Electronic Colloquium on Computational Complexity, Report No. 114 (2022)

Direct Sum Theorems From Fortification

Hao Wu*

August 16, 2022

Abstract

We revisit the direct sum theorems in communication complexity which askes whether the resource to solve n communication problems together is (approximately) the sum of resources to solve these problems separately. Our work starts with the observation that Meir and Dinur's fortification lemma[DM18] for protocol size over rectangles can be generalized to a general fortification lemma for a sub-additive measure over set. By applying this lemma to the case of cover number, we obtain a dual form of cover number, called "δ-fooling set" which is a generalized fooling set. Given a communication problem $S \subseteq (X \times Y) \times Z$, let $\Lambda \subseteq X \times Y$ be a δ-fooling set of S, then given any subset $\tilde{\Lambda} \subseteq \Lambda$ such that $|\tilde{\Lambda}|/|\Lambda| > \delta$, there is no monochromatic rectangle that covers the subset $\tilde{\Lambda}$. Particularly, there is a $\frac{16 \log |X||Y|}{\mathsf{Cov}(S)}$-fooling set of communication problem S.

With this fact, we are able to reprove the classic direct sum theorem[KKN95] of cover number with a simple double counting argument. Formally, let $S \subseteq (A \times B) \times O$ and $T \subseteq (P \times Q) \times Z$ be two communication problems, $\log \mathsf{Cov}\,(S \times T) \geq \log \mathsf{Cov}\,(S) + \log \mathsf{Cov}(T) - \log\log|P||Q| - 4$. where Cov denotes the cover number.

One issue of current deterministic direct sum theorems[FKNN95, KKN95] about commutation complexity or protocol size is that they provide no information when n is small, especially when $n = 2$. In this work, we prove a new direct sum theorem about protocol size which imply a better direct sum theorem for two functions in terms of protocol size. Formally, let L denote the protocol size, given a communication problem $F : A \times B \to \{0, 1\}$, $\log \mathsf{L}\,(F \times F) \geq \log \mathsf{L}\,(F) + \Omega\left(\sqrt{\log \mathsf{L}\,(F)}\right) - \log\log|A||B| - 4$.

We also address other direct sum type problem such like the agree problem introduced by Amos Beimel et al.[BDKW14]. We prove a tight cover number lower bound for the agree problem. Formally, let $S_i \subseteq X_i \times Y_i \times Z, i \in [k]$ be k two-party communication problems, $\mathsf{Cov}\,(\mathtt{agree}(S_1, \ldots, S_k)) \geq \min_{i\in[k]} \left\{\frac{\mathsf{Cov}(S_i)}{16 \log |X_i||Y_i|}\right\}$.

All our direct sum type results are obtained in a similar way, that is using the δ-fooling set to construct a hardcore for the direct sum type problem.

Contents

*College of Information Engineering, Shanghai Maritime University, Shanghai, China. My email is haowu@shmtu.edu.cn, you can also reach me via wealk@outlook.com.

ISSN 1433-8092

1 Introduction

The direct sum question, in general, asks following question: whether the resource to solve several tasks together is (approximately) the sum of resources to solve these tasks separately. Particularity, we want to know whether the resource to solve n copies of certain task is (approximately) n times the resource to solve one copy of the task. In the field of communication complexity, the direct sun question was proposed by Karchmer, Raz, and Wigderson[KRW91]. Let communication problem $F : X \times Y \to \{0,1\}$ be a function and C denote the communication complexity of a problem, current known deterministic direct sum theorems[FKNN95, KKN95][1] tells us solving n copies of communication problem F requires about $\Omega\left(n \cdot \sqrt{\mathsf{C}(F)}\right)$ bits of communication. But in some cases, current direct sum theorems are not satisfactory. When n is small, especially when $n = 2$, current direct sum theorems tell us nothing more than the trivial lower bound. Intuitively, we should be able to prove stronger results when $n = 2$, that if the communication complexity of F is not too small, then solving two copies of F should require strictly more communication than solving only one copy of F. Formally, we have following conjecture which is consistent with current know direct sum theorems.

Conjecture 1.1. *Let communication problem $F : X \times Y \to \{0,1\}$ be a function,* $\mathsf{C}(F \times F) \geq \mathsf{C}(F) + \Omega\left(\sqrt{\mathsf{C}(F)}\right)$.

Let $\mathsf{L}(F)$ denote the protocol size of the communication problem $F : X \times Y \to \{0,1\}$, similarly, we have following conjecture about protocol size.

Conjecture 1.2. *Let communication problem $F : X \times Y \to \{0,1\}$ be a function,* $\log \mathsf{L}(F \times F) \geq \log \mathsf{L}(F) + \Omega\left(\sqrt{\mathsf{L}(F)}\right)$.

Beside the standard direct sum question, there are many variants. For example, Amos Beimel et al.[BDKW14] introduced variants such as the eliminate problem, the choose problem and the agree problem. Take the agree problem as example, given k communication problems $F_i : (\{0,1\}^n \times \{0,1\}^n) \to \{0,1\}$, the agree problem of $F_1, F_2, \cdots, F_k$, denoted by $\texttt{agree}(F_1, F_2, \cdots, F_k) : (\{0,1\}^n)^k \times (\{0,1\}^n)^k \to \{0,1\}$, is following problem: Alice is given an $\mathbf{x} \in (\{0,1\}^n)^k$, Bob is given a $\mathbf{y} \in (\{0,1\}^n)^k$, they are asked to output a $z \in \{0,1\}$ such that there is an $i \in [k]$, $F_i(\mathbf{x}_i, \mathbf{y}_i) = z$. Intuitively, they are asked to solve one function out of k functions without to specify which copy they have solved. Given $z \in \{0,1\}$, let $\mathsf{Cov}^z(F)$ denote the cover number needed to cover all (x,y) such that $F(x,y) = z$, Amos Beimel et al.[BDKW14] show following lower bound about the agree problem of two functions $F_1, F_2 : (\{0,1\}^n \times \{0,1\}^n) \to \{0,1\}$: $\mathsf{C}(\texttt{agree}(F_1,F_2)) \geq \max\{\min\{\log \mathsf{Cov}^1(F_1), \log \mathsf{Cov}^0(F_2)\}, \min\{\log \mathsf{Cov}^0(F_1), \log \mathsf{Cov}^1(F_2)\}\} - \log(2n)$. It is natural to consider whether there is a clearer lower bound for the agree problem and it is easy to see the complexity of the agree problem is at most the complexity to solve the easiest one out of k functions, thus, we have following conjecture.

[1] See [Pan13] for a more detailed introduction of direct sum problems in communication complexity.

Conjecture 1.3. *Given k communication problems $F_i : (\{0,1\}^n \times \{0,1\}^n) \to \{0,1\}$, let $\mathsf{Cov}(F)$ denote the cover number of communication problem F, we have*

$$\log \mathsf{Cov}\left(\boldsymbol{agree}(F_1, F_2, \cdots, F_k)\right) \geq \min_{i\in[k]} \log \mathsf{Cov}(F_i) - O(\log n).$$

Finally, in all direct sum type question, particularly, in the case of cover number, an ideal situation is that there is a 'hardcore' of cover number, when we know some information about this hardcore, the residual hardness is just the result of the complexity of the hardcore minus the mount of known information. A potential hardcore of cover number may be some kind of generalized form of standard fooling set, it is well known that large standard fooling set implies large cover number, but not vice versa. So naturally, we have following question.

Question 1.4. *Is there a generalized form of fooling set which can be viewed as a dual form of cover number? Particularly, is large cover number implies some kind of fooling set?*

In this paper, we tackle these questions and make some progress about them.

1.1 Our results

All our results rely on following fact: there is a dual form of cover number, δ-fooling set, a concept generalized from the standard fooling set. Formally, we have following concept.

Definition 1.5 (δ-fooling set)**.** Let $S \subseteq (X \times Y) \times Z$ be a communication problem, we call a set $\Lambda \subseteq X \times Y$ a δ-fooling set of S if for any subset $\tilde{\Lambda} \subseteq \Lambda$ such that $\frac{|\tilde{\Lambda}|}{|\Lambda|} > \delta$, there is no monochromatic rectangle that covers all elements in the subset $\tilde{\Lambda}$.

Note that a standard fooling set Λ is just a special case of δ-fooling set where $\delta = 1/|\Lambda|$. It is easy to see that a δ-fooling set with small δ implies a large cover number lower bound. The harder direction is to show large cover number implies a δ-fooling set with small δ. This is done by the technique of "fortification". The term "fortification" is introduced by Moshkovitz [Mos14] to prove parallel repetition theorem. Then Dinur and Meir[DM18] introduced this idea into communication complexity and proved a fortification lemma of protocol size over rectangles. The spirit of this concept is that given some hard problem, we want to 'fortify' it into a hardcore such that if we already know some information about this hardcore, the residual hardness is just the result of the complexity of the hardcore minus the mount of known information. We observer that Dinur and Meir's fortification lemma can be generalized into a general form then apply it to the case of cover number. Formally, we have following result about fortification of cover number thus complete the harder direction of the duality.

Proposition 1.6 (Fortification of cover number)**.** *Let $S \subseteq (X \times Y) \times Z$ be a communication problem, there exists $\Lambda \subseteq X \times Y$ such that for any subset $\tilde{\Lambda} \subseteq \Lambda$, we have*

$$\mathsf{Cov}(\tilde{\Lambda}) \geq \frac{|\tilde{\Lambda}|}{|\Lambda|} \cdot \frac{\mathsf{Cov}(S)}{16 \log |X||Y|}.$$

Particularly, when $\frac{|\tilde{\Lambda}|}{|\Lambda|} > \frac{16 \log |X||Y|}{\mathsf{Cov}(S)}$, we have $\mathsf{Cov}(\tilde{\Lambda}) > 1$, this means Λ is a $\frac{16 \log |X||Y|}{\mathsf{Cov}(S)}$-fooling set.

Use this dual form of cover number, we are able to reprove the direct sum theorem of cover number.

Theorem 1.7. *Given two communication problems $S \subseteq (A\times B)\times O$ and $T \subseteq (P\times Q)\times Z$,we have* $\log \mathsf{Cov}\,(S \times T) \geq \log \mathsf{Cov}\,(S) + \log \mathsf{Cov}(T) - \log\log|P||Q| - 4$.

Along the way, we prove a new direct sum result of protocol size which imply a better direct sum theorem for two functions in terms of protocol size. This gives a positive answer to Conjecture 1.2.

Theorem 1.8. *Given two communication problem $S \subseteq (A\times B)\times O$ and $T \subseteq (P\times Q)\times Z$, we have*

$$\log \mathsf{L}\,(S\times T) \geq \log \mathsf{L}\,(S) + \log \mathsf{Cov}(T) - \log\log|P||Q| - 4$$

Corollary 1.9. *Given a communication problem $F : A\times B \to \{0,1\}$,*

$$\log \mathsf{L}\,(F\times F) \geq \log \mathsf{L}\,(F) + \Omega\left(\sqrt{\log \mathsf{L}\,(F)}\right) - \log\log|A||B| - 4.$$

For conjecture 1.1, our approach does not work due to that the measure of communication complexity is less structural than the measure of protocol size, and we leave this conjecture as an interesting open problem.

We also give a positive answer to Conjecture 1.3 in a stronger form which is a cover number lower bound for the agree problem of relations.

Theorem 1.10. *Let $S_i \subseteq X_i \times Y_i \times Z, i \in [k]$ be k two-party communication problems, we have*

$$\mathsf{Cov}\left(\boldsymbol{agree}(S_1,\ldots,S_k)\right) \geq \min_{i\in[k]}\left\{\frac{\mathsf{Cov}(S_i)}{16\log|X_i||Y_i|}\right\}.$$

1.2 Our approach

In this section, at first, we show how to generalize Dinur and Meir's fortification lemma with the right abstraction. Then by applying this general fortification lemma to the case of cover number, we have the fortification lemma of cover number and existence of δ-fooling set. Secondly, we take the direct sum theorem of cover number as a running example of proving direct sum type theorem using δ-fooling set. The direct sum theorem of protocol size and lower bound for the agree problem follow similar paradigm, that is using the δ-fooling set to construct a hardcore for the direct sum type problem.

Dinur and Meir's fortification lemma can be generalized into following setting: let Σ be a nonempty finite set, let $\mu : 2^{\Sigma} \to \mathbb{N}$ be a sub-additive measure over Σ with following properties:

- semipositivity: $\mu(\emptyset) = 0$ and if $\Lambda \subseteq \Sigma$ is not empty, $\mu(\Lambda) \geq 1$,
- subadditivity: given two subsets $\Lambda, \Lambda' \subseteq \Sigma$, $\mu(\Lambda \cup \Lambda') \leq \mu(\Lambda) + \mu(\Lambda')$.

And the general fortification lemma states following fact: there is a subset $\Lambda \subseteq \Sigma$ such that give any subset $\tilde{\Lambda} \subseteq \Lambda$, it holds that

$$\mu(\tilde{\Lambda}) \geq \frac{1}{4\log|\Sigma|} \cdot \frac{|\tilde{\Lambda}|}{|\Lambda|} \cdot \mu(\Lambda),$$

and $\mu(\Lambda) \geq \frac{1}{4}\mu(\Sigma)$. Given a communication problem $S \subseteq (X \times Y) \times Z$, given a rectangle $A \times B \subseteq X \times Y$, recall $\mathsf{L}(A \times B)$ denote the protocol size of the rectangle. Now give a fixed $A \subseteq X$, set $\mathsf{L}_{A\times}(B) = \mathsf{L}(A \times B)$ where $B \subseteq Y$, similarly we can define $\mathsf{L}_{\times B}$ for some fixed $B \subseteq Y$. It is easy to verify that $\mathsf{L}_{A\times}$(respectively $\mathsf{L}_{\times B}$) is a sub-additive measure over Y(respectively X). Dinur and Meir's original fortification lemma[DM18] is exactly about the two measures $\mathsf{L}_{A\times}$ and $\mathsf{L}_{\times B}$.

Now consider the measure of cover number, let Σ be any subset of $X \times Y$, cover number Cov is a sub-additive measure over Σ. Note that Σ is not necessarily a rectangle. Set $\Sigma = X \times Y$, by the general fortification lemma, there is a subset $\Lambda \subseteq X \times Y$ such that for any subset $\tilde{\Lambda} \subseteq \Lambda$,

$$\mathsf{Cov}(\tilde{\Lambda}) \geq \frac{1}{16\log|X||Y|} \cdot \frac{|\tilde{\Lambda}|}{|\Lambda|} \cdot \mathsf{Cov}(S).$$

Note that when $\frac{|\tilde{\Lambda}|}{|\Lambda|} > \frac{16\log|X||Y|}{\mathsf{Cov}(S)}$, $\mathsf{Cov}(\tilde{\Lambda}) > 1$, this means Λ is a $\frac{16\log|X||Y|}{\mathsf{Cov}(G)}$-fooling set.

Now we show how to use δ–fooling set to prove direct sum type theorem. The basic idea is to construct the hardcore of the direct sum problem from hardcore of each problem. Cartesian product of each problem's δ–fooling set is a hardcore of the direct sum of problems, but sometimes, to prove a stronger results, we need to construct a more delicated hardcore.

Take the direct sum problem of cover number as an example, given two communication problems $S \subseteq (A \times B) \times O$ and $T \subseteq (P \times Q) \times Z$, let Λ be a δ-fooling set for problem T, we want to lower bound the cover number of their direct sum problem $S \times T$. Given any $(p, q) \in \Lambda$, note that $(A \times \{p\}) \times (B \times \{q\})$ is a rectangle of $S \times T$, and we construct the hardcore for $S \times T$ to be the collection of all such rectangles $(A \times \{p\}) \times (B \times \{q\})$ for every $(p, q) \in \Lambda$. Formally, the hardcore is simply $\cup_{(p,q)\in\Lambda}(A \times \{p\}) \times (B \times \{q\})$.

Now we give the intuition that why this hardcore is indeed hard. At first, note that every such rectangle $(A \times \{p\}) \times (B \times \{q\})$ will need at least $\mathsf{Cov}(S)$ monochromatic rectangles to cover it. Since there are $|\Lambda|$ such rectangles, if we allow multiplicity, the total number to cover all such rectangles is at least $|\Lambda| \cdot \mathsf{Cov}(S)$. Now we handle the problem of multiplicity since a monochromatic rectangle R could cover elements from different rectangles $(A \times \{p\}) \times (B \times \{q\})$ for different $(p, q) \in \Lambda$. Fortunately, we can show a monochromatic rectangle R could cover elements from at most $\delta|\Lambda|$ different rectangles. Denote $\{(p, q)|\exists((a, p), (b, q)) \in R\}$ by $R|_T$, if R is monochromatic, then $R|_T$ is also monochromatic rectangle which contains no more than $\delta|\Lambda|$ such (p, q), otherwise it would contradict that Λ is a δ–fooling set of T. This means a monochromatic rectangle R could cover elements from at most $\delta|\Lambda|$ different rectangles, thus we need at least $|\Lambda| \cdot \mathsf{Cov}(S)/\delta|\Lambda| = \mathsf{Cov}(S)/\delta$ monochromatic rectangles to cover the hardcore $\cup_{(p,q)\in\Lambda}(A \times \{p\}) \times (B \times \{q\})$.

1.3 Organization of the rest of the paper

We provide the necessary preliminaries in Section 2. In Section 3, we define the δ-fooling set, present the general fortification lemma then apply it to the case of cover number. In Section 4, we reprove the direct sum theorem of cover number and prove a new direct sum theorem of protocol size. In Section 5, we prove the cover lower bound for the agree problem. Finally, in Section 6, we conclude and discuss some future directions.

2 Preliminaries

In this section, we provide some basic notations, definitions and facts. Let $\mathbb{N}$ be the set of nature number, for any $n \in \mathbb{N}$, we denote by $[n]$ the set $\{1, \ldots, n\}$. We often use bold font to indicate $\mathbf{x} \in X^n$ is a vector, and denote the i-th coordinate of the vector by $\mathbf{x}_i$.

We assume the readers are familiar with the basic knowledge of communication complexity, a more detailed introduction of communication complexity can be found in textbooks such as [KN97, RY20].

Definition 2.1 (Two party communication problems)**.** In a two party communication problem $S \subseteq (X \times Y) \times Z$, there are two involved players–Alice and Bob who need to solve following task: Alice is given an input $x \in X$ and Bob is given an input $y \in Y$, they need to output a element $z \in Z$ such that $(x, y, z) \in S$.

Rectangle cover and cover number

Definition 2.2. Given a communication problem $S \subseteq (X \times Y) \times Z$, let $R = A \times B \subset X \times Y$ be a rectangle, if for every $(x, y) \in A \times B$, $(x, y, z) \in S$, we say rectangle R is monochromatic with color z or z-monochromatic for short. Let $\Sigma \subseteq X \times Y$ and χ be a set of monochromatic rectangles of S, we say χ is a rectangle cover for Σ, or simply χ covers Σ, if for every element $(x, y) \in \Sigma$ there is a monochromatic rectangle $R \in \chi$ such that $(x, y) \in R$.

The cover number of Σ, denoted by $\mathsf{Cov}(\Sigma)$, is the minimum number of monochromatic rectangles to cover Σ, formally,

$$\mathsf{Cov}(\Sigma) = \min_{\chi \text{covers } \Sigma} |\chi|.$$

Particularly, when $\Sigma = X \times Y$, we simply write $\mathsf{Cov}(S)$, that is the cover number of communication problem S.

Deterministic protocol

Definition 2.3. A deterministic protocol $\Pi : X \times Y \to Z$ for a communication problem $S \subseteq (X \times Y) \times Z$ is a rooted binary tree with following structure:

- Every node v in the tree belongs to Alice or Bob and is associated with a rectangle $R_v = X_v \times Y_v \subseteq X \times Y$. Particularly, the root of protocol tree is associated with the rectangle $X \times Y$.

- Given an internal node v, let v_0, v_1 be two children of v. Recall v is associated with a rectangle $R_v = X_v \times Y_v$, if v is owned by Alice, then v_0 is associated with $X_{v_0} \times Y_v$, v_1 is associated with $X_{v_1} \times Y_v$ where $X_{v_0} \cap X_{v_1} = \emptyset$ and $X_{v_0} \cup X_{v_1} = X_v$; if v is owned by Bob, then v_0 is associated with $X_v \times Y_{v_0}$, v_1 is associated with $X_v \times Y_{v_1}$ where $Y_{v_0} \cap Y_{v_1} = \emptyset$ and $Y_{v_0} \cup Y_{v_1} = Y_v$.
- Every leaf node ℓ is associated with a monochromatic rectangle R_ℓ with color z and z is the output of the protocol.

Communication complexity and protocol size

Definition 2.4. Given a protocol tree Π, its depth $\mathsf{D}(\Pi)$ is the length of the longest path from the root to a leaf in the tree. Given a communication problem $S \subseteq (X \times Y) \times Z$, the (deterministic) communication complexity $\mathsf{C}(S)$ of communication problem S is the minimum $\mathsf{D}(\Pi)$ over all protocol Π for the problem S. Given a protocol tree Π, its protocol size $\mathsf{L}(\Pi)$ is the number of leaves of the tree. Given a communication problem S, its protocol size $\mathsf{L}(S)$ is minimum $\mathsf{L}(\Pi)$ over all protocol Π for the problem S.

It is well known that protocol size is sub-additive over rectangles. Formally, we have following fact.

Fact 2.5. Given a communication problem $S \subseteq (X \times Y) \times Z$, let $A \times B \subseteq X \times Y$ and $\mathsf{L}(A \times B)$ be the protocol size to solve problem S when restricted to rectangle $A \times B$, we have

- $\mathsf{L}\left((A_0 \cup A_1) \times B\right) \leq \mathsf{L}\left(A_0 \times B\right) + \mathsf{L}\left(A_1 \times B\right)$.
- $\mathsf{L}\left(A \times (B_0 \cup B_1)\right) \leq \mathsf{L}\left(A \times B_0\right) + \mathsf{L}\left(A \times B_1\right)$.

Fact 2.6. [KN97] For every communication problem S it holds that

$$\log \mathsf{L}(S) \leq \mathsf{C}(S) \leq 2 \log \mathsf{L}(S)$$

and hence $\mathsf{C}(S) = \Theta(\log \mathsf{L}(S))$.

Fact 2.7. [KN97]Let communication problem $F : X \times Y \to \{0, 1\}$ be a function, then

$$\log \mathsf{Cov}(F) = \Omega\left(\sqrt{\mathsf{C}(F)}\right).$$

3 Generalized Fooling Set and Fortification of Cover Number

In this section, we introduce a generalized form of standard fooling set called the δ-fooling set.

Definition 3.1 (δ-fooling set)**.** Let $S \subseteq (X \times Y) \times Z$ be a communication problem, we call a set $\Lambda \subseteq X \times Y$ a δ-fooling set of S if for any subset $\tilde{\Lambda} \subseteq \Lambda$ such that $\frac{|\tilde{\Lambda}|}{|\Lambda|} > \delta$, there is no monochromatic rectangle that covers all elements in the subset $\tilde{\Lambda}$.

The δ-fooling set can be viewed as a dual form of cover number, given a communication problem, a large cover number for this problem is equivalent to there is a δ-fooling set with small δ for this problem. At first, we show the easy direction, that is a δ-fooling set with small δ implies large cover number. This mimics the effect of standard fool set.

Proposition 3.2. *Let $S \subseteq (X \times Y) \times Z$ be a communication problem, let $\Lambda \subseteq X \times Y$ be a δ-fooling set of S, then $\mathsf{Cov}(\Lambda) \geq 1/\delta$.*

Proof. Since any monochromatic rectangle can only cover at most $\delta|\Lambda|$ elements from Λ, at least $1/\delta$ monochromatic rectangles are required to cover all elements from Λ. □

Now we present the other direction: that is large cover number implies δ-fooling set with small δ. This is achieved by applying the general fortification lemma to the case of cover number. At first, we need a notion called sub-additive measure over set.

Definition 3.3. Let Σ be a nonempty finite set, a sub-additive measure over set Σ is a function $\mu : 2^{\Sigma} \to \mathbb{N}$ with following properties:

- semipositivity: $\mu(\emptyset) = 0$ and if $\Lambda \subseteq \Sigma$ is not empty, $\mu(\Lambda) \geq 1$,
- subadditivity: given two subsets $\Lambda, \Lambda' \subseteq \Sigma$, $\mu(\Lambda \cup \Lambda') \leq \mu(\Lambda) + \mu(\Lambda')$.

Given a communication problem $S \subseteq (X \times Y) \times Z$, the cover number is a sub-additive measure over any subset Σ of $X \times Y$. Formally we have following fact.

Fact 3.4. Give a communication problem $S \subseteq (X \times Y) \times Z$, let $\Sigma \subseteq X \times Y$ be a subset, then cover number Cov according to the communication problem S is a sub-additive measure over Σ.

Proof. Due to the importance of this fact, we verify cover number Cov is indeed subadditive. Given two subsets $\Lambda, \Lambda' \subseteq \Sigma$ and these two sets may not necessarily be rectangles. Let $\mathcal{R}$ be the collection of monochromatic rectangles which cover Λ, or formally $\Lambda \subseteq \cup_{R \in \mathcal{R}} \mathcal{R}$. Let $\mathcal{R}'$ be the collection of monochromatic rectangles which cover Λ'. It is easy to see $\mathcal{R} \cup \mathcal{R}'$ covers $\Lambda \cup \Lambda'$ because we allow overlapping between rectangles. Moreover $|\mathcal{R} \cup \mathcal{R}'| \leq |\mathcal{R}| + |\mathcal{R}'|$, thus the subadditivity of Cov follows. □

Next we define the notion of general fortification.

Definition 3.5. Let Σ be a nonempty finite set, μ be a sub-additive measure over set Σ and Λ be a subset of Σ. Given any subset $\tilde{\Lambda} \subseteq \Lambda$, we say Λ is ρ-fortified with respect to measure μ, if for any such $\tilde{\Lambda}$, it holds that

$$\mu(\tilde{\Lambda}) \geq \rho \cdot \frac{|\tilde{\Lambda}|}{|\Lambda|} \cdot \mu(\Lambda).$$

Lemma 3.6 (General fortification lemma)**.** *Given a set Σ and a sub-additive measure μ over Σ. There exists $\Lambda \subseteq \Sigma$ such that*

- *Λ is $\frac{1}{4 \log |\Sigma|}$-fortified*

- *and* $\mu(\Lambda) \geq \frac{1}{4}\mu(\Sigma)$.

The proof of the general fortification lemma is similar to its less general form in [DM18] and is deferred to Appendix A. Now we can apply it to Fact 3.4 to obtain the fortification of cover number.

Proposition 3.7 (Fortification of cover number)**.** *Let $S \subseteq (X \times Y) \times Z$ be a communication problem, there exists $\Lambda \subseteq X \times Y$ such that for any subset $\tilde{\Lambda} \subseteq \Lambda$, we have*

$$\mathsf{Cov}(\tilde{\Lambda}) \geq \frac{|\tilde{\Lambda}|}{|\Lambda|} \cdot \frac{\mathsf{Cov}(S)}{16 \log |X||Y|}.$$

Particularly, when $\frac{|\tilde{\Lambda}|}{|\Lambda|} > \frac{16 \log |X||Y|}{\mathsf{Cov}(S)}$, we have $\mathsf{Cov}(\tilde{\Lambda}) > 1$, this means Λ is a $\frac{16 \log |X||Y|}{\mathsf{Cov}(S)}$-fooling set.

4 Direct Sum Theorems from Fortification

4.1 Direct sum theorem of cover number, revisit

In this section, we revisited the direct sum problem of cover number and present a simpler and conceptual proof. In our proof, we only use Proposition 3.7 and a double counting argument. Formally, we have following theorem.

Theorem 4.1. *Given two communication problems $S \subseteq (A \times B) \times O$ and $T \subseteq (P \times Q) \times Z$, let Λ be a δ-fooling set for problem T, we have*

$$\mathsf{Cov}\left(S \times T\right) \geq \mathsf{Cov}\left(S\right)/\delta.$$

Particularly, by Proposition 3.7, we have

$$\log \mathsf{Cov}\left(S \times T\right) \geq \log \mathsf{Cov}\left(S\right) + \log \mathsf{Cov}(T) - \log\log |P||Q| - 4.$$

Before proving the theorem, we want to state following simple but important fact about rectangles of $S \times T$.

Fact 4.2. Given two communication problems $S \subseteq (A \times B) \times O$ and $T \subseteq (P \times Q) \times Z$, let $R \subseteq (A \times P) \times (B \times Q)$ be a monochromatic rectangle of $S \times T$. Denote the set $\{(a,b) | \exists ((a,p),(b,q)) \in R\}$ by $R|_S$ and similarly $\{(p,q) | \exists ((a,p),(b,q)) \in R\}$ by $R|_T$, we have $R|_S$(respectively $R|_T$) is a monochromatic rectangle of S(respectively T).

Proof. We prove it for $R|_S$, the case for $R|_T$ is similar. At first, we will show if $(a,b),(a',b')$ are contained in $R|_S$, so are $(a',b),(a,b')$. If $(a,b),(a',b')$ are contained in $R|_S$, there must be two elements $((a,p),(b,q)),((a',p'),(b',q')) \in R$, that is $((a,p),(b',q')),((a',p'),(b,q)) \in R$, which means $(a',b),(a,b')$ are contained in $R|_S$. Furthermore, since R is monochromatic with some color $(o,z) \in O \times Z$, every $(a,b) \in R|_S$ can be colored with o, thus $R|_S$ is a monochromatic rectangle of S as required. □

Proof. (of Theorem 4.1)Let χ be a rectangle cover of $S \times T$, we will prove $|\chi| \geq \mathsf{Cov}\left(S\right)/\delta$. Given any $(p,q) \in \Lambda$, $(A \times \{p\}) \times (B \times \{q\})$ is a rectangle of $S \times T$, every such rectangle will need at least $\mathsf{Cov}(S)$ monochromatic rectangle to cover it. Since there are $|\Lambda|$ such rectangles, if we allow multiplicity, the total number to cover all such rectangles is at least $|\Lambda| \cdot \mathsf{Cov}(S)$. Formally, let $R \in \chi$, denote

$$\left(R \cup (A \times \{p\}) \times (B \times \{q\})\right)|_S$$

by $R_{(p,q)}$, we have

$$\sum_{R \in \chi} \sum_{(p,q) \in \Lambda} \mathbf{1}_{R_{(p,q)} \neq \emptyset} = \sum_{(p,q) \in \Lambda} \left(\sum_{R \in \chi} \mathbf{1}_{R_{(p,q)} \neq \emptyset} \right) \geq |\Lambda| \cdot \mathsf{Cov}(S)$$

Now we handle the problem of multiplicity since a monochromatic rectangle R in χ could cover elements from different rectangles $(A \times \{p\}) \times (B \times \{q\})$ for different $(p,q) \in \Lambda$, but fortunately a monochromatic rectangle R in χ could cover elements from at most $\delta|\Lambda|$ different rectangles. Formally, we have

$$\sum_{(p,q) \in \Lambda} \mathbf{1}_{R_{(p,q)} \neq \emptyset} \leq \delta|\Lambda|,$$

if not, by Fact 4.2, we know that $R|_T$ is a monochromatic rectangle which contains more than $\delta|\Lambda|$ such (p,q), this contradicts that Λ is a δ-fooling set of T. Finally, we have

$$|\chi| = \sum_{R \in \chi} \mathbf{1} \geq \sum_{R \in \chi} \frac{\sum_{(p,q) \in \Lambda} \mathbf{1}_{R_{(p,q)} \neq \emptyset}}{\delta|\Lambda|} \geq |\Lambda| \cdot \mathsf{Cov}(S)/\delta|\Lambda| = \mathsf{Cov}(S)/\delta.$$

□

4.2 A direct sum theorem of protocol size

In this section, we prove a new direct sum theorem about protocol size. The proof is inspired by ideas in [DM18]. Formally, we have following theorem.

Theorem 4.3. *Given two communication problems $S \subseteq (A \times B) \times O$ and $T \subseteq (P \times Q) \times Z$, let Λ be a δ-fooling set for cover number of T, we have*

$$\mathsf{L}\left(S \times T\right) = \mathsf{L}\left(S\right)/\delta.$$

Particularly, by Proposition 3.7, we have

$$\log \mathsf{L}\left(S \times T\right) = \log \mathsf{L}\left(S\right) + \log \mathsf{Cov}(T) - \log\log |P||Q| - 4.$$

To prove this theorem, at first, we need to recall some notations. Let $R \subseteq (A \times P) \times (B \times Q)$ be a rectangle of $S \times T$. Denote the set $\{(a,b)|\exists((a,p),(b,q)) \in R\}$ by $R|_S$ and similarly $\{(p,q)|\exists((a,p),(b,q)) \in R\}$ by $R|_T$. Furthermore, given any $(p,q) \in \Lambda$, denote $\left(R \cup (A \times \{p\}) \times (B \times \{q\})\right)|_S$ by $R_{(p,q)}$.

The sub-additive measure over protocol tree. We introduce the definition of sub-additive measure over protocol tree as follows.

Definition 4.4 ([DM18])**.** Given a rooted binary tree T and let V be the set of nodes of tree T, we say that $\phi : V \to \mathbb{N}$ is a sub-additive measure on T if for every vertex v with children v_0 and v_1 in T it holds that $\phi(v) \leq \phi(v_0) + \phi(v_1)$.

Now we define a special sub-additive measure over protocol tree following the similar idea in [DM18].

Definition 4.5. Given a protocol tree Π for $S \times T$, let π be a node in the protocol tree Π, denote the rectangle associated with the node π by $R_\pi \subseteq (A \times P) \times (B \times Q)$, let Λ be a δ-fooling set for cover number of T, we define a measure ϕ on all such π as follows:

$$\phi(\pi) = \frac{1}{|\Lambda|} \sum_{(p,q)\in\Lambda} \mathsf{L}\left(R_{\pi(p,q)}\right).$$

Intuitively, the measure ϕ is just the average complexity of all such rectangles $R_{\pi(p,q)}$ where $(p,q) \in \Lambda$. It easy to verify following fact about the measure ϕ.

Fact 4.6. The measure ϕ is a sub-additive measure on protocol tree Π. Furthermore, ϕ assigns $\mathsf{L}(A \times B) = \mathsf{L}(S)$ to the root of Π.

Proof. At first, the measure ϕ is sub-additive since, by Fact 2.5, for every fixed (p,q), the measure $\mathsf{L}\left(R_{\pi(p,q)}\right)$ is sub-additive over the protocol tree Π. Furthermore, ϕ assigns $\mathsf{L}(A \times B)$ to the root of Π, since when π is the root, $R_{\pi(p,q)}$ simply is $A \times B$, for every (p,q). □

We will also need following fact which claims for each leaf in the protocol tree, its measurement is small.

Fact 4.7. Given a protocol Π which solves $S \times T$ and ℓ is a leaf of Π, then $\phi(\ell) \leq \delta$.

Proof. Let R_ℓ be the rectangle associated with the leaf ℓ. Since ℓ is a leaf, R_ℓ is monochromatic and $\mathsf{L}(R_\ell) \leq 1$, this means for every $(p,q) \in \Lambda$, $0 \leq \mathsf{L}(R_{\ell(p,q)}) \leq 1$, and furthermore $R_\ell|_S$ is monochromatic.

Let $\tilde{\Lambda}$ be the set of all (p,q) such that $\mathsf{L}(R_{\ell(p,q)}) \neq 0$. Since $\tilde{\Lambda}$ is contained in monochromatic rectangle $R|_S$, this means $|\tilde{\Lambda}| \leq \delta|\Lambda|$ due to Λ is a δ-fooling set for cover number of T. Now we are ready to bound $\phi(\ell)$, that is

$$\phi(\ell) = \frac{1}{|\Lambda|} \sum_{(p,q)\in\Lambda} \mathsf{L}(R_{\ell(p,q)}) = \frac{1}{|\Lambda|} \sum_{(p,q)\in\Lambda} \mathbf{1}_{\mathsf{L}(R_{\ell(p,q)})\neq 0} = \frac{|\tilde{\Lambda}|}{|\Lambda|} \leq \delta.$$

□

Now we are ready to prove our theorem about protocol size.

Proof. (of Theorem 4.3)Given a protocol Π for $S \times T$, let r be the root of protocol Π, by the subadditivity of ϕ,

$$\phi(r) \leq \sum_{\ell \text{ is a leaf}} \phi(\ell).$$

By Fact 4.6 and Fact 4.7, we have

$$\mathsf{L}(S) \leq \mathsf{L}(\Pi) \cdot \delta,$$

that is

$$\mathsf{L}(\Pi) \geq \mathsf{L}(S)/\delta.$$

□

By Theorem 4.3, Fact 2.6 and Fact 2.7, we have following corollary.

Corollary 4.8. *Given a communication problem $F : A \times B \to \{0,1\}$,*

$$\log \mathsf{L}\left(F \times F\right) \geq \log \mathsf{L}\left(F\right) + \Omega\left(\sqrt{\log \mathsf{L}\left(F\right)}\right) - \log\log |A||B| - 4.$$

5 Cover Number Lower Bound for the Agree Problem

In this section, we prove a stronger cover number lower bound for the agree problem, at first, we present a more general form of agree problem of relations.

Definition 5.1. Let $S_i \subseteq X_i \times Y_i \times Z, i \in [k]$ be k communication problems, the agree problem $\texttt{agree}(S_1, \ldots, S_k) \subseteq \left((\times_{i=1}^k X_i) \times (\times_{i=1}^k Y_i)\right) \times Z$ is following relation:

$$\texttt{agree}(S_1, \ldots, S_k) = \{(\mathbf{x}, \mathbf{y}, z) | \text{ for some } i, (\mathbf{x}_i, \mathbf{y}_i, z) \in S_i\}.$$

Theorem 5.2. *Let $S_i \subseteq X_i \times Y_i \times Z, i \in [k]$ be k communication problems, for each $i \in [k]$, S_i have a δ_i-fooling set Λ_i, we have a $(\max_i \delta_i)$-fooling set $\mathbf{\Lambda}$ for the problem $\texttt{agree}(S_1, \ldots, S_k)$, and the set $\mathbf{\Lambda}$ is simply the following:*

$$\mathbf{\Lambda} = \{(\mathbf{x}, \mathbf{y}) | \textit{ for every } i, (\mathbf{x}_i, \mathbf{y}_i) \in \Lambda_i\}.$$

Furthermore, by Proposition 3.7 and Proposition 3.2, we have

$$\mathsf{Cov}\left(\texttt{agree}(S_1, \ldots, S_k)\right) \geq \min_{i \in [k]} \left\{ \frac{\mathsf{Cov}(S_i)}{16 \log |X_i||Y_i|} \right\}.$$

At first, similar to Fact 4.2, we have following fact.

Fact 5.3. Denote $\times_{i=1}^k X_i$ by $\mathbf{X}$ and $\times_{i=1}^k Y_i$ by $\mathbf{Y}$, let $R \subseteq \mathbf{X} \times \mathbf{Y}$ be a rectangle, denote $\{(\mathbf{x}_i, \mathbf{y}_i) | (\mathbf{x}, \mathbf{y}) \in \mathbf{X} \times \mathbf{Y}\}$ by $R|_i$, $R|_i \subseteq X_i \times Y_i$ is a rectangle, for every $i \in [k]$.

Proof. (of Theorem 5.2)Let δ be $\max_i \delta_i$, and $R \subseteq \mathbf{X} \times \mathbf{Y}$ be a rectangle, we will show if R contains more than $\delta|\mathbf{\Lambda}|$ elements from $\mathbf{\Lambda}$, R can not be monochromatic, that is there is no $i \in [k]$ such that $R|_i$ is monochromatic. Note that by Fact 5.3, for every $i \in [k]$, $R|_i$ is a rectangle, and we have

$$\delta|\mathbf{\Lambda}| < |R \cup \mathbf{\Lambda}| \leq \prod_{i\in[k]} |R|_i \cup \Lambda_i| \leq |R|_i \cup \Lambda_i| \cdot \prod_{j\neq i} |\Lambda_j|,$$

this means for every $i \in [k]$, $|R|_i \cup \Lambda_i| > \delta|\Lambda_i| \geq \delta_i|\Lambda_i|$, since Λ_i is δ_i-fooling set of S_i, $R|_i$ can not be monochromatic for every i as required. □

Remark 5.4. Now we discuss the other two problems introduced by Amos Beimel et al.[BDKW14]: the choose problem and the eliminate problem. The choose problem asks the players to output (i, z) where $(\mathbf{x}_i, \mathbf{y}_i, z) \in S_i$, that is the players also need to specify which problem they solve out of the k problems. The eliminate problem asks the players to output a vector $\mathbf{z} \in Z^k$, such that there exists at least one $i \in [k]$,$(\mathbf{x}_i, \mathbf{y}_i, \mathbf{z}_i) \notin S_i$. Note the agree problem can be reduced to the choose problem, so any lower bound of the agree problem is a lower bound of the choose problem. The case of eliminate problem is more complicated. When all $S_1, \ldots, S_k$ are functions, the eliminate problem can be reduced to the agree problem, but this reduction does not work when the problems are relations. The reason that our approach doesn't work in the case of the eliminate problem is that a non-monochromatic rectangle of the eliminate problem must contain all colors $\mathbf{z} \in Z^n$, while a non-monochromatic rectangle R of the agree problem only needs to satisfy that for every $i \in [k]$,$R|_i$ contain all $z \in Z$. To make things easier, we can assume, every S_i is the same function $G : X \times Y \to Z$, the situation here is similar to those in the lifting theorems, after communicating about $\mathsf{C}(G)$ bits, we need to show the residual problem contains all colors $\mathbf{z} \in Z^n$. It is unclear how to achieve this with δ-fooling set.

6 Conclusion and Discussion

We conclude with some discussion about our results and future direction. The first question is can we fortify other measures in communication complexity besides cover number? Particularly, can we fortify the protocol size L in a similar way like cover number? Here we show this may not be the case. Given a communication problem $S \subseteq (X \times Y) \times Z$, suppose there is a subset $\Lambda \subseteq X \times Y$ such that give any subset $\tilde{\Lambda} \subseteq \Lambda$, it holds that $\mathsf{L}(\tilde{\Lambda}) \geq \rho \cdot \frac{|\tilde{\Lambda}|}{|\Lambda|} \cdot \mathsf{L}(\Lambda)$, where $\mathsf{L}(\tilde{\Lambda})$ means the minimum protocol size to solve all the inputs (x, y) from $\tilde{\Lambda}$. Note that in this case, $\mathsf{Cov}(\Lambda) \geq \rho \cdot \mathsf{L}(\Lambda)$. Furthermore, there are communication problems such that their cover number is exponential smaller than their protocol size, so in general $\rho \cdot \mathsf{L}(\Lambda)$ must be exponential smaller than $\mathsf{L}(S)$ thus no same strong fortification lemma can be proved for protocol size.

So we should consider other measures which avoid such large gap. An interesting question is whether we can fortify any useful measures in randomized communication complexity? Note that if we relax rectangle cover to cover of nearly monochromatic rectangles, the lemma also works, the issue here is we don't know whether a small cover number of nearly monochromatic rectangles implies a small randomize complexity. Besides measures in communication complexity, we can apply the fortification lemma to other measures such as the measure of entropy H. Let $\mathbf{X}_1, \mathbf{X}_2, \cdots, \mathbf{X}_n$ be n joint distributed random variables, the measure entropy H is sub-additive over these random variables, thus can be fortified. It is interesting that whether these fortifications lead to further applications.

References

[BDKW14] Amos Beimel, Sebastian Ben Daniel, Eyal Kushilevitz, and Enav Weinreb. Choosing, agreeing, and eliminating in communication complexity. *Comput. Complex.*, 23(1):1–42, 2014.

[DM18] Irit Dinur and Or Meir. Toward the KRW composition conjecture: Cubic formula lower bounds via communication complexity. *Comput. Complex.*, 27(3):375–462, 2018.

[FKNN95] Tomás Feder, Eyal Kushilevitz, Moni Naor, and Noam Nisan. Amortized communication complexity. *SIAM J. Comput.*, 24(4):736–750, 1995.

[KKN95] Mauricio Karchmer, Eyal Kushilevitz, and Noam Nisan. Fractional covers and communication complexity. *SIAM J. Discret. Math.*, 8(1):76–92, 1995.

[KN97] Eyal Kushilevitz and Noam Nisan. *Communication complexity.* Cambridge University Press, 1997.

[KRW91] M. Karchmer, R. Raz, and A. Wigderson. Super-logarithmic depth lower bounds via direct sum in communication complexity. In *[1991] Proceedings of the Sixth Annual Structure in Complexity Theory Conference*, pages 299–304, 1991.

[Mos14] Dana Moshkovitz. Parallel repetition from fortification. In *55th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2014, Philadelphia, PA, USA, October 18-21, 2014*, pages 414–423. IEEE Computer Society, 2014.

[Pan13] Denis Pankratov. Direct sum questions in classical communication complexity (master's thesis). 2013.

[RY20] Anup Rao and Amir Yehudayoff. *Communication Complexity: and Applications.* Cambridge University Press, 2020.

A The Proof of General Fortification Lemma

The general fortification lemma is proved in a similar way to its less general form in [DM18]. And for completeness of this paper, we present it here. At first, we show a so called the weak fortification.

Proposition A.1. *Given a set Σ, a sub-additive measure μ over Σ and $0 < \rho < 1$, there exists $\Lambda_1 \subseteq \Sigma$ such that:*

- *for every $\tilde{\Lambda} \subseteq \Lambda_1$, it holds that*

$$\mu(\tilde{\Lambda}) \geq \rho \cdot \frac{|\tilde{\Lambda}|}{|\Sigma|} \cdot \mu(\Sigma).$$

- $\mu\left(\Lambda_1\right) \geq (1-\rho) \cdot \mu(\Sigma)$.

Proof. Let $\Lambda_{\max} \subseteq \Sigma$ be a maximal subset under the order of set inclusion that satisfies

$$\mu\left(\Lambda_{\max}\right) < \rho \cdot \frac{|\Lambda_{\max}|}{|\Sigma|} \cdot \mu(\Sigma). \tag{A.1}$$

Let $\Lambda_1 \overset{\text{def}}{=} \Sigma - \Lambda_{\max}$, by the subadditivity of the measure μ, we have

$$\mu(\Sigma) = \mu(\Lambda_1 \cup \Lambda_{\max}) \leq \mu(\Lambda_1) + \mu(\Lambda_{\max}),$$

thus by rearranging above inequality, we have obtained the second item in this proposition, that is

$$\mu\left(\Lambda_1\right) \geq \mu(\Sigma) - \mu(\Lambda_{\max}) > \mu(\Sigma) - \rho \cdot \frac{|\Lambda_{\max}|}{|\Sigma|} \cdot \mu(\Sigma) \geq (1-\rho) \cdot \mu(\Sigma).$$

Now to obtain the first item of this proposition, for the sake of contradiction, suppose that there is a nonempty subset $\tilde{\Lambda} \subseteq \Lambda_1$, such that $\mu(\tilde{\Lambda}) < \rho \cdot \frac{|\tilde{\Lambda}|}{|\Sigma|} \cdot \mu(\Sigma)$. Then, this would imply that

$$\begin{aligned}
\mu\left(\tilde{\Lambda} \cup \Lambda_{\max}\right) &\leq \mu(\tilde{\Lambda}) + \mu\left(\Lambda_{\max}\right), \text{by subadditivity of } \mu \\
&< \rho \cdot \frac{|\tilde{\Lambda}|}{|\Sigma|} \cdot \mu(\Sigma) + \rho \cdot \frac{|\Lambda_{\max}|}{|\Sigma|} \cdot \mu(\Sigma), \text{ by assumptions on } \tilde{\Lambda} \text{ and } \Lambda_{\max} \\
&= \rho \cdot \frac{\left|\tilde{\Lambda} \cup \Lambda_{\max}\right|}{|\Sigma|} \cdot \mu(\Sigma).
\end{aligned}$$

It turns out that $\tilde{\Lambda} \cup \Lambda_{\max}$ is a set that satisfies Inequality (A.1) and that strictly contains $\Lambda_{\max}$, thus contradicting the maximality of $\Lambda_{\max}$. Hence, no such set $\tilde{\Lambda}$ exists, the first item of this Proposition holds. □

The above lemma is weak because the measure of $\tilde{\Lambda}$ is propositional to its density in Σ rather than Λ, to proceed, we need following fact about "inverse fortification".

Proposition A.2. *Given a set Σ and a sub-additive measure μ over Σ, for every $c \geq 1$, there exists a subset $\Lambda_0 \subseteq \Sigma$ such that for every $\tilde{\Lambda} \subseteq \Lambda_0$ it holds that*

$$\frac{|\tilde{\Lambda}|}{|\Lambda_0|} \geq \left(\frac{\mu(\tilde{\Lambda})}{\mu\left(\Lambda_0\right)}\right)^c \tag{A.2}$$

and

$$\mu\left(\Lambda_0\right) \geq \left(\frac{1}{|\Sigma|}\right)^{\frac{1}{c}} \cdot \mu(\Sigma). \tag{A.3}$$

Proof. At first, we set Λ_0 to be a minimal set under the order of set inclusion that satisfies

$$\frac{|\Lambda_0|}{|\Sigma|} \leq \left(\frac{\mu\left(\Lambda_0\right)}{\mu(\Sigma)}\right)^c$$

Observe that Λ_0 indeed satisfies Inequality (A.2): if not, there must be a proper subset $\tilde{\Lambda} \subsetneq \Lambda_0$ which satisfies

$$\frac{|\tilde{\Lambda}|}{|\Lambda_0|} < \left(\frac{\mu(\tilde{\Lambda})}{\mu\left(\Lambda_0\right)}\right)^c.$$

and this would have implied that

$$\frac{|\tilde{\Lambda}|}{|\Sigma|} = \frac{|\tilde{\Lambda}|}{|\Lambda_0|} \cdot \frac{|\Lambda_0|}{|\Sigma|} < \left(\frac{\mu(\tilde{\Lambda})}{\mu\left(\Lambda_0\right)}\right)^c \cdot \left(\frac{\mu\left(\Lambda_0\right)}{\mu(\Sigma)}\right)^c = \left(\frac{\mu(\tilde{\Lambda})}{\mu(\Sigma)}\right)^c$$

thus contradicting the minimality of Λ_0. Now it remains to show that Λ_0 satisfies Inequality (A.3). Recall that we set Λ_0 to satisfy

$$\frac{|\Lambda_0|}{|\Sigma|} \leq \left(\frac{\mu\left(\Lambda_0\right)}{\mu(\Sigma)}\right)^c,$$

by rearranging above inequality, we have

$$\mu\left(\Lambda_0\right) \geq \left(\frac{|\Lambda_0|}{|\Sigma|}\right)^{\frac{1}{c}} \cdot \mu(\Sigma) \geq \left(\frac{1}{|\Sigma|}\right)^{\frac{1}{c}} \cdot \mu(\Sigma)$$

as required. □

Finally, we are ready to prove our general fortification lemma.

Proof. (Proof of Lemma 3.6). Our goal is to find a subset $\Lambda \subseteq \Sigma$ such that

- Λ is $\frac{1}{4\log|\Sigma|}$-fortified,
- and $\mu\left(\Lambda\right) \geq \frac{1}{4} \cdot \mu(\Sigma)$

Now we apply Proposition A.2 to Σ with $c = \log|\Sigma|$ and obtain a subset $\Lambda_0 \subseteq \Sigma$. Then, we apply Proposition A.1 to Λ_0 with $\rho = \frac{1}{2\log|\Sigma|}$, thus obtaining a subset $\Lambda_1 \subseteq \Lambda_0$. Finally, we choose Λ to be Λ_1. We prove that Λ has the required properties. At first, we show $\mu\left(\Lambda\right) \geq \frac{1}{4} \cdot \mu(\Sigma)$. Note that by Proposition A.1, it holds that

$$\mu\left(\Lambda\right) \geq \left(1 - \frac{1}{2\log|\Sigma|}\right) \cdot \mu\left(\Lambda_0\right) \geq \frac{1}{2} \cdot \mu\left(\Lambda_0\right) \tag{A.4}$$

and that by Proposition A.2, it holds that

$$\mu\left(\Lambda_0\right) \geq \left(\frac{1}{|\Sigma|}\right)^{\frac{1}{\log\Sigma}} \cdot \mu(\Sigma) \geq \frac{1}{2} \cdot \mu(\Sigma).$$

Therefore,

$$\mu\left(\Lambda\right) \geq \frac{1}{4} \cdot \mu(\Sigma)$$

as required. It remains to show Λ is $\frac{1}{4\log|\Sigma|}$–fortified. Let $\tilde{\Lambda} \subseteq \Lambda$. By Proposition A.1, it holds that

$$\mu(\tilde{\Lambda}) \geq \frac{1}{2\log|\Sigma|} \cdot \frac{|\tilde{\Lambda}|}{|\Lambda_0|} \cdot \mu\left(\Lambda_0\right) \geq \frac{1}{2\log|\Sigma|} \cdot \frac{|\Lambda|}{|\Lambda_0|} \cdot \frac{|\tilde{\Lambda}|}{|\Lambda|} \cdot \mu\left(\Lambda\right)$$

Next, by Proposition A.2, it holds that

$$\begin{aligned} \frac{|\Lambda|}{|\Lambda_0|} \geq \left(\frac{\mu\left(\Lambda\right)}{\mu\left(\Lambda_0\right)}\right)^{\log|\Sigma|} &\geq \left(1 - \frac{1}{2\log|\Sigma|}\right)^{\log|\Sigma|} \text{,by Equation A.4} \\ &\geq \frac{1}{2}. \end{aligned}$$

Thus,

$$\mu(\tilde{\Lambda}) \geq \frac{1}{4\log|\Sigma|} \cdot \frac{|\tilde{\Lambda}|}{|\Lambda|} \cdot \mu\left(\Lambda\right).$$

This means Λ is $\frac{1}{4\log|\Sigma|}$–fortified as required. □

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il