde{\mathsf{Q}}$ can be seen as TURPs up to their TPRP-security.

Given a (public) constant $C \in \{0,1\}^c$ for an integer c such that $0 \le c \le n$, the first construction, dubbed $\mathsf{XoTP1}_c$, is defined as follows.

$$\mathsf{XoTP1}_c(X,Y) \stackrel{\text{def}}{=} \widetilde{\mathsf{P}}(Y, C \,\|\, X) \oplus \widetilde{\mathsf{Q}}(Y, C \,\|\, X)$$

for $X \in \{0,1\}^{n-c}$ and $Y \in \{0,1\}^t$ (see Figure 1). One can view $\mathsf{XoTP1}$ as XoP in the multi-user setting, where the number of users is 2^t and each user is allowed to make at most 2^{n-c} queries. Note that $\mathsf{XoTP1}_c$ is parameterized by c (instead of C) since its security depends only on the length of the constant.

We prove that the adversarial advantage in breaking the PRF-security of $\mathsf{XoTP1}_c$ is upper bounded by $O\left(\frac{q}{2^{n+c}}\right)$. In particular, when $t < 2n$, $\mathsf{XoTP1}_{\frac{t}{2}}$ is secure up to $2^{n+\frac{t}{2}}$ queries. When $t \ge 2n$, $\mathsf{XoTP1}_n$ is obviously secure up to 2^t queries.

In our second construction, dubbed $\mathsf{XoTP2}$, the position of X and Y are partially switched over $\widetilde{\mathsf{P}}$ and $\widetilde{\mathsf{Q}}$. When $t \ge n - c$,

$$\mathsf{XoTP2}_c(X,Y,W) = \widetilde{\mathsf{P}}(W \,\|\, Y, C \,\|\, X) \oplus \widetilde{\mathsf{Q}}(W \,\|\, X, C \,\|\, Y)$$

for X, $Y \in \{0,1\}^{n-c}$ and $W \in \{0,1\}^{t-n+c}$, and when $t < n - c$,

$$\mathsf{XoTP2}_c(X,Y,W) = \widetilde{\mathsf{P}}(Y, C \,\|\, W \,\|\, X) \oplus \widetilde{\mathsf{Q}}(X, C \,\|\, W \,\|\, Y)$$

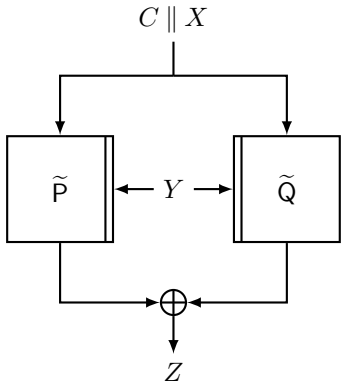
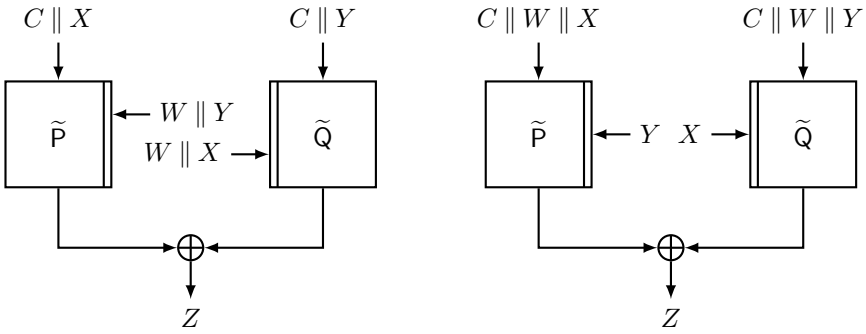


Fig. 1: $\mathsf{XoTP1}_c$ based on $\widetilde{\mathsf{P}}$ and $\widetilde{\mathsf{Q}}$.

for X, $Y \in \{0,1\}^t$ and $W \in \{0,1\}^{n-t-c}$ (see Figure 2). In this way, $\mathsf{XoTP2}_c$ becomes a $(t+n-c)$-to-n bit pseudorandom function.

We prove that when $t \geq n-c$ (resp. $t < n-c$), the adversarial advantage in breaking the PRF-security of $\mathsf{XoTP2}_c$ is upper bounded by $O\left(\min\{\frac{q}{2^{n+2c}}, \frac{q^2}{2^{3n}}\}\right)$ (resp. $O\left(\max\{\frac{q}{2^{n+t+c}}, \frac{q}{2^{n+2c}}\}\right)$). In particular, when $c < t$, the adversarial distinguishing advantage is upper bounded by $O\left(\frac{q}{2^{n+2c}}\right)$. Since the input size of $\mathsf{XoTP2}_c$ is $(t+n-c)$ bits, the threshold number of queries is maximized when $c = \frac{t}{3}$ (assuming $t \leq 3n$). Then $\mathsf{XoTP2}_{\frac{t}{3}}$ is secure up to $2^{n+\frac{2t}{3}}$ queries. Figure 3 shows the threshold number of queries q as a function of tweak size t for $\mathsf{XoTP1}_{\min\{\frac{t}{2},n\}}$ and $\mathsf{XoTP2}_{\frac{t}{3}}$. We see that $\mathsf{XoTP1}_{\frac{t}{2}}$ (resp. $\mathsf{XoTP2}_{\frac{t}{3}}$) enjoys security beyond the block and the tweak length bounds when $t < 2n$ (resp. $t < 3n$).



(a) $\mathsf{XoTP2}_c$ when $t \geq n-c$ (b) $\mathsf{XoTP2}_c$ when $t < n-c$

Fig. 2: $\mathsf{XoTP2}_c$ based on $\widetilde{\mathsf{P}}$ and $\widetilde{\mathsf{Q}}$.

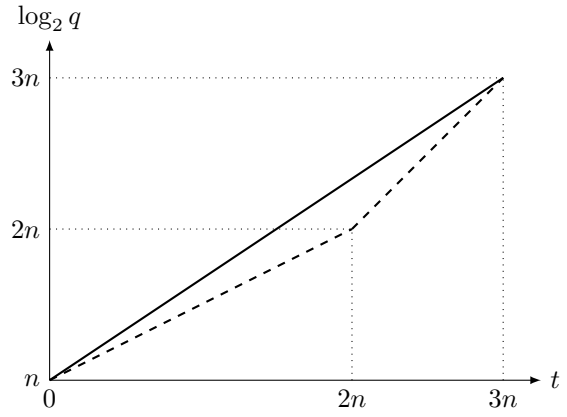


Fig. 3: The threshold number of queries q as a function of tweak size t. The dashed line is the bound for $\mathsf{XoTP1}_{\min\{\frac{t}{2},n\}}$, and the solid line is the bound for $\mathsf{XoTP2}_{\frac{t}{3}}$.

Application. Many deterministic MAC schemes can be viewed as an instance of the Hash-then-PRF paradigm; a variable-length message is first mapped onto a fixed-length value through a universal hash function, and then a PRF is applied to the hashed message, obtaining a tag. When it comes to TBC-based constructions using two TBC calls at the finalization step, most of such schemes provide at most n-bit security; PMAC-TBC1k [29] and PMACx [26] provide n-bit security and ZMAC [18] provides min $\left\{n, \frac{n+t}{2}\right\}$-bit security.

If $\mathsf{XoTP2}_c$ is combined with any birthday bound-secure $(t+n-c)$-bit hash function (though constructing such a nice hash function is an independent open question), then one might expect $\min\{\frac{t+n-c}{2}, \max\{n+2c, \frac{3n}{2}\}\}$-bit security for the resulting MAC scheme. When $n < t < 6n$, it will provide $\frac{2t+3n}{5}$-bit security with $c = \frac{t-n}{5}$, which is stronger than existing TBC-based MAC schemes (providing n-bit security) or using a trivial t-to-n bit PRF with a single TBC call.

If a TBC is used to construct a CTR-type encryption mode of rate 1 with a nonce as a tweak input and a block counter as a block cipher input, then the adversarial distinguishing advantage against this mode will be tightly upper bounded by

$$\frac{\sigma l}{2^n}$$

where l is the maximum message length and σ is the total number of message blocks. This security bound might not be sufficient, in particular when n is small.

In order to achieve stronger security (at the cost of worse efficiency), one might use an $(n+t-c)$-to-n bit PRF $\mathsf{XoTP2}_c$ to construct a CTR-type encryption mode of rate $\frac{1}{2}$. When $c = \frac{t}{3}$, $n + \frac{2t}{3}$ bits are available for nonces and counters, while the adversarial distinguishing advantage against this mode is

upper bounded by

$$O\left(\frac{\sigma}{2^{n+\frac{2t}{3}}}\right).$$

As a numerical example, consider the SKINNY-64-192 tweakable block cipher operating on 64-bit blocks using 192-bit tweakeys. If 128 bits are used as a key, then one can use 64-bit tweaks. In this case, one can use 106 input bits to $\mathsf{XoTP2}_{21}$ as nonces and counters (say, 64-bit nonces and 32-bit counters), and the resulting encryption mode will be secure as long as the total number of message blocks is small in front of 2^{106}.

If $n + \frac{2t}{3}$ bits are not sufficient for nonces and counters, one can simply take a small constant c so that the input size of the resulting PRF is almost $n + t$ bits. For the encryption mode using this PRF, the adversarial distinguishing advantage is still upper bounded by

$$O\left(\frac{\sigma^2}{2^{3n}}\right).$$

Proof Technique. Our proof is based on the standard H-coefficient technique, where Patarin's Mirror theory [34] is used for the counting arguments. Mirror theory allows one to sharply lower bound the number of solutions to a certain type of system of equations and non-equations. In our security proof, we will consider the following system of equations; for two sets of unknowns $\mathcal{V}_P = \{P_1, \ldots, P_q\}$ and $\mathcal{V}_Q = \{Q_1, \ldots, Q_q\}$, and for constants Z_i, $i = 1, \ldots, q$,

$$\Gamma : \begin{cases} P_1 \oplus Q_1 = Z_1, \\ P_2 \oplus Q_2 = Z_2, \\ \qquad \vdots \\ P_q \oplus Q_q = Z_q. \end{cases}$$

This system of equations can be represented by a simple graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \mathcal{V}_P \sqcup \mathcal{V}_Q$ and P_i and Q_i are connected by a Z_i-weighted edge for $i = 1, \ldots, q$. This graph consists of q isolated edges, so the size of the largest component in this graph, denoted $\xi_{\max}$, is two. The system of equations with $\xi_{\max} = 2$ appears in the security proof of the sum of two independent random permutations, where all the unknowns in $\mathcal{V}_P$ (resp. $\mathcal{V}_Q$) should be distinct since they are supposed to be outputs from a fixed permutation. These additional constraints can be viewed as non-equations between the unknowns. The resulting system of equations and non-equations has been studied in [34], and later revisited with more complete and detailed arguments [7, 11].

When it comes to a *tweakable* permutation, all the outputs are not necessarily distinct, in particular, when they are defined with distinct tweaks. With this observation, we relax the constraints of non-equations by defining partitions of $\mathcal{V}_P$ and $\mathcal{V}_Q$; if P_i and P_j (resp. Q_i and Q_j) are contained in the same block, then $P_i \neq P_j$ (resp. $Q_i \neq Q_j$). In this way, we generalize Mirror theory for $\xi_{\max} = 2$, and it leads to the security proof of XoTP1 and XoTP2.

History. A relaxed version of Mirror theory was also studied by Mennink et al. [28]. However, it was based on the original Mirror theory [34], which has been controversial due to some mistakes and gaps in the paper. Nandi [31] also pointed out that some part of [28] is flawed. Many researchers have revisited Mirror theory in more verifiable ways, while newly established Mirror theory takes more limited conditions for q and $\xi_{\max}$. Datta et al. [10] studied Mirror theory for $q = O\left(2^{\frac{2n}{3}}\right)$ and $\xi_{\max} = 3$ to prove the security of the DWCDM nonce-based MAC scheme. Dutta et al. [12] extended it to q and $\xi_{\max}$ such that $q = O\left(2^{\frac{2n}{3}}\right)$ and $q \cdot \xi_{\max} \leq 2^{n-2}$, and proved the security of the CWC+ AEAD mode. Jha and Nandi [21] further extended it to q and $\xi_{\max}$ such that $q = O\left(2^{\frac{3n}{4}}\right)$ and $q \cdot \xi_{\max} \leq 2^{n-1}$ to tightly prove the security of CLRW2. Kim et al. [22] studied Mirror theory for $q = O\left(2^{\frac{3n}{4}}\right)$ assuming that the number of components of size ≥ 3 is smaller than $2^{\frac{n}{2}}$, and it was sufficient to tightly prove the security of DbHtS MAC schemes. Recently, Dutta et al. [11] and Cogliati and Patarin [7] independently revisited Mirror theory for $q = O\left(2^n\right)$, giving clearer and verifiable proofs, while both assume $\xi_{\max} = 2$. In this line of research, we firstly establish Mirror theory for $q \gg 2^n$.

Open Problems. First of all, the exact security of the XoTP1 and XoTP2 constructions still remains open. Secondly, one can consider an alternative approach to constructing PRFs using a single call to the underlying primitive: to truncate outputs from a tweakable permutation. Fix two positive integers c and m such that c, $m \leq n$ as well as a constant $C \in \{0,1\}^c$, and let

$$\mathsf{TTRP}_{c,m}(X \,\|\, Y) \stackrel{\text{def}}{=} \mathsf{Tr}_m\left(\widetilde{\mathsf{P}}(Y, C \,\|\, X)\right)$$

for $X \in \{0,1\}^{n-c}$ and $Y \in \{0,1\}^t$. Since TRP_m permits an attack using $2^{n-\frac{m}{2}}$ queries, we need to fix a part of the input, so that an adversary is not able to make that many queries for a single tweak. We leave the (exact) security of $\mathsf{TTRP}_{c,m}$ as an open problem.

When it comes to Mirror theory, relaxing the constraint $\xi_{\max} = 2$ seems to be an important open question from both theoretical and practical point of view. If one can improve Mirror theory in this direction, many practical constructions based on a tweakable block cipher could be proposed. For example, one would be able to construct CENC-like encryption modes [17] of stronger provable security.

2 Preliminaries

Notation. Throughout this work, we fix positive integers n, t, and q. We denote 0^n (i.e., n-bit string of all zeros) by $\mathbf{0}$. For integers a and b such that $0 \leq a < b$, we write $[a,b] \stackrel{\text{def}}{=} \{a, \ldots, b\}$ and $[b] \stackrel{\text{def}}{=} \{1, \ldots, b\}$. Given a non-empty set $\mathcal{X}$, $x \leftarrow_{\$} \mathcal{X}$ denotes that x is chosen uniformly at random from $\mathcal{X}$. The set of all functions from $\mathcal{X}$ to $\mathcal{Y}$ is denoted $\mathsf{Func}(\mathcal{X}, \mathcal{Y})$. We use an indicator function,

denoted $\mathbb{1}$, such that for a statement E, $\mathbb{1}(E) = 1$ if a statement E is true, and $\mathbb{1}(E) = 0$ otherwise. When two sets $\mathcal{X}$ and $\mathcal{Y}$ are disjoint, their (disjoint) union is denoted $\mathcal{X} \sqcup \mathcal{Y}$.

Tweakable Block Cipher. A *tweakable block cipher* (TBC) is a keyed function $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{X} \to \mathcal{X}$, where $\mathcal{K}$ is the key space, $\mathcal{T} = \{0,1\}^t$ is the tweak space, and $\mathcal{X} = \{0,1\}^n$ is the message space, such that for any $(K, T) \in \mathcal{K} \times \mathcal{T}$, $\widetilde{E}(K, T, \cdot)$ is a permutation over $\mathcal{X}$.

A *tweakable permutation* is the mapping $\widetilde{\mathsf{P}} : \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ such that $\widetilde{\mathsf{P}}(T, \cdot)$ is a permutation of $\mathcal{X}$ for any tweak $T \in \mathcal{T}$. When a tweakable permutation is chosen uniformly at random from the set of all possible tweakable permutations, such an ideal object is called a *tweakable uniform random permutation* (TURP). A secure tweakable block cipher should behave like a tweakable uniform random permutation with the same message and tweak spaces (when the key is chosen uniformly at random from the key space and kept secret), and hence it is viewed as a *tweakable pseudorandom permutation* (TPRP).

Pseudorandom Function. Let $\mathsf{C} : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ be a keyed function with key space $\mathcal{K}$, domain $\mathcal{X}$, and range $\mathcal{Y}$. We will consider an information theoretic distinguisher $\mathcal{D}$ that makes oracle queries to C, and returns a single bit. The advantage of $\mathcal{D}$ in breaking the PRF-security of C, i.e., in distinguishing C from a uniformly chosen function $\mathsf{F} \leftarrow_{\$} \mathsf{Func}(\mathcal{X}, \mathcal{Y})$, is defined as

$$\mathbf{Adv}^{\mathsf{prf}}_{\mathsf{C}}(\mathcal{D}) = \left| \Pr\left[K \leftarrow_{\$} \mathcal{K} : \mathcal{D}^{\mathsf{C}(K,\cdot)} = 1\right] - \Pr\left[\mathsf{F} \leftarrow_{\$} \mathsf{Func}(\mathcal{X}, \mathcal{Y}) : \mathcal{D}^{\mathsf{F}(\cdot)} = 1\right]\right|.$$

We define $\mathbf{Adv}^{\mathsf{prf}}_{\mathsf{C}}(q)$ as the maximum of $\mathbf{Adv}^{\mathsf{prf}}_{\mathsf{C}}(\mathcal{D})$ over all the distinguishers against C making at most q queries.

H-coefficient Technique. Consider a PRF construction $\mathsf{C}[\widetilde{\mathsf{P}}, \widetilde{\mathsf{Q}}] : \mathcal{X} \to \mathcal{Y}$ based on two TURPs $\widetilde{\mathsf{P}}$ and $\widetilde{\mathsf{Q}}$. In this case, $\widetilde{\mathsf{P}}$ and $\widetilde{\mathsf{Q}}$ can be viewed as keys. Suppose that an information-theoretic distinguisher $\mathcal{D}$ adaptively makes q queries to the construction oracle, which is either $\mathsf{C}[\widetilde{\mathsf{P}}, \widetilde{\mathsf{Q}}]$ (in the real world) or a truly random function F (in the ideal world), recording all the queries $(X_i, Y_i)_{1 \le i \le q}$. So according to the instantiation, it would imply either $\mathsf{C}[\widetilde{\mathsf{P}}, \widetilde{\mathsf{Q}}](X_i) = Y_i$ or $\mathsf{F}(X_i) = Y_i$. We will call

$$\tau = ((X_1, Y_1), \ldots, (X_q, Y_q))$$

the *transcript* of the attack; it contains all the information that $\mathcal{D}$ has obtained at the end of the attack. When we consider an information theoretic distinguisher, we can assume that the distinguisher is deterministic without making any redundant query.

Fix a transcript $\tau = (X_i, Y_i)_{1 \le i \le q}$. If there exists a function $\mathsf{F} \in \mathsf{Func}(\mathcal{X}, \mathcal{Y})$ such that $\mathsf{F}(X_i) = Y_i$ for every $i = 1, \ldots, q$, then we will call the transcript τ *attainable*. We denote Γ the set of attainable transcripts. We also denote T_{re} (resp. T_{id}) the probability distribution of the transcript τ induced by the real world (resp. the ideal world). By extension, we use the same notation to denote a

random variable distributed according to each distribution. Without considering "bad events", the coefficient-H technique is summarized as follows.

Lemma 1. *Let $\varepsilon > 0$. Suppose that*

$$\frac{\Pr\left[\mathsf{T}_{\mathrm{re}} = \tau\right]}{\Pr\left[\mathsf{T}_{\mathrm{id}} = \tau\right]} \geq 1 - \varepsilon$$

for any $\tau \in \Gamma$. Then one has

$$\mathbf{Adv}^{\mathsf{prf}}_{\mathsf{C}}(q) \leq \varepsilon.$$

Useful Lemma. Dutta et al. [11] proved the following combinatorial lemma. This lemma will also be used in our extended Mirror theory.

Lemma 2. *Let m be a positive integer, and let $(D_{\alpha,\beta})_{\alpha,\beta}$ be a two-dimensional sequence of non-negative numbers, where $1 \leq \alpha \leq m$ and $\beta \leq \alpha - 1$. Suppose that $D_{\alpha,\beta} = 0$ if $\beta \leq 0$, and if $2 \leq \alpha \leq m$ and $\beta \leq \alpha - 3$, then the following recurrence relation holds.*

$$D_{\alpha,\beta} \leq D_{\alpha-1,\beta-1} + 2A \cdot D_{\alpha-1,\beta} + A^2 \cdot D_{\alpha-1,\beta+1} + \frac{C}{(2^n - 2A)^{m-\alpha+\beta}}$$

for some positive constants A and C such that $A < 2^{n-1}$. Then, for any integer r such that $1 \leq r \leq \frac{\alpha}{2} - 1$, one has

$$D_{\alpha,1} \leq \sum_{i=r}^{2r} \binom{2r}{i} A^i D_{\alpha-r,1-r+i} + \sum_{j=0}^{r-1} \sum_{i=j}^{2j} \binom{2j}{i} \frac{A^i C}{(2^n - 2A)^{m-\alpha+1+i}}. \quad (1)$$

Lemma 2 is proved by mathematical induction on r. Its full proof is given in the Supplementary Material.

3 Mirror Theory for $\xi_{max} = 2$ with Relaxed Constraints

For a fixed positive integer q, let

$$\mathcal{V}_P \stackrel{\text{def}}{=} \{P_1, \ldots, P_q\},$$
$$\mathcal{V}_Q \stackrel{\text{def}}{=} \{Q_1, \ldots, Q_q\}$$

be sets of *unknowns* such that $P_i, Q_i \in \{0,1\}^n$ for $i \in [q]$. For a sequence of constants $(Z_1, \ldots, Z_q) \in (\{0,1\}^n)^q$, consider a system of equations

$$\Gamma : \begin{cases} P_1 \oplus Q_1 = Z_1, \\ P_2 \oplus Q_2 = Z_2, \\ \qquad \vdots \\ P_q \oplus Q_q = Z_q. \end{cases}$$

We will fix two partitions of $[q]$, namely,

$$\mathbb{P} = \left\{\mathcal{P}^{(1)}, \ldots, \mathcal{P}^{(a)}\right\},$$
$$\mathbb{Q} = \left\{\mathcal{Q}^{(1)}, \ldots, \mathcal{Q}^{(b)}\right\}$$

for some positive integers a and b, where

$$[q] = \mathcal{P}^{(1)} \sqcup \cdots \sqcup \mathcal{P}^{(a)} = \mathcal{Q}^{(1)} \sqcup \cdots \sqcup \mathcal{Q}^{(b)}.$$

Let

$$A \stackrel{\text{def}}{=} \max_{i\in[a], j\in[b]} \left\{\left|\mathcal{P}^{(i)}\right|, \left|\mathcal{Q}^{(j)}\right|\right\}$$

denote the size of the largest block in the two partitions. Throughout this section, we will assume

$$A \leq \frac{2^n}{13}.$$

We will write $i \overset{P}{\sim} j$ (resp. $i \overset{Q}{\sim} j$) if there exists k such that i, $j \in \mathcal{P}^{(k)}$ (resp. i, $j \in \mathcal{Q}^{(k)}$). With respect to these relations, we will put additional constraints on Γ as follows.

1. If $i \overset{P}{\sim} j$, then $P_i \neq P_j$.
2. If $i \overset{Q}{\sim} j$, then $Q_i \neq Q_j$.

The goal of our Mirror theory is to sharply lower bound the number of solutions to Γ, denoted $h(\Gamma, \overset{P}{\sim}, \overset{Q}{\sim})$, subject to the above constraints. In order to state the main result of our Mirror theory, we need to define sets

$$\mathcal{P}_i \stackrel{\text{def}}{=} \left\{j \in [i-1] \,\middle|\, j \overset{P}{\sim} i\right\}, \ \mathcal{Q}_i \stackrel{\text{def}}{=} \left\{j \in [i-1] \,\middle|\, j \overset{Q}{\sim} i\right\}. \tag{2}$$

for $i \in [q]$. We note that $\mathcal{P}_i$ (resp. $\mathcal{Q}_i$) is a subset of the block containing i in partition $\mathbb{P}$ (resp. $\mathbb{Q}$). If i is the smallest element in the block, then $\mathcal{P}_i$ or $\mathcal{Q}_i$ is an empty set.

Theorem 1. *One has*

$$h(\Gamma, \overset{P}{\sim}, \overset{Q}{\sim}) \geq \left(1 - \sum_{i=1}^{q}\left(\frac{2\left|\mathcal{P}_i \cap \mathcal{Q}_i\right|}{2^{2n}} + \frac{20\left|\mathcal{P}_i\right|\left|\mathcal{Q}_i\right|}{2^{3n}}\right) - \frac{6(n+1)^3}{2^{2n}}\right)$$
$$\times \prod_{i=1}^{q}\left(\frac{(2^n - |\mathcal{P}_i|)(2^n - |\mathcal{Q}_i|)}{2^n}\right).$$

The proof of Theorem 1 will be given in the next section. Let

$$B \stackrel{\text{def}}{=} \max_{i\in[a], j\in[b]} \left\{\left|\mathcal{P}^{(i)} \cap \mathcal{Q}^{(j)}\right|\right\}.$$

Then we have the following lemma.

Lemma 3. *One has*

$$\sum_{i=1}^{q} |\mathcal{P}_i| \, |\mathcal{Q}_i| \le \min\left\{A^2 q, Bq^2\right\}.$$

Proof. Since $\mathcal{P}_i$ (resp. $\mathcal{Q}_i$) is a subset of a single block in $\mathbb{P}$ (resp. $\mathbb{Q}$), we have

$$\sum_{i=1}^{q} |\mathcal{P}_i| \, |\mathcal{Q}_i| \le \sum_{i=1}^{q} A^2 = A^2 q. \tag{3}$$

For $k \in [a]$, let $U_k = \left|\mathcal{P}^{(k)} \cap [q-1]\right|$, and for $l \in [b]$, let $V_l = \left|\mathcal{Q}^{(l)} \cap [q-1]\right|$. Then, we see that

$$\sum_{k\in[a]} U_k = \sum_{l\in[b]} V_l = q - 1.$$

For $i \in [q]$, there exists a unique pair (k, l) such that $i \in \mathcal{P}^{(k)} \cap \mathcal{Q}^{(l)}$, in which case $|\mathcal{P}_i| \le U_k$ and $|\mathcal{Q}_i| \le V_l$. On the other hand, for $(k, l) \in [a] \times [b]$, there are at most B indices i such that $i \in \mathcal{P}^{(k)} \cap \mathcal{Q}^{(l)}$. Therefore, we have

$$\sum_{i=1}^{q} |\mathcal{P}_i| \, |\mathcal{Q}_i| \le \sum_{(k,l)\in[a]\times[b]} (BU_k V_l) = B \sum_{k\in[a]} U_k \sum_{l\in[b]} V_l = B(q-1)^2. \tag{4}$$

By (3) and (4), the proof is complete. □

By Lemma 3 and since $|\mathcal{P}_i \cap \mathcal{Q}_i| \le B-1$ for every $i \in [q]$, Theorem 1 is simplified as follows.

Corollary 1. *One has*

$$h(\Gamma, \overset{P}{\sim}, \overset{Q}{\sim}) \ge \left(1 - \frac{2(B-1)q + 6(n+1)^3}{2^{2n}} - \frac{20\min\left\{A^2 q, Bq^2\right\}}{2^{3n}}\right) \times \prod_{i=1}^{q} \left(\frac{(2^n - |\mathcal{P}_i|)(2^n - |\mathcal{Q}_i|)}{2^n}\right).$$

3.1 Proof of Theorem 1

Graph Representation, Definitions and Notations. Let $\alpha \in [q]$. For a set of α indices $\mathcal{I} = \{i_1, \ldots, i_\alpha\} \subset [q]$, we define

$$\begin{aligned}
\mathcal{V}[\mathcal{I}] &\overset{\text{def}}{=} \{P_{i_1}, Q_{i_1} \ldots, P_{i_\alpha}, Q_{i_\alpha}\}, \\
\mathcal{E}[\mathcal{I}] &\overset{\text{def}}{=} \{(P_{i_1}, Q_{i_1}, Z_{i_1}), \ldots, (P_{i_\alpha}, Q_{i_\alpha}, Z_{i_\alpha})\}, \\
\mathcal{G}[\mathcal{I}] &\overset{\text{def}}{=} (\mathcal{V}[\mathcal{I}], \mathcal{E}[\mathcal{I}]),
\end{aligned}$$

where $(P, Q, Z) \in \mathcal{E}[\mathcal{I}]$ represents an edge connecting P and Q with weight Z. When $\mathcal{I} = [\alpha]$, we will simply write $\mathcal{G}_\alpha$ to denote $\mathcal{G}[\mathcal{I}]$. By definition, $\mathcal{G}_0 = \emptyset$. We will identify $\mathcal{G}[\mathcal{I}]$ with a system of equations $P_i \oplus Q_i = Z_i$ for $i \in \mathcal{I}$. So $\mathcal{G}_q$ becomes Γ.

For a set of edges $\mathcal{F}$ such that every edge of $\mathcal{F}$ connects vertices of $\mathcal{G}[\mathcal{I}]$, we will write $\mathcal{G}[\mathcal{I}] \cup \mathcal{F}$ to denote $(\mathcal{V}[\mathcal{I}], \mathcal{E}[\mathcal{I}] \cup \mathcal{F})$. The number of solutions to $\mathcal{G}[\mathcal{I}] \cup \mathcal{F}$ subject to relations $\overset{P}{\sim}$ and $\overset{Q}{\sim}$ will be denoted $h(\mathcal{G}[\mathcal{I}] \cup \mathcal{F})$. By definition, $h(\mathcal{G}_0) = 1$. When $h(\mathcal{G}[\mathcal{I}] \cup \mathcal{F}) > 0$, we say that $\mathcal{G}[\mathcal{I}] \cup \mathcal{F}$ is *valid*. Note that $\mathcal{G}_q$ (with $\mathcal{I} = [q]$ and $\mathcal{F} = \emptyset$) is valid if $A \leq 2^{n-1}$.

Let l be a positive integer. For a trail of length l connecting two vertices V_0 and V_1, say

$$T(V_0, V_l) : ((V_0, V_1, E_1), \ldots, (V_{l-1}, V_l, E_l))$$

in $\mathcal{G}[\mathcal{I}] \cup \mathcal{F}$, the *weight* of $T(V_0, V_l)$ is defined as

$$w(T(V_0, V_l)) \stackrel{\text{def}}{=} E_1 \oplus E_2 \oplus \cdots \oplus E_l.$$

In order for $\mathcal{G}[\mathcal{I}] \cup \mathcal{F}$ to be valid, the following conditions should be satisfied.

1. For any distinct i and j such that $i \overset{P}{\sim} j$, and for any trail $T(P_i, P_j)$ in $\mathcal{G}[\mathcal{I}] \cup \mathcal{F}$, $w(T(P_i, P_j)) \neq \mathbf{0}$.
2. For any distinct i and j such that $i \overset{Q}{\sim} j$, and for any trail $T(Q_i, Q_j)$ in $\mathcal{G}[\mathcal{I}] \cup \mathcal{F}$, $w(T(Q_i, Q_j)) \neq \mathbf{0}$.

For $\alpha \in [2, q]$, let $\mathcal{I} \subset [q]$ be an index set such that $|\mathcal{I}| = \alpha$. For $\beta \in [\alpha - 1]$, let

$$\mathcal{J} = (j_1, \ldots, j_{\beta+1}) \in \mathcal{I}^{\beta+1}$$

be a sequence of *distinct* indices in $\mathcal{I}$, and let

$$\mathcal{L} = (L_1, \ldots, L_\beta) \in (\{0,1\}^n)^\beta$$

be a sequence of n-bit weights. Then we define an edge set

$$\mathcal{F}[\mathcal{J}, \mathcal{L}] \stackrel{\text{def}}{=} \left\{(P_{j_1}, Q_{j_2}, L_1), \ldots, (P_{j_\beta}, Q_{j_{\beta+1}}, L_\beta)\right\}$$

and a weighted graph

$$\mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}] \stackrel{\text{def}}{=} \mathcal{G}[\mathcal{I}] \cup \mathcal{F}[\mathcal{J}, \mathcal{L}].$$

We also define subgraphs of $\mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}]$ as follows.

$$\mathcal{G}^{-+}[\mathcal{I}, \mathcal{J}, \mathcal{L}] \stackrel{\text{def}}{=} \mathcal{G}[\mathcal{I}] \cup (\mathcal{F}[\mathcal{J}, \mathcal{L}] \setminus \{(P_{j_1}, Q_{j_2}, L_1)\}),$$
$$\mathcal{G}^{+-}[\mathcal{I}, \mathcal{J}, \mathcal{L}] \stackrel{\text{def}}{=} \mathcal{G}[\mathcal{I} \setminus \{j_{\beta+1}\}] \cup (\mathcal{F}[\mathcal{J}, \mathcal{L}] \setminus \left\{(P_{j_\beta}, Q_{j_{\beta+1}}, L_\beta)\right\}),$$
$$\mathcal{G}^{--}[\mathcal{I}, \mathcal{J}, \mathcal{L}] \stackrel{\text{def}}{=} \mathcal{G}[\mathcal{I} \setminus \{j_{\beta+1}\}] \cup (\mathcal{F}[\mathcal{J}, \mathcal{L}] \setminus \{(P_{j_1}, Q_{j_2}, L_1), (P_{j_\beta}, Q_{j_{\beta+1}}, L_\beta)\}).$$

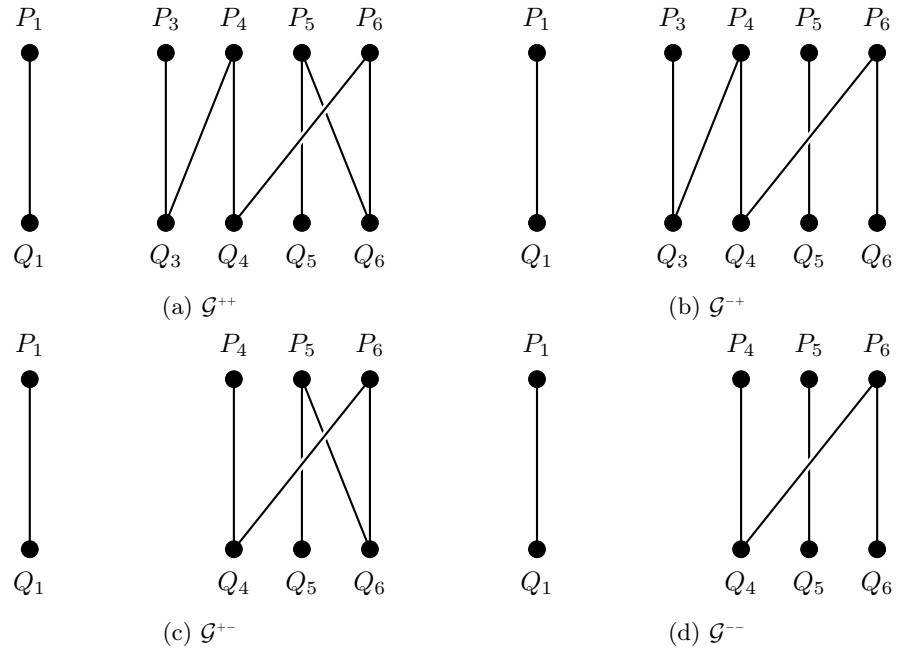


Fig. 4: An example of $\mathcal{G}^x$ for $x \in \{++, -+, +-, --\}$, where $q = 6$, $\mathcal{I} = \{1, 3, 4, 5, 6\}$ and $\mathcal{J} = (5, 6, 4, 3)$.

When $\mathcal{I}$, $\mathcal{J}$ and $\mathcal{L}$ are clear from the context, we will simply write

$$\mathcal{G}^{++} = \mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}], \quad \mathcal{G}^{-+} = \mathcal{G}^{-+}[\mathcal{I}, \mathcal{J}, \mathcal{L}], \quad \mathcal{G}^{+-} = \mathcal{G}^{+-}[\mathcal{I}, \mathcal{J}, \mathcal{L}], \quad \mathcal{G}^{--} = \mathcal{G}^{--}[\mathcal{I}, \mathcal{J}, \mathcal{L}].$$

Note that $\mathcal{G}^{-+}$ is obtained from $\mathcal{G}^{++}$ by removing one edge, namely (P_{j_1}, Q_{j_2}, L_1), while $\mathcal{G}^{+-}$ is obtained from $\mathcal{G}^{++}$ by removing two edges that are incident with $Q_{j_{\beta+1}}$. See Figure 4 for an example of $\mathcal{G}^{++}$, $\mathcal{G}^{-+}$, $\mathcal{G}^{+-}$ and $\mathcal{G}^{--}$. When $\beta = 0$, we have $\mathcal{L} = \emptyset$ and $\mathcal{F}[\mathcal{J}, \mathcal{L}] = \emptyset$ by definition, in which case, $\mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}] = \mathcal{G}[\mathcal{I}]$. We note that if $\mathcal{G}^{++}$ is valid for given $\mathcal{I}$, $\mathcal{J}$, and $\mathcal{L}$, then $\mathcal{G}^{-+}$, $\mathcal{G}^{+-}$ and $\mathcal{G}^{--}$ are also valid.

For an index set $\mathcal{I} \subset [q]$ and $i \in [q]$, we define the following sets.

$$\begin{aligned}
\mathcal{P}_i[\mathcal{I}] &\stackrel{\text{def}}{=} \left\{ j \in \mathcal{I} \,\middle|\, j \overset{P}{\sim} i \text{ and } j \neq i \right\}, \\
\mathcal{Q}_i[\mathcal{I}] &\stackrel{\text{def}}{=} \left\{ j \in \mathcal{I} \,\middle|\, j \overset{Q}{\sim} i \text{ and } j \neq i \right\}, \\
\mathcal{R}_i[\mathcal{I}] &\stackrel{\text{def}}{=} \left\{ j \in \mathcal{I} \,\middle|\, j \overset{P}{\sim} i, j \overset{Q}{\sim} i, Z_j = Z_i \text{ and } j \neq i \right\}.
\end{aligned}$$

When $\mathcal{I} = [\alpha]$ for some $\alpha \in [q]$, we will simply write $\mathcal{P}_\alpha$, $\mathcal{Q}_\alpha$, and $\mathcal{R}_\alpha$ to denote $\mathcal{P}_\alpha[\mathcal{I}]$, $\mathcal{Q}_\alpha[\mathcal{I}]$, and $\mathcal{R}_\alpha[\mathcal{I}]$, respectively.[1] Note that $\mathcal{R}_\alpha \subset \mathcal{P}_\alpha \cap \mathcal{Q}_\alpha$ for any $\alpha \in [q]$.

[1] This notation is consistent with the previous definition of $\mathcal{P}_i$ and $\mathcal{Q}_i$ in (2).

ORANGE EQUATION. We can recursively compute $h(\mathcal{G}_\alpha)$ using the following lemma.

Lemma 4. *For any positive integer $\alpha \in [q]$, one has*

$$h(\mathcal{G}_\alpha) = (2^n - |\mathcal{P}_\alpha| - |\mathcal{Q}_\alpha| + |\mathcal{R}_\alpha|)h(\mathcal{G}_{\alpha-1}) + \sum_{E \in \mathbb{L}[\mathcal{G}_\alpha]} h(\mathcal{G}_{\alpha-1} \cup \{E\}) \quad (5)$$

where

$$\mathbb{L}[\mathcal{G}_\alpha] = \{(P_i, Q_j, Z_\alpha) \,|\, i \in \mathcal{P}_\alpha,\ j \in \mathcal{Q}_\alpha,\ i \neq j,\ h(\mathcal{G}_{\alpha-1} \cup \{(P_i, Q_j, Z_\alpha)\}) > 0\}.$$

Recurrence relation (5) is called the *Orange equation* in Mirror theory. The proof of Lemma 4 is given in the Supplementary Material. The Orange equation can be easily generalized as follows: to any set of indices $\mathcal{I}$ such that $|\mathcal{I}| = \alpha$ and $j \in \mathcal{I}$,

$$h(\mathcal{G}^{++}) = (2^n - |\mathcal{P}_j[\mathcal{I}]| - |\mathcal{Q}_j[\mathcal{I}]| + |\mathcal{R}_j[\mathcal{I}]|)h(\mathcal{G}^{+-}) + \sum_{E \in \mathbb{L}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E\})$$

where $\mathcal{G}^{++} = \mathcal{G}[\mathcal{I}, \mathcal{J}, \emptyset] (= \mathcal{G}[\mathcal{I}])$ with $\mathcal{J} = (j)$ and

$$\mathbb{L}[\mathcal{G}^{++}] = \{(P_k, Q_l, Z_j) \mid k \in \mathcal{P}_j[\mathcal{I}],\ l \in \mathcal{Q}_j[\mathcal{I}],\ k \neq l\}.$$

Example 1. For $n = 2$ and $q = 3$, let $\mathcal{P}^{(1)} = \{1, 3\}$, $\mathcal{P}^{(2)} = \{2\}$, $\mathcal{Q}^{(1)} = \{1\}$, $\mathcal{Q}^{(2)} = \{2, 3\}$, $Z_1 = 00$, $Z_2 = 01$ and $Z_3 = 10$. For $\alpha = 3$, we see that

$$\mathcal{P}_3 = \{1\}, \mathcal{Q}_3 = \{2\}, \mathcal{R}_3 = \emptyset.$$

Hence, it follows that

$$\mathbb{L}[\mathcal{G}_3] = \{(P_1, Q_2, 10)\},$$

and therefore,

$$\begin{aligned} h(\mathcal{G}_3) &= (4 - 1 - 1 + 0)h(\mathcal{G}_2) + h(\mathcal{G}_2 \cup \{(P_1, Q_2, 10)\}) \\ &= 2 \cdot h(\mathcal{G}_2) + h(\mathcal{G}_2 \cup \{(P_1, Q_2, 10)\}). \end{aligned} \quad (6)$$

Graphs $\mathcal{G}_3$ and $\mathcal{G}_2 \cup \{(P_1, Q_2, 10)\}$ are pictorially represented in Figure 5. Since $\mathcal{G}_2$ consists of two independent equations, namely, $P_1 \oplus Q_1 = 00$ and $P_2 \oplus Q_2 = 01$, we have

$$h(\mathcal{G}_2) = (2^n)^2 = 16.$$

On the other hand, $\mathcal{G}_2 \cup \{(P_1, Q_2, 10)\}$ consists of a single connected component, and assignment of an arbitrary value to a fixed vertex determines all the other unknowns. So, we have

$$h(\mathcal{G}_2 \cup \{(P_1, Q_2, 10)\}) = 2^n = 4.$$

By (6), we have $h(\mathcal{G}_3) = 36$.

(a) $\mathcal{G}_3$ (b) $\mathcal{G}_2 \cup \{(P_1, Q_2, 10)\}$

Fig. 5: Graphs $\mathcal{G}_3$ and $\mathcal{G}_2 \cup \{(P_1, Q_2, 10)\}$ in Example 1. Vertices in the same block are represented by the same shape.

PURPLE EQUATION. In order to use Lemma 4, we need to sharply lower bound $h(\mathcal{G}_{\alpha-1} \cup \mathcal{E})$ for a certain set of edges $\mathcal{E}$. We can recursively estimate $h(\mathcal{G}_{\alpha-1} \cup \mathcal{E})$ using graphs with a smaller number of connected components.

Lemma 5. *Fix integers α and β such that $1 \leq \beta < \alpha \leq q$, an index set $\mathcal{I} \subset [q]$ such that $|\mathcal{I}| = \alpha$, a sequence of distinct indices $\mathcal{J} = (j_1, \ldots, j_{\beta+1}) \in \mathcal{I}^{\beta+1}$, and a sequence of weights $\mathcal{L} = (L_1, \ldots, L_\beta) \in (\{0,1\}^n)^\beta$. If $\mathcal{G}^{++} (= \mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}])$ is valid, then one has*

$$h(\mathcal{G}^{++}) = h(\mathcal{G}^{+-}) - \sum_{E \in \mathbb{M}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E\}) + \sum_{\{E,E'\} \in \mathbb{N}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E, E'\}). \quad (7)$$

where

$$\begin{aligned}
\mathbb{M}[\mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}]] = \{E = (P_{j_\beta}, Q_k, L_\beta \oplus Z_k \oplus Z_{j_{\beta+1}}) \mid \\
k \in \mathcal{P}_{j_{\beta+1}}[\mathcal{I} \setminus \mathcal{J}],\ h(\mathcal{G}^{+-} \cup \{E\}) > 0\} \\
\cup \{E = (P_{j_\beta}, Q_k, L_\beta) \mid k \in \mathcal{Q}_{j_{\beta+1}}[\mathcal{I} \setminus \mathcal{J}],\ h(\mathcal{G}^{+-} \cup \{E\}) > 0\}, \\
\mathbb{N}[\mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}]] = \{\{E, E'\} = \{(P_{j_\beta}, Q_k, L_\beta \oplus Z_k \oplus Z_{j_{\beta+1}}), (P_k, Q_l, Z_{j_{\beta+1}})\} \mid \\
k \in \mathcal{P}_{j_{\beta+1}}[\mathcal{I} \setminus \mathcal{J}], l \in \mathcal{Q}_{j_{\beta+1}}[\mathcal{I} \setminus \mathcal{J}], k \neq l, h(\mathcal{G}^{+-} \cup \{E, E'\}) > 0\}.
\end{aligned}$$

Recurrence relation (7) is called the *Purple equation*. The proof of Lemma 5 is given in the Supplementary Material.

Example 2. For $n = 2$ and $q = 6$, let

$$\begin{aligned}
&\mathcal{P}^{(1)} = \{1, 3, 4\},\ \mathcal{P}^{(2)} = \{2\},\ \mathcal{P}^{(3)} = \{5, 6\}, \\
&\mathcal{Q}^{(1)} = \{1, 5, 6\},\ \mathcal{Q}^{(2)} = \{2, 3, 4\}, \\
&Z_1 = 00,\ Z_2 = 01,\ Z_3 = 10,\ Z_4 = 10,\ Z_5 = 11,\ Z_6 = 11.
\end{aligned}$$

For $\alpha = m = 6$ and $\beta = 2$, let

$$\mathcal{I} = \{1, 2, 3, 4, 5, 6\},$$

$$\mathcal{J} = (5, 6, 4) \text{ (with } j_1 = 5,\ j_2 = 6,\ j_3 = 4),$$
$$\mathcal{L} = (10, 01).$$

One can see that $\mathcal{G}^{++}$ is valid and,

$$\mathcal{F}[\mathcal{J}, \mathcal{L}] = \{(P_5, Q_6, 10), (P_6, Q_4, 01)\},$$
$$\mathcal{G}^{+-} = \mathcal{G}[\{1, 2, 3, 5, 6\}] \cup \{(P_5, Q_6, 10)\},$$
$$\mathcal{P}_{j_{\beta+1}}[\mathcal{I} \setminus \mathcal{J}] = \mathcal{P}_4[\{1, 2, 3\}] = \{1, 3\},$$
$$\mathcal{Q}_{j_{\beta+1}}[\mathcal{I} \setminus \mathcal{J}] = \mathcal{Q}_4[\{1, 2, 3\}] = \{2, 3\}.$$

Then we have

$$\mathbb{M}[\mathcal{G}^{++}] = \{(P_6, Q_1, 11), (P_6, Q_2, 01), (P_6, Q_3, 01)\}, \quad \mathbb{N}[\mathcal{G}^{++}] = \{\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3\},$$

where

$$\mathcal{E}_1 = \{(P_6, Q_1, 11), (P_1, Q_2, 10)\},$$
$$\mathcal{E}_2 = \{(P_6, Q_1, 11), (P_1, Q_3, 10)\},$$
$$\mathcal{E}_3 = \{(P_6, Q_3, 01), (P_3, Q_2, 10)\}.$$

Note that $\mathcal{G}^{+-} \cup \{(P_6, Q_1, 11)\}$ is invalid since it implies $Q_1 \oplus Q_6 = 0$. Since $\mathcal{G}^{+-} \cup \mathcal{E}_1$ and $\mathcal{G}^{+-} \cup \mathcal{E}_2$ are also invalid, we have

$$h(\mathcal{G}^{++}) = h(\mathcal{G}^{+-}) - h(\mathcal{G}^{+-} \cup \{(P_6, Q_2, 01)\}) \\ - h(\mathcal{G}^{+-} \cup \{(P_6, Q_3, 01)\}) + h(\mathcal{G}^{+-} \cup \{(P_6, Q_3, 01), (P_3, Q_2, 10)\}).$$

See Figure 6 for a pictorial representation of this example.

Size Lemma. Our next step is to estimate the size of sets $\mathbb{L}[\mathcal{G}_\alpha]$, $\mathbb{M}[\mathcal{G}^{++}]$ and $\mathbb{N}[\mathcal{G}^{++}]$ appearing in Lemmas 4 and 5. In order to state Lemma 6, we need to reorder the indices of $\mathcal{G}_q$; any reordering of the indices does not affect the number of solutions to $\mathcal{G}_q$.

For $k = 1, \ldots, q$, there is a unique pair $(i_k, j_k) \in [a] \times [b]$ such that $k \in \mathcal{P}^{(i_k)} \cap \mathcal{Q}^{(j_k)}$. In this way, we can define an ordered multiset of q elements $\{(i_1, j_1, Z_1), \ldots, (i_q, j_q, Z_q)\}$. From this multiset, we choose as many different elements as possible, put them in a separate list, remove them from the multiset, and recursively perform the same procedure for the remaining elements. This reordering of triples obviously defines a reordering of the edges (indices) since we can associate each triple with a unique $k \in [q]$. With this reordering of the indices, we have

$$\max_{\substack{i,j \in [\alpha], \\ Z \in \{0,1\}^n}} \{|\{k \in \mathcal{P}_i \cap \mathcal{Q}_j \mid Z_k = Z\}|\} \leq |\mathcal{R}_{\alpha+1}|\,. \tag{8}$$

Example 3. For $n = 1$ and $q = 6$, graph $\mathcal{G}_q$ and partitions $\mathbb{P}$ and $\mathbb{Q}$ are defined as follows.

$$\mathcal{P}^{(1)} = \{1, 2, 3, 4, 5\}\,,\ \mathcal{P}^{(2)} = \{6\}\,,$$

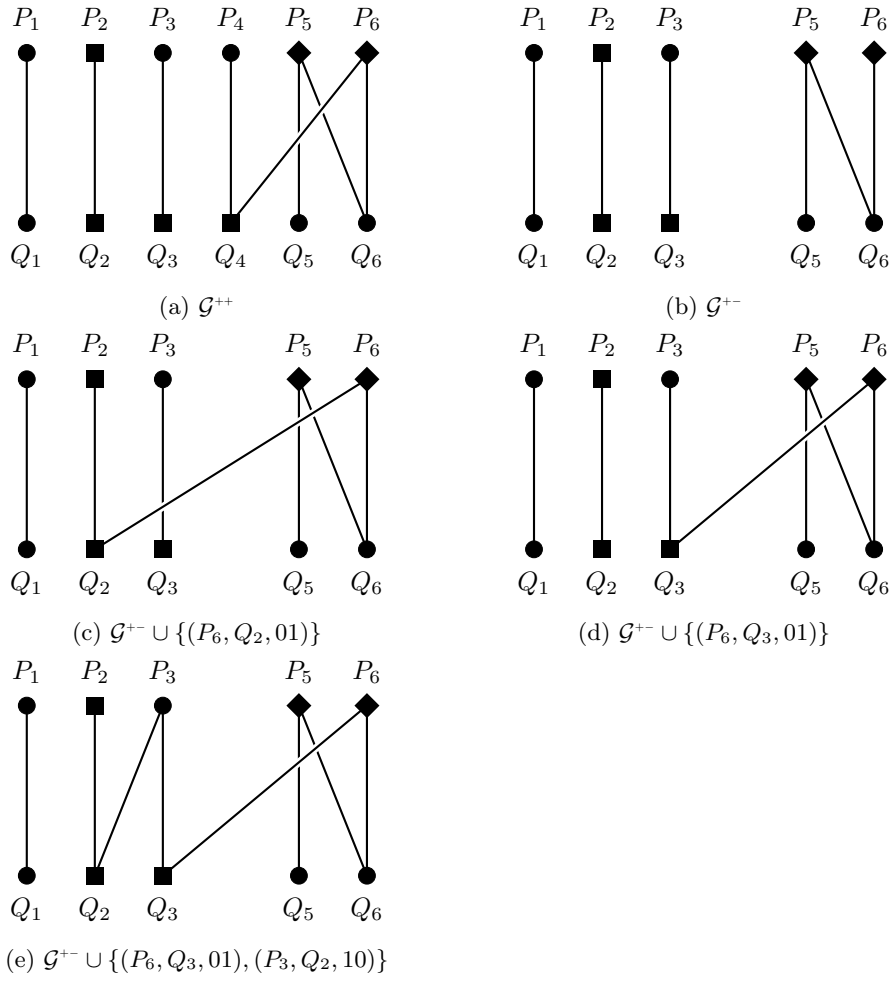


Fig. 6: Graphs appearing in Example 2. Vertices in the same block are represented by the same shape.

$$\mathcal{Q}^{(1)} = \{1,2,3,6\}\,,\ \mathcal{Q}^{(2)} = \{4,5\}\,,$$
$$Z_1 = 0,\ Z_2 = 0,\ Z_3 = 0,\ Z_4 = 0,\ Z_5 = 1,\ Z_6 = 0.$$

Then we can define an ordered multiset

$$\{(1,1,0),(1,1,0),(1,1,0),(1,2,0),(1,2,1),(2,1,0)\}\,,$$

where the k-th element is associated with index k for $k \in [6]$. By the procedure described above, we can reorder the elements of the multiset as follows.

$$\{(1,1,0),(1,2,0),(1,2,1),(2,1,0),(1,1,0),(1,1,0)\}$$

This reordering corresponds to a permutation π on the set of indices, where $\pi(1) = 1$, $\pi(2) = 5$, $\pi(3) = 6$, $\pi(4) = 2$, $\pi(5) = 3$, $\pi(6) = 4$ (though such a correspondence is not unique). With this permutation, we obtain the following partitions and sequence of weights.

$$\mathcal{P}^{(1)} = \{1,2,3,5,6\}\,,\ \mathcal{P}^{(2)} = \{4\}\,,$$
$$\mathcal{Q}^{(1)} = \{1,4,5,6\}\,,\ \mathcal{Q}^{(2)} = \{2,3\}\,,$$
$$Z_1 = 0,\ Z_2 = 0,\ Z_3 = 1,\ Z_4 = 0,\ Z_5 = 0,\ Z_6 = 0.$$

For the reordered graph, we have

$$\mathcal{R}_1 = \mathcal{R}_2 = \mathcal{R}_3 = \mathcal{R}_4 = \emptyset,\ \mathcal{R}_5 = \{1\},\ \mathcal{R}_6 = \{1,5\}.$$

Assuming (8), we can prove the following lemma.

Lemma 6. *Fix positive integers α, β and m such that $2 \le \beta < \alpha \le m \le q$. Then one has*

$$|\mathbb{L}[\mathcal{G}_\alpha]| = (|\mathcal{P}_\alpha| - |\mathcal{R}_\alpha|)(|\mathcal{Q}_\alpha| - |\mathcal{R}_\alpha|) - |\mathcal{P}_\alpha \cap \mathcal{Q}_\alpha| + |\mathcal{R}_\alpha|\,.$$

For an index set $\mathcal{I} \subset [m]$ such that $|\mathcal{I}| = \alpha$, a sequence of distinct indices $\mathcal{J} = (j_1, \ldots, j_{\beta+1}) \in \mathcal{I}^{\beta+1}$, and a sequence of weights $\mathcal{L} \in (\{0,1\}^n)^\beta$ such that $\mathcal{G}^{++}(= \mathcal{G}[\mathcal{I},\mathcal{J},\mathcal{L}])$ is valid, one has

$$|\mathbb{M}[\mathcal{G}^{-+}]| - 2(|\mathcal{R}_{m+1}| + 1) \le |\mathbb{M}[\mathcal{G}^{++}]| \le 2A,$$
$$|\mathbb{N}[\mathcal{G}^{-+}]| - 2A(|\mathcal{R}_{m+1}| + 1) \le |\mathbb{N}[\mathcal{G}^{++}]| \le A^2.$$

When $\beta = 1$, one has

$$|\mathcal{P}_{j_2}[\mathcal{I}]| + |\mathcal{Q}_{j_2}[\mathcal{I}]| - |\mathcal{R}_{j_2}[\mathcal{I}]| - 2(|\mathcal{R}_{m+1}| + 1) \le |\mathbb{M}[\mathcal{G}^{++}]| \le 2A,$$
$$|\mathbb{L}[\mathcal{G}^{-+}]| - 2A(|\mathcal{R}_{m+1}| + 1) \le |\mathbb{N}[\mathcal{G}^{++}]| \le A^2.$$

Lemma 6 is called the Size Lemma. Its proof is given in the Supplementary Material.

Adding a Single Edge to $\mathcal{G}_\alpha$. Fix a positive integer m such that $m \le q$. We will define a two-dimensional sequence $D^m_{\alpha,\beta}$, where $1 \le \alpha \le m$ and β is an integer, as follows.

– When $1 \leq \beta \leq \alpha - 1$,

$$D^m_{\alpha,\beta} = \max_{\mathcal{I},\mathcal{J},\mathcal{L}} \left\{ \left| \frac{h(\mathcal{G}^{-+}[\mathcal{I},\mathcal{J},\mathcal{L}])}{2^n} - h(\mathcal{G}[\mathcal{I},\mathcal{J},\mathcal{L}]) \right| \right\},$$

where the maximum is taken over all possible index sets $\mathcal{I} \subset [m]$ such that $|\mathcal{I}| = \alpha$, sequences of distinct indices $\mathcal{J} \in \mathcal{I}^{\beta+1}$, and sequences of weights $\mathcal{L} \in (\{0,1\}^n)^\beta$ such that $\mathcal{G}[\mathcal{I},\mathcal{J},\mathcal{L}]$ is valid.

– When $\beta \leq 0$,

$$D^m_{\alpha,\beta} = 0.$$

In order to upper bound $D^m_{\alpha,\beta}$, we begin with the following lemma.

Lemma 7. *For any $\mathcal{I} \subset [m]$, $\mathcal{J} \in \mathcal{I}^{\beta+1}$, $\mathcal{L} \in (\{0,1\}^n)^\beta$ such that $|\mathcal{I}| = \alpha$ and $\mathcal{G}[\mathcal{I},\mathcal{J},\mathcal{L}]$ is valid, one has*

$$h(\mathcal{G}[\mathcal{I},\mathcal{J},\mathcal{L}]) \leq \frac{h(\mathcal{G}_m)}{(2^n - 2A)^{m-\alpha+\beta}}.$$

The proof of Lemma 7 is given in the Supplementary Material. For $h(\mathcal{G}^{++})(= \mathcal{G}[\mathcal{I},\mathcal{J},\mathcal{L}])$,

$$\frac{h(\mathcal{G}^{-+})}{2^n} \leq \frac{h(\mathcal{G}_m)}{(2^n - 2A)^{m-\alpha+\beta-1} \cdot 2^n} \leq \frac{h(\mathcal{G}_m)}{(2^n - 2A)^{m-\alpha+\beta}}.$$

Therefore, we have

$$D^m_{\alpha,\beta} \leq \max\left\{ \frac{h(\mathcal{G}^{-+})}{2^n}, h(\mathcal{G}^{++}) \right\} \leq \frac{h(\mathcal{G}_m)}{(2^n - 2A)^{m-\alpha+\beta}}. \tag{9}$$

When $\beta = 1$, we have a sharper upper bound on $D^\alpha_{\alpha,1}$ as follows.

Lemma 8. *If $2n + 2 \leq m < q$, then one has*

$$D^m_{m,1} \leq \frac{(15\,|\mathcal{R}_{m+1}| + 17)h(\mathcal{G}_m)}{2^{2n}}.$$

The proof is given in Section 3.2. Note that $D^m_{m,1}$ compares the number of solutions between a graph $\mathcal{G}_m$ $(=\mathcal{G}^{-+}[\mathcal{I},\mathcal{J},\mathcal{L}])$ and the graph obtained by adding a single edge to $\mathcal{G}_m$, namely $\mathcal{G}[\mathcal{I},\mathcal{J},\mathcal{L}]$, and Lemma 8 upper bounds their difference.

Proof of Theorem 1. For $m \geq 0$, let

$$H_m = 2^{nm} h(\mathcal{G}_m),$$
$$J_m = \prod_{i=1}^{m} (2^n - |\mathcal{P}_i|)(2^n - |\mathcal{Q}_i|).$$

If $\frac{H_q}{J_q} \geq 1 - \varepsilon$ for some $\varepsilon \geq 0$, then we have

$$h(\mathcal{G}_q) = \frac{H_q}{J_q} \cdot \frac{\prod_{i=1}^{q} (2^n - |\mathcal{P}_i|)(2^n - |\mathcal{Q}_i|)}{2^{nq}}$$

$$\geq (1-\varepsilon)\cdot\prod_{i=1}^{q}\left(\frac{(2^n-|\mathcal{P}_i|)(2^n-|\mathcal{Q}_i|)}{2^n}\right). \tag{10}$$

On the other hand, by Lemma 4, for any $m \leq q-1$, we have

$$h(\mathcal{G}_{m+1}) = (2^n - |\mathcal{P}_{m+1}| - |\mathcal{Q}_{m+1}| + |\mathcal{R}_{m+1}|)h(\mathcal{G}_m) + \sum_{E\in\mathbb{L}[\mathcal{G}_{m+1}]} h(\mathcal{G}_m \cup \{E\}). \tag{11}$$

If $m \geq 2n+2$ and $(P_i, Q_j, Z_{m+1}) \in \mathbb{L}[\mathcal{G}_{m+1}]$, then we have

$$\left|\frac{h(\mathcal{G}_m)}{2^n} - h(\mathcal{G}_m \cup \{(P_i, Q_j, Z_{m+1})\})\right| \leq \frac{(15\,|\mathcal{R}_{m+1}|+17)h(\mathcal{G}_m)}{2^{2n}}$$

by Lemma 8. So we have

$$h(\mathcal{G}_m \cup \{(P_i, Q_j, Z_{m+1})\}) \geq \frac{h(\mathcal{G}_m)}{2^n}\left(1 - \frac{15\,|\mathcal{R}_{m+1}|+17}{2^n}\right). \tag{12}$$

In the following computation, we simply write $a = |\mathcal{P}_{m+1}|$, $b = |\mathcal{Q}_{m+1}|$, $c = |\mathcal{P}_{m+1} \cap \mathcal{Q}_{m+1}|$, and $d = |\mathcal{R}_{m+1}|$. Combining (11), (12) and Lemma 6, we have

$$\frac{h(\mathcal{G}_{m+1})}{h(\mathcal{G}_m)} \geq 2^n - a - b + d + \frac{(a-d)(b-d)-c+d}{2^n}\left(1 - \frac{15d+17}{2^n}\right).$$

Since $(a-d)(b-d)-c+d \leq ab$, $2^n - a - b - \frac{15ab}{2^n} \geq 0$ and $a, b \leq \frac{2^n}{13}$, we have

$$\begin{aligned}
\frac{H_{m+1}}{J_{m+1}} &\geq \frac{2^{2n} - (a+b-d)2^n + ((a-d)(b-d)-c+d)\left(1-\frac{15d+17}{2^n}\right)}{(2^n-a)(2^n-b)}\cdot\frac{H_m}{J_m} \\
&\geq \left(1 + \frac{d(2^n - a - b - \frac{15ab}{2^n}) - c + d^2 + d - \frac{17ab}{2^n}}{(2^n-a)(2^n-b)}\right)\frac{H_m}{J_m} \\
&\geq \left(1 - \frac{c + \frac{17ab}{2^n}}{(2^n-a)(2^n-b)}\right)\frac{H_m}{J_m} \\
&\geq \left(1 - \frac{2c}{2^{2n}} - \frac{20ab}{2^{3n}}\right)\frac{H_m}{J_m}.
\end{aligned}$$

Therefore we have

$$\begin{aligned}
\frac{H_q}{J_q} &\geq \prod_{i=2n+3}^{q}\left(1 - \frac{2\,|\mathcal{P}_i \cap \mathcal{Q}_i|}{2^{2n}} - \frac{20\,|\mathcal{P}_i|\,|\mathcal{Q}_i|}{2^{3n}}\right)\frac{H_{2n+2}}{J_{2n+2}} \\
&\geq \left(1 - \sum_{i=2n+3}^{q}\left(\frac{2\,|\mathcal{P}_i \cap \mathcal{Q}_i|}{2^{2n}} + \frac{20\,|\mathcal{P}_i|\,|\mathcal{Q}_i|}{2^{3n}}\right)\right)\frac{H_{2n+2}}{J_{2n+2}}.
\end{aligned} \tag{13}$$

If $m \leq 2n+1$, then we have

$$h(\mathcal{G}_{m+1}) \geq (2^n - |\mathcal{P}_{m+1}| - |\mathcal{Q}_{m+1}|)h(\mathcal{G}_m)$$

by Lemma 4. Then it follows that

$$\frac{H_{m+1}}{J_{m+1}} \geq \frac{2^n(2^n - |\mathcal{P}_{m+1}| - |\mathcal{Q}_{m+1}|)}{(2^n - |\mathcal{P}_{m+1}|)(2^n - |\mathcal{Q}_{m+1}|)} \cdot \frac{H_m}{J_m}$$
$$\geq \left(1 - \frac{|\mathcal{P}_{m+1}|\,|\mathcal{Q}_{m+1}|}{(2^n - |\mathcal{P}_{m+1}|)(2^n - |\mathcal{Q}_{m+1}|)}\right) \frac{H_m}{J_m}.$$

Since $|\mathcal{P}_{m+1}|, |\mathcal{Q}_{m+1}| \leq \min\{m, \frac{2^n}{13}\}$ and $H_1 = J_1 = 2^{2n}$, we have

$$\frac{H_{2n+2}}{J_{2n+2}} \geq \left(1 - 2\sum_{i=1}^{2n+1} \frac{i^2}{2^{2n}}\right) \frac{H_1}{J_1}$$
$$\geq 1 - \frac{(2n+1)(2n+2)(4n+3)}{3} \cdot \frac{1}{2^{2n}} \geq 1 - \frac{6(n+1)^3}{2^{2n}}. \qquad (14)$$

By combining (13) and (14), we have

$$\frac{H_q}{J_q} \geq \left(1 - \sum_{i=2n+3}^{q} \left(\frac{2\,|\mathcal{P}_i \cap \mathcal{Q}_i|}{2^{2n}} + \frac{20\,|\mathcal{P}_i|\,|\mathcal{Q}_i|}{2^{3n}}\right)\right)\left(1 - \frac{6(n+1)^3}{2^{2n}}\right)$$
$$\geq 1 - \sum_{i=1}^{q} \left(\frac{2\,|\mathcal{P}_i \cap \mathcal{Q}_i|}{2^{2n}} + \frac{20\,|\mathcal{P}_i|\,|\mathcal{Q}_i|}{2^{3n}}\right) - \frac{6(n+1)^3}{2^{2n}}.$$

Setting $\varepsilon = \sum_{i=1}^{q} \left(\frac{2|\mathcal{P}_i \cap \mathcal{Q}_i|}{2^{2n}} + \frac{20|\mathcal{P}_i||\mathcal{Q}_i|}{2^{3n}}\right) + \frac{6(n+1)^3}{2^{2n}}$ in (10), the proof is completed.

3.2 Proof of Lemma 8

We will prove that if $2 \leq \alpha \leq m$ and $\beta \leq \alpha - 3$, then

$$D^m_{\alpha,\beta} \leq D^m_{\alpha-1,\beta-1} + 2A \cdot D^m_{\alpha-1,\beta} + A^2 \cdot D^m_{\alpha-1,\beta+1} + \frac{C}{(2^n - 2A)^{m-\alpha+\beta}}, \qquad (15)$$

where

$$C \stackrel{\text{def}}{=} \frac{(3\,|\mathcal{R}_{m+1}| + 3)h(\mathcal{G}_m)}{2^n}.$$

The proof of (15) will be given at the end of this section. Then, by Lemma 2, we obtain an upper bound on $D^m_{\alpha,1}$ as follows.

$$D^m_{\alpha,1} \leq \sum_{i=n}^{2n} \binom{2n}{i} A^i D^m_{\alpha-n,1+i-n} + \sum_{j=0}^{n-1} \sum_{i=j}^{2j} \binom{2j}{i} \frac{A^i C}{(2^n - 2A)^{m-\alpha+i+1}} \qquad (16)$$

for $n \leq \frac{\alpha}{2} - 1$. Since $\binom{2n}{i} \leq \left(\frac{2en}{i}\right)^i \leq (2e)^i$ when $n \leq i \leq 2n$ and $\frac{2eA}{2^n - 2A} \leq \frac{1}{2}$, and by (9), we have

$$\sum_{i=n}^{2n} \binom{2n}{i} A^i D^m_{\alpha-n,1+i-n} \leq \sum_{i=n}^{2n} \binom{2n}{i} \frac{A^i h(\mathcal{G}_m)}{(2^n - 2A)^{m-\alpha+i+1}}$$

$$\leq \frac{h(\mathcal{G}_m)}{(2^n-2A)^{m-\alpha+1}} \sum_{i=n}^{2n} \left(\frac{2eA}{2^n-2A}\right)^i$$
$$\leq \frac{h(\mathcal{G}_m)}{(2^n-2A)^{m-\alpha+1}} \sum_{i=n}^{\infty} \left(\frac{1}{2}\right)^i$$
$$\leq \frac{2h(\mathcal{G}_m)}{(2^n-2A)^{m-\alpha+1}} \cdot \frac{1}{2^n}. \tag{17}$$

We also have

$$\sum_{j=0}^{n-1} \sum_{i=j}^{2j} \binom{2j}{i} \left(\frac{A}{2^n-2A}\right)^i \leq \sum_{j=0}^{n-1} \sum_{i=j}^{2j} \left(\frac{2eA}{2^n-2A}\right)^i$$
$$\leq 2 \sum_{j=0}^{\infty} \frac{1}{2^j} \leq 4. \tag{18}$$

By (16), (17) and (18) with $\alpha = m$, we have

$$D^m_{m,1} \leq \frac{2h(\mathcal{G}_m)}{2^{2n}} + \frac{(12\,|\mathcal{R}_{m+1}|+12)h(\mathcal{G}_m)}{(2^n-2A)2^n} \leq \frac{(15\,|\mathcal{R}_{m+1}|+17)h(\mathcal{G}_m)}{2^{2n}}.$$

Proof of (15). When $\alpha \in \{2,3\}$, (15) trivially holds since $D^m_{\alpha,\beta}$ is nonnegative and $D^m_{\alpha,\beta} = 0$ when $\beta \leq 0$. So we can assume that $\alpha \geq 4$.

First, suppose that $2 \leq \beta \leq \alpha - 3$. For any $\mathcal{G}[\mathcal{I},\mathcal{J},\mathcal{L}]$ such that $|\mathcal{I}| = \alpha$, $\mathcal{J} \in \mathcal{I}^{\beta+1}$, and $\mathcal{L} \in (\{0,1\}^n)^\beta$, we have

$$h(\mathcal{G}^{++}) = h(\mathcal{G}^{+-}) - \sum_{E \in \mathbb{M}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E\}) + \sum_{\{E,E'\} \in \mathbb{N}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E,E'\}), \tag{19}$$
$$h(\mathcal{G}^{-+}) = h(\mathcal{G}^{--}) - \sum_{E \in \mathbb{M}[\mathcal{G}^{-+}]} h(\mathcal{G}^{--} \cup \{E\}) + \sum_{\{E,E'\} \in \mathbb{N}[\mathcal{G}^{-+}]} h(\mathcal{G}^{--} \cup \{E,E'\}) \tag{20}$$

by Lemma 5. Since $\mathcal{G}^{--} = (\mathcal{G}^{+-})^{-+}$, we have

$$\left| \frac{h(\mathcal{G}^{--})}{2^n} - h(\mathcal{G}^{+-}) \right| \leq D^m_{\alpha-1,\beta-1}. \tag{21}$$

For each edge $E \in \mathbb{M}[\mathcal{G}^{++}]$, we have

$$\left| \frac{h(\mathcal{G}^{--} \cup \{E\})}{2^n} - h(\mathcal{G}^{+-} \cup \{E\}) \right| \leq D^m_{\alpha-1,\beta}.$$

Since $|\mathbb{M}[\mathcal{G}^{++}]| \leq 2A$ and $|\mathbb{M}[\mathcal{G}^{-+}] \setminus \mathbb{M}[\mathcal{G}^{++}]| \leq 2\,|\mathcal{R}_{m+1}| + 2$ by Lemma 6, and by Lemma 7, we have

$$\left| \sum_{E \in \mathbb{M}[\mathcal{G}^{-+}]} \frac{h(\mathcal{G}^{--} \cup \{E\})}{2^n} - \sum_{E \in \mathbb{M}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E\}) \right|$$

$$\leq \sum_{E\in\mathbb{M}[\mathcal{G}^{++}]}\left|\frac{h(\mathcal{G}^{--}\cup\{E\})}{2^n}-h(\mathcal{G}^{+-}\cup\{E\})\right|+\sum_{E\in\mathbb{M}[\mathcal{G}^{-+}]\setminus\mathbb{M}[\mathcal{G}^{++}]}\left|\frac{h(\mathcal{G}^{--}\cup\{E\})}{2^n}\right|$$
$$\leq 2A\cdot D^m_{\alpha-1,\beta}+\frac{2(|\mathcal{R}_{m+1}|+1)h(\mathcal{G}_m)}{2^n(2^n-2A)^{m-\alpha+\beta}}, \tag{22}$$

where $\mathcal{G}^{--}\cup\{E\}$ can be seen as $\mathcal{G}[\mathcal{I}',\mathcal{J}',\mathcal{L}']$ for some $\mathcal{I}'$, $\mathcal{J}'$, and $\mathcal{L}'$ such that $|\mathcal{I}'|=\alpha-1$ and $|\mathcal{J}'|=\beta-1$.

For each pair of edges $\{E,E'\}\in\mathbb{N}[\mathcal{G}^{++}]$, we have $\mathcal{G}^{--}\cup\{E,E'\}=(\mathcal{G}^{+-}\cup\{E,E'\})^{-+}$, and hence

$$\left|\frac{h(\mathcal{G}^{--}\cup\{E,E'\})}{2^n}-h(\mathcal{G}^{+-}\cup\{E,E'\})\right|\leq D^m_{\alpha-1,\beta+1}.$$

Since $|\mathbb{N}[\mathcal{G}^{++}]|\leq A^2$ and $|\mathbb{N}[\mathcal{G}^{-+}]\setminus\mathbb{N}[\mathcal{G}^{++}]|\leq 2A(|\mathcal{R}_{m+1}|+1)$ by Lemma 6, and by Lemma 7, we have

$$\left|\sum_{\{E,E'\}\in\mathbb{N}[\mathcal{G}^{-+}]}\frac{h(\mathcal{G}^{--}\cup\{E,E'\})}{2^n}-\sum_{\{E,E'\}\in\mathbb{N}[\mathcal{G}^{++}]}h(\mathcal{G}^{+-}\cup\{E,E'\})\right|$$
$$\leq A^2\cdot D^m_{\alpha-1,\beta+1}+\frac{2A(|\mathcal{R}_{m+1}|+1)h(\mathcal{G}_m)}{2^n(2^n-2A)^{m-\alpha+\beta+1}}. \tag{23}$$

By subtracting (19) from $\frac{1}{2^n}\times$ (20), combined with (21), (22) and (23), we have

$$\left|\frac{h(\mathcal{G}^{-+})}{2^n}-h(\mathcal{G}^{++})\right|\leq D^m_{\alpha-1,\beta-1}+2A\cdot D^m_{\alpha-1,\beta}+A^2\cdot D^m_{\alpha-1,\beta+1}$$
$$+\frac{(2\,|\mathcal{R}_{m+1}|+2)h(\mathcal{G}_m)}{2^n(2^n-2A)^{m-\alpha+\beta}}+\frac{2A(|\mathcal{R}_{m+1}|+1)h(\mathcal{G}_m)}{2^n(2^n-2A)^{m-\alpha+\beta+1}}.$$

Since $\frac{2A}{2^n-2A}\leq 1$, we have

$$D^m_{\alpha,\beta}\leq D^m_{\alpha-1,\beta-1}+2A\cdot D^m_{\alpha-1,\beta}+A^2\cdot D^m_{\alpha-1,\beta+1}+\frac{(3\,|\mathcal{R}_{m+1}|+3)h(\mathcal{G}_m)}{2^n(2^n-2A)^{m-\alpha+\beta}}.$$

Next, suppose that $\beta=1$. Consider $\mathcal{G}[\mathcal{I},\mathcal{J},\mathcal{L}]$ such that $|\mathcal{I}|=\alpha$, $\mathcal{J}=(j_1,j_2)$ for some $j_1,j_2\in\mathcal{I}$, and $\mathcal{L}=(L)$ for some $L\in\{0,1\}^n$. By definition, we have $\mathcal{G}^{-+}=\mathcal{G}[\mathcal{I}]$ and $\mathcal{G}^{--}=\mathcal{G}[\mathcal{I}\setminus\{j_2\}]$. Applying the (generalized) Orange equation to $\mathcal{G}^{-+}$, we have

$$h(\mathcal{G}^{++})=h(\mathcal{G}^{+-})-\sum_{E\in\mathbb{M}[\mathcal{G}^{++}]}h(\mathcal{G}^{+-}\cup\{E\})+\sum_{\{E,E'\}\in\mathbb{N}[\mathcal{G}^{++}]}h(\mathcal{G}^{+-}\cup\{E,E'\}), \tag{24}$$
$$h(\mathcal{G}^{-+})=(2^n-|\mathcal{P}_{j_2}[\mathcal{I}]|-|\mathcal{Q}_{j_2}[\mathcal{I}]|+|\mathcal{R}_{j_2}[\mathcal{I}]|)h(\mathcal{G}^{--})$$
$$+\sum_{E\in\mathbb{L}[\mathcal{G}^{-+}]}h(\mathcal{G}^{--}\cup\{E\}). \tag{25}$$

Since $\mathcal{G}^{+-} = \mathcal{G}^{--}$, we have

$$h(\mathcal{G}^{--}) - h(\mathcal{G}^{+-}) = 0. \tag{26}$$

For each edge $E \in \mathbb{M}[\mathcal{G}^{++}]$, we have

$$\left| \frac{h(\mathcal{G}^{--})}{2^n} - h(\mathcal{G}^{+-} \cup \{E\}) \right| \leq D^m_{\alpha-1,1}.$$

Since $\mathbb{M}[\mathcal{G}^{++}] \leq 2A$ and

$$|\mathcal{P}_{j_2}[\mathcal{I}]| + |\mathcal{Q}_{j_2}[\mathcal{I}]| - |\mathcal{R}_{j_2}[\mathcal{I}]| - |\mathbb{M}[\mathcal{G}^{++}]| \leq 2\,|\mathcal{R}_{m+1}| + 2$$

by Lemma 6, and by Lemma 7, we have

$$\left| (|\mathcal{P}_{j_2}[\mathcal{I}]| + |\mathcal{Q}_{j_2}[\mathcal{I}]| - |\mathcal{R}_{j_2}[\mathcal{I}]|) \frac{h(\mathcal{G}^{--})}{2^n} - \sum_{E \in \mathbb{M}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E\}) \right| \leq 2A \cdot D^m_{\alpha-1,1} + \frac{2(|\mathcal{R}_{m+1}| + 1)h(\mathcal{G}_m)}{2^n(2^n - 2A)^{m-\alpha+1}}. \tag{27}$$

Note that each edge $E = (P_k, Q_l, Z_{j_2}) \in \mathbb{L}[\mathcal{G}^{-+}]$ uniquely determines an edge $E' = (P_{j_1}, Q_k, L \oplus Z_k \oplus Z_{j_2})$ such that $\{E, E'\} \in \mathbb{N}[\mathcal{G}^{++}]$. For such a pair of edges, we have

$$\left| \frac{h(\mathcal{G}^{--} \cup \{E\})}{2^n} - h(\mathcal{G}^{+-} \cup \{E, E'\}) \right| \leq D^m_{\alpha-1,2}.$$

It implies that

$$\left| \sum_{E \in \mathbb{L}[\mathcal{G}^{-+}]} \frac{h(\mathcal{G}^{--} \cup \{E\})}{2^n} - \sum_{\{E,E'\} \in \mathbb{N}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E, E'\}) \right| \leq A^2 \cdot D^m_{\alpha-1,\beta+1} + \frac{2A(|\mathcal{R}_{m+1}| + 1)h(\mathcal{G}_m)}{2^n(2^n - 2A)^{m-\alpha+\beta+1}}. \tag{28}$$

By subtracting (24) from $\frac{1}{2^n} \times$ (25), combined with (26), (27) and (28), we have

$$D^m_{\alpha,1} \leq 2A \cdot D^m_{\alpha-1,1} + A^2 \cdot D^m_{\alpha-1,2} + \frac{(3\,|\mathcal{R}_{m+1}| + 3)h(\mathcal{G}_m)}{2^n(2^n - 2A)^{m-\alpha+\beta}}.$$

4 TPRP-based PRFs: XoTP1 and XoTP2

In this section, we propose two PRF constructions XoTP1 and XoTP2, and prove their security, where each construction is based on two n-bit TPRPs $\widetilde{\mathsf{P}}$ and $\widetilde{\mathsf{Q}}$ using t-bit tweaks. We will assume that they are independent TURPs.

4.1 XoTP1: Multiple Instances of XoP

Given a constant $C \in \{0,1\}^c$ for an integer c such that $0 \le c \le n$, a $(t+n-c)$-to-n bit pseudorandom function $\mathsf{XoTP1}_c$ is defined as follows.

$$\mathsf{XoTP1}_c(X,Y) \stackrel{\text{def}}{=} \widetilde{\mathsf{P}}(Y, C \parallel X) \oplus \widetilde{\mathsf{Q}}(Y, C \parallel X)$$

for $X \in \{0,1\}^{n-c}$ and $Y \in \{0,1\}^t$.

Security of $\mathsf{XoTP1}_c$. Suppose that a distinguisher $\mathcal{D}$ makes q queries $(X_i, Y_i) \in \{0,1\}^{n-c} \times \{0,1\}^t$, obtaining the corresponding responses Z_i for $i = 1, \ldots, q$. In this way, $\mathcal{D}$ obtains a transcript

$$\tau = ((X_1, Y_1, Z_1), \ldots, (X_q, Y_q, Z_q)).$$

In the real world, $P_i =^{\text{def}} \widetilde{\mathsf{P}}(Y_i, C \parallel X_i)$ and $Q_i =^{\text{def}} \widetilde{\mathsf{Q}}(Y_i, C \parallel X_i)$ should be a solution to the following system of equations.

$$\Gamma : \begin{cases} P_1 \oplus Q_1 = Z_1, \\ P_2 \oplus Q_2 = Z_2, \\ \qquad \vdots \\ P_q \oplus Q_q = Z_q, \end{cases}$$

subject to the partitions $\mathbb{P} = \left\{\mathcal{P}^{(M)}\right\}_{M \in \{0,1\}^t}$ and $\mathbb{Q} = \left\{\mathcal{Q}^{(M)}\right\}_{M \in \{0,1\}^t}$, where

$$(\mathcal{Q}^{(M)} =)\mathcal{P}^{(M)} \stackrel{\text{def}}{=} \{i \in [q] \mid Y_i = M\}$$

ignoring repetition of the same block. Since $\mathcal{D}$ is allowed to make at most 2^{n-c} queries for each tweak,[2] we have

$$A = \max_{M \in \{0,1\}^t} \left\{ \left|\mathcal{P}^{(M)}\right|, \left|\mathcal{Q}^{(M)}\right| \right\} \le 2^{n-c},$$
$$B = \max_{M, M' \in \{0,1\}^t} \left\{ \left|\mathcal{P}^{(M)} \cap \mathcal{Q}^{(M')}\right| \right\} \le 2^{n-c}.$$

By Corollary 1, if $c \ge 4$ (and hence $A \le 2^{n-4}$), then we have

$$h(\tau, \overset{P}{\sim}, \overset{Q}{\sim}) \ge \left(1 - \frac{2q}{2^{n+c}} - \min\left\{\frac{20q^2}{2^{2n+c}}, \frac{20q}{2^{n+2c}}\right\} - \frac{6(n+1)^3}{2^{2n}}\right) \times \prod_{i=1}^{q} \left(\frac{(2^n - |\mathcal{P}_i|)(2^n - |\mathcal{Q}_i|)}{2^n}\right).$$

Since

$$\Pr[\mathsf{T}_{\text{re}} = \tau] = \frac{h(\tau, \overset{P}{\sim}, \overset{Q}{\sim})}{\prod_{i=1}^{q}(2^n - |\mathcal{P}_i|)(2^n - |\mathcal{Q}_i|)},$$

[2] We can assume that $\mathcal{D}$ makes no redundant query.

$$\Pr[\mathsf{T}_{\mathrm{id}} = \tau] = \frac{1}{(2^n)^q},$$

we have

$$\begin{aligned}\frac{\Pr\left[\mathsf{T}_{\mathrm{re}} = \tau\right]}{\Pr\left[\mathsf{T}_{\mathrm{id}} = \tau\right]} &\geq 1 - \frac{2q}{2^{n+c}} - \min\left\{\frac{20q^2}{2^{2n+c}}, \frac{20q}{2^{n+2c}}\right\} - \frac{6(n+1)^3}{2^{2n}} \\ &\geq 1 - \frac{2q}{2^{n+c}} - \frac{20q}{2^{n+2c}} - \frac{6(n+1)^3}{2^{2n}}.\end{aligned}$$

By Lemma 1, we obtain the following theorem.

Theorem 2. *Let n, t, c and q be positive integers such that $4 \leq c \leq n$. Then one has*

$$\mathbf{Adv}^{\mathsf{prf}}_{\mathsf{XoTP1}_c}(q) \leq \frac{2q}{2^{n+c}} + \frac{20q}{2^{n+2c}} + \frac{6(n+1)^3}{2^{2n}}.$$

In particular, when $c = \frac{t}{2}$ and $t \leq 2n$, we have an $(n + \frac{t}{2})$-to-n bit PRF $\mathsf{XoTP1}_{\frac{t}{2}}$ such that

$$\mathbf{Adv}^{\mathsf{prf}}_{\mathsf{XoTP1}_{\frac{t}{2}}}(q) \leq \frac{22q}{2^{n+\frac{t}{2}}} + \frac{6(n+1)^3}{2^{2n}}.$$

Remark 1. One can alternatively count the number of solutions by dividing Γ into sub-systems Γ_M, $M \in \{0,1\}^t$, where Γ_M consists of equations $P_i \oplus Q_i = Z_i$ such that $i \in \mathcal{P}^{(M)}$. By multiplying all the number of solutions to Γ_M, $M \in \{0,1\}^t$, one obtains

$$h(\Gamma, \overset{P}{\sim}, \overset{Q}{\sim}) = \prod_{M \in \{0,1\}^t} h(\Gamma_M, \overset{P}{\sim}, \overset{Q}{\sim}).$$

By Theorem 1, the number of solutions to Γ_M is estimated as follows.

$$\begin{aligned}h(\Gamma_M, \overset{P}{\sim}, \overset{Q}{\sim}) \geq &\left(1 - \frac{2q_M^2}{2^{2n}} - \frac{20q_M^3}{2^{3n}} - \frac{6(n+1)^3}{2^{2n}}\right) \\ &\times \prod_{i \in \mathcal{P}^{(M)}} \left(\frac{(2^n - |\mathcal{P}_i|)(2^n - |\mathcal{Q}_i|)}{2^n}\right) \qquad (29)\end{aligned}$$

where $q_M = \left|\mathcal{P}^{(M)}\right|$. We note that (29) can also be obtained by recent results of Mirror theory [11, 7], while they do not apply to the security proof of $\mathsf{XoTP2}$ to be discussed in the next section as equations are not partitioned according to distinct tweaks that determine independent random permutations.

4.2 XoTP2: Xor of Tweakable Permutations with Input Switching

Given a constant $C \in \{0,1\}^c$ for an integer c such that $0 \leq c \leq n$, a $(t + n - c)$-to-n bit pseudorandom function $\mathsf{XoTP2}_c$ is defined as follows.

– When $t \geq n - c$,

$$\mathsf{XoTP2}_c(X, Y, W) = \widetilde{\mathsf{P}}(W \parallel Y, C \parallel X) \oplus \widetilde{\mathsf{Q}}(W \parallel X, C \parallel Y)$$

for X, $Y \in \{0,1\}^{n-c}$ and $W \in \{0,1\}^{t-n+c}$.
– When $t < n - c$,

$$\mathsf{XoTP2}_c(X, Y, W) = \widetilde{\mathsf{P}}(Y, C \parallel W \parallel X) \oplus \widetilde{\mathsf{Q}}(X, C \parallel W \parallel Y)$$

for X, $Y \in \{0,1\}^{t}$ and $W \in \{0,1\}^{n-t-c}$.

Security of $\mathsf{XoTP2}_c$ when $t \geq n - c$. Suppose that a distinguisher $\mathcal{D}$ makes q queries $(X_i, Y_i, W_i) \in \{0,1\}^{n-c} \times \{0,1\}^{n-c} \times \{0,1\}^{t-n+c}$, obtaining the corresponding responses Z_i for $i = 1, \ldots, q$. In this way, $\mathcal{D}$ obtains a transcript

$$\tau = ((X_1, Y_1, W_1, Z_1), \ldots, (X_q, Y_q, W_q, Z_q)).$$

In the real world, $P_i =^{\text{def}} \widetilde{\mathsf{P}}(W_i \parallel Y_i, C \parallel X_i)$ and $Q_i =^{\text{def}} \widetilde{\mathsf{Q}}(W_i \parallel X_i, C \parallel Y_i)$ should be a solution to the following system of equations.

$$\Gamma : \begin{cases} P_1 \oplus Q_1 = Z_1, \\ P_2 \oplus Q_2 = Z_2, \\ \qquad \vdots \\ P_q \oplus Q_q = Z_q, \end{cases}$$

subject to the partitions $\mathbb{P} = \left\{\mathcal{P}^{(M)}\right\}_{M \in \{0,1\}^t}$ and $\mathbb{Q} = \left\{\mathcal{Q}^{(M)}\right\}_{M \in \{0,1\}^t}$, where

$$\mathcal{P}^{(M)} \stackrel{\text{def}}{=} \{i \in [q] \mid W_i \parallel Y_i = M\},$$
$$\mathcal{Q}^{(M)} \stackrel{\text{def}}{=} \{i \in [q] \mid W_i \parallel X_i = M\}.$$

Using these partitions, we can define relations $\overset{P}{\sim}$ and $\overset{Q}{\sim}$. Since $i \overset{P}{\sim} j \Rightarrow i \overset{Q}{\not\sim} j$ and $i \overset{Q}{\sim} j \Rightarrow i \overset{P}{\not\sim} j$, we have $\left|\mathcal{P}^{(M)} \cap \mathcal{Q}^{(M')}\right| = 1$ for any $M, M' \in \{0,1\}^t$. Since $\mathcal{D}$ is allowed to make at most 2^{n-c} queries for each tweak, we have

$$A = \max_{M \in \{0,1\}^t} \left\{\left|\mathcal{P}^{(M)}\right|, \left|\mathcal{Q}^{(M)}\right|\right\} \leq 2^{n-c},$$
$$B = \max_{M, M' \in \{0,1\}^t} \left\{\left|\mathcal{P}^{(M)} \cap \mathcal{Q}^{(M')}\right|\right\} = 1.$$

By Corollary 1, if $c \geq 4$, then we have

$$h(\tau, \overset{P}{\sim}, \overset{Q}{\sim}) \geq \left(1 - \min\left\{\frac{20q}{2^{n+2c}}, \frac{20q^2}{2^{3n}}\right\} - \frac{6(n+1)^3}{2^{2n}}\right) \times \prod_{i=1}^{q} \left(\frac{(2^n - |\mathcal{P}_i|)(2^n - |\mathcal{Q}_i|)}{2^n}\right).$$

Similarly to the analysis of $\mathsf{XoTP1}$, we have

$$\frac{\Pr\left[\mathsf{T}_{\mathrm{re}}=\tau\right]}{\Pr\left[\mathsf{T}_{\mathrm{id}}=\tau\right]} \geq 1-\min\left\{\frac{20q}{2^{n+2c}}, \frac{20q^2}{2^{3n}}\right\} - \frac{6(n+1)^3}{2^{2n}}.$$

By Lemma 1, we obtain the following theorem.

Theorem 3. *Let n, t, c and q be positive integers such that $t \geq n-c$ and $4 \leq c \leq n$. Then one has*

$$\mathbf{Adv}^{\mathsf{prf}}_{\mathsf{XoTP2}_c}(q) \leq \min\left\{\frac{20q}{2^{n+2c}}, \frac{20q^2}{2^{3n}}\right\} + \frac{6(n+1)^3}{2^{2n}}.$$

When $c=\frac{t}{3}$ and $\frac{3n}{4} \leq t \leq 3n$, we have an $(n+\frac{2t}{3})$-to-n bit PRF $\mathsf{XoTP2}_{\frac{t}{3}}$ such that

$$\mathbf{Adv}^{\mathsf{prf}}_{\mathsf{XoTP2}_{\frac{t}{3}}}(q) \leq \frac{20q}{2^{n+\frac{2t}{3}}} + \frac{6(n+1)^3}{2^{2n}}.$$

When $4 \leq c \leq \frac{n}{4}$, we have an $(n+t-c)$-to-n bit PRF $\mathsf{XoTP2}_c$ such that

$$\mathbf{Adv}^{\mathsf{prf}}_{\mathsf{XoTP2}_c}(q) \leq \frac{20q^2}{2^{3n}} + \frac{6(n+1)^3}{2^{2n}}.$$

Security of $\mathsf{XoTP2}_c$ when $t < n-c$. We can prove the security of $\mathsf{XoTP2}_c$ such that $t < n-c$ similarly to the case that $t \geq n-c$, where the main difference is that

$$A = \max_{M\in\{0,1\}^t}\left\{\left|\mathcal{P}^{(M)}\right|, \left|\mathcal{Q}^{(M)}\right|\right\} \leq 2^{n-c},$$
$$B = \max_{M,M'\in\{0,1\}^t}\left\{\left|\mathcal{P}^{(M)} \cap \mathcal{Q}^{(M')}\right|\right\} \leq 2^{n-t-c}.$$

Then, using Lemma 1, we can prove the following theorem.

Theorem 4. *Let n, t, c and q be positive integers such that $t < n-c$ and $4 \leq c \leq n$. Then one has*

$$\mathbf{Adv}^{\mathsf{prf}}_{\mathsf{XoTP2}_c}(q) \leq \frac{2q}{2^{n+t+c}} + \frac{20q}{2^{n+2c}} + \frac{6(n+1)^3}{2^{2n}}.$$

When $c=\frac{t}{3}$ and $12 \leq t < \frac{3n}{4}$, we have an $(n+\frac{2t}{3})$-to-n bit PRF $\mathsf{XoTP2}_{\frac{t}{3}}$ such that

$$\mathbf{Adv}^{\mathsf{prf}}_{\mathsf{XoTP2}_{\frac{t}{3}}}(q) \leq \frac{22q}{2^{n+\frac{2t}{3}}} + \frac{6(n+1)^3}{2^{2n}}.$$

References

[1] C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich, and S. M. Sim. The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS. In M. Robshaw and J. Katz, editors, *Advances in Cryptology – CRYPTO 2016 (Proceedings, Part II)*, volume 9815 of *LNCS*, pages 123–153. Springer, 2016.

[2] M. Bellare and R. Impagliazzo. A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion. IACR Cryptology ePrint Archive, Report 1999/024, 1999. Available at `http://eprint.iacr.org/1999/024`.

[3] M. Bellare, T. Krovetz, and P. Rogaway. Luby-Rackoff Backwards: Increasing Security by Making Block Ciphers Non-invertible. In K. Nyberg, editor, *Advances in Cryptology - EUROCRYPT '98*, volume 1403 of *LNCS*, pages 266–280. Springer, 1998.

[4] S. Bhattacharya and M. Nandi. Full Indifferentiable Security of the Xor of Two or More Random Permutations Using the χ^2 Method. In J. B. Nielsen and V. Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018 (Proceedings, Part I)*, volume 10820 of *LNCS*, pages 387–412. Springer, 2018.

[5] W. Choi, B. Lee, and J. Lee. Indifferentiability of Truncated Random Permutations. In S. D. Galbraith and S. Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019 (Proceedings, Part I)*, volume 11921 of *LNCS*, pages 175–195. Springer, 2019.

[6] B. Cogliati, R. Lampe, and Y. Seurin. Tweaking Even-Mansour Ciphers. In R. Gennaro and M. Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 (Proceedings, Part I)*, volume 9215 of *LNCS*, pages 189–208. Springer, 2015.

[7] B. Cogliati and J. Patarin. Mirror Theory: A simple proof of the $P_i \oplus P_j$ Theorem with $\xi_{\max} = 2$. IACR Cryptology ePrint Archive, Report 2020/734, 2020. Available at `https://eprint.iacr.org/2020/734`.

[8] P. Crowley. Mercy: A Fast Large Block Cipher for Disk Sector Encryption. In B. Schneier, editor, *Fast Software Encryption - FSE 2000*, volume 1978 of *LNCS*, pages 49–63. Springer, 2000.

[9] W. Dai, V. T. Hoang, and S. Tessaro. Information-Theoretic Indistinguishability via the Chi-Squared Method. In J. Katz and H. Shacham, editors, *Advances in Cryptology - CRYPTO 2018 (Proceedings, Part III)*, volume 10403 of *LNCS*, pages 497–523. Springer, 2017.

[10] N. Datta, A. Dutta, M. Nandi, and K. Yasuda. Encrypt or Decrypt? To Make a Single-Key Beyond Birthday Secure Nonce-Based MAC. In H. Shacham and A. Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 (Proceedings, Part I)*, volume 10991 of *LNCS*, pages 631–661. Springer, 2018.

[11] A. Dutta, M. Nandi, and A. Saha. Proof of Mirror Theory for $\xi_{\max} = 2$. *IEEE Transactions on Information Theory*, pages 1–1, 2022.

[12] A. Dutta, M. Nandi, and S. Talnikar. Beyond Birthday Bound Secure MAC in Faulty Nonce Model. In Y. Ishai and V. Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 (Proceedings, Part I)*, volume 11476 of *LNCS*, pages 437–466. Springer, 2019.

[13] N. Ferguson, S. Lucks, B. Schneier, D. Whiting, M. Bellare, T. Kohno, J. Callas, and J. Walker. The Skein Hash Function Family. *Submission to NIST (round 3)*, 2010.

[14] S. Gilboa, S. Gueron, and B. Morris. How Many Queries are Needed to Distinguish a Truncated Random Permutation from a Random Function? *Journal of Cryptology*, 31(1):162–171, 2018.

[15] A. Gunsing and B. Mennink. The Summation-Truncation Hybrid: Reusing Discarded Bits for Free. In D. Micciancio and T. Ristenpart, editors, *Advances in Cryptology – CRYPTO 2020 (Proceedings, Part I)*, volume 12170 of *LNCS*, pages 187–217. Springer, 2020.

[16] C. Hall, D. Wagner, J. Kelsey, and B. Schneier. Building PRFs from PRPs. In H. Krawczyk, editor, *Advances in Cryptology - CRYPTO '98*, volume 1462 of *LNCS*, pages 370–389. Springer, 1998.

[17] T. Iwata. New Blockcipher Modes of Operation with Beyond the Birthday Bound Security. In *International Workshop on Fast Software Encryption*, pages 310–327. Springer, 2006.

[18] T. Iwata, K. Minematsu, T. Peyrin, and Y. Seurin. ZMAC: A Fast Tweakable Block Cipher Mode for Highly Secure Message Authentication. In J. Katz and H. Shacham, editors, *Advances in Cryptology - CRYPTO 2017 (Proceedings, Part III)*, volume 10403 of *LNCS*, pages 34–65. Springer, 2017.

[19] J. Jean, I. Nikolic, and T. Peyrin. Tweaks and Keys for Block Ciphers: The TWEAKEY Framework. In P. Sarkar and T. Iwata, editors, *Advances in Cryptology – ASIACRYPT 2014 (Proceedings, Part II)*, volume 8874 of *LNCS*, pages 274–288. Springer, 2014.

[20] J. Jean, I. Nikolic, T. Peyrin, and Y. Seurin. Deoxys v1. 41. *Submitted to CAESAR*, 2016.

[21] A. Jha and M. Nandi. Tight Security of Cascaded LRW2. *Journal of Cryptology*, 33(3):1272–1317, 2020.

[22] S. Kim, B. Lee, and J. Lee. Tight Security Bounds for Double-block Hash-then-Sum MACs. In *39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings*, volume 12105 of *Lecture Notes in Computer Science*. Springer, 2020.

[23] W. Landecker, T. Shrimpton, and R. S. Terashima. Tweakable Blockciphers with Beyond Birthday-Bound Security. In R. Safavi-Naini and R. Canetti, editors, *Advances in Cryptology - CRYPTO 2012*, volume 7417 of *LNCS*, pages 14–30. Springer, 2012.

[24] J. Lee. Indifferentiability of the Sum of Random Permutations Toward Optimal Security. *IEEE Transactions on Information Theory*, 63(6):4050–4054, 2017.

[25] M. Liskov, R. L. Rivest, and D. Wagner. Tweakable Block Ciphers. In *Advances in Cryptology - CRYPTO 2002*, volume 2442 of *LNCS*, pages 31–46. Springer, 2002.

[26] E. List and M. Nandi. Revisiting full-PRF-secure PMAC and using it for beyond-birthday authenticated encryption. In *Cryptographers' Track at the RSA Conference*, pages 258–274. Springer, 2017.

[27] B. Mennink. XPX: Generalized Tweakable Even-Mansour with Improved Security Guarantees. In *Advances in Cryptology – CRYPTO 2016 (Proceedings, Part I)*, volume 9814 of *LNCS*, pages 64–94. Springer, 2016.

[28] B. Mennink and S. Neves. Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory. In J. Katz and H. Shacham, editors, *Advances in Cryptology - CRYPTO 2017 (Proceedings, Part III)*, volume 10403 of *LNCS*, pages 556–583. Springer, 2017.

[29] Y. Naito. Full PRF-secure message authentication code based on tweakable block cipher. In *International Conference on Provable Security*, pages 167–182. Springer, 2015.

[30] Y. Naito. Tweakable Blockciphers for Efficient Authenticated Encryptions with Beyond the Birthday-Bound Security. *IACR Transactions on Symmetric Cryptology*, 2017, Issue 2:1–26, 2017.

[31] M. Nandi. Mind the Composition: Birthday Bound Attacks on EWCDMD and SoKAC21. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 203–220. Springer, 2020.

[32] J. Patarin. A Proof of Security in $O(2^n)$ for the Xor of Two Random Permutations. In R. Safavi-Naini, editor, *Information Theoretic Security*, pages 232–248, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

[33] J. Patarin. Introduction to Mirror Theory: Analysis of Systems of Linear Equalities and Linear Non Equalities for Cryptography. IACR Cryptology ePrint Archive, Report 2010/287, 2010. Available at `http://eprint.iacr.org/2010/287`.

[34] J. Patarin. Introduction to Mirror Theory: Analysis of Systems of Linear Equalities and Linear Non Equalities for Cryptography. In *IACR Cryptology ePrint Archive 2010/287*, 2010.

[35] R. Schroeppel and H. Orman. The Hasty Pudding Cipher. *AES candidate submitted to NIST*, 1998.

[36] Y. Shen, C. Guo, and L. Wang. Improved Security Bounds for Generalized Feistel Networks. *IACR Transactions on Symmetric Cryptology*, 2020, Issue 1:425–457, 2020.

Supplementary Material

A Proof of Lemma 2

We will use induction on r. One can easily see that (1) holds when $r = 1$. Suppose that (1) holds for r such that $r \leq \frac{\alpha}{2} - 2$. By the recurrence relation, we have

$$\begin{aligned}\sum_{i=r}^{2r} \binom{2r}{i} A^i D_{\alpha-r,1-r+i} \leq \sum_{i=r}^{2r} \binom{2r}{i} A^i \Bigg(& D_{\alpha-r-1,i-r} + 2A \cdot D_{\alpha-r-1,1-r+i} \\ & + A^2 \cdot D_{\alpha-r-1,2-r+i} + \frac{C}{(2^n - 2A)^{m-\alpha+1+i}} \Bigg) \\ = \sum_{i=r}^{2r+1} B_i D_{\alpha-r-1,1-r+i} & + \sum_{i=r}^{2r} \binom{2r}{i} \frac{A^i C}{(2^n - 2A)^{m-\alpha+1+i}},\end{aligned}$$

for some B_i, where

$$\begin{aligned}B_i &= \binom{2r}{i+1} A^{i+1} + \binom{2r}{i} A^i \cdot 2A + \binom{2r}{i-1} A^{i-1} \cdot A^2 \\ &= \left(\binom{2r}{i+1} + 2\binom{2r}{i} + \binom{2r}{i-1} \right) A^{i+1} \\ &= \left(\binom{2r+1}{i+1} + \binom{2r+1}{i} \right) A^{i+1} \\ &= \binom{2r+2}{i+1} A^{i+1}\end{aligned}$$

when $r + 1 \leq i \leq 2r - 1$. Even for $i \in \{r, 2r, 2r + 1\}$, one easily sees that $B_i \leq \binom{2r+2}{i+1} A^{i+1}$. Therefore, we have

$$\begin{aligned}\sum_{i=r}^{2r} \binom{2r}{i} A^i D_{\alpha-r,1-r+i} \leq & \sum_{i=r+1}^{2r+2} \binom{2r+2}{i} A^i D_{\alpha-r-1,i-r} \\ & + \sum_{i=r}^{2r} \binom{2r}{i} \frac{A^i C}{(2^n - 2A)^{m-\alpha+1+i}}.\end{aligned}$$

Combined with the induction hypothesis, we have

$$\begin{aligned}D_{\alpha,1} &\leq \sum_{i=r}^{2r} \binom{2r}{i} A^i D_{\alpha-r,1-r+i} + \sum_{j=0}^{r-1} \sum_{i=j}^{2j} \binom{2j}{i} \frac{A^i C}{(2^n - 2A)^{m-\alpha+1+i}} \\ &\leq \sum_{i=r+1}^{2r+2} \binom{2r+2}{i} A^i D_{\alpha-r-1,i-r} + \sum_{i=r}^{2r} \binom{2r}{i} \frac{A^i C}{(2^n - 2A)^{m-\alpha+1+i}}\end{aligned}$$

$$+\sum_{j=0}^{r-1}\sum_{i=j}^{2j}\binom{2j}{i}\frac{A^iC}{(2^n-2A)^{m-\alpha+1+i}}$$
$$\le\sum_{i=r+1}^{2r+2}\binom{2r+2}{i}A^iD_{\alpha-r-1,i-r}+\sum_{j=0}^{r}\sum_{i=j}^{2j}\binom{2j}{i}\frac{A^iC}{(2^n-2A)^{m-\alpha+1+i}},$$

which completes the proof.

B Proof of Lemma 4

For each solution $S=(X_1,Y_1,\ldots,X_{\alpha-1},Y_{\alpha-1})\in(\{0,1\}^n)^{2\alpha-2}$ to $\mathcal{G}_{\alpha-1}$, let

$$\mathcal{X}=\{X_i\mid i\in\mathcal{P}_\alpha\},$$
$$\mathcal{Y}=\{Y_j\oplus Z_\alpha\mid j\in\mathcal{Q}_\alpha\}.$$

Once S is fixed, one should choose P_α from $\{0,1\}^n\setminus(\mathcal{X}\cup\mathcal{Y})$. Therefore we have

$$\begin{aligned}h(\mathcal{G}_\alpha)&=\sum_{S\in\mathbb{S}}(2^n-|\mathcal{X}\cup\mathcal{Y}|)\\&=\sum_{S\in\mathbb{S}}(2^n-|\mathcal{P}_\alpha|-|\mathcal{Q}_\alpha|+|\mathcal{X}\cap\mathcal{Y}|)\\&=(2^n-|\mathcal{P}_\alpha|-|\mathcal{Q}_\alpha|)h(\mathcal{G}_{\alpha-1})+\sum_{S\in\mathbb{S}}|\mathcal{X}\cap\mathcal{Y}|\,,\end{aligned}\tag{30}$$

where $\mathbb{S}$ denote the set of all solutions to $\mathcal{G}_{\alpha-1}$. In particular, we have

$$\sum_{S\in\mathbb{S}}|\mathcal{X}\cap\mathcal{Y}|=\sum_{S\in\mathbb{S}}\sum_{\substack{i\in\mathcal{P}_\alpha\\j\in\mathcal{Q}_\alpha}}\mathbb{1}(X_i\oplus Y_j=Z_\alpha).$$

1. If $X_i\oplus Y_i=Z_\alpha$ for $i\in\mathcal{P}_\alpha\cap\mathcal{Q}_\alpha$, then it should be the case that $i\in\mathcal{R}_\alpha$. For each $i\in\mathcal{R}_\alpha$, we have

$$\sum_{S\in\mathbb{S}}\mathbb{1}(X_i\oplus Y_i=Z_\alpha)=\sum_{S\in\mathbb{S}}1=h(\mathcal{G}_{\alpha-1}).$$

2. If $i\in\mathcal{P}_\alpha$, $j\in\mathcal{Q}_\alpha$ and $i\neq j$, then we have

$$\sum_{S\in\mathbb{S}}\mathbb{1}(X_i\oplus Y_j=Z_\alpha)=h(\mathcal{G}_{\alpha-1}\cup\{(P_i,Q_j,Z_\alpha)\}).$$

To summarize, we have

$$\sum_{S\in\mathbb{S}}\sum_{\substack{i\in\mathcal{P}_\alpha\\j\in\mathcal{Q}_\alpha}}\mathbb{1}(X_i\oplus Y_j=Z_\alpha)=\sum_{S\in\mathbb{S}}\sum_{i\in\mathcal{P}_\alpha\cap\mathcal{Q}_\alpha}\mathbb{1}(X_i\oplus Y_i=Z_\alpha)$$

$$+\sum_{S\in\mathbb{S}}\sum_{\substack{i\in\mathcal{P}_\alpha\\ j\in\mathcal{Q}_\alpha\\ i\neq j}}\mathbb{1}(X_i\oplus Y_j=Z_\alpha)$$

$$=|\mathcal{R}_\alpha|\,h(\mathcal{G}_{\alpha-1})+\sum_{E\in\mathbb{L}[\mathcal{G}_\alpha]}h(\mathcal{G}_{\alpha-1}\cup\{E\}). \tag{31}$$

Lemma 4 follows from (30) and (31).

C Proof of Lemma 5

Without loss of generality, we assume that $\mathcal{I}=[\alpha]$, $\mathcal{J}=(\alpha-\beta,\alpha-\beta+1,\ldots,\alpha)$. Let $\mathbb{S}\subset(\{0,1\}^n)^{2\alpha}$ and $\mathbb{S}'\subset(\{0,1\}^n)^{2\alpha-2}$ denote the sets of solutions to $\mathcal{G}^{++}$ and $\mathcal{G}^{+-}$, respectively. Each solution $(X_1,Y_1,\ldots,X_\alpha,Y_\alpha)\in\mathbb{S}$ uniquely determines a solution to $\mathcal{G}^{+-}$, namely $(X_1,Y_1,\ldots,X_{\alpha-1},Y_{\alpha-1})\in\mathbb{S}'$. On the other hand, for each solution $(X_1,Y_1,\ldots,X_{\alpha-1},Y_{\alpha-1})\in\mathbb{S}'$, let

$$X_\alpha=X_{\alpha-1}\oplus L_\beta\oplus Z_\alpha,$$
$$Y_\alpha=X_{\alpha-1}\oplus L_\beta.$$

Then $(X_1,Y_1,\ldots,X_\alpha,Y_\alpha)$ is a solution to $\mathcal{G}^{++}$ if and only if X_α and Y_α do not violate the constraints due to the relations $\overset{P}{\sim}$ and $\overset{Q}{\sim}$. For this condition to hold, it should be the case that

$$X_\alpha\neq X_k\Leftrightarrow X_{\alpha-1}\oplus L_\beta\oplus Z_\alpha\neq X_k\Leftrightarrow X_{\alpha-1}\neq X_k\oplus L_\beta\oplus Z_\alpha$$

for any index k such that $k\overset{P}{\sim}\alpha$. Furthermore, for an index k such $k\overset{Q}{\sim}\alpha$, the following non-equation is also required.

$$Y_\alpha\neq Y_k\Leftrightarrow X_{\alpha-1}\neq Y_k\oplus L_\beta.$$

So, for each solution $(X_1,Y_1,\ldots,X_{\alpha-1},Y_{\alpha-1})\in\mathbb{S}'$, $(X_1,Y_1,\ldots,X_\alpha,Y_\alpha)$ becomes a solution to $\mathcal{G}^{++}$ if and only if $X_{\alpha-1}\in\{0,1\}^n\setminus(\mathcal{X}\cup\mathcal{Y})$, where

$$\mathcal{X}\overset{\text{def}}{=}\{X_k\oplus L_\beta\oplus Z_\alpha\mid k\in\mathcal{P}_\alpha\},$$
$$\mathcal{Y}\overset{\text{def}}{=}\{Y_k\oplus L_\beta\mid k\in\mathcal{Q}_\alpha\}.$$

Therefore we have

$$h(\mathcal{G}^{++})=\sum_{S\in\mathbb{S}'}(1-\mathbb{1}(X_{\alpha-1}\in\mathcal{X}\cup\mathcal{Y}))$$
$$=h(\mathcal{G}^{+-})-\sum_{S\in\mathbb{S}'}\mathbb{1}(X_{\alpha-1}\in\mathcal{X})$$
$$-\sum_{S\in\mathbb{S}'}\mathbb{1}(X_{\alpha-1}\in\mathcal{Y})+\sum_{S\in\mathbb{S}'}\mathbb{1}(X_{\alpha-1}\in\mathcal{X}\cap\mathcal{Y}). \tag{32}$$

Suppose that $X_{\alpha-1}\in\mathcal{X}$, in which case $X_\alpha=X_k$ for some $k\in\mathcal{P}_\alpha$.

1. If $k \in \mathcal{P}_\alpha[\mathcal{J}]$, then there exists a trail $T(X_k, X_\alpha)$ such that
$$w(T(X_k, X_\alpha)) \neq \mathbf{0}$$
since $\mathcal{G}^{++}$ is a valid graph. It implies that $X_\alpha \neq X_k$, which is a contradiction.
2. If $k \in \mathcal{P}_\alpha[\mathcal{I} \setminus \mathcal{J}]$, then a solution to $\mathcal{G}^{+-}$ such that $X_\alpha = X_k$ becomes a solution to
$$\mathcal{G}^{+-} \cup \{(X_{\alpha-1}, Y_k, L_\beta \oplus Z_k \oplus Z_\alpha)\}.$$

Suppose that $X_{\alpha-1} \in \mathcal{Y}$, in which case $Y_\alpha = Y_k$ for some $k \in \mathcal{Q}_\alpha$. Then it follows that $k \in \mathcal{Q}_\alpha[\mathcal{I} \setminus \mathcal{J}]$. Furthermore, a solution to $\mathcal{G}^{+-}$ such that $Y_\alpha = Y_k$ becomes a solution to a graph
$$\mathcal{G}^{+-} \cup \{(X_{\alpha-1}, Y_k, L_\beta)\}.$$

To summarize, we have
$$\sum_{S \in \mathbb{S}'} \mathbb{1}(X_{\alpha-1} \in \mathcal{X}) = \sum_{E \in \mathbb{M}_1} h(\mathcal{G}^{+-} \cup \{E\}), \tag{33}$$
$$\sum_{S \in \mathbb{S}'} \mathbb{1}(X_{\alpha-1} \in \mathcal{Y}) = \sum_{E \in \mathbb{M}_2} h(\mathcal{G}^{+-} \cup \{E\}), \tag{34}$$

where
$$\mathbb{M}_1 \stackrel{\text{def}}{=} \{(P_{\alpha-1}, Q_k, L_\beta \oplus Z_k \oplus Z_\alpha) \mid k \in \mathcal{P}_\alpha[\mathcal{I} \setminus \mathcal{J}]\},$$
$$\mathbb{M}_2 \stackrel{\text{def}}{=} \{(P_{\alpha-1}, Q_k, L_\beta) \mid k \in \mathcal{Q}_\alpha[\mathcal{I} \setminus \mathcal{J}]\}.$$

Suppose that $X_{\alpha-1} \in \mathcal{X} \cap \mathcal{Y}$, in which case
$$X_{\alpha-1} = X_k \oplus L_\beta \oplus Z_\alpha,$$
$$X_{\alpha-1} = Y_l \oplus L_\beta$$
for some $k \in \mathcal{P}_\alpha[\mathcal{I} \setminus \mathcal{J}]$ and $l \in \mathcal{Q}_\alpha[\mathcal{I} \setminus \mathcal{J}]$. Replacing X_k by $Y_k \oplus Z_k$ in the first equation, and $X_{\alpha-1}$ by $X_k \oplus L_\beta \oplus Z_\alpha$ in the second equation, we have
$$X_{\alpha-1} \oplus Y_k = L_\beta \oplus Z_k \oplus Z_\alpha,$$
$$X_k \oplus Y_l = Z_\alpha.$$

There are two cases.

1. If $k \neq l$, then a solution to $\mathcal{G}^{+-}$ such that $X_{\alpha-1} \oplus Y_k = L_\beta \oplus Z_k \oplus Z_\alpha$ and $X_k \oplus Y_l = Z_\alpha$ is a solution to a graph
$$\mathcal{G}^{+-} \cup \{(X_{\alpha-1}, Y_k, L_\beta \oplus Z_k \oplus Z_\alpha), (X_k, Y_l, Z_\alpha)\}.$$
2. If $k = l$, then $k \in \mathcal{P}_\alpha[\mathcal{I} \setminus \mathcal{J}] \cap \mathcal{Q}_\alpha[\mathcal{I} \setminus \mathcal{J}]$.
   (a) If $Z_k = Z_\alpha$, then edge (X_k, Y_l, Z_α) is redundant. Therefore, a solution to $\mathcal{G}^{+-}$ such that $X_{\alpha-1} \oplus Y_k = L_\beta \oplus Z_k \oplus Z_\alpha$ and $X_k \oplus Y_l = Z_\alpha$ is a solution to a graph
   $$\mathcal{G}^{+-} \cup \{(X_{\alpha-1}, Y_k, L_\beta)\}.$$

(b) If $Z_k \neq Z_\alpha$, then there is no solution to the graph.

Therefore we have

$$\sum_{S\in\mathbb{S}'} \mathbb{1}(X_{\alpha-1} \in \mathcal{X} \cap \mathcal{Y}) = \sum_{E\in\mathbb{M}_3} h(\mathcal{G}^{+-} \cup \{E\}) + \sum_{\{E,E'\}\in\mathbb{N}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E, E'\}) \quad (35)$$

where

$$\mathbb{M}_3 \stackrel{\text{def}}{=} \{(P_{\alpha-1}, Q_k, L_\beta) \mid k \in \mathcal{R}_\alpha[\mathcal{I} \setminus \mathcal{J}]\}.$$

Since

$$\sum_{E\in\mathbb{M}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E\}) = \sum_{E\in\mathbb{M}_1\cup\mathbb{M}_2} h(\mathcal{G}^{+-} \cup \{E\}) = \sum_{E\in\mathbb{M}_1} h(\mathcal{G}^{+-} \cup \{E\}) + \sum_{E\in\mathbb{M}_2} h(\mathcal{G}^{+-} \cup \{E\}) - \sum_{E\in\mathbb{M}_3} h(\mathcal{G}^{+-} \cup \{E\})$$

and by (32), (33), (34) and (35), the proof is complete.

D Proof of Lemma 6

We can prove the five (in)equalities as follows.

1. Each edge $(P_i, Q_j, Z_\alpha) \in \mathbb{L}[\mathcal{G}_\alpha]$ falls into one of the following four cases.
   - Case 1: $i \in \mathcal{P}_\alpha \setminus \mathcal{Q}_\alpha$ and $j \in \mathcal{Q}_\alpha \setminus \mathcal{P}_\alpha$. Note that $\mathcal{G}_\alpha \cup \{(P_i, Q_j, Z_\alpha)\}$ is valid. The number of edges of this type is
   $$(|\mathcal{P}_\alpha| - |\mathcal{P}_\alpha \cap \mathcal{Q}_\alpha|)(|\mathcal{Q}_\alpha| - |\mathcal{P}_\alpha \cap \mathcal{Q}_\alpha|).$$
   - Case 2: $i \in \mathcal{P}_\alpha \cap \mathcal{Q}_\alpha$ and $j \in \mathcal{Q}_\alpha \setminus \mathcal{P}_\alpha$. Equations $P_i \oplus Q_j = Z_\alpha$ and $P_i \oplus Q_i = Z_i$ imply $Q_i \oplus Q_j = Z_\alpha \oplus Z_i$. Since $i \overset{\mathcal{Q}}{\sim} j$, it should be the case that $Z_i \neq Z_\alpha$. The number of such edges is
   $$(|\mathcal{P}_\alpha \cap \mathcal{Q}_\alpha| - |\mathcal{R}_\alpha|)(|\mathcal{Q}_\alpha| - |\mathcal{P}_\alpha \cap \mathcal{Q}_\alpha|).$$
   - Case 3: $i \in \mathcal{P}_\alpha \setminus \mathcal{Q}_\alpha$ and $j \in \mathcal{P}_\alpha \cap \mathcal{Q}_\alpha$. Similarly to Case 2, we see that the number of edges of this type is
   $$(|\mathcal{P}_\alpha \cap \mathcal{Q}_\alpha| - |\mathcal{R}_\alpha|)(|\mathcal{P}_\alpha| - |\mathcal{P}_\alpha \cap \mathcal{Q}_\alpha|).$$
   - Case 4: $i, j \in \mathcal{P}_\alpha \cap \mathcal{Q}_\alpha$ where $i \neq j$. It should be the case that $Z_i \neq Z_\alpha$ and $Z_j \neq Z_\alpha$ since otherwise the resulting graph is invalid. The number of such edges is
   $$(|\mathcal{P}_\alpha \cap \mathcal{Q}_\alpha| - |\mathcal{R}_\alpha|)(|\mathcal{P}_\alpha \cap \mathcal{Q}_\alpha| - |\mathcal{R}_\alpha| - 1).$$

Therefore, we conclude that

$$|\mathbb{L}[\mathcal{G}_\alpha]| = (|\mathcal{P}_\alpha| - |\mathcal{R}_\alpha|)(|\mathcal{Q}_\alpha| - |\mathcal{R}_\alpha|) - (|\mathcal{P}_\alpha \cap \mathcal{Q}_\alpha| - |\mathcal{R}_\alpha|).$$

2. Note that $\mathbb{M}[\mathcal{G}^{++}] \subset \mathbb{M}[\mathcal{G}^{-+}]$ when $\beta \geq 2$. Each edge E in $\mathbb{M}[\mathcal{G}^{-+}] \setminus \mathbb{M}[\mathcal{G}^{++}]$ is of the form either $(P_{j_\beta}, Q_k, L_\beta \oplus Z_k \oplus Z_{j_{\beta+1}})$ for $k \in \mathcal{P}_{j_{\beta+1}}[(\mathcal{I} \setminus \mathcal{J}) \cup \{j_1\}]$ or $(P_{j_\beta}, Q_k, L_\beta)$ for $k \in \mathcal{Q}_{j_{\beta+1}}[(\mathcal{I} \setminus \mathcal{J}) \cup \{j_1\}]$. Such an edge falls into at least one of the following three cases.
   - Case 1: $k = j_1$. At most two edges fall into this case.
   - Case 2: $E = (P_{j_\beta}, Q_k, L_\beta \oplus Z_k \oplus Z_{j_{\beta+1}})$ for $k \in \mathcal{P}_{j_{\beta+1}}[\mathcal{I} \setminus \mathcal{J}]$. Since $E \in \mathbb{M}[\mathcal{G}^{-+}] \setminus \mathbb{M}[\mathcal{G}^{++}]$, $\mathcal{G}^{++}$ and $\mathcal{G}^{--} \cup \{E\}$ are valid, while $\mathcal{G}^{+-} \cup \{E\}$ is invalid, which means that $k \overset{Q}{\sim} j_1$, and $w(T(Q_{j_1}, Q_k)) = \mathbf{0}$ for a (unique) trail $T(Q_{j_1}, Q_k)$ connecting Q_{j_1} and Q_k, which means

     $$Z_k = Z_{j_1} \oplus \ldots \oplus Z_{j_{\beta+1}} \oplus L_1 \oplus \ldots \oplus L_\beta (\overset{\text{def}}{=} Z).$$

     The number of such edges E is at most $\left|\{k \in \mathcal{P}_{j_{\beta+1}} \cap \mathcal{Q}_{j_1} \mid Z_k = Z\}\right|$, where by (8)

     $$\left|\{k \in \mathcal{P}_{j_{\beta+1}} \cap \mathcal{Q}_{j_1} \mid Z_k = Z\}\right| \leq |\mathcal{R}_{m+1}|.$$

   - Case 3: $E = (P_{j_\beta}, Q_k, L_\beta)$ for $k \in \mathcal{Q}_{j_{\beta+1}}[\mathcal{I} \setminus \mathcal{J}]$. Similarly to Case 2, we see that the number of edges of this type is at most $|\mathcal{R}_{m+1}|$.

   It is easy to see that $|\mathbb{M}[\mathcal{G}^{++}]| \leq 2A$. Therefore, we conclude that

   $$|\mathbb{M}[\mathcal{G}^{-+}]| - 2(|\mathcal{R}_{m+1}| + 1) \leq |\mathbb{M}[\mathcal{G}^{++}]| \leq 2A.$$

3. Note that $\mathbb{N}[\mathcal{G}^{++}] \subset \mathbb{N}[\mathcal{G}^{-+}]$ when $\beta \geq 2$. For each pair of edges $\{E, E'\}$ in $\mathbb{N}[\mathcal{G}^{-+}] \setminus \mathbb{N}[\mathcal{G}^{++}]$, we can assume that $E = (P_{j_\beta}, Q_k, L_\beta \oplus Z_k \oplus Z_{j_{\beta+1}})$ for some $k \in \mathcal{P}_{j_{\beta+1}}[(\mathcal{I} \setminus \mathcal{J}) \cup \{j_1\}]$, and $E' = (P_k, Q_l, Z_{j_{\beta+1}})$ for some l such that $l \neq k$ and $l \in \mathcal{Q}_{j_{\beta+1}}[(\mathcal{I} \setminus \mathcal{J}) \cup \{j_1\}]$. Such a pair (E, E') falls into at least one of the following three cases.
   - Case 1: $k \in \mathcal{P}_{j_{\beta+1}}[(\mathcal{I} \setminus \mathcal{J}) \cup \{j_1\}]$ and $l = j_1$. Since

     $$\left|\mathcal{P}_{j_{\beta+1}}[(\mathcal{I} \setminus \mathcal{J}) \cup \{j_1\}]\right| \leq A,$$

     the number of pairs of edges of this type is at most A.
   - Case 2: $k = j_1$ and $l \in \mathcal{Q}_{j_{\beta+1}}[(\mathcal{I} \setminus \mathcal{J}) \cup \{j_1\}]$. Similarly to Case 1, the number of pairs of edges of this type is at most A.
   - Case 3: $k \in \mathcal{P}_{j_{\beta+1}}[\mathcal{I} \setminus \mathcal{J}]$ and $l \in \mathcal{Q}_{j_{\beta+1}}[\mathcal{I} \setminus \mathcal{J}]$. Since $\mathcal{G}^{+-} \cup \{E, E'\}$ is invalid, there exist $k', l' \in \{j_1, \ldots, j_\beta, k, l\}$ such that either

     $$k' \overset{Q}{\sim} l' \wedge w(T(Q_{k'}, Q_{l'})) = \mathbf{0}$$

     for a (unique) trail $T(Q_{k'}, Q_{l'})$ connecting $Q_{k'}$ and $Q_{l'}$, or

     $$k' \overset{P}{\sim} l' \wedge w(T(P_{k'}, P_{l'})) = \mathbf{0}$$

     for a (unique) trail $T(P_{k'}, P_{l'})$ connecting $P_{k'}$ and $P_{l'}$. Since $\mathcal{G}^{++}$ and $\mathcal{G}^{--} \cup \{E, E'\}$ are valid, two possibilities remain as follows.

(a) $k \overset{Q}{\sim} j_1$ and $w(T(Q_k, Q_{j_1})) = \mathbf{0}$ for a (unique) trail $T(Q_k, Q_{j_1})$ connecting Q_{j_1} and Q_k, which means

$$Z_k = Z_{j_1} \oplus \ldots \oplus Z_{j_{\beta+1}} \oplus L_1 \oplus \ldots \oplus L_\beta.$$

The number of pairs of edges of this type is at most $|\mathcal{R}_{m+1}|\, A$.

(b) $l \overset{P}{\sim} j_1$ and $w(T(P_l, P_{j_1})) = \mathbf{0}$ for a (unique) trail $T(P_l, P_{j_1})$ connecting P_{j_1} and P_l, which means

$$Z_l = Z_{j_2} \oplus \ldots \oplus Z_{j_\beta} \oplus L_1 \oplus \ldots \oplus L_\beta.$$

The number of pairs of edges of this type is at most $|\mathcal{R}_{m+1}|\, A$.

It is easy to see that $|\mathbb{N}[\mathcal{G}^{++}]| \leq A^2$. Therefore, we conclude that

$$|\mathbb{N}[\mathcal{G}^{-+}]| - 2A(|\mathcal{R}_{m+1}| + 1) \leq |\mathbb{N}[\mathcal{G}^{++}]| \leq A^2.$$

4. Suppose that $\beta = 1$. Let $\mathbb{M}'$ be the set of edges of the form either (P_{j_1}, Q_k, L_1) for $k \in \mathcal{Q}_{j_2}[\mathcal{I}]$ or $(P_{j_1}, Q_k, L_1 \oplus Z_k \oplus Z_{j_2})$ for $k \in \mathcal{P}_{j_2}[\mathcal{I}]$. Note that $|\mathbb{M}'| = |\mathcal{P}_{j_2}[\mathcal{I}]| + |\mathcal{Q}_{j_2}[\mathcal{I}]| - |\mathcal{R}_{j_2}[\mathcal{I}]|$ and $\mathbb{M}[\mathcal{G}^{++}] \subset \mathbb{M}'$. Each edge E in $\mathbb{M}' \setminus \mathbb{M}[\mathcal{G}^{++}]$ falls into at least one of the following three cases.
   - Case 1: $k = j_1$. At most two edges fall into this case.
   - Case 2: $E = (P_{j_1}, Q_k, L_1 \oplus Z_k \oplus Z_{j_2})$ for $k \in \mathcal{P}_{j_2}[\mathcal{I} \setminus \mathcal{J}]$. Since $E \in \mathbb{M}' \setminus \mathbb{M}[\mathcal{G}^{++}]$, $\mathcal{G}^{++}$ is valid, while $\mathcal{G}^{+-} \cup \{E\}$ is invalid, which means that $k \overset{Q}{\sim} j_1$, and $w(T(Q_{j_1}, Q_k)) = \mathbf{0}$ for a (unique) trail $T(Q_{j_1}, Q_k)$ connecting Q_{j_1} and Q_k, which means

     $$Z_k = Z_{j_1} \oplus Z_{j_2} \oplus L_1 (\overset{\text{def}}{=} Z').$$

     The number of such edges E is at most $|\{k \in \mathcal{P}_{j_2} \cap Q_{j_1} \mid Z_k = Z'\}|$, where by (8)

     $$|\{k \in \mathcal{P}_{j_2} \cap Q_{j_1} \mid Z_k = Z'\}| \leq |\mathcal{R}_{m+1}|\,.$$

   - Case 3: $E = (P_{j_1}, Q_k, L_1)$ for $k \in \mathcal{Q}_{j_2}[\mathcal{I} \setminus \mathcal{J}]$. Similarly to Case 2, we see that the number of edges of this type is at most $|\mathcal{R}_{m+1}|$.

   It is easy to see that $|\mathbb{M}[\mathcal{G}^{++}]| \leq 2A$. Therefore, we conclude that

   $$|\mathcal{P}_{j_2}[\mathcal{I}]| + |\mathcal{Q}_{j_2}[\mathcal{I}]| - |\mathcal{R}_{j_2}[\mathcal{I}]| - 2(|\mathcal{R}_{m+1}| + 1) \leq |\mathbb{M}[\mathcal{G}^{++}]| \leq 2A.$$

5. Suppose that $\beta = 1$. Let $\mathbb{N}'$ denote the set of pairs of edges $\{E, E'\}$ where $E = (P_{j_1}, Q_k, L_1 \oplus Z_k \oplus Z_{j_2})$ and $E' = (P_k, Q_l, Z_{j_2})$ such that $k \in \mathcal{P}_{j_2}[\mathcal{I}]$, $l \in \mathcal{Q}_{j_2}[\mathcal{I}]$, $k \neq l$ and $h(\mathcal{G}^{-+} \cup \{E'\}) > 0$. Then we have $\mathbb{N}[\mathcal{G}^{++}] \subset \mathbb{N}'$ and $|\mathbb{N}'| = |\mathbb{L}[\mathcal{G}^{-+}]|$ since $\mathbb{L}[\mathcal{G}^{-+}]$ is obtained by collecting E' for all $\{E, E'\} \in \mathbb{N}'$. Each pair $\{E, E'\} \in \mathbb{N}' \setminus \mathbb{N}[\mathcal{G}^{++}]$ falls into at least one of the following three cases.

- Case 1: $k \in \mathcal{P}_{j_2}[\mathcal{I}]$ and $l = j_1$. Since $|\mathcal{P}_{j_2}[\mathcal{I}]| \leq A$, the number of pairs of edges of this type is at most A.
- Case 2: $k = j_1$ and $l \in \mathcal{Q}_{j_2}[\mathcal{I}]$. Similarly to Case 1, the number of pairs of edges of this type is at most A.
- Case 3: $k \in \mathcal{P}_{j_2}[\mathcal{I} \setminus \mathcal{J}]$ and $l \in \mathcal{Q}_{j_2}[\mathcal{I} \setminus \mathcal{J}]$. Since $\{E, E'\} \in \mathbb{N}' \setminus \mathbb{N}[\mathcal{G}^{++}]$, $\mathcal{G}^{++}$ and $\mathcal{G}^{--} \cup \{E'\}$ are valid, while $\mathcal{G}^{+-} \cup \{E, E'\}$ is invalid. Then at least one of the following two conditions holds:
  (a) $k \overset{Q}{\sim} j_1$ and $w(T(Q_k, Q_{j_1})) = \mathbf{0}$ for a (unique) trail $T(Q_k, Q_{j_1})$ connecting Q_{j_1} and Q_k, which means $Z_k = Z_{j_1} \oplus Z_{j_2} \oplus L_1$. The number of pairs of edges of this type is at most $|\mathcal{R}_{m+1}|\, A$.
  (b) $l \overset{P}{\sim} j_1$ and $w(T(P_l, P_{j_1})) = \mathbf{0}$ for a (unique) trail $T(P_l, P_{j_1})$ connecting P_{j_1} and P_l, which means $Z_l = L_1$. The number of pairs of edges of this type is at most $|\mathcal{R}_{m+1}|\, A$.

It is easy to see that $|\mathbb{N}[\mathcal{G}^{++}]| \leq A^2$. Therefore we conclude that

$$|\mathbb{L}[\mathcal{G}^{-+}]| - 2A(|\mathcal{R}_{m+1}| + 1) \leq |\mathbb{N}[\mathcal{G}^{++}]| \leq A^2.$$

E Proof of Lemma 7

Without loss of generality, we assume that $\mathcal{I} = [\alpha]$. Let $\mathbb{S}$ denote the set of solutions to $\mathcal{G}_\alpha$. For each solution $(X_1, Y_1, \ldots, X_\alpha, Y_\alpha) \in \mathbb{S}$, $(X_1, Y_1, \ldots, X_{\alpha+1}, Y_{\alpha+1})$ becomes a solution to $\mathcal{G}_{\alpha+1}$ if and only if $X_{\alpha+1} \in \{0,1\}^n \setminus (\mathcal{X} \cup \mathcal{Y})$, where

$$\mathcal{X} \overset{\text{def}}{=} \left\{ X_i \,\middle|\, i \overset{P}{\sim} (\alpha+1), i \in [\alpha] \right\},$$
$$\mathcal{Y} \overset{\text{def}}{=} \left\{ Y_i \oplus Z_{\alpha+1} \,\middle|\, i \overset{Q}{\sim} (\alpha+1), i \in [\alpha] \right\}.$$

Therefore, we have

$$h(\mathcal{G}_{\alpha+1}) \geq \sum_{S \in \mathbb{S}} (2^n - |\mathcal{X} \cup \mathcal{Y}|) \geq (2^n - 2A) h(\mathcal{G}_\alpha).$$

By repeatedly applying the above inequality, we have

$$h(\mathcal{G}_\alpha) \leq \frac{h(\mathcal{G}_m)}{(2^n - 2A)^{m-\alpha}}, \tag{36}$$

which completes the proof of Lemma 7 when $\beta = 0$.

Suppose that $\beta \geq 1$. Fix $\mathcal{J} = (\alpha-\beta, \alpha-\beta+1, \ldots, \alpha)$ without loss of generality, and let $\mathcal{L} = (L_1, \ldots, L_\beta) \in (\{0,1\}^n)^\beta$. For each solution $(X_1, Y_1, \ldots, X_\alpha, Y_\alpha)$ to $\mathcal{G}^{++} (= \mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}])$, $X_{\alpha-\beta}$ and $Y_{\alpha-\beta}$ can be replaced by $X'_{\alpha-\beta}$ and $Y'_{\alpha-\beta}$, respectively, giving a solution to $\mathcal{G}^{-+}$, if $X'_{\alpha-\beta} \in \{0,1\}^n \setminus (\mathcal{X}' \cup \mathcal{Y}')$ and $Y'_{\alpha-\beta} = X'_{\alpha-\beta} \oplus Z_{\alpha-\beta}$, where

$$\mathcal{X}' \overset{\text{def}}{=} \left\{ X_i \,\middle|\, i \overset{P}{\sim} (\alpha-\beta), i \in [\alpha] \setminus \{\alpha-\beta\} \right\},$$

$$\mathcal{Y}' \stackrel{\text{def}}{=} \left\{ Y_i \oplus Z_{\alpha-\beta} \,\middle|\, i \overset{Q}{\sim} (\alpha-\beta), i \in [\alpha] \setminus \{\alpha-\beta\} \right\}.$$

Therefore, we have

$$h(\mathcal{G}^{-+}) \geq \sum_{S \in \mathbb{S}'} (2^n - |\mathcal{X}' \cup \mathcal{Y}'|) \geq (2^n - 2A) h(\mathcal{G}^{++}),$$

where $\mathbb{S}'$ denotes the set of all solutions to $\mathcal{G}^{++}$. By repeatedly applying the above inequality, we have

$$h(\mathcal{G}^{++}) \leq \frac{h(\mathcal{G}_\alpha)}{(2^n - 2A)^\beta} \tag{37}$$

The proof is complete by (36) and (37).