DETERMINISTIC RANDOMNESS EXTRACTION FROM GENERALIZED AND DISTRIBUTED SANTHA–VAZIRANI SOURCES[*]

SALMAN BEIGI[†], OMID ETESAMI[†], AND AMIN GOHARI[‡]

Abstract. A Santha–Vazirani (SV) source is a sequence of random bits where the conditional distribution of each bit, given the previous bits, can be partially controlled by an adversary. Santha and Vazirani show that deterministic randomness extraction from these sources is impossible. In this paper, we study the generalization of SV sources for nonbinary sequences. We show that unlike the binary setup of Santha and Vazirani, deterministic randomness extraction in the generalized case is sometimes possible. In particular, if the adversary has access to s "nondegenerate" dice that are c-sided and can choose one die to throw based on the previous realizations of the dice, then deterministic randomness extraction is possible if $s < c$. We present a necessary condition and a sufficient condition for the possibility of deterministic randomness extraction. These two conditions complement each other in the nondegenerate cases. Next, we turn to a distributed setting. In this setting the SV source consists of a random sequence of pairs $(a_1, b_1), (a_2, b_2), \ldots$ distributed between two parties, where the first party receives a_i's and the second one receives b_i's. The goal of the two parties is to extract common randomness without communication. Using the notion of *maximal correlation*, we prove a necessary condition and a sufficient condition for the possibility of common randomness extraction from these sources. Based on these two conditions, the problem of common randomness extraction essentially reduces to the problem of randomness extraction from (nondistributed) SV sources. This result generalizes results of Gács and Körner, and Witsenhausen about common randomness extraction from independently and identically distributed sources to adversarial sources.

Key words. randomness extraction, Santha–Vazirani sources, common randomness extraction

AMS subject classifications. 68W20, 68Q87, 60C05

DOI. 10.1137/15M1027206

1. Introduction.

Randomized algorithms are simpler and more efficient than their deterministic counterparts in many applications. In some settings such as communication complexity and distributed computing, it is even possible to prove unconditionally that allowing randomness improves the efficiency of algorithms (see, e.g., [29, 18, 12]). However, access to sources of randomness (especially common randomness) may be limited, or the quality of randomness in the source may be far from perfect. Having such an imperfect source of randomness, one may be able to extract (almost) unbiased and independent random bits using *randomness extractors.* A randomness extractor is a function applied to an imperfect source of randomness whose outcome is an almost perfect source of randomness.

The problem of randomness extraction from imperfect sources of randomness was perhaps first considered by Von Neumann [26]. A later important work in this area is

[*] Received by the editors June 22, 2015; accepted for publication (in revised form) October 4, 2016; published electronically January 12, 2017. A preliminary conference version of this paper appeared in the Proceedings of the International Colloquium on Automata, Languages and Programming, ICALP, Springer, Berlin, 2015, pp. 143–154.

http://www.siam.org/journals/sicomp/46-1/M102720.html

Funding: This work was supported by the Institute for Research in Fundamental Sciences (IPM), grant 94050034, and by Iran National Science Foundation (INSF), grant 95824657.

[†] School of Mathematics, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran (salman.beigi@gmail.com, etesami@ipm.ir).

[‡] Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran (aminzadeh@sharif.edu).

[21] where Santha and Vazirani introduced the imperfect sources of randomness now often called Santha–Vazirani (SV) sources, also known as "unpredictable-bit sources," e.g., in [22]. These sources can easily be defined in terms of an adversary with two coins. Consider an adversary who has two different coins, one of which is biased towards heads (e.g., Pr(heads) $= 2/3$) and the other one is biased towards tails (e.g., Pr(heads) $= 1/3$). The adversary, in each time step, chooses one of the two coins and tosses it. Adversary's choice of coin may depend (probabilistically) on the previous outcomes of the tosses. The sequence of random outcomes of these coin tosses is called an SV source.

For a family of sequences of random variables $(C_1, C_2, \dots)$ on alphabet $\mathcal{C}$ (such as the family of SV sources), we say that *randomness can be extracted from the family* if there are functions (extractors) $\Gamma_n : \mathcal{C}^n \to \{0, 1\}$, $n \geq 1$, such that the bias of $\Gamma_n(C_1, \dots, C_n)$ is at most $\epsilon(n)$ for every sequence $(C_1, C_2, \dots)$ in the family, where $\epsilon(n)$ tends to zero as $n \to \infty$.

Santha and Vazirani [21] show that randomness extraction from the above SV sources through a deterministic method is impossible. More precisely, they show that for every deterministic way of extracting one random bit, there is a strategy for the adversary such that the extracted bit is biased or, more specifically, the extracted bit is 0 with probability either $\geq 2/3$ or $\leq 1/3$. Subsequently, other proofs for this result have been found (see, e.g., [20, 1]).

1.1. Main result 1: Existence of deterministic extractors for generalized SV sources. Although [21] proves the impossibility of deterministic randomness extraction from SV sources, this impossibility is shown only for binary sources. In this paper we show that if we consider a generalization of SV sources over *nonbinary* alphabets, deterministic randomness extraction is indeed possible under certain conditions.

To generalize SV sources over nonbinary alphabets, we assume that the adversary, instead of coins, has some multifaceted (say 6-sided) dice. The numbers written on the faces of different dice are the same, but each die may have a different probability for a given face value. The adversary throws these dice n times, each time choosing a die to throw depending on the results of the previous throws. Again, the outcome is an imperfect source of randomness, for which we may ask whether deterministic randomness extraction is possible or not.

When the dice are nondegenerate, i.e., all faces of all dice have nonzero probability, we give a necessary and sufficient condition for the existence of a deterministic strategy for extracting one bit with arbitrarily small constant bias. The following (informal) theorem summarizes our results.

THEOREMS 4 AND 9 (informal). *Given a generalized SV source defined by a set of nondegenerate dice, we can extract one bit of randomness with arbitrarily small constant bias if and only if the convex hull of the set of probability distributions associated with the set of dice does not have full dimension in the probability simplex.*

For example, when the dice are 6-sided, the necessary and sufficient condition implies that we can deterministically extract an almost unbiased bit when the adversary has access to any arbitrary set of five nondegenerate dice, but randomness extraction is not possible in general when the adversary has access to six nondegenerate 6-sided dice. Furthermore, we emphasize that when we prove the possibility of deterministic extraction, we also provide an *explicit* extractor.

1.2. Main result 2: Common randomness extractors for distributed SV sources. Common random bits, shared by distinct parties, constitute an important resource for distributed algorithms; common random bits can be used by the parties to synchronize the randomness of their local actions. We may ask the question of randomness extraction in this setting too. Assuming that the parties are provided with an imperfect source of common randomness, the question is whether perfect common randomness can be extracted from this source or not.

Gács and Körner [14] and Witsenhausen [27] have looked at the problem of extraction of common random bits from a very special class of imperfect sources, namely, independently and identically distributed (i.i.d.) sources. In this case, the *bipartite* source available to the parties is generated as follows. In time step i, a pair (A_i, B_i) with some predetermined distribution $p(a, b)$ and independent of the past is generated; A_i is revealed to the first party and B_i is revealed to the second party. In other words, the two parties receive i.i.d. repetitions of a pair of random variables (A, B).

After receiving arbitrarily many repetitions of random variables, i.e., $(A_1, \dots, A_n)$ and $(B_1, \dots, B_n)$ for some large n, the two parties aim to extract a common random bit. It is known that in this case, the two parties (who are not allowed to communicate) can generate a common random bit if and only if A and B have common data [27]. This means that common randomness generation is possible if A and B can be expressed as $A = (A', C)$ and $B = (B', C)$ for a nonconstant common part C, i.e., there are nonconstant functions f, g such that $C = f(A) = g(B)$. Observe that when a common part exists, common randomness can be extracted by the parties by applying the same (deterministic) extractor on the sequence of C's. That is, the problem of common randomness extraction in the i.i.d. case is reduced to the problem of ordinary randomness extraction.

In this paper we consider the problem of common randomness extraction from *distributed SV sources* defined as follows. In a distributed SV source, the adversary again has some multifaceted dice, but here, instead of a single number, a pair of numbers (A, B) is written on each face. As before, the set of values written on the faces of the dice is the same, but the probabilities of face values may differ in different dice. In other words, if we index the dice with variable $s \in \mathcal{S}$, we have a probability distribution $p_s(ab)$ for each die $s \in \mathcal{S}$. In each time step, the adversary, based on the results of the previous throws, picks a die and throws it. In other words, if S_i denotes the index of the die chosen by the adversary for the ith throw, and (A_i, B_i) is the result of the ith throw, the following holds: S_i is chosen by the adversary based on the history $(S_{1:i-1}, A_{1:i-1}, B_{1:i-1})$. Also, random variables (A_i, B_i) are distributed according to $p_{S_i}(ab)$. Given (A_i, B_i) (the result of the ith throw), A_i is given to the first party and B_i to the second party. Thus, the two parties will observe random variables $(A_1, A_2, \dots)$ and $(B_1, B_2, \dots)$ whose joint distribution depends on the choice of die by the adversary.

Now the question is whether common randomness can be extracted from such a family of distributed sources.

Example 1. A concrete example of a distributed SV source is as follows. Let us start with the original source considered by Santha and Vazirani with two coins. Assume that the adversary at time step i, chooses coin $S_i \in \{1, 2\}$, where coin 1 is biased towards heads and coin 2 is biased towards tails, and let the outcome of the throw of the coin be denoted by random variable C_i.

The first party, Alice, is assumed to observe both the identity of the coin chosen by the adversary, i.e., S_i, and the outcome of the coin, which is C_i. The second party, Bob, observes the outcome of the coin C_i, but only gets to see the choice of the adversary with probability 0.99. That is, Bob gets $B_i = (C_i, \tilde{S}_i)$, where $\tilde{S}_i$ is the result of passing S_i through a binary erasure channel with erasure probability 0.01. Here the common part of $A_i = (C_i, S_i)$ and $B_i = (C_i, \tilde{S}_i)$ is C_i.

We will elaborate on the definition of common data for an SV source in subsections 3.2 and 3.3. Roughly speaking, C is a common part of a given set of dice $p_s(ab)$ if there are functions f and g such that $C = f(A) = g(B)$ when $(A, B) \sim p_s(ab)$ for any $s \in \mathcal{S}$. We note that in the above example C_i is the *maximal* common part of (A_i, B_i) that can be computed from any of A_i and B_i individually. We observe that as in the i.i.d. case, this maximal common part is unique. We then call $(C_1, C_2, \dots)$ the *common data* of the distributed SV source. We also note that $(C_1, C_2, \dots)$ itself is a generalized SV source, and the set of all sequences of random variables $(C_1, C_2, \ldots)$ derived in this way is a family of generalized SV sources.

THEOREM 25 (informal). *Let (A_i, B_i) be the outcome of the ith throw in a distributed SV source. Let C_i be the (unique maximal) common data of A_i and B_i, common over all different dice. When the family of generalized SV sources $(C_1, C_2, \ldots)$ is nondegenerate, i.e., each possibility for C_i has positive probability over all different dice, we can extract a common random bit from the distributed SV source if and only if it is possible to extract randomness from the generalized SV sources $(C_1, C_2, \dots)$. Note that in the degenerate cases, extracting randomness from $(C_1, C_2, \dots)$ is clearly still sufficient for common randomness extraction.*

In the nondegenerate case, similar to the i.i.d. setting, the problem of common randomness extraction from distributed SV sources is reduced to the problem of randomness extraction from nonbinary generalized SV sources. Thus, as for nondistributed SV sources, we have an almost complete answer to the problem in the distributed case. For instance, in Example 1, our result (Theorem 25) implies that Alice and Bob cannot benefit from their knowledge of the actions of the adversary, and should only consider the C sequence. But then from the result of [21], we can conclude that common random bit extraction is impossible in this example.

1.3. Proof techniques.

We briefly explain the techniques used in the proof of the above results.

To show the possibility of deterministic extraction, we use a nonzero real function of the die face values that has zero expectation under all distributions induced by the different dice of the adversary. Then as we throw the dice several times, we consider the sum of the value of this function applied to the outcome of the dice throws. This sum forms a *martingale*. We stop the martingale once its absolute value exceeds a particular large bound. Since the function used was nonzero, the martingale has large variance after a few throws, and therefore the martingale will be stopped with high probability. By the theorem of stopping times, the martingale has zero mean whenever we stop it. Then, the extracted bit, determined by whether the stopped martingale is positive or is negative, would be nearly unbiased because

- the two values beyond or below which we stop the martingale are symmetric around the origin;
- we stop the martingale before the absolute value of the martingale passes the bound too much: the bound is much larger than the changes in the value of the martingale at each step.

To show the impossibility of deterministic extraction, we view a deterministic extractor that extracts one bit from a generalized SV source as labeling the leaves of a rooted tree with zeros and ones. Each sequence of dice throws corresponds to a path from the root to one of the leaves, and at each node, the adversary has some limited control of which branch to take while moving from the root towards the leaves.

We need to show that either the minimum or the maximum of the probability of the output bit being zero, over all adversary's strategies, is far from 1/2. Our idea is to track these maximum and minimum probabilities in a recursive way, i.e., to find these probabilities for any node of the tree in terms of these values for its children. We then by induction show that for each node of the tree either the minimum probability or the maximum probability is far from 1/2.

To be more precise, given a deterministic extractor, let α be the minimum probability of the output bit being zero (over all strategies of the adversary). Similarly, let β be the maximum probability of the output bit being zero (over all strategies of the adversary). Then we show that under certain conditions, there exists a *continuous* function $g(\cdot)$ on the interval $[0, 1]$, such that $\beta \geq g(\alpha)$ and furthermore $g(1/2) > 1/2$. We prove $\beta \geq g(\alpha)$ inductively using the tree structure discussed above. This implies the desired impossibility result, as by the continuity of $g(\cdot)$, both α and β cannot be close to 1/2. For instance, for the binary SV source with two coins having probability of heads, respectively, equal to 1/3 and 2/3, Figure 1 shows a curve where (α, β) always lies on or above it. This curve is clearly isolated from $(1/2, 1/2)$.

We follow similar ideas for proving our impossibility result for common randomness extraction from a distributed SV source; again we construct a continuous function, which somehow captures not only the minimum and maximum of the probability of the extracted common bit being zero, but also the probability that the two parties agree on their extracted bits. The construction of this function is more involved in the distributed case; it has two terms one of which is similar to the function in the nondistributed case, and the other is a quadratic term inspired by the definition of *maximal correlation*. Maximal correlation is a measure of correlation which is also used by Witsenhausen [27] in his impossibility proof of common randomness generation from i.i.d. sources explained above.

1.4. Related works.

As shown by Vazirani and Vazirani [24, 25], randomized polynomial-time algorithms that use perfect random bits can be simulated using SV sources. This fact can also be verified using the fact that the min-entropy [7] of SV sources is linear in the size of the source. Indeed, by the later theory of randomness extraction (e.g., see [30]), it is possible to efficiently extract polynomially many almost random bits from such sources with high min-entropy if we are, in addition to the imperfect source, endowed with a perfectly random seed of logarithmic length. (In fact, for the special case of SV sources, a seed of constant length is enough [22, Problem 6.6]). For the application of randomized polynomial-time algorithms, we can enumerate in polynomial time over all possible seeds.

Enumerating over all seeds may be inefficient for some applications, or does not work at all, e.g., in interactive proofs and one-shot scenarios such as cryptography. Therefore, it is natural to ask whether deterministic randomness extraction from imperfect sources of randomness is possible. For most applications, it is also necessary to require that the extractor be explicit, i.e., extraction can be done efficiently (in polynomial time). Previous to this work, explicit deterministic extractors had been constructed for many different classes of sources, including i.i.d. bits with unknown bias [26], Markov chains [4], affine sources [6, 13], polynomial sources [11, 10], and sources consisting of independent blocks [5].

The generalized SV sources considered in this paper are also a generalization of "block sources" defined by Chor and Goldreich [7], where the source is divided into several blocks such that each block has min-entropy at least k conditioned on the value of the previous blocks. Such a block source can be thought as a generalized SV source where the adversary can generate each block (given previous blocks) using any "flat" distribution with support 2^k. Being a special case of generalized SV sources (defined here), block sources have another difference as well: Since it is impossible to extract from a single block source deterministically, the common results regarding extraction from block sources are about either seeded extractors (see, e.g., [16]) or extraction from at least two independent block sources (see, e.g., [19]).

As mentioned above, the problem of common randomness extraction from i.i.d. sources has been studied in the information theory community. Then our work provides a generalization and an alternative proof of known results in the i.i.d. case. In particular, we give a new proof of Witsenhausen's result [27] on the impossibility of common randomness extraction from certain i.i.d. sources.

We also would like to point out that a generalized SV source as we define, is indeed an arbitrarily varying source [8, 9] with a causal adversary. These sources are studied in the information theory literature from the point of view of source coding [3].

1.5. Notation.

Random variables are denoted by capital letters, and their values by lowercase letters (such as s, c, y, y, etc). Deterministic constants or values are also shown by lowercase letters. Sets are denoted by calligraphic letters, e.g., $\mathcal{C}, \mathcal{T}$. Total variation distance (or the statistical distance) between two distributions $p(x)$ and $q(x)$ is equal to $\frac{1}{2}\sum_x |p(x) - q(x)|$.

When discussing a generalized SV source, we use $\mathcal{C}$ as the alphabet of the source. The sequence of realizations is denoted by $(c_1, c_2, \ldots, c_n)$. When viewed as random variables, we use capital letters $(C_1, C_2, \ldots, C_n)$. For simplicity of notation a sequence $(C_1, \ldots, C_n)$ of (not necessarily i.i.d.) random variables is denoted by C^n. Similarly for $c_1, \ldots, c_n \in \mathcal{C}$ we use $c^n = (c_1, \ldots, c_n)$. We also use the notation $c_{[k:k+\ell]} = (c_k, c_{k+1}, \ldots, c_{k+\ell})$.

We sometimes have several distributions over the same set $\mathcal{C}$ which are indexed by elements $s \in \mathcal{S}$; these are denoted by $p_s(c)$. In this case to avoid confusion, the expected value and variance are specified by a subscript s, as $\mathbb{E}_{(s)}[\cdot]$ and $\mathrm{Var}_{(s)}[\cdot]$, respectively.

In the section on SV sources, we consider functions $X : \mathcal{C} \to \mathbb{R}$. When a distribution is imposed on $\mathcal{C}$, such a function can be thought of as a random variable $X = X(C)$. Just like random variables, capital letters are used for functions. We sometimes, for simplicity, use the notation $X(c) = x_c$. Consistent with the notation set above, when the distribution on C is $p_s(c)$, we use $\mathbb{E}_{(s)}[X]$ to denote $\sum_c p_s(c)X(c) = \sum_c p_s(c)x_c$. The variance $\mathrm{Var}_{(s)}[X]$ is defined similarly.

We use expressions like $\mathbb{E}_*[X]$ and $\mathrm{Var}_*[\cdot]$ to denote expected value and variance when the underlying distribution is assumed to be uniform, e.g., for a function $X : \mathcal{C} \mapsto \mathbb{R}$, we define $\mathbb{E}_*[X] = \frac{1}{|\mathcal{C}|}\sum_c X(c)$. Similarly, we define

$$\|X\|_*^2 = \frac{1}{|\mathcal{C}|}\sum_c X(c)^2.$$

For two functions $X, X' : \mathcal{C} \mapsto \mathbb{R}$, we define

$$\langle X, X' \rangle_* = \frac{1}{|\mathcal{C}|}\sum_c X(c)X'(c).$$

We use $\mathbf{1}_{\mathcal{C}}$ to denote the unity function $\mathcal{C} \to \mathbb{R}$, that is, $\mathbf{1}_{\mathcal{C}}(c) = 1$ for all $c \in \mathcal{C}$.

In the section on distributed SV sources, we use $\mathcal{A}$ and $\mathcal{B}$ for alphabets, and random variables A and B for the random realization of the distributed sources. We sometimes have several distributions over the same set $\mathcal{A} \times \mathcal{B}$ which are indexed by elements $s \in \mathcal{S}$; these are denoted by $p_s(ab)$. In the section on distributed SV sources, random variable C generally serves as the common part of A and B in the sense that will be defined later.

2. Randomness extraction from generalized SV sources.

Definition 2 (generalized SV source). *Let $\mathcal{C}$ be a finite alphabet set. Consider a* finite *set of distributions over $\mathcal{C}$ indexed by a set $\mathcal{S}$. That is, assume that for any $s \in \mathcal{S}$ we have a distribution over $\mathcal{C}$ determined by numbers $p_s(c)$ for all $c \in \mathcal{C}$. A sequence $(C_1, C_2, \ldots)$ of random variables, each over alphabet set $\mathcal{C}$, is said to be a* generalized SV source *with respect to distributions $p_s(c)$, if the sequence is generated as follows: Assume that $C_1, \ldots, C_{i-1}$ are already generated. In order to determine C_i, an adversary chooses $s_i \in \mathcal{S}$, depending only*[1] *on $c_1, \ldots, c_{i-1}$. Then C_i is sampled from the distribution $p_{s_i}(c)$.*

We can think of specifying s as choosing a particular multifaceted die, and c as the facet that results from throwing the die. The joint probability distribution of random variables $C_1, \ldots, C_n$ and $S_1, \ldots, S_n$ in a generalized SV source factorizes as follows:

$$\begin{aligned} p(c_1,&c_2, \cdots, c_n, s_1, s_2, \cdots, s_n) \\ &= q(s_1)p_{s_1}(c_1)q(s_2|c_1)p_{s_2}(c_2)\cdots q(s_n|c_1\cdots c_{n-1})p_{s_n}(c_n), \end{aligned}$$

where $q(s_i|c_1\cdots c_{i-1})$ describes the action of the adversary at time i. Here, first the adversary chooses s_1 with probability $q(s_1)$, and then c_1 is generated with probability $p_{s_1}(c_1)$. Then the adversary chooses s_2 with probability $q(s_2|c_1)$ and then c_2 is generated with probability $p_{s_2}(c_2)$, and so on.

Generalized SV sources can be alternatively characterized as follows: $(C_1, C_2, \ldots)$ belongs to the family of generalized SV sources determined by $p_s(c)$'s if for every given i and $C_1 = c_1, \ldots, C_{i-1} = c_{i-1}$, the conditional distribution of C_i is a convex combination of the set of $|\mathcal{S}|$ distributions $\{p_s(\cdot) : s \in \mathcal{S}\}$.

We emphasize that even after fixing distributions $p_s(c)$, the generalized SV source (similar to ordinary SV sources) is not a fixed source, but rather a class of sources. This is because in each step s_i is chosen arbitrarily by the adversary as a (probabilistic) function of $C_1, \ldots, C_{i-1}$. Nevertheless, once we fix adversary's strategy, the generalized SV source is fixed in that class of sources.

Definition 3 (deterministic extraction). *We say that deterministic randomness extraction from the generalized SV source determined by distributions $p_s(c)$ is possible if for every $\epsilon > 0$ there exist n and $\Gamma_n : \mathcal{C}^n \to \{0, 1\}$ such that for every strategy of the adversary, the distribution of $\Gamma_n(C^n)$ is ϵ-close, in total variation distance, to the uniform distribution. That is, independent of adversary's strategy, $\Gamma_n(C^n)$ is an almost uniform bit.*

In the following we present a necessary condition and separately a sufficient condition for the existence of deterministic extractors for generalized SV sources. In the

[1] We can allow for the adversary to choose s_i depending both on $c_1, \ldots, c_{i-1}$ and on $s_1, \ldots, s_{i-1}$, but this relaxation is not important, since it is only the marginal distribution $p(c_1, c_2, \cdots, c_n)$ that matters to us. In other words, when extraction is not possible, the adversary only needs to remember $c_1, \ldots, c_{i-1}$ to choose s_i (does not need to remember $s_1, \ldots, s_{i-1}$). And when extraction is possible, it is so even if adversary gets both of $c_1, \ldots, c_{i-1}$ and $s_1, \ldots, s_{i-1}$.

nondegenerate case, i.e., when $p_s(c) > 0$ for all s, c, these two conditions complement each other. Thus we fully characterize the possibility of deterministic randomness extraction from generalized SV sources in the nondegenerate case.

2.1. A sufficient condition for the existence of randomness extractors. In this subsection we prove the following theorem.

THEOREM 4. *Consider a generalized SV source with alphabet $\mathcal{C}$, set of dice $\mathcal{S}$, and probability distributions $p_s(c)$. Suppose that there exists $\psi : \mathcal{C} \to \mathbb{R}$ such that for every $s \in \mathcal{S}$ we have $\mathbb{E}_{(s)}[\psi(C)] = 0$ and $\mathrm{Var}_{(s)}[\psi(C)] > 0$, where $\mathbb{E}_{(s)}$ and $\mathrm{Var}_{(s)}$ are expectation and variance with respect to the distribution $p_s(\cdot)$, i.e., $\mathbb{E}_{(s)}[\psi(C)] = \sum_c p_s(c)\psi(c)$. Then randomness can be extracted from this SV source.*

Observe that if $p_s(c) > 0$ for all s, c, then this theorem can equivalently be stated as follows: Thinking of each distribution $p_s(\cdot)$ as a point in the probability simplex, if the convex hull of the set of points $\{p_s(\cdot) : s \in \mathcal{S}\}$ in the probability simplex does not have full dimension, then deterministic randomness extraction is possible. For instance, if $|\mathcal{S}| < |\mathcal{C}|$ this condition is always satisfied and then we can deterministically extract randomness.

Before providing the proof, it is useful to review some definitions and results from martingale theory. A sequence $(Z_0, Z_1, \dots)$ of random variables is a martingale with respect to another sequence $(X_0, X_1, \dots)$ if $\mathbb{E}(|Z_n|) < \infty$ and $\mathbb{E}(Z_{n+1} \mid X_1, \dots, X_n) = Z_n$ for all n. It is called a submartingale if we replace the second condition by $\mathbb{E}(Z_{n+1} \mid X_1, \dots, X_n) \geq Z_n$. A stopping time for a sequence $Z_0, Z_1, \dots$ is a random variable τ taking values in $\{0, 1, 2, \dots\}$ such that the occurrence or nonoccurrence of the event $\tau = t$ is determined by $Z_0, Z_1, \dots, Z_t$. The optional stopping theorem for submartingales states that under certain conditions (such as the stopping time always being bounded by some constant c), we have that $\mathbb{E}(Z_\tau) \geq \mathbb{E}(Z_0)$.

Proof of Theorem 4. Pick a sufficiently large (but constant) number m. Define random variables $X_1, \dots, X_n$ and $Y_0, \dots, Y_n$ inductively as follows: Let $Y_0 = 0$, and for $i = 1, \dots, n$, define $Y_i = Y_{i-1} + X_i$, where $X_i = \psi(C_i)$ and C_i is the ith element of the SV source sequence. Observe that by our assumption we have $\mathbb{E}[X_i|X_1, \dots, X_{i-1}] = 0$, so $Y_0, \dots, Y_n$ forms a martingale.

Let τ be the first time $t \in \{0, 1, 2, \dots, n\}$ such that $|Y_t| \geq m$; if no such t exists, define $\tau = n$. Clearly, τ is a stopping time for the martingale. Now define the extracted bit to be 1 if $Y_\tau \geq m$; otherwise define it to be 0. We show that this is a true random bit extractor.

Let $v = \min_s \mathrm{Var}_{(s)}[\psi] > 0$. Define $Z_i = Y_i^2 - iv$. We claim that Z_i is a submartingale with respect to $X_1, \dots, X_n$. To show this we compute

$$\begin{aligned}\mathbb{E}[Z_i|X_1, \dots, X_{i-1}] &= \mathbb{E}\big[(X_i + Y_{i-1})^2 - iv\big|X_1, \dots, X_{i-1}\big] \\ &= \mathbb{E}\big[(Y_{i-1}^2 - (i-1)v) + (X_i^2 - v) + 2X_iY_{i-1}\big|X_1, \dots, X_{i-1}\big] \\ &\geq Z_{i-1}.\end{aligned}$$

Here we used $Z_{i-1} = Y_{i-1}^2 - (i-1)v$, and

$$\mathbb{E}[X_iY_{i-1}|X_1, \dots, X_{i-1}] = Y_{i-1}\mathbb{E}[X_i|X_1, \dots, X_{i-1}] = 0,$$

and that by the law of total variance

$$\mathbb{E}[X_i^2|X_1, \dots, X_{i-1}] = \mathrm{Var}[\psi(C_i)|X_1, \dots, X_{i-1}] \geq \mathrm{Var}[\psi(C_i)|X_1, \dots, X_{i-1}, S_i] \geq v.$$

Therefore by the optional stopping theorem for submartingales, we have

$$\mathbb{E}[Z_\tau] \geq \mathbb{E}[Z_0] = 0$$

or, equivalently,

$$\mathbb{E}[Y_\tau^2] \geq v\mathbb{E}[\tau].$$

Let $m' = \max_c |\psi(c)|$. Then, by the definition of τ we have $|Y_\tau| \leq m' + m$. Therefore,

$$\mathbb{E}[\tau] \leq \frac{\mathbb{E}[Y_\tau^2]}{v} \leq \frac{(m'+m)^2}{v}.$$

Hence by the Markov inequality we have

$$\Pr[\tau = n] \leq \frac{(m'+m)^2}{vn} = O\left(\frac{1}{n}\right).$$

This means that

$$\Pr\left[Y_\tau \in [m, m'+m) \cup (-m-m', -m]\right] = 1 - O\left(\frac{1}{n}\right).$$

On the other hand, for the martingale $Y_0, Y_1, \ldots$, we have $\mathbb{E}[Y_\tau] = \mathbb{E}[Y_0] = 0$. Together with $|Y_\tau| \leq m + m'$, this implies

$$\frac{m}{2m+m'} - O\left(\frac{1}{n}\right) \leq \Pr[Y_\tau \in [m, m+m')] \leq \frac{m+m'}{2m+m'} + O\left(\frac{1}{n}\right).$$

Therefore, the extracted bit has sufficiently small bias as m, n are chosen sufficiently large. This is because $m' = \max_c |\psi(c)|$ is a constant, independent of m and n. □

Remark 5. Note that we could have chosen $m = \Theta(n^{1/3})$ in the above proof. Then the analysis would have shown that the bias is polynomially small, namely, a bias of $\Theta(n^{-1/3})$. (Notice that in the above asymptotic notation, the constants in the big Θ may depend on the family of generalized SV sources.)

Remark 6. Note that the extractor constructed in the above proof is *explicit*, i.e., the extractor function can be computed deterministically and in polynomial time (in terms of the length of the input n, and in terms of the size of the description of the set of dice), and is not based on the so-called probabilistic method. Indeed, given the set of dice $\mathcal{S}$, one can easily compute ψ, v, and m'.

By Remark 5, the running time of the extractor is also polynomial in the error/bias.

COROLLARY 7. *Given ℓ and ϵ, we can extract ℓ bits of randomness from any SV source of length $O(\ell\epsilon^{-3})$ satisfying the properties of Theorem 4 such that each bit has bias $\leq \epsilon$ given the previous bits. (The constant in the big-Oh notation depends on the set of dice.) In other words, the extracted bits themselves are a binary SV source with bias ϵ and length ℓ. In particular, the extracted bits have statistical distance at most $\ell\epsilon$ from the uniform distribution on ℓ-bit strings.*

Proof. We partition the SV source sequence into ℓ blocks, each of length $\Theta(\epsilon^{-3})$. By Remark 5, one can, from each block, extract one bit of randomness that has bias at most ϵ given the past blocks and, hence, given the past produced bits.

The statistical distance of an SV source of length ℓ and bias ϵ from the uniform distribution is at most $\ell\epsilon$: We can couple the SV source with the uniform distribution such that for each bit of SV source it is equal to the uniform distribution with probability $\geq 1 - \epsilon$. □

Remark 8. Assume the adversary has an *infinite* number of dice. Then, the extractor of Theorem 4 remains valid as long as $\mathrm{Var}_{(s)}[\psi(C)] \geq \epsilon > 0$ for some ϵ independent of s. On the other hand, if there is a finite subset of the dice using which the adversary can defeat any extractor (as is shown in the next subsection under certain conditions), then clearly there is no extractor for an adversary using the full infinite set of dice.

2.2. A necessary condition for the existence of randomness extractors. The main result of this subsection is the following theorem.

THEOREM 9. *Consider a generalized SV source with alphabet $\mathcal{C}$, set of dice $\mathcal{S}$, and probabilities $p_s(c)$. Suppose that there is no nonzero function $\psi : \mathcal{C} \to \mathbb{R}$ such that for all $s \in \mathcal{S}$ we have $\mathbb{E}_{(s)}[\psi(C)] = 0$. Then deterministic randomness extraction from this generalized SV source is impossible.*

Again, let us consider the case where $p_s(c) > 0$ for all s, c. In this case ψ being nonzero is equivalent to $\mathrm{Var}_{(s)}[\psi] > 0$ for all s. Then comparing to Theorem 4 we find that the necessary and sufficient condition for the possibility of deterministic extraction is the existence of a nonzero ψ with $\mathbb{E}_{(s)}[\psi] = 0$.

In Appendix B we give a proof of this theorem based on ideas in [20]. Here we present another proof whose ideas will be used in the distributed case too.

Proof of Theorem 9. Any deterministic randomness extraction algorithm corresponds to a subset $\mathcal{I} \subseteq \mathcal{C}^n$ such that the extracted bit is 0 if the observed c^n is in $\mathcal{I}$, and is 1 otherwise. For any n, and any such $\mathcal{I} \subseteq \mathcal{C}^n$, let $\alpha(\mathcal{I})$ and $\beta(\mathcal{I})$, respectively, be the minimum and maximum of the probability of output 0 over all strategies of the adversary, i.e.,

$$\alpha(\mathcal{I}) := \min \Pr[C^n \in \mathcal{I}], \qquad \beta(\mathcal{I}) := \max \Pr[C^n \in \mathcal{I}],$$

where minimum and maximum are taken over adversary's strategies. Observe that we define $\alpha(\mathcal{I})$ and $\beta(\mathcal{I})$ for *any arbitrary* n and any subset $\mathcal{I} \subseteq \mathcal{C}^n$.

Fix a deterministic algorithm for randomness extraction. To prove the theorem we show that for every n and every $\mathcal{I} \subseteq \mathcal{C}^n$, either $\alpha(\mathcal{I})$ or $\beta(\mathcal{I})$ is far from 1/2. We now use the following lemma whose proof comes after the proof of Theorem 9.

LEMMA 10. *Suppose that $g : [0,1] \to \mathbb{R}$ is a function that satisfies the following:*

- *g is continuous and* monotonically nondecreasing*;*
- *we have*

$$g(0) = 0, \qquad g(1) = 1, \qquad g(1/2) > 1/2; \tag{1}$$

- *and for all $X : \mathcal{C} \to [0,1]$ we have*

$$\max_s \mathbb{E}_{(s)}[g(X)] \geq \min_{s'} g\big(\mathbb{E}_{(s')}[X]\big)$$

or, equivalently,

$$\max_{s,s'} \mathbb{E}_{(s)}[g(X)] - g\big(\mathbb{E}_{(s')}[X]\big) \geq 0, \tag{2}$$

where $\mathbb{E}_{(s)}[g(X)] = \sum_c p_s(c) g(X(c))$ and $\mathbb{E}_{(s')}[X] = \sum_c p_{s'}(c) X(c)$.

Then for any n and any set $\mathcal{I} \subseteq \mathcal{C}^n$, we have that $\beta(\mathcal{I}) \geq g(\alpha(\mathcal{I}))$.

If such a function g with the above properties exists, then $\alpha(\mathcal{I})$ and $\beta(\mathcal{I})$ cannot both be arbitrarily close to 1/2. To verify this, note that $\beta(\mathcal{I}) \geq g(\alpha(\mathcal{I}))$. If for every

$\epsilon > 0$, one can find n and a set $\mathcal{I} \subset \mathcal{C}^n$ such that $\alpha(\mathcal{I}), \beta(\mathcal{I})$ are within ϵ distance of $1/2$, then by the continuity of g and letting ϵ converge to zero, we obtain that $1/2 \geq g(1/2)$. This is a contradiction since $g(1/2) > 1/2$. As a result, we only need to prove the existence of the function g.

Let $f : [0, 1] \to \mathbb{R}$ be a smooth function such that $f(1/2) > 0$ and $f(0) = f(1) = 0$. We show that the function g_ϵ defined by

$$g_\epsilon(x) := x + \epsilon f(x) \tag{3}$$

for sufficiently small $\epsilon > 0$, satisfies the desired properties. Verification of (1) is easy. For the monotonicity of g_ϵ, note that since f is smooth and defined on the closed interval $[0, 1]$, there is a uniform upper bound on the derivative of f as follows:

$$|f'(x)| \leq m \quad \forall x \in [0, 1].$$

Then for $\epsilon < 1/m$, the function g_ϵ is monotone. It remains to show (2).

Define

$$\mathcal{T} := \big\{T : \mathcal{C} \to [0, 1] : \ \|T\|_* = 1, \ \mathbb{E}_*[T] = 0\big\},$$

where $\|T\|_*$ and $\mathbb{E}_*[T]$ are computed with respect to the uniform distribution on $\mathcal{C}$, i.e.,

$$\|T\|_*^2 = \sum_c \frac{1}{|\mathcal{C}|} T(c)^2$$

and

$$\mathbb{E}_*[T] = \sum_c \frac{1}{|\mathcal{C}|} T(c).$$

For every $T \in \mathcal{T}$ we have

$$\max_{s,s'} \mathbb{E}_{(s)}[T] - \mathbb{E}_{(s')}[T] > 0,$$

because otherwise $\max_{s,s'} \mathbb{E}_{(s)}[T] - \mathbb{E}_{(s')}[T] = 0$ implies that $\mathbb{E}_{(s)}[T] = \mathbb{E}_{(s')}[T]$ for all s, s', and $\psi(c) = T(c) - \mathbb{E}_{(s)}[T]$ will be a nonconstant function satisfying $\mathbb{E}_{(s')}[\psi(C)] = 0$ for all s', which is in contradiction with our assumption in the statement of the theorem. Therefore, using the compactness of $\mathcal{T}$, there is $\Delta > 0$ such that

$$\max_{s,s'} \mathbb{E}_{(s)}[T] - \mathbb{E}_{(s')}[T] > \Delta \qquad \forall T \in \mathcal{T}. \tag{4}$$

Let $X : \mathcal{C} \to [0, 1]$ be an arbitrary function. Then, letting $\bar{x} = \mathbb{E}_*[X(C)]$ and $r = \sqrt{\mathrm{Var}_*[X(C)]} \geq 0$ we get that

$$X = \bar{x}\mathbf{1}_{\mathcal{C}} + rT = \bar{x} + rT$$

for some $T \in \mathcal{T}$. Here, if $r = 0$, $T \in \mathcal{T}$ can be chosen arbitrarily, and otherwise we let $T = (X - \bar{x})/r$. Observe that in the latter case $\mathbb{E}_*[T] = 0$ and $\|T\|_*^2 = \mathrm{Var}_*[T] = 1$, so $T \in \mathcal{T}$.

From $g_\epsilon(x) = x + \epsilon f(x)$ we have

$$\begin{aligned}
&\max_{s,s'} \mathbb{E}_{(s)}[g_\epsilon(X)] - g_\epsilon\big(\mathbb{E}_{(s')}[X]\big) \\
&\qquad = \max_{s,s'} \mathbb{E}_{(s)}[X + \epsilon f(X)] - \mathbb{E}_{(s')}[X] - \epsilon f(\mathbb{E}_{(s')}[X]) \\
&\qquad = \max_{s,s'} \big(\mathbb{E}_{(s)}[X] - \mathbb{E}_{(s')}[X]\big) + \epsilon\Big(\mathbb{E}_{(s)}[f(X)] - f(\mathbb{E}_{(s')}[X])\Big) \\
&\qquad = \max_{s,s'} \big(\bar{x} + r\mathbb{E}_{(s)}[T] - \bar{x} - r\mathbb{E}_{(s')}[T]\big) + \epsilon\Big(\mathbb{E}_{(s)}[f(\bar{x} + rT)] - f(\mathbb{E}_{(s')}[\bar{x} + rT])\Big) \\
&\qquad = \max_{s,s'} r\big(\mathbb{E}_{(s)}[T] - \mathbb{E}_{(s')}[T]\big) + \epsilon\Big(\mathbb{E}_{(s)}[f(\bar{x} + rT)] - f\big(\bar{x} + r\mathbb{E}_{(s')}[T]\big)\Big).
\end{aligned}$$

Since f is a smooth function, for every $0 \leq x, y \leq 1$ there is some z (between x and y) such that $f(y) = f(x) + (y - x)f'(z)$. Remember that since we assumed that f is a smooth function defined on the closed interval $[0, 1]$, the absolute value of its derivative can be uniformly bounded from above by a constant m. We then obtain,

$$f(\bar{x}) - m|y - \bar{x}| \leq f(y) \leq f(\bar{x}) + m|y - \bar{x}|.$$

Therefore, using the fact that $|T(c)| \leq \sqrt{|\mathcal{C}|} \leq |\mathcal{C}|$ (implied by $\|T\|_* = 1$), we have

$$\begin{aligned}
\mathbb{E}_{(s)}[f(\bar{x} + rT)] &\geq f(\bar{x}) - mr\mathbb{E}_{(s)}[|T|] \geq f(\bar{x}) - mr|\mathcal{C}|, \\
\big(\bar{x} + r\mathbb{E}_{(s')}[T]\big) &\leq f(\bar{x}) + rm|\mathbb{E}_{(s')}[T]| \leq f(\bar{x}) + mr|\mathcal{C}|.
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\max_{s,s'} \mathbb{E}_{(s)}[g_\epsilon(X)] - g_\epsilon\big(\mathbb{E}_{(s')}[X]\big) \\
&\qquad = \max_{s,s'} r\big(\mathbb{E}_{(s)}[T] - \mathbb{E}_{(s')}[T]\big) + \epsilon\Big(\mathbb{E}_{(s)}[f(\bar{x} + rT)] - f\big(\bar{x} + r\mathbb{E}_{(s')}[T]\big)\Big) \\
&\qquad \geq \max_{s,s'} r\big(\mathbb{E}_{(s)}[T] - \mathbb{E}_{(s')}[T]\big) + \epsilon\Big(f(\bar{x}) - mr|\mathcal{C}| - f(\bar{x}) - mr|\mathcal{C}|\Big)\Big) \\
&\qquad = \max_{s,s'} r\big(\mathbb{E}_{(s)}[T] - \mathbb{E}_{(s')}[T]\big) - 2\epsilon mr|\mathcal{C}| \\
&\qquad \geq r(\Delta - 2\epsilon m|\mathcal{C}|),
\end{aligned} \tag{5}$$

where in (5), we used (4). Observe that the expression in (5) is strictly positive if $\epsilon < \Delta/(2m|\mathcal{C}|)$. Then the function g_ϵ for

$$\epsilon < \min\{1/m, \Delta/(2m|\mathcal{C}|)\},$$

has all the desired properties. □

In the above proof we show that for any deterministic strategy for randomness extraction (specified by a subset $\mathcal{I} \subseteq \mathcal{C}^n$) either $\alpha(\mathcal{I})$ or $\beta(\mathcal{I})$ which, respectively, are the minimum and maximum probability of output 0 over adversary's strategies, is away from 1/2. In the original binary SV sources, the set of such pairs $(\alpha(\mathcal{I}), \beta(\mathcal{I}))$ can be characterized exactly. For details we refer the reader to Appendix A. Also see Figure 1 for an example.

Proof of Lemma 10. The numbers $\alpha(\mathcal{I}), \beta(\mathcal{I})$ can be computed recursively as follows. For every $c \in \mathcal{C}$, let $\mathcal{I}_c := \{c_{[2:n]} : (c, c_{[2:n]}) \in \mathcal{I}\}$. Note that $\mathcal{I}_c$ is a subset of

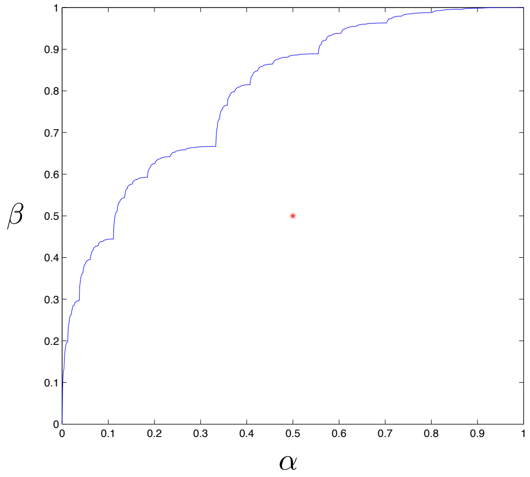

FIG. 1. *Given any deterministic extractor, the pair* (α, β) *is on or above the curve specified in this figure, where* α *and* β *are the minimum and maximum value of the probability of the output being zero that the adversary can achieve by choosing its strategy. The plot is for the binary SV source with two coins with probability of heads respectively equal to* $1/3$ *and* $2/3$*. The point* $(1/2, 1/2)$*, specified by a star, is below the curve, so randomness extraction from this binary SV source is impossible. It can be shown that the curve has fractal-like self-similarity: It can be split at point* $(1/3, 2/3)$ *into two curves each of which is a normalized version of the whole curve. In other words, if* $f : [0, 1] \to [0, 1]$ *is the equation for the curve,* $f(x) = \frac{2}{3}f(3x)$ *for* $x \in [0, 1/3]$ *and* $f(x) = 2/3 + \frac{1}{3}f(\frac{3}{2}(x - 1/3))$ *for* $x \in [1/3, 2/3]$*. We relegate the reason why the curve has this property to Corollary* 35 *in Appendix* A.

$\mathcal{C}^{n-1}$ for which $\alpha(\mathcal{I}_c)$ is defined. (Remember that α is defined for sequences of any length). We claim that

$$\alpha(\mathcal{I}) = \min_s \sum_c p_s(c)\alpha(\mathcal{I}_c). \tag{6}$$

To verify this, suppose that the adversary in the first step chooses $s_1 = s$. Then $C_1 = c$ occurs with probability $p_s(c)$. Assuming $C_1 = c$, the final extracted bit is equal to 0 if $(C_2, \dots, C_n) \in \mathcal{I}_c$. Since, by definition, the minimum of the probability of this latter event is $\alpha(\mathcal{I}_c)$, the (unconditional) probability of the extracted bit being 0 is equal to $\sum_c p_s(c)\alpha(\mathcal{I}_c)$. Taking the minimum of this expression over all $s_1 = s$ gives $\alpha(\mathcal{I})$. To simplify the notation, we can rewrite (6) by defining a random variable C on alphabet $\mathcal{C}$ with pmf $p_s(c)$ as follows:

$$\alpha(\mathcal{I}) = \min_s \mathbb{E}_{(s)}[\alpha(\mathcal{I}_C)],$$

where $\mathbb{E}_{(s)}$ is the expected value with respect to $p_s(c)$. We similarly have

$$\beta(\mathcal{I}) = \max_s \mathbb{E}_{(s)}[\beta(\mathcal{I}_C)].$$

By the above discussion to compute $\alpha(\mathcal{I})$ and $\beta(\mathcal{I})$ for $\mathcal{I} \subseteq \mathcal{C}^n$ it suffices to compute these numbers for subsets of $\mathcal{C}^{n-1}$. Thus the functions $\alpha(\cdot)$ and $\beta(\cdot)$ can be computed recursively. The above recursive procedure can be understood as assigning two values to each node of the tree associated with the extractor, as described in the "proof techniques" subsection of the introduction.

Let Φ_n be the set of pairs $(\alpha(\mathcal{I}), \beta(\mathcal{I}))$ for all subsets $\mathcal{I} \subseteq \mathcal{C}^n$. In other words, for $n \geq 1$ define

$$\Phi_n := \big\{(\alpha(\mathcal{I}), \beta(\mathcal{I})) : \mathcal{I} \subseteq \mathcal{C}^n\big\}.$$

Also let

$$\Phi_0 = \{(0,0),(1,1)\}.$$

Observe that Φ_0 corresponds to the case when there is no SV source to look at, and the deterministic extractor outputs a constant bit. Now by the above discussion, Φ_n is indeed the set of pairs (x, y) for which there exist $X, Y : \mathcal{C} \to \mathbb{R}$ such that $(X(c), Y(c)) \in \Phi_{n-1}$ for every $c \in \mathcal{C}$, and that

$$\begin{aligned} \mathsf{x} &= \min_s \mathbb{E}_{(s)}[X] = \min_s \sum_c p(c|s)X(c), \\ \mathsf{y} &= \max_s \mathbb{E}_{(s)}[Y] = \max_s \sum_c p(c|s)Y(c). \end{aligned} \tag{7}$$

A full characterization of the set Φ_n for the original binary SV source is given in Appendix A.

To complete the proof of the lemma, it suffices to show that for all $(\mathsf{x}, \mathsf{y}) \in \Phi_n$ we have $\mathsf{y} \geq g(\mathsf{x})$. The latter statement can be proved by induction on n. The base of induction, $n = 0$, follows from $g(0) = 0$ and $g(1) = 1$. Assume that $(\mathsf{x}, \mathsf{y}) \in \Phi_n$ is obtained from (7) for $(X(c), Y(c)) \in \Phi_{n-1}$ for $c \in \mathcal{C}$. By the induction hypothesis we have $Y(c) \geq g(X(c))$ for all c. In other words, $Y \geq g(X)$, and then

$$\begin{aligned} g(\mathsf{x}) &= g\big(\min_s \mathbb{E}_{(s)}[X]\big) \\ &= \min_s g\big(\mathbb{E}_{(s)}[X]\big) \\ &\leq \max_s \mathbb{E}_{(s)}[g(X)] \\ &\leq \max_s \mathbb{E}_{(s)}[Y] \\ &= \mathsf{y}. \end{aligned}$$

Here in the second line we use the monotonicity of g, and in the fourth line we use the induction hypothesis. ☐

COROLLARY 11. *Consider a generalized SV source with alphabet $\mathcal{C}$, set of dice $\mathcal{S}$, and probabilities $p_s(c)$. Let $\mathcal{S}'$ be a subset of $\mathcal{S}$ and let $\mathcal{C}'$ be the set of all c for which there exists some $s \in \mathcal{S}'$ such that $p_s(c) > 0$. Suppose that there is no nonzero function $\psi : \mathcal{C} \to \mathbb{R}$ such that* (i) *ψ is zero on $\mathcal{C} - \mathcal{C}'$, and* (ii) *for all $s \in \mathcal{S}'$ we have $\mathbb{E}_{(s)}[\psi(C)] = 0$. Then deterministic randomness extraction from this generalized SV source is impossible.*

Proof. We show that the adversary can defeat the extractor even when it is restricted to the smaller set of dice $\mathcal{S}'$. When restricted to the set of dice $\mathcal{S}'$, the faces labeled by $\mathcal{C} - \mathcal{C}'$ show up with probability 0. So, we can pretend as if these faces did not exist. Now the condition that no such function ψ exists is exactly the condition in Theorem 9 for the set of dice $\mathcal{S}'$ having faces labeled from $\mathcal{C} - \mathcal{C}'$. ☐

3. Distributed SV sources.

Distributed SV sources can be defined similarly to generalized SV sources except that, in this case, the outcome in each time step is a pair that is distributed between two parties.

Definition 12. *Fix finite sets $\mathcal{A}, \mathcal{B}$, $\mathcal{S}$. Let $p_s(ab)$ be a probability distribution over $\mathcal{A} \times \mathcal{B}$ for any $s \in \mathcal{S}$. A distributed SV source with respect to distributions $p_s(ab)$ is defined as follows. The adversary in each time step i, depending on the previous outcomes $(a_1, b_1), \dots, (a_{i-1}, b_{i-1})$ chooses some s_i. Then (A_i, B_i) is sampled from the distribution $p_{s_i}(a_i b_i)$. The sequence of random variables $(A_1, B_1), (A_2, B_2), \dots,$ is called a distributed SV source.*

Here we assume that the outcomes of this SV source are distributed between two parties, say Alice and Bob. That is, in each time step i, A_i is revealed to Alice and B_i is revealed to Bob. So Alice receives the sequence $(A_1, A_2, \dots)$, and Bob receive the sequence $(B_1, B_2, \dots)$.

In this section we are interested in whether two parties can generate a common random bit from distributed SV sources. To be more precise, let us first define the problem more formally.

Definition 13. *We say that common randomness can be extracted from the family of distributed SV sources determined by $\{p_s(ab) : s \in \mathcal{S}\}$ if for every $\epsilon > 0$ there is n and functions $\Gamma_n : \mathcal{A}^n \to \{0, 1\}$ and $\Lambda_n : \mathcal{B}^n \to \{0, 1\}$ such that for every $(A_1, B_1), (A_2, B_2), \dots$ determined by a strategy of adversary as above, the distributions of $K_1 = \Gamma_n(A^n)$ and $K_2 = \Lambda_n(B^n)$ are ϵ-close (in total variation distance) to the uniform distribution, and that* $\Pr[K_1 \neq K_2] < \epsilon$.

In the above definition we considered only deterministic protocols for extracting a common random bit. We could also consider probabilistic protocols where Γ_n and Λ_n are random functions depending on the *private* randomnesses of Alice and Bob, respectively. More precisely, we could take $K_1 = \Gamma_n(A^n, R_1)$ and $K_2 = \Lambda_n(B^n, R_2)$ with the above conditions on K_1, K_2, where R_1 and R_2 are the private randomnesses of Alice and Bob, respectively, which are independent of the SV source and of each other. Nevertheless, if a common random bit can be extracted with probabilistic protocols, then common randomness extraction with deterministic protocols is also possible.

Lemma 14. *In the problem of common random bit extraction, with no loss of generality, we may assume that the parties do not have private randomness.*

Proof. Given a distributed SV source (A^n, B^n), assume that Alice and Bob produce binary random variables $K_1 = \Gamma_n(A^n, R_1)$ and $K_2 = \Lambda_n(B^n, R_2)$, where R_1 and R_2 are the private randomnesses of Alice and Bob respectively, which are independent of the SV source and of each other. The bits K_1 and K_2 are ϵ-close to the uniform distribution over $\{0, 1\}$ and that $\Pr[K_1 \neq K_2] < \epsilon$. Define

$$K_1' = \Gamma_n'(A^n) = \mathrm{argmax}_k \Pr[K_1 = k | A^n]$$

and

$$K_2' = \Lambda_n'(B^n) = \mathrm{argmax}_k \Pr[K_2 = k | B^n].$$

Then K_1' and K_2' are (deterministic) functions of A^n and B^n, respectively. We claim that

$$\Pr[K_1' \neq K_2'] \leq 3\epsilon$$

and

$$\left|\Pr[K_1' = 0] - \frac{1}{2}\right|, \left|\Pr[K_2' = 0] - \frac{1}{2}\right| \leq 2\epsilon.$$

Proving these inequalities would complete the proof.

Observe that for every $A^n = a^n$ we have

$$\Pr[K_1' \neq K_1 | A^n = a^n] = \min\{\Pr[K_1 = 0|a^n], \Pr[K_1 = 1|a^n]\}.$$

On the other hand,

$$\begin{aligned}\Pr[K_2 \neq K_1|a^n] &= \Pr[K_2 = 1|a^n]\Pr[K_1 = 0|a^n] + \Pr[K_2 = 0|a^n]\Pr[K_1 = 1|a^n]\\ &\geq \min\{\Pr[K_1 = 0|a^n], \Pr[K_1 = 1|a^n]\}\\ &= \Pr[K_1' \neq K_1|A^n = a^n].\end{aligned}$$

As a result, we have

$$\Pr[K_1' \neq K_1] \leq \Pr[K_2 \neq K_1] \leq \epsilon,$$

which gives

$$\left|\Pr[K_1' = 0] - \frac{1}{2}\right| \leq 2\epsilon.$$

This inequality for K_2' is proved similarly.

Next we have

$$\begin{aligned}\Pr[K_1' \neq K_2'] &\leq \Pr[K_1' \neq K_1] + \Pr[K_1 \neq K_2] + \Pr[K_2 \neq K_2']\\ &\leq \epsilon + \epsilon + \epsilon.\end{aligned}$$ □

3.1. Maximal correlation.

Let us first consider the problem of common randomness extraction in a simpler case where there is no adversary (in the i.i.d. case). That is, let us assume that we have only one distribution $p(ab)$, and Alice and Bob in each time i receive samples A_i and B_i from this distribution. The question of the possibility of common randomness extraction can be raised in this case too. Witsenhausen [27] used a measure of correlation called maximal correlation to prove a necessary and sufficient condition for the possibility of common randomness extraction from i.i.d. sources.

Definition 15 (maximal correlation). *The maximal correlation of random variables A and B with joint distribution $p(ab)$ defined on $\mathcal{A}$ and $\mathcal{B}$, respectively, is denoted by $\rho(A;B)$ and defined as follows:*

$$\begin{aligned}\rho(A;B) := \quad \max \quad & \mathbb{E}[XY],\\ \text{subject to: } & \mathbb{E}[X] = \mathbb{E}[Y] = 0,\\ & \mathbb{E}[X^2] = \mathbb{E}[Y^2] = 1,\end{aligned} \tag{8}$$

where the maximum is taken over all functions $X : \mathcal{A} \to \mathbb{R}$, $Y : \mathcal{B} \to \mathbb{R}$. Here the expected values are with respect to $p(ab)$, e.g., $\mathbb{E}[XY] = \sum_{a,b} p(ab)X(a)Y(b)$.

Maximal correlation has the intriguing property that if (A^n, B^n) is n i.i.d. copies of (A, B), then $\rho(A^n; B^n) = \rho(A; B)$. Moreover, maximal correlation does not increase under local stochastic maps [27].

From the definition and using the Cauchy–Schwarz inequality it is not hard to verify that $0 \leq \rho(A;B) \leq 1$. Further, $\rho(A;B) = 0$ if and only if A, B are independent. To characterize the other extreme case $\rho(A;B) = 1$ we need the notion of common data.

Definition 16. *We say that A, B have common data if there are nonconstant functions $\Gamma(A)$ and $\Lambda(B)$ with arbitrary but the same images, such that $\Gamma(A) = \Lambda(B)$ with probability one.*

Thus A and B have common data if Alice and Bob, having access to A and B, respectively, can compute the same nonconstant data (i.e., $\Gamma(A) = \Lambda(B)$) without communication. We have $\rho(A; B) = 1$ if and only if A, B have common data.

THEOREM 17 (see [27]). *A common random bit can be extracted from i.i.d. copies of A, B if and only if $\rho(A; B) = 1$.*

Here, we give an alternative proof of this theorem whose ideas will be used later. This proof of Witsenhausen's theorem can also be of independent interest.

To motivate our proof technique, and to elaborate on the difficulty we should overcome, assume that A and B have no common part ($\rho(A; B) < 1$), but Alice and Bob can extract common randomness by applying functions Γ and Λ on their observations, i.e., $\Gamma(A^n)$ and $\Lambda(B^n)$ are almost uniform, and $\Gamma(A^n) = \Lambda(B^n)$ with high probability. Since $\Gamma(A^n) = \Lambda(B^n)$ with high probability, there is some $(a_1, \dots, a_{n-1})$ and $(b_1, \dots, b_{n-1})$ such that conditioned on $A^{n-1} = a^{n-1}$ and $B^{n-1} = b^{n-1}$ we still have $\Gamma(A^n) = \Lambda(B^n)$ with high probability. Now we observe that after conditioning on $A^{n-1} = a^{n-1}$ and $B^{n-1} = b^{n-1}$, the functions $\Gamma(A^n)$ and $\Lambda(B^n)$ depend only on A_n and B_n. So we have found functions of A and B, respectively, that are equal with high probability. This may seem to be a contradiction with our assumption that A, B do not have common data. However, the random variables $\Gamma(A^n)$ or $\Lambda(B^n)$ may no longer be uniform when we condition on $A^{n-1} = a^{n-1}$ and $B^{n-1} = b^{n-1}$. In fact, $\Gamma(A^n)$ or $\Lambda(B^n)$ may even become constant after conditioning.

To overcome the difficulty discussed above, we consider three conditional probabilities after conditioning on $A^{n-1} = a^{n-1}$ and $B^{n-1} = b^{n-1}$. That is, we keep track of the conditional probability of $\Gamma(A^n) = \Lambda(B^n)$, as well as the marginal distributions of $\Gamma(A^n)$ and $\Lambda(B^n)$; our proof works by simultaneously keeping track of the values of these three conditional probabilities.

Proof. If $\rho(A; B) = 1$, then A, B have common data as defined above, and a common random bit can be extracted from that common data by standard randomness extractors for i.i.d. sources.

For the other direction, suppose that $\rho(A; B) = \rho < 1$, and that we can extract one bit of common randomness from A, B. By Lemma 14 we may assume that Alice and Bob's strategies for extracting common randomness are deterministic. That is, we may assume that there are subsets $\mathcal{I} \subseteq \mathcal{A}^n$ and $\mathcal{J} \subseteq \mathcal{B}^n$ such that Alice's extracted bit is $K_1 = 0$ if $A^n \in \mathcal{I}$ and Bob's extracted bit $K_2 = 0$ if $B^n \in \mathcal{J}$, and that K_1, K_2 are equal with high probability, and their distributions are close to the uniform distribution over $\{0, 1\}$.

Let us define

$$\begin{aligned}
\alpha(\mathcal{I}) &:= \Pr[A^n \in \mathcal{I}], \\
\beta(\mathcal{J}) &:= \Pr[B^n \in \mathcal{J}], \\
\gamma(\mathcal{I}, \mathcal{J}) &:= \Pr[A^n \in \mathcal{I} \ \&\ B^n \in \mathcal{J}].
\end{aligned}$$

By the assumption about the existence of randomness extractors the three numbers $\alpha(\mathcal{I}), \beta(\mathcal{J})$, and $\gamma(\mathcal{I}, \mathcal{J})$ are all close to 1/2.

For every $a \in \mathcal{A}$ and $b \in \mathcal{B}$ define $\mathcal{I}_a = \{a_{[2:n]} : (a, a_{[2:n]}) \in \mathcal{I}\}$ and $\mathcal{J}_b := \{b_{[2:n]} : (b, b_{[2:n]}) \in \mathcal{J}\}$. Then as in the proof of Theorem 9 the numbers $\alpha(\mathcal{I}), \beta(\mathcal{J})$, and $\gamma(\mathcal{I},\mathcal{J})$ can be computed recursively:

$$\alpha(\mathcal{I}) = \sum_a p(a)\alpha(\mathcal{I}_a) = \mathbb{E}[\alpha(\mathcal{I}_A)],$$
$$\beta(\mathcal{J}) = \sum_b p(b)\beta(\mathcal{J}_b) = \mathbb{E}[\beta(\mathcal{J}_B)],$$
$$\gamma(\mathcal{I},\mathcal{J}) = \sum_{a,b} p(a,b)\gamma(\mathcal{I}_a,\mathcal{J}_b) = \mathbb{E}[\gamma(\mathcal{I}_A,\mathcal{J}_B)].$$

For $n \geq 1$, let Φ_n be the set of triples $(\alpha(\mathcal{I}), \beta(\mathcal{J}), \gamma(\mathcal{I},\mathcal{J}))$ for all $\mathcal{I} \subseteq \mathcal{A}^n$ and $\mathcal{J} \subseteq \mathcal{B}^n$. Also let

$$\Phi_0 = \big\{\mathbf{e}_0 = (1,1,1), \mathbf{e}_1 = (1,0,0), \mathbf{e}_2 = (0,1,0), \mathbf{e}_3 = (0,0,0)\big\}. \tag{9}$$

Observe that Φ_0 corresponds to deterministic strategies of Alice and Bob that determine K_1, K_2 without looking at any random source. If, for instance, Alice always outputs $K_1 = 0$ and Bob always outputs $K_2 = 1$, then $\Pr[K_1 = 0] = 1$, $\Pr[K_2 = 0] = 0$, and $\Pr[K_1 = K_2 = 0] = 0$. This gives the triple $\mathbf{e}_1 = (1,0,0)$ in Φ_0.

Now since by the above discussions the numbers $\alpha(\mathcal{I}), \beta(\mathcal{J})$, and $\gamma(\mathcal{I},\mathcal{J})$ can be computed recursively, the sets Φ_n can be analyzed recursively too. Indeed, Φ_n for $n \geq 1$ is contained in the set of triples $(\mathsf{x},\mathsf{y},\mathsf{z})$ for which there exist functions $X : \mathcal{A} \mapsto \mathbb{R}$, $Y : \mathcal{B} \mapsto \mathbb{R}$, $Z : \mathcal{A}\times\mathcal{B} \mapsto \mathbb{R}$ such that for every pair (a,b), the triple $(X(a), Y(b), Z(a,b)) \in \Phi_{n-1}$, and that

$$\mathsf{x} = \mathbb{E}[X], \qquad \mathsf{y} = \mathbb{E}[Y], \qquad \mathsf{z} = \mathbb{E}[Z], \tag{10}$$

where the expected values are with respect to $p(ab)$, e.g., $\mathbb{E}[X] = \sum_a p(a)X(a), \mathbb{E}[Z] = \sum_{a,b} p(ab)Z(a,b)$.

Let us define the function $f : [0,1]^2 \to \mathbb{R}$ by

$$f(x,y,z) := (x+y)\rho - 2z + 2xy - (x^2+y^2)\rho, \tag{11}$$

where $\rho = \rho(A;B) < 1$.

We claim that $f(\alpha(\mathcal{I}), \beta(\mathcal{J}), \gamma(\mathcal{I},\mathcal{J})) \geq 0$. Assuming this, we conclude that $\alpha(\mathcal{I}), \beta(\mathcal{J})$, and $\gamma(\mathcal{I},\mathcal{J})$ cannot all be close to $1/2$ because f is continuous and

$$f(1/2,1/2,1/2) = -\frac{1-\rho}{2} < 0.$$

To prove our claim it suffices to show that $f(\mathsf{x},\mathsf{y},\mathsf{z}) \geq 0$ for all $(\mathsf{x},\mathsf{y},\mathsf{z}) \in \Phi_n$, which itself can be proved by induction on n. The base of induction, $n = 0$, follows from $f(\mathbf{e}_\ell) \geq 0$ for $0 \leq \ell \leq 3$, where $\mathbf{e}_\ell$ is defined in (9). Now suppose that $(\mathsf{x},\mathsf{y},\mathsf{z}) \in \Phi_n$ is obtained from functions X, Y, Z as above that satisfy (10). By the induction hypothesis for every (a,b) we have $f(X(a), Y(b), Z(ab)) \geq 0$. Then to prove $f(\mathsf{x},\mathsf{y},\mathsf{z}) \geq 0$, it suffices to show that

$$f(\mathsf{x},\mathsf{y},\mathsf{z}) \geq \mathbb{E}[f(X,Y,Z)].$$

Using (10), we need to show that

$$f(\mathbb{E}[X], \mathbb{E}[Y], \mathbb{E}[Z]) \geq \mathbb{E}[f(X,Y,Z)].$$

Using the definition of the function $f(\cdot)$ in (11), and by expanding both sides and canceling the linear terms, we need to show that

$$2\mathbb{E}[X]\mathbb{E}[Y] - \rho(\mathbb{E}[X]^2 + \mathbb{E}[Y]^2) \geq 2\mathbb{E}[XY] - \rho(\mathbb{E}[X^2] + \mathbb{E}[Y^2]).$$

Let us define $X' = X - \mathbb{E}[X]$ and $Y' = Y - \mathbb{E}[Y]$. Then, expressing the above inequality in terms of X', Y' we need to show that

$$2\mathbb{E}[X'Y'] \leq \rho(\mathbb{E}[X'^2] + \mathbb{E}[Y'^2]).$$

This inequality is a consequence of the definition of $\rho = \rho(A; B)$ because $\mathbb{E}[X'] = \mathbb{E}[Y'] = 0$ and then

$$\mathbb{E}[X'Y'] \leq \rho\sqrt{\mathbb{E}[X'^2]\mathbb{E}[Y'^2]} \leq \frac{1}{2}\rho(\mathbb{E}[X'^2] + \mathbb{E}[Y'^2]).$$

This completes the proof. □

Remark 18. To understand our choice of quadratic function $f(x, y, z)$ in (11), observe that $f(x, y, z) \geq 0$ is equivalent with

$$\rho \geq \frac{z - xy}{\frac{1}{2}(x - x^2) + \frac{1}{2}(y - y^2)}.$$

Let us take binary random variables K_1 and K_2, and let $x = p(K_1 = 0)$, $y = p(K_2 = 0)$, and $z = p(K_1 = 0, K_2 = 0)$. Then,

$$\begin{aligned}\frac{z - xy}{\frac{1}{2}(x - x^2) + \frac{1}{2}(y - y^2)} &= \frac{\mathrm{Cov}(K_1, K_2)}{\frac{1}{2}\mathrm{Var}(K_1) + \frac{1}{2}\mathrm{Var}(K_2)}\\ &\leq \frac{\mathrm{Cov}(K_1, K_2)}{\sqrt{\mathrm{Var}(K_1)\mathrm{Var}(K_2)}}\\ &\leq \rho(K_1; K_2).\end{aligned}$$

Therefore the inequality

$$\rho = \rho(A, B) \geq \frac{z - xy}{\frac{1}{2}(x - x^2) + \frac{1}{2}(y - y^2)}$$

is in some sense comparing $\rho(A; B)$ with a lower bound on $\rho(K_1; K_2)$.

3.2. Common data. In the previous subsection we briefly discussed the notion of common data and recalled that $\rho(A; B) = 1$ if and only if common data exist. To state our result, however, we need a more precise characterization of common data. (A similar discussion of common data in terms of bipartite graphs can be found in [28].)

Suppose that A, B have common data, meaning that there are nonconstant functions $\Gamma(A)$ and $\Lambda(B)$ such that $\Gamma(A) = \Lambda(B)$. Let $\mathcal{C}$ be the images of these functions. For any $c \in \mathcal{C}$ define $\mathcal{A}_c = \Gamma^{-1}(c)$ and $\mathcal{B}_c = \Lambda^{-1}(c)$. Given the fact that $\Gamma(A) = \Lambda(B)$ always holds, then for every $c \neq c'$ and $(a, b) \in \mathcal{A}_c \times \mathcal{B}_{c'}$ we must have $p(ab) = 0$.

To understand this more precisely consider a bipartite graph $\mathcal{G}$ on the vertex set $\mathcal{A} \cup \mathcal{B}$ with an edge between (a, b) if $p(ab) \neq 0$. Then by the above observation, the existence of common data implies that the graph $\mathcal{G}$ is disconnected (and also at least two of the connected compoenents are not singletons); if $c \neq c'$ then there is no edge between vertices in $\mathcal{A}_c \cup \mathcal{B}_c$ and $\mathcal{A}_{c'} \cup \mathcal{B}_{c'}$.

Conversely, if $\mathcal{G}$ is disconnected (and also at least two of the connected components are not singletons) then common data exist; letting $\mathcal{C}$ be the sets of connected components, and defining $\Gamma(a), \Lambda(b)$ to be the index of the connected component to

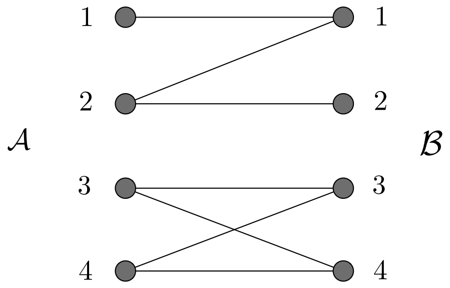

FIG. 2. *The graph associated with the probability distribution given in Example* 20. *This graph has two nonsingleton connected components, so A and B have common data.*

which a, b belong, we have $\Gamma(A) = \Lambda(B)$. As a result, $\rho(A;B) = 1$ if and only if $\mathcal{G}$ is disconnected (and at least two of the connected components are not singletons).

We summarize the above discussion in the following lemma.

LEMMA 19. *Let C be the random variable associated with the index of the connected component of $\mathcal{G}$ to which (A, B) belong. Then C can be computed as a function of A or B individually. Moreover, any common data of A, B is a function of C, and $\rho(A;B) = 1$ if and only if C is nonconstant (i.e., $\mathcal{G}$ has at least two nonsingleton connected components).*

Example 20. Consider the following joint distribution on $\mathcal{A} \times \mathcal{B}$ where $\mathcal{A} = \mathcal{B} = \{1, 2, 3, 4\}$:

		B			
		1	2	3	4
	1	0.1	0	0	0
A	2	0.1	0.2	0	0
	3	0	0	0.1	0.1
	4	0	0	0.2	0.2

The graph associated with this distribution is given in Figure 2. This graph is disconnected. The common data of A, B is a binary random variable, determined by whether A and B are both in $\{1, 2\}$ or in $\{3, 4\}$.

Let $c \in \mathcal{C}$ be a connected component of $\mathcal{G}$. Then $p(ab|c)$, the distribution of A, B conditioned on $C = c$, does not have common data. This is because the bipartite graph associated with this conditional distribution is nothing but the cth connected component of $\mathcal{G}$, which by definition is connected. Denoting the maximal correlation of this conditional distribution by $\rho(A;B|C = c)$ we find that

$$\rho(A;B|C = c) < 1. \tag{12}$$

DEFINITION 21 (conditional maximal correlation [2]). *Let $p(abc)$ be a tripartite distribution. We define*

$$\rho(A;B|C) := \max_{c\colon p(c)>0} \rho(A;B|C = c),$$

where $\rho(A;B|C = c)$ is the maximal correlation of the conditional bipartite distribution $p(ab|c)$.

With this definition, for all bipartite distributions $p(ab)$, if we define C to be the common part of A and B, (12) then implies that

$$\rho(A;B|C) < 1. \tag{13}$$

3.3. Common data of a distributed SV source. Given a family of distributed SV sources specified by distributions $p_s(ab)$, our goal is to determine whether a common random bit can be extracted from this source or not. Suppose that for some $s \in \mathcal{S}$, the maximal correlation of $p_s(ab)$, which we denote by $\rho_s(A;B)$, is less than 1. Then, by Theorem 17 common randomness extraction is impossible because the adversary can in all time steps choose $S_i = s$ to obtain an i.i.d. source. So we may assume that $\rho_s(A;B) = 1$ for all s.

Let $\mathcal{G}_s$ be the bipartite graph associated with the bipartite distribution $p_s(ab)$. By the above observation we let $\rho_s(A;B) = 1$ and then $\mathcal{G}_s$ has at least two nonsingleton connected components. We claim that even the graph $\bigcup_s \mathcal{G}_s$, obtained by the union of edges of individual graphs $\mathcal{G}_s$, should also have at least two nonsingleton components. To see this, assume that the adversary in each time step chooses $s_i \in \mathcal{S}$ uniformly at random and independent of the past. Then we obtain an i.i.d. source with distribution

$$q(ab) = \frac{1}{|\mathcal{S}|}\sum_s p_s(ab).$$

Then common randomness can be extracted from this i.i.d. source, only if the bipartite graph associated with $q(ab)$ is disconnected. It is easy to verify that this bipartite graph is nothing but $\bigcup_s \mathcal{G}_s$. So without loss of generality we may assume that $\bigcup_s \mathcal{G}_s$ has at least two nonsingleton connected components.

The following lemma summarizes the above discussion.

LEMMA 22. *For a family of distributed SV sources determined by distributions $p_s(ab)$, $s \in \mathcal{S}$, we let $\mathcal{G}_s$ be the bipartite graph associated with $p_s(ab)$, and define $\bar{\mathcal{G}} = \bigcup_s \mathcal{G}_s$. Then a common bit can be extracted from the distributed SV source only if $\bar{\mathcal{G}}$ has at least two nonsingleton connected components.*

DEFINITION 23. *Let $\bar{\mathcal{G}}$ be the bipartite graph defined in Lemma 22 associated with the family of distributed SV sources determined by $p_s(ab)$ for $s \in \mathcal{S}$. Let $\mathcal{C}$ be the set of connected components of $\bar{\mathcal{G}}$. Then we define the distributions $p_s(abc)$ on $\mathcal{A} \times \mathcal{B} \times \mathcal{C}$ as follows: if $p_s(ab) > 0$ and $c \in \mathcal{C}$ is the connected component containing the edge $\{a, b\}$ in $\bar{\mathcal{G}}$ we let $p_s(abc) = p_s(ab)$; otherwise we let $p_s(abc) = 0$.*

Let $\Gamma : \mathcal{A} \to \mathcal{C}$ be the function that assigns $a \in \mathcal{A}$ to the connected component containing it. Similarly, let $\Lambda : \mathcal{B} \to \mathcal{C}$ be the function that assigns $b \in \mathcal{B}$ to the connected component containing b. Then letting $(A_1, B_1), (A_2, B_2), \dots$ be a distributed SV source for a fixed strategy of the adversary, we have $C_i = \Gamma(A_i) = \Lambda(B_i)$. Indeed, $(C_1, C_2, \dots)$ itself is a generalized SV source which can be computed by any of the parties individually. Thus, $(C_1, C_2, \dots)$ is a common part of the distributed SV source. Moreover, by the above discussion, if the adversary always outputs $s \in \mathcal{S}$ uniformly at random, C_i is the maximal common part that can be computed by both the parties given A_i and B_i.

Example 24. Consider the following two joint distributions on A and B. The graph corresponding to both of these distributions has three connected components. But if we superimpose these two distributions over each other (by choosing each with probability half), the graph of the resulting distribution has only two connected components:

		B			
		1	2	3	4
A	1	0.1	0	0	0
	2	0	0.2	0	0
	3	0	0	0.1	0.1
	4	0	0	0.3	0.2

		B			
		1	2	3	4
A	1	0.2	0	0	0
	2	0.1	0.1	0	0
	3	0	0	0.3	0
	4	0	0	0	0.3

3.4. Common random bit extraction from distributed SV sources.

We now have all the required tools to state and prove our main result about common randomness extraction from distributed SV sources.

THEOREM 25. *Consider a distributed SV source (as in Definition* 12*) with corresponding sets $\mathcal{S}$, $\mathcal{A}$, and $\mathcal{B}$ and corresponding distributions $p_s(ab)$. Let $p_s(abc)$, $s \in \mathcal{S}$, be the distributions given in Definition* 23*. Suppose that there is no nonzero function $\psi : \mathcal{C} \to \mathbb{R}$ such that $\mathbb{E}_{(s)}[\psi(C)] = 0$ for all s, where the expectation value is computed with respect to $p_s(abc)$. Then common randomness cannot be extracted from this distributed SV source.*

A possible algorithm to extract common random bits is one that would focus on the common part that can be computed by both Alice and Bob. Indeed, $(C_1, C_2, \dots)$ itself can be thought of as a generalized SV source. If deterministic randomness extraction from this source is possible, then Alice and Bob can obtain a common random bit by individually applying the randomness extraction protocol. Comparing with Theorems 4 and 9, and assuming $p_s(c) > 0$ for all s, c, the above theorem states that a common random bit can be extracted if and only if deterministic randomness extraction from $(C_1, C_2, \dots)$ is possible.

The proof of this theorem is essentially obtained by combining the ideas developed in the proofs of Theorems 9 and 17. We present the proof in the following section.

4. Proof of Theorem 25.

First we show that it suffices to prove Theorem 25 in the following special case.

LEMMA 26. *If Theorem* 25 *holds in the special case where distributions $p_s(ab)$ satisfy*

$$p_s(a), p_s(b) > 0 \qquad \forall s, a, b \tag{14}$$

and

$$\rho(A;B|CS) := \max_s \rho_s(A;B|C) < 1, \tag{15}$$

where $\rho_s(A;B|C)$ denotes the conditional maximal correlation of A and B given C with respect to the distribution $p_s(abc)$, then the theorem holds in general.

Proof. For any $s \in \mathcal{S}$ define $q_s(a,b)$ as follows:

$$q_s(a,b) := \frac{2}{3} p_s(a,b) + \frac{1}{3|\mathcal{S}|} \sum_{s' \in \mathcal{S}} p_{s'}(a,b). \tag{16}$$

Observe that $q_s(\cdot)$ is in the convex hull of distributions $p_{s'}(\cdot)$ for different values of s'. Thus in each step, the adversary can enforce that the pair (a,b) generated by the source has distribution $q_s(a,b)$ via a randomized strategy. As a result, it suffices to show the impossibility of common randomness extraction from the distributed SV source with distributions $q_s(\cdot)$ instead of $p_s(\cdot)$. Now we only need to show that $q_s(\cdot)$ satisfies (14) and (15) as well as the assumption of Theorem 25.

First, by the definitions of $q_s(\cdot)$ given in (16) the support of $q_s(\cdot)$ does not depend on s, and, if $q_s(a) = 0$ for some a, implies that $p_s(a) = 0$ for all s. In this case $A = a$ can never occur regardless of s. Therefore, it can be removed from $\mathcal{A}$. Thus, without loss of generality, we may assume that for any $a \in \mathcal{A}$ we have $q_s(a) > 0$. Similarly, we may assume that for any $b \in \mathcal{B}$ we have $q_s(b) > 0$.

Second, it is not hard to see that the graph $\mathcal{G}'_s$ associated with distributions $q_s(\cdot)$ is the same for all s and is equal to the graph $\bar{\mathcal{G}} = \cup_s \mathcal{G}_s$ associated with the original distributions $p_s(\cdot)$. This, in particular, implies that $\bar{\mathcal{G}}' = \bar{\mathcal{G}}$ and the common part remains the same. Moreover, for any s, c, we have $\rho(A;B|c,s) < 1$ for distribution $q_s(\cdot)$ because the connected components of the graph $\bar{\mathcal{G}}$ are nothing but elements of $\mathcal{C}$.

We finally verify that there is no nonzero $\psi : \mathcal{C} \to \mathbb{R}$ such that the expected value of $\psi(C)$ with respect to $q_s(\cdot)$ is zero for all s. Suppose such a function ψ exists. Then, from the definition of $q_s(\cdot)$ in (16), we have

$$\frac{2}{3}\mathbb{E}_{(s)}[\psi] + \frac{1}{3|\mathcal{S}|}\sum_{s'}\mathbb{E}_{(s')}[\psi] = 0, \tag{17}$$

where $\mathbb{E}_{(s)}[\cdot]$ denotes expectation with respect to $p_s(\cdot)$. Summing the above equations for all $s \in \mathcal{S}$, we find that

$$\sum_s \mathbb{E}_{(s)}[\psi] = 0,$$

and then using (17) again we obtain

$$\frac{2}{3}\mathbb{E}_{(s)}[\psi] - \frac{1}{3|\mathcal{S}|}\mathbb{E}_{(s)}[\psi] = 0.$$

This implies that $\mathbb{E}_{(s)}[\psi] = 0$. Therefore by the assumption of Theorem 25 the function ψ should be zero. ∎

By the above lemma, from now on we assume that the distributions $p_s(\cdot)$ satisfy the extra assumptions (14) and (15).

Suppose that common random bit extraction is possible. By Lemma 14 we may assume that Alice and Bob's protocol is deterministic and is described by subsets $\mathcal{I} \subseteq \mathcal{A}^n$ and $\mathcal{J} \subseteq \mathcal{B}^n$. That is, Alice's output is $K_1 = 0$ if $a^n \in \mathcal{I}$ and Bob's output is $K_2 = 0$ if $b^n \in \mathcal{J}$.

Let us define

$$\begin{aligned}\alpha(\mathcal{I}) &:= \max \Pr[A^n \in \mathcal{I}],\\ \beta(\mathcal{J}) &:= \max \Pr[B^n \in \mathcal{J}],\\ \gamma(\mathcal{I},\mathcal{J}) &:= \min \Pr[A^n \in \mathcal{I},\, B^n \in \mathcal{J}],\end{aligned}$$

where A^n denotes the sequence $(A_1, A_2, \ldots, A_n)$ which is not necessarily i.i.d. due to the adversarial nature of the SV source; similarly B^n denotes the sequence $(B_1, B_2, \ldots, B_n)$ of the SV source.

The maximizations and the minimization are computed over all strategies of the adversary. If common randomness extraction is possible, then there are n and $\mathcal{I} \subseteq \mathcal{A}^n$ and $\mathcal{J} \subseteq \mathcal{B}^n$ such that all three numbers $\alpha(\mathcal{I}), \beta(\mathcal{J})$, and $\gamma(\mathcal{I},\mathcal{J})$ are close to 1/2.

For $n \geq 1$ let Φ_n be the set of triples $(\alpha(\mathcal{I}), \beta(\mathcal{J}), \gamma(\mathcal{I}, \mathcal{J}))$ for all subsets $\mathcal{I} \subseteq \mathcal{A}^n$ and $\mathcal{J} \subseteq \mathcal{B}^n$. We also define

$$\Phi_0 = \big\{\mathbf{e}_0 = (1,1,1), \mathbf{e}_1 = (1,0,0), \mathbf{e}_2 = (0,1,0), \mathbf{e}_3 = (0,0,0)\big\}.$$

As discussed in the proof of Theorem 17 the set Φ_0 corresponds to deterministic strategies where the parties do not look at the source at all. By the above discussion we need to show that $(1/2, 1/2, 1/2)$ is far from $\cup_n \Phi_n$.

By the same ideas as in the proofs of Theorems 9 and 17 the sets Φ_n can be analyzed recursively. For every a, b and $\mathcal{I} \subseteq \mathcal{A}^n$ and $\mathcal{J} \subseteq \mathcal{B}^n$ define

$$\mathcal{I}_a := \{a_{[2:n]} : (a, a_{[2:n]}) \in \mathcal{I}\}, \qquad \mathcal{J}_b := \{b_{[2:n]} : (b, b_{[2:n]}) \in \mathcal{J}\}.$$

Then we have

$$\alpha(\mathcal{I}) = \max_s \mathbb{E}_{(s)}[\alpha(\mathcal{I}_A)],$$
$$\beta(\mathcal{J}) = \max_s \mathbb{E}_{(s)}[\beta(\mathcal{J}_B)],$$
$$\gamma(\mathcal{I}, \mathcal{J}) = \min_s \mathbb{E}_{(s)}[\gamma(\mathcal{I}_A, \mathcal{J}_B)],$$

where, as before,

$$\mathbb{E}_{(s)}[\alpha(\mathcal{I}_A)] = \sum_a p_s(a)\alpha(\mathcal{I}_a)$$

and

$$\mathbb{E}_{(s)}[\gamma(\mathcal{I}_A, \mathcal{J}_B)] = \sum_{a,b} p_s(ab)\gamma(\mathcal{I}_a, \mathcal{J}_b).$$

As a result, the sets Φ_n can be analyzed recursively as follows. Φ_n is indeed contained in the set of triples $(\mathsf{x}, \mathsf{y}, \mathsf{z})$ for which there are functions $X : \mathcal{A} \mapsto \mathbb{R}$, $Y : \mathcal{B} \mapsto \mathbb{R}$, $Z : \mathcal{A} \times \mathcal{B} \mapsto \mathbb{R}$ such that for every pair (a, b), the triple $(x_a, y_b, z_{ab}) \in \Phi_{n-1}$, where $x_a = X(a)$, $y_b = Y(b)$, and $z_{ab} = Z(ab)$ and, furthermore,

$$\mathsf{x} = \max_s \mathbb{E}_{(s)}[X], \qquad \mathsf{y} = \max_s \mathbb{E}_{(s)}[Y], \qquad \mathsf{z} = \min_s \mathbb{E}_{(s)}[Z]. \tag{18}$$

We now prove that Φ_n for every n is far from $(1/2, 1/2, 1/2)$.

THEOREM 27. *Let*

$$0 < \epsilon \leq \frac{\Delta'(1-\rho)}{1+\Delta'}$$

and $\kappa \geq 24|\mathcal{A}||\mathcal{B}|/\Delta + 2$, *where* Δ *and* Δ' *are two positive constants that are specified later (in Lemmas* 29 *and* 30*). Define*

$$f(x, y, z) = \kappa(x + y) - 2(\kappa + \epsilon)z + 2xy - (1 - \epsilon)(x^2 + y^2).$$

Then with the assumption of Theorem 25 *and* (14) *and* (15), *for all functions* $X : \mathcal{A} \mapsto \mathbb{R}$, $Y : \mathcal{B} \mapsto \mathbb{R}$, $Z : \mathcal{A} \times \mathcal{B} \mapsto \mathbb{R}$, *we have*

$$f(\mathsf{x}, \mathsf{y}, \mathsf{z}) \geq \min_s \mathbb{E}_{(s)}[f(X, Y, Z)],$$

where

$$\mathsf{x} = \max_s \mathbb{E}_{(s)}[X], \qquad \mathsf{y} = \max_s \mathbb{E}_{(s)}[Y], \qquad \mathsf{z} = \min_s \mathbb{E}_{(s)}[Z].$$

Given this theorem we can finish the proof of Theorem 25. Observe that $f(\mathbf{e}_i) \geq 0$ for $0 \leq i \leq 3$. Then by the above theorem and a simple induction, for any $(\mathsf{x}, \mathsf{y}, \mathsf{z}) \in \Phi_n$ we have $f(\mathsf{x}, \mathsf{y}, \mathsf{z}) \geq 0$. We, however, have $f(1/2, 1/2, 1/2) = -\epsilon/2 < 0$. Then by the continuity of f, the point $(1/2, 1/2, 1/2)$ is far from Φ_n for any n.

The proof of Theorem 27 is the most technical part of this paper; its proof is given after stating some definitions and lemmas.

4.1. Some preliminary definitions and lemmas.

In this section, we let $\mathbb{E}_{(cs)}[\cdot]$ be the expectation with respect to the conditional probability distribution $p_s(ab|c)$.

A characterization of conditional maximal correlation.

LEMMA 28. *Assume that $\rho(A;B|CS)$ is strictly less than one for the collection of distributions $p_s(ab|c)$ given in Definition 23. Then,*

$$\mathbb{E}_{(s)}[XY] \leq \rho(A;B|CS)\sqrt{\mathbb{E}_{(s)}[X^2]\mathbb{E}_{(s)}[Y^2]} \tag{19}$$

holds for all s and functions $X : \mathcal{A} \to \mathbb{R}, Y : \mathcal{B} \to \mathbb{R}$ such that

$$\mathbb{E}_{(cs)}[X] = \mathbb{E}_{(cs)}[Y] = 0 \qquad \forall c$$

where we use the notation set up before, e.g., $\mathbb{E}_{(cs)}[X] = \sum_{ab} p_s(ab|c)X(a)$.

Proof of Lemma 28. Assume that $\rho = \rho(A;B|CS) < 1$. Fix a value of s and take two arbitrary functions $X : \mathcal{A} \to \mathbb{R}$ and $Y : \mathcal{B} \to \mathbb{R}$ such that

$$\mathbb{E}_{(cs)}[X] = \mathbb{E}_{(cs)}[Y] = 0 \qquad \forall c.$$

Here $\mathbb{E}_{(cs)}[X] = \sum_{ab} p_s(ab|c)x_a = \sum_a p_s(a|c)x_a$, where $x_a = X(a)$ for any $a \in \mathcal{A}$. Similarly $\mathbb{E}_{(cs)}[Y] = \sum_b p_s(b|c)y_b$. Then, from the definition of $\rho = \rho(A;B|CS)$ we must have

$$\mathbb{E}_{(cs)}[XY] \leq \rho\sqrt{\mathbb{E}_{(cs)}[X^2]\mathbb{E}_{(cs)}[Y^2]} \tag{20}$$

for all c. Using the joint convexity of $f(x,y) = \sqrt{xy}$ we have that

$$\begin{aligned}
\mathbb{E}_{(s)}[XY] &\leq \sum_c p_s(c)\rho\sqrt{\mathbb{E}_{(cs)}[X^2]\mathbb{E}_{(cs)}[Y^2]} \\
&\leq \rho\sqrt{\left(\sum_c p_s(c)\mathbb{E}_{(cs)}[X^2]\right)\left(\sum_c p_s(c)\mathbb{E}_{(cs)}[Y^2]\right)} \\
&= \rho\sqrt{\mathbb{E}_{(s)}[X^2]\mathbb{E}_{(s)}[Y^2]}. \qquad (21)
\end{aligned}$$

On the other hand, (21) implies (20) by choosing X and Y to be zero whenever C is not equal to some given c. Therefore (19) is a complete characterization of the conditional maximal correlation. □

Definitions of $\mathcal{L}_A$, $\mathcal{L}_B$, $\mathcal{L}_A^\perp$ and $\mathcal{L}_B^\perp$. Let $\mathcal{L}_A$ be the linear space of functions $X : \mathcal{A} \to \mathbb{R}$ such that $\mathbb{E}_{(s)}[X]$ is independent of s, i.e.,

$$\mathcal{L}_A := \{X : \mathcal{A} \to \mathbb{R} : \mathbb{E}_{(s)}[X] = \mathbb{E}_{(s')}[X], \ \forall s, s'\}. \tag{22}$$

Let $\mathcal{L}_A^\perp$ be the orthogonal complement of $\mathcal{L}_A$ with respect to the inner product $\langle\cdot,\cdot\rangle_*$, which is the inner product with respect to the uniform distribution, i.e.,

$$\mathcal{L}_A^\perp := \left\{X : \mathcal{A} \to \mathbb{R} : \langle X, X'\rangle_* = \sum_a \frac{1}{|\mathcal{A}|}X(a)X'(a) = 0, \ \forall X' \in \mathcal{L}_A\right\}.$$

We define $\mathcal{L}_B$ and $\mathcal{L}_B^\perp$ similarly.

LEMMA 29. *There is $\Delta > 0$ such that for all vectors $X \in \mathcal{L}_A^{\perp}$ and $Y \in \mathcal{L}_B^{\perp}$ we have*

$$\max_{s,s'} \mathbb{E}_{(s)}[X] - \mathbb{E}_{(s')}[X] \geq \Delta \|X\|_*$$

and

$$\max_{s,s'} \mathbb{E}_{(s)}[Y] - \mathbb{E}_{(s')}[Y] \geq \Delta \|Y\|_*.$$

Proof. It suffices to show that

$$\max_{s,s'} \mathbb{E}_{(s)}[X] - \mathbb{E}_{(s')}[X] > 0$$

for any $X \in \mathcal{L}_A^{\perp}$ with $\|X\|_* = 1$. The proof then follows from the compactness of the unit ball in $\mathcal{L}_A^{\perp}$. To show the above inequality note that the left-hand side is always nonnegative, and that it is zero if and only if $X \in \mathcal{L}_A$. But since $0 \neq X \in \mathcal{L}_A^{\perp}$, it cannot be in $\mathcal{L}_A$. We are done. □

Definitions of $\mathcal{L}'_A$ and $\mathcal{L}'_B$. In Theorem 25 we assume that there is no nonconstant $\psi : \mathcal{C} \to \mathbb{R}$ such that $\mathbb{E}_{(s)}[\psi]$ is independent of s. To state this property in terms of our notations, let us define $\mathcal{K}_A$ be the set of functions $U : \mathcal{A} \to \mathbb{R}$ such that U is determined by C, i.e.,

$$\mathcal{K}_A := \{U : \mathcal{A} \to \mathbb{R} : \, U(a) = U(a'), \ \forall a, a' \text{ s.t. } C(a) = C(a')\}.$$

With abuse of notation for a function $U \in \mathcal{K}_A$ we may use $U(c)$ since U is indeed a function of C.

Then the assumption of Theorem 25 equivalently means that $\mathcal{L}_A \cap \mathcal{K}_A$ contains only constant functions, i.e.,

$$\mathcal{L}_A \cap \mathcal{K}_A = \{r\mathbf{1}_{\mathcal{A}} : \, r \in \mathbb{R}\}.$$

Let us define

$$\mathcal{L}'_A := \mathcal{L}_A \cap (\mathbf{1}_{\mathcal{A}})^{\perp}, \tag{23}$$

where $(\mathbf{1}_{\mathcal{A}})^{\perp}$ is computed with respect to the inner product $\langle \cdot, \cdot \rangle_*$ (inner product with respect to the uniform distribution). Then the above condition implies that

$$\mathcal{L}'_A \cap \mathcal{K}_A = \{0\}. \tag{24}$$

We similarly define $\mathcal{K}_B$ and $\mathcal{L}'_B$ and have $\mathcal{L}'_B \cap \mathcal{K}_B = \{0\}$.

Definitions of $\mathcal{K}_A^{\perp_s}$ and $\mathcal{K}_B^{\perp_s}$. Let $\mathcal{K}_A^{\perp_s}$ and $\mathcal{K}_B^{\perp_s}$ be the orthogonal complements of $\mathcal{K}_A$ and $\mathcal{K}_B$, respectively, with respect to the inner product $\langle \cdot, \cdot \rangle_{(s)}$. We define

$$\mathcal{K}_A^{\perp_s} = \{U' : \mathcal{A} \to \mathbb{R} : \mathbb{E}_{(s)}[U'X] = 0, \ \forall X \in \mathcal{K}_A\},$$

and similarly we define $\mathcal{K}_B^{\perp_s}$. Note that $\langle \cdot, \cdot \rangle_{(s)}$ is indeed an inner product because of assumption (14). Then the above orthogonal complement is well-defined. Observe that

$$\mathcal{K}_A^{\perp_s} = \{U' : \mathcal{A} \to \mathbb{R} : \, \mathbb{E}_{(cs)}[U'] = 0, \ \forall c\}.$$

We can write any function $X : \mathcal{A} \to \mathbb{R}$ as $X = U + U'$, where $U \in \mathcal{K}_A$ and $U' \in \mathcal{K}_A^{\perp_s}$. Indeed, let

$$U = \mathbb{E}_{(C(a)s)}[X].$$

Then we have

$$\mathbb{E}_{(cs)}[U'] = \mathbb{E}_{(cs)}[X - U] = \mathbb{E}_{(cs)}[X] - U(c) = 0.$$

Therefore, by definition $U' \in \mathcal{K}_A^{\perp_s}$.

Lemma 30. *There is $\Delta' > 0$ such that for any $X \in \mathcal{L}'_A$, $Y \in \mathcal{L}'_B$, and $s \in \mathcal{S}$ we have*

$$\|U'\|_{(s)} \geq \Delta' \|U\|_{(s)}, \qquad \|V'\|_{(s)} \geq \Delta' \|V\|_{(s)},$$

where $U \in \mathcal{K}_A$ and $U' \in \mathcal{K}_A^{\perp_s}$ are such that $X = U + U'$. Functions $V \in \mathcal{K}_B$ and $V' \in \mathcal{K}_B^{\perp_s}$ are defined similarly.

Proof. Without loss of generality, we can restrict to $X \in \mathcal{L}'_A$, where $\|X\|_{(s)} = 1$. Using (24) we have $U' \neq 0$ for any such X. Thus $\|U\|_{(s)}/\|U'\|_{(s)}$ is well-defined and continuous as a function on the unit sphere of $\mathcal{L}'_A$. Therefore, it achieves its maximum. Let $\kappa_s < \infty$ be the maximum of $\|U\|_{(s)}/\|U'\|_{(s)}$ and $\|V\|_{(s)}/\|V'\|_{(s)}$ over the unit balls of $\mathcal{L}'_A$ and $\mathcal{L}'_B$. Then the the choice of $\Delta' = \min_s(1/\kappa_s)$ works. □

Now we have all the required tools to prove Theorem 27.

4.2. Proof of Theorem 27.

First note that $f(x, y, z)$ is monotonically increasing in its first and second arguments on $[0, 1]$ and monotonically decreasing in its third argument. For instance, the derivative with respect to y is $\kappa + 2z - 2(1 - \epsilon)x$ which is nonnegative for $x, z \in [0, 1]$ since $\kappa \geq 2$. Therefore, we have

$$\begin{aligned} f(\mathsf{x}, \mathsf{y}, \mathsf{z}) &= f\left(\max_{s_1} \mathbb{E}_{(s_1)}[X], \max_{s_2} \mathbb{E}_{(s_2)}[Y], \min_{s_3} \mathbb{E}_{(s_3)}[Z]\right) \\ &= \max_{s_1, s_2, s_3} f\big(\mathbb{E}_{(s_1)}[X], \mathbb{E}_{(s_2)}[Y], \mathbb{E}_{(s_3)}[Z]\big), \end{aligned}$$

where to recall our notation, for instance, $\mathbb{E}_{(s_1)}[X] = \sum_a p_{s_1}(a) X(a)$. To prove the theorem, we thus need to show that for any arbitrary functions $X : \mathcal{A} \mapsto \mathbb{R}$, $Y : \mathcal{B} \mapsto \mathbb{R}$, $Z : \mathcal{A} \times \mathcal{B} \mapsto \mathbb{R}$, we have

$$g(X, Y, Z) := \max_{s, s_1, s_2, s_3} \Big(f\big(\mathbb{E}_{(s_1)}[X], \mathbb{E}_{(s_2)}[Y], \mathbb{E}_{(s_3)}[Z]\big) - \mathbb{E}_{(s)}[f(X, Y, Z)] \Big) \geq 0.$$

Let $X = X' + X''$, where $X' \in \mathcal{L}_A$ and $X'' \in \mathcal{L}_A^{\perp}$. Therefore using (22) we have

$$\mathbb{E}_{(s)}[X'] = \mathbb{E}_{(s_1)}[X'] \qquad \forall s, s_1. \tag{25}$$

Similarly let $Y = Y' + Y''$ where $Y' \in \mathcal{L}_B$ and $Y'' \in \mathcal{L}_B^{\perp}$. Assume without loss of generality that

$$\|X''\|_* \geq \|Y''\|_*. \tag{26}$$

We now compute

$$\begin{aligned}
g(X,Y,Z) &\geq \max_{s,s_1} f\big(\mathbb{E}_{(s_1)}[X],\mathbb{E}_{(s)}[Y],\mathbb{E}_{(s)}[Z]\big) - \mathbb{E}_{(s)}[f(X,Y,Z)]\\
&= \max_{s,s_1} \bigg(\kappa(\mathbb{E}_{(s_1)}[X]+\mathbb{E}_{(s)}[Y]) - 2(\kappa+\epsilon)\mathbb{E}_{(s)}[Z] + 2\mathbb{E}_{(s_1)}[X]\mathbb{E}_{(s)}[Y]\\
&\qquad - (1-\epsilon)(\mathbb{E}_{(s_1)}[X]^2+\mathbb{E}_{(s)}[Y]^2)\\
&\qquad - \mathbb{E}_{(s)}\big[\kappa(X+Y) - 2(\kappa+\epsilon)Z + 2XY - (1-\epsilon)(X^2+Y^2)\big]\bigg)\\
&= \max_{s,s_1} \kappa\Big(\mathbb{E}_{(s_1)}[X] - \mathbb{E}_{(s)}[X]\Big) + 2\Big(\mathbb{E}_{(s_1)}[X]\mathbb{E}_{(s)}[Y] - \mathbb{E}_{(s)}[XY]\Big)\\
&\quad - (1-\epsilon)\Big(\mathbb{E}_{(s_1)}[X]^2 - \mathbb{E}_{(s)}[X^2] + \mathbb{E}_{(s)}[Y]^2 - \mathbb{E}_{(s)}[Y^2]\Big)\\
&= \max_{s,s_1} \kappa\Big(\mathbb{E}_{(s_1)}[X''] - \mathbb{E}_{(s)}[X'']\Big) + 2\Big(\mathbb{E}_{(s_1)}[X]\mathbb{E}_{(s)}[Y] - \mathbb{E}_{(s)}[XY]\Big)\\
&\quad - (1-\epsilon)\Big(\mathbb{E}_{(s_1)}[X]^2 - \mathbb{E}_{(s)}[X^2] + \mathbb{E}_{(s)}[Y]^2 - \mathbb{E}_{(s)}[Y^2]\Big), \qquad (27)
\end{aligned}$$

where in (27) we use (25) and the fact that $X = X' + X''$. By Lemma 29 there are s, s_1 such that

$$\mathbb{E}_{(s_1)}[X''] - \mathbb{E}_{(s)}[X''] \geq \Delta\|X''\|_*. \qquad (28)$$

From now on we fix s, s_1 to be the ones that achieve the above inequality. By this choice we obtain a lower bound on the first term of (27):

$$\begin{aligned}
g(X,Y,Z) &\geq \kappa\Delta\|X''\|_* + 2\Big(\mathbb{E}_{(s_1)}[X]\mathbb{E}_{(s)}[Y] - \mathbb{E}_{(s)}[XY]\Big)\\
&\qquad - (1-\epsilon)\Big(\mathbb{E}_{(s_1)}[X]^2 - \mathbb{E}_{(s)}[X^2] + \mathbb{E}_{(s)}[Y]^2 - \mathbb{E}_{(s)}[Y^2]\Big).
\end{aligned}$$

To bound the second term of (27), we use $X = X' + X''$ and $Y = Y' + Y''$ to write

$$\begin{aligned}
\mathbb{E}_{(s_1)}[X]\mathbb{E}_{(s)}[Y] &= \mathbb{E}_{(s_1)}[X']\mathbb{E}_{(s)}[Y'] + \mathbb{E}_{(s_1)}[X']\mathbb{E}_{(s)}[Y'']\\
&\quad + \mathbb{E}_{(s_1)}[X'']\mathbb{E}_{(s)}[Y'] + \mathbb{E}_{(s_1)}[X'']\mathbb{E}_{(s)}[Y'']\\
&\geq \mathbb{E}_{(s_1)}[X']\mathbb{E}_{(s)}[Y'] - x'_{\max}y''_{\max} - x''_{\max}y'_{\max} - x''_{\max}y''_{\max}, \qquad (29)
\end{aligned}$$

where $x'_{\max} = \max_a |X'(a)|$, and $x''_{\max}, y'_{\max}$ and $y''_{\max}$ are defined similarly. Now note that $\|X\|_*^2 = \|X'\|_*^2 + \|X''\|_*^2$. Moreover, $\|X\|_*^2 \leq 1$ since $X(a) \in [0,1]$ for all a. Therefore, $\|X'\|_*^2 \leq 1$ and $\|X''\|_*^2 \leq 1$. Using the fact that

$$\|X'\|_* = \sqrt{\sum_a \frac{1}{|\mathcal{A}|}X'(a)^2} \geq \frac{1}{\sqrt{|\mathcal{A}|}}x'_{\max}$$

and similarly for other terms, we can conclude that $x'_{\max}, x''_{\max} \leq \sqrt{|\mathcal{A}|}$, $y'_{\max}, y''_{\max} \leq \sqrt{|\mathcal{B}|}$, and

$$\max\left\{\frac{1}{\sqrt{|\mathcal{A}|}}x''_{\max}, \frac{1}{\sqrt{|\mathcal{B}|}}y''_{\max}\right\} \leq \max\{\|X''\|_*, \|Y''\|_*\} = \|X''\|_*,$$

where here we use (26).

We can then use these inequalities in (29) to obtain

$$\mathbb{E}_{(s_1)}[X]\mathbb{E}_{(s)}[Y] \geq \mathbb{E}_{(s_1)}[X']\mathbb{E}_{(s)}[Y'] - 3\sqrt{|\mathcal{A}||\mathcal{B}|} \cdot \|X''\|_*. \tag{30}$$

By the same analysis on $\mathbb{E}_{(s)}[XY]$ we get

$$\begin{aligned}\mathbb{E}_{(s)}[XY] &\leq \mathbb{E}_{(s)}[X'Y'] + x'_{\max}y''_{\max} + x''_{\max}y'_{\max} + x''_{\max}y''_{\max} \\ &\leq \mathbb{E}_{(s)}[X'Y'] + 3\sqrt{|\mathcal{A}||\mathcal{B}|} \cdot \|X''\|_*.\end{aligned}$$

As a result,

$$\mathbb{E}_{(s_1)}[X]\mathbb{E}_{(s)}[Y] - \mathbb{E}_{(s)}[XY] \geq \mathbb{E}_{(s_1)}[X']\mathbb{E}_{(s)}[Y'] - \mathbb{E}_{(s)}[X'Y'] - 6\sqrt{|\mathcal{A}||\mathcal{B}|} \cdot \|X''\|_*.$$

Applying the same lines of inequalities for the other terms we obtain

$$\mathbb{E}_{(s_1)}[X]^2 - \mathbb{E}_{(s)}[X^2] \leq \mathbb{E}_{(s_1)}[X']^2 - \mathbb{E}_{(s)}[X'^2] + 6|\mathcal{A}| \cdot \|X''\|_* \tag{31}$$

and

$$\mathbb{E}_{(s)}[Y]^2 - \mathbb{E}_{(s)}[Y^2] \leq \mathbb{E}_{(s)}[Y']^2 - \mathbb{E}_{(s)}[Y'^2] + 6|\mathcal{B}| \cdot \|X''\|_*. \tag{32}$$

Putting (28), (30), (31), and (32) together we obtain

$$\begin{aligned}&g(X,Y,Z) \\ &\quad\geq \kappa\Delta\|X''\|_* + 2\Big(\mathbb{E}_{(s_1)}[X']\mathbb{E}_{(s)}[Y'] - \mathbb{E}_{(s)}[X'Y'] - 6|\mathcal{A}||\mathcal{B}| \cdot \|X''\|_*\Big) \\ &\qquad - (1-\epsilon)\Big(\big(\mathbb{E}_{(s_1)}[X']^2 - \mathbb{E}_{(s)}[X'^2]\big) + \big(\mathbb{E}_{(s)}[Y']^2 - \mathbb{E}_{(s)}[Y'^2]\big) + 12|\mathcal{A}||\mathcal{B}| \cdot \|X''\|_*\Big) \\ &\quad\geq (\kappa\Delta - 24|\mathcal{A}||\mathcal{B}|)\|X''\|_* + 2\Big(\mathbb{E}_{(s_1)}[X']\mathbb{E}_{(s)}[Y'] - \mathbb{E}_{(s)}[X'Y']\Big) \\ &\qquad - (1-\epsilon)\Big(\mathbb{E}_{(s_1)}[X']^2 - \mathbb{E}_{(s)}[X'^2] + \mathbb{E}_{(s)}[Y']^2 - \mathbb{E}_{(s)}[Y'^2]\Big) \\ &\quad\geq 2\Big(\mathbb{E}_{(s)}[X']\mathbb{E}_{(s)}[Y'] - \mathbb{E}_{(s)}[X'Y']\Big) \\ &\qquad - (1-\epsilon)\Big(\mathbb{E}_{(s)}[X']^2 - \mathbb{E}_{(s)}[X'^2] + \mathbb{E}_{(s)}[Y']^2 - \mathbb{E}_{(s)}[Y'^2]\Big),\end{aligned}$$

where in the last line we use (25) and the fact that $\kappa\Delta - 24|\mathcal{A}||\mathcal{B}| \geq 0$.

Let

$$\begin{aligned}h(X',Y') &= 2\Big(\mathbb{E}_{(s)}[X']\mathbb{E}_{(s)}[Y'] - \mathbb{E}_{(s)}[X'Y']\Big) \\ &\qquad - (1-\epsilon)\Big(\mathbb{E}_{(s)}[X']^2 - \mathbb{E}_{(s)}[X'^2] + \mathbb{E}_{(s)}[Y']^2 - \mathbb{E}_{(s)}[Y'^2]\Big), \qquad \text{(33a)} \\ &= 2\Big(\mathrm{Cov}_{(s)}(X',Y')\Big) + (1-\epsilon)\Big(\mathrm{Var}_{(s)}[X'] + \mathrm{Var}_{(s)}[Y']\Big). \qquad \text{(33b)}\end{aligned}$$

Then it suffices to show that $h(X',Y') \geq 0$ for every $X' \in \mathcal{L}_A$ and $Y' \in \mathcal{L}_B$. Since (33b) is in terms of variance and covariance, for every $r,t \in \mathbb{R}$ we have that

$$h(X' + r\mathbf{1}_\mathcal{A}, Y' + t\mathbf{1}_\mathcal{B}) = h(X',Y').$$

This means that with no loss of generality we may assume that $X' \in \mathcal{L}'_A = \mathcal{L}_A \cap (\mathbf{1}_\mathcal{A})^\perp$ and $Y' \in \mathcal{L}'_B = \mathcal{L}_B \cap (\mathbf{1}_\mathcal{A})^\perp$.

Let $U \in \mathcal{K}_A$ and $U' \in \mathcal{K}_A^{\perp_s}$ such that $X' = U + U'$. Similarly let $Y' = V + V'$, where $V \in \mathcal{K}_B$ and $V' \in \mathcal{K}_B^{\perp_s}$. Since $U \in \mathcal{K}_A$, its values can be denoted by u_c. We similarly denote the values of V by v_c. Therefore, we have

$$\mathbb{E}_{(cs)}[U'] = \mathbb{E}_{(cs)}[V'] = 0 \qquad \forall c. \tag{34}$$

Thus by the characterization of $\rho = \rho(A;B|CS)$ given in Lemma 28 we have

$$\mathbb{E}_{(s)}[U'V'] \le \rho\sqrt{\mathbb{E}_{(s)}[U'^2]\mathbb{E}_{(s)}[V'^2]} \le \frac{\rho}{2}\Big(\mathbb{E}_{(s)}[U'^2] + \mathbb{E}_{(s)}[V'^2]\Big). \tag{35}$$

Further (34) implies that $\mathbb{E}_{(s)}[U'] = \mathbb{E}_{(s)}[V'] = 0$ and then

$$\mathbb{E}_{(s)}[X'] = \mathbb{E}_{(s)}[U], \qquad \mathbb{E}_{(s)}[Y'] = \mathbb{E}_{(s)}[V]. \tag{36}$$

Moreover using (34) we find that

$$\begin{aligned}\mathbb{E}_{(s)}[X'Y'] &= \mathbb{E}_{(s)}[UV] + \mathbb{E}_{(s)}[UV'] + \mathbb{E}_{(s)}[U'V] + \mathbb{E}_{(s)}[U'V'] \\ &= \mathbb{E}_{(s)}[UV] + \sum_c p_s(c)u_c\mathbb{E}_{(cs)}[V'] + \sum_c p_s(c)v_c\mathbb{E}_{(cs)}[U'] + \mathbb{E}_{(s)}[U'V'] \\ &= \mathbb{E}_{(s)}[UV] + \mathbb{E}_{(s)}[U'V']. \qquad (37)\end{aligned}$$

A similar argument shows that

$$\mathbb{E}_{(s)}[X'^2] = \mathbb{E}_{(s)}[U^2] + \mathbb{E}_{(s)}[U'^2], \tag{38}$$

$$\mathbb{E}_{(s)}[Y'^2] = \mathbb{E}_{(s)}[V^2] + \mathbb{E}_{(s)}[V'^2]. \tag{39}$$

Using (36)–(39), we compute a lower bound for $h(X',Y')$:

$$\begin{aligned}&h(X',Y') \\ &\quad\ge 2\Big(\mathbb{E}_{(s)}[U]\mathbb{E}_{(s)}[V] - \mathbb{E}_{(s)}[UV] - \mathbb{E}_{(s)}[U'V']\Big) \\ &\qquad - (1-\epsilon)\Big(\mathbb{E}_{(s)}[U]^2 - \mathbb{E}_{(s)}[U^2] - \mathbb{E}_{(s)}[U'^2] + \mathbb{E}_{(s)}[V]^2 - \mathbb{E}_{(s)}[V^2] - \mathbb{E}_{(s)}[V'^2]\Big).\end{aligned}$$

Using (35) we continue

$$\begin{aligned}
&h(X',Y')\\
&\quad\geq \Big(2\mathbb{E}_{(s)}[U]\mathbb{E}_{(s)}[V]-2\mathbb{E}_{(s)}[UV]+\mathbb{E}_{(s)}[U^2]-\mathbb{E}_{(s)}[U]^2+\mathbb{E}_{(s)}[V^2]-\mathbb{E}_{(s)}[V]^2\Big)\\
&\qquad+\epsilon\Big(\mathbb{E}_{(s)}[U]^2-\mathbb{E}_{(s)}[U^2]+\mathbb{E}_{(s)}[V]^2-\mathbb{E}_{(s)}[V^2]\Big)-2\mathbb{E}_{(s)}[U'V']\\
&\qquad+(1-\epsilon)\Big(\mathbb{E}_{(s)}[U'^2]+\mathbb{E}_{(s)}[V'^2]\Big)\\
&\quad\geq \Big(2\mathbb{E}_{(s)}[U]\mathbb{E}_{(s)}[V]-2\mathbb{E}_{(s)}[UV]+\mathbb{E}_{(s)}[U^2]-\mathbb{E}_{(s)}[U]^2+\mathbb{E}_{(s)}[V^2]-\mathbb{E}_{(s)}[V]^2\Big)\\
&\qquad+\epsilon\Big(\mathbb{E}_{(s)}[U]^2-\mathbb{E}_{(s)}[U^2]+\mathbb{E}_{(s)}[V]^2-\mathbb{E}_{(s)}[V^2]\Big)\\
&\qquad+(1-\epsilon-\rho)\Big(\mathbb{E}_{(s)}[U'^2]+\mathbb{E}_{(s)}[V'^2]\Big)\\
&\quad=\mathbb{E}_{(s)}\Big[\big((U-\mathbb{E}_{(s)}[U])-(V-\mathbb{E}_{(s)}[V])\big)^2\Big]\\
&\qquad+\epsilon\Big(\mathbb{E}_{(s)}[U]^2-\mathbb{E}_{(s)}[U^2]+\mathbb{E}_{(s)}[V]^2-\mathbb{E}_{(s)}[V^2]\Big)\\
&\qquad+(1-\epsilon-\rho)\Big(\mathbb{E}_{(s)}[U'^2]+\mathbb{E}_{(s)}[V'^2]\Big)\\
&\quad\geq\epsilon\Big(\mathbb{E}_{(s)}[U]^2-\mathbb{E}_{(s)}[U^2]+\mathbb{E}_{(s)}[V]^2-\mathbb{E}_{(s)}[V^2]\Big)\\
&\qquad+(1-\epsilon-\rho)\Big(\mathbb{E}_{(s)}[U'^2]+\mathbb{E}_{(s)}[V'^2]\Big)\\
&\quad\geq-\epsilon\Big(\mathbb{E}_{(s)}[U^2]+\mathbb{E}_{(s)}[V^2]\Big)+(1-\epsilon-\rho)\Big(\mathbb{E}_{(s)}[U'^2]+\mathbb{E}_{(s)}[V'^2]\Big)\\
&\quad=-\epsilon\big(\|U\|_{(s)}^2+\|V\|_{(s)}^2\big)+(1-\epsilon-\rho)\big(\|U'\|_{(s)}^2+\|V'\|_{(s)}^2\big).
\end{aligned}$$

Now using Lemma 30 we have

$$\|U'\|_{(s)}\geq\Delta'\|U\|_{(s)},\qquad\qquad \|V'\|_{(s)}\geq\Delta'\|V\|_{(s)}.$$

Hence,

$$\begin{aligned}
h(X',Y')&\geq-\epsilon\big(\|U\|_{(s)}^2+\|V\|_{(s)}^2\big)+(1-\epsilon-\rho)\Delta'\big(\|U\|_{(s)}^2+\|V\|_{(s)}^2\big)\\
&=\big(\Delta'(1-\rho)-(1+\Delta')\epsilon\big)\big(\|U'\|_s^2+\|V'\|_{(s)}^2\big)\\
&\geq 0.
\end{aligned}$$

These inequalities hold since $\epsilon\leq\Delta'(1-\rho)/(1+\Delta')$.

5. Future work.

In this paper we completely characterized the randomness extraction problem for nondegenerate cases. A future study could be to solve this problem for the degenerate cases. In the degenerate cases, for generalized nondistributed sources, Corollary 11 gives a mildly stronger necessary condition than Theorem 9, but there is still a gap between this necessary condition and the sufficient condition of Theorem 4.

We note that our randomness extractor in Theorem 4 extracts a bit whose bias is inversely polynomially small in the length of the source sequence. It is interesting to see if this extractor could be improved to yield a bit with an exponentially small bias. Furthermore, if we want to produce more than one bit of randomness, the trade-off between the number of produced random bits and their quality is open.

Another interesting problem is to look at efficient adversaries, similar to the work of [1]. Our proofs only show existence of inefficient adversaries.

Another way to restrict the adversary is to put limitations on the number of times the adversary can choose a strategy $s \in \mathcal{S}$, i.e., there can be a cost associated with each strategy s.

A different type of limitation can be on the adversary's knowledge about the sequence generated so far. More specifically, the adversary might have *noisy or partial* access to the previous outcomes in the sequence (these sources are called "active sources" [17]). These sources model adversaries with limited memory. Space bounded sources have been studied in [15, 23].

Finally, the problem of common randomness extraction can be studied for three or more parties instead of just two parties.

Appendix A. Exact bias of deterministic extractors for the SV source. SV sources were originally defined in the binary case [21]. Such a source is specified by two distributions, i.e., $\mathcal{S} = \{0, 1\}$ over $\mathcal{C} = \{0, 1\}$ with

$$p_0(0) = \delta \qquad \text{and} \qquad p_1(0) = 1 - \delta,$$

where $0 < \delta < 1/2$. It is proved in [21] and can also be concluded from Theorem 9 that randomness extraction from this SV source is impossible. Our goal in this appendix is to exactly characterize the set $\cup_n \Phi_n$ for this source, where Φ_n is defined in the proof of Theorem 9.

Let us describe our problem here more precisely.

Definition 31. *Fix an algorithm for extracting randomness from the binary SV source with parameter δ. Let α be the minimum of the probability of the extracted bit being 0, where the minimum is taken over all adversary's strategies. Similarly let β be the maximum of this probability over all strategies of the adversary. We call (α, β) the pair associated with the extractor. Define H_δ as the set of all such pairs (α, β) over all possible extractors.*

Our goal is to determine the set H_δ.

To state the result we need some notation.

Definition 32. *Fix $0 < \delta < 1$. For $x_1, x_2, \ldots, x_n \in \{0, 1\}$, define*

$$(0.x_1x_2\ldots x_n)_\delta = \sum_{i=1}^{n} x_i(1-\delta)^i \left(\frac{\delta}{1-\delta}\right)^{s_x(i)},$$

where

$$s_x(i) = \sum_{j=1}^{i-1} x_j.$$

Observe that when $\delta = 1/2$, we get the standard binary expansion.

Definition 33. *For two pairs (α_1, β_1) and (α_2, β_2) of real numbers we say that (α_1, β_1)* dominates *(α_2, β_2) if $\alpha_1 \le \alpha_2$ and $\beta_1 \ge \beta_2$.*

The set H_δ can be characterized using the following proposition that implicitly appears in the conference version of [21] (at the beginning of their sketch of the proof of their Theorem 6).

As mentioned in the introduction, a deterministic extractor has a corresponding depth-n binary tree, with leaves marked by either 0 or 1.

PROPOSITION 34 (see [21]). *Assume that the depth-n binary tree associated with the deterministic extractor has exactly x leaves that are marked with bit 0. Let $x = (x_1 \dots x_n)_2$ be the binary expansion of x. Then the maximum probability y that the extracted bit is 0 is at least $(0.x_1 \dots x_n)_\delta$, and the equality occurs when the x leaves of value 0 form a left prefix of all leaves, i.e., they appear consecutively from the leftmost leaf towards the right (or, in other words, the extractor assigns 0 to the sequence $(y_1, \dots, y_n)$ iff $(y_1, \dots, y_n)_2 < x$).*

The following corollary is used to plot Figure 1 for the binary SV source with $\delta = 1/3$.

(Notice that $(0.x_1, \dots, x_n)_\delta = (1-\delta)(0.x_2, \dots, x_n)_\delta$ when $x_1 = 0$. Furthermore, $(0.x_1, \dots, x_n)_\delta = (1-\delta) + \delta(0.x_2, \dots, x_n)_\delta$ when $x_1 = 1$. This is the reason behind the self-similarity of Figure 1.)

COROLLARY 35. *Let*

$$F_\delta := \big\{((0.x_1 \dots x_n)_{1-\delta}, (0.x_1 \dots x_n)_\delta) : \forall n, \forall x_1, \dots x_n \in \{0,1\}\big\} \cup \big\{(1,1)\big\}.$$

Then $F_\delta \subseteq H_\delta$. Furthermore, any $(\alpha, \beta) \in H_\delta$ is dominated by a pair in F_δ.

Proof. By symmetry, the maximum probability that the extracted bit be 1 is minimized when all leaves with value 1 form a left prefix, hence, when the leaves with value 0 form a right prefix. In other words (and again by symmetry), the minimum probability that the extracted bit be 0 is maximized when all leaves with value 0 form a left prefix. Thus, both the minimum of y and maximum of x occur when all 0-leaves form a left prefix. Observe that the pair (x, y) associated with the tree having 0-leaves as a left prefix is $((0.x_1 \dots x_n)_{1-\delta}, (0.x_1 \dots x_n)_\delta)$. □

Santha and Vazirani argue that Proposition 34 follows from inequality (43), which is not proved in their paper. Lemma 36 below gives a proof for the inequality and hence the proposition.

LEMMA 36. *For $0 < \delta < 1/2$, if*

$$(0.x_1 \dots x_n)_{1/2} + (0.y_1 \dots y_n)_{1/2} = (0.z_1 \dots z_n)_{1/2} \tag{40}$$

and

$$(0.x_1 \dots x_n)_{1/2} \geq (0.y_1 \dots y_n)_{1/2}, \tag{41}$$

then

$$(0.x_1 \dots x_n)_\delta + \frac{\delta}{1-\delta}(0.y_1 \dots y_n)_\delta \geq (0.z_1 \dots z_n)_\delta. \tag{42}$$

Remark 37. This lemma in particular shows that for $0 < \delta < 1/2$, if $x = (x_1 \dots x_n)_2, y = (y_1 \dots y_n)_2, z = (z_1 \dots z_{n+1})_2, x + y = z, x \geq y$, then

$$(0.0x_1 \dots x_n)_{1/2} + (0.0y_1 \dots y_n)_{1/2} = (0.z_1 \dots z_{n+1})_{1/2}$$

and, hence,

$$(1-\delta)(0.x_1 \dots x_n)_\delta + \delta(0.y_1 \dots y_n)_\delta \geq (0.z_1 \dots z_{n+1})_\delta. \tag{43}$$

This latter equation proves the induction step in the proof of [21].

Proof of Lemma 36. First, we show that, without loss of generality, we may assume $x_i \geq y_i$ for all i. For the first i for which $x_i \neq y_i$, we have $x_i > y_i$. Consider the first i for which $x_i < y_i$. If for this i, we swap x_j with y_j for all $j \geq i$, we still have (40) but $(0.x_1 \dots x_n)_\delta + \frac{\delta}{1-\delta}(0.y_1 \dots y_n)_\delta$ decreases by

$$(1-\delta)^{i-1}\left(\left(\frac{\delta}{1-\delta}\right)^{s_x(i)} - \left(\frac{\delta}{1-\delta}\right)^{s_y(i)+1}\right)((0.x_i \dots x_n)_\delta - (0.y_i \dots y_n)_\delta)$$

which is nonnegative because $s_x(i) \geq s_y(i) + 1$ and $(0.x_i \dots x_n)_\delta \leq (0.y_i \dots y_n)_\delta$. We can successively do these swaps until $x_i \geq y_i$ for all i.

Now we prove the lemma by induction on n. Assume for the sake of contradiction that inequality (42) does not hold.

If $z_1 = 0$, then $x_1 = y_1 = z_1 = 0$. Then we can remove x_1, y_1, z_1, decrease n by 1, and prove the lemma using the induction hypothesis. Thus, assume that $z_1 = 1$. Now we can partition the indices $\{1, \dots, n\}$ into blocks such that in the addition of $(0.x_1 \dots x_n)_{1/2}$ with $(0.y_1 \dots y_n)_{1/2}$, no carry is passed from one block to the next block, but within each block there is always a passed carry. Consider the leftmost block that begins from index 1 and ends at index m.

If $m = 1$, then we should have $x_1 = 1, y_1 = 0, z_1 = 1$. If we change x_1 and z_1 to 0, then we still have (40). Also, inequality (41) holds because $x_i \geq y_i$ for $i \geq 2$. Furthermore, both $(0.x_1 \dots x_n)_\delta$ and $(0.z_1 \dots z_n)_\delta$ are decreased by $1-\delta$ and then multiplied by $\delta/(1-\delta) \leq 1$, while $(0.y_1 \dots y_n)_\delta$ does not change. Therefore, inequality (42) holds if and only if it holds after changing x_1 and z_1 to 0. Since now $z_1 = 0$, we can use the induction hypothesis.

If $m > 1$, then we should have $x_1 = 0, x_2 = x_3 = \cdots = x_m = 1, y_1 = 0, z_1 = 1, y_2 = z_2, \dots, y_{m-1} = z_{m-1}, y_m = 1, z_m = 0$. Let i be an index $\in [2, m-1]$ such that $y_i = 0$ (if such an i exists.) If we change y_i and z_i both to 1, then (40) holds. Inequality (41) also holds since $x_i \geq y_i$ for all i. Furthermore, $\frac{\delta}{1-\delta}(0.y_1 \dots y_n)_\delta - (0.z_1 \dots z_n)_\delta$ decreases by

$$\begin{aligned}
&\frac{\delta}{1-\delta}(1-\delta)^{i-1}\left(\frac{\delta}{1-\delta}\right)^{s_y(i)}\left(1-\frac{\delta}{1-\delta}\right)((0.y_i \dots y_n)_\delta) \\
&\qquad - (1-\delta)^{i-1}\left(\frac{\delta}{1-\delta}\right)^{s_z(i)}\left(1-\frac{\delta}{1-\delta}\right)((0.z_i \dots z_n)_\delta) \\
&\quad = \frac{\delta}{1-\delta}(1-\delta)^{i-1}\left(\frac{\delta}{1-\delta}\right)^{s_y(i)}\left(1-\frac{\delta}{1-\delta}\right)((0.y_i \dots y_n)_\delta - (0.z_i \dots z_n)_\delta)
\end{aligned}$$

because $s_y(i) = s_z(i) - 1$. This decrease is nonnegative because $(0.y_{i+1} \dots y_n)_\delta > (0.z_{i+1} \dots y_n)_\delta$ (since $y_m > z_m$). So, to prove the claim, without loss of generality, we can assume $x_2 = \cdots = x_m = y_2 = \cdots = y_m = z_1 = \cdots = z_{m-1} = 1$. But now if we make the values of x_i, y_i, z_i equal to 0 for all $i \in [1, m]$, we still have (40) and inequality (41), while this does not change the difference of the two sides of inequality (42). Given $z_1 = 0$, we can use the induction hypothesis as above. □

Appendix B. Another proof of Theorem 9.

Consider the set of points $\{p_s(\cdot) : s \in \mathcal{S}\}$ in the probability simplex. Then, by assumption, there is a point $q(\cdot)$ in the interior of the convex hull of these points. Fix a deterministic extractor specified by a subset $\mathcal{I} \subseteq \mathcal{C}^n$, i.e., if the observed c^n is in $\mathcal{I}$ then the extracted bit is 0, and otherwise it is 1. Consider the probability distribution $q^n(\cdot)$ on $\mathcal{C}^n$ that is the i.i.d. repetition of $q(\cdot)$. Without loss of generality, assume that $q^n(\mathcal{I}) \geq 1/2$. Let $\mathcal{I}_0 \subseteq \mathcal{I}$ be a minimal subset such that $q^n(\mathcal{I}_0) \geq 1/2$. That is, let $\mathcal{I}_0 \subseteq \mathcal{I}$ be such that $q^n(\mathcal{I}_0) \geq 1/2$ and no proper subset of $\mathcal{I}_0$ has this property. Observe that for any $c^n \in \mathcal{C}^n$ we have $q^n(c^n) \leq 2^{-\Theta(n)}$. Therefore, by the definition of $\mathcal{I}_0$ we have $q^n(\mathcal{I}_0) = 1/2 + 2^{-\Theta(n)}$.

Let $\widetilde{p}(\cdot)$ be a tweak of the distribution $q^n(\cdot)$ obtained as follows. Let $\epsilon > 0$ be a small constant, and define $\widetilde{p}(c^n) = (1+\epsilon)q^n(c^n)$ for $c^n \in \mathcal{I}_0$; also, for $c^n \notin \mathcal{I}_0$, define $\widetilde{p}(c^n) = (1-\epsilon-2^{-\Theta(n)})q^n(c^n)$ to make $\widetilde{p}(\cdot)$ a probability distribution.

We claim that $\widetilde{p}(\cdot)$ is in the class of distributions associated with the generalized SV source, i.e., the adversary can choose a strategy to generate this distribution. Assuming this claim, observe that the probability that the extracted bit is 0 would be equal to

$$\widetilde{p}(\mathcal{I}) \geq \widetilde{p}(\mathcal{I}_0) = (1+\epsilon)q^n(\mathcal{I}_0) \geq (1+\epsilon)/2.$$

Thus the adversary can force the bias of the extracted bit to be at least ϵ. This would finish the proof.

What remains to show is that $\widetilde{p}(\cdot)$ can be generated by the adversary. Observe that for any $\mathcal{J} \subseteq \mathcal{C}^n$ we have

$$\widetilde{p}(\mathcal{J}) = (1+O(\epsilon))q^n(\mathcal{J}), \tag{44}$$

where as in standard big-Oh notation, $O(\epsilon)$ is not necessarily positive, and may be positive or negative. In particular, for any $c_1, \dots, c_i$, we have

$$\widetilde{p}(C_1 = c_1, \dots, C_i = c_i) = (1+O(\epsilon)) \prod_{j=1}^{i} q(c_j).$$

Therefore,

$$\widetilde{p}(C_i = c_i | C_1 = c_1, \dots, C_{i-1}) = \frac{1+O(\epsilon)}{1+O(\epsilon)} q(c_i) = (1+O(\epsilon))q(c_i).$$

Since $q(\cdot)$ is in the interior of the convex hull of $\{p_s(\cdot) : s \in \mathcal{S}\}$, then for sufficiently small $\epsilon > 0$, any probability distribution of the form $((1+O(\epsilon))q(\cdot)$ is in this convex hull too. Thus, by definition $\widetilde{p}(\cdot)$ can be produced by the adversary.

Acknowledgments. We thank Amir Azizi JirAbadi for pointing out typos in our manuscript. We also would like to thank the anonymous referees for their useful comments.

REFERENCES

[1] P. Austrin, K.-M. Chung, M. Mahmoody, R. Pass, and K. Seth, *On the impossibility of cryptography with tamperable randomness*, in Advances in Cryptology–Crypto 2014, Springer, Heidelberg, 2014, pp. 462–479, https://doi.org/10.1007/978-3-662-44371-2_26.

[2] S. Beigi and D. Tse, *private communication.*

[3] T. Berger, *The source coding game*, IEEE Trans. Inform. Theory, 17 (1971), pp. 71–76, https://doi.org/10.1109/TIT.1971.1054577.

[4] M. Blum, *Independent unbiased coin flips from a correlated biased source: A finite state Markov chain*, Combinatorica, 6 (1986), pp. 97–108, https://doi.org/10.1007/BF02579167.

[5] J. Bourgain, *More on the sum-product phenomenon in prime fields and its applications*, Int. J. Number Theory, 1 (2005), pp. 1–32, https://doi.org/10.1142/S1793042105000108.

[6] J. Bourgain, *On the construction of affine extractors*, Geom. Funct. Anal., 17 (2007), pp. 33–57, https://doi.org/10.1007/s00039-007-0593-z.

[7] B. Chor and O. Goldreich, *Unbiased bits from sources of weak randomness and probabilistic communication complexity*, SIAM J. Comput., 17 (1988), pp. 230–261, https://doi.org/10.1137/0217015.

[8] R. Dobrushin, *Individual methods for transmission of information for discrete channels without memory and messages with independent components*, Sov. Math, 4 (1963), pp. 253–256.

[9] R. Dobrušin, *Unified methods of optimal quantizing of messages*, Sov. Math, 4 (1963), pp. 284–292.

[10] Z. Dvir, *Extractors for varieties*, Comput. Complexity, 21 (2012), pp. 515–572, https://doi.org/10.1007/s00037-011-0023-3.

[11] Z. Dvir, A. Gabizon, and A. Wigderson, *Extractors and rank extractors for polynomial sources*, Comput. Complexity, 18 (2009), pp. 1–58, https://doi.org/10.1007/s00037-009-0258-4.

[12] M. J. Fischer and N. A. Lynch, *A lower bound for the time to assure interactive consistency*, Inform. Process. Lett., 14 (1982), pp. 183–186, https://doi.org/10.1016/0020-0190(82)90033-3.

[13] A. Gabizon, *Deterministic extractors for affine sources over large fields*, in Deterministic Extraction from Weak Random Sources, Springer, Heidelberg, 2011, pp. 33–53, https://doi.org/10.1007/978-3-642-14903-0_3.

[14] P. Gács and J. Körner, *Common information is far less than mutual information*, Probl. Control Inform. Theory, 2 (1973), pp. 149–162.

[15] J. Kamp, A. Rao, S. Vadhan, and D. Zuckerman, *Deterministic extractors for small-space sources*, in Proceedings of the Thirty-Eighth Annual ACM Symposium on Theory of Computing, ACM, New York, 2006, pp. 691–700, https://doi.org/10.1145/1132516.1132613.

[16] N. Nisan and D. Zuckerman, *Randomness is linear in space*, J. Comput. System Sci., 52 (1996), pp. 43–52, https://doi.org/10.1006/jcss.1996.0004.

[17] H. Palaiyanur, C. Chang, and A. Sahai, *Lossy compression of active sources*, in 2008 IEEE International Symposium on Information Theory, IEEE, Piscataway, NJ, 2008, pp. 1977–1981, https://doi.org/10.1109/ISIT.2008.4595335.

[18] M. O. Rabin, *Randomized byzantine generals*, in 24th Annual Symposium on IEEE Foundations of Computer Science, IEEE Computer Society, Los Angeles, 1983, pp. 403–409, https://doi.org/10.1109/SFCS.1983.48.

[19] A. Rao, *Extractors for a constant number of polynomially small min-entropy independent sources*, SIAM J. Comput., 39 (2009), pp. 168–194, https://doi.org/10.1137/060671218.

[20] O. Reingold, S. Vadhan, and A. Wigderson, *A Note on Extracting Randomness from Santha-Vazirani Sources*, https://omereingold.files.wordpress.com/2014/10/svsources.pdf (2004).

[21] M. Santha and U. V. Vazirani, *Generating quasi-random sequences from semi-random sources*, J. Comput. System Sci., 33 (1986), pp. 75–87, https://doi.org/10.1016/0022-0000(86)90044-9.

[22] S. Vadhan, *Pseudorandomness*, Found. Trends Theor. Comput. Sci., 7 (2012), pp. 1–336 https://doi.org/10.1561/0400000010.

[23] U. Vazirani, *Efficiency considerations in using semi-random sources*, in Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing, ACM, New York, 1987, pp. 160–168, https://doi.org/10.1145/28395.28413.

[24] U. V. Vazirani and V. V. Vazirani, *Random polynomial time is equal to slightly-random polynomial time*, in IEEE 26th Annual Symposium on Foundations of Computer Science, IEEE Computer Society, Los Angeles, 1985, pp. 417–428, https://doi.org/10.1109/SFCS.1985.45.

[25] U. V. Vazirani and V. V. Vazirani, *Sampling a population with a semi-random source*, in International Conference on Foundations of Software Technology and Theoretical Computer Science, Springer, Berlin, 1986, pp. 443–452, https://doi.org/10.1007/3-540-17179-7_27.

[26] J. Von Neumann, *Various techniques used in connection with random digits*, in Monte Carlo Method, Appl. Math. Ser. 12, U.S. National Bureau of Standards, Washington, DC, 1951, pp. 36–38.

[27] H. S. Witsenhausen, *On sequences of pairs of dependent random variables*, SIAM J. Appl. Math., 28 (1975), pp. 100–113, https://doi.org/10.1137/0128010.

[28] S. Wolf and J. Wullschleger, *New monotones and lower bounds in unconditional two-party computation*, IEEE Trans. Inform. Theory, 54 (2008), pp. 2792–2797, https://doi.org/10.1109/TIT.2008.921674.

[29] A. C.-C. Yao, *Some complexity questions related to distributive computing (preliminary report)*, in Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing, ACM, New York, 1979, pp. 209–213, https://doi.org/10.1145/800135.804414.

[30] D. Zuckerman, *Randomness-optimal oblivious sampling*, Random Structures Algorithms, 11 (1997), pp. 345–367.