Electronic Colloquium on Computational Complexity, Report No. 350 (2026)

# Asymptotically Optimal Two Source Extractors for Arbitrary Constant Entropy Rate

Xin Li*

**Abstract**

We construct explicit two-source extractors for any constant entropy rate with asymptotically optimal parameters. Specifically, for sources on $n$ bits with min-entropy $k = \delta n$ for any constant $\delta \in (0, 1]$, and error $\varepsilon \geq 2^{-b_\delta n}$ where $b_\delta$ is a constant depending on $\delta$, our extractor outputs $2k - O(\log(1/\varepsilon) + 1)$ bits that are $\varepsilon$ close to uniform. In particular, this gives two-source extractors with $\Omega(n)$ output bits and $2^{-\Omega(n)}$ error for any constant entropy rate. Previously, explicit two source extractors with such error are only known to work for entropy rate roughly $4/9$ (Bourgain 2005, Lewko 2019). We also extend our constructions to give (strong) non-malleable two source extractors and sumset extractors for any constant entropy rate with asymptotically optimal parameters.

Our extractors can be extended to handle slightly sub-constant entropy rate, with sub-optimal error. Using a different construction and analysis, we give explicit (non-malleable) two source extractors for entropy $k \geq Cn/\log n$ for some constant $C > 1$ with $\Omega(k)$ output bits and error close to $2^{-\Omega(\sqrt{n})}$.

An independent work of Doron and Goodman constructed explicit two-source extractors for entropy $k \geq n^{1-\alpha}$ with error $2^{-k^\alpha}$ for some constant $\alpha > 0$. Their extractors work for smaller entropy than ours, while our extractors have better error and output length for any constant entropy rate. Our extractors for entropy $k \geq Cn/\log n$ are obtained independently before we were aware of their results, while our extractors for constant entropy rate with asymptotically optimal parameters are obtained after we learned their unpublished results at the Simons Institute, using different ideas and techniques.

*Department of Computer Science, Johns Hopkins University, lixints@cs.jhu.edu.

ISSN 1433-8092

# Contents

**1 Introduction** **1**
1.1 Our results . . . 3
1.2 Overview of the techniques . . . 4

**2 Preliminaries and common tools** **16**
2.1 Source-strong extraction and entropy-slack transfer . . . 17
2.2 Elementary probability, Fourier analysis, and rank . . . 18
2.3 Odd-power features and dense spans . . . 21
2.4 Approximate duality and its rank-sensitive form . . . 24
2.5 Published seeded primitives and entropy-efficient extraction . . . 25
2.6 Constant-seed strong condenser . . . 27
2.7 Uniform quantitative results for a growing number of rows . . . 27
2.8 Weighted approximate duality for arbitrary common features . . . 28
2.9 A uniform shared-feature regularization theorem . . . 29

**3 Constant-rate extraction with small error** **32**
3.1 Ordinary two-source extraction . . . 32
3.2 Sumset extraction . . . 38
3.3 Fixed-$C$ non-malleable two-source extraction . . . 55

**4 Entropy-efficient output at constant rate** **79**
4.1 Two-source output with additive entropy loss . . . 80
4.2 Source-strong non-malleable output with additive entropy loss . . . 85
4.3 Corollary: ordinary source-strong output with additive entropy loss . . . 94
4.4 Sumset output with additive entropy loss . . . 94

**5 Decreasing entropy rates** **100**
5.1 Growing-row ingredients and their proofs . . . 100
5.2 Short-output non-malleability: construction and proof . . . 109
5.3 Source-strong output with additive entropy loss . . . 112

# 1 Introduction

The theory of *randomness extraction* concerns the process of extracting almost uniform random bits from *weak random sources*, which are probability distributions with various defects and bias. Through decades of study, many different kinds of *randomness extractors*, which are explicitly constructed objects that perform randomness extraction, have been designed. These objects have since become fundamental objects in the area of pseudorandomness, with wide applications in other areas such as cryptography, complexity theory, graph theory, and so on. In this paper, we use the standard *min-entropy* to measure the amount of randomness in a weak random source. Specifically, the min-entropy of a random variable $X$ is defined as $H_\infty(X) = \min_{x \in \mathrm{supp}(X)} \log_2(1/\Pr[X = x])$. A source $X$ with support in $\{0,1\}^n$ is said to be an $(n, H_\infty(X))$-source, with entropy rate $H_\infty(X)/n$.

It is well known that a single arbitrary weak source with only a min-entropy guarantee admits no deterministic extraction in general, thus motivating models with structures.

**Definition 1.1.** Let $\mathcal{X}$ be a family of distributions over $\{0,1\}^n$. A function $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}^m$ is a deterministic extractor for $\mathcal{X}$ with error $\varepsilon$ if for every distribution $X \in \mathcal{X}$, we have

$$\Delta(\mathrm{Ext}(X), U_m) \leqslant \varepsilon,$$

where $U_m$ stands for the uniform distribution over $\{0,1\}^m$, and $\Delta()$ denotes the statistical distance. Sometimes we also write $\mathrm{Ext}(X) \approx_\varepsilon U_m$. We say Ext is explicit if it is computable by a polynomial-time algorithm.

Again, many such models have been studied. Some of the most well studied ones include for example two source extractors, where the input to the extractor consists of two independent $(n,k)$ sources $X, Y$; affine extractors, where the input source is the uniform distribution over some unknown affine subspace; sumset extractors, where the input is $X + Y$ for two independent $(n,k)$ sources $X, Y$ (here $+$ is bitwise addition over $\mathbb{F}_2$); and non-malleable two source extractors, where the extractor has an additional security guarantee against tamperings on the input sources. In this paper we study two source extractors, sumset extractors, and non-malleable two source extractors. We briefly survey the history of these extractors below.

**Two-source extractors.** Chor and Goldreich [20] initiated the formal study of weak random sources and explicit two-source extractors. Their construction gives an explicit two source extractor for entropy rate above $1/2$ with exponentially small error, while the probabilistic method shows the existence of two source extractors with error $\varepsilon$, output length $m = 2k - 2\log(1/\varepsilon) - O(1)$ when the entropy $k$ of each source is slightly larger than $\log n + 2\log(1/\varepsilon) + O(1)$. In particular, this implies the existence of two source extractors with output length $\Omega(k)$ and error $2^{-\Omega(k)}$ when $k \geq c \log n$ for some constant $c > 1$. Dodis, Elbaz, Oliveira, and Raz [28] improved the output length of the extractor in [20], but the entropy rate remains above $1/2$. Raz [56] constructed an explicit two source extractor where one source is required to have entropy rate above $1/2$, while the other one can have logarithmic entropy. Breaking the entropy rate $1/2$ barrier has since been a major open problem in the study of two source extractors.

A 2005 work by Bourgain [11] first breaks the entropy rate $1/2$ barrier, by using sum-product phenomena and estimates for exponential sums. However Bourgain's extractor only works for entropy rate slightly below one half. Subsequently, Lewko [39] revisited this approach and improved the min-entropy rate to be arbitrarily close to $4/9$. Both of these extractors have error $2^{-\Omega(n)}$.

On the other hand, a long line of works [4, 5, 56, 11, 54, 6, 40, 42, 44, 43, 45, 22, 24, 17, 46, 27, 14, 23, 7, 25, 26, 47, 48, 49] studied the more general model of several independent sources,

and gradually reduced the number of sources. These works finally led to the breakthrough of Chattopadhyay and Zuckerman [17], which obtained an explicit one-bit two-source extractor for entropy $k \geqslant \log^C n$ for some constant $C > 1$ with polynomially small error. Later works refined the constructions and culminated in Li's 2023 work [49], which constructed explicit two source extractors for asymptotically optimal entropy of $O(\log n)$, with one bit of output and constant error. These extractors also give currently the best known explicit constructions of *Ramsey graphs*.

However, the two source extractors constructed recently following the framework of [17] only have polynomially small error at the best, which is insufficient for cryptographic tasks, where one naturally requires negligible error. Given that one of the main applications of randomness extractors is in cryptography, the quest for small error two source extractors remains an important open problem, where the previously best known construction due to Lewko [39] still requires entropy rate roughly 4/9.

**Sumset Extractors.** Chattopadhyay and Li [15] introduced and initiated the study of extractors for sumset sources, which unifies several previously studied models such as independent sources, affine sources, and small space sources. Here, unlike the case of two source extractors, a simple application of the probabilistic method fails to show the existence of such extractors for small entropy (e.g., $O(\log n)$). Nevertheless, [15] constructed explicit extractors for the sum of a constant number of independent sources with poly-logarithmic entropy, and achieved a polynomially small error. Chattopadhyay and Liao [16] later improved this to work for the *sum of two* independent sources, with entropy $k = \text{polylog}(n)$ and polynomially small error, or entropy $k = \log n(\log\log n)^{1+o(1)}$ with constant error. Li [49] subsequently obtained sumset extractors for the sum of two independent sources with asymptotically optimal entropy of $O(\log n)$ and constant error.

However, if one requires negligible error, then since sumset extractors are stronger than two source extractors, the entropy requirement of the former is at least that of the latter. One known construction is the Paley graph extractor in [20], although the sum there is over a field with odd characteristic. The extractor requires one source to have entropy rate above 1/2 while the other can have entropy $k$ as small as $O(\log n)$, and the extractor has error $2^{-\Omega(k)}$. Thus for $k = \omega(\log n)$ the error is negligible. The analysis is based on character sum estimates of Karatsuba [37, 38].

**Non malleable extractors.** Many of the standard models of randomness extractors can also be extended to a stronger version, known as *non-malleable extractors*. This notion arises from cryptographic applications, such as privacy amplification with an active adversary [30] and non-malleable codes [34]. Due to their cryptographic applications and recent surprising connections to constructing standard extractors [42, 17], such extractors have also been the focus of much study in the past 15 years or so. In this setting, the input to the extractor is tampered with by a certain kind of adversary, and the non-malleable extractor guarantees that the output of the extractor on the original inputs is still close to uniform even conditioned on the tampered output. We begin the discussion of non-malleable extractors by defining tampering functions.

**Definition 1.2** (Tampering Function)**.** For any function $f : S \to S$, we say $f$ has no fixed points if $f(s) \neq s$ for all $s \in S$. For any $n > 0$, let $\mathcal{F}_n$ denote the set of all functions $f : \{0,1\}^n \to \{0,1\}^n$. Any subset of $\mathcal{F}_n$ is a family of tampering functions.

As in recent literature, for non-malleable extractors we only consider tampering functions with no fixed points, since if the tampering is the identity function then non-malleability is impossible. A more general definition can be found for example in [18]. We can now extend two source extractors to their corresponding non-malleable version.

**Definition 1.3.** A function $\mathsf{nmExt} : (\{0,1\}^n)^2 \to \{0,1\}^m$ is a $(k,\varepsilon)$ $C$-non-malleable two source extractor, if it satisfies the following property: Let $X, Y$ be two independent $(n,k)$ sources, and $\{(f_i, g_i)\}_{i\in[C]}$ be $C$ arbitrary pairs of tampering functions such that for each $i \in [C]$, at least one of $f_i, g_i$ has no fixed points, then

$$(\mathsf{nmExt}(X,Y), (\mathsf{nmExt}(f_i(X), g_i(Y)))_{i=1}^C) \approx_\varepsilon (U_m, (\mathsf{nmExt}(f_i(X), g_i(Y)))_{i=1}^C),$$

where $U_m$ is independent of $(\mathsf{nmExt}(f_i(X), g_i(Y)))_{i=1}^C$. We say the non-malleable two source extractor is (source) strong if the above property holds with the additional conditioning of the source $X$ or $Y$.

*Remark* 1.4. In the special case of $C = 0$, this gives a standard two source extractor, and the strong version gives a *strong two source extractor*.

The probabilistic method can be used to prove the existence of such non-malleable extractors with excellent parameters. For example, [18] showed that for $C = 1$, such extractors exist for $(n,k)$ sources when $k \geq m + \frac{3}{2}\log(1/\varepsilon) + O(1)$ and $k \geq \log n + 3\log(1/\varepsilon) + O(1)$. If the error is small, then for non-malleable two source extractors against $C$ tampering functions, a necessary information theoretic bound is that $k \geq (C+1)m/2$. For the strong version, we need $k \geq (C+1)m$.

Not surprisingly, constructing explicit non-malleable extractors is significantly harder than constructing standard extractors, due to their much stronger properties. Historically, Chattopadhyay, Goyal, and Li [13] gave the first explicit non-malleable two-source extractors for sources of entropy $n - n^{\Omega(1)}$, with polynomial-size output and exponentially small error. They also developed many-tampering versions in the same very-high-entropy regime. Subsequent works [14, 47, 48, 21, 49] improved the constructions in various ways, leading to an explicit construction of Li [49], which gave non-malleable two-source extractors requiring entropy $(2/3+\gamma)n$ in one source and $k \geqslant C\log n$ in the other for some constant $C > 1$, with output length $\Omega(k)$ and error $2^{-\Omega(k)}$. In the regime of small entropy, Li and Zhong [51] also obtained non-malleable two source extractors that match their standard counterparts: extractors for polylogarithmic entropy with polynomially small error, and for $O(\log n)$ entropy with constant error.

In summary, the question of constructing small error (e.g., negligible error) (non-malleable) two source related extractors remains an important open question. For two source extractors and sumset extractors, the bottleneck is slightly below entropy rate $1/2$ at the best; for non-malleable two source extractors, the bottleneck is at entropy rate $2/3$.

## 1.1 Our results

In this paper we significantly improve previous results in terms of small error (non-malleable) two source and sumset extractors. We first state our main results of two source extractors.

**Theorem 1.5.** There are absolute constants $C_0, C_1 > 0$ such that, for every constant $0 < \delta \leqslant 1$, there are constants $b_\delta > 0$ and $n_\delta$ with the following property. For all $n \geqslant n_\delta$, integer $\delta n \leqslant k \leqslant n$, and $2^{-b_\delta n} \leqslant \varepsilon \leqslant \frac{1}{4}$, there is an explicit two source extractor $\mathrm{TExt} : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}^m$ such that, for any two independent $(n,k)$ sources $X, Y$,

$$\Delta(\mathrm{TExt}(X,Y), U_m) \leqslant \varepsilon, \qquad m \geqslant 2k - C_0\log(1/\varepsilon) - C_1.$$

Thus our extractor achieves asymptotically optimal parameters for any constant entropy rate. In particular, this implies a two source extractor for any constant entropy rate with output length $\Omega(n)$ and error $2^{-\Omega(n)}$.

We can extend our results to sumset extractors and non-malleable two source extractors. Specifically, we have the following theorems.

**Theorem 1.6.** For every constant $0 < \delta \leqslant 1$ there are constants $b_\delta > 0$ and $n_\delta$ such that the following holds. For all $n \geqslant n_\delta$, integer $\delta n \leqslant k \leqslant n$, and $2^{-b_\delta n} \leqslant \varepsilon \leqslant \frac{1}{4}$, there is an explicit sumset extractor $\mathrm{SumExt} : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m$ such that, for any two independent $(n,k)$ sources $X, Y$,

$$\Delta(\mathrm{SumExt}(X+Y), U_m) \leqslant \varepsilon, \qquad m \geqslant k - 2\log(1/\varepsilon) - 10.$$

**Theorem 1.7.** For every constant $0 < \delta \leqslant 1$ and integer $C \geqslant 0$ there is a constant $b_{\delta,C} > 0$ such that, for sufficiently large $n$, integer $\delta n \leqslant k \leqslant n$, and $2^{-b_{\delta,C} n} \leqslant \varepsilon \leqslant 1/4$, there is an explicit non malleable two source extractor $\mathsf{nmExt} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$ with

$$m \geqslant \frac{k}{C+1} - O(\log(1/\varepsilon) + 1)$$

such that, for any two independent $(n,k)$ sources $X, Y$, and any $C$ pairs of tampering functions $\{(f_i, g_i)\}_{i \in [C]}$ such that for each $i \in [C]$, at least one of $f_i, g_i$ has no fixed points,

$$(\mathsf{nmExt}(X,Y), (\mathsf{nmExt}(f_i(X), g_i(Y)))_{i=1}^C, Y) \approx_\varepsilon (U_m, (\mathsf{nmExt}(f_i(X), g_i(Y)))_{i=1}^C, Y), \tag{1.1}$$

$$(\mathsf{nmExt}(X,Y), (\mathsf{nmExt}(f_i(X), g_i(Y)))_{i=1}^C, X) \approx_\varepsilon (U_m, (\mathsf{nmExt}(f_i(X), g_i(Y)))_{i=1}^C, X). \tag{1.2}$$

*Remark* 1.8. Note that in the above theorem, the special case of $C = 0$ also gives a standard strong two source extractor with output length $m \geqslant k - O(\log(1/\varepsilon) + 1)$.

We can extend our results to slightly sub constant entropy rate. Specifically, we have the following theorem.

**Theorem 1.9** (Entropy rate $C/\log n$)**.** Fix an integer $t \geqslant 0$ and $0 < \vartheta < 1/2$. There are constants $C_{t,\vartheta} > 0$ and $n_0$ such that, for every $n \geqslant n_0$, integer $C_{t,\vartheta} n/\log n \leqslant k \leqslant n$, and $2^{-n^{1/2-\vartheta}} \leqslant \varepsilon \leqslant 1/4$, there is an explicit strong $t$-non-malleable two-source extractor $\mathsf{nmExt} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$ with

$$m \geqslant \frac{k}{t+1} - O\big(\log(1/\varepsilon) + 1\big).$$

## 1.2 Overview of the techniques

Here we give an informal overview of the techniques used in our constructions. Throughout, we will focus more on the constructions of standard two source extractors to illustrate our main ideas. We start by describing the ideas behind our two source extractor for any constant entropy rate with $\Omega(n)$ output length and $2^{-\Omega(n)}$ error. Without loss of generality, we consider flat sources, which are the uniform distributions over some unknown subsets.

Our starting point is the work of Ben-Sasson and Ron-Zewi [9], which shows how to construct two source extractors from a sufficiently good affine extractor. We will not be following this specific approach here, but we will use one of their important observations: let $E : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$ be a function and view it as a $2^n \times 2^n$ matrix $M_E$ over $\mathbb{F}_2$ in the natural way, where the $(x,y)$ entry corresponds to $E(x,y)$. Let $r$ be the rank of $M_E$ over $\mathbb{F}_2$, then there also exist functions $h_X, h_Y : \mathbb{F}_2^n \to \mathbb{F}_2^r$ such that $E(x,y) = \langle h_X(x), h_Y(y) \rangle$ where $\langle , \rangle$ denotes the inner product over $\mathbb{F}_2$. Furthermore, if $E$ is a two source disperser for entropy rate $\rho$ with rank $O(n)$, then for any constant $\gamma > 0$, $E$ is also a two source extractor for entropy rate $\rho + \gamma$ with error $2^{-\Omega(n)}$. Here, a two source disperser is a weaker object than a two source extractor, in the sense that it only requires the output to be non-constant (in the case of one bit output). The proof uses *approximate duality*: if instead the function is not a two source extractor with the above parameters, then one can find a relatively large subrectangle

in the matrix $M_E$ where the entries are all the same, which contradicts the disperser property. Therefore, our goal is reduced to constructing a two source disperser for any constant entropy rate, with rank $O(n)$. Once we have it, we can use approximate duality to lift it to an extractor with error $2^{-\Omega(n)}$. To get output length $\Omega(n)$, we show that we can actually produce $\Omega(n)$ output bits such that the parity of any non-trivial subset of these bits is still $2^{-\Omega(n)}$ close to uniform. Hence by a standard XOR lemma, these $\Omega(n)$ bits are themselves $2^{-\Omega(n)}$ close to uniform.

We now explain the ingredients we use to get such a two source extractor. Towards that goal, we first use standard techniques to get a *somewhere high entropy source* from each input weak source. In particular, we use the seeded condenser in [56] which has constant seed length, and can condense any weak source with entropy rate $\delta/2$ to $1-\beta$ with error $\varepsilon$ and output length $\Omega(n)$. Here $\delta, \beta, \varepsilon$ are arbitrary fixed constants, and the seed length $d$ is a constant depending on these. By enumerating all possible seeds, we get a somewhere high entropy source with a constant $r = 2^d$ number of rows, such that when averaged over the constant seed space, each row is close to some distribution of entropy rate at least $1-\beta$. This is in contrast to some of the condensers in e.g., [6, 58], which only guarantee that at least one row is close to having high entropy, but with exponentially small error. The error $\varepsilon$ here is larger, but for our purpose of getting a disperser first, this is already enough. For input sources $X, Y$, let the two somewhere high entropy sources be $\widetilde{X}, \widetilde{Y}$. In our analysis, we then show that there exist two *subsources* $X^*, Y^*$ such that when restricted to $X^*, Y^*$, each somewhere high entropy source $\widetilde{X^*}, \widetilde{Y^*}$ has at least $\frac{3r}{4}+1$ rows which have entropy rate at least $1-\tau/2$ for some small constant $\tau > 0$. Hence, let $D = \frac{r}{2}$, there are at least $D+1$ rows that simultaneously have entropy rate at least $1-\tau/2$ in both $\widetilde{X^*}$ and $\widetilde{Y^*}$. We now delete an arbitrary row from $\widetilde{X^*}$ and $\widetilde{Y^*}$, and we end up with $r-1$ rows such that at least $D$ rows simultaneously have entropy rate at least $1-\tau/2$ in both $\widetilde{X^*}$ and $\widetilde{Y^*}$. These are the good rows we will use in the analysis, and from now on we'll treat the input sources as $X = X^*, Y = Y^*$.

At this point, our construction goes by applying a specific two source extractor TExt for high entropy sources to each row $a$ in $\widetilde{X}, \widetilde{Y}$, i.e., compute $\mathrm{TExt}(\widetilde{X}_a, \widetilde{Y}_a)$. Then we use a merger to merge these $r-1$ outputs together. However, in order to carry out our previous plan, we need to construct the two source extractor TExt and the merger carefully. At first, it seems tempting to just use inner product as TExt. This indeed has rank $O(n)$, but then it is unclear how to merge the outputs together later. To address this, we use a slightly modified two source extractor. Specifically, let $M$ be the length of each row in $\widetilde{X}$ and $\widetilde{Y}$. Let $K = \mathbb{F}_{2^M}$ and identify each row as an element in $K$. For the $a$'th row, denote $U_a(X) = \widetilde{X}_a$ and $V_a(Y) = \widetilde{Y}_a$. Next we choose an appropriate $\ell = \Theta(n) < M$ such that $M = L\ell$, and let $F = \mathbb{F}_{2^\ell}$. Finally, choose an integer $J \geqslant 1$ and compute the following function:

$$H_J(U_a(X), V_a(Y)) = \sum_{j=1}^{J} U_a(X)^{2j-1} V_a(Y)^{2j-1} = \langle \Psi_J(U_a(X)), \Psi_J(V_a(Y)) \rangle_K, \quad \Psi_J(z) = (z, z^3, \ldots, z^{2J-1}),$$

and $W_a(X,Y) = \mathrm{TExt}(U_a(X), V_a(Y)) = \mathrm{Tr}_{K/F} H_J(U_a(X), V_a(Y))$, where the $\mathrm{Tr}_{K/F}$ linear map to the smaller field $F$ is necessary for the function to be a two source extractor.

It is not hard to show that $\mathrm{TExt}(U_a(X), V_a(Y))$ is indeed a two source extractor if each input has high enough entropy, and any parity of the output bits has rank $O(n)$ over $\mathbb{F}_2$, since the function $\mathrm{Tr}_{K/F} H_J(U_a(x), V_a(y))$ only has constant rank over $F$. However, it remains to see how to merge these outputs together. Towards that, we prove a *lower bound* on the rank of any non-trivial parity of the output bits when *restricted to* a sufficiently large rectangle $A \times B$, where $A$ and $B$ are the supports of $U_a(X)$ and $V_a(Y)$ respectively. For a good row $a$, we have that $|A|, |B| \geq 2^{(1-\tau)M}$. This step crucially uses Weil bound to argue that any non-trivial parity character of the encoding $\Psi_J(z)$ has small bias over $K$, and the odd exponents in the encoding are used to guarantee the Weil bound

in fields with characteristic 2. We use this to show that when $|A|, |B| \geq 2^{(1-\tau)M}$, the span of $\Psi_J(A)$ and $\Psi_J(B)$ both have dimension at least $JM - \tau M - 1$. Indeed, in the extreme case where $\tau = 0$, both spans have full dimension $JM$, for otherwise there will be a non-trivial parity character that is fixed, contradicting the Weil bound. Now any non-trivial parity of the output bits can be written as $h_{J,\lambda} = \mathrm{Tr}_{K/\mathbb{F}_2}(\lambda H_J(U_a(X), V_a(Y)))$ for some $\lambda \in K, \lambda \neq 0$. Since the binary bilinear form

$$B_\lambda(p, q) = \mathrm{Tr}_{K/\mathbb{F}_2}\left(\lambda \sum_{j=1}^{J} p_j q_j\right) \qquad (p, q \in K^J)$$

is nondegenerate, restricting its arguments to the spans of $\Psi_J(A)$ and $\Psi_J(B)$ costs at most the sum of their binary codimensions. Consequently, for all $|A|, |B| \geq 2^{(1-\tau)M}$, we have

$$\boxed{\mathrm{rank}_{\mathbb{F}_2}[h_{J,\lambda}]_{A\times B} \geq (J - 2\tau)M - 2, \qquad \mathrm{rank}_{\mathbb{F}_2}[h_{J,\lambda}]_{K\times K} \leq JM.} \tag{1.3}$$

This immediately suggests an approach to separate the good rows: we can choose a different number $J_a$ for a different row $a$. Here we use an idea similar to the construction of affine extractors for any constant entropy rate in [41], by choosing the numbers to be a geometric sequence: $J_a = 2^{a-1}$, and thus the summation of all $J_b, b < a$ is $\kappa_a = \sum_{b<a} J_b = J_a - 1$.

We use this property to show that on the $D$ good rows, for simplicity of exposition assume row 1 to $D$, the joint distribution $(W_1(X, Y), \cdots, W_D(X, Y))$ has full support of $F^D$. Towards that, we actually show that the distribution of $(W_1(X, Y), \cdots, W_D(X, Y))$, when restricted to $X^*, Y^*$, is exponentially close to uniform, with error $< 2^{-D\ell}$ where $\ell$ is the output length of each $W_i(X, Y)$. This follows from a hybrid argument: for any $a \in [D]$, let the transcript $\Pi_a = (W_1(X, Y), \cdots, W_{a-1}(X, Y))$, we show that the joint distribution $(W_a(X, Y), \Pi_a)$ is $2^{-\Omega(M)}$ close to $(U_F, \Pi_a)$. To show this, consider row $a$, and let $U = U_a(X), V = V_a(Y)$. By fixing extra randomness, the previous $a - 1$ rows can be viewed as deterministic functions of $(U, V)$, and hence the transcript $\Pi_a$ is also a deterministic function $\Pi_a(U, V)$. We now use a standard XOR lemma, and show that for any $\mu \in F, \mu \neq 0$, and any $\beta \in \mathbb{F}_2^{\ell(a-1)}$, the parity character

$$\mathrm{Tr}_{F/\mathbb{F}_2}(\mu W_a) + \beta \cdot \Pi_a = \mathrm{Tr}_{K/\mathbb{F}_2}(\mu H_{J_a}(U, V)) + \beta \cdot \Pi_a$$

has bias $2^{-\Omega(M)}$. This is one of the key steps in the analysis.

The proof follows from our rank bounds above and another application of the approximate duality lift. Specifically, the previous rank lower and upper bounds together imply that, when restricted to $A \times B$, every such mixed parity character is *nonconstant* because the rank of the parity is at least $(J_a - 2\tau)M - 2 - ((J_a - 1)M) = (1 - 2\tau)M - 2 > 1$ for sufficiently large $M$. Recall that in our construction we ensure that in a good row, each $U_a(X)$ and $V_a(Y)$ actually has entropy $(1 - \tau/2)M$, we can now apply approximate-duality to lift the bias of the character to be $2^{-\Omega(M)}$. By a careful choice of parameters, the total error is $< 2^{-D\ell}$. This finishes the first part of our analysis.

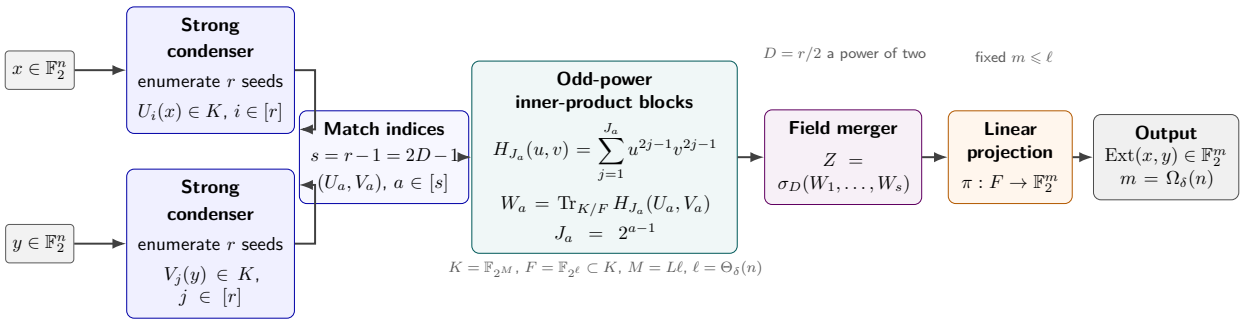
**The merger.** We now describe our final merger, which outputs $\Omega(n)$ bits. It needs to satisfy two properties: first it needs to merge the $2D - 1$ rows together, and ensure that any non-trivial parity of the output bits is non-constant. Second, it needs to keep any such parity to have rank $O(n)$, so that we can apply the approximate duality lift again to achieve exponentially small error.

The second property is actually easier to achieve. Since we are working over a large field $F$, and each output $W_a(x, y) \in F$ can be written as $W_a(x, y) = \sum_{j=1}^{R} A_j(x) B_j(y)$ where $R$ is a constant, and each $A_j, B_j$ is a function from $\mathbb{F}_2^n$ to $F$, applying any constant degree polynomial over $F$ to the

$2D-1$ outputs and taking parity will keep the rank to be $O(n)$, by a trace dual basis. To achieve the first property, we design the merger as follows: first apply the following symmetric polynomial on the $s = 2D-1$ outputs: $\sigma_D(z_1, \ldots, z_s) = \sum_{\substack{S \subseteq [s] \\ |S|=D}} \prod_{a \in S} z_a$, then take a fixed surjective binary-linear projection to $m = \Omega(n)$ bits, where $m$ is sufficiently small so that we can apply the XOR lemma to ensure that the output bits are $2^{-\Omega(n)}$ close to uniform.

To see why this works, recall that previously we showed that there are $D$ good rows which have the full support $F^D$. In particular, this means for any element $\alpha \in F$, there is a positive probability that all the $D$ good rows take the value $\alpha$. Because $D = \frac{r}{2} = 2^{d-1}$ is a power of two, in characteristic two we have $(1+\alpha T)^D = 1 + \alpha^D T^D$. Notice that the coefficient of $T^D$ in the generating function $\prod_{a=1}^{2D-1}(1+W_a T)$ is exactly $\sigma_D(W_1, \ldots, W_{2D-1})$. Thus whenever any $D$ of the $W_a$'s equal $\alpha$, we have $\sigma_D(W_1, \ldots, W_{2D-1}) = \alpha^D$, regardless of the remaining $D-1$ inputs. Equivalently, this can be viewed as taking the *majority* of the outputs. Therefore, the output of $\sigma_D$ also has full support in $F$, and thus any non-trivial parity of the linear projection is non-constant. Finally, we can use approximate duality lift again to achieve exponentially small error, and use a XOR lemma again to conclude that the $\Omega(n)$ output bits are $2^{-\Omega(n)}$-close to uniform. In particular, in the analysis we use approximate duality lift twice to reduce the error.

Below is a figure illustrating the construction:




**Evaluated operations only:** constant-seed strong condenser on each source; evaluation of only the $r-1$ matched odd-power inner products over $K$; trace to $F$; elementary symmetric degree-$D$ merger; fixed linear projection. Here $J_a = 2^{a-1}$, $F = \mathbb{F}_{2^\ell} \subset K = \mathbb{F}_{2^M}$, $\ell = \Theta_\delta(n)$, and $D$ is a power of two.

**Sumset extractor.** Our construction of the sumset extractor roughly has the same structure as the two source extractor, with a couple of modifications. First of all, if we just apply an arbitrary condenser and try every possible seed, this destroys the sumset structure, and the subsequent analysis won't work. Instead, we need a condenser where for each fixed seed, the function is a linear function. We build such a condenser to replace Raz's condenser, by first using the somewhere high entropy linear condenser of Li and Zhong [50], and then merge the rows together by using a curved merger as in [33, 32].

Second, because now the only input we get is a sum $X+Y$, we won't be able to apply the function $H_J(U_a(X), V_a(Y)) = \sum_{j=1}^{J} U_a(X)^{2j-1} V_a(Y)^{2j-1}$ directly. Instead, we use $(U_a(X) + V_a(Y))^d$, where $d = 2^h - 1, h \geqslant 3$. Again let $u = U_a(X), v = V_a(Y)$, in characteristic two, Lucas's theorem implies

that all binomial coefficients of $d$ are odd, so

$$\boxed{(u+v)^d = \sum_{j=0}^{d} u^j v^{d-j}.} \tag{1.4}$$

Consequently, for every nonzero $\lambda \in K$,

$$\operatorname{rank}_2 \left[\operatorname{Tr}_{K/\mathbb{F}_2}(\lambda(u+v)^d)\right]_{u,v\in K} \leqslant (d+1)M = 2^h M. \tag{1.5}$$

As long as $h$ is a constant, the global rank is still $O_h(M) = O(n)$. We then use a moment–trace-code argument and show in Proposition 3.20, that by choosing $h$ appropriately, we can ensure that the *restricted* rank on a high entropy rectangle $A \times B$ can grow by an arbitrarily large fixed multiple of $M$. Thus we can again use the previous strategy: choose a different $h$ for different rows to separate the good rows, and the remaining argument can follow.

**Non-malleable two source extractor.** On the high level, our $C$ tampering non-malleable two source extractor follows the general framework as our standard two source extractor, by applying a constant-seed strong condenser on each source, computing a suitable *non-malleable* two source extractor for high entropy rate on each aligned pair of rows, and merging the row outputs with $\sigma_D$. In particular, we will use rank properties of our construction and approximate duality lift. The additional difficulty is that we need to ensure the non-malleable property. Here we briefly explain several new ingredients needed in the new construction.

First, to prove non-malleability, our strategy is to use a non-malleable version of XOR lemma on the output bits, such as that in [29]. This requires to show that any mixed binary character, which corresponds to the linear combination of any non-empty subset of the output bits from the original inputs, and any subset of the output bits from the tampered inputs, has exponentially small bias. In the analysis of the standard two source extractor, we prove this by showing that the joint distribution of the $D$ "good outputs" has full support of $F^D$, and then use the property that $\sigma_D$ acts like the majority function. This implies the output of $\sigma_D$ has full support of $F$. Thus any non-trivial character is non-constant, and we then reduce the bias to exponentially small by an approximate duality lift. Here, similarly, our strategy to show that the joint distribution of the $D$ good outputs, together with all their $C$ tampered versions, has full support of $F^{D(C+1)}$, hence the joint output after applying $\sigma_D$ has full support of $F^{C+1}$.

However, in general this is false, since some of the tamperings may not have entropy at all, and some of the tamperings may be the same. To address this, we analyze one mixed binary character at a time. If an active tampering pair has a heavy input value on either side, we restrict to that value on the corresponding original source, which doesn't cause much entropy loss. The contribution of the tampering pair to the character then depends only on the other original source, so we further fix that one-bit contribution at an additional entropy cost of at most one bit, and remove this pair of tamperings from the character. Repeating this process leaves only tamperings whose two input marginals have the required entropy. For identical tampering copies, we can combine the parities on these outputs together into one parity on just one copy of such outputs. Hence, we can assume that we have at most $C$ tamperings that are all different, and each of them has enough entropy.

**Distinguishing the executions.** As in previous constructions of non-malleable extractors, we need a strategy to distinguish the original inputs and their tampered versions. Here we use a simpler strategy than the advice generators in previous works. Specifically, we view each full input

$x$ as the coefficient vector of a polynomial $P_x$ over a field with a small linear number of bits per element. Thus the polynomial has some constant degree $b$. For each index $a$ of the rows in the condenser output, we choose a different fixed evaluation point $t_a$, and compute the tag (or advice) $(P_x(t_a), P_y(t_a))$. This approach has the advantage that each ($P_x(t_a)$ or $P_y(t_a)$) is a deterministic function of $X$ and $Y$ respectively, and thus it's convenient to condition on the fixing of such tags while preserving the independence of $X$ and $Y$.

To apply the $\sigma_D$ as majority argument above, we would like to argue that there are a majority of $D$ good rows that have the *same* indices in every tampered execution of the extractor, as well as the execution on the original inputs. Since we will eventually apply a non-malleable two source extractor for high entropy rate to each row, we want to ensure that in these $D$ rows, *all* inputs are distinguished by the tags. Recall that we assumed before that every tampering is different. Intuitively, we want to argue that every two different set of tags $\{(P_x(t_a), P_y(t_a))\}$ computed from $(x, y)$ and $\{(P_{x'}(t_a), P_{y'}(t_a))\}$ computed from $(x', y')$ can agree on at most $b$ positions (recall $b$ is the degree of the polynomials $P_x, P_y$). So, altogether there are at most $\binom{C+1}{2}b$ positions that can have a collision in tags. We can make sure these positions, together with the bad seeds of the condenser, consist of $< 1/2$ fraction of all possible rows, by cycling through the condenser seeds to create enough rows if necessary.

However, there are a couple of issues with the above argument. First, we only know that any pair of tamperings are different from the original pair of inputs on every possible input strings, but for two different pairs of tamperings, they may still be the same on certain inputs. Second, even if two pairs of tamperings (or one pair of tampering and the original pair of inputs) are different on every possible input strings, the positions where the tags are different can depend on the specific input strings. To address these issues, we *fix* the equality/inequality patterns and move to a subsource. Specifically, let the original inputs be $x_0 = x, y_0 = y$, and the $C$ tampered inputs be $x_i = f_i(x), y_i = g_i(y)$ for $i \in [C]$. For every $0 \le i < j \le C$, we record two bits of whether $x_i = x_j$ and $y_i = y_j$. Altogether these give $2\binom{C+1}{2}$ bits, and we can fix one particular pattern of these bits such that both sources only lose at most $\binom{C+1}{2}$ bits of entropy, and they are still independent. Crucially, conditioned on this fixing, for every $i, j$, the equality $x_i = x_j$ is either always true or always false on the retained left support, and the same holds for $y_i = y_j$ on the retained right support. Furthermore, the two equalities cannot hold simultaneously unless $i, j > 0$. If this happens for some $i, j$, then again we can merge these two tamperings in our analysis of the mixed character. Hence, after this step we can assume that the tampering functions are also different on at least one side for every possible input strings. This takes care of the first issue.

Next, we do the same and fix *tag equality indicators*. Suppose we have $R$ rows in total from the previous possible cycling of the condenser seeds. For every different $i, j$, at row $a \in [R]$, their tags are $(P_{x_i}(t_a), P_{y_i}(t_a))$ and $(P_{x_j}(t_a), P_{y_j}(t_a))$. We now record two bits of whether $P_{x_i}(t_a) = P_{x_j}(t_a)$ and $P_{y_i}(t_a) = P_{y_j}(t_a)$. Again there are at most $2R\binom{C+1}{2}$ bits, and we can fix one particular pattern of these bits such that both sources only lose at most $R\binom{C+1}{2}$ bits of entropy, and they are still independent. Now conditioned on this fixing, for any $i, j$, the set of indices $a$ with tag collisions are the *same* for all input strings throughout the retained product support. This takes care of the second issue.

**A tagged high entropy non-malleable extractor against one tampering.** Next, we use a tagged high entropy non-malleable extractor against one tampering as the starter extractor to apply on each pair of rows. We will later modify it to one against $C$ tamperings. In [49], Li constructed explicit non-malleable two source extractors for entropy rate $1 - \delta$; however, the rank properties we

need here are not supplied by the non-malleable extractor guarantee alone. Therefore, we come up with a new construction tailored for that.

The new tagged high entropy non-malleable extractor is an asymmetric extractor, specifically tailored to satisfy the rank properties. Let $z, w \in \mathbb{F}_2^M$ denote the complete left and right rows, where $M = 6n_0$. Choose binary fields $K \subset F \subseteq L$ with $L = \mathbb{F}_{2^{n_0}}$ and $[F : K] = 2$. Let $\bar{x}$ be a prefix of $z$ with $n_0$ bits and view $\bar{x}$ as an element in $L$. Parse the complete right row as $w = (r, t, Y) \in L^2 \times K^J$, where $J \log_2 |K| = 4n_0$. For a coefficient vector $d = (d_0, d_1, \ldots)$, write $P_d(T) = \sum_j d_j T^j$. Define

$$\Gamma_c(\bar{x}) = (\bar{x}, \bar{x}^{1+2}, \ldots, \bar{x}^{1+2^c}), \tag{1.6}$$

$$S_\alpha(\bar{x}) = V_0(\bar{x}) + \alpha V_1(\bar{x}) = (u, v) \in K^2. \tag{1.7}$$

Here $\alpha \in F$ is a fixed numerical tag as we described above, and we identify $F$ with $K^2$ by using a fixed $K$-basis. The functions $V_0, V_1$ come from Li's near-full-entropy affine non-malleable extractor [49]. For distinct fixed tags $\alpha \neq \alpha'$ and any affine map $h : L \to L$ (including the identity), the honest seed $S_\alpha(U_L)$ is exponentially close to uniform even given $S_{\alpha'}(h(U_L))$. The tag enters the evaluated starter only through the coordinates $(u, v)$ of $S_\alpha(\bar{x})$.

Before the final output-shortening trace, the extractor computes the following $K$-valued function:

$$\mathcal{E}_\alpha(z, w) = E_\alpha(\bar{x}; r, t, Y) = \underbrace{\mathrm{Tr}_{L/K}\Big(tP_{\Gamma_c(\bar{x})}(r)\Big)}_{\text{Gold recognition}} + \underbrace{vP_Y(u)}_{\text{tagged extraction}}, \qquad (u, v) = S_\alpha(\bar{x}). \tag{1.8}$$

Thus the extractor ignores the unused suffix of the honest left row, but its arbitrary left tampering may depend on that suffix. The Gold coordinates of $\bar{x}$ have binary degree at most two, whereas the second term computes the right coefficient polynomial at the seed coordinate $u$ and multiplies by $v$.

The two summands have distinct purposes: the *Gold term* recognizes when an arbitrary left tampering behaves like an affine tampering, while the *tagged evaluation term* rules out a constant mixed character once that affine structure has been found. On the other hand, the right tampering can be any arbitrary function.

More specifically, consider two independent sources that are uniform on sets $A$ and $B$, and two tampering functions $f$ and $g$. We will argue that for distinct tags $\alpha \neq \alpha'$, the mixed binary character

$$\chi(z, w) = \mathrm{Tr}_{K/\mathbb{F}_2}(\lambda \mathcal{E}_\alpha(z, w) + \mu \mathcal{E}_{\alpha'}(f(z), g(w))), \qquad \lambda \neq 0,$$

is non-constant on $A \times B$, and then use approximate duality lift to reduce the bias to exponentially small on slightly larger product sets. The case where $\mu = 0$ is easy to analyze, so we focus on the case where $\mu \neq 0$. Towards that, fix the unused left suffix in the analysis, the left tampering function $f$ is then a deterministic function of $\bar{x}$. With slight abuse of notation, let the corresponding prefix of the tampered left row be $f(\bar{x})$, and suppose that $\bar{x}$ is still supported on $A$. If $f$ is an affine function, then $\Gamma_c(f(\bar{x}))$ is also a quadratic function in the bits of $\bar{x}$. We thus measure how far $f$ is from an affine function by the *Gold defect* $d_c(f; A)$, defined to be the dimension of the span of the binary coordinate functions of $\Gamma_c \circ f$ modulo the space of all Boolean functions of degree at most 2, restricted to $A$.

If $d_c(f; A)$ is large, then this implies that the rank of the sum of the Gold terms in $\chi(z, w)$ is already large, because $\Gamma_c(\bar{x})$ are quadratic in the bits of $\bar{x}$, while $d_c(f; A)$ measures the dimension of $\Gamma_c(f(\bar{x}))$ outside of the space of quadratic Boolean functions. On the other hand, the rank of the sum of the tagged extraction part is small, since each of them expands into $J$ separated products over $K$ and has binary matrix rank at most $J \log_2 |K|$. Together, this implies that $\chi(z, w)$ has binary matrix rank $> 1$, and hence is non-constant.

Conversely, if $\chi(z,w)$ is a constant, then this forces $d_c(f;A)$ to be small. Our amortized recognition theorem (Theorem 3.41) produces a large subset $A_1 \subseteq A$ on which $f$ agrees with an affine map $h$. The crucial feature of our theorem is that the Gold defect $\rho = d_c(f;A)$ contributes only $O(\rho/c)$ to the entropy deficiency of the affine-agreement subset, rather than $O(\rho)$. More precisely, the theorem gives an affine-agreement subset $A_1 \subseteq A$ of ambient entropy deficiency $O(a+\rho/c+c)$, where $a = n_0 - \log_2|A|$. Thus in our application, we can choose $a$ to be a small enough constant fraction of $n_0$, and $c$ to be a sufficiently large constant, so that the deficiency of $A_1$ is an arbitrarily small fraction of $n_0$. Although $A_1$ need not be an affine subspace, the affine non-malleable extractor property on the ambient uniform affine subspace implies, by counting, that there exists a value $z'$ such that $\{S_\alpha(\bar{x}) : \bar{x} \in A_1,\ S_{\alpha'}(h(\bar{x})) = z'\}$ contains many distinct values. We then use this and a dimension argument to arrive at another contradiction. Roughly, we fix $S_{\alpha'}(h(\bar{x})) = z'$, as well as a pair of $(r,t)$ and its tampered version $(r',t')$, such that the right row still has much entropy. Now in the mixed character $\chi(z,w)$, every term in the summation becomes a local function of either $\bar{x}$ or $w$, except the tagged extraction term $vP_Y(u)$ on the original inputs. Using the bilinear form of $vP_Y(u)$ and the assumption that $\chi(z,w)$ is a constant, we can argue that two subspaces related to $w$ and an encoding of $\bar{x}$ are orthogonal, contradicting the bounds on their dimension.

**Extending to $C$ tamperings.** The above tagged extractor is left-source-strong against one tampering. We next extend it to handle $C$ tamperings, using a recursive procedure similar to alternating extraction, which doubles the number of tamperings at each intermediate level. However, we must maintain *two different invariants*: the left-source strong extractor property, needed to run the recursion, and bounded *field separation*, needed to keep the global binary character rank linear in the input length. In particular, a bound on the binary matrix rank alone would not suffice for the second invariant, because the intermediate steps perform non-linear operations and may increase the rank.

At level $i+1$, let $Z, W \in \mathbb{F}_2^N$ be the two input rows, and let $\mathrm{Ext}^i$ be the left-source-strong extractor we constructed at the previous level. First we apply $\mathrm{Ext}^i$ to two short prefixes of $Z$ and $W$, say $Z'$ and $W'$, using the same tag throughout the construction. Suppose $\mathrm{Ext}^i$ produces $\mathsf{R} = \mathsf{R}(Z',W')$ of length $w_0$. Put $q = C+1$ and $v = w_0/(256q)$, let $P$ be a prefix of $\mathsf{R}$ with $64v$ bits. Compute

$$\mathsf{L} = H_{8v}(Z;P), \qquad \mathrm{Ext}^{i+1}(Z,W) = H_v(\mathsf{R};\mathsf{L}).$$

Here $H_t$ is a standard strong seeded extractor of a particular form: for a seed $(u,t_0)$ over $\mathbb{F}_{2^{4t}}$, we treat the source as a coefficient word $d = (d_j)$, and

$$H_t(d;(u,t_0)) = \mathrm{Tr}_{\mathbb{F}_{2^{4t}}/\mathbb{F}_{2^t}}\left(t_0 \sum_j d_j u^j\right).$$

In both $H_{8v}$ and $H_v$, the input sources have length a fixed multiple of the relevant field degree, so the coefficient polynomials have degree $O_C(1)$.

*The statistical induction.* Suppose $\mathrm{Ext}^i$ handles $C_i$ comparisons, we show that $\mathrm{Ext}^{i+1}$ can handle $C_{i+1} = 2C_i$ tamperings. Towards that, divide the $2C_i$ tamperings into two groups $T, S$ of size $C_i$. Let $\mathsf{R}_0$ and $\mathsf{L}_0$ be the outputs of $\mathsf{R}$ and $\mathsf{L}$ on the original inputs. We will gradually fix a sequence of random variables while preserving the independence between $Z$ and $W$.

First fix the prefixes $Z'$ in all executions, thus all the $\mathsf{R}$ variables produced are deterministic functions of $W$, and $Z$ still has enough entropy if we choose $Z'$ to be short enough. By the fact that $\mathrm{Ext}^i$ handles $C_i$ tamperings, $P_0$ is close to uniform and independent of $\mathbf{P}_S = (P_j)_{j\in S}$. Thus, the strong extractor property of $H_{8v}$ guarantees that $\mathsf{L}_0$ is close to uniform and independent of

$\mathbf{L}_S = (\mathsf{L}_j)_{j\in S}$. Furthermore, we can fix all the $P$ variables while still preserving this property, and now the $\mathsf{L}$ variables are deterministic functions of $Z$. Notice that at the beginning, again by the fact that $\mathrm{Ext}^i$ handles $C_i$ tamperings and is left source strong, $\mathsf{R}_0$ is close to uniform and independent of all the $\mathsf{R}$-variables in the tampering set $T$. We can therefore fix all these $\mathsf{R}$-variables, in addition to the previous fixing of all the $P$ variables. By our choice of the length parameters, $\mathsf{R}_0$ still has enough entropy. Finally, the strong extractor property of $H_v$ guarantees that the new output of $\mathrm{Ext}^{i+1}$ on the original inputs is close to uniform and independent of all the tampering outputs in $S$, and all the $\mathsf{L}$ variables. Since all the $\mathsf{R}$-variables in $T$ have already been fixed, this means the output of $\mathrm{Ext}^{i+1}$ on the original inputs is actually close to uniform and independent of all the tampered outputs in $S \cup T$, as well as strong in the left source.

*Achieving the rank properties.* Recall that as in the analysis of the standard two source extractor, we need the output of each row of pairs to satisfy the following two rank properties: (1) every mixed character of the output and the tampered outputs, where the honest-output coefficient is nonzero, can have rank at least $K_*N$ for every prescribed constant $K_* > 0$ when restricted to a high entropy rectangle $A \times B$, which we need to merge the final outputs together; and (2) the global rank of any character of the output is bounded by $O(N)$, which we need for the final step of approximate duality lift. This is the place where we use the special form of the strong seeded extractors $H$ above. The idea is that we will work over a suitable common base field $E = \mathbb{F}_{2^{\Theta_C(N)}}$, so that every field word appearing in this fixed-depth recursion has only $O_C(1)$ coordinates over $E$. We choose the coordinate bases compatibly over $E$, and all prefixes and coefficient selections use whole $E$-coordinate blocks. Thus these selections and the relative traces are $E$-linear, while multiplication has a bounded coordinate expansion. For an $E$-valued function of the two *unconditioned* inputs, define its separation width by

$$\mathrm{sep}_E(U) := \min\left\{ r :\ U(z,w) = \sum_{i=1}^{r} a_i(z) b_i(w), \quad a_i, b_i \text{ are } E\text{-valued} \right\}.$$

The point is that if the $E$-valued function has constant separation width, then any parity of the output bits has $O(N)$ binary matrix rank. In particular, the $H$ functions above have constant separation width over $E$. The separation width has the following elementary closure rules:

$$\begin{aligned} \mathrm{sep}_E(U+V) &\leqslant \mathrm{sep}_E(U) + \mathrm{sep}_E(V), \\ \mathrm{sep}_E(UV) &\leqslant \mathrm{sep}_E(U)\,\mathrm{sep}_E(V), \\ \mathrm{sep}_E(U^{2^j}) &\leqslant \mathrm{sep}_E(U). \end{aligned}$$

Applying these rules inductively, and noting that we are only doing the recursion for a constant number of steps, we can bound the separation width of all intermediate outputs to be $O_C(1)$.

However, we also need to get a lower bound on the binary rank restricted to a high entropy rectangle $A \times B$. Therefore we change *the last level of the recursion*, and replace the function $H_v(\mathsf{R};\mathsf{L})$ by

$$\mathrm{Tr}_{L/K}\Big(bt(1+ur)^{J-1}\Big), \qquad \mathsf{L} = (u,b) \in K^2, \quad \mathsf{R} = (r,t) \in L^2,$$

where $J$ is a sufficiently large fixed power of two. In characteristic 2, the identity $(1+ur)^{J-1} = \sum_{i=0}^{J-1}(ur)^i$ expresses this as a fixed-width polynomial in already separated field words; hence its *global* binary character rank is still $O_{C,J}(N)$. But, on the product rectangles obtained from our argument, by a similar argument as in the standard two source extractors, the large supports of the honest $\mathsf{R}_0$ and $\mathsf{L}_0$ give the independent *restricted* rank lower bound

$$\mathrm{rank}_{\mathrm{restricted}} \geqslant 4Jv - \frac{w_0}{3} - 5.$$

Choosing $J$ after the entropy parameters can thus make this larger than any prescribed constant times $N$.

**Finishing the extractor.** The rest of the construction and the analysis are similar to the standard two source extractor we described before. The final step is to merge the constant number of outputs together, and in the analysis we make two other uses of approximate duality lift to reduce the error to exponentially small.

**Achieving optimal output length.** We use our extractors with $\Omega(n)$ output length and $2^{-\Omega(n)}$ error to achieve modified extractors with optimal output length for a given error $\varepsilon$. Here we illustrate the main ideas by using the standard two source extractor that achieves output length $2k - O(\log(1/\varepsilon) + 1)$ as an example. Our previous two source extractor $G(X, Y)$ with error $2^{-\Omega(n)}$ is actually a strong two source extractor, so this suggests the following natural approach: first use that two source extractor to produce a short seed $S = G(X, Y)$ with $d$ bits, then take two strong seeded extractors with optimal parameters $E_L, E_R$, and output

$$\mathrm{Ext}(X, Y) = \big(S, E_L(X, S), E_R(Y, S)\big).$$

The strong property guarantees that either $(S, E_L(X, S))$ or $(S, E_R(Y, S))$ is close to uniform. However, proving that $\big(S, E_L(X, S), E_R(Y, S)\big)$ is close to uniform is not straightforward.

Let $s = \lceil \log_2(1/\varepsilon) \rceil$, we choose the two output lengths asymmetrically: $E_L(X, S)$ outputs $p_L = k - d - 2s - O(1)$ bits, and $E_R(Y, S)$ outputs $p_R = k - O(s + 1)$ bits. In the analysis, the main issue is the dependence of $S$ on both sources. We resolve this by bounding the conditional collision probability of the first output and seed, weighted by the actual marginal distribution of $Y$. By using Cauchy Schwarz, one can convert the resulting conditional collision probability bound into statistical distance. This naturally suggests that we need to consider the output of $G(X, Y)$ on different copies of $X$ conditioned on $Y$, which can be captured by the stronger property of *one-sided non-malleability*. That is, we only need $G(X, Y)$ to be non-malleable against one sided tampering. Therefore, we can for example simply take $G(X, Y)$ to be our non-malleable two source extractor described above. With the parameter choices in Section 4.1, this gives

$$(Y, S, E_L(X, S)) \approx_{\varepsilon/4} (Y, U_d, U_{p_L}),$$

where the uniform variables on the right are independent of each other and of $Y$. Once we have this property, we can safely append the second output of $E_R(Y, S)$ by using the strong seeded extractor $E_R$, and the output length and error follow.

For strong non-malleable extraction against $C$ tamperings, we use the symmetric construction

$$\mathsf{nmExt}(X, Y) = \big(S, E(X, S) \oplus E(Y, S)\big),$$

where $E$ is a strong seeded extractor. Here the seed must withstand $2C + 1$ tamperings, because the collision argument introduces a second input for each original and tampered input. Fortunately, our multi-tampering non-malleable two source extractor with $\Omega(n)$ output length and $2^{-\Omega(n)}$ can still handle this.

For sumset extractors, we use a seed $S = G(Z)$ computable from $Z = X + Y$, by using our previous sumset extractor, together with a linear seeded extractor LExt. As before, we will need the sumset extractor to have one-sided non-malleability, thus we use a slightly modified construction which achieves this property in Theorem 3.33. The construction is

$$\mathrm{SumExt}(Z) = \big(S, \mathrm{LExt}(Z, S)\big).$$

**Achieving $Cn/\log n$ entropy.** Our constructions above can be directly pushed to handle slightly sub-constant entropy rate. However, to achieve $Cn/\log n$ entropy, we use a somewhere high entropy condenser such as those in [6, 58, 50], which outputs a polylogarithmic number of rows each of length $n/\operatorname{polylog} n$, such that at least one row is exponentially close to having high entropy. Suppose we get $r = 2^d$ rows from each source, now we try every possible pair of rows from the two sources, resulting in $r^2$ pairs such that at least one pair has high entropy from both sources.

From here, we simply treat each row as a vector in $F^t$ for some appropriately chosen field $F = \mathbb{F}_{2^\ell}$, and apply the standard inner product two source extractor over $F$. We show that by choosing the parameters appropriately, the joint distribution of the $r^2$ outputs is exponentially close to a convex combination of *affine somewhere random sources*, which is an affine source on $r^2$ rows such that some row is actually uniform.

This is motivated by the work of Aggarwal, Dodis, and Lovett [1] on split-state non-malleable codes, where they showed that if $L$ and $R$ are two independent uniformly random strings over $\mathbb{F}_p^n$ for some prime number $p$, and $f, g : \mathbb{F}_p^n \to \mathbb{F}_p^n$ are two arbitrary functions on $L$ and $R$, then the joint distribution $(\langle L, R\rangle, \langle f(L), g(R)\rangle)$ is "close" to the convex combination of "affine distributions" $\{(U, aU + b) | a, b \in \mathbb{F}_p\}$, where $U$ is the uniform distribution over $\mathbb{F}_p$. In our situation, instead, the $L$ and $R$ are two independent high entropy sources we obtain from the outputs of the somewhere high entropy condenser on $X$ and $Y$, and by fixing extra randomness, the other outputs we get from the condenser can be viewed as deterministic tampering functions on $L$ and $R$. Furthermore, in our application we have $r^2 - 1$ pairs of tampering functions instead of just one pair. There is also the technical issue that now we are working over the field $\mathbb{F}_{2^\ell}$ instead of a prime field $\mathbb{F}_p$.

Nevertheless, we can indeed prove such a binary-affine, many-output analogue of the result in [1] for high-min-entropy sources. The proof again uses the approximate duality formulation in [8] and roughly goes as follows. First of all, instead of using an arbitrary somewhere high entropy condenser which has non-linear maps, we use the linear condenser in [50] as we did in our construction of sumset extractors. The advantage is that in the analysis, every binary parity character of an inner product output is actually a bilinear function in the *original input bits*. This is still true if we consider a joint binary parity character of the $r^2$ outputs. Thus the combined feature dimension is only $2n$, independent of the number of pairs $r^2$, which helps us get better parameters when applying approximate duality. On the other hand, using a non-linear somewhere high entropy condenser could result in a much larger feature dimension that depends on $r^2$. Now, in the analysis we look at the joint distribution of the $r^2$ outputs and consider the affine span of the support. If the distribution is already close to being uniform on the affine subspace, then we are essentially done because the inner product guarantees that one output is close to uniform. Otherwise, some non-trivial character on this affine subspace has large bias under the distribution, and we can invoke approximate duality to find a large rectangle on which that character is constant. We then use this rectangle to divide the original input space into disjoint rectangles (thus maintaining the property of independent sources) and continue this process. Using a potential function, we show that this process terminates in a finite number of steps, and except for a small probability mass, the distributions on the outputs of the rest rectangles are close to being uniform on an affine subspace. Furthermore, we show that we don't lose much entropy in this process, and therefore on any sufficiently large rectangle, by the property of the condenser and the inner product two source extractor, some good row projection of the output affine subspace has full support. The uniform distribution on this affine subspace therefore has an exactly uniform honest row. We can now conclude that the original joint distribution is close to a convex combination of affine somewhere-random sources with $r^2$ rows.

As long as the number of rows $r^2$ here is relatively smaller than the length of each row, there are very good known extractors, e.g., those by Rao [55] using repeated conditioning and later works

using affine correlation breakers [12, 49] that can extract random bits with exponentially small error from such affine somewhere random sources. For non-malleable extractors, some extra work needs to be done here, and we eventually apply an advice based correlation breaker.

However, the above approach only gives us a two source extractor with error $2^{-k^{\Omega(1)}}$ instead of $2^{-\Omega(k)}$, even for constant entropy rate. Indeed, the error comes from two steps in the above construction: the step of converting to an affine somewhere random source, and the later step of extracting from such a source. To get $2^{-\Omega(k)}$ error from the second step, even with a constant number of rows, one would need the row length to be $\Omega(k)$, which will force us to take a field of size $2^{\Omega(k)}$ in the first step and therefore only a constant number of blocks in the inner product. In this case, the analysis of approximate duality breaks. The limitation can be seen more precisely from the entropy-loss bound in our regularization theorem (Theorems 2.30 and 5.5). For a constant number of rows and constant entropy rate, if each field inner-product output has $\ell$ bits, then the two principal contributions to the regularization entropy loss, with rank threshold $R$, are roughly $O\left(\frac{k\ell}{R}\right)$ from high-rank approximate-duality, and $O(\ell R)$ from low-rank exact-message steps. Balancing these two terms gives $R = \Theta(\sqrt{k})$ and a combined entropy loss of $O(\ell\sqrt{k})$. This forces us to choose $\ell = O(\sqrt{k})$ with a sufficiently small constant factor. Hence we only get a square-root scale of the output length and error exponent by this approach. One can combine with a strong seeded extractor to increase the output length to $\Omega(k)$, but the error will still be $2^{-\Omega(\sqrt{k})}$. At entropy rate $\Theta(1/\log n)$, the number of rows we get from the condenser further increases to poly-logarithmic, and output-extension losses lead to $2^{-n^{1/2-\vartheta}}$ error range for every fixed $\vartheta > 0$. Not surprisingly, our extractors for constant entropy rate with asymptotically optimal parameters use genuinely different constructions and techniques.

**Independent work and Acknowledgments.** The work of Doron and Goodman [31] constructed explicit two-source extractors for entropy $k \geq n^{1-\alpha}$ with error $2^{-k^{\alpha}}$ for some constant $\alpha > 0$. Their error is still $2^{-k^{\alpha}}$ for constant entropy rate. Hence their extractors work for smaller entropy than ours, while our extractors have better error and output length for any constant entropy rate. Their techniques share some similarity with our extractors for entropy $Cn/\log n$, in that both constructions use approximate duality to first convert the two sources into a convex combination of affine somewhere random sources, and then apply an extractor for such sources. Doron and Goodman went further, and used additional new ideas and techniques to reduce the entropy to $k \geq n^{1-\alpha}$. On the other hand, our asymptotically optimal extractors for constant entropy rate also use new ideas and techniques that are unrelated to their results.

Doron and Goodman obtained their preliminary results at the end of December 2025. While they were filling in the details and writing up their results, the author independently discovered the extractors for entropy $Cn/\log n$ in this paper around August 2026, without being aware of their results. The author has since been pursuing two directions: reducing the entropy requirement and improving the error. However, while attending the Pseudorandomness and High-Dimensional Expansion program at Simons Institute in September 2026, the author learned their unpublished results and their high level ideas. The author then focused on reducing the error of the extractors, and finally obtained the new constructions of extractors for constant entropy rate with asymptotically optimal parameters. The author thanks the Simons Institute for its hospitality and support.

**AI Disclosure.** The author used ChatGPT Astra substantially for exploring proof ideas, literature survey, and drafting the manuscript. Most of the high level ideas belong to the author, while ChatGPT also contributed important technical ideas towards the complete proofs. ChatGPT Astra

is also used to help with the tedious work of choosing appropriate parameters. During numerous exchanges with ChatGPT, many intermediate approaches have failed before the final successful constructions emerged. The constructions presented here also include simplifications of previous, more complicated constructions.

**Organization of the paper.** Section 2 collects the common preliminaries, including source-strong extractors, rank-sensitive approximate duality, condensers, seeded primitives, and the shared-feature regularization theorem. Section 3 develops the constant-rate constructions with linear output length and exponentially small error: standard two-source extractors, sumset extractors, and non-malleable two-source extractors against any fixed number of tamperings. Section 4 uses the preceding constructions as short seeds and develops entropy-recycling arguments to obtain optimal output lengths for the above extractors. Finally, Section 5 gives constructions for entropy $k = \Omega(n/\log n)$.

## 2 Preliminaries and common tools

A cited theorem is used only under its stated hypotheses. Internal lemmas and their proofs are arranged in the order needed by the constructions. The same symbol may denote a local field length in different subsections; the original input length remains $n$.

**Notation and conventions.** For a nonnegative integer $r$, write $[r] = \{1, \dots, r\}$, with $[0] = \varnothing$, and $(x)_+ = \max\{x, 0\}$. The notation $\mathbf{1}_E$ denotes the indicator of an event or set $E$. For a nonempty finite set $S$, $U_S$ is its uniform distribution; $U_m$ abbreviates $U_{\mathbb{F}_2^m}$. A product $U_S^{\otimes r}$ consists of $r$ independent uniform copies. In an ideal comparison, a newly introduced uniform variable is independent of the retained variables unless stated otherwise. We write $\mathcal{L}(X)$ for the distribution of $X$, $\operatorname{supp} X$ for its positive-probability support, and $X \approx_\varepsilon Y$ when $\Delta(\mathcal{L}(X), \mathcal{L}(Y)) \leqslant \varepsilon$, using the statistical distance defined below. The symbol $\perp$ between random tuples means independence. For a distribution $P$ on a finite alphabet, its collision probability is $\operatorname{cp}(P) = \sum_z P(z)^2$; we also write $\operatorname{cp}(X) = \operatorname{cp}(\mathcal{L}(X))$. For a subdistribution the same sum is used, without normalizing its mass.

Unless another field is specified, vector-space spans, dimensions, codimensions, orthogonality, and matrix ranks are over $\mathbb{F}_2$. The notation $\operatorname{rank}_2 h$ for a Boolean kernel means the rank of its matrix of 0/1 values, not the real rank of its sign matrix. For a finite set $A$, $\mathbb{F}_2^A$ denotes the space of all functions $A \to \mathbb{F}_2$. For a nonempty subset $S$ of a binary vector space and any $s_0 \in S$, its affine hull is

$$\operatorname{aff}(S) = s_0 + \operatorname{span}_{\mathbb{F}_2}\{s - s_0 : s \in S\}.$$

Its dimension is the dimension of the displayed direction space. An affine source is uniform on an affine subspace; a tuple is *jointly affine* when its concatenation has this property. For a kernel $Q$, the notation $Q(A, B)$ means $\{Q(x, y) : x \in A,\ y \in B\}$, not a probability distribution. All affine maps between binary-coordinate representations of fields are $\mathbb{F}_2$-affine unless another field is specified.

For a bit string $z$, $\operatorname{prefix}_d(z)$ denotes its first $d$ coordinates, with $0 \leqslant d \leqslant |z|$. The operation $\oplus$ on bit strings is coordinatewise addition modulo two, while $z \parallel z'$ denotes concatenation. On vector spaces or codes, $\oplus$ denotes a direct sum. For a field $K$, both $K^*$ and $K^\times$ denote $K \setminus \{0\}$.

**Definition 2.1** (Ordinary two-source and sumset extraction)**.** An ordinary two-source extractor at component entropy $k$ and error $\varepsilon$ is a map $E : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$ such that $E(X, Y) \approx_\varepsilon U_m$ for every independent pair with min-entropies at least $k$. A sumset extractor is a map $S : \mathbb{F}_2^n \to \{0,1\}^m$ such that $S(X + Y) \approx_\varepsilon U_m$ for every such pair. A guarantee for a sum-only evaluator does not by itself assert source strength after an original summand is revealed.

**Definition 2.2** (Non-malleable two-source extraction)**.** A map $E : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$ is a $t$-non-malleable two-source extractor at entropy $k$ and error $\varepsilon$ if, for independent sources $X, Y$ of entropy at least $k$ and arbitrary separate maps $f_j, g_j$ satisfying $\Pr[(f_j(X), g_j(Y)) = (X, Y)] = 0$, one has

$$\Delta\big((E(X,Y), (E(f_j(X), g_j(Y)))_{j=1}^t), (U_m, (E(f_j(X), g_j(Y)))_{j=1}^t)\big) \leqslant \varepsilon.$$

The fresh uniform variable is independent of the actual joint tampered-output distribution. No entropy assumption is made on tampered inputs. For $t = 0$ the comparison tuple is empty and the definition is ordinary two-source extraction. All fixed-$C$ statements use this convention.

## 2.1 Source-strong extraction and entropy-slack transfer

**Definition 2.3** (Separate source strength)**.** Let $Z = F(X, Y)$, and, for an admissible tuple of $t$ separate tamperings, put $T_j = F(f_j(X), g_j(Y))$ and $\mathbf{T} = (T_1, \ldots, T_t)$. A $t$-non-malleable function $F$ is *source strong with error* $\xi$ at component entropy $k$ if, for all independent $k$-sources and all such tamperings,

$$\Delta((Z, \mathbf{T}, X), (U_m, \mathbf{T}, X)) \leqslant \xi, \qquad \Delta((Z, \mathbf{T}, Y), (U_m, \mathbf{T}, Y)) \leqslant \xi.$$

The two guarantees are separate; neither discloses $(X, Y)$ jointly. For ordinary source-strong extraction, set $t = 0$ and omit $\mathbf{T}$.

**Lemma 2.4** (A source-strong output cannot exceed one source's entropy)**.** Let $k$ be an integer with $0 \leqslant k \leqslant n$. If a deterministic two-source function is source strong with error $\varepsilon < 1$ at component entropy $k$ and output length $m$, then

$$\varepsilon \geqslant 1 - 2^{k-m}, \qquad \text{hence} \qquad m \leqslant k + \log \frac{1}{1-\varepsilon}.$$

In particular, for $\varepsilon < 1/2$, a source-strong output cannot contain more than $k$ bits.

*Proof.* Take $Y$ uniform on exactly $2^k$ points and choose any independent $k$-source $X$. For each fixed value $X = x$, the conditional honest output is a function of only the $2^k$ points in the support of $Y$, hence has support size at most $2^k$. Its distance from uniform on $2^m$ outputs is at least $1 - 2^{k-m}$. Average over $x$ to obtain the strong-distance lower bound. Rearranging proves the claim. □

**Finite initial lengths.** When a linear-output theorem is stated for every positive input length but its field construction is given only for $n \geqslant n_0$, the following deterministic completion suffices. For $1 \leqslant n < n_0$, return one constant zero bit. Even with an arbitrary comparison tuple and either original source retained, replacing that bit by an independent uniform bit has statistical distance exactly $1/2$. Every output character has binary truth-table rank zero. If the large-length output and error constants are $c, a > 0$, replace them by $\min\{c, 1/n_0\}$ and $\min\{a, 1/n_0\}$. Then the one-bit completion satisfies both $m(n) \geqslant cn$ and error at most $2^{-an}$ throughout the finite initial range. This convention is invoked explicitly below; it does not extend an additive-loss theorem beyond its stated nontrivial error range.

**Lemma 2.5** (Atomwise entropy-slack strongification)**.** Let $F$ be a $t$-non-malleable two-source extractor at component entropy threshold $h$, output length $m_0$, and error $\gamma$, where $t = 0$ denotes ordinary extraction. Fix $k \geqslant h$, let $0 \leqslant r \leqslant m_0$, and let $F_r$ be the first $r$ output bits. For every independent $k$-source pair and every admissible tuple of $t$ tamperings, both source-strong comparisons for $F_r$ have error at most

$$2^{(t+1)r}(\gamma + 2^{h-k}). \tag{2.1}$$

The statement remains true if a fixed binary-linear surjection of rank $r$ replaces coordinate truncation, with all actual tampered outputs projected through the same map.

*Proof.* Truncation and any fixed surjective linear projection preserve the initial $t$-non-malleability error by data processing, so work with the $r$-bit outputs. Let $\mathbf{T}$ denote the actual comparison tuple. Fix an atom $(z, \mathbf{v})$ of the $(t+1)r$ output bits and, for each numerical $x$ in the original left support, define

$$D_{z,\mathbf{v}}(x) = \Pr[Z = z, \mathbf{T} = \mathbf{v} \mid X = x] - 2^{-r} \Pr[\mathbf{T} = \mathbf{v} \mid X = x].$$

Write $b = k - h$. If the set $E = \{x : D_{z,\mathbf{v}}(x) > \gamma\}$ had probability at least $2^{-b}$, conditioning $X$ on $E$ would leave min-entropy at least $h$ (each conditional atom is at most $2^{-k}/\Pr[E]$). The independent source $Y$ would remain unchanged, and the original tampering maps would remain admissible on the smaller product support. On that source, the positive excess of this single joint atom would exceed $\gamma$, contrary to non-malleability. Thus $\Pr[E] < 2^{-b}$. Because $|D_{z,\mathbf{v}}(x)| \leqslant 1$,

$$\mathbb{E}_X[D_{z,\mathbf{v}}(X)]_+ \leqslant \gamma + 2^{-b}.$$

The conditional signed atom differences sum to zero. Hence the conditional total variation equals the sum of their positive parts. Summing over the $2^{(t+1)r}$ atoms proves the first comparison of (2.1). Repeating the argument after exchanging $X$ and $Y$ proves the second. No independence or entropy is assumed for the tampered images. □

*Remark* 2.6 (Recycling parameters and conditional entropy). For source-strong output extension, $C \geqslant 0$ counts the final tampered outputs, while the short seed is required to handle $R = 2C + 1$ auxiliary tamperings. This distinction is maintained throughout Section 4.2. For finite variables, write

$$\widetilde{H}_\infty(A \mid T) = -\log \sum_t \Pr[T = t] \max_a \Pr[A = a \mid T = t].$$

Revealing a variable with at most $2^b$ values costs at most $b$ in this average conditional min-entropy. Markov's inequality then gives pointwise entropy at least the average bound minus $\log(1/\xi)$, outside mass $\xi$. For subdistributions we use half the $\ell_1$ distance as well; discarded mass is charged explicitly in the centered recycling proof. Conditional source independence is used only on rectangular communication leaves or in an explicitly independent reference experiment.

## 2.2 Elementary probability, Fourier analysis, and rank

**Definition 2.7** (Sources and extraction)**.** For a finite random variable $X$, its min-entropy is $H_\infty(X) = -\log \max_x \Pr[X = x]$. A *flat $k$-source*, for integral $k$, is uniform on a set of exactly $2^k$ points. We use the statistical distance $\Delta(P, Q) = \frac{1}{2}\sum_z |P(z) - Q(z)|$ between finite distributions $P, Q$.

A strong seeded $(k, \varepsilon)$ extractor $E$ satisfies

$$\Delta((U_d, E(X, U_d)), U_{d+m}) \leqslant \varepsilon$$

for every source of min-entropy at least $k$, with $U_d$ independent of $X$. An ordinary two-source extractor uses independent $X, Y$; separate strength means the two guarantees retaining $X$ or retaining $Y$, separately. A Boolean two-source *disperser* at side threshold $k$ is nonconstant on every product of supports of sizes at least $2^k$.

**Lemma 2.8** (Flat decomposition and elementary conditioning)**.** Every distribution with point probabilities at most $1/K$, for an integer $K \geqslant 1$, is a convex combination of uniform distributions on $K$-element sets. Independent such decompositions produce a convex combination of product distributions. If an event $A$ depends only on $X$, then for every deterministic view $T$,

$$H_\infty(T(X) \mid A) \geqslant H_\infty(T(X)) + \log \Pr[A].$$

Separate events in independent sources preserve independence.

*Proof.* The polytope $\{p : \sum_x p_x = 1,\ 0 \leqslant p_x \leqslant 1/K\}$ has only the uniform distributions on $K$-element sets as extreme points. Indeed, if two coordinates are strictly between their bounds, shifting a sufficiently small amount between them expresses the point as a nontrivial midpoint. If only one coordinate were fractional, the equation $\sum p_x = 1$ and integrality of $K$ would make it a bound coordinate too. A finite-dimensional polytope is the convex hull of its extreme points. Tensor the two convex decompositions for the independence assertion. The conditioning bound follows from $\Pr[T(X) = z \mid A] \leqslant \Pr[T(X) = z]/\Pr[A]$. The joint conditional distribution under separate events factors directly. □

Integer floors in flat decompositions cost at most one entropy bit; every later use reserves a fixed positive linear entropy margin.

**Lemma 2.9** (Source-local disclosure)**.** If $H_\infty(X) \geqslant k$ and $L(X)$ takes at most $2^v$ values, then, except on labels of total probability at most $2^{-t}$,

$$H_\infty(X \mid L(X) = l) \geqslant k - v - t.$$

*Proof.* Discard labels of probability below $2^{-(v+t)}$. There are at most $2^v$ of them. On each remaining label, apply Lemma 2.8. □

**Lemma 2.9a** (Interactive-transcript disclosure)**.** *Let $X, Y$ be independent finite random variables. Let $T$ be the transcript of a finite deterministic binary communication protocol: at each internal node the speaker is determined by the preceding transcript, and the next bit is a function of that speaker's input and the preceding transcript. Suppose the left and right parties send at most $b_L$ and $b_R$ bits, respectively, on every execution. Every supported transcript leaf preserves independence of $X, Y$. For every $u > 0$, outside transcript probability at most $2^{1-u}$, simultaneously for every deterministic view $V(X)$ and $W(Y)$,*

$$H_\infty(V(X) \mid T = \tau) \geqslant H_\infty(V(X)) - b_L - u,$$
$$H_\infty(W(Y) \mid T = \tau) \geqslant H_\infty(W(Y)) - b_R - u.$$

*The same good leaves work for all views: conditioning on such a leaf increases the probability of any event depending only on $X$ by at most $2^{b_L+u}$, and of any event depending only on $Y$ by at most $2^{b_R+u}$. Moreover, with the average conditional min-entropy convention of Remark 2.6,*

$$\widetilde{H}_\infty(V(X) \mid T) \geqslant H_\infty(V(X)) - b_L, \qquad \widetilde{H}_\infty(W(Y) \mid T) \geqslant H_\infty(W(Y)) - b_R.$$

*Proof.* Each supported transcript has a rectangular preimage $A_\tau \times B_\tau$. Put $p_\tau = \Pr[X \in A_\tau]$ and $q_\tau = \Pr[Y \in B_\tau]$. Independence gives $\Pr[T = \tau] = p_\tau q_\tau$, and the conditional distribution on this leaf is the product of $X \mid A_\tau$ and $Y \mid B_\tau$.

Fix a numerical right input $y$. Pruning the protocol tree to that input leaves only left-message branching: each right message is determined by $y$ and the preceding transcript. The pruned binary tree has at most $b_L$ branching bits along a path, hence at most $2^{b_L}$ leaves. Averaging over $y$ gives

$$\sum_\tau q_\tau = \mathbb{E}_Y\big|\{\tau : Y \in B_\tau\}\big| \leqslant 2^{b_L}.$$

The symmetric argument gives $\sum_\tau p_\tau \leqslant 2^{b_R}$. Consequently,

$$\Pr_T[p_T < 2^{-b_L-u}] = \sum_{\tau: p_\tau < 2^{-b_L-u}} p_\tau q_\tau \leqslant 2^{-b_L-u} \sum_\tau q_\tau \leqslant 2^{-u}.$$

Similarly, $\Pr_T[q_T < 2^{-b_R-u}] \leqslant 2^{-u}$. On every leaf outside the union of these two exceptional sets, every left-local event $E$ satisfies

$$\Pr[E \mid T = \tau] = \Pr[E \mid X \in A_\tau] \leqslant \frac{\Pr[E]}{p_\tau} \leqslant 2^{b_L+u} \Pr[E].$$

This gives the left event and min-entropy bounds, simultaneously for all left-local views. The same argument proves the right bounds. No union bound over the number of views is used.

Finally, write $a_V = \max_v \Pr[V(X) = v]$. The same conditional-atom bound, now averaged over all supported leaves, gives

$$\sum_\tau \Pr[T = \tau] \max_v \Pr[V(X) = v \mid T = \tau] \leqslant \sum_\tau p_\tau q_\tau \frac{a_V}{p_\tau} \leqslant 2^{b_L} a_V.$$

Taking negative binary logarithms proves the average conditional min-entropy assertion on the left; the right is identical. The proof does not require either source to be flat or any view to be injective. □

**Lemma 2.10** (Conditional representative tables)**.** For any finite pair $(U, X)$, its distribution is a convex combination of distributions $(U, f(U))$, where the random choice of the deterministic table $f$ is independent of the subsequent $U$ and every component has the original $U$ marginal. This operation can be performed independently on two sides of a product distribution.

*Proof.* Independently for every $u$ of positive probability, draw $f(u)$ according to $X \mid U = u$, and then draw $U$ from its original distribution. Averaging over all tables reproduces the pair. Fill zero-probability entries arbitrarily. If $U$ is a function of $X$, every sampled representative is in its correct fiber. Independence of the two table selections proves the last assertion. □

**Lemma 2.11** (Fourier distance)**.** Let $P, Q$ be distributions on $\mathbb{F}_2^m$, and write $\widehat{P}(\lambda) = \mathbb{E}_{Z\sim P}(-1)^{\lambda\cdot Z}$. Then

$$\Delta(P, Q) \leqslant \frac{1}{2}\left(\sum_{\lambda\in\mathbb{F}_2^m} |\widehat{P}(\lambda) - \widehat{Q}(\lambda)|^2\right)^{1/2}.$$

In particular, if every nonzero character of $P$ has bias at most $\beta$, then $\Delta(P, U_m) \leqslant 2^{m/2}\beta/2$. If $(A, B)$ is compared with $(U_a, B)$, only characters with a nonzero $A$ coefficient contribute.

*Proof.* Parseval gives $2^m \sum_z (P(z) - Q(z))^2 = \sum_\lambda |\widehat{P}(\lambda) - \widehat{Q}(\lambda)|^2$. Apply Cauchy–Schwarz to $\frac{1}{2}\sum_z |P(z) - Q(z)|$. The assertions about uniform marginals follow by orthogonality. □

Statistical distance contracts under deterministic maps and stochastic kernels, and is convex under mixtures with common weights. These facts follow directly from the triangle inequality for the defining $\ell_1$ sum.

**Definition 2.12** (Separation and common features)**.** A field-valued kernel has separation length at most $R$ over $F$ if $H(x,y) = \sum_{i=1}^{R} a_i(x)b_i(y)$. For a Boolean kernel this is its truth-table rank over $\mathbb{F}_2$. A vector output has *common binary features of dimension* $R$ if there are fixed $u(x), v(y) \in \mathbb{F}_2^R$ such that every output character is a bilinear form in this same pair of maps.

Ranks are subadditive under addition and cannot increase under arbitrary separate precomposition. Separation lengths multiply under products. For $F = \mathbb{F}_{2^\ell}$, a separated $F$-product has absolute-trace rank at most $\ell$. More generally, trace-dual bases for a degree-$a$ extension $K/F$ give

$$\mathrm{Tr}_{K/F}(xy) = \sum_{j=1}^{a} x_j y_j.$$

Thus relative trace costs at most $a$ separated products. Concatenating all left and right factors of finitely many field-valued rows produces one common binary feature pair for the entire table, not merely independent rank bounds for its separate characters.

**Explicit fields.** We use fixed binary bases and deterministic finite-field construction in fixed characteristic, as in Shoup [57]. A relative extension degree that is required only to exceed a fixed constant can be chosen to be a power of two; a fixed-height quadratic tower then supplies $K/F$ and its relative trace. All such arithmetic is polynomial-time in the displayed binary field degree. Field constants are fixed independently of the sources.

## 2.3 Odd-power features and dense spans

**Lemma 2.13** (Rank under restriction)**.** Let $H : V \times W \to \mathbb{F}_2$ be bilinear, and let $V_0 \leqslant V$, $W_0 \leqslant W$. Then

$$\mathrm{rank}(H|_{V_0 \times W_0}) \geqslant \mathrm{rank}(H) - \mathrm{codim}\, V_0 - \mathrm{codim}\, W_0.$$

If $A \subseteq V$ and $B \subseteq W$ span $V_0$ and $W_0$, respectively, the matrix $[H(a,b)]_{a \in A, b \in B}$ has exactly the rank of $H|_{V_0 \times W_0}$.

*Proof.* Restriction of one argument deletes at most its codimension in independent rows or columns. This proves the inequality. For the second assertion, select spanning bases from $A$ and $B$. The corresponding submatrix represents the restricted bilinear form, and every other row or column is a linear combination of these. □

**Lemma 2.14** (Odd-degree additive-character bound)**.** *Reference.* [53, Lemma 1] (the characteristic-two odd-degree case of the additive Weil bound). Let $K = \mathbb{F}_{2^N}$ and let $P \in K[z]$ have positive odd degree $d$. Then

$$\left| \mathbb{E}_{z \sim U_K} (-1)^{\mathrm{Tr}_{K/\mathbb{F}_2} P(z)} \right| \leqslant (d-1) 2^{-N/2}.$$

This is the additive Weil bound in characteristic two; positive odd leading degree excludes the Artin–Schreier exceptional form. We use it at fixed degree and sufficiently large $N$; see [53, Lemma 1]. Linear nonconstant phases have bias zero.

**Lemma 2.15** (Small character bias forces a dense feature span)**.** Let $\Phi : \Omega \to \mathbb{F}_2^r$ and suppose every nonzero character of $\Phi(U_\Omega)$ has absolute bias at most $\beta$. If $A \subseteq \Omega$ has density at least $\alpha > 0$ and $\beta \leqslant \alpha/2$, then

$$\operatorname{codim}_{\mathbb{F}_2} \operatorname{span} \Phi(A) \leqslant \log(1/\alpha) + 1.$$

*Proof.* Write $V = \mathbb{F}_2^r$, and regard $V^* = \operatorname{Hom}_{\mathbb{F}_2}(V, \mathbb{F}_2)$ as the space of all binary-linear characters, using the standard dot product to identify $V^*$ with $V$. Let

$$S = \operatorname{span}_{\mathbb{F}_2}\{\Phi(\omega) : \omega \in A\} \leqslant V, \qquad c = \operatorname{codim}_{\mathbb{F}_2} S.$$

The annihilator of $S$ is

$$S^\perp = \{a \in V : a \cdot s = 0 \text{ for all } s \in S\}.$$

Elementary linear algebra gives $\dim S^\perp = c$, so $|S^\perp| = 2^c$. We first justify the character-orthogonality identity, for every $v \in V$,

$$\mathbf{1}[v \in S] = 2^{-c} \sum_{a \in S^\perp} (-1)^{a \cdot v}. \tag{2.2}$$

If $v \in S$, every summand is 1. If $v \notin S$, the double annihilator identity $(S^\perp)^\perp = S$ supplies an $a_0 \in S^\perp$ with $a_0 \cdot v = 1$. The terms indexed by $a$ and $a + a_0$ then have opposite signs and cancel, so the sum is zero.

Let $U$ be uniform on the finite set $\Omega$. Every $\omega \in A$ satisfies $\Phi(\omega) \in S$, even if $\Phi$ is noninjective. Consequently,

$$\Pr[\Phi(U) \in S] \geqslant \Pr[U \in A] = \frac{|A|}{|\Omega|} \geqslant \alpha. \tag{2.3}$$

Substitute $v = \Phi(U)$ into (2.2) and average over $U$. Since the zero character has expectation one, we obtain the *exact* identity

$$\begin{aligned} \Pr[\Phi(U) \in S] &= 2^{-c} \sum_{a \in S^\perp} \mathbb{E}_U (-1)^{a \cdot \Phi(U)} \\ &= 2^{-c} + 2^{-c} \sum_{a \in S^\perp \setminus \{0\}} \mathbb{E}_U (-1)^{a \cdot \Phi(U)}. \end{aligned} \tag{2.4}$$

The hypothesis bounds the absolute value of each nonzero-character expectation by $\beta$. There are exactly $2^c - 1$ such terms, so (2.3) and (2.4) imply

$$\alpha \leqslant 2^{-c} + (1 - 2^{-c})\beta = \beta + (1 - \beta)2^{-c}.$$

Because $\beta \leqslant \alpha/2$ and $\alpha \leqslant 1$, we have $\beta < 1$. Rearranging gives the slightly sharper bound

$$2^{-c} \geqslant \frac{\alpha - \beta}{1 - \beta} \geqslant \frac{\alpha}{2}.$$

Taking base-two logarithms now yields

$$c \leqslant \log_2(2/\alpha) = \log_2(1/\alpha) + 1,$$

as claimed. The proof only uses the density of $A$ in $\Omega$; it does not assume that $A$ is affine or that $\Phi$ is injective. □

**Lemma 2.16** (Whole-field odd-power features)**.** For $K = \mathbb{F}_{2^N}$ and a fixed integer $J \geqslant 1$, define

$$\Psi_J(z) = (z, z^3, \dots, z^{2J-1}) \in K^J.$$

Every nonzero binary character of $\Psi_J(U_K)$ has bias at most $\beta_J = (2J-2)2^{-N/2}$. For every fixed $0 < \tau < 1/2$ and sufficiently large $N$ (depending on $J, \tau$), each $A \subseteq K$ with $|A| \geqslant 2^{(1-\tau)N}$ satisfies

$$\operatorname{codim}_{\mathbb{F}_2} \operatorname{span} \Psi_J(A) \leqslant \tau N + 1 \quad \text{inside the } JN\text{-dimensional binary space } K^J.$$

*Proof.* We view $K^J$ as a binary vector space of dimension $JN$. By nondegeneracy of the absolute-trace pairing on $K$, every $\mathbb{F}_2$-linear functional $\ell : K \to \mathbb{F}_2$ is uniquely of the form $\ell(x) = \operatorname{Tr}_{K/\mathbb{F}_2}(ax)$ for some $a \in K$. Indeed, for $a \neq 0$ the functional $x \mapsto \operatorname{Tr}(ax)$ is nonzero, because multiplication by $a$ is a permutation of $K$ and the absolute trace is a nonzero binary-linear functional. The resulting injective map from $K$ to its binary dual is an isomorphism by equality of dimensions. Applying this fact coordinatewise, every binary character of $K^J$ has the unique form

$$\chi_{\mathbf{a}}(v_1, \dots, v_J) = (-1)^{\operatorname{Tr}_{K/\mathbb{F}_2}(\sum_{j=1}^{J} a_j v_j)}, \qquad \mathbf{a} = (a_1, \dots, a_J) \in K^J. \tag{2.5}$$

It is nonzero as a binary-linear character precisely when $\mathbf{a} \neq 0$. Its evaluation on $\Psi_J(z)$ is

$$\chi_{\mathbf{a}}(\Psi_J(z)) = (-1)^{\operatorname{Tr}_{K/\mathbb{F}_2} P_{\mathbf{a}}(z)}, \qquad P_{\mathbf{a}}(z) = \sum_{j=1}^{J} a_j z^{2j-1}.$$

Choose the largest index $j_0$ with $a_{j_0} \neq 0$. The exponents $1, 3, \dots, 2J-1$ are distinct, so $P_{\mathbf{a}}$ has positive odd degree $e = 2j_0 - 1 \leqslant 2J - 1$ and nonzero leading coefficient.

If $e = 1$, then $P_{\mathbf{a}}(z) = a_1 z$ with $a_1 \neq 0$. Its absolute trace is a nonzero binary-linear functional, which takes each of the values 0 and 1 on exactly half of $K$; therefore its character expectation is exactly zero. If $e \geqslant 3$, Lemma 2.14 gives

$$\left| \mathbb{E}_{z \sim U_K} (-1)^{\operatorname{Tr}_{K/\mathbb{F}_2} P_{\mathbf{a}}(z)} \right| \leqslant (e-1)2^{-N/2} \leqslant (2J-2)2^{-N/2}.$$

The odd leading degree is significant: a nonconstant polynomial of the form $R(z)^2 + R(z) + c$ has even degree, whereas such Artin–Schreier phases are the exceptional case for additive character sums in characteristic two. Combining the linear and higher-degree cases proves the first assertion, uniformly for every nonzero binary character of the entire $JN$-bit feature vector.

Next fix $0 < \tau < 1/2$. When $J = 1$, the preceding character bias is zero, and the following argument works for every $N$. For $J \geqslant 2$, since $J$ and $\tau$ are fixed, choose $N$ large enough that

$$(1/2 - \tau)N \geqslant 1 + \log_2(2J-2). \tag{2.6}$$

This is equivalent to

$$\beta_J = (2J-2)2^{-N/2} \leqslant 2^{-\tau N - 1}.$$

Let $A \subseteq K$ satisfy $|A| \geqslant 2^{(1-\tau)N}$. Its density in $K$ is at least

$$\frac{|A|}{|K|} \geqslant 2^{-\tau N} =: \alpha_0.$$

Take $\Omega = K$ and $\Phi = \Psi_J$, with a fixed binary-coordinate identification $K^J \cong \mathbb{F}_2^{JN}$. The character bound just proved says that every nonzero binary character of $\Phi(U_K)$ has bias at most $\beta_J \leqslant \alpha_0/2$. Lemma 2.15 therefore applies and gives

$$\operatorname{codim}_{\mathbb{F}_2} \operatorname{span}_{\mathbb{F}_2} \Psi_J(A) \leqslant \log_2(1/\alpha_0) + 1 = \tau N + 1.$$

All dimensions here are *binary* dimensions inside $K^J$; we do not take the $K$-linear span of $\Psi_J(A)$. The strict inequality $\tau < 1/2$ makes the condition (2.6) achievable for every fixed $J$. □

## 2.4 Approximate duality and its rank-sensitive form

**Lemma 2.17** (Set form of approximate duality)**.** *Reference.* [10, Lemma 7.9], using the polynomial Freiman–Ruzsa theorem [35]. There is an absolute $C$ such that the following holds. For finite $A, B \subseteq \mathbb{F}_2^R$ with $|\mathbb{E}_{A\times B}(-1)^{\langle a,b\rangle}| \geqslant \varepsilon$, and every fixed positive integer $t$, there is a constant subrectangle with relative density at least $2^{-q}$ on both sides, where

$$q \leqslant C\left[\frac{R}{t} + 2^t \log\frac{2}{\varepsilon} + (t+1)\log(R+2)\right]. \tag{2.7}$$

This is the characteristic-two consequence of Bhowmick–Dvir–Lovett [10, Lemma 7.9 and its proof], with doubling parameter $K = 2^{R/t}$, using the polynomial Freiman–Ruzsa theorem proved by Gowers–Green–Manners–Tao [35]. The proof of the cited estimate bounds the two relative densities separately and applies to unequal set sizes. Its polynomial factors become logarithmic terms as displayed above. Bounded $R$ and integer rounding are absorbed into $C$. We need its rank-sensitive indexed version, so repetitions are removed explicitly rather than charged by appending all raw input labels.

**Lemma 2.18** (Biased indexed matrix)**.** Let $M$ be a binary matrix indexed by nonempty sets $A, B$ of sizes at most $2^n$, of rank $r \geqslant 1$. Suppose

$$\left|\mathbb{E}_{A\times B}(-1)^{M(x,y)}\right| \geqslant \varepsilon.$$

For every fixed positive integer $L$, there is a monochromatic rectangle $A' \times B'$ whose relative densities on both sides are at least $2^{-q}$, with

$$q \leqslant C\frac{r}{L} + C_L\left(\log\frac{2}{\varepsilon} + \log(n+2) + \log(r+2)\right). \tag{2.8}$$

Here $C$ is absolute and $C_L$ depends only on $L$.

*Proof.* Factor $M(x,y) = \langle a_x, b_y\rangle$ in $\mathbb{F}_2^r$. Split the distribution of $a_X$, for uniform $X \in A$, into dyadic classes of its nonzero atom probabilities. Since those probabilities are at least $2^{-n}$, at most $n+1$ classes are needed. Do the same for $b_Y$.

The signed average is a sum of at most $(n+1)^2$ class-pair contributions. Some contribution has absolute value at least $\varepsilon/(n+1)^2$. Both class probabilities and the absolute conditional bias on that class pair are at least $\varepsilon/(n+1)^2$.

Within a class with $t$ distinct labels the conditional probabilities differ by at most a factor two. They are at most $2/t$, so the distribution is a convex combination of uniforms on $\max\{1, \lfloor t/2\rfloor\}$-element sets. These sizes are at least $t/3$ (singletons are harmless). Independent decompositions on the two sides produce one pair of flat label sets with absolute bias at least $\varepsilon/(n+1)^2$.

Apply (2.7) to that pair. If its monochromatic label subsets have relative densities $\rho$, each selected subset has conditional mass at least $\rho/6$ in its entire dyadic class: every label there has probability at least $1/(2t)$. Lifting to the original indices consequently gives relative masses at least

$$\frac{\varepsilon\rho}{6(n+1)^2}$$

on both sides. Insert $\varepsilon/(n+1)^2$ into (2.7) and include the logarithm of this last lifting factor. For fixed $L$, the result is (2.8) after changing constants. □

**Lemma 2.19** (Asymmetric rank-to-bias upgrade)**.** Let two input lengths $n_L, n_R$ lie between fixed positive constant multiples of $n$. Let a family of Boolean matrices have rank at most $An$. Suppose every member is nonconstant on all permitted subrectangles with side sizes at least $2^{a_0 n_L}$ and $2^{b_0 n_R}$, and permitted supports are closed under separate restrictions. For fixed $0 < a_0 < a_1 \leqslant 1$ and $0 < b_0 < b_1 \leqslant 1$, there is $\eta > 0$ such that every member has absolute bias at most $2^{-\eta n}$ on independent sources of entropies at least $a_1 n_L, b_1 n_R$ in that class.

*Proof.* Take independent flat components using Lemma 2.8. If the bias were at least $2^{-\eta n}$, Lemma 2.18 would give a constant subrectangle with logarithmic density loss at most

$$CAn/t + C_t(\eta n + O(\log(n+2))).$$

First choose fixed $t$ so the first term is smaller than one quarter of both available entropy gaps. Then choose $\eta$ so the coefficient of $n$ in the second term is also smaller than one quarter of both gaps. For large $n$ the logarithmic terms and one-bit floors fit the remaining slack. The resulting rectangle is above the two forbidden thresholds, a contradiction. Uniformity of the constants and convexity of absolute bias allow averaging the independent flat decompositions. □

**Corollary 2.20** (Linear-rank dispersion upgrade)**.** For fixed $A, \rho, \xi > 0$ with $\rho + \xi \leqslant 1$, there is $\eta > 0$ such that every Boolean $\rho n$-two-source disperser of rank at most $An$ is an ordinary extractor at side entropy $(\rho + \xi)n$ with error $2^{-\eta n}$. The exponent is uniform over all functions satisfying these two hypotheses.

*Proof.* Apply Lemma 2.19 with equal input lengths and equal entropy gaps, then use that one-bit statistical distance is half its character bias. The low-rank disperser-to-extractor principle originates with Ben-Sasson–Ron-Zewi [9, Lemma 2.17]. Its exponentially small-error consequence originally used the polynomial Freiman–Ruzsa conjecture, now proved by Gowers–Green–Manners–Tao [35]. See also Alrabiah–Goodman–Mosheiff–Ribeiro [2, Theorem 9] for this unconditional formulation. □

**Lemma 2.21** (Uniform tolerance of a low-rank transcript)**.** Fix constants $0 < \rho < \rho + \xi \leqslant 1$, $A, \kappa \geqslant 0$ and $\omega > 0$. Let $U(x,y) \in \mathbb{F}_2^u$, $V(x,y) \in \mathbb{F}_2^v$ be functions of two $N$-bit inputs. Suppose, uniformly for $\alpha \neq 0$ and $\beta$, the phase $\alpha \cdot U + \beta \cdot V$ has global binary rank at most $AN$ and restricted rank greater than $(\kappa + \omega)N$ on every rectangle of side entropy at least $\rho N$. Let $T(x,y) \in \mathbb{F}_2^z$ have every parity of global rank at most $\kappa N$. There is $\eta > 0$, depending only on the fixed constants, such that, for sufficiently large $N$, independent sources of entropy at least $(\rho + \xi)N$, and $u + v + z \leqslant \eta N$,

$$(U, V, T) \approx_{2^{-\eta N/2}} (U_u, V, T).$$

The ideal distribution retains the actual joint marginal of $(V, T)$.

*Proof.* For $\alpha \neq 0$, adding a transcript parity leaves restricted rank at least $\omega N > 1$ and global rank at most $(A + \kappa)N$. Corollary 2.20, after decreasing its exponent to absorb the bias/distance factor two, gives uniform bias $2^{-\eta N}$. Only characters with $\alpha \neq 0$ contribute to comparison with $(U_u, V, T)$. Lemma 2.11 gives distance at most $2^{(u+v+z)/2 - \eta N}/2 \leqslant 2^{-\eta N/2}$. No value of the jointly computed transcript is conditioned on. □

## 2.5 Published seeded primitives and entropy-efficient extraction

We state seeded results in the convention that the seed is *not* counted in the output length. Where a source counts it, we delete its fixed seed coordinates explicitly.

**Theorem 2.22** (Two strong seeded parameter regimes)**.** *Reference.* [36, Theorems 5.12 and 5.14 and Remark 5.15]; see also [12, Lemma 4.10]. There are absolute constants with the following properties. For an $n$-bit source of entropy $k$ and error $\zeta$, put $s = \log(1/\zeta)$.

(i) A strong seeded extractor outputs at least $k - 2s - O(1)$ bits with seed length $\log(n+2) + O(\log(k+2)\log((k+2)/\zeta))$.

(ii) Whenever $k \geqslant B(\log(n+2) + s + 1)$ for a sufficiently large absolute constant $B$, a strong seeded extractor outputs $\lfloor k/2 \rfloor$ bits with seed length $O(\log(n+2) + s + 1)$.

Both constructions are polynomial-time in $n + s$. An endpoint $k = n$ can be treated by appending one fixed input bit when invoking a statement formulated for $k < n$.

Part (i) is Theorem 5.14 and Remark 5.15 of GUV [36], after deleting the seed coordinates. Part (ii) follows from their fixed-fraction theorem and strongness remark; the displayed entropy lower bound absorbs the seed coordinates and all additive constants. It is also recorded in a convenient half-output form in [12, Lemma 4.10].

**Lemma 2.23** (Strong seeded extraction with near-total output)**.** There are absolute $A, B > 0$ such that, for every $n$, integer $k \leqslant n$, and $0 < \zeta \leqslant 1/4$, there is a strong seeded extractor with error at most $\zeta$, output length at least $\max\{0, k - A(s+1)\}$ up to an integer floor, and seed length at most

$$B\left[\log^2(n+2) + (s+1)\log\left(2 + \frac{n}{s+1}\right)\right], \qquad s = \log(1/\zeta). \tag{2.9}$$

It is deterministic polynomial-time in $n + s$. Ignored seed padding and output truncation preserve the conclusion.

*Proof.* If $s \leqslant \log(n+2)$, use part (i) of Theorem 2.22. Its seed length is $O(\log^2(n+2))$ and its entropy loss is $O(s+1)$. If the claimed output is nonpositive, use the empty output.

Suppose now $s > \log(n+2)$. Let $T = \lceil \log_2(n+2) \rceil + 2$, set the error of each extraction stage to $\zeta_0 = \zeta/(8T)$, and put

$$t = \lceil s + \log(8T) \rceil + 1.$$

Start with cumulative output length $M = 0$. At a stage define $h = k - M - t$. If $h < H_*$, stop, where $H_* = B_*(s + \log(n+2) + \log(8T) + 1)$ and $B_*$ is a sufficiently large absolute constant. Otherwise apply part (ii) with threshold $h$ and error $\zeta_0$, using a fresh independent seed, output $\lfloor h/2 \rfloor$ bits, and add that length to $M$.

All thresholds and lengths are deterministic functions of $n, k, \zeta$. Condition on any fixing of all previous seeds. The original source still has min-entropy $k$ before its previous output is disclosed. Since that output has exactly $M$ bits, Lemma 2.9 shows that, outside conditional probability at most $2^{-t}$, the source conditioned on its previous output has entropy at least $h$. Averaging over the previous seeds gives the same exception bound. The strong guarantee at the current stage therefore makes its output uniform independently of its seed and the actual preceding output/seed transcript, to error at most $\zeta_0 + 2^{-t}$.

Iterating this comparison proves that the complete output, jointly with all seeds, is within the sum of the stage errors of uniform. A formal induction compares the actual prefix/current-output distribution first with the actual prefix times a fresh uniform current output, then applies the previous induction hypothesis. Future seeds are independent and can be attached throughout. No replacement of the source distribution after an earlier hybrid is needed.

The quantity $h$ is replaced by $\lceil h/2 \rceil$ at each stage, so there are at most $T$ stages and in fact $O(\log(2+n/(s+1)))$ stages. Their total error is at most $\zeta$. At termination $k - M \leqslant t + H_* + O(1) = O(s+1)$, since $s > \log(n+2)$. Each seed has length $O(s+1)$ in this regime, so the total is $O((s+1)\log(2+n/(s+1)))$. This proves the unified bound. At most $O(\log n)$ polynomial-time seeded calls are made. □

*Remark* 2.24 (Why this seed length is sufficient). The additive-loss output proofs require that the generated seed fit within a sufficiently small linear number of bits when $s = \log(1/\varepsilon) \leqslant b_\delta n$. The function in (2.9) has this property because $b\log(2+1/b) \to 0$ as $b \to 0$. This explicit derivation from GUV avoids needing a stronger entropy-efficient seeded parameter statement. Its somewhat larger internal seed is harmless because that seed is retained in the final output.

## 2.6 Constant-seed strong condenser

**Theorem 2.25** (Constant-seed strong condenser)**.** *Reference.* [58, Definition 2.10 and Theorem 4.3]. For fixed $0 < \rho \leqslant 1$ and $0 < \beta, \varepsilon < 1$, there are a constant seed length $d$ and an efficient map

$$\mathrm{Cond} : \{0,1\}^n \times \{0,1\}^d \longrightarrow \{0,1\}^{m_0}, \qquad m_0 = \Omega(n),$$

such that, for every $X$ of min-entropy at least $\rho n$,

$$2^{-d} \sum_{i \in \{0,1\}^d} \min_{Z_i:\ H_\infty(Z_i) \geqslant (1-\beta)m_0} \Delta(\mathrm{Cond}(X,i), Z_i) \leqslant \varepsilon.$$

We use the strong-condenser convention of Zuckerman [58, Definition 2.10 and Theorem 4.3, attributed to Raz]. The maps need not be linear. For the small target deficiencies used below their output lengths may be taken at most $2n$ for sufficiently large $n$, by the support-size bound on a uniform input.

## 2.7 Uniform quantitative results for a growing number of rows

The uniformity in the next three statements is essential. Their constants are absolute; their algorithms do not require the entropy rate or the number of rows to be fixed.

**Lemma 2.26** (Quantitative approximate duality)**.** *Reference.* [8, Lemma 1.11], with the PFR theorem [35]. There is an absolute constant $C_{\mathrm{AD}}$ such that the following holds. If $A, B \subseteq \mathbb{F}_2^a$ are nonempty and

$$|\mathbb{E}_{x \sim U_A, y \sim U_B} (-1)^{x \cdot y}| \geqslant 2^{-v},$$

then, for every integer $u \geqslant 1$, there are nonempty $A' \subseteq A$ and $B' \subseteq B$ on which $x \cdot y$ is constant and both relative sizes are at least

$$2^{-C_{\mathrm{AD}}\{a/u + 2^u(v+1) + (u+1)\log(a+2)\}}. \tag{2.10}$$

This is Lemma 1.11 of Ben-Sasson–Lovett–Ron-Zewi [8], with its PFR hypothesis supplied by [35]. In that lemma take its parameter $K = 2^{a/u}$, so its parameter $t = a/\log K$ is exactly $u$. The negative logarithms of its two density bounds are at most an absolute multiple of $a/u + 2^u(v+1) + u\log(4a) + \log a$. This gives (2.10), with the small dimensions covered by increasing $C_{\mathrm{AD}}$. We use the full tradeoff, not only the special case $v \leqslant \sqrt{a}$. In particular, $u$ may grow with $n$.

**Theorem 2.27** (Uniform linear somewhere condenser)**.** *Reference.* [50, Theorem 31 and Algorithm 4], using [35]. There are absolute constants $A \geqslant 1$, $C_c \geqslant 1$, $c_c > 0$, and $\beta_0 > 0$ such that, in the parameter ranges used below, for $0 < \delta \leqslant 1/2$ there are uniformly explicit binary-linear maps

$$C_1, \dots, C_J : \mathbb{F}_2^n \to \mathbb{F}_2^m$$

with

$$J \leqslant C_c \delta^{-A}, \qquad C_c^{-1} n \delta^A \leqslant m \leqslant n, \tag{2.11}$$

whose tuple on every source of min-entropy at least $\delta n$ is $2^{-c_c m}$-close to a mixture having a designated row of min-entropy at least $(1/2 + \beta_0)m$. The polynomial exponents and the constants are independent of $\delta$.

This is the general-weak-source version of Li–Zhong's linear condenser, Theorem 31 and Algorithm 4 of [50]. Its $O(\log(1/\delta))$ stages have a constant branching factor and a constant length reduction per stage, giving the absolute polynomial bounds in (2.11). The general-weak-source analysis uses the proved PFR theorem. Enlarging $A, C_c$ accommodates integer rounding and the finitely many initial lengths. We use this statement only when $m$ grows as $n$ divided by a fixed power of $\log n$, so all stage and error estimates are in their large-length range. This is stronger than simply writing $O_\delta(1)$ rows and $\Theta_\delta(n)$ bits without tracking the rate dependence.

**Table conventions.** An elementary *somewhere-uniform* distribution on $T$ rows of $s$ bits has at least one exactly uniform row marginal; its other rows can be arbitrarily correlated with that row. A somewhere-uniform distribution is a positive mixture of elementary distributions, with the good index allowed to vary across components. An *affine somewhere-random* distribution is uniform on an affine subspace whose projection onto some row is all of $\mathbb{F}_2^s$. Neither convention assumes independence among rows.

**Theorem 2.28** (Affine somewhere-random extraction with growing row count)**.** *Reference.* [52, Lemma 3.6(iii)]; compare [50, Theorem 39]. There is an absolute integer $A_0 \geqslant 1$ such that, with

$$H(T) = (2T)^{A_0 \log(2T)}, \qquad a_s = s/H(T),$$

the following holds whenever $a_s \geqslant (2T)^4$. There is a uniformly explicit map on $T$ rows of $s$ bits which extracts at least $\lfloor a_s \rfloor$ bits, with error at most $2^{-a_s}$, from every uniform affine source whose projection onto at least one row is all of $\mathbb{F}_2^s$. Evaluation is polynomial-time in this parameter range.

We use Li's affine somewhere-random extractor in the quantitative form of Li–Zhong [52, Lemma 3.6(iii)]; see also [50, Theorem 39]. The original construction has $O(\log T)$ recursive stages and a loss $T^{O(\log T)}$, with absolute exponents. No internal independence of the rows is required. For $T = (\log n)^{O(1)}$, one has

$$H(T) = 2^{O((\log\log n)^2)} = n^{o(1)}. \tag{2.12}$$

A theorem only for fixed $T$, with unspecified $T$-dependent constants, would not be enough. No degree bound on this final affine extractor is needed in our application.

## 2.8 Weighted approximate duality for arbitrary common features

For the decreasing-rate two-source application the features are the raw input bits (and their source-local tampered copies). We state the analysis for arbitrary separate feature maps because the regularization theorem applies equally to nonlinear precompositions.

**Lemma 2.29** (Weighted rank-projection lemma)**.** Let $X, Y$ be independent flat sources on subsets of $\mathbb{F}_2^n$. Suppose a Boolean phase is affine-bilinear in separate feature variables of at most $P$ bits per side, and its bilinear part on the two current feature affine hulls has rank $r$. If its bias exceeds $2^{-H}$, then for every integer $u \geqslant 1$ there are nonempty raw subsets $A', B'$ on which the phase is constant, with both relative probabilities at least $2^{-g(r,H,u)}$, where

$$g(r, H, u) = C_w \left\{ \frac{r+2}{u} + 2^u(H+1) + (u+1)\log(n+P+2) \right\}. \tag{2.13}$$

The constant $C_w$ is absolute. The feature maps need not be injective, linear in the raw inputs, or uniformly distributed.

*Proof.* In affine coordinates on the two feature hulls write the phase as

$$f(x, y) = L(x) \cdot R(y) + a(x) + b(y) + c,$$

where the rank factors have $r$ coordinates. Here all functions are composed with their respective raw feature maps. The independent projections

$$Z = (L(X), a(X), 1), \qquad W = (R(Y), 1, b(Y) + c)$$

lie in $\mathbb{F}_2^{r+2}$ and satisfy $f(X, Y) = Z \cdot W$. Their positive atom probabilities are integer multiples of $1/|\operatorname{supp} X|$ and $1/|\operatorname{supp} Y|$, hence at least $2^{-n}$.

Set $\varepsilon = 2^{-H}$ and choose a sign so the signed correlation is larger than $\varepsilon$. Divide each projected support into at most $n+1$ dyadic probability buckets. If $p_i, q_j$ are the bucket masses and $c_{ij}$ their conditional signed correlations, then $\sum p_i q_j c_{ij} > \varepsilon$. The bucket pairs with $c_{ij} > \varepsilon/2$ have total weight greater than $\varepsilon/2$: otherwise the sum is at most $\varepsilon/2 + (1 - \varepsilon/2)\varepsilon/2 < \varepsilon$. Some such pair has

$$p_i q_j > \frac{\varepsilon}{2(n+1)^2}. \tag{2.14}$$

Each individual bucket mass is also at least this quantity.

Inside a bucket of size $N_1$, every conditional atom lies between $1/(2N_1)$ and $2/N_1$. Put $m_1 = \max\{1, \lfloor N_1/2 \rfloor\}$. These atoms are at most $1/m_1$, so Lemma 2.8 decomposes the conditional distribution into flat distributions on $m_1$ points, where $m_1 \geqslant N_1/3$. Do this independently on the right. Some pair of flat components has signed correlation above $\varepsilon/2$. Apply Lemma 2.26 to that pair in dimension $r+2$ with exponent $H+1$. If the monochromatic sets have relative flat density at least $2^{-b}$, then their conditional probability under their original buckets is at least $2^{-b}/6$ on either side. Taking their entire raw preimages and using (2.14) gives relative raw probability at least

$$\frac{\varepsilon}{12(n+1)^2} 2^{-C_{\mathrm{AD}}\{(r+2)/u + 2^u(H+2) + (u+1)\log(r+4)\}}.$$

Taking negative logarithms and using $r \leqslant P$ proves (2.13) after increasing one absolute constant. Pulling back the monochromatic sets preserves the phase identity. It does not require the projected sources to have been flat before bucket selection. □

## 2.9 A uniform shared-feature regularization theorem

Let

$$\mathcal{F} : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^D.$$

Assume fixed maps $u_L, u_R : \mathbb{F}_2^n \to \mathbb{F}_2^P$ represent every character by a bilinear form:

$$\lambda \cdot \mathcal{F}(x,y) = u_L(x)^{\mathsf{T}} M_\lambda u_R(y) \qquad (\lambda \in \mathbb{F}_2^D). \tag{2.15}$$

Padding features by zero coordinates permits one common length $P$. The same maps must work for *all* $\lambda$.

**Theorem 2.30** (Uniform positive affine regularization)**.** There is an absolute $C_0$ such that the following holds. For independent flat inputs, integers $1 \leqslant r_* \leqslant P$, $u \geqslant 1$, and real $H \geqslant 0, t \geqslant 1$, there is a finite partition into raw product rectangles. On every leaf, the conditional output is within $2^{D/2-H-1}$ of uniform on its exact affine hull. Outside total leaf mass at most $2^{1-t}$, each source loses at most

$$\mathcal{L} = C_0\Big[\frac{P}{u} + \frac{P}{r_*}\big(2^u(H+1) + (u+1)\log(n+P+2)\big) + D(r_*+2) + t\Big] \tag{2.16}$$

bits of min-entropy. The comparison is a positive mixture of uniform affine distributions. The partition is proof-only and need not be computed.

### 2.9.1 The progress rule

On a current rectangle $A \times B$, let $U, V$ be the affine hulls of $u_L(A), u_R(B)$ and let $W$ be the affine hull of $\mathcal{F}(A,B)$. If every character nonconstant on $W$ has bias at most $2^{-H}$, terminate. Otherwise select an offending character and let $r$ be the rank of its bilinear part on the directions of $U, V$.

When $r > r_*$, use Lemma 2.29 to obtain a monochromatic subrectangle $A' \times B'$. If $U', V'$ are its feature affine hulls, then

$$\operatorname{codim}_U U' + \operatorname{codim}_V V' \geqslant r. \tag{2.17}$$

Indeed, the four-point difference of a constant affine-bilinear phase vanishes. Thus its bilinear part vanishes on the two direction spaces of $U', V'$. Restriction to codimensions $c_1, c_2$ deletes at most $c_1 + c_2$ from matrix rank, proving (2.17). Query membership, on one raw input, in the preimage of a feature affine hull that has codimension at least $r/2$. Its yes probability is at least $2^{-g(r,H,u)}$. It is less than one since the queried feature hull is proper, and both outcomes remain raw product rectangles.

When $r \leqslant r_*$, write the character in current affine coordinates as $L(x) \cdot R(y) + a(x) + b(y) + c$. Reveal $(L(x), a(x))$, at most $r+1$ bits, then the right bit $L(x) \cdot R(y) + b(y) + c$. This makes the character constant, using at most $r_* + 2$ declared message bits. Because the character was nonconstant on $W$, every resulting nonempty output hull has dimension at least one smaller.

All choices can be fixed for each rectangle, making a deterministic finite tree. Every completed action strictly reduces the raw rectangle cardinality on each branch. At high rank both membership outcomes are proper; at low rank a phase-value cell cannot be the whole support of a nonconstant phase. The tree is finite even though no efficient bound on its depth is asserted.

### 2.9.2 One shared potential controls every high-rank character

The sum of the two current feature-affine-hull dimensions starts at most $2P$ and never increases. On high-rank yes answers it decreases by at least $r/2$. Therefore, pathwise,

$$\sum_{\text{high yes}} r_j \leqslant 4P, \qquad N_+ \leqslant 4P/r_*. \tag{2.18}$$

The output hull loses dimension on every low-rank action, so there are at most $D$ such actions. Their total declared message length is at most

$$B_{\mathrm{ex}} \leqslant D(r_* + 2). \tag{2.19}$$

Since high ranks are at least two, $r + 2 \leqslant 2r$ there. Equations (2.13) and (2.18) give a deterministic bound on affirmative information:

$$I_+ \leqslant C_1 \left[ \frac{P}{u} + \frac{P}{r_*} \bigl( 2^u (H+1) + (u+1) \log(n + P + 2) \bigr) \right]. \tag{2.20}$$

Different character factorizations alone would not prove this bound; it is the fixed feature pair (2.15) that makes the potential common to the whole path.

### 2.9.3 Two surprisal supermartingales

Let $I_-$ be the total information of high-rank no answers. At a query whose yes probability is $p$, the conditional multiplier of $2^{I_-/2 - N_+}$ has mean

$$(1-p)(1-p)^{-1/2} + p/2 = \sqrt{1-p} + p/2 \leqslant 1.$$

Other actions leave it unchanged. It is a nonnegative supermartingale starting at one, and the tree is finite. Markov's inequality implies

$$\Pr[I_- > 2N_+ + 2t] \leqslant 2^{-t}. \tag{2.21}$$

This controls arbitrarily many rejected queries without counting them.

Let $I_{\mathrm{ex}}$ be the information of all low-rank exact messages, and let $B$ be their accumulated declared bit lengths. At an $a$-bit message with positive outcome probabilities $p_z$, the conditional multiplier of $2^{I_{\mathrm{ex}} - B}$ has expectation

$$\sum_{z : p_z > 0} p_z \, (2^a p_z)^{-1} = \frac{|\{z : p_z > 0\}|}{2^a} \leqslant 1.$$

This process is unchanged at high-rank queries. Equations (2.19) and Markov's inequality give

$$\Pr[I_{\mathrm{ex}} > D(r_* + 2) + t] \leqslant 2^{-t}. \tag{2.22}$$

Neither estimate assumes independent or unbiased transcript bits.

### 2.9.4 Entropy and positive affine completion

For a leaf $A' \times B'$ within the initial flat rectangle $A \times B$, its probability is $(|A'|/|A|)(|B'|/|B|)$. Answer probabilities telescope, so its negative logarithm is exactly $I_+ + I_- + I_{\mathrm{ex}}$. Each individual source's entropy loss is nonnegative and at most this sum. Outside the union of (2.21) and (2.22), combine (2.20), $2N_+ \leqslant 8P/r_*$, and the message bound to obtain (2.16), with an absolute $C_0$.

At every terminal leaf all nonconstant characters of its affine hull $W$ have bias at most $2^{-H}$. In affine coordinates on $W$, Parseval and Cauchy–Schwarz imply

$$\Delta(\mathcal{F}(X,Y) \mid \mathrm{leaf}, U_W) \leqslant \tfrac{1}{2} \sqrt{2^{\dim W} - 1}\, 2^{-H} \leqslant 2^{D/2 - H - 1}.$$

Averaging these uniform distributions with the original leaf probabilities is a positive mixture, and proves Theorem 2.30. For bilinear raw maps, $u_L(x) = x, u_R(y) = y$ gives $P = n$. This is the special economy used by the inverse-logarithmic two-source construction.

# 3 Constant-rate extraction with small error

All three constructions in this section have linear output and error exponentially small in the original input length. The fixed-$C$ theorem includes every fixed number of separate tamperings. For $\delta n \leqslant k \leqslant n$, an output length $c_\delta n$ is in particular at least $c_\delta k$. Throughout the manuscript, for any field $F$ and $1 \leqslant D \leqslant s$, define

$$\sigma_D(z_1, \dots, z_s) := \sum_{\substack{I \subseteq \{1,\dots,s\} \\ |I|=D}} \prod_{i \in I} z_i, \qquad z_1, \dots, z_s \in F.$$

Thus $\sigma_D$ is the elementary symmetric polynomial of degree $D$; equivalently, it is the coefficient of $T^D$ in $\prod_{i=1}^{s}(1 + z_i T)$.

**Reading the construction boxes.** Each numbered construction box starts with the previously established primitives it uses, then separates *public setup* from the steps performed on an input. Public constants, field representations, row orders, projections, and subroutine parameters are fixed from the stated lengths, entropy thresholds, error target, and tampering count, never from a source support or a tampering map. A proof may later certify that a sufficiently small or large public constant works; evaluation does not search for that constant on the input. Except for a seeded subroutine's displayed seed argument, no external randomness is supplied. Good rows, subsources, conditional representative tables, and approximate-duality partitions are analysis objects, not hidden algorithmic steps. The boxes use a separate counter, so all existing theorem and equation numbers are retained.

**Evaluating the common field merger.** Every call to $\sigma_D(w_1, \dots, w_s)$ can be evaluated by the same fixed recurrence: initialize $e_0 = 1$ and $e_1 = \cdots = e_D = 0$; for $i = 1, \dots, s$, update $e_j \leftarrow e_j + w_i e_{j-1}$ in decreasing order $j = \min\{i, D\}, \dots, 1$; return $e_D$. The descending update order uses the previous polynomial coefficients, so after row $i$, $e_j$ is the coefficient of $T^j$ in $\prod_{b=1}^{i}(1 + w_b T)$, for $j \leqslant D$. This is an evaluation rule, not the proof's selection or forcing of good rows.

## 3.1 Ordinary two-source extraction

### 3.1.1 Ingredients and proofs: odd-power restricted rank and dense good rows

Fix

$$\tau = 2^{-10}. \tag{3.1}$$

For $K = \mathbb{F}_{2^M}$, the kernel $H_J(u, v) = \sum_{j=1}^{J} u^{2j-1} v^{2j-1}$ is the field inner product $H_J(u, v) = \langle \Psi_J(u), \Psi_J(v) \rangle_K$.

**Lemma 3.1** (Odd-power restricted rank)**.** For every fixed $J \geqslant 1$, sufficiently large $M$, and $\lambda \in K^\times$, put $h_\lambda(u, v) = \mathrm{Tr}_{K/\mathbb{F}_2}(\lambda H_J(u, v))$. Its global binary matrix rank is at most $JM$. On arbitrary $A, B \subseteq K$ with $|A|, |B| \geqslant 2^{(1-\tau)M}$,

$$\mathrm{rank}_2[h_\lambda]_{A \times B} \geqslant (J - 2\tau)M - 2. \tag{3.2}$$

The deficiency $\tau$ is independent of $J$.

*Proof.* The trace pairing $\mathrm{Tr}_{K/\mathbb{F}_2}(\lambda \sum_j p_j q_j)$ is nondegenerate on $K^J$, of binary dimension $JM$. By Lemma 2.16, the spans of $\Psi_J(A)$ and $\Psi_J(B)$ each have codimension at most $\tau M + 1$. Lemma 2.13 loses at most their sum and proves the lower bound. Expanding the $J$ separated field products and using trace-dual bases proves the global upper bound. □

**Lemma 3.2** (Designated-pair freshness)**.** Fix $J \geqslant 1$ and $0 \leqslant \kappa < J - 2\tau$. There is $\eta > 0$ such that, for sufficiently large $M$, any transcript $T : K^2 \to \mathbb{F}_2^v$ whose parities have rank at most $\kappa M$, any surjective binary-linear map $\pi : K \to \mathbb{F}_2^u$, and independent sources $U, V$ of entropy at least $(1 - \tau/2)M$ satisfy

$$(\pi H_J(U,V), T(U,V)) \approx_{2^{-\eta M/2}} (U_u, T(U,V)), \qquad u + v \leqslant \eta M. \tag{3.3}$$

The exponent is uniform in $T$, $\pi$, and the sources.

*Proof.* Each nonzero projected character is an absolute-trace character with nonzero coefficient. By Lemma 3.1, it has global rank at most $JM$ and restricted rank at least $(J - 2\tau)M - 2$. Choose $\omega = (J - 2\tau - \kappa)/2 > 0$ and increase the length threshold. Apply Lemma 2.21 with no current comparison coordinates, $\rho = 1 - \tau$, and $\xi = \tau/2$. This proves the assertion. □

### 3.1.2 Selecting subsources with many good rows

For a distribution $P$ on $\{0,1\}^{m_0}$ and $0 \leqslant h \leqslant m_0$, define

$$e_h(P) = \sum_z (P(z) - 2^{-h})_+.$$

This equals its distance to the closest $h$-source. Indeed, every such source must remove this excess mass; conversely, clipping to the cap $2^{-h}$ and distributing the removed mass into the unused capacity achieves this distance.

**Lemma 3.3** (Many good rows on an actual subsource)**.** Suppose deterministic rows $C_i(X) \in \{0,1\}^{m_0}$, $1 \leqslant i \leqslant r$, satisfy $\sum_i e_h(C_i(X)) \leqslant \varepsilon_c r$, where $\varepsilon_c < 1/8$. There is a distribution $X^*$ obtained by conditioning $X$ together with auxiliary randomness on an event of probability at least $(1 - 8\varepsilon_c)2^{-r}$, and an index set $I$ with $|I| \geqslant 7r/8$, such that

$$H_\infty(C_i(X^*)) \geqslant h - r - \log \frac{1}{1 - 8\varepsilon_c} \qquad (i \in I).$$

In particular $\operatorname{supp} X^* \subseteq \operatorname{supp} X$.

*Proof.* Let $p_i(z) = \mathbb{P}[C_i(X) = z]$. Conditional on $X = x$, sample acceptance indicators $A_i$ with

$$\mathbb{P}[A_i = 1 \mid X = x] = \min\{1, 2^{-h}/p_i(C_i(x))\}.$$

Only positive-probability values are sampled, so this ratio is defined. The indicators may be sampled independently conditional on $X$. Then $\mathbb{P}[A_i = 0] = e_h(C_i(X))$. For $N_{\mathrm{rej}} = \sum_i (1 - A_i)$, one has $\mathbb{E}N_{\mathrm{rej}} \leqslant \varepsilon_c r$; hence Markov's inequality gives

$$\mathbb{P}[N_{\mathrm{rej}} > r/8] \leqslant 8\varepsilon_c.$$

On the complementary event there are at least $7r/8$ acceptances. This is a statement about an integer count and needs no divisibility assumption on $r$. Among the at most $2^r$ exact acceptance

patterns, some pattern with at least $7r/8$ acceptances has probability $p \geqslant (1-8\varepsilon_c)2^{-r}$. Condition on this pattern, and let $I$ be its accepted indices. The resulting marginal of $X$ is $X^*$.

For $i \in I$, the conditioning event implies $A_i = 1$, and hence

$$\mathbb{P}[C_i(X^*) = z] \leqslant \frac{\mathbb{P}[C_i(X) = z, A_i = 1]}{p} = \frac{\min\{p_i(z), 2^{-h}\}}{p} \leqslant \frac{2^{-h}}{p}.$$

Taking logarithms proves the entropy bound. Conditioning cannot add points to the support of $X$. □

The auxiliary randomness creates no randomness in the extractor. This conditioning is used only to prove that both original input supports contain a product subsource on which the needed events occur. Applying the lemma separately to independent $X$ and $Y$ preserves independence of $X^*$ and $Y^*$.

### 3.1.3 Main theorem and construction interface

**Theorem 3.4** (Linear output and exponential error)**.** Fix $0 < \delta \leqslant 1$. There are positive constants $c_\delta, a_\delta, C_\delta$ and a deterministic polynomial-time family

$$\mathrm{Ext}_n : \{0,1\}^n \times \{0,1\}^n \longrightarrow \mathbb{F}_2^{m(n)}, \qquad m(n) \geqslant c_\delta n,$$

such that independent sources $X, Y$ with $H_\infty(X), H_\infty(Y) \geqslant \delta n$ satisfy

$$\Delta(\mathrm{Ext}_n(X,Y), U_{m(n)}) \leqslant 2^{-a_\delta n}.$$

For every $\beta \in \mathbb{F}_2^{m(n)} \setminus \{0\}$,

$$\mathrm{rank}_2\big((x,y) \mapsto \beta \cdot \mathrm{Ext}_n(x,y)\big) \leqslant C_\delta n.$$

In addition, there are a field $F_n = \mathbb{F}_{2^{\ell(n)}}$ with $\ell(n) = \Theta_\delta(n)$, an integer $R = O_\delta(1)$, explicit maps $G_L, G_R : \{0,1\}^n \to F_n^R$, and a surjective binary-linear map $\pi_n : F_n \to \mathbb{F}_2^{m(n)}$ such that

$$\mathrm{Ext}_n(x,y) = \pi_n(\langle G_L(x), G_R(y)\rangle_{F_n}). \tag{3.4}$$

Thus each encoding has $R\ell(n) = O_\delta(n)$ bits. A separately source-strong linear-output companion is proved in Corollary 3.9, with the same rank form.

This is an independent pair-input construction: it is not obtained by applying the sumset extractor to $x + y$. Enumerate the same $r$ strong-condenser seeds on both inputs, with $r \geqslant 4$ a power of two. Use only the corresponding left/right rows and delete the fixed last index, leaving $s = r - 1 = 2D - 1$ columns with $D = r/2$. At column $a$, interpret the $a$th row of each input as an element of one common field $K$ and use

$$H_{J_a}(u,v) = \sum_{j=1}^{J_a} u^{2j-1} v^{2j-1}, \qquad W_a = \mathrm{Tr}_{K/F}\, H_{J_a}(u,v), \qquad J_a = 2^{a-1}. \tag{3.5}$$

Return a fixed binary-linear projection of $Z = \sigma_D(W_1, \ldots, W_s)$. The common output field $F$ has $\Theta_\delta(n)$ bits. Source-dependent good rows, subsources, and conditional representative tables occur only in the analysis.

### 3.1.4 Complete deterministic evaluator: parameter order and fields

**Construction 3.1 Ordinary constant-rate two-source extractor**

**Ingredients from earlier parts.** The strong condenser of Theorem 2.25; the odd-power kernel and freshness bound of Lemmas 3.1–3.2; finite-field representations and relative traces from Section 2.2. The polynomial $\sigma_D$ is defined at the start of this section.

**Public parameters and fixed setup.** Fix $0 < \delta \leqslant 1$ and $\tau = 2^{-10}$. Instantiate the condenser at rate $\delta/2$, target deficiency $\tau/4$, and error $1/100$. Pad its seed by ignored bits so that its seed space has $r = 2^d \geqslant 4$ elements, in a fixed order. Let $m_0 = m_0(n)$ be its output length. Choose the remaining constants in the following order:

$$s = r - 1 = 2D - 1, \qquad D = r/2. \tag{3.6}$$

For $a = 1, \dots, s$, set

$$J_a = 2^{a-1}, \qquad \kappa_a = \sum_{b<a} J_b = J_a - 1. \tag{3.7}$$

Let $\eta_a > 0$ be the exponent supplied by Lemma 3.2 for $(J_a, \kappa_a)$, put $\eta = \min_a \eta_a$, and fix a power of two

$$L \geqslant \max\{2, 4s/\eta\}. \tag{3.8}$$

For each sufficiently large input length $n$, set

$$\ell = \lfloor m_0/L \rfloor, \qquad M = L\ell, \qquad K = \mathbb{F}_{2^M}, \quad F = \mathbb{F}_{2^\ell} \subseteq K. \tag{3.9}$$

Fix binary bases and a surjective binary-linear map $\pi_n : F \to \mathbb{F}_2^{m(n)}$, where $m(n) = \min\{\ell, \lfloor \nu_\delta n \rfloor\}$ and $\nu_\delta > 0$ is the fixed sufficiently small constant certified in Section 3.1.7. The choice is source independent.

**Input.** An ordered pair $(x, y) \in \{0,1\}^n \times \{0,1\}^n$.

**Evaluation steps.**

1. **Condense each input.** For every seed index $i \in [r]$, evaluate the condenser on $x$ and on $y$. Retain the first $M$ bits of each result and identify them with $U_i(x), V_i(y) \in K$.
2. **Use the fixed matched columns.** Keep the pairs $(U_a(x), V_a(y))$ for $a = 1, \dots, s$. Omit index $r$ on both sides; do not select columns based on their entropy.
3. **Evaluate every prescribed row kernel.** Compute

$$W_a(x, y) = \mathrm{Tr}_{K/F} \sum_{j=1}^{J_a} U_a(x)^{2j-1} V_a(y)^{2j-1} \quad (a \in [s]). \tag{3.10}$$

4. **Merge in the field and then project.** Compute

$$Z_n(x, y) = \sigma_D(W_1(x, y), \dots, W_s(x, y)), \tag{3.11}$$

and return $\pi_n(Z_n(x, y))$.

**Output.** $m(n) = \Omega_\delta(n)$ bits, with the guarantee of Theorem 3.4. For the finite initial range, use the one-bit completion $x_1 + y_1$ in Section 3.1.7.

**Not evaluated.** Acceptance patterns, high-entropy subsources, representative tables, and monochromatic rectangles.

### 3.1.5 Complete-prefix freshness on actual subsources

Start with independent sources of entropy at least $(\delta/2)n$. Apply Lemma 3.3 separately on the two sides, with $h = (1-\tau/4)m_0$. On the resulting product distribution $(X^*, Y^*)$, there are accepted sets $I_X, I_Y \subseteq [r]$ of sizes at least $7r/8$. Since $\varepsilon_c = 1/100$ gives $\log(1/(1-8\varepsilon_c)) < 1$, every $i \in I_X$ has, after truncation,

$$H_\infty(U_i(X^*)) \geqslant h - r - 1 - (m_0 - M) \geqslant (1-\tau/2)M, \tag{3.12}$$

and the analogous bound holds for $V_i(Y^*)$ when $i \in I_Y$, for sufficiently large $n$. The last inequality uses $m_0 - M < L$, where $L, r$ are constants, while $M = \Theta_\delta(n)$. A retained column $a$ is good when $a \in I_X \cap I_Y$. Therefore

$$\begin{aligned} |(I_X \cap I_Y) \cap [r-1]| &\geqslant |I_X| + |I_Y| - r - 1 \\ &\geqslant 3r/4 - 1 \geqslant r/2 = D, \end{aligned} \tag{3.13}$$

where the last inequality uses $r \geqslant 4$. Thus the fixed deletion preserves the required majority without choosing indices from the sources.

**Lemma 3.5** (Every good block is fresh relative to its complete prefix)**.** On this same selected product distribution, every good column $a$ satisfies

$$(W_a, W_{<a}) \approx_{2^{-\eta M/2}} (U_F, W_{<a}). \tag{3.14}$$

*Proof.* Apply Lemma 2.10 to the original left input conditional on $U_a$, and independently on the right conditional on $V_a$. Fixing the two representative tables preserves these good marginals exactly. Every earlier character is now a separate precomposition of its own row kernel and has rank at most $J_b M$; every prefix parity has rank at most $\kappa_a M$. On the designated row spaces, the current character plus a prefix parity consequently has restricted rank at least

$$(J_a - 2\tau)M - 2 - (J_a - 1)M = (1-2\tau)M - 2 > 1.$$

The relative trace is surjective. Its output and complete prefix have combined length $a\ell \leqslant s\ell \leqslant \eta M/4 \leqslant \eta_a M$. Lemma 3.2 applies, and averaging over the independent tables proves (3.14). The prefix itself is never fixed. Different good columns may use different table representations; all conclusions refer to the same original selected distribution. Neither the representative-table argument nor rank subtraction requires an off-diagonal pair of condenser indices. In particular, using the same deterministic seed index on both inputs does not compromise their independence. □

**Corollary 3.6** (Joint uniformity of selected good blocks)**.** For any set $I$ of good columns, $\Delta(W_I, U_F^{\otimes |I|}) \leqslant |I| 2^{-\eta M/2}$.

*Proof.* Order $I$ increasingly and project each complete-prefix estimate onto the preceding selected coordinates. Induction and contraction of statistical distance give the sum of the errors. □

### 3.1.6 Majority forcing on original product supports

**Lemma 3.7** (Forcing every field value)**.** Let $D$ be a power of two, let $s = 2D - 1$, and let $F$ have characteristic two. If any specified $D$ of $z_1, \ldots, z_s$ equal $\alpha$, then

$$\sigma_D(z_1, \ldots, z_s) = \alpha^D \tag{3.15}$$

for arbitrary values of the other coordinates. On Boolean inputs, $\sigma_D$ is strict majority.

*Proof.* The polynomial $\sigma_D$ is the coefficient of $t^D$ in $\prod_i(1+z_it)$. Let $H \subseteq [2D-1]$ be the specified set of $D$ indices whose entries equal $\alpha$, fixing the specified coordinates gives

$$\prod_i(1+z_it) = (1+\alpha t)^D \prod_{i\notin H}(1+z_it) = (1+\alpha^D t^D)\prod_{i\notin H}(1+z_it).$$

The remaining product has degree at most $D-1$, proving (3.15). On a Boolean input of weight $w < 2D$, the value is $\binom{w}{D}$ modulo two. The coefficient of $t^D$ in $(1+t)^w$ is the binary digit of $w$ at the power $D$, so it equals one precisely when $w \geqslant D$. □

**Proposition 3.8** (Full image on every large original rectangle)**.** For sufficiently large $n$, $Z_n(A\times B) = F$ whenever $A, B \subseteq \{0,1\}^n$ have sizes at least $2^{(\delta/2)n}$.

*Proof.* Start from $U_A, U_B$ and choose $D$ good columns on the actual product subsource above. For every $\alpha \in F$ their simultaneous value $(\alpha,\dots,\alpha)$ has probability at least $2^{-D\ell} - D2^{-\eta M/2} > 0$, by (3.8). Lemma 3.7 forces $Z_n = \alpha^D$ there, regardless of the other columns. Since $D$ is a power of two, $\alpha \mapsto \alpha^D$ permutes $F$. Every witness is an actual point of $A \times B$. □

### 3.1.7 Original-input rank and the final extraction step

A trace-dual $F$-basis of $K$ expands each separated $K$-product into at most $L = [K:F]$ separated $F$-products. Thus, including all condenser preprocessing, column $a$ has separation length

$$R_a \leqslant LJ_a. \tag{3.16}$$

Expanding the fixed polynomial $\sigma_D$ gives, pointwise on the original $n$-bit input domains,

$$Z_n(x,y) = \sum_{t=1}^{R} A_t(x)B_t(y), \qquad R \leqslant \sum_{|I|=D}\prod_{a\in I} LJ_a \leqslant \prod_{a=1}^{s}(1+LJ_a) = O_\delta(1). \tag{3.17}$$

Every absolute-trace character therefore has binary rank at most $R\ell = O_\delta(n)$. Its nonconstancy on original rectangles follows from Proposition 3.8, not from a claim that a restricted-rank lower bound survives arbitrary condenser preprocessing.

Corollary 2.20, with original entropy gap $\delta n/2$, gives a common $\theta_\delta > 0$ such that every nonzero character has bias at most $2^{-\theta_\delta n}$ on sources of entropy $\delta n$, after decreasing the exponent and increasing the length threshold. Choose a fixed positive rational $\nu_\delta \leqslant \theta_\delta$ and set

$$m(n) = \min\{\ell, \lfloor \nu_\delta n \rfloor\}, \tag{3.18}$$

$$\mathrm{Ext}_n(x,y) = \pi_n(Z_n(x,y)). \tag{3.19}$$

where $\pi_n$ is any fixed surjective binary-linear map of this rank. By Lemma 2.11,

$$\Delta(\mathrm{Ext}_n(X,Y), U_{m(n)}) \leqslant \tfrac{1}{2}2^{m(n)/2-\theta_\delta n} \leqslant 2^{-\theta_\delta n/2}.$$

The same character identity preserves the original-input rank bound. Taking $G_L = (A_t)_t$, $G_R = (B_t)_t$ proves (3.4). The algorithm uses a constant number of fixed powers and field operations and an explicit condenser; it never finds the proof-side subsources.

For the finitely many lengths below a fixed cutoff $N_\delta$, use one bit $x_1 + y_1$. Its error, including separately conditioned error, is at most $1/2$, and its rank is at most two. It has the field-pairing representation $(x_1, 1)\cdot(1, y_1)$ over $\mathbb{F}_{2^n}$, followed by a coordinate projection. Pad all encodings to one constant length and decrease the output and error constants to at most $1/N_\delta$. This completes Theorem 3.4 at every positive length.

### 3.1.8 Source-strong linear-output companion

**Corollary 3.9** (Separate source strength at constant entropy rate)**.** For every fixed $\delta > 0$ there are $c'_\delta, a'_\delta > 0$ and an explicit deterministic polynomial-time family $\mathrm{Ext}^{\mathrm{ss}}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{r_n}$, $r_n \geqslant c'_\delta n$, such that for independent sources of min-entropy at least $\delta n$,

$$\Delta((\mathrm{Ext}^{\mathrm{ss}}_n(X,Y),X),(U_{r_n},X)), \quad \Delta((\mathrm{Ext}^{\mathrm{ss}}_n(X,Y),Y),(U_{r_n},Y)) \leqslant 2^{-a'_\delta n}.$$

Its output is a fixed linear projection of the field-valued inner-product evaluator constructed above, and every nonzero output parity still has binary truth-table rank $O_\delta(n)$.

**Construction 3.2 Source-strong ordinary linear-output companion**

**Ingredients from earlier parts.** The ordinary extractor of Theorem 3.4 (Construction 3.1) and entropy-slack strongification, Lemma 2.5 with zero comparisons.

**Public parameters and fixed setup.** Fix $\delta > 0$ and put $h := \delta n/4$. Instantiate the ordinary family at rate $\delta/4$, equivalently at component entropy threshold $h$; denote its output and error constants by $c_0, a_0 > 0$. Fix $0 < b_\delta < \min\{c_0/2, a_0/4, \delta/16\}$ and set $r_n = \lfloor b_\delta n \rfloor$ in the sufficiently large range.

**Input.** $(x,y) \in \{0,1\}^n \times \{0,1\}^n$.

**Evaluation steps.**

1. Evaluate the rate-$\delta/4$ ordinary extractor on $(x,y)$.
2. Return its first $r_n$ output bits. In the finite initial range, return the base family's one-bit completion $x_1 + y_1$.

**Output.** The companion $\mathrm{Ext}^{\mathrm{ss}}_n(x,y)$ of Corollary 3.9; the *same* function is strong in either source separately. No additional seeded-extractor call or conditioning step is performed.

**Proof.** For all sufficiently large $n$, let the base construction at entropy $h = \delta n/4$ have at least $c_0 n$ output bits and error at most $2^{-a_0 n}$. Choose $0 < b_\delta < \min\{c_0/2, a_0/4, \delta/16\}$. For input entropy $k \geqslant \delta n$, the slack $k - h$ is at least $3\delta n/4$. Lemma 2.5 with $t = 0$ bounds both source-strong errors by

$$2^{r_n}\left(2^{-a_0 n} + 2^{-3\delta n/4}\right) \leqslant 2^{-\Omega_\delta(n)}.$$

Thus, for some fixed integer $N_\delta \geqslant 1$ and $a_* > 0$, the error is at most $2^{-a_* n}$ and $r_n \geqslant b_\delta n/2$ for $n \geqslant N_\delta$. Below $N_\delta$, the one-bit completion has both strong errors at most $1/2$. Taking

$$c'_\delta = \min\{b_\delta/2, 1/N_\delta\}, \qquad a'_\delta = \min\{a_*, 1/N_\delta\}$$

proves the displayed bounds for every $n \geqslant 1$. A fixed output projection preserves the rank and separated-field representation, proving the final assertions. □

## 3.2 Sumset extraction

### 3.2.1 Ingredients and their proofs: linear strong condenser and moment rank

We recall the two sumset-specific cited theorems and the character-sum lemma; the rank-sensitive approximate-duality upgrade is already proved in the preliminaries. The reduction after these inputs is given below.

**Theorem 3.10** (Linear somewhere condenser)**.** *Reference.* [50, Theorem 31 and Lemma 27], with PFR supplied by [35]. For each fixed $\rho > 0$, there are fixed $t \geqslant 1$, $\beta \in (0, 1/4]$, $c, c' > 0$, and explicit binary-linear maps

$$P_1, \dots, P_t : \mathbb{F}_2^n \to \mathbb{F}_2^m, \qquad m = \Theta_\rho(n),$$

such that, for every $H_\infty(X) \geqslant \rho n$, the tuple $(P_i X)_{i \leqslant t}$ is within $2^{-c'n}$ of a positive mixture of distributions having some coordinate of min-entropy at least $(1/2 + \beta)m$.

This is the fixed-rate consequence of the general-weak-source construction in Theorem 31 of Li–Zhong [50], obtained from the basic rate-boosting Lemma 27 in Section 4 and constant-depth iteration. The polynomial Freiman–Ruzsa input is supplied by [35]. Padding or truncation by a fixed number of bits is handled below. The coordinates are jointly binary-linear functions of the original input, not nonlinear source condensers.

**Theorem 3.11** (The constant-seed curve merger)**.** *Reference.* [33] and [32, Theorem 18]. Let $\mathbb{E} = \mathbb{F}_q$, choose distinct $\gamma_1, \dots, \gamma_t \in \mathbb{E}$, and let $c_i(U)$ be their Lagrange basis polynomials of degree at most $t - 1$. Define, for any number $v$ of $\mathbb{E}$ coordinates,

$$\mathrm{CM}((z_i)_{i \leqslant t}, u) = \sum_{i=1}^{t} c_i(u) z_i. \tag{3.20}$$

If $(Z_i)_{i \leqslant t}$ is a mixture with one uniform coordinate in $\mathbb{E}^v$, and $U$ is independent uniform on $\mathbb{E}$, then for $0 < \vartheta, \varepsilon < 1$ and

$$q \geqslant \max\{t, (2t/\varepsilon)^{1/\vartheta}\},$$

$\mathrm{CM}(Z, U)$ is $\varepsilon$-close to a distribution of min-entropy at least $(1 - \vartheta) v \log q$.

This is the Dvir–Wigderson curve construction [33] with Dvir–Kopparty–Saraf–Sudan's Theorem 18 [32]. Crucially the lower bound on $q$ is independent of $v$. Each fixed-seed map is $\mathbb{E}$-linear in the entire table, and commutes with every $\mathbb{E}$-linear map on its coordinate vectors. We prove the high-entropy rather than uniform-row consequence instead of assuming it.

The odd-degree additive-character estimate is Lemma 2.14.

We use the uniform linear-rank disperser upgrade from Corollary 2.20. For one-bit characters, decrease its error exponent if necessary to absorb the factor two between bias and statistical distance.

Compatible finite fields and their operations can be constructed in deterministic polynomial time in fixed characteristic [57]. All extension ratios used by the final evaluator are fixed constants.

For a field $F$, a function $B(x, y)$ has separation length at most $r$ if $B(x, y) = \sum_{j=1}^{r} a_j(x) b_j(y)$. Separate precomposition cannot increase this length, sums add it, and products multiply it. If $F = \mathbb{F}_{2^\ell}$, each absolute trace character of such a function has binary rank at most $r\ell$, by a trace-dual basis for $F/\mathbb{F}_2$. Tracing a separated product from an extension $K/F$ of degree $a$ uses at most $a$ separated $F$ products.

### 3.2.2 From a linear somewhere condenser to many good linear views

For a finite alphabet $\Omega$ and $h \leqslant \log |\Omega|$, let $\mathcal{K}_h$ be the distributions with every atom at most $2^{-h}$, and define

$$e_h(P) = \sum_{z \in \Omega} (P(z) - 2^{-h})_+.$$

**Lemma 3.12** (Distance to an entropy cap)**.** $e_h(P) = \min_{Q \in \mathcal{K}_h} \Delta(P, Q)$. Any subdistribution capped by $2^{-h}$ can be extended to a probability distribution with that cap.

*Proof.* Every comparison distribution with atom cap $2^{-h}$ must remove the displayed excess mass. Capping $P$ at that value achieves the removal, and its missing mass fits in the remaining capacity since $|\Omega|2^{-h} \geqslant 1$. Redistribute the mass there. □

**Lemma 3.13** (Lifting a capped comparison through a function)**.** Let $Z$ take values in $\Omega$, and let $A : \Omega \to \Omega'$ be onto. If $AZ$ is $\varepsilon$-close to a distribution in $\mathcal{K}_h$, then $Z$ is also $\varepsilon$-close to a distribution in $\mathcal{K}_h$.

*Proof.* Lift a capped comparison distribution $Q$ of $AZ$ by the conditional distribution of $Z$ on each nonempty actual fiber of $A$ (arbitrarily on empty fibers). Each lifted atom is at most its image mass $Q(w) \leqslant 2^{-h}$, and summing total variation over fibers preserves the distance. □

**Lemma 3.14** (A proof-only linear projection)**.** For $Z \in \mathbb{F}_q^v$ of min-entropy at least $h$ and an integer $r \leqslant v$, there is an $\mathbb{F}_q$-linear map $A : \mathbb{F}_q^v \to \mathbb{F}_q^r$ with

$$\Delta(AZ, U_{\mathbb{F}_q^r}) \leqslant \tfrac{1}{2}\sqrt{q^r 2^{-h}}.$$

If this bound is less than $1/2$, the selected map is onto.

*Proof.* For a uniformly random $r \times v$ linear matrix $A$,

$$\mathbb{E}_A \operatorname{cp}(AZ) = q^{-r} + (1 - q^{-r}) \operatorname{cp}(Z).$$

Cauchy–Schwarz and the collision-to-distance bound show that the average distance to $U_{\mathbb{F}_q^r}$ is at most $\frac{1}{2}\sqrt{q^r \operatorname{cp}(Z)} \leqslant \frac{1}{2}\sqrt{q^r 2^{-h}}$. Choose a matrix attaining this average bound. A nonsurjective matrix has output supported on at most $q^{r-1}$ values, at distance $\geqslant 1 - 1/q \geqslant 1/2$ from uniform. □

**Lemma 3.15** (High-entropy inputs to the curve merger)**.** Suppose $(Z_1, \ldots, Z_t) \in (\mathbb{F}_q^v)^t$ is a positive mixture having some row of min-entropy at least $h$. Fix $0 < \tau < 1/2$ and choose

$$r = \left\lfloor \frac{h - 2\log(1/\tau)}{\log q} \right\rfloor \geqslant 1.$$

Under the field-size condition in Theorem 3.11, $\mathrm{CM}(Z, U_q)$ is $(\tau + \varepsilon)$-close to $\mathcal{K}_{(1-\vartheta)r \log q}$.

*Proof.* Consider one mixture component with a high-entropy row $Z_g$. Lemma 3.14 supplies an onto $A$ such that $AZ_g$ is within $\tau/2$ of uniform. Replace this marginal by uniform while retaining the conditional distributions of all other projected rows. The projected table changes by at most $\tau$, becomes somewhere random, and the curve merger brings its output within $\tau + \varepsilon$ of the stated entropy cap. Since

$$A \,\mathrm{CM}(Z, u) = \mathrm{CM}((AZ_i)_i, u),$$

Lemma 3.13 transfers this capped comparison back to the unprojected output. The projection may depend on the component: it is proof-only. Averaging over components works because the entropy-cap class is convex and the target entropy is common. □

**Lemma 3.16** (Disclosing a constant seed)**.** Let $S$ be uniform on a set of size $Q$, with arbitrary joint distribution with $Z$, and suppose $e_h(Z) \leqslant \varepsilon$. Then

$$\frac{1}{Q}\sum_s e_{h-\log Q}(Z \mid S = s) \leqslant \varepsilon.$$

*Proof.* Put $p_{s,z} = \Pr[S = s, Z = z]$ and $c = 2^{-h}$. By uniformity of $S$, the left side is $\sum_{s,z}(p_{s,z} - c)_+$. For nonnegative $a_s$, $\sum_s (a_s - c)_+ \leqslant (\sum_s a_s - c)_+$, so

$$\sum_{s,z}(p_{s,z} - c)_+ \leqslant \sum_z \left(\sum_s p_{s,z} - c\right)_+ = e_h(Z).$$

Use Lemma 3.12 to identify excess mass with distance. □

**Theorem 3.17** (Constant-seed linear strong condenser above half)**.** Fix $\rho > 0$ and a constant $\varepsilon_* > 0$. There are constants $\beta > 0$, a power of two $Q \geqslant 16$, and explicit binary-linear maps

$$L_u : \mathbb{F}_2^n \to \mathbb{F}_2^M, \quad u \in \mathbb{F}_Q, \qquad M = \Theta_\rho(n),$$

such that every $H_\infty(X) \geqslant \rho n$ satisfies

$$\frac{1}{Q}\sum_{u \in \mathbb{F}_Q} \min_{Z_u : H_\infty(Z_u) \geqslant (1/2+\beta/2)M} \Delta(L_u X, Z_u) \leqslant \varepsilon_*. \tag{3.21}$$

All constants may also depend on $\varepsilon_*$. The maps are linear for each fixed seed, not just low-degree polynomials.

**Construction 3.3 Constant-seed linear strong condenser**

**Ingredients from earlier parts.** The linear somewhere condenser of Theorem 3.10 and the curve merger of Theorem 3.11. Lemmas 3.15 and 3.16 provide the high-entropy and retained-seed analysis, not extra evaluation steps.

**Public parameters and fixed setup.** Given a fixed rate $\rho > 0$ and constant error $\varepsilon_* > 0$, instantiate Theorem 3.10 to obtain $P_1, \dots, P_t$, row length $m$, and $0 < \beta \leqslant 1/4$. Put $\vartheta = \beta/4$ and $\varepsilon = \min\{\varepsilon_*/4, 1/8\}$. Fix a power of two $Q = 2^s \geqslant \max\{16, t, (2t/\varepsilon)^{1/\vartheta}\}$, distinct $\gamma_1, \dots, \gamma_t \in \mathbb{F}_Q$, and their Lagrange basis polynomials $c_i(U)$. Put $M = s\lceil m/s \rceil$.

**Input.** $z \in \mathbb{F}_2^n$ and a numerical seed $u \in \mathbb{F}_Q$.

**Evaluation steps.**

1. Evaluate $P_i(z)$ for all $i \in [t]$ and append zeros to give each row exactly $M$ bits. Parse each as a vector of $M/s$ elements of $\mathbb{F}_Q$.
2. Compute the coordinatewise field sum $L_u(z) = \sum_{i=1}^t c_i(u) P_i(z)$ and return its $M$ binary coordinates.

**Output.** One $M$-bit linear view. To obtain the full deterministic table, run the same procedure at every $u \in \mathbb{F}_Q$ in the fixed field order; no seed is sampled in that use. The guarantee is Theorem 3.17.

**Not evaluated.** The source-dependent linear projection in Lemma 3.14; it is not part of $L_u$.

*Proof.* Use Theorem 3.10, with its $t, m, \beta$ and decrease $\beta$ if necessary to ensure $\beta \leqslant 1/4$. Choose $\vartheta = \beta/4$ and $\tau = \varepsilon = \min\{\varepsilon_*/4, 1/8\}$. Choose a fixed power of two $Q = 2^s \geqslant 16$ satisfying

$$Q \geqslant \max\{t, (2t/\varepsilon)^{1/\vartheta}\}.$$

Pad each $P_i$ by fewer than $s$ zero bits to length $M = s\lceil m/s \rceil$, and regard it as a vector in $\mathbb{F}_Q^{M/s}$. Define the actual maps by

$$L_u(z) = \sum_{i=1}^t c_i(u) P_i(z), \qquad u \in \mathbb{F}_Q, \tag{3.22}$$

with the padding understood. Multiplication by a fixed element of $\mathbb{F}_Q$ is binary-linear, so all these maps are binary-linear.

The input comparison table has row entropy $h = (1/2 + \beta)m$. Lemma 3.15 makes the output with an independent uniform seed close to entropy

$$H = (1 - \vartheta)s \left\lfloor \frac{h - 2\log(1/\tau)}{s} \right\rfloor.$$

The total error is at most $2^{-c'n} + \tau + \varepsilon \leqslant \varepsilon_*$ for sufficiently large $n$. Apply Lemma 3.16: the average fixed-seed distance to entropy $H - s$ has the same bound. Finally,

$$H - s \geqslant (1 - \beta/4)(1/2 + \beta)m - O_{\rho,\varepsilon_*}(1) \geqslant (1/2 + \beta/2)M$$

for sufficiently large $n$. The last inequality has a positive linear margin, since $(1 - \beta/4)(1/2 + \beta) - (1/2 + \beta/2) = 3\beta/8 - \beta^2/4 > 0$. This proves (3.21). □

*Remark* 3.18 (Which error is required). The seed space $\mathbb{F}_Q$ is fixed for constant $\rho, \varepsilon_*$. This theorem does not claim exponentially small strong-condenser error with constant seed length. Only the small constant error in (3.21) will be used in a dispersion proof.

### 3.2.3 One actual product subsource with a common majority

**Lemma 3.19** (Capped-pattern selection)**.** Suppose $Q$ marginal views $L_iX$ satisfy $Q^{-1}\sum_i e_h(L_iX) \leqslant \varepsilon_*$, with $\varepsilon_* \leqslant 1/32$. There is an actual source-local conditional distribution $X^*$, supported in $\operatorname{supp} X$, and a set $G_X$ of at least $15Q/16$ indices such that

$$H_\infty(L_iX^*) \geqslant h - Q - 1 \qquad (i \in G_X).$$

The selected conditioning event, allowing private auxiliary coins, has probability at least $2^{-Q-1}$.

*Proof.* Given a row value $v$, independently accept index $i$ with probability $\min\{1, 2^{-h}/p_i(v)\}$, where $p_i$ is the distribution of $L_iX$. The expected number of rejections is at most $Q\varepsilon_*$. Markov's inequality gives probability at least $1 - 16\varepsilon_* \geqslant 1/2$ of accepting $15Q/16$ indices. Among at most $2^Q$ acceptance patterns, one such pattern has probability $p \geqslant 2^{-Q-1}$. Condition on it. At any accepted index,

$$\Pr[L_iX = v \mid \text{pattern}] \leqslant \frac{\Pr[L_iX = v,\ i \text{ accepted}]}{p} \leqslant 2^{-h}/p \leqslant 2^{-h+Q+1}.$$

The pattern is source-local, and conditioning adds no support points. □

Apply this lemma separately to independent $X, Y$. The private coins and selection events are on their own sides, so $X^*, Y^*$ remain independent. At least $7Q/8$ indices belong to $G_X \cap G_Y$. Delete one fixed index from the algorithm's list and write

$$T = Q - 1 = 2D - 1, \qquad D = Q/2. \tag{3.23}$$

Since $Q \geqslant 16$, at least $7Q/8 - 1 \geqslant D$ retained columns are good for both sources. The same map is used on each summand at a given column; there is no unknown pairing of different left and right row indices.

Later we pad the maps from length $M$ to $N = a\lceil M/a \rceil$, where $a$ is a fixed constant. With $h = (1/2 + \beta/2)M$, the good viewed sources then have, for sufficiently large $n$, min-entropy at least

$$\alpha_1 N, \qquad \alpha_1 = 1/2 + \beta/4. \tag{3.24}$$

Indeed their entropy is at least $h - Q - 1$, and padding adds fewer than $a$ bits. All these losses are constants after the rate has been fixed. We need only one positive-weight product distribution in the support of each original product source; no statistical replacement by this distribution is made.

### 3.2.4 The moment–trace-code restricted-rank bound

Write $K = \mathbb{F}_{2^N}$, let $h \geqslant 3$ and $d = 2^h - 1$ be fixed, and assume $N > 2h$ is sufficiently large. All traces in this subsubsection are absolute.

**Proposition 3.20** (Moment–trace-code restricted rank)**.** Let $p \geqslant 1$, $2p \leqslant 2^{h-2}$, $\lambda \in K^\times$, $A, B \subseteq K$, $|A| \geqslant p$, and $|B| \geqslant 2(d-1)2^{N/2}$. Then

$$\operatorname{rank}_2[\operatorname{Tr}(\lambda(x+y)^d)]_{A\times B} \geqslant p\log|A| - p\log p + \log|B| - N - 1. \tag{3.25}$$

The full binary matrix has rank at most $(d+1)N = 2^h N$.

*Proof. The trace-code restriction loss.* Let $\mathcal{C}_d$ be the binary space of functions

$$f(z) = \varepsilon + \operatorname{Tr}\left(\sum_{\substack{1\leqslant j\leqslant d\\ j \text{ odd}}} a_j z^j\right), \qquad \varepsilon \in \mathbb{F}_2,\ a_j \in K.$$

Every polynomial trace of degree at most $d$ belongs to this space: write each positive exponent as $2^v j$ with $j$ odd and use $\operatorname{Tr}(az^{2^v j}) = \operatorname{Tr}(a^{2^{N-v}} z^j)$. For a nonzero coefficient tuple, the largest nonvanishing odd term has positive odd degree at most $d$. The odd-degree character bound (Lemma 2.14) makes its absolute bias strictly less than one for sufficiently large $N$. Hence the coefficients (including $\varepsilon$) are unique, and every nonconstant member of $\mathcal{C}_d$ has bias at most $(d-1)2^{-N/2}$.

Let $r$ be the dimension of the kernel of restriction $\mathcal{C}_d \to \mathbb{F}_2^B$. This kernel does not contain the constant function one, and all its members vanish on $B$. Orthogonality gives

$$\frac{|B|}{2^N} \leqslant 2^{-r} \sum_{f \text{ in the kernel}} \mathbb{E}_z(-1)^{f(z)} \leqslant 2^{-r} + (d-1)2^{-N/2}.$$

The lower bound on $|B|$ therefore implies

$$r \leqslant N - \log|B| + 1. \tag{3.26}$$

*Moments in the unrestricted row span.* By Lucas's theorem, all binomial coefficients in $(x+y)^d$ are one modulo two. For each odd $j > d/2$, the coefficient of $y^j$ in the unique odd-exponent trace representation of $\operatorname{Tr}(\lambda(x+y)^d)$ is exactly $\lambda x^{d-j}$: no higher even exponent can reduce to $j$, since $2j > d$. Taking $j = d - 2v$ for $0 \leqslant v < 2^{h-2}$, then dividing by $\lambda$ and applying inverse Frobenius, recovers the moment vector

$$(1, x, x^2, \ldots, x^{2^{h-2}-1})$$

by binary-linear operations on the unrestricted row-function space. For two distinct $p$-element subsets of $A$, equality of the sums of these vectors would give a nontrivial binary relation among at most $2p$ distinct Vandermonde columns. The first $2p$ coordinates rule out such a relation. Thus the full-domain row span has dimension at least

$$\log\binom{|A|}{p} \geqslant p\log|A| - p\log p.$$

*Restriction and global rank.* All row functions belong to $\mathcal{C}_d$. Restricting the right argument to $B$ loses at most the kernel dimension in (3.26), yielding (3.25). The global upper bound follows either by expanding $(x+y)^d$ into $d+1$ separated $K$-products or by the single-product realization (3.29) and a trace-dual basis. □

**Corollary 3.21** (Arbitrary mask margin at a fixed rate)**.** Fix $1/2 < \alpha_0 < \alpha_1 < 1$ and $\kappa \geqslant 0$. Choose

$$p = \left\lceil \frac{\kappa + 4}{\alpha_0} \right\rceil, \qquad h \geqslant 3, \quad 2^{h-2} \geqslant 2p.$$

There is $\theta > 0$, uniform over $N$, $\lambda \in K^\times$ and every Boolean kernel $T : K^2 \to \mathbb{F}_2$ of global rank at most $\kappa N$, such that for independent $U, V$ of entropy at least $\alpha_1 N$,

$$\left| \mathbb{E}(-1)^{\mathrm{Tr}(\lambda(U+V)^{2^h-1}) + T(U,V)} \right| \leqslant 2^{-\theta N} \tag{3.27}$$

for sufficiently large $N$.

*Proof.* On rectangles of side entropy at least $\alpha_0 N$, the size condition on $B$ holds for large $N$, because $\alpha_0 > 1/2$. Proposition 3.20 gives rank at least

$$(p\alpha_0 + \alpha_0 - 1)N - p \log p - 1 > (\kappa + 2)N.$$

Adding $T$ leaves rank greater than one, so the phase is a disperser at that threshold. Its global rank is at most $(2^h + \kappa)N$. Corollary 2.20, with entropy increment $\alpha_1 - \alpha_0$, gives the bias estimate after decreasing its exponent. The uniformity of the cited lemma gives uniformity over all masks and nonzero coefficients. The permitted entropy rates are fixed before the requested margin $\kappa$; only $p, h, \theta$ depend on it. □

### 3.2.5 Theorem

All logarithms are base two. Entropy is binary min-entropy. Statistical distance is $\Delta(P, Q) = \frac{1}{2}\sum_z |P(z) - Q(z)|$. The original input length is $n$; a sumset extractor sees only $z = x + y \in \mathbb{F}_2^n$.

**Theorem 3.22** (Constant-rate sumset extraction)**.** For every fixed $0 < \delta \leqslant 1$, there are positive constants $c_\delta, e_\delta, C_\delta$ such that, for all sufficiently large $n$, a uniformly polynomial-time computable map

$$\mathrm{Ext}_n : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^{m_n}, \qquad m_n \geqslant c_\delta n,$$

satisfies

$$\Delta(\mathrm{Ext}_n(X + Y), U_{m_n}) \leqslant 2^{-e_\delta n}$$

for every independent pair with $H_\infty(X), H_\infty(Y) \geqslant \delta n$. For every nonzero output functional $\lambda$, the matrix

$$[\lambda \cdot \mathrm{Ext}_n(x + y)]_{x,y \in \mathbb{F}_2^n}$$

has rank over $\mathbb{F}_2$ at most $C_\delta n$. More precisely, the output is a binary-linear projection of a field-valued expression having a constant number of separated products over a field of binary dimension $\Theta_\delta(n)$. Thus explicit separated encodings of total binary length $O_\delta(n)$ are available for its lifted characters.

Here "uniformly polynomial-time" is for each fixed rate: the constants in the algorithm are fixed independently of the source distributions and of $n$. The construction is not a search for successful coefficients.

### 3.2.6 Complete sum-only construction

The evaluator has the form

$$\mathrm{Ext}_n(z) = \pi\,\sigma_D\left(\mathrm{Tr}_{K/F}((L_1 z)^{2^{h_1}-1}), \ldots, \mathrm{Tr}_{K/F}((L_{2D-1} z)^{2^{h_{2D-1}}-1})\right). \tag{3.28}$$

Here $L_i : \mathbb{F}_2^n \to K$ are fixed binary-linear maps, $D$ is a fixed power of two, $K = \mathbb{F}_{2^N}$, $F = \mathbb{F}_{2^\ell}$ with $N = a\ell = \Theta_\delta(n)$ and fixed $a$, and $\sigma_D$ is the elementary symmetric polynomial of degree $D$. The moment exponents $h_i$ increase according to a fixed rank hierarchy. The map $\pi$ is a fixed binary-linear output projection.

**One large-field product per block.** For the rank analysis only, write $z = x + y$ and put $d_i = 2^{h_i} - 1$. Take an extension $E_i/K$ of degree $d_i + 1$, with trace-dual $K$-bases $(e_{i,j})_{0\leqslant j\leqslant d_i}$ and $(e^*_{i,j})_{0\leqslant j\leqslant d_i}$. Define the source-local encodings

$$A_i(x) = \sum_{j=0}^{d_i} (L_i x)^j e_{i,j}, \qquad B_i(y) = \sum_{j=0}^{d_i} (L_i y)^{d_i - j} e^*_{i,j}.$$

Since every binomial coefficient of $(x+y)^{2^{h_i}-1}$ is odd, trace duality gives the exact identity

$$\mathrm{Tr}_{K/F}\big((L_i(x+y))^{d_i}\big) = \mathrm{Tr}_{E_i/F}\big(A_i(x)B_i(y)\big). \tag{3.29}$$

The field degree $[E_i : F] = a2^{h_i}$ is constant once the entropy rate and column have been fixed. This is an algebraic representation, not a change to the sum-only evaluator. In particular, its binary characters have global rank at most $2^{h_i}N$.

The new input-side step is an explicit linear strong condenser with a constant seed space and output rate above one half. A small constant error is sufficient: it is used to select one actual product subsource for a support argument, and is not carried into the final statistical error. All seeds of this condenser are enumerated by the evaluator.

### 3.2.7 Parameter schedule, native fields and actual row algorithm

**Construction 3.4 Constant-rate sumset extractor**

**Ingredients from earlier parts.** The linear strong condenser of Theorem 3.17 (Construction 3.3); the moment-mask margin of Corollary 3.21; the polynomial $\sigma_D$ and its forcing identity, Lemma 3.7; relative traces from Section 2.2.

**Public parameters and fixed setup.** Fix $\delta > 0$. Instantiate the condenser at $\rho = \delta/2$ and $\varepsilon_* = 2^{-12}$, obtaining $Q$ linear views of length $M = M(n)$ and the constant $\beta > 0$. Enumerate the seeds once, omit the fixed last seed, and call the remaining maps $L_1, \dots, L_T$, where $T = Q - 1 = 2D - 1$ and $D = Q/2$. Put $\alpha_0 = 1/2 + \beta/8$ and $\alpha_1 = 1/2 + \beta/4$. In increasing column order, define

$$\kappa_i = \sum_{j<i} 2^{h_j}, \qquad p_i = \left\lceil \frac{\kappa_i + 4}{\alpha_0} \right\rceil, \tag{3.30}$$

and take the smallest $h_i \geqslant 3$ with $2^{h_i - 2} \geqslant 2p_i$. Let $\theta_i > 0$ be the resulting exponent in Corollary 3.21, and put $\theta = \min_i \theta_i$. Fix an integer

$$a \geqslant \max\{2, 4T/\theta\}. \tag{3.31}$$

Set $\ell = \lceil M/a \rceil$, $N = a\ell$, and fix compatible fields $F = \mathbb{F}_{2^\ell} \subseteq K = \mathbb{F}_{2^N}$ and binary bases. Fix a surjective binary-linear output projection $\pi : F \to \mathbb{F}_2^{m_n}$ with $m_n = \min\{\ell, \lfloor \zeta_\delta n \rfloor\}$, for the fixed bias constant $\zeta_\delta$ certified in the proof of Theorem 3.22.

**Input.** Only $z \in \mathbb{F}_2^n$, interpreted in the theorem as $X + Y$.

**Evaluation steps.**

1. Evaluate $L_i(z)$ for every $i \in [T]$, append $N - M$ zero bits, and identify the result with an element of $K$.
2. For every retained column, compute
$$W_i(z) = \mathrm{Tr}_{K/F}\big((L_i z)^{2^{h_i - 1}}\big) \in F. \tag{3.32}$$
3. Compute $Z_n(z) = \sigma_D(W_1(z), \dots, W_T(z))$ in $F$, and return $\pi(Z_n(z))$.

**Output.** $m_n = \Omega_\delta(n)$ bits with the guarantee of Theorem 3.22. All preprocessing maps are binary-linear; no decomposition of $z$ as $x + y$ is supplied to the evaluator.

**Not evaluated.** Good-column selection, capped patterns, representative tables, and the extension fields $E_i$ in the separated-product proof.

The coefficient field $\mathbb{F}_Q$ used for the linear maps need not be a subfield of $K$: it specifies binary-linear preprocessing. The trace fields $F \subseteq K$ have the displayed compatible representation.

For every output character of $W_j(x + y)$, trace transitivity and Proposition 3.20 give the global binary rank bound $2^{h_j} N$. Hence every parity of the full earlier prefix

$$\Pi_i = (W_1(X + Y), \dots, W_{i-1}(X + Y))$$

has rank at most $\kappa_i N$. This bound is independent of the later choice of $a$: the row output is shortened, but the native field core still acts on $N$ bits. All asymptotic estimates in the local theorem hold uniformly for these field degrees.

### 3.2.8 Freshness on the actual product source

We first give the elementary representative-table device used to transfer a local rank estimate without fixing a joint prefix.

**Lemma 3.23** (Separate representative tables)**.** Let $X, Y$ be independent and let $U = L(X)$, $V = R(Y)$. There are independent random deterministic maps $\mathsf{T}, \mathsf{S}$, independent of $U, V$, such that

$$(\mathsf{T}(U), \mathsf{S}(V)) \overset{\text{distribution}}{=} (X, Y), \qquad L(\mathsf{T}(u)) = u, \quad R(\mathsf{S}(v)) = v$$

on the supported values. Separate precomposition by each fixed map pair cannot increase the binary rank of any raw kernel.

*Proof.* Sample each table entry $\mathsf{T}(u)$ from the conditional distribution $X \mid U = u$, before independently drawing $U$; then $\mathsf{T}(U)$ reproduces $X$, with $L(\mathsf{T}(u)) = u$ on its support. Repeat independently on the right. For fixed tables, separate precomposition selects or repeats matrix rows and columns, so it cannot increase binary rank. □

**Lemma 3.24** (Complete-prefix freshness)**.** Let $X^*, Y^*$ be an actual independent product distribution for which the $i$th viewed marginals have entropy at least $\alpha_1 N$. Then the rows (3.32) satisfy

$$\Delta((W_i(X^* + Y^*), \Pi_i), (U_F, \Pi_i)) \leqslant \frac{1}{2}\, 2^{i\ell/2 - \theta_i N} \leqslant 2^{-\theta N/2} \tag{3.33}$$

for sufficiently large $n$. No hypothesis is imposed on the entropy of the earlier rows.

*Proof.* Fix a nonzero character of the current field output and any binary character of the prefix. In the native field, their combined phase is

$$\mathrm{Tr}_{K/\mathbb{F}_2}(\lambda(L_i x + L_i y)^{2^{h_i}-1}) + T_{\mathrm{pre}}(x, y), \qquad \lambda \in F^\times \subset K^\times.$$

The raw mask has rank at most $\kappa_i N$. Use Lemma 3.23 for the current two views. For every fixed representative-table pair it is still a mask of rank at most $\kappa_i N$ on $K^2$, while the two viewed distributions remain independent and retain their entropies. Corollary 3.21 bounds the phase bias by $2^{-\theta_i N}$. Average over the table pairs; this is the same original joint output/prefix distribution.

Compare that distribution with a uniform current field value independent of the actual prefix. Fourier coefficients with zero current character cancel exactly. At most $(2^\ell - 1)2^{(i-1)\ell}$ coefficients remain. Parseval and Cauchy–Schwarz give the first bound in (3.33). Since $a \geqslant 4T/\theta$, one has $i\ell/2 \leqslant \theta N/8$, which implies the second, weaker bound. We have not conditioned the two sources on $\Pi_i$; prefix freshness was proved by mixed characters on the independent source pair. □

### 3.2.9 Majority forcing and the final error bound

The forcing identity from Lemma 3.7 applies to the same $\sigma_D$ over the sumset output field $F$.

**Proposition 3.25** (Full output support on every lower-rate rectangle)**.** For the fixed construction above, put

$$Z_n(z) = \sigma_D(W_1(z), \ldots, W_{2D-1}(z)) \in F.$$

For any $A, B \subseteq \mathbb{F}_2^n$ with $|A|, |B| \geqslant 2^{(\delta/2)n}$, one has $Z_n(A + B) = F$ for sufficiently large $n$.

*Proof.* Apply the strong linear condenser to $U_A$ and $U_B$. Use Lemma 3.19 separately and obtain one actual product distribution $X^*, Y^*$ supported in $A \times B$, with at least $D$ common good retained columns. Fix a set $H$ of $D$ such indices in their algorithmic order. Their viewed entropies are at least $\alpha_1 N$ by (3.24), so Lemma 3.24 applies to every index. Project each earlier prefix to the earlier selected indices and use successive replacements. This gives

$$\Delta((W_i(X^* + Y^*))_{i\in H}, U_F^{\otimes D}) \leqslant D2^{-\theta N/2}.$$

The elementary induction here first replaces the current coordinate against the actual preceding selected marginal, then replaces that preceding marginal by uniform using the previous induction bound. It does not require independence of bad or future columns.

By (3.31), $D\ell \leqslant \theta N/4$. Hence, for large $n$,

$$D2^{-\theta N/2} < 2^{-D\ell} = |F|^{-D}.$$

For every $u \in F$, the event that all selected columns equal $u$ therefore has positive probability under the actual product distribution. Lemma 3.7 makes the merged value $u^D$ on that event. The map $u \mapsto u^D$ is a Frobenius automorphism of $F$, so every field value occurs. All these pairs belong to $A \times B$. □

**Lemma 3.26** (Rank of the actual sum-only composition)**.** Each $W_i(x + y)$ has separation length at most $a2^{h_i}$ over $F$. Consequently $Z_n(x + y)$ has separation length at most

$$R_* := \sum_{\substack{I\subseteq[2D-1]\\|I|=D}} \prod_{i\in I} a2^{h_i}, \tag{3.34}$$

a constant depending only on the fixed rate. Every absolute trace character of $Z_n(x + y)$ has binary rank at most $R_*\ell = O_\delta(n)$.

*Proof.* Apply the exact field-product identity (3.29) to $W_i(x + y)$. Trace duality over $E_i/F$ yields at most $[E_i : F] = a2^{h_i}$ separated $F$-products. A fixed product of rows multiplies their separation lengths, and sums add them; expanding $\sigma_D$ therefore gives (3.34). Finally, each separated $F$-product contributes at most $\ell$ binary rank after absolute trace. All identities hold for the actual unconditioned sum-only evaluator. □

*Proof of Theorem 3.22.* For every nonzero $\lambda \in F$, the Boolean function

$$f_\lambda(x, y) = \mathrm{Tr}_{F/\mathbb{F}_2}(\lambda Z_n(x + y))$$

is nonconstant on every rectangle of side entropy $(\delta/2)n$, by Proposition 3.25. Lemma 3.26 gives a uniform $O_\delta(n)$ rank bound. Corollary 2.20, now on the original $n$-bit summands with entropy increment $\delta/2$, yields some $\zeta_\delta > 0$ such that every such character has bias at most $2^{-\zeta_\delta n}$ on all independent entropy-$\delta n$ inputs. Take any fixed surjective binary-linear projection to

$$m_n = \min\{\ell, \lfloor\zeta_\delta n\rfloor\} = \Omega_\delta(n)$$

bits. Nonzero output parities are nonzero absolute-trace characters of $F$. Thus

$$\Delta(\pi Z_n(X + Y), U_{m_n}) \leqslant \tfrac{1}{2}\sqrt{2^{m_n} - 1}\, 2^{-\zeta_\delta n} \leqslant \tfrac{1}{2}\, 2^{-\zeta_\delta n/2}.$$

This gives the error and output claims and retains the rank bound.

The linear maps, powers, fields, and symmetric polynomial are fixed independently of sources. Finite-field construction and arithmetic are polynomial-time for fixed characteristic; the number of views, moment orders, field-extension ratio, and merger degree are fixed constants. The symmetric polynomial can also be evaluated by its elementary coefficient recurrence. No good-column selection, hash projection used in Lemma 3.15, acceptance pattern, representative table, or approximate-duality rectangle is computed by the evaluator. All length roundings cost only constants at the relevant stage and are absorbed for sufficiently large $n$. This proves uniform explicitness. □

### 3.2.10 Ingredients and proofs for the one-sided non-malleable sumset seed

**Lemma 3.27** (Rank and Fourier conventions)**.** Separate precomposition cannot increase the binary rank of a function matrix. Ranks are subadditive. If $F = \mathbb{F}_{2^\ell}$ and $H(x, y) = \sum_{j=1}^{r} a_j(x)b_j(y)$ over $F$, then every absolute-trace character of $H$ has binary rank at most $r\ell$. A fixed-degree relative trace costs at most its degree in separated products.

If $(Z, T) \in \mathbb{F}_2^q \times \mathbb{F}_2^v$ and every mixed character with nonzero coefficient on $Z$ has bias at most $\omega$, then

$$\Delta((Z, T), (U_q, T)) \leqslant \tfrac{1}{2}\sqrt{(2^q - 1)2^v}\,\omega.$$

For a pair of $q$-bit outputs this applies with $v = q$.

*Proof.* The rank assertions are the common separation and trace-duality facts of Section 2.2; the distance bound is Lemma 2.11 with only honest-bearing characters retained. □

**Lemma 3.28** (Actual conditional representatives)**.** For a deterministic map $U = T(X)$, one can write the joint distribution of $(X, U)$ as a mixture of $(R(U), U)$ with $R$ a random deterministic table independent of $U$, and $T(R(u)) = u$ for all positive-probability $u$. Separate such representations for independent sources preserve their independence and do not increase any separately lifted matrix rank after fixing the tables.

*Proof.* Apply Lemma 2.10. Its representatives lie in their actual fibers, and separate precomposition cannot increase matrix rank. □

### 3.2.11 Moment secants against one-sided tampering

Fix $h \geqslant 3$, $d = 2^h - 1$, $K = \mathbb{F}_{2^N}$, and $N > 2h$, taking $N$ sufficiently large below. Put $L = 2^{h-2}$.

**Lemma 3.29** (The trace-code restriction kernel)**.** Let

$$\mathcal{C}_d = \left\{ \varepsilon + \mathrm{Tr}_{K/\mathbb{F}_2} \sum_{\substack{1 \leqslant j \leqslant d \\ j \text{ odd}}} c_j y^j \right\}.$$

Its displayed coefficients are unique, and every nonconstant member has bias at most $(d-1)2^{-N/2}$. If $B \subseteq K$ has size at least $2(d-1)2^{N/2}$, then

$$\dim \ker(\mathcal{C}_d \to \mathbb{F}_2^B) \leqslant N - \log|B| + 1.$$

*Proof.* These are precisely the unique-coefficient and restriction-kernel claims established in the first part of the proof of Proposition 3.20; equation (3.26) gives the displayed dimension bound. That argument uses only the right set $B$ and applies unchanged to secant row functions. □

**Lemma 3.30** (A forest of moment secants)**.** Let $A$ be a finite subset of a field $K$ of characteristic two and $f : A \to K$ satisfy $f(x) \neq x$. For nonzero $a, b \in K$, put

$$v_L(x) = (1, x, \dots, x^{L-1}), \qquad w(x) = av_L(x) + bv_L(f(x)).$$

If $4p \leqslant L$ and $|A| \geqslant \max\{12, 4p\}$, then

$$\dim_{\mathbb{F}_2} \operatorname{span}\{w(x) : x \in A\} \geqslant \log \binom{\lfloor |A|/3 \rfloor}{p} \geqslant p \log |A| - p \log(4p).$$

*Proof.* Draw the undirected edge $\{x, f(x)\}$ for every $x \in A$. There are no loops; an undirected edge is represented at most twice, so there are at least $|A|/2$ distinct edges. The directed graph has out-degree at most one (vertices outside $A$ have out-degree zero), hence each undirected component has at most one cycle. After duplicate reciprocal edges are identified, every cycle has length at least three. Delete one edge per cycle. The remaining forest has at least two thirds of the distinct edges, hence at least $|A|/3$ edges. Choose one domain representative for each of $\lfloor |A|/3 \rfloor$ retained edges.

Sums of $w(x)$ over different $p$-element subsets of these representatives are distinct. Otherwise their symmetric difference is a nonempty forest of at most $2p$ edges and at most $4p$ vertices. At a leaf vertex its coefficient in the proposed relation is either $a$ or $b$, and is nonzero. The relation among the corresponding at most $4p \leqslant L$ Vandermonde columns is therefore nontrivial, a contradiction. There are $\binom{\lfloor |A|/3 \rfloor}{p}$ distinct sums in the binary span. Finally $\lfloor |A|/3 \rfloor \geqslant |A|/4$ for $|A| \geqslant 12$, and $\binom{u}{p} \geqslant (u/p)^p$. □

**Proposition 3.31** (Mixed restricted-rank bound)**.** For $\lambda \in K^\times$, $\mu \in K$, and fixed-point-free $f : A \to K$, let

$$M(x, y) = \operatorname{Tr}_{K/\mathbb{F}_2}(\lambda(x + y)^d + \mu(f(x) + y)^d).$$

If $4p \leqslant L$, $|A| \geqslant \max\{12, 4p\}$, and $|B| \geqslant 2(d-1)2^{N/2}$, then

$$\operatorname{rank}_2 M[A, B] \geqslant p \log |A| - p \log(4p) + \log |B| - N - 1. \tag{3.35}$$

The full-domain matrix, for any extension of $f$, has rank at most $2^{h+1}N$.

*Proof.* All row functions lie in $\mathcal{C}_d$. For $0 \leqslant t < L$, the exponent $d - 2t$ is odd and exceeds $d/2$. In the binomial expansion, no other exponent can reduce to it under trace, so its coefficient is exactly

$$\lambda x^{2t} + \mu f(x)^{2t}.$$

Coefficient extraction followed by inverse squaring is binary-linear and gives $\sqrt{\lambda}\, v_L(x) + \sqrt{\mu}\, v_L(f(x))$. If $\mu \neq 0$, Lemma 3.30 lower-bounds the full row span. If $\mu = 0$, sums over distinct $p$-subsets of $A$ are distinct by ordinary Vandermonde independence; the same weaker bound follows. Lemma 3.29 bounds the dimension lost on restricting to $B$.

Each of the two binomial expansions has $d + 1 = 2^h$ separated $K$-products; Lemma 3.27 gives the global bound. The one-output character bound is $2^h N$. □

**Corollary 3.32** (Fixed-rate masks of any prescribed linear rank)**.** Fix $1/2 < \alpha_0 < \alpha_1 < 1$ and a constant $\kappa > 0$. One can choose a fixed $h$ such that, for all sufficiently large $N$, every fixed-point-free $f : K \to K$, every $\lambda \neq 0$, every $\mu$, and every Boolean mask $T$ of global rank at most $\kappa N$ satisfy

$$\left| \mathbb{E}(-1)^{\operatorname{Tr}(\lambda(U+V)^{2^h-1} + \mu(f(U)+V)^{2^h-1}) + T(U,V)} \right| \leqslant 2^{-\theta N}$$

for independent $U, V$ of min-entropy at least $\alpha_1 N$, where $\theta > 0$ is uniform over $f, \lambda, \mu, T$. The same conclusion for $\mu = 0$ requires no condition on $f$.

*Proof.* Choose $p$ with $(p+1)\alpha_0 - 1 > \kappa + 2$, then $h$ with $4p \leqslant 2^{h-2}$. On every side-$\alpha_0 N$ rectangle, Proposition 3.31 leaves rank greater than one after the mask is added. The full rank is at most $(2^{h+1} + \kappa)N$. Corollary 2.20, with entropy increment $\alpha_1 - \alpha_0$, proves the result. A map known to be fixed-point-free only on the actual left support may be extended outside it by a nonzero translation; all distributions in the application are unchanged. □

### 3.2.12 One-sided non-malleable sumset seed: main theorem

The same source-compatible architecture has a strengthening used in the *sumset* entropy-recycling theorem of Section 4.4. Only the first summand is tampered. This does not assert two-sided non-malleability of a function of the sum. The same seed also supplies the one-sided interface used by the ordinary entropy-recycling wrapper in Section 4.1. The independent ordinary constant-rate construction in Section 3.1 does not use this seed.

**Theorem 3.33** (One-sided non-malleable sumset seed)**.** For every fixed $0 < \sigma \leqslant 1$, there are $c_\sigma, e_\sigma > 0$ and a deterministic polynomial-time map $G_n : \mathbb{F}_2^n \to \mathbb{F}_2^{q_n}$, $q_n \geqslant c_\sigma n$, such that independent sources of min-entropy at least $\sigma n$ and every $f$ with no fixed points on $\operatorname{supp} X$ satisfy

$$(G_n(X+Y), G_n(f(X)+Y)) \approx_{2^{-e_\sigma n}} (U_{q_n}, G_n(f(X)+Y)). \tag{3.36}$$

Every output character has global lifted binary rank $O_\sigma(n)$, as does every one-comparison mixed character. Ordinary extraction follows by choosing any nonzero translation $f$ and projecting the honest output. The family is defined for every positive integer $n$, using the finite-length completion specified below.

**Construction.** Augment the linear strong-condenser views by polynomial-evaluation fingerprints of the original input. Enumerate a constant-size evaluation set, so every nonzero raw difference survives in almost every fingerprint. On each augmented view apply a moment power of order chosen in a fixed rank hierarchy, trace to a common field, and merge with the same degree-$D$ elementary symmetric polynomial. The larger moment orders protect the honest-bearing secant coefficients against every earlier-prefix character. A final binary-linear projection supplies the seed. Only the sum input is read by this evaluator; the tampering map occurs solely in the proof.

**Proof.** We first establish the secant-rank estimate and then give the full parameter and support-forcing argument.

### 3.2.13 Complete one-sided construction and its proof

**Construction 3.5 One-sided non-malleable sumset seed**

**Ingredients from earlier parts.** The linear strong condenser of Theorem 3.17; the secant-mask bound of Corollary 3.32; the majority polynomial of Lemma 3.7; fixed field representations and relative traces.

**Public parameters and fixed setup.** Fix the target component rate $\sigma > 0$. Instantiate the condenser at rate $\nu = \sigma/64$ and error $2^{-16}$, obtaining maps $L_u$, $u \in \mathbb{F}_Q$, row length $M$, and constant $\beta$. Put $r = \lfloor \beta M/16 \rfloor$, $E = \mathbb{F}_{2^r}$, and $b_n = \lceil n/r \rceil$. Fix a constant $b_*$ bounding $b_n$ in the large-length range, a power of two $R \geqslant 64b_*$, and distinct $v_1, \dots, v_R \in E$. Order $\mathbb{F}_Q \times [R]$ lexicographically and delete its last pair. The retained number is $T = QR - 1 = 2D - 1$, $D = QR/2$.

Set $\alpha_0 = 1/2 + \beta/8$ and $\alpha_1 = 1/2 + \beta/4$. For each retained index $i$, in order, put $\kappa_i = 1 + 2\sum_{j<i} 2^{h_j}$ and choose $h_i$ by Corollary 3.32. Concretely, its proof permits an integer $p_i$ with $(p_i+1)\alpha_0 - 1 > \kappa_i + 2$, followed by $h_i \geqslant 3$ with $2^{h_i-2} \geqslant 4p_i$. Let $\theta = \min_i \theta_i > 0$ be the supplied bias exponent and fix $a \geqslant \max\{2, 16T/\theta\}$. Put $\ell = \lceil (M+r)/a \rceil$, $N = a\ell$, and $F = \mathbb{F}_{2^\ell} \subseteq K = \mathbb{F}_{2^N}$. Fix a surjective projection to $q_n = \min\{\ell, \lfloor cn/2 \rfloor\}$ bits, using the constant $c > 0$ certified by the final global lift below.

**Input.** Only $z \in \mathbb{F}_2^n$.

**Evaluation steps.**

1. Pad $z$ to $b_n r$ bits, parse it as $z_0, \dots, z_{b_n-1} \in E$, and form $P_z(V) = \sum_{j<b_n} z_j V^j$.
2. For every retained pair $(u, v_j)$, concatenate $T_{u,v_j}(z) = (L_u z, P_z(v_j))$. Append zeros to reach $N$ bits; identify the result with $T_i(z) \in K$ in the fixed column order.
3. Compute $W_i(z) = \mathrm{Tr}_{K/F}(T_i(z)^{2^{h_i}-1})$ for all $i \in [T]$.
4. Compute $Z_n(z) = \sigma_D(W_1(z), \dots, W_T(z))$ and return its fixed $q_n$-bit projection $G_n(z)$.

**Output.** The seed in Theorem 3.33. Its non-malleability allows tampering with the first summand only, with the second unchanged. For the finite initial range, return one zero bit as specified after the proof.

**Not evaluated.** The map $f$, its functional graph and forest, acceptance patterns, and the decision whether a comparison image has a heavy atom. They do not affect the evaluated list of views or exponents.

**Linear fingerprints prevent local fixed points** Use Theorem 3.17 at raw threshold $\nu n$ with $\nu = \sigma/64$ and error $\varepsilon_c = 2^{-16}$. Let $M, Q, \beta$ be its parameters. Put

$$r = \lfloor \beta M/16 \rfloor, \qquad E = \mathbb{F}_{2^r}, \qquad b_n = \lceil n/r \rceil.$$

For large $n$, $b_n \leqslant b_*$ for a fixed $b_*$. Pad $z$ to $b_n$ field coefficients and write $P_z(V) = \sum_{j<b_n} z_j V^j$. Choose a power of two $R \geqslant 64b_*$ and fixed distinct $v_1, \dots, v_R \in E$. Define all augmented linear views

$$T_{u,v}(z) = (L_u z, P_z(v)) \in \mathbb{F}_2^{M+r}. \tag{3.37}$$

Every distinct raw pair has different fingerprints at all but $b_n - 1$ of these indices, by the polynomial root bound. Thus at least $63R/64$ fingerprints detect $x \neq f(x)$, pointwise in $x$.

**Actual common good views** Suppose $X, f(X), Y$ all have entropy at least $\nu n$. Let $K_t = (1/2 + \beta/2)M$. For each $L_u X$ and $L_u f(X)$ introduce a source-local acceptance bit, accepting value $z$ with probability $\min\{1, 2^{-K_t}/P(z)\}$. The rejection probability equals the excess above the entropy cap and is at most the distance in Theorem 3.17. The expected fraction of indices with either left

rejection is at most $2\varepsilon_c$. Hence with probability at least $1 - 32\varepsilon_c > 1/2$, at most $Q/16$ indices are left-bad.

Also record the $R$ deterministic fingerprint-difference bits. There are at most $2^{2Q+R}$ full left patterns. A pattern satisfying the rejection bound has probability at least $2^{-2Q-R-1}$. Fix it. Each accepted row marginal of both $X$ and $f(X)$ is capped by $2^{-K_t+2Q+R+1}$. The set of detecting fingerprint indices is fixed and has size at least $63R/64$. Independently on the right, a positive pattern makes at least $15Q/16$ rows of $Y$ capped at entropy $K_t - O(Q)$. Denote the resulting independent actual source distributions by $X^*, Y^*$.

At least $7Q/8$ indices $u$ are good for all three marginals. Pair them with the detecting fingerprint indices. Among the $QR$ augmented views, more than $3QR/4$ have both honest and comparison left views, and the right view, of entropy at least $K_t - O(Q + R)$, and satisfy

$$T_{u,v}(x) \neq T_{u,v}(f(x)) \quad \text{on the selected left support.} \tag{3.38}$$

Delete one fixed grid index and write

$$T = QR - 1 = 2D - 1, \qquad D = QR/2.$$

Then $D$ is a power of two and at least $D$ retained columns are common good. For a single execution, use the same argument without the comparison cap or difference bits: more than half the columns are good whenever $X, Y$ have entropy at least $\nu n$.

Let

$$\alpha_0 = 1/2 + \beta/8, \qquad \alpha_1 = 1/2 + \beta/4.$$

After padding by any fixed number of bits to a native length $N = M + r + O(1)$, every common good view has entropy at least $\alpha_1 N$ for sufficiently large $n$. Indeed $(1/2 + \beta/2) > (1/2 + \beta/4)(1 + \beta/16)$, with a fixed positive margin; all pattern and padding losses are constants.

**Hierarchy, actual prefixes, and field lengths** Order the retained columns once. Recursively set

$$\kappa_i = 1 + 2\sum_{j<i} 2^{h_j}$$

and choose $h_i$ by Corollary 3.32 with that mask budget and the fixed rates $\alpha_0, \alpha_1$. Let $\theta_i > 0$ be its exponent and $\theta = \min_i \theta_i > 0$. Choose a fixed integer $a \geqslant \max\{2, 16T/\theta\}$, then put

$$\ell = \lceil (M + r)/a \rceil, \qquad N = a\ell, \qquad F = \mathbb{F}_{2^\ell} \subseteq K = \mathbb{F}_{2^N}.$$

Pad every view by fewer than $a$ zero bits and identify it with $K$. The actual field rows are

$$W_i(z) = \mathrm{Tr}_{K/F}(T_i(z)^{2^{h_i}-1}). \tag{3.39}$$

Each character has rank at most $2^{h_i}N$. The complete pair prefix

$$\Pi_i = (W_j(X^* + Y^*), W_j(f(X^*) + Y^*) : j < i)$$

has every parity of rank below $\kappa_i N$ on the original raw domain.

**Lemma 3.34** (Pair freshness for a common good column)**.** On the one actual product distribution selected above, every common good column obeys

$$\Delta((W_i, W_i', \Pi_i), (U_F, U_F', \Pi_i)) \leqslant 2^{-\theta N/2}$$

for sufficiently large $n$, where $W_i' = W_i(f(X^*) + Y^*)$. For a single execution the analogous prefix distribution holds with no larger error.

*Proof.* Take $U = T_i X^*$ and $V = T_i Y^*$. By Lemma 3.28, fix independent conditional representative tables for the two raw inputs. On attained $u$, the comparison view is a deterministic map $f_i(u)$ distinct from $u$, by (3.38). Extend $f_i$ outside the attained support without fixed points. Every prefix parity, after this separate substitution, still has rank below $\kappa_i N$. The native honest core is $(U+V)^{2^{h_i-1}}$; trace transitivity sends every nonzero $F$ coefficient to a nonzero native coefficient.

Apply Corollary 3.32 and average the representative tables. Lemma 3.27 gives

$$\Delta((W_i, W_i', \Pi_i), (U_F, W_i', \Pi_i)) \leqslant \tfrac{1}{2} 2^{i\ell - \theta_i N}.$$

Now represent the raw left input conditional on its comparison view instead. That view has the same high entropy, the honest view is pointwise different, and the right source is unchanged. The same bound makes $W_i'$ fresh relative to $(W_i, \Pi_i)$. Both claims concern the original joint distribution, not a hybrid source. The operations replacing each current coordinate by independent uniform randomness commute and contract statistical distance. Their sum costs at most $2^{i\ell-\theta_i N} \leqslant 2^{-\theta N/2}$. No conditioning on the joint prefix is performed. The single-execution proof uses $\mu = 0$. □

**Forcing, heavy comparisons, and the global lift** Define

$$Z_n(z) = \sigma_D(W_1(z), \dots, W_{2D-1}(z)). \tag{3.40}$$

If $D$ entries equal $u$, then the degree-$D$ elementary symmetric polynomial equals $u^D$, regardless of the others: the generating polynomial has factor $(1+ut)^D = 1 + u^D t^D$, while the remaining factor has degree at most $D-1$.

For a set of $D$ common good indices, Lemma 3.34 and successive replacement give distance at most $D2^{-\theta N/2}$ from $U_F^{\otimes 2D}$. For sufficiently large $n$, this is less than $|F|^{-2D}$, since $2D\ell \leqslant \theta N/8$. Therefore every event prescribing all honest selected entries to be $u$ and all comparison selected entries to be $v$ has positive probability. It forces $(Z_n, Z_n') = (u^D, v^D)$. As $D$ is a power of two, this pair has full support $F^2$. The single-execution argument gives full support $F$ on every raw product support of side entropy at least $\nu n$.

It suffices first to treat globally fixed-point-free $f$. A map with no fixed points only on the original left support can be extended outside that support by a nonzero translation, without changing either evaluated distribution. To prove mixed dispersion at side entropy $(\sigma/2)n$, take uniform $X, Y$ on any corresponding supports, and a proposed constant mixed character with nonzero honest coefficient. If $f(X)$ has an atom of mass greater than $2^{-\sigma n/8}$, fix it on the left. This leaves honest left entropy at least $3\sigma n/8$. The comparison character is now a Boolean function only of $Y$; fix its value at cost at most one bit. The independent honest sources still exceed $\nu n$, so single-execution full support contradicts constancy. If no such atom exists, $X, f(X), Y$ all meet the condenser threshold. The common-good construction and pair forcing give the contradiction. The case with zero comparison coefficient is already single-execution dispersion.

Each row in (3.39) has field separation at most $a2^{h_i}$, because $T_i$ is linear. The separation of (3.40) is at most

$$R_* := \sum_{|I|=D} \prod_{i \in I} a 2^{h_i} = O_\sigma(1).$$

A mixed character of $Z_n(x+y), Z_n(f(x)+y)$ has rank at most $2R_*\ell = O_\sigma(n)$. Corollary 2.20, now on the original $n$-bit sources, raises the threshold from $\sigma n/2$ to $\sigma n$ and gives all honest-bearing biases at most $2^{-cn}$, uniformly over $f$. Project to $q_n = \min\{\ell, \lfloor cn/2 \rfloor\}$ bits. Lemma 3.27 gives one-sided non-malleability error at most $2^{q_n - 1 - cn} = 2^{-\Omega_\sigma(n)}$. This proves Theorem 3.33 for all sufficiently large $n$. All parameter choices are fixed before the source is known.

For the remaining finite set of positive lengths, return one zero bit and decrease $c_\sigma, e_\sigma$ as in the finite-length convention in Section 2. This preserves one-sided non-malleability, ordinary extraction, and the lifted rank bound, and completes the theorem at every positive length.

*Remark* 3.35 (Only one summand is tampered). Theorem 3.33 does not allow simultaneous translations of both summands. Such translations preserve $X + Y$ and would make honest and comparison outputs equal, which is incompatible with ordinary non-malleability. There is no such contradiction when the second summand stays unchanged and $f$ has no fixed points.

## 3.3 Fixed-$C$ non-malleable two-source extraction

### 3.3.1 Tagged affine seeds and one-sided Gold recognition

The starter below uses a short left prefix and a longer right row. Its inverse argument recognizes only the left tampering. The outer construction supplies distinct numerical tags by source-local fingerprints of the original inputs.

**Theorem 3.36** (Near-full affine non-malleability)**.** *Reference.* [49, Theorem 1.12 and Section 3]. There are absolute constants $\delta_A, c_A, e_A > 0$ and an explicit map $V_N$ on $N$ bits, with at least $c_A N$ output bits, which is an affine non-malleable extractor at entropy $(1 - \delta_A)N$ and error $2^{-e_A N}$. It also has the ordinary affine-extraction guarantee at that threshold.

This is Li's Theorem 1.12 and its construction in Section 3 of [49]. The no-fixed-point convention can be used on an active affine support by the next elementary extension lemma.

**Lemma 3.37** (Extending an affine comparison off its active support)**.** If $A \subseteq \mathbb{F}_2^N$ is a nonempty affine space and $f$ is affine with $f(x) \neq x$ for every $x \in A$, there is a globally fixed-point-free affine $\widetilde{f}$ agreeing with $f$ on $A$.

*Proof.* Choose an affine retraction $P : \mathbb{F}_2^N \to A$ and set $\widetilde{f}(x) = f(Px) + x + Px$. Then $\widetilde{f}(x) + x = f(Px) + Px \neq 0$ for every $x$, and on $A$ one has $Px = x$. □

**Lemma 3.38** (Equality partition)**.** For uniform affine $Z \in \mathbb{F}_2^N$, an affine map $f$, and an integer $t \geqslant 1$, there is an affine partition, apart from probability at most $2^{-t}$, on whose parts $f(Z) = Z$ identically or $f(Z) \neq Z$ everywhere. Every part lowers the entropy of $Z$ by at most $t$.

*Proof.* The image of $f(Z) + Z$ is affine. If it omits zero, no partition is needed. Otherwise it is a linear space of dimension $r$, on which the image is uniform. If $r \leqslant t$, fix the complete image. If $r > t$, fix a surjective $t$-bit linear projection of it and discard the zero value. All nonzero values guarantee inequality. Every retained fixing uses at most $t$ independent affine equations; the discarded probability in the latter case is $2^{-t}$. □

**Lemma 3.39** (An affine-in-tag seed family)**.** There is an absolute integer $A_* \geqslant 1$ such that, for $N = A_* s$ and $F = \mathbb{F}_{2^s}$, one can explicitly compute two source-local functions $V_0, V_1 : \mathbb{F}_2^N \to F$ for which

$$S_a(z) = V_0(z) + aV_1(z) \qquad (a \in F) \tag{3.41}$$

satisfies, for every affine $f$ and distinct $a, a' \in F$,

$$(S_a(U_N), S_{a'}(f(U_N))) \approx_{2^{-2s}} (U_F, S_{a'}(f(U_N))). \tag{3.42}$$

Every field element is an allowed tag. The parameter $A_*$ is independent of all subsequent moment widths and rank margins.

*Proof.* Choose $A_*$ large enough that $4s \leqslant \delta_A N/2$, $c_A N \geqslant 2s$, and $e_A N \geqslant 8s$. Truncate $V_N$ to $2s$ bits and identify them with $(V_0, V_1) \in F^2$. Apply Lemma 3.38 with $t = 4s$ to $U_N, f(U_N)$. The honest entropy on each retained part is at least $N - 4s \geqslant (1 - \delta_A)N$.

On a noncopy part, extend its comparison by Lemma 3.37. Theorem 3.36 makes $(V_0, V_1)$ uniform independently of the comparison vector to error $2^{-8s}$. Its nonzero linear evaluation at $a$ is therefore uniform independently of the comparison evaluation. On a copy part, ordinary affine extraction makes the coefficient pair uniform to the same error. The two evaluation vectors $(1, a), (1, a')$ are independent, so their two values are exactly independent uniform under that comparison distribution. Restoring the actual comparison marginal costs at most another $2^{-8s}$. Averaging the parts and charging the discarded mass gives at most $2 \cdot 2^{-8s} + 2^{-4s} \leqslant 2^{-2s}$ for sufficiently large $s$. □

We identify $\mathbb{F}_2^N$ with $L = \mathbb{F}_{2^N}$ and retain $F \subseteq L$. In this subsection and the next ones, a subscript on $S_a$ denotes a field tag, not a uniform seed supplied to the final evaluator. Formula (3.41) will account for the actual input-dependent advice without assuming any degree bound on $V_0, V_1$.

**Gold defect and graph energy.** For $z \in L$ put $\Gamma_c(z) = (z, z^{1+2}, \ldots, z^{1+2^c})$. For a finite subset $S$ of a binary vector space, write $E(S) = |\{(z_1, z_2, z_3, z_4) \in S^4 : z_1 + z_2 + z_3 + z_4 = 0\}|$. Let $A \subseteq V = \mathbb{F}_2^N$ and let $f : A \to W = \mathbb{F}_2^M$ be arbitrary. Define the graph of the restriction of $f$ to $A$ by

$$\mathrm{Graph}(f|_A) := \{(x, f(x)) : x \in A\} \subseteq V \times W.$$

Here $f$ already has domain $A$; the restriction notation is retained for compatibility with the subsequent graph-energy statements. Define its normalized graph energy by

$$\varepsilon_f = 2^{-3N} E(\mathrm{Graph}(f|_A)).$$

All probabilities below use uniform variables in the whole ambient spaces; membership in $A$ is part of the event.

**Lemma 3.40** (Restricted homomorphism testing)**.** *Reference.* [3, Lemma 3.3]. There are absolute $D_0, d_0 \geqslant 1$ such that, for all positive integers $N, M$, every $A \subseteq \mathbb{F}_2^N$, every map $f : A \to \mathbb{F}_2^M$, and $0 < \rho \leqslant 1$,

$$E(\mathrm{Graph}(f|_A)) \geqslant \rho 2^{3N} \quad \Longrightarrow \quad |\{x \in A : f(x) = \ell(x)\}| \geqslant D_0^{-1} \rho^{d_0} 2^N \tag{3.43}$$

for some affine map $\ell : \mathbb{F}_2^N \to \mathbb{F}_2^M$.

This is [3, Lemma 3.3]. Only its existential assertion is used; its algorithmic complexity is irrelevant here.

Fix the binary identification $L \cong \mathbb{F}_2^N$. The binary coordinate span of the Gold encoding is the following space of functions on $L$:

$$\mathcal{C}_c = \left\{ z \longmapsto \mathrm{Tr}_{L/\mathbb{F}_2} \left( a_0 z + \sum_{j=1}^{c} a_j z^{1+2^j} \right) : a_0, \ldots, a_c \in L \right\}.$$

This agrees with the span of the binary coordinate functions of $\Gamma_c$ by nondegeneracy of the trace pairing. For $A \subseteq L$ and $f : A \to L$, its pullback space is

$$(\mathcal{C}_c \circ f)|_A := \{x \mapsto \varphi(f(x)) : \varphi \in \mathcal{C}_c\} \leqslant \mathbb{F}_2^A.$$

Here $\circ$ denotes function composition. The space $\mathrm{RM}(2,N)|_A$ consists of restrictions to $A$ of Boolean polynomials of degree at most two in the fixed binary coordinates of $L$; it includes the constant functions. Define the full Gold defect by

$$d_c(f;A) = \dim_{\mathbb{F}_2}\left(\frac{(\mathcal{C}_c\circ f)|_A + \mathrm{RM}(2,N)|_A}{\mathrm{RM}(2,N)|_A}\right). \tag{3.44}$$

Put

$$\mathcal{U}_f := (\mathcal{C}_c\circ f)|_A, \qquad \mathcal{Q}_A := \mathrm{RM}(2,N)|_A.$$

Both are binary vector subspaces of $\mathbb{F}_2^A$, but $\mathcal{Q}_A$ need not be contained in $\mathcal{U}_f$. The symbol $+$ in (3.44) denotes their vector-space sum, so that the denominator $\mathcal{Q}_A$ is a subspace of the numerator. The fraction denotes the *quotient vector space*: two functions are identified when their difference on $A$ belongs to $\mathcal{Q}_A$. In particular, adding a quadratic function does not change the quotient class. The second isomorphism theorem gives

$$\frac{\mathcal{U}_f+\mathcal{Q}_A}{\mathcal{Q}_A} \cong \frac{\mathcal{U}_f}{\mathcal{U}_f\cap\mathcal{Q}_A}, \qquad d_c(f;A) = \dim_{\mathbb{F}_2}\mathcal{U}_f - \dim_{\mathbb{F}_2}(\mathcal{U}_f\cap\mathcal{Q}_A). \tag{3.45}$$

Thus $d_c(f;A)$ counts the independent binary Gold-coordinate combinations which remain after identifying combinations that agree with quadratic functions on $A$. No injectivity of $f$ is assumed. In particular, $d_c(f;A)=0$ if $f$ is binary-affine, since the Gold coordinates of an affine map have binary degree at most two.

**Equivalent quadratic-plus-small-error representation.** The quotient definition has the following concrete consequence, which will be used in the proof of Theorem 3.41. Put $B = L^{c+1}$, viewed as an $N(c+1)$-dimensional binary vector space, and write $r = d_c(f;A)$. There exist a vector-valued polynomial map $Q_f : L \to B$ of binary degree at most two, a function $e_f : A \to B$, and a *fixed* binary linear subspace $W_f \leqslant B$ of dimension $r$, such that

$$\Gamma_c(f(x)) = Q_f(x) + e_f(x), \qquad e_f(x)\in W_f \quad (x\in A). \tag{3.46}$$

Indeed, consider the binary-linear map

$$T : B^* \longrightarrow \mathbb{F}_2^A/\mathcal{Q}_A, \qquad T(\lambda) = [x \longmapsto \lambda(\Gamma_c(f(x)))].$$

The image of $T$ is precisely $(\mathcal{U}_f+\mathcal{Q}_A)/\mathcal{Q}_A$, so $\operatorname{rank} T = r$. Choose a basis $\lambda_1,\dots,\lambda_{\dim B-r}$ of $\ker T$ and extend it to a basis of $B^*$. For each basis functional in $\ker T$, choose a Boolean polynomial $q_i$ of degree at most two on $L$ agreeing on $A$ with $x\mapsto\lambda_i(\Gamma_c(f(x)))$; for the remaining $r$ basis functionals put $q_i=0$. Because the $\lambda_i$ form a basis of $B^*$, there is a unique map $Q_f : L\to B$ satisfying $\lambda_i(Q_f(x)) = q_i(x)$ for every $i$. Its binary coordinates are linear combinations of degree-at-most-two polynomials, so $Q_f$ is quadratic. Now set $e_f(x) = \Gamma_c(f(x)) - Q_f(x)$ on $A$. Every $\lambda\in\ker T$ annihilates $e_f(x)$, whence

$$e_f(A)\subseteq W_f := (\ker T)^\perp := \{z\in B : \lambda(z)=0 \text{ for all } \lambda\in\ker T\}, \qquad \dim_{\mathbb{F}_2} W_f = r.$$

This proves (3.46). In particular, $e_f$ takes at most $2^r$ distinct values; the quadratic map is defined on all of $L$, while the decomposition is asserted only on $A$.

For a real function $g$ on a finite binary vector space $V$, write

$$\|g\|_{U^3}^8 := \mathbb{E}_{x,h_1,h_2,h_3\sim U_V}\prod_{\omega\in\{0,1\}^3} g(x+\omega_1h_1+\omega_2h_2+\omega_3h_3),$$

where the four sampled vectors are independent. This is the third Gowers uniformity norm (for real functions). Repeated Cauchy–Schwarz gives $|\mathbb{E}g| \leqslant \|g\|_{U^3}$. For $g = \mathbf{1}_D$, the displayed average is exactly the probability that all eight vertices of the random affine three-cube lie in $D$. The directions need not be linearly independent, so degenerate cubes and repeated vertices are included. In the next proof, $V = L^p$, viewed as a binary vector space.

**Theorem 3.41** (Amortized recognition for arbitrary maps)**.** For integer $p \geqslant 1$, $c \geqslant 8p-1$, $N > 2c$, $|A| = 2^{N-a}$ and $r = d_c(f; A)$, some affine map agrees with $f$ on a subset of $A$ of size at least $2^{N-O(a+r/p+p)}$. The constant is absolute.

*Proof.* We give the two algebraic and probabilistic facts used in the argument, and then explain how taking $p$ copies amortizes the defect $r$. Throughout, every cube is sampled by choosing its base point and its three directions independently and uniformly; directions may be zero.

*Step 1: a short Gold relation has small binary span.* Suppose that $z_1, \dots, z_m \in L$ satisfy

$$\sum_{\nu=1}^{m} \Gamma_c(z_\nu) = 0, \qquad m \leqslant 8p \leqslant c+1. \tag{3.47}$$

Put $d = \dim_{\mathbb{F}_2} \operatorname{span}\{z_1, \dots, z_m\}$ and form the $m \times m$ Moore matrix over $L$,

$$\mathsf{M} = (z_\nu^{2^i})_{0 \leqslant i < m,\, 1 \leqslant \nu \leqslant m}.$$

For $i < j$, the $(i, j)$ entry of $\mathsf{M}\mathsf{M}^{\mathsf{T}}$ is

$$\sum_{\nu} z_\nu^{2^i + 2^j} = \left( \sum_{\nu} z_\nu^{1+2^{j-i}} \right)^{2^i} = 0,$$

because $1 \leqslant j - i \leqslant m - 1 \leqslant c$. The entries with $i > j$ vanish by symmetry, and the diagonal entries vanish since

$$\sum_{\nu} z_\nu^{2^{i+1}} = \left( \sum_{\nu} z_\nu \right)^{2^{i+1}} = 0.$$

Thus $\mathsf{M}\mathsf{M}^{\mathsf{T}} = 0$. The Moore determinant criterion, including its rectangular-rank form, says that $\operatorname{rank}_L \mathsf{M} = d$: the rank is the $\mathbb{F}_2$-dimension of the span of the labels, even if some labels repeat. Since the image of $\mathsf{M}^{\mathsf{T}}$ is contained in the kernel of $\mathsf{M}$,

$$d = \operatorname{rank} \mathsf{M} = \operatorname{rank} \mathsf{M}^{\mathsf{T}} \leqslant \dim \ker \mathsf{M} = m - d.$$

Consequently

$$\dim_{\mathbb{F}_2} \operatorname{span}\{z_1, \dots, z_m\} \leqslant m/2. \tag{3.48}$$

No distinctness assumption on the $z_\nu$ is used here.

*Step 2: a proper relation on one three-cube is a graph-energy test.* Let $I$ be any nonempty proper subset of $\mathbb{F}_2^3$, and fix $b \in L$. We claim that a uniform affine three-cube $(x_\omega)_\omega$ in $L$ satisfies

$$\Pr\bigl[x_\omega \in A \ (\forall \omega), \quad \sum_{\omega \in I} f(x_\omega) = b\bigr] \leqslant \varepsilon_f^{1/4}. \tag{3.49}$$

Choose $\omega_* \in I$ and $\omega_\circ \notin I$. Their two-point affine line in $\mathbb{F}_2^3$ is the simultaneous 1-fiber of two independent affine Boolean functions $\beta_1, \beta_2$. Complete $1, \beta_1, \beta_2$ by one more affine Boolean function $\beta_3$ to a basis of all affine functions on $\mathbb{F}_2^3$. A uniform affine cube can consequently be written

$$x_\omega = z_0 + \beta_1(\omega) U + \beta_2(\omega) V + \beta_3(\omega) z_3,$$

where $z_0, z_3, U, V$ are independent uniform elements of $L$. Fix $z_0, z_3$ and let $F(U,V)$ be the indicator of the event in (3.49). If $\rho = \mathbb{E}_{U,V} F(U,V)$, the two-variable Cauchy–Schwarz (box) inequality gives

$$\rho^4 \leqslant \mathbb{E}_{U,U',V,V'} F(U,V)F(U',V)F(U,V')F(U',V'),$$

for independent uniform $U, U', V, V'$. If all four events on the right hold, add their four output equations. In characteristic two the four copies of $b$ cancel. For any vertex $\omega \in I$ other than $\omega_*$, at least one of $\beta_1(\omega), \beta_2(\omega)$ is zero, so its contribution occurs in identical pairs and cancels as well. The only remaining terms are the four values of $f$ at $\omega_*$. Their arguments are

$$z + U + V, \quad z + U' + V, \quad z + U + V', \quad z + U' + V', \qquad z = z_0 + \beta_3(\omega_*) z_3.$$

All four arguments belong to $A$, their sum is zero, and their $f$-values sum to zero. For every fixed $z$, three of these four arguments are independent uniform elements of $L$; the fourth is their sum. The probability of this latter graph-parallelogram event is therefore exactly

$$2^{-3N} E(\mathrm{Graph}(f|_A)) = \varepsilon_f.$$

Hence $\rho^4 \leqslant \varepsilon_f$ for each fixed $z_0, z_3$. Averaging proves (3.49). The bound holds uniformly in the chosen set $I$ and the constant $b$.

*Step 3: represent the defect by an $r$-dimensional error space.* Apply the quadratic-plus-small-error representation (3.46) established immediately following the definition of $d_c(f;A)$. Write $Q = Q_f$, $e = e_f$ and $W = W_f \leqslant B = L^{c+1}$. Thus

$$\Gamma_c(f(x)) = Q(x) + e(x), \qquad e(A) \subseteq W, \qquad \dim_{\mathbb{F}_2} W = r. \tag{3.50}$$

The key point is that the error $e$ takes at most $2^r$ values, whereas $Q$ has binary degree at most two on the full ambient input space. No assumption that $f$ is injective or globally polynomial is involved.

Define $E_p : A^p \to W$ by $E_p(x_1, \ldots, x_p) = \sum_{i=1}^p e(x_i)$. Some fiber $\mathcal{D} = E_p^{-1}(w)$ has size at least $|A|^p/2^r$. As a subset of the ambient space $L^p$, its density satisfies

$$\alpha = \frac{|\mathcal{D}|}{2^{Np}} \geqslant 2^{-pa-r}. \tag{3.51}$$

The $U^3$ inequality for a nonnegative indicator gives

$$\Pr[\text{all eight vertices of a uniform three-cube in } L^p \text{ belong to } \mathcal{D}] = \|\mathbf{1}_{\mathcal{D}}\|_{U^3}^8 \geqslant \alpha^8 \geqslant 2^{-8(pa+r)}. \tag{3.52}$$

For every cube counted here, sum (3.50) over its eight vertices and over $i \in [p]$. The eight identical values $w$ cancel. The sum of the values of $\sum_i Q(x_i)$ also vanishes, because the third additive derivative of any binary quadratic polynomial is zero. Thus

$$\sum_{i=1}^{p} \sum_{\omega \in \mathbb{F}_2^3} \Gamma_c(f(x_{i,\omega})) = 0.$$

There are $8p$ output labels in this sum, and (3.48) implies that their binary span has dimension at most $4p$.

*Step 4: extract many proper relations and apply the four-corner bound independently across blocks.* Reveal the $p$ coordinate cubes one block at a time. If $d_i$ is the increment in the binary dimension of the output-label span when the eight labels of block $i$ are added, then

$$0 \leqslant d_i \leqslant 8, \qquad \sum_{i=1}^{p} d_i \leqslant 4p.$$

At most $4p/7$ blocks can have $d_i \geqslant 7$. Hence at least $3p/7$ blocks have $d_i \leqslant 6$. For each such block, the eight labels, considered modulo the span of all earlier labels, have a space of binary relations of dimension at least two. We may select a nonzero relation supported on a nonempty *proper* subset $I_i \subsetneq \mathbb{F}_2^3$: a two-dimensional relation space cannot consist only of the zero vector and the all-ones vector. For some fixed binary coefficients $b_{i,h,\omega}$, this relation is

$$\sum_{\omega \in I_i} f(x_{i,\omega}) = \sum_{h<i} \sum_{\omega \in \mathbb{F}_2^3} b_{i,h,\omega} f(x_{h,\omega}). \tag{3.53}$$

The set of selected blocks, the subsets $I_i$, and the coefficient vectors in (3.53) have at most $2^{O(p^2)}$ possible joint specifications. This estimate is independent of $N$ because all coefficients are binary and only $8p$ labels occur.

Fix one specification with at least $3p/7$ selected blocks. The coordinate cubes in $L^p$ are independent uniform three-cubes. When we reveal them sequentially, at each selected block the right side of (3.53) is already a fixed value of $L$. Therefore (3.49) bounds its conditional success probability, including membership in $A$ of the eight current vertices, by $\varepsilon_f^{1/4}$. Iterated conditioning bounds the probability that all specified relations hold by $\varepsilon_f^{3p/28}$. Every cube from (3.52) admits at least one such specification. A union bound now gives

$$2^{-8(pa+r)} \leqslant 2^{O(p^2)} \varepsilon_f^{3p/28}. \tag{3.54}$$

Taking logarithms (or treating $\varepsilon_f = 0$ separately, when the inequality is impossible) yields

$$\varepsilon_f \geqslant 2^{-O(a+r/p+p)}.$$

Finally apply the restricted homomorphism-testing Lemma 3.40. Its constants are absolute, so it gives an affine map $\ell : L \to L$ agreeing with $f$ on at least $2^{N-O(a+r/p+p)}$ points of $A$, as claimed. □

### 3.3.2 An asymmetric tagged starter

**Lemma 3.42** (Scaled polynomial evaluation)**.** For $K = \mathbb{F}_{2^m}$ set $\Phi_J(u, v) = v(1, u, \dots, u^{J-1}) \in K^J$. If $D \subseteq K^2$ has density $2^{-d}$ and $(J-1)2^{-m} \leqslant 2^{-d-1}$, the binary affine span of $\Phi_J(D)$ has codimension at most $d + 1$.

*Proof.* Put $q = |K| = 2^m$ and let $\chi(z) = (-1)^{\mathrm{Tr}_{K/\mathbb{F}_2}(z)}$. Every binary linear functional on $K^J$ has the form

$$\Lambda(z_0, \dots, z_{J-1}) = \mathrm{Tr}_{K/\mathbb{F}_2}\left(\sum_{i=0}^{J-1} a_i z_i\right)$$

for a unique vector $(a_0, \dots, a_{J-1}) \in K^J$, by nondegeneracy of the trace pairing. If $\Lambda \neq 0$, the polynomial $P(T) = \sum_{i=0}^{J-1} a_i T^i$ is nonzero and has degree at most $J - 1$. Hence, for independent

uniform $U, V \in K$,

$$\begin{aligned}\mathbb{E}_{U,V}(-1)^{\Lambda(\Phi_J(U,V))} &= \mathbb{E}_U \mathbb{E}_V \chi(VP(U)) \\ &= \Pr_U[P(U) = 0] \\ &\leqslant (J-1)q^{-1} =: \beta.\end{aligned}$$

The middle equality is exact: if $P(u) \neq 0$, the map $v \mapsto \mathrm{Tr}_{K/\mathbb{F}_2}(vP(u))$ is a nonzero binary functional and its character average is zero; if $P(u) = 0$, the average is one.

Let $H = \mathrm{aff}_{\mathbb{F}_2}(\Phi_J(D))$, and write its binary codimension in $K^J$ as $b$. If $H = z_* + W$ and $W^\perp \leqslant (K^J)^*$ is the annihilator of its direction space, character orthogonality gives

$$\mathbf{1}_H(z) = 2^{-b} \sum_{\Lambda \in W^\perp} (-1)^{\Lambda(z - z_*)}.$$

Taking expectation at $z = \Phi_J(U, V)$, bounding the zero character by one and the other $2^b - 1$ characters by $\beta$, gives

$$\Pr[\Phi_J(U,V) \in H] \leqslant 2^{-b} + (1 - 2^{-b})\beta \leqslant 2^{-b} + \beta.$$

But $\Phi_J(D) \subseteq H$, so the probability on the left is at least $|D|/|K|^2 = 2^{-d}$. Under the hypothesis $\beta \leqslant 2^{-d-1}$, we have

$$2^{-b} \geqslant 2^{-d} - \beta \geqslant 2^{-d-1}.$$

Thus $b \leqslant d + 1$. Notice that the conclusion concerns the binary *affine* span; its difference space has the same dimension, and we will use the bound for differences as well as for the full span. □

**Bias and separate source strength.** Call a character honest-bearing if its honest coefficient is nonzero. If each such character has absolute bias at most $\epsilon$ for all independent sources at threshold $k_0$, then at threshold $k_0 + d$ its average absolute conditional bias given either source is at most $\epsilon + 2^{1-d}$. Partition that source by the sign of its conditional bias. Each class of mass at least $2^{-d}$ preserves the threshold and independence; the other classes have total mass at most $2^{1-d}$. For $q$ outputs of $m$ bits, conditional Fourier inversion and the triangle inequality bound either strong error by $2^{qm-1}(\epsilon + 2^{1-d})$: the honest-free coefficients cancel against uniform times the actual comparison marginal. We use the linear-rank approximate-duality lift of Corollary 2.20 with fixed linear entropy slack to obtain the initial bias from nonconstancy on every lower-threshold rectangle.

**Compatible $M$-bit rows.** In the following, we use this term to denote an arithmetic restriction on the *length*, not a restriction on the distributions of the two rows or a promise about the tampering maps. For the starter extractor, choose the absolute integer $A_*$ from Lemma 3.39, and a fixed output-shortening divisor $D_1 = 12A_*t_*$, where $t_*$ is a fixed positive integer chosen in the proof. A starter length $M$ is *compatible* if it can be written

$$M = 6n_0, \qquad n_0 = A_* s, \qquad 2t_* \mid s,$$

with $s$ sufficiently large for the fixed constants $c, J$, and with fixed representations of the tower

$$K = \mathbb{F}_{2^{s/2}} \subset F = \mathbb{F}_{2^s} \subset L = \mathbb{F}_{2^{n_0}}.$$

Then the right row parses into two $L$-words and $J = 8A_*$ $K$-words, since $2n_0 + J(s/2) = 6n_0 = M$, and the final trace can land in the subfield of degree $s/(2t_*) = M/D_1$. Every input bit has a

specified coordinate in these fixed bases. There is no random choice or extra entropy condition hidden in the word "compatible." The set of admissible starter lengths contains all sufficiently large multiples of the fixed integer $12A_*t_*$.

**Lemma 3.43** (Tagged starter extractor)**.** For every sufficiently large compatible row length $M$ as defined above, there is a fixed-tag extractor against one arbitrary separate tampering with a distinct tag, strong in the left source, at entropy $(1-\tau_1)M$ for an absolute $\tau_1 > 0$. It has output length $\Omega(M)$ and error $2^{-\Omega(M)}$. Furthermore, it admits constant field separation over compatible subfields for the actual advice below.

**Construction 3.6 Asymmetric tagged starter extractor**

**Ingredients from earlier parts.** The affine-in-tag seed of Lemma 3.39 and field polynomial evaluation.

**Public parameters and fixed setup.** Write $n_0 = A_*s$, $K = \mathbb{F}_{2^{s/2}} \subset F = \mathbb{F}_{2^s} \subset L = \mathbb{F}_{2^{n_0}}$, $J = 8A_*$ and $M = 6n_0$. Use the fixed width $c$ chosen in the proof.

**Input.** Two arbitrary $M$-bit rows (with a compatible public length) and a fixed numerical tag $a \in F$.

**Evaluation steps.**

1. Denote the complete left and right input rows by $z, w \in \mathbb{F}_2^M$. Take the first $n_0$ bits of $z$ as $x = \mathrm{prefix}_{n_0}(z) \in L$, and parse the complete right row as $w = (r, t, Y) \in L^2 \times K^J$. Write $S_a(x) = (u, v) \in K^2$.
2. For a coefficient vector $D$, put $P_D(T) = \sum_{i \geqslant 0} D_i T^i$ over its indexed coordinates starting at zero. Compute
$$E_a = \mathrm{Tr}_{L/K}\big(tP_{\Gamma_c(x)}(r)\big) + vP_Y(u).$$

**Output.** Return a relative trace of $E_a$ to an appropriate output subfield specified in the proof below. The length of the output field word is a fixed positive fraction of $M$.

*Proof.* We prove the fixed-tag statement by ruling out a constant mixed character on every rectangle of sufficiently small side deficiency. The error and the separate left-source guarantee then follow from the rank-to-bias theorem and entropy slack. Throughout this proof the tags $a \neq a'$ are fixed field elements; the later outer construction is responsible for fixing its current input-dependent tags.

*The input rectangle and the two terms.* Fix supports of size at least $2^{M-\alpha M}$ on both sides, where $\alpha > 0$ will be chosen after the other constants. Let $z, w \in \mathbb{F}_2^M$ denote the *complete* left and right rows, and let $T_L, T_R : \mathbb{F}_2^M \to \mathbb{F}_2^M$ denote the arbitrary separate comparison maps. The starter uses only the first $n_0$ bits of $z$; fix its unused suffix at a most frequent value $s_0$ and write $z = (x, s_0)$. Its resulting prefix support $A \subseteq L$ has $|A| \geqslant 2^{n_0 - a_0}$ with $a_0 \leqslant \alpha M$. The comparison's *short left prefix* is then the deterministic, possibly noninjective function

$$f(x) := \mathrm{prefix}_{n_0}(T_L(x, s_0)), \qquad x \in A.$$

The tampering $T_L$ is arbitrary and need not preserve the prefix. Let $B$ denote the support of the *complete* right row $w$, $|B| \geqslant 2^{6n_0 - b_0}$ with $b_0 \leqslant \alpha M$. Parse $w = (r(w), t(w), Y(w))$ and its tampered value $T_R(w) = (r'(w), t'(w), Y'(w))$; $T_R$ remains entirely arbitrary. Thus, after fixing $s_0$, the restricted product rectangle is parameterized by $(x, w) \in A \times B$. From now on, $x$ always means the short left prefix and $w$ the complete right row.

Put $m_K = s/2$, so that $K = \mathbb{F}_{2^{m_K}}$ and $Jm_K = 4n_0$. Consider the absolute-trace character of the two untruncated starter outputs, with nonzero honest coefficient $\lambda \in K^\times$ and arbitrary comparison coefficient $\mu \in K$:

$$\chi_{s_0}(x, w) = \mathrm{Tr}_{K/\mathbb{F}_2}\big(\lambda E_a(x; r(w), t(w), Y(w)) + \mu E_{a'}(f(x); r'(w), t'(w), Y'(w))\big)\,.$$

Suppose it is constant on $A\times B$. Here $E_a$ is the untruncated prefix-level formula from Construction 3.6, not a function whose left argument is the entire $M$-bit row. For the honest terms, abbreviate

$$E_a(x;w)=G(x;w)+T_a(x;w),\qquad G(x;w)=\mathrm{Tr}_{L/K}(t(w)P_{\Gamma_c(x)}(r(w))),\qquad T_a(x;w)=vP_{Y(w)}(u),$$

the tagged term is the pairing of the $J$ coordinates of $\Phi_J(u,v)$ with the $J$ coefficients of $Y$. After any separate precomposition on the two sides, its binary character matrix has rank at most $Jm_K=4n_0$. Thus the sum of the two tagged terms, including a possible constant matrix, has rank at most

$$k_G:=2Jm_K+1=8n_0+1. \tag{3.55}$$

Constancy of the full mixed character forces the corresponding mixed Gold term, restricted to $A\times B$, to have matrix rank at most $k_G$. This assertion uses ordinary binary matrix rank: for a function $h:A\times B\to\mathbb{F}_2$ its matrix is $(h(x,y))_{x\in A,y\in B}$; a product of a left function and a right function contributes rank one.

*The dense spans of the two Gold feature families.* Let $D_G=(c+1)n_0$, the binary dimension of $L^{c+1}$. For a nonzero binary character $\Lambda$ of $\Gamma_c(Z)$, where $Z$ is uniform in $L$, write its Boolean phase as

$$q(z)=\Lambda(\Gamma_c(z))=\mathrm{Tr}_{L/\mathbb{F}_2}\left(\gamma_0 z+\sum_{i=1}^{c}\gamma_i z^{1+2^i}\right),\qquad \gamma_i\in L.$$

If $\gamma_1=\cdots=\gamma_c=0$, then $q$ is a nonzero binary-linear function and its character bias is zero. Otherwise let $j\leqslant c$ be the largest index for which $\gamma_j\neq 0$. We spell out why the polar radical of $q$ is small. The associated polar form is

$$\begin{aligned}B_q(z,h)&:=q(z+h)+q(z)+q(h)\\&=\mathrm{Tr}_{L/\mathbb{F}_2}\left(\sum_{i=1}^{j}\gamma_i(zh^{2^i}+hz^{2^i})\right).\end{aligned}$$

Indeed, $(z+h)^{2^i}=z^{2^i}+h^{2^i}$ in characteristic two, so expanding $(z+h)^{1+2^i}$ leaves precisely the two displayed cross terms; the linear term $\gamma_0 z$ disappears. The absolute trace is Frobenius-invariant. Thus, for any $w,z\in L$,

$$\mathrm{Tr}_{L/\mathbb{F}_2}(wz^{2^i})=\mathrm{Tr}_{L/\mathbb{F}_2}(w^{2^{-i}}z),\qquad w^{2^{-i}}:=w^{2^{n_0-i}},$$

where the exponent $2^{-i}$ denotes the inverse $i$-fold Frobenius automorphism, not a rational exponent. Applying this identity to $w=\gamma_i h$ rewrites the polar form as

$$B_q(z,h)=\mathrm{Tr}_{L/\mathbb{F}_2}(zR(h)),\qquad R(h):=\sum_{i=1}^{j}\left(\gamma_i h^{2^i}+(\gamma_i h)^{2^{-i}}\right).$$

By nondegeneracy of the binary trace pairing on $L$, the polar radical is exactly

$$\mathrm{Rad}(q):=\{h\in L:B_q(z,h)=0\text{ for every }z\in L\}=\{h\in L:R(h)=0\}.$$

All the Frobenius maps appearing in $R$ are $\mathbb{F}_2$-linear, so $\mathrm{Rad}(q)$ is a binary subspace. To bound its size, raise the equation $R(h)=0$ to the $2^j$th power. As the Frobenius automorphism is bijective, this is equivalent to

$$0=R(h)^{2^j}=\sum_{i=1}^{j}\left(\gamma_i^{2^j}h^{2^{i+j}}+(\gamma_i h)^{2^{j-i}}\right).$$

Here $n_0 > 2c \geqslant 2j$ ensures that all exponents $i + j$ are strictly below $n_0$, so no Frobenius powers wrap around. The term with $i = j$ in the first sum is $\gamma_j^{2^j} h^{2^{2j}}$, with nonzero coefficient, and every other monomial has strictly smaller degree. Therefore this is a nonzero ordinary polynomial in $h$ of degree exactly $2^{2j}$, and it has at most $2^{2j}$ roots in $L$. Hence

$$|\operatorname{Rad}(q)| \leqslant 2^{2j}.$$

Finally, put $\beta = \mathbb{E}_{z \in L}(-1)^{q(z)}$. Squaring the bias and making the change of variables $(z, z') = (z, z + h)$, then averaging first over $z$, gives

$$\begin{aligned}\beta^2 &= \mathbb{E}_{z,h \in L}(-1)^{q(z)+q(z+h)} \\ &= \mathbb{E}_{h \in L}(-1)^{q(h)} \mathbb{E}_{z \in L}(-1)^{B_q(z,h)} \\ &= \mathbb{E}_{h \in L}\big[\mathbf{1}_{\operatorname{Rad}(q)}(h)(-1)^{q(h)}\big] \leqslant \frac{|\operatorname{Rad}(q)|}{|L|} \leqslant 2^{2j-n_0}.\end{aligned}$$

The penultimate equality again uses nondegeneracy of the trace pairing: the average of $(-1)^{B_q(z,h)}$ over $z$ is one if $R(h) = 0$ and zero otherwise. Taking square roots yields

$$\left|\mathbb{E}_{Z \in L}(-1)^{\Lambda(\Gamma_c(Z))}\right| \leqslant 2^{j-n_0/2} \leqslant 2^{c-n_0/2} \tag{3.56}$$

for every nonzero coordinate character $\Lambda$. For fixed $c$ and sufficiently large $n_0$, the last bound is at most $2^{-a_0-1}$. If the binary affine span of $\Gamma_c(A)$ has codimension $u$, expanding the indicator of that span in its $2^u$ annihilator characters, exactly as in Lemma 3.42, gives

$$2^{-a_0} \leqslant 2^{-u} + 2^{c-n_0/2}.$$

Hence $u \leqslant a_0 + 1$. The coordinate functions of the honest Gold features, restricted to $A$, consequently have binary span of dimension at least $D_G - a_0 - 1$.

On the right, the projection of $B$ to $(r, t) \in L^2$ has at least $2^{2n_0-b_0}$ elements: every pair $(r, t)$ has at most $|K|^J = 2^{4n_0}$ preimages. The projection thus has density at least $2^{-b_0}$ in $L^2$. Apply Lemma 3.42 over $L$ with width $c + 1$. Its root-bound hypothesis holds for fixed $c$ and sufficiently large $n_0$. We obtain affine-span codimension at most $b_0 + 1$ for

$$\Phi_{c+1}(r, t) = t(1, r, \ldots, r^c) \in L^{c+1}.$$

*If the comparison Gold coefficient is nonzero, recognize the left tampering.* Assume $\mu \neq 0$. Let $\mathsf{U}$ be the binary feature matrix whose row indexed by $x \in A$ concatenates the coordinate vectors of $\Gamma_c(x)$ and $\Gamma_c(f(x))$. Let $\mathsf{V}$ similarly concatenate, for each right input in $B$, the feature vectors $\Phi_{c+1}(r, t)$ and $\Phi_{c+1}(r', t')$, where $(r', t')$ are the first two $L$-words of the tampered right input. The mixed Gold character matrix is

$$\mathsf{U}\,\mathsf{P}\,\mathsf{V}^{\mathsf{T}},$$

where $\mathsf{P}$ is a nondegenerate block-diagonal binary trace pairing on a space of dimension $2D_G$; its two blocks are nondegenerate because $\lambda, \mu \neq 0$. In particular $\mathsf{P}$ is invertible.

The honest block of $\mathsf{U}$ has rank at least $D_G - a_0 - 1$. Every binary coordinate of $\Gamma_c(x)$ is a quadratic Boolean function of $x$, whereas the span of the coordinates of $\Gamma_c(f(x))$ modulo all quadratics on $A$ has dimension $d_c(f; A)$. Thus adjoining the tampered block increases rank by at least this defect:

$$\operatorname{rank} \mathsf{U} \geqslant D_G - a_0 - 1 + d_c(f; A).$$

The honest block alone gives $\operatorname{rank}\mathsf{V} \geqslant D_G - b_0 - 1$. Sylvester's rank inequality, applied to the product above, yields

$$\begin{aligned} k_G &\geqslant \operatorname{rank}(\mathsf{U}\mathsf{P}\mathsf{V}^{\mathsf{T}}) \\ &\geqslant \operatorname{rank}\mathsf{U} + \operatorname{rank}\mathsf{V} - 2D_G \\ &\geqslant d_c(f;A) - a_0 - b_0 - 2. \end{aligned}$$

Therefore

$$d_c(f;A) \leqslant k_G + a_0 + b_0 + 2. \tag{3.57}$$

By Theorem 3.41, there is a subset $A_1 \subseteq A$ on which $f$ agrees with an affine map $\ell : L \to L$ and whose ambient deficiency satisfies

$$a_1 := n_0 - \log_2 |A_1| \leqslant C_{\mathrm{rec}} \left( a_0 + \frac{k_G + a_0 + b_0 + 2}{p} + p + 1 \right) \tag{3.58}$$

for an absolute $C_{\mathrm{rec}}$. Choose the constant $p$ large compared with $A_*$ and $C_{\mathrm{rec}}$, then set $c = 8p$; only after these choices take $\alpha > 0$ sufficiently small. Since $k_G = 8n_0 + 1$ and $s = n_0/A_*$, the right side of (3.58) is at most $s/8$ for all sufficiently large compatible lengths. This choice also ensures $n_0 > 2c$ and the span estimates above.

When $\mu = 0$, the comparison Gold block is absent and no recognition is needed. We may take $A_1 = A$ and use ordinary affine extraction of $S_a$ in the argument below; this case retains at least as much right entropy as the $\mu \neq 0$ case.

*Fix one comparison seed without destroying the honest seed span.* First take $\mu \neq 0$. On $A_1$ we have $f = \ell$, where $\ell$ is affine. For the distinct tags $a, a'$, the affine-in-tag seed lemma gives on the ambient uniform $Z \in L$

$$(S_a(Z), S_{a'}(\ell(Z))) \approx_{2^{-2s}} (U_{K^2}, S_{a'}(\ell(Z))).$$

Put $\beta = |A_1|/|L| = 2^{-a_1}$. For each possible comparison seed value $z'$, let $T_{z'}$ be the set of honest seed values $S_a(x)$ occurring for $x \in A_1$ with $S_{a'}(\ell(x)) = z'$. Then

$$\beta \leqslant \Pr\left[S_a(Z) \in T_{S_{a'}(\ell(Z))}\right] \leqslant \max_{z'} \frac{|T_{z'}|}{2^s} + 2^{-2s}.$$

Since $a_1 \leqslant s/8$, some $z'$ has

$$|T_{z'}| \geqslant 2^{s-a_1-1} \tag{3.59}$$

for large $s$. Restrict the left source to the corresponding nonempty fiber and, if necessary, choose one left input for each honest seed in $T_{z'}$. The comparison seed is now constant but the honest seeds still realize a set of density at least $2^{-a_1-1}$ inside $K^2$. We now use the estimates below to arrive at a contradiction. For $\mu = 0$ there is no comparison seed to fix. Ordinary affine extraction gives $S_a(U_L) \approx U_{K^2}$; applied to the set $A_1 = A$, the same counting argument supplies a set of at least $2^{s-a_0-1}$ honest seed values. The estimates below also apply to this case by using $a_1 = a_0$ with no tampered terms.

*Fix the Gold coefficients on the right and obtain the contradiction.* On the right restrict to a largest fiber of the honest pair $(r,t) \in L^2$ and of the tampered pair $(r',t') \in L^2$ (omit the latter if $\mu = 0$). These four field words reveal at most $4n_0$ bits, so the remaining coefficient-vector set $\mathcal{Y} \subseteq K^J$ has size at least

$$|\mathcal{Y}| \geqslant 2^{6n_0 - b_0 - 4n_0} = 2^{2n_0 - b_0}. \tag{3.60}$$

This is a bound on the number of distinct $Y$ coefficient vectors: for each choice of $Y$ and fixed $(r,t)$ there is only one honest right input, so the projection is injective on that fiber. In the chosen rectangle, both Gold terms depend only on the left input, because their coefficient pairs have been fixed. The tampered tagged term depends only on the right input, because the comparison seed is fixed. Only the honest tagged term remains genuinely mixed.

To make the cancellation precise, let $\mathcal{X}$ be the retained set of short left prefixes in the selected comparison-seed fiber, and let $\mathcal{B}$ be the retained set of *complete* right rows in the chosen coefficient fiber. On the product $\mathcal{X}\times\mathcal{B}$, the preceding fixings let us write the supposedly constant mixed Boolean character in the form

$$\chi_{s_0}(x,w)=L_{\mathrm{loc}}(x)+R_{\mathrm{loc}}(w)+\mathrm{Tr}_{K/\mathbb{F}_2}(\lambda\,\Phi_J(u(x),v(x))\cdot Y(w))=c_\chi\in\mathbb{F}_2. \tag{3.61}$$

Here $(u(x),v(x))=S_a(x)$, $Y(w)$ is the honest $K^J$ coefficient vector of the complete right row $w$, and $\cdot$ is the ordinary $K$-inner product on $K^J$. The function $L_{\mathrm{loc}}$ contains the two Gold contributions (whose honest and tampered right coefficient pairs have been fixed); $R_{\mathrm{loc}}$ contains the tampered tagged contribution (whose comparison seed has been fixed). If $\mu=0$, the corresponding comparison terms are simply absent. Thus no assumption on the right tampering map is needed for this decomposition.

Choose arbitrary $x_1,x_2\in\mathcal{X}$ and $w_1,w_2\in\mathcal{B}$, and abbreviate

$$\begin{gathered}(u_i,v_i)=S_a(x_i),\qquad \Phi_i=\Phi_J(u_i,v_i),\qquad Y_j=Y(w_j),\\ L_i=L_{\mathrm{loc}}(x_i),\qquad R_j=R_{\mathrm{loc}}(w_j),\qquad H_{ij}=\mathrm{Tr}_{K/\mathbb{F}_2}(\lambda\Phi_i\cdot Y_j).\end{gathered}$$

Constancy of $\chi_{s_0}$ on the full product rectangle yields

$$\begin{aligned}L_1+R_1+H_{11}&=c_\chi,\quad L_1+R_2+H_{12}=c_\chi,\\ L_2+R_1+H_{21}&=c_\chi,\quad L_2+R_2+H_{22}=c_\chi.\end{aligned} \tag{3.62}$$

Add these four equalities in $\mathbb{F}_2$. Each $L_i$ occurs *twice*, once with $w_1$ and once with $w_2$, so the left-only contributions cancel. Likewise each $R_j$ occurs *twice*, once with $x_1$ and once with $x_2$, and cancels. The constant on the right contributes $4c_\chi=0$. Consequently,

$$0=H_{11}+H_{12}+H_{21}+H_{22}=\mathrm{Tr}_{K/\mathbb{F}_2}(\lambda(\Phi_1\cdot Y_1+\Phi_1\cdot Y_2+\Phi_2\cdot Y_1+\Phi_2\cdot Y_2))\,.$$

By bilinearity of the $K$-inner product, the four mixed terms factor, giving

$$\mathrm{Tr}_{K/\mathbb{F}_2}\left(\lambda\left[\Phi_J(u_1,v_1)+\Phi_J(u_2,v_2)\right]\cdot(Y_1+Y_2)\right)=0. \tag{3.63}$$

Because the two left prefixes and the two right rows were arbitrary, this is an orthogonality relation between *every* difference of honest scaled-evaluation features and *every* difference of retained right coefficient vectors. The binary span of the differences of honest feature vectors has dimension at least $Jm_K-a_1-2=4n_0-a_1-2$, by Lemma 3.42 applied to the set of seed values in (3.59); multiplication by $\lambda\neq0$ preserves this dimension. On the other hand the binary span of differences of vectors in $\mathcal{Y}$ has dimension at least $\log_2|\mathcal{Y}|\geqslant 2n_0-b_0$. Its annihilator under the nondegenerate trace pairing on $K^J$ therefore has dimension at most $4n_0-(2n_0-b_0)=2n_0+b_0$. Equation (3.63) would force

$$4n_0-a_1-2\leqslant 2n_0+b_0,$$

contradicting $a_1\leqslant s/8$, $b_0\leqslant\alpha M$ and a sufficiently small fixed $\alpha$. Thus no honest-bearing mixed character is constant on the claimed rectangles.

*Exponential error, left source strength, and prefix reuse.* For fixed numerical tags, each Gold term is a sum of $(c+1)n_0$ separated binary products, and each tagged term is a sum of $Jm_K$ such products. Thus every mixed character has global binary rank $O(M)$ with a constant depending only on the fixed starter parameters. Apply the linear-rank approximate-duality lift of Corollary 2.20 to the nonconstancy just proved, using a fixed positive fraction of $\alpha M$ as entropy slack. It gives character bias $2^{-\Omega(M)}$ at a slightly higher min-entropy threshold. Partitioning the honest left source by the sign of its conditional character bias, as described before this lemma, makes the bound hold on average *with that entire source retained*; the small sign classes cost at most an exponential tail.

Finally apply a relative trace $\mathrm{Tr}_{K/K'}$ to a subfield $K' = \mathbb{F}_{2^{M/D_1}} \subseteq K$, choosing the fixed divisor $D_1 = 12A_*t_*$ sufficiently large. Every nonzero character of $K'$ pulls back to a nonzero character of $K$, while the shorter output length makes the Fourier inversion factor harmless. The result has output length $M/D_1 = \Omega(M)$ and error $2^{-\Omega(M)}$, with left-source strength at entropy $(1-\tau_1)M$ for a fixed $\tau_1 > 0$ (one may take $\tau_1 = \alpha/4$ after fixing the slack constants).

The same primitive may be applied to prefixes of longer source words. For clarity, let $Z$ be the honest left prefix and let $X$ be the complete left word. Independently of $Z$, sample a *table* that assigns to each prefix value $z$ a complete word drawn from the conditional distribution $X \mid Z = z$. Evaluating the table at the sampled $Z$ reproduces the original distribution of $X$. For each fixed table, a tampered prefix is a deterministic function of the honest prefix; the two original sides still have independent tables. The left-strong guarantee for the prefix retains both $Z$ and its table and hence retains the complete left word it generates. Averaging over the tables proves the needed statement for arbitrary separate tamperings of the longer inputs. This completion argument will be used at every recursion level. □

### 3.3.3 Doubling the number of comparisons

**The ordinary strong hash.** For output length $v$, parse a source word into coefficients of $P$ over $K = \mathbb{F}_{2^{4v}}$ (pad with zeros) and an $8v$-bit seed into $(u,t) \in K^2$. Use $H_v = \mathrm{Tr}_{K/\mathbb{F}_{2^v}}(tP(u))$. For two distinct words of a fixed length, collision probability on a uniform seed is at most $2^{-v} + d_{\max}2^{-4v}$ by the root bound, where $d_{\max}$ bounds the degrees used. For constant word/field length ratios the degree bound is constant. Cauchy–Schwarz on the average collision probability of the output conditional on the seed gives strong error at most $\frac{1}{2}\sqrt{2^v(2^{-k} + O(2^{-4v}))}$ at min-entropy $k$. In particular $k \geqslant 3v$ suffices for error $O(2^{-v})$.

**Compatible $N$-bit rows.** Similarly, in the following we use this term to denote an arithmetic restriction on the length. Specifically, once $C$ is fixed, the wrapper has only $h = \max\{1, \lceil \log_2 C \rceil\}$ levels. A length $N$ at a wrapper level is *compatible* when

$$p = \frac{N}{8q} \in \mathbb{N}, \qquad w = \mathrm{outlen}(\mathcal{E}_{\mathrm{prev,p}}), \qquad v = \frac{w}{256q} \in \mathbb{N}, \quad q = C+1,$$

its $p$-bit prefixes are compatible at the preceding level, and the fixed tower and output field at the current level have the indicated integer degrees. In particular $w = 256qv$ makes the splittings

$$\mathsf{R} \in \mathbb{F}_{2^{w/2}}^2, \qquad \mathsf{L} \in \mathbb{F}_{2^{4v}}^2, \qquad \mathbb{F}_{2^{4v}} \subseteq \mathbb{F}_{2^{w/2}}$$

valid at the final level; the intermediate polynomial hash uses $\mathbb{F}_{2^{4v}}$, whereas the hash producing $\mathsf{L}$ uses $\mathbb{F}_{2^{32v}}$ and a $64v$-bit seed. Since all ratios and the number of levels are fixed once $C$ is fixed, we may select a single fixed divisibility lattice for the input lengths and choose the field embeddings in advance. The integer $J$ below is chosen *after* this lattice and does not change it.

For the outer extractor, one does not assume an arbitrary condenser row length already belongs to this lattice. Instead, after fixing its integer constants one takes a compatible prefix of length $N = A_C H j \ell \leqslant M$, where $\ell = \lfloor M/(A_C H j) \rfloor$. Thus $0 \leqslant M - N < A_C H j = O_{\delta,C}(1)$, and discarding that bounded number of bits costs only $O_{\delta,C}(1)$ in entropy. The same choice ensures the nested fields $\mathbb{F}_{2^\ell} \subset \mathbb{F}_{2^{j\ell}} \subset \mathbb{F}_{2^{Hj\ell}}$ used in the outer construction. Any further fixed tag-field embedding is arranged as part of this public constant-divisibility setup. "Compatible" never means that the input data have a special algebraic form.

**Theorem 3.44** (Tagged row with adjustable mixed rank)**.** Fix $C \geqslant 1$. For all sufficiently large compatible lengths $N$ as defined above, there are a deficiency $\tau_C > 0$ and native output degree $N/A_C$, both ratios fixed before choosing a margin $K_* > 0$. For each fixed margin the evaluator below has the following property. On every rectangle with side sizes at least $2^{(1-\tau_C)N}$ every honest-bearing mixed character of the row and at most $C$ separate comparisons has binary rank $> K_* N$ whenever the designated fixed tag differs from each comparison tag. Comparison tags may coincide. Every character has global rank $O_{C,K_*}(N)$ and constant field separation over compatible fields, including after the actual fingerprint substitution below.

For the doubling recursion, write $\mathsf{R}$ for the preceding level's output and $\mathsf{L}$ for the new left-hash word. These are intermediate outputs, not input subsets $A, B$. Their names reflect the locality established *after* the transcript fixings in the proof below.

**Construction 3.7 Tagged row for a fixed number of comparisons**

**Ingredients from earlier parts.** Construction 3.6, $H_v$ and Lemma 3.42.

**Public parameters and fixed setup.** Put $q = C+1$, $h = \max\{1, \lceil \log_2 C \rceil\}$. Start with the left-strong one-comparison starter. Apply the following recursion for $h$ levels, using the last formula only at level $h$. All shrinking ratios depend only on $C$. At a level of input length $N$, the preceding level is called on length $p = N/(8q)$ and gives a word of length $w$. Set $v = w/(256q)$. Require integrality by taking compatible lengths.

**Input.** Two rows $x, y$ and a numerical tag $a$ in the innermost starter field.

**Evaluation steps.**

1. Compute $\mathsf{R}$ by running the preceding evaluator with tag $a$ on the two $p$-bit prefixes. Set $P = \mathrm{prefix}_{64v}(\mathsf{R})$ and $\mathsf{L} = H_{8v}(x; P)$.
2. At an intermediate level return $H_v(\mathsf{R}; \mathsf{L})$. At the final level split $\mathsf{L} = (u, b) \in K^2$, $\mathsf{R} = (r, t) \in L^2$, where $K = \mathbb{F}_{2^{4v}} \subseteq L = \mathbb{F}_{2^{w/2}}$. Return

$$\mathrm{Tr}_{L/K}\left(bt(1+ur)^{J-1}\right).$$

Choose $J$ a power of two with $4Jv - w/3 - 5 > K_* N$.

**Output.** A native field word of $4v = N/A_C$ bits. Only $J$ depends on the requested margin.

*Proof.* We distinguish the *statistical induction* used at all intermediate levels from the *restricted-rank argument* used only at the final level. The former is independent of $J$; in particular, no margin-dependent entropy requirement is introduced during the recursion. We use the following notation: execution 0 is the honest pair, while executions $i \geqslant 1$ are arbitrary separate tamperings. Their numerical tags are fixed and the honest tag differs from each comparison tag. Let $q = C + 1$.

*The induction hypothesis and entropy of the prefixes.* Suppose the preceding evaluator has a $w$-bit output and is left-source-strong against at least $t_0$ comparisons, at some fixed near-full entropy rate,

with error $2^{-\Omega(p)}$ on $p$-bit rows. A current level has $N$ input bits on each side and uses $p = N/(8q)$ prefix bits. A source with entropy at least $(1-\tau)N$ has a $p$-bit prefix with min-entropy at least $p - \tau N$, because discarding $N - p$ bits reduces min-entropy by at most $N - p$. We fix $\tau > 0$ small enough that $\tau N \leqslant \frac{1}{2}\tau_{\mathrm{prev}} p$ and $\tau \leqslant 1/16$, where $\tau_{\mathrm{prev}} > 0$ is the preceding level's allowed deficiency rate. Thus the preceding evaluator applies to the prefix distributions with a uniform linear entropy margin. Only finitely many levels are used, so the minimum of these fixed positive choices is again positive and does not depend on $J$.

Partition the at most $2t_0$ comparisons into $T$ and $S$, each of size at most $t_0$. At the current level compute

$$\mathsf{R}_i = \mathcal{E}_{\mathrm{prev}}(x_i^{\mathrm{pre}}, y_i^{\mathrm{pre}}), \quad P_i = \mathrm{prefix}_{64v}(\mathsf{R}_i), \quad \mathsf{L}_i = H_{8v}(x_i; P_i), \qquad i = 0, 1, \ldots, t.$$

The honest $\mathsf{R}_0$ is close to uniform given the $\mathsf{R}_i$ for either of the two groups and given the entire honest left prefix. To justify retaining the *tampered* left prefixes as well, use the completion-table argument at the end of Lemma 3.43: conditioned on a sampled left completion table, every tampered prefix is a deterministic function of the honest prefix. The preceding source-strength statement can therefore retain their complete vector. After averaging the tables, for both $Q = T$ and $Q = S$ we have

$$(\mathsf{R}_0, \mathsf{R}_Q, Z) \approx_{2^{-\Omega(p)}} (U_w, \mathsf{R}_Q, Z), \tag{3.64}$$

where $Z$ is the vector of all left prefixes, honest and tampered. Its total length is at most $qp = N/8$.

*The two-sided transcript and its locality.* Once $Z$ is disclosed, the honest and tampered $\mathsf{R}_i$ depend only on the original right source. Disclose next $\mathbf{P} = (P_0, \ldots, P_t)$, a tuple of at most $64qv = w/4$ bits. The tuple is right-local after $Z$ is fixed. Now, conditional on $(Z, \mathbf{P})$, the $\mathsf{L}_i$ depend only on the original left source; the $\mathsf{R}_i$ remain right-local. All these are deterministic functions of the corresponding original source after the transcript values have been fixed. Consequently every retained positive-probability transcript leaf is a *product* distribution on the two original sides. This fact is the reason for the order of disclosure.

We will repeatedly use a standard min-entropy tail rule. If a random variable $W$ has min-entropy at least $k$ and a message $M$ has at most $2^b$ values, then except on message mass at most $2^{-s}$ the conditional min-entropy of $W$ is at least $k - b - s$: indeed a message of probability at least $2^{-b-s}$ cannot raise any atom above $2^{-k+b+s}$. The same rule applies after any already-fixed product transcript; all error estimates below are averaged over leaves rather than asserted for every exceptionally unlikely leaf.

*Freshness of the new left-local word* $\mathsf{L}_0$. Fix $Z$ and $P_S$. By (3.64) with $Q = S$, $P_0$ is exponentially close to an independent uniform $64v$-bit seed, even given $P_S, Z$. Conditional on these values, the left source and the remaining right-local seed tuple are independent. Revealing $\mathsf{L}_S$ costs at most $8qv$ additional left-side bits, and it does not restrict the right source because $\mathsf{L}_S$ is left-local after $P_S, Z$ have been specified.

The honest left source initially has entropy $(1-\tau)N$. On good transcript mass, the total cost of $Z$, $\mathsf{L}_S$, and two $v$-bit tail allowances is at most $qp + 8qv + 2v$. Thus its residual min-entropy is at least

$$(1-\tau)N - qp - 8qv - 2v > 24v \tag{3.65}$$

for the stipulated fixed ratios and sufficiently large lengths. The seed of $H_{8v}$ is $P_0$, with exactly $64v$ bits, and the ordinary strong-hash calculation preceding this theorem gives error $O(2^{-v})$ at the $24v$-bit entropy threshold. Replace $P_0$ by an independent uniform seed, apply that strong hash bound on each good left conditional distribution, and restore the true seed distribution using (3.64).

Importantly, we can also retain the *whole* vector $\mathbf{P}$ in this comparison. Given $(Z, P_S, \mathsf{L}_S)$, the conditional left-side distribution is the same for every further right-local seed value; the strong-hash error is averaged with respect to the honest seed $P_0$ and is not increased by disclosing auxiliary information about that seed. One can formalize this by first adjoining the entire right-local tuple to the ideal uniform-seed distribution, then attaching the same left conditional distribution in each case. We obtain

$$(\mathsf{L}_0, \mathsf{L}_S, Z, \mathbf{P}) \approx_{2^{-\Omega(v)}} (U_{8v}, \mathsf{L}_S, Z, \mathbf{P}). \tag{3.66}$$

This is the first half of the comparison doubling.

*Enough entropy in* $\mathsf{R}_0$ *for the second ordinary hash.* Use (3.64) with $Q = T$ to replace the joint distribution $(\mathsf{R}_0, \mathsf{R}_T, Z)$ by the distribution with a uniform, independent $\mathsf{R}_0$. Attach the rest of the right input using the original conditional distribution given $(\mathsf{R}_0, \mathsf{R}_T, Z)$, and then attach the independent left side given $Z$. This changes the full experiment by at most its previous extraction error and preserves the conditional product structure. This smoothing viewpoint avoids conditioning on the value of $\mathsf{R}_T$, which need not have high probability in an individual leaf.

In the smoothed experiment $\mathsf{R}_0$ starts with $w$ bits of entropy even given $\mathsf{R}_T, Z$. Disclosing the entire $\mathbf{P}$ can cost at most $w/4$ more bits. After fixing $\mathsf{R}_T$ and $\mathsf{L}_S$ on their respective sides, a comparison output in $T$ is left-local (its $\mathsf{R}_i$ has been fixed), while an output in $S$ is right-local (its $\mathsf{L}_i$ has been fixed). The latter outputs expose at most $qv$ further bits about $\mathsf{R}_0$. Using a $2v$-bit tail slack, its remaining min-entropy on the good product leaves satisfies

$$H_\infty(\mathsf{R}_0 \mid \text{current right-side messages}) \geqslant w - w/4 - qv - 2v > 3v. \tag{3.67}$$

The inequality holds in the smoothed, good-leaf sense; the exceptional mass and the smoothing cost are both exponentially small in $v$.

By (3.66), the honest seed $\mathsf{L}_0$ is fresh against $\mathsf{L}_S, Z, \mathbf{P}$. Conditional on the fixed product transcript, it is left-local and the residual $\mathsf{R}_0$ is right-local. Apply the strong hash $H_v(\mathsf{R}_0; \mathsf{L}_0)$ with the entropy bound (3.67). Keep the $T$-comparison outputs, which are left-local on the fixed $\mathsf{R}_T$ leaf, and the $S$-comparison outputs, which are right-local once $\mathsf{L}_S$ is fixed. The seed-specific averaging argument allows us to retain the entire original left input as well. Replacing smoothed distributions by the actual distributions and restoring the actual comparison marginal costs only the preceding exponentially small errors. Thus

$$\big(H_v(\mathsf{R}_0; \mathsf{L}_0),\ (H_v(\mathsf{R}_i; \mathsf{L}_i))_{i=1}^t,\ X\big) \approx_{2^{-\Omega(v)}} \big(U_v,\ (H_v(\mathsf{R}_i; \mathsf{L}_i))_{i=1}^t,\ X\big). \tag{3.68}$$

This completes the induction for every intermediate level, and doubles the number of allowed comparisons. A bounded number of levels gives an exponentially accurate left-strong statistical evaluator for all the groups needed at the final level.

*The final level: supports rather than statistical extraction.* At the last level, run the same transcript and freshness argument on *uniform distributions* on any rectangle of side sizes $2^{(1-\tau_C)N}$. We now extract support-size information. From (3.64) with $Q = T$, the honest $\mathsf{R}_0$ is close to uniform conditioned on $(\mathsf{R}_T, Z)$. The message $\mathbf{P}$ takes at most $2^{w/4}$ values. For fixed $(\mathsf{R}_T, Z)$, the union over all values of $\mathbf{P}$ of those conditional supports of $\mathsf{R}_0$ having fewer than $2^{2w/3}$ points has size at most

$$2^{w/4} 2^{2w/3} = 2^{11w/12}.$$

A uniform $w$-bit word lies in this union with probability at most $2^{-w/12}$; the statistical approximation adds its exponentially small error. Except on that small joint mass, therefore,

$$|\operatorname{supp}(\mathsf{R}_0 \mid \mathsf{R}_T, Z, \mathbf{P})| \geqslant 2^{2w/3}. \tag{3.69}$$

Similarly (3.66) implies that, except on exponentially small transcript mass, the support of the honest $8v$-bit $\mathsf{L}_0$ given $(\mathsf{L}_S, Z, \mathbf{P})$ contains at least $2^{8v-1}$ points. Indeed, on a leaf with a smaller support, its conditional statistical distance from uniform is at least $1/2$; the average distance in (3.66) is exponentially small. Consequently

$$|\operatorname{supp}(\mathsf{L}_0 \mid \mathsf{L}_S, Z, \mathbf{P})| \geqslant 2^{8v-1} \tag{3.70}$$

on all but exponentially small mass.

Choose a simultaneous good transcript, then fix the comparison words $\mathsf{R}_T$ on the right and $\mathsf{L}_S$ on the left. These are opposite-side restrictions of a product leaf, so they do not reduce the other side's conditional support. We obtain a nonempty product rectangle on which (3.69) and (3.70) both hold. The final comparison terms in $T$ depend only on the left variable, and those in $S$ only on the right variable. In a binary character matrix their total contribution therefore has rank at most two, regardless of how many comparisons occur in either group.

*Rank of the honest geometric-series hash.* Write $\mathsf{L}_0 = (u, b) \in K^2$ with $K = \mathbb{F}_{2^{4v}}$ and $\mathsf{R}_0 = (r, t) \in L^2$ with $L = \mathbb{F}_{2^{w/2}}$. Because $J$ is a power of two, the polynomial identity

$$(1+z)^{J-1} = \sum_{i=0}^{J-1} z^i$$

holds in characteristic two. Hence, for any nonzero character coefficient $\lambda \in K^\times$,

$$\operatorname{Tr}_{K/\mathbb{F}_2}\left(\lambda \operatorname{Tr}_{L/K}(bt(1+ur)^{J-1})\right) = \operatorname{Tr}_{L/\mathbb{F}_2}\left(\lambda \sum_{i=0}^{J-1} (bu^i)(tr^i)\right).$$

This is the nondegenerate absolute-trace pairing between the scaled evaluation vectors

$$\Phi_J(u,b) = b(1, u, \dots, u^{J-1}) \in K^J, \quad \Phi_J(r,t) = t(1, r, \dots, r^{J-1}) \in L^J.$$

The pairing of $K^J$ with $L^J$ is nondegenerate on the $K^J$ side: for nonzero $z \in K^J$ the trace pairing against $L^J$ is not identically zero.

The $\mathsf{L}_0$ support has density at least $1/2$ in $K^2$ by (3.70). Lemma 3.42, with deficiency $d \leqslant 1$, gives affine-span codimension at most two in $K^J$ and hence linear-span dimension at least

$$4Jv - 2.$$

Likewise the $\mathsf{R}_0$ support has density at least $2^{-w/3}$ in $L^2$. Applying the same lemma over $L$ gives affine-span codimension at most $w/3 + 1$ in $L^J$. Both applications satisfy the lemma's root-bound hypothesis for sufficiently large compatible lengths, since $J$ is a *fixed* constant once the desired margin has been selected.

Restricting a nondegenerate pairing to a short-side span of dimension at least $4Jv - 2$ and a long-side span of codimension at most $w/3 + 1$ can decrease its rank by at most that latter codimension. Therefore the honest character matrix has rank at least $4Jv - w/3 - 3$. Subtracting the left-local and right-local comparison contribution costs at most two additional ranks, giving

$$\operatorname{rank}(\text{honest-bearing mixed character}) \geqslant 4Jv - \frac{w}{3} - 5 > K_* N, \tag{3.71}$$

where $J$ was chosen in the public setup. The rectangle was chosen inside an arbitrary starting rectangle of the asserted size; therefore that starting rectangle has rank greater than $K_* N$ as well. This proves the adjustable restricted-rank assertion.

*Global rank, actual tags, and field compatibility.* For each fixed $C$ and $J$, the hashes use only fixed-degree polynomial evaluations, powers, additions, multiplications, and relative traces in fields whose extension ratios are fixed. A fixed-tag binary character is consequently an explicit sum of a constant number of products of one left field-valued function and one right field-valued function. In the outer construction the tag is not fixed but has the form

$$a(x, y) = \iota(P_x(t), P_y(t)) = a_L(x) + a_R(y),$$

where the last equality uses the linearity of $\iota$. Substituting it into $S_a(z) = V_0(z) + aV_1(z)$ gives a sum of separated terms even though the functions $V_0, V_1$ themselves need not be linear or low-degree in their source bits. Subsequent fixed powers and products increase the *number* of separated field terms by a constant factor depending on $C, J$, but not on the input length. Expanding each such field product using trace-dual bases costs at most the binary degree of the common base field, which is $O(N)$. Thus every actual character has global binary rank $O_{C,K_*}(N)$ and an explicit separated encoding.

The required extensions and trace maps are valid because of the length convention preceding this theorem. Taking all bit blocks in fixed bases over the common subfield ensures that prefix operations and restrictions to subfields preserve the separated representation. The finite recursion permits shrinking $\tau_C$ once so that all entropy allowances, smoothing errors, and field-size hypotheses hold simultaneously. Neither $\tau_C$ nor the native output length $4v = N/A_C$ depends on the final width $J$. □

### 3.3.4 Constant-rate non-malleability and separate source strength

**Theorem 3.45** (Fixed-$C$ non-malleability with exponential error)**.** Fix $C \geqslant 1$ and $\delta > 0$ with $\delta \leqslant 1$. There is an explicit polynomial-time map $G : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$ with $m = \Omega_{\delta,C}(n)$ and $\epsilon = 2^{-\Omega_{\delta,C}(n)}$ such that, for independent sources of min-entropy $k \geqslant \delta n$ and any admissible $C$ separate tamperings, writing $V = (G(f_i(X), g_i(Y)))_{i=1}^{C}$, one has simultaneously for the same map

$$\Delta((G(X,Y), V, H), (U_m, V, H)) \leqslant \epsilon \qquad \text{for each } H \in \{X, Y\}.$$

Here $U_m$ is independent of $(V, H)$. Dropping $H$ gives ordinary non-malleability. Every output character has binary rank $O_{\delta,C}(n)$ with explicit separated encodings of that length. There is no entropy condition on comparison images.

**Construction 3.8 Constant-rate fixed-$C$ non-malleable extractor**

**Ingredients from earlier parts.** The strong condenser of Theorem 2.25, the row evaluator of Theorem 3.44, and the forcing identity of Lemma 3.7.

**Public parameters and fixed setup.** Put $q = C + 1$. Instantiate the condenser at rate $\delta/(16q)$, deficiency $\tau_C/64$ and average row error at most $1/(1000q)$. Write $M \geqslant c_D n$ for its row length and $r$ for its power-of-two row count (repeat rows by ignoring extra seed bits if necessary). Choose a fixed integer $H \geqslant 4$ with $4 \mid H$ and $q/(A_C H) \leqslant \tau_C/64$, taking $H$ to be a sufficiently large multiple of all fixed compatibility divisors in the row construction. Specifically, for every sufficiently large integer $d$, require $N = A_C H d$ to be a compatible row length, every working-field degree and prefix or block length within the row evaluator to be an integer multiple of $d$, and the innermost tag field to have binary degree at least $2d$. In particular, $v = Hd/4$ is an integer. These conditions involve only the fixed length ratios of the row construction, which depend on $C$ and are independent of the adjustable column widths. Thus $H$ can be fixed before those widths and before $j$. For a fixed $j$ chosen below use

$$\ell = \lfloor M/(A_C H j) \rfloor, \quad d = j\ell, \quad N = A_C H d, \qquad F_0 = \mathbb{F}_{2^\ell} \subset K_0 = \mathbb{F}_{2^d} \subset F = \mathbb{F}_{2^{Hd}}.$$

The row native field is $F$; the innermost tag field contains $K_0$ and has room for a fixed $K_0$-linear injection $\iota : K_0^2 \to$ tag field. Use whole-subfield-block bases as in the row proof. For large $n$, $M - N < A_C H j$ and $d \geqslant M/(2A_C H)$, so $b = \lceil n/d \rceil \leqslant b_* := \lceil 2A_C H/c_D \rceil$. Choose a power of two $R \geqslant \max\{4, r, 8\binom{q}{2}(b_* - 1)\}$, put $D = R/2$, and take distinct $t_a \in K_0$ for $1 \leqslant a \leqslant R$. Use $i(a) = 1 + ((a-1) \bmod r)$. In increasing order set $K_a = 3 + q \sum_{b' < a} C_{b'}$, where $C_{b'} N$ bounds the rank of each actual advised character of column $b'$. Choose its width by Theorem 3.44. These bounds can be taken before choosing $j$: expand the actual expression in $K_0$-coordinates. Each product of one left and one right field element costs at most $d$ binary rank after a character is applied. The ratios of field degrees to $d$ are fixed, and projection to $F_0$ only pulls a character back to $F$. Thus this finite symbolic expansion gives a valid $C_{b'}$. Choose $j$ from the local bias exponent as in Step 7 of the proof. After fixing $j$, bound the rank of the complete merged output and choose the global bias exponent as in Step 8; only then choose the final projection length as in Step 9.

**Input.** Two original words $x, y$ of length $n$.

**Evaluation steps.**

1. Compute the condenser rows on each source and keep their first $N$ bits. Pad each original input to $b$ coefficients in $K_0$ and denote its coefficient polynomial by $P_x$ or $P_y$.
2. For each $1 \leqslant a < R$, form the numerical tag $\alpha_a = \iota(P_x(t_a), P_y(t_a))$. Run the column-$a$ evaluator on the two rows with index $i(a)$ and tag $\alpha_a$. Trace its output from $F$ to $F_0$ to obtain $W_a$.
3. Return a fixed surjective binary projection of $\sigma_D(W_1, \ldots, W_{2D-1})$ onto $m$ bits.

**Output.** One extractor with both separate source-strength guarantees.

*Proof.* Fix independent sources $X, Y$ as in the statement and an admissible tuple of separate tamperings $(f_i, g_i)_{i=1}^C$. Write $S_X = \mathrm{supp}(X)$ and $S_Y = \mathrm{supp}(Y)$. Since every point of $S_X \times S_Y$ has positive probability, admissibility means

$$(f_i(x), g_i(y)) \neq (x, y) \qquad \text{for every } (x, y) \in S_X \times S_Y \text{ and every } i \in [C].$$

This property is preserved when either support is restricted.

We first prove a *dispersion statement*: every binary mixed character with nonzero coefficient on the designated honest field output is nonconstant on every product rectangle contained in $S_X \times S_Y$ with side sizes at least $2^{\delta n/2}$. We next bound the global binary rank of these actual input-dependent-tag characters and apply the support-relative approximate-duality rank-to-bias

lemma. Finally we use entropy slack to retain either complete original source. The proof-only restrictions and representative tables below are not evaluations performed by $G$.

*Step 1: remove comparison images that have heavy atoms.* Fix a product rectangle $A_X \times A_Y \subseteq S_X \times S_Y$ with $|A_X|, |A_Y| \geqslant 2^{\delta n/2}$. For Steps 1–7, start with the independent uniform distributions on $A_X$ and $A_Y$ and apply the successive source-local restrictions described below. Suppose that a mixed character of the honest and $C$ comparison *field-valued* merger outputs, with nonzero honest coefficient, is constant on this rectangle. Write $q = C + 1$ and set

$$h_{\mathrm{raw}} = \frac{\delta n}{4q}.$$

If the left or right marginal of some active comparison has a value with probability greater than $2^{-h_{\mathrm{raw}}}$, restrict that original side to the preimage of this value. The restriction costs fewer than $h_{\mathrm{raw}}$ bits of min-entropy. The chosen comparison output, after this fixing, is a function of the other original side only. Fix the value of its one-bit character contribution on that other side, at a further cost of at most one bit, and remove this comparison from the character. The remaining character is still constant on a positive-weight product rectangle, and its honest coefficient has not changed.

Recompute the surviving comparison marginals and repeat. Each iteration removes an active comparison, so at most $C$ iterations occur. The total entropy loss on either original side is at most $Ch_{\mathrm{raw}} + C$. Since $C/q < 1$, the honest sources still have min-entropy at least

$$\frac{\delta n}{2} - \frac{C\delta n}{4q} - C \geqslant \frac{\delta n}{4} - O_C(1).$$

All surviving comparison marginals on both sides now have min-entropy at least $h_{\mathrm{raw}}$. This reduction is essential: non-malleability never assumes that a tampering image retains entropy.

*Step 2: obtain fixed distinct execution pairs.* On each original side separately choose a *most probable* pattern of the equality/inequality indicators for every pair among the honest input and the remaining comparison inputs, and condition on that pattern. There are only $O(C^2)$ bits per side, so each chosen pattern has conditional probability at least $2^{-O(C^2)}$; this costs only $O(C^2)$ entropy bits and preserves the product structure. Any two executions now either coincide on that original side everywhere on the restricted support, or differ there everywhere. If two full execution pairs coincide, combine their coefficients in the mixed character. Delete any representative whose combined coefficient becomes zero. The honest representative is not merged with a tampered one, because each admissible tampering has no fixed point as a pair on the original product support. Thus its coefficient remains nonzero. We obtain $r_0 \leqslant q$ surviving representatives with pairwise distinct full input pairs, where every distinct pair of representatives differs on at least one original side throughout the current product distribution.

*Step 3: choose common high-entropy condenser rows.* The strong condenser was instantiated below the entropy threshold of every remaining honest and comparison marginal, so for each such marginal its seeded output table is, on average over the $r$ condenser indices, close to a distribution capped at the prescribed near-full row entropy $h$. Here is the useful elementary form of the capping argument. For a row distribution $P$ on $M$ bits, mark a value $z$ as *accepted* with conditional probability

$$a_P(z) = \min\{1, 2^{-h}/P(z)\}$$

(and accept with probability one at $P(z) = 0$). The accepted subdistribution assigns mass $\min\{P(z), 2^{-h}\}$ to each $z$. Its rejection mass is $\sum_z (P(z) - 2^{-h})_+$, at most the distance of $P$

from the class of distributions with min-entropy at least $h$. Thus the condenser error bounds the average rejection probability, including the random choice of row index.

Introduce these accept/reject indicators for each row and each surviving execution, using coins local to the corresponding original side. The condenser parameters ensure that on either side the expected *fraction of indices with any rejection* is at most $1/1000$ (after summing over the at most $q$ executions). Markov's inequality shows that with probability at least $1 - 16/1000$ at least $15r/16$ indices are accepted for *all* the executions on that side. Fix one indicator pattern of probability at least $(1 - 16/1000)2^{-qr}$ with this property. Since $q, r$ are constants, its probability is bounded below by a positive constant. Conditional on this pattern, every accepted row marginal has maximum atom at most

$$\frac{2^{-h}}{\Pr[\text{chosen pattern}]},$$

because its point mass before normalization is bounded by $2^{-h}$. It therefore loses only $O_{\delta,C}(1)$ bits of min-entropy. Do this independently on the two original sides; all restrictions remain product restrictions. The accepted rows are *common across all surviving executions* on each side.

*Step 4: freeze fingerprint equality patterns, not all their values.* Every original word is represented by its fixed polynomial $P_x(T)$ over $K_0$, of degree less than $b \leqslant b_* = O_{\delta,C}(1)$. For each pair of surviving executions, each original side, and each of the $R$ positions, choose a most probable joint pattern of the Boolean bits telling whether their two evaluations at $t_a$ coincide, and condition on that pattern. There are at most $R\binom{q}{2}$ such bits per side, so the chosen pattern has probability at least $2^{-R\binom{q}{2}}$ and costs only $O_{\delta,C}(1)$ entropy while preserving independence.

For two different execution pairs, at least one of the original sides has different full words everywhere on the restricted support. Let $Z_{ij} \subseteq [R]$ be the set of positions where their fingerprints agree on that side. Because the equality indicators have been fixed, $Z_{ij}$ is the same for every input in the conditioned support, although the difference polynomial itself may vary with that input. Choose any one input in this support, and denote its two distinct full words by $u$ and $v$. Their coefficient polynomials satisfy

$$Q_*(T) := P_u(T) - P_v(T) \not\equiv 0, \qquad \deg Q_* \leqslant b - 1, \qquad Z_{ij} = \{a \in [R] : Q_*(t_a) = 0\}.$$

The fixed evaluation points $t_a$ are distinct, so the root bound gives $|Z_{ij}| \leqslant b - 1$. By injectivity of $\iota$, a collision of the full tags requires agreement of the fingerprints on both sides and hence can occur only in $Z_{ij}$. Thus this pair has a common set of at most $b - 1$ possible tag-collision positions. Taking the union over at most $\binom{q}{2}$ pairs, no more than

$$\binom{q}{2}(b_* - 1) \leqslant R/8$$

column positions suffer any pairwise tag collision.

The balanced row schedule repeats each of the $r$ condenser indices exactly $R/r$ times. Since at least $15r/16$ indices are commonly accepted on each side, the bad data indices exclude at most $R/16$ positions per side, or $R/8$ altogether. After excluding those and the tag-collision positions, at least $3R/4$ of the $R$ positions remain. We do not use position $R$, so among the actual $R - 1 = 2D - 1$ evaluated columns there are at least

$$\frac{3R}{4} - 1 \geqslant D = R/2 \tag{3.72}$$

positions which are simultaneously good for all surviving executions and have pairwise distinct tags. Fix any $D$ of them in increasing order:

$$I = \{a_1 < \cdots < a_D\} \subseteq [2D-1].$$

This set is chosen *once on one actual product subsource*; it is not allowed to depend on the execution, the desired field output, or a later Fourier character.

Truncating each accepted $M$-bit row to its public compatible $N$-bit prefix loses at most $M - N = O_{\delta,C}(1)$ bits. Together with the preceding constant losses, for sufficiently large $n$ every selected row marginal has min-entropy at least $(1 - \tau_C/8)N$.

*Step 5: fix only the numerical tags in the current column.* Consider one selected index $a \in I$. Disclose the $K_0$-valued fingerprints $P_{x_i}(t_a)$ and $P_{y_i}(t_a)$ for all $r_0$ surviving executions. The left disclosures depend only on the left original input; the right disclosures only on the right. Each side therefore reveals at most $qd$ bits. An elementary min-entropy tail bound says that, except on message mass at most $2^{-t}$, conditioning on a message with at most $2^b$ values lowers min-entropy by at most $b + t$. Take $t = \tau_C N/16$. Since the public setup guarantees

$$\frac{qd}{N} = \frac{q}{A_C H} \leqslant \frac{\tau_C}{64},$$

we obtain, outside exponentially small total mass, the row entropy bound

$$\begin{aligned} H_\infty(\text{current designated data row} \mid \text{current fingerprint messages}) &\geqslant (1 - \tau_C/8)N - qd - \tau_C N/16 \\ &\geqslant (1 - \tau_C/2)N. \end{aligned}$$

We fix these *current* fingerprint values only. All current tags become fixed numerical tags with the honest-designated tag distinct from every comparison tag. We never condition on the fingerprint values or evaluated outputs of preceding columns; those remain nonconstant functions to be controlled by their separated-rank bounds.

*Step 6: last-active-column rank dominates the complete prefix.* For each column $b$, the public symbolic expansion of the actual advised evaluator supplies a global binary-character rank bound $C_b N$, uniformly in the source and the tamperings. The widths were chosen successively so that, for column $a$,

$$K_a = 3 + q \sum_{b<a} C_b \tag{3.73}$$

and the row theorem gives restricted mixed rank greater than $K_a N$ at that column. These choices were made with fixed parameters and do not depend on the subsources selected in this proof.

Take a nonzero binary character of the complete vector of the $r_0 D$ selected field outputs. Let $a \in I$ be its last column with a nonzero coefficient and choose one execution whose coefficient there is nonzero. Regard that execution as the designated row for the rank argument. The row distributions of that execution have entropy at least $(1 - \tau_C/2)N$, and its numerical tag differs from every other tag at position $a$. Theorem 3.44 therefore provides restricted rank $> K_a N$ against the other at most $C$ executions, even if their comparisons are arbitrarily dependent on the designated inputs.

We spell out the passage from the original source variables to the designated condensed row. For each row value $u$, sample an original left word from the conditional distribution of the current left subsource given its designated row $u$, and store these samples in a table $T_L(u)$. Sample an analogous independent right table $T_R(v)$. The tables are sampled independently of the designated row values.

Drawing the row values first and then evaluating the tables reproduces exactly the original product distribution. For every fixed pair of tables, each tampered row and each earlier-column output is a separate deterministic function of the designated left and right row values. Separate precomposition cannot increase matrix rank, so all columns preceding $a$ contribute together at most

$$qN \sum_{b<a} C_b$$

to the binary character matrix. The current column has rank $> K_a N$ on every row rectangle at the stipulated threshold. By rank subadditivity, the complete character has restricted rank strictly greater than

$$K_a N - qN \sum_{b<a} C_b = 3N.$$

The same reasoning applies after restricting to any subrectangle of the designated row supports of side size at least $2^{(1-\tau_C)N}$, because the available row entropy has the fixed slack $\tau_C N/2$.

Apply the local linear-rank approximate-duality lift of Corollary 2.20 on the designated product row distribution, then average over representative tables and over the current fingerprint leaves. The exceptional rare-message mass is $2^{-\Omega(N)}$. There are only $D = O_{\delta,C}(1)$ selected columns, each with $N = \Omega_{\delta,C}(n)$, so we obtain a constant $\eta = \eta(\delta, C) > 0$, chosen from the individual-column character bounds independently of $j$, such that every nonzero character $\chi$ of the joint selected-column output obeys

$$\left|\mathbb{E}(-1)^{\chi(\mathbf{W}_I)}\right| \leqslant 2^{-\eta n}, \qquad \mathbf{W}_I \in F_0^{r_0 D}. \tag{3.74}$$

This is freshness relative to the *complete prefix* of selected columns, not merely to a separately chosen earlier output or a fixed earlier transcript.

*Step 7: Fourier inversion and majority forcing.* Let $L_0 = r_0 D\ell$ be the binary length of the joint selected vector. For any prescribed $w \in F_0^{r_0 D}$, Fourier inversion and (3.74) give

$$\Pr[\mathbf{W}_I = w] \geqslant 2^{-L_0}\left(1 - (2^{L_0} - 1)2^{-\eta n}\right). \tag{3.75}$$

Choose the constant divisor $j$ in the public field setup so that $L_0 \leqslant qD\ell \leqslant \eta n/2$ for sufficiently large $n$. The right side of (3.75) is then strictly positive for *every* $w$. Thus one can prescribe independently the values of all $D$ selected columns in all $r_0$ executions while staying on the current product subsource.

Choose arbitrary $\beta_0, \ldots, \beta_{r_0-1} \in F_0$ and prescribe $W_{i,a} = \beta_i$ for every $a \in I$ and every execution $i$. Since $D = R/2$ is a power of two, the coefficient of $T^D$ in

$$(1 + \beta_i T)^D \prod_{a \notin I} (1 + W_{i,a} T)$$

is exactly $\beta_i^D$: in characteristic two, $(1 + \beta_i T)^D = 1 + \beta_i^D T^D$, and the remaining $D - 1$ factors have degree less than $D$. Consequently

$$\sigma_D(W_{i,1}, \ldots, W_{i,2D-1}) = \beta_i^D.$$

The Frobenius map $\beta \mapsto \beta^D$ is a permutation of $F_0$. As the $\beta_i$ vary independently, the tuple of merged field outputs visits *every* point of $F_0^{r_0}$. No nontrivial honest-bearing mixed field character can therefore be constant on the starting rectangle. This is the required dispersion conclusion.

*Step 8: global rank and the exponential-error lift.* It remains important that the evaluated tags depend on the *actual* inputs. At each column,

$$\alpha_a(x,y) = \iota(P_x(t_a), P_y(t_a)) = \alpha_{a,L}(x) + \alpha_{a,R}(y).$$

The affine-in-tag seed is $V_0(x^{\mathrm{pre}}) + \alpha_a(x,y)V_1(x^{\mathrm{pre}})$. Even though $V_0, V_1$ can be nonlinear, this expression has a bounded number of terms separated into left-local and right-local field factors. We now fix $j$ as in Step 7 and expand the completed evaluator in coordinates over $F_0$. In particular,

$$[K_0 : F_0] = j, \qquad [F : F_0] = Hj.$$

All working fields have extension degree over $F_0$ bounded by a constant depending only on $\delta, C, j$. The compatible field bases make coordinate projections and relative traces $F_0$-linear, while field multiplication has a bounded coordinate expansion. The fixed number of recursive field operations and the fixed-degree polynomial $\sigma_D$ therefore give each merged field output a representation

$$\sum_{\nu=1}^{T_{\delta,C,j}} a_\nu(x) b_\nu(y), \qquad a_\nu(x), b_\nu(y) \in F_0,$$

with $T_{\delta,C,j}$ independent of $n$. The same separation bound holds after composition with any separate left and right tampering. For a binary character, each term becomes $\mathrm{Tr}_{F_0/\mathbb{F}_2}(\lambda a_\nu(x) b_\nu(y))$ and has binary matrix rank at most $\ell$ in trace-dual $\mathbb{F}_2$-bases of $F_0$. Summing over the at most $q = C + 1$ executions gives, for every actual honest-bearing mixed character of the complete merged output tuple,

$$\mathrm{rank}_2[\chi(x,y)]_{x,y} \leqslant qT_{\delta,C,j}\ell \leqslant A_{\delta,C,j}n$$

for a constant $A_{\delta,C,j}$ independent of $n$.

The individual-column constants $C_{b'}$ and the local exponent $\eta$ were chosen before $j$. The constant $A_{\delta,C,j}$ for the *complete merger* is chosen only after $j$: multiplying the shortened column outputs may introduce a separation width depending on $[K_0 : F_0] = j$. Since Step 7 fixes $j$ as a function of $\delta, C$, the resulting global rank bound is still $O_{\delta,C}(n)$.

For the approximate-duality application, take the permitted supports to be all nonempty products $A \times B \subseteq S_X \times S_Y$. This class is closed under separate restrictions, and every such restriction preserves admissibility. Steps 1–7 show that every honest-bearing mixed character is nonconstant on each permitted rectangle with $|A|, |B| \geqslant 2^{\delta n/2}$. Together with the global rank bound $A_{\delta,C,j}n$, this verifies the hypotheses of Lemma 2.19 with

$$n_L = n_R = n, \qquad a_0 = b_0 = \delta/2, \qquad a_1 = b_1 = 3\delta/4.$$

The entropy gap on each side is $\delta n/4 > 0$. The lemma therefore gives, uniformly for every such mixed character and every independent pair of sources supported on $S_X$ and $S_Y$ with side min-entropy at least $3\delta n/4$,

$$|\,\mathrm{bias}(\chi)| \leqslant 2^{-\zeta n} \tag{3.76}$$

for a constant $\zeta = \zeta(\delta, C) > 0$, uniform over the admissible supports, tampering maps, and mixed characters. This constant is fixed only after $j$ and the complete-merger rank constant above have been chosen. The final projection length is chosen afterward in Step 9. A nonzero character after the surjective binary projection $\pi : F_0 \to \mathbb{F}_2^m$ pulls back to a nonzero field character, so the same bound applies to the projected outputs.

*Step 9: retain either original source and finish.* Fix such a mixed character $\chi$, and first retain $X$. Put

$$b(x) = \mathbb{E}_Y (-1)^{\chi(x,Y)}.$$

Partition the $X$-space into the two sign classes of $b(x)$. A class with probability at least $2^{-d_s}$, where $d_s = \delta n/4$, has conditional min-entropy at least $\delta n - d_s = 3\delta n/4$; conditioning on that class affects only the left source and preserves its independence from $Y$. Its product support remains contained in $S_X \times S_Y$, so the tamperings remain admissible and the restricted distribution belongs to the permitted class from Step 8. Apply (3.76) to each such class. The two classes of mass below $2^{-d_s}$ contribute at most $2^{1-d_s}$. This yields

$$\mathbb{E}_X |b(X)| \leqslant 2^{-\zeta n} + 2^{1-\delta n/4}. \tag{3.77}$$

The argument is symmetric if we retain $Y$ instead. Fourier inversion of the honest output and the $C$ actual comparison outputs, conditional on the retained original source, now gives

$$\Delta\big((G(X,Y),V,H),(U_m,V,H)\big) \leqslant 2^{qm-1}\big(2^{-\zeta n} + 2^{1-\delta n/4}\big), \qquad H \in \{X,Y\}.$$

We used only characters having a nonzero coefficient on the honest output; characters involving solely $V$ cancel against the actual comparison marginal, which is retained unchanged. Choose the public surjective projection length as in the setup,

$$m = \min\left\{\ell, \left\lfloor \frac{n \min\{\zeta, \delta/4\}}{2q} \right\rfloor\right\}.$$

Since $\ell = \Theta_{\delta,C}(n)$ and $q$ is constant, $m = \Omega_{\delta,C}(n)$, and the last statistical-distance bound is $2^{-\Omega_{\delta,C}(n)}$. The construction itself is polynomial-time for fixed $\delta, C$: all publicly enumerated row schedules and field-operation counts are constant, and the remaining operations are explicit polynomial-time field arithmetic. For the finitely many shorter lengths, the stipulated one-bit constant completion has statistical error $1/2$ and character rank zero; reducing the global positive constants covers this finite range without changing the asymptotic statements. □

**Corollary 3.46** (Separate source strength with linear output)**.** Construction 3.8 retains either original source separately with the full comparison tuple, output $\Omega_{\delta,C}(k)$ and error $2^{-\Omega_{\delta,C}(n)}$.

*Proof.* Use the two choices of $H$ in Theorem 3.45. □

# 4 Entropy-efficient output at constant rate

The construction boxes in this section distinguish the internally generated seed from each seeded extractor's public seed interface. They record all seed and payload lengths explicitly; the collision arguments that follow are analysis, not evaluation steps.

This section first proves ordinary two-source output with additive entropy loss, then source-strong $C$-tampering output, its $C = 0$ ordinary source-strong corollary, and finally sumset output with additive loss. The ordinary concatenation and sumset wrappers share the one-payload lemma and may share the seed of Theorem 3.33. The centered non-malleable wrapper uses the fixed-$C$ theorem from Section 3.3. Each nonempty-output statement specifies its nontrivial exponentially small error range.

## 4.1 Two-source output with additive entropy loss

### 4.1.1 Prerequisite: proof of the one-payload collision lemma

The following weighted argument retains the actual other source. It applies directly to arbitrary min-entropy distributions; no flat-source reduction or assumption on an individual tampered image is required.

**Lemma 4.1** (One-sided source-strong collision recycling)**.** Let $X, Y$ be independent $n$-bit sources of min-entropy at least $k$, put $K = 2^k$, let $G$ be a $d$-bit seed, and put $D = 2^d$. Suppose that

(i) $G$ is one-sided non-malleable against every fixed-point-free left map at component threshold $k-4$ with error $\gamma$, and is an ordinary extractor there with error $\gamma$;

(ii) on the current product distribution, $\Delta((X, G(X,Y)), (X, U_d)) \leqslant \eta$;

(iii) $E : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^p$ is a strong seeded extractor at entropy $k$, with error $\zeta$.

Write $M = 2^p$, and suppose $K \geqslant 16M$. For $0 < \theta < 1$ let $\beta = 3(1+\theta)\zeta/\theta + 2\eta$. Then

$$\Delta((Y, G(X,Y), E(X, G(X,Y))), (Y, U_{d+p})) \leqslant \beta + \frac{1}{2}\sqrt{\theta + 2\beta + 2(1+\theta)D^2\gamma + DM/K}. \tag{4.1}$$

The symmetric conclusion with $X$ retained follows by exchanging the sources and using the right-tampering version of (i).

*Proof.* Write $p_x = \Pr[X = x]$ and $q_y = \Pr[Y = y]$, so $p_x, q_y \leqslant 1/K$. For a numerical seed $v \in \{0,1\}^d$, partition the support of $X$ into hash fibers $A_{v,a} = \{x : p_x > 0,\ E(x,v) = a\}$, of masses $w_{v,a} = \sum_{x \in A_{v,a}} p_x$. Retain the fibers whose masses are at most $(1+\theta)/M$, and denote their union by $A_v$. Write $r_v = \Pr[X \in A_v]$. If $r_v < 1/2$, discard the entire numerical seed $v$.

For an arbitrary probability distribution on $M$ atoms, the mass of atoms larger than $(1+\theta)/M$ is at most $(1+\theta)/\theta$ times its statistical distance from uniform. The strong seeded-extractor guarantee, averaged over numerical uniform seeds, therefore shows

$$D^{-1} \sum_v (1 - r_v) \leqslant (1+\theta)\zeta/\theta.$$

Markov's inequality shows that the discarded numerical seeds have uniform mass at most $2(1+\theta)\zeta/\theta$. The two deletion events are measurable from $(X, v)$ and from $v$, respectively. Hypothesis (ii), applied to the current product distribution itself, transfers each one from a uniform $v$ to $v = G(X,Y)$ at cost at most $\eta$. Thus the distribution $P$ of $(Y, G(X,Y), E(X, G(X,Y)))$ has a surviving subdistribution $\mu \leqslant P$ of mass $t_0 \geqslant 1 - \beta$.

We bound its *conditional* collision energy, weighted by the original $Y$-marginal:

$$\mathcal{C}_Y(\mu) = \sum_{y : q_y > 0} \frac{1}{q_y} \sum_{v,a} \mu(y,v,a)^2.$$

For a retained seed $v$ and a retained fiber $A_{v,a}$, put

$$e_{v,a}(y) = \sum_{x \in A_{v,a}} p_x \mathbf{1}_{\{G(x,y) = v\}},$$

and set $e_{v,a}(y) = 0$ for discarded seeds or fibers. Independence gives $\mu(y,v,a) = q_y e_{v,a}(y)$, and hence

$$\mathcal{C}_Y(\mu) = \sum_y q_y \sum_{v,a} e_{v,a}(y)^2. \tag{4.2}$$

The diagonal terms $x = x'$ contribute at most $\sum_x p_x^2 \leqslant 1/K$, since each raw pair $(x, y)$ has a unique genuine seed.

For a retained numerical seed $v$, define the total weight of ordered distinct pairs in a retained hash fiber by

$$N_v = \sum_{a:\ A_{v,a} \text{ retained}} \sum_{\substack{x,x' \in A_{v,a} \\ x \neq x'}} p_x p_{x'}.$$

Because $r_v \geqslant 1/2$ and there are at most $M$ hash values,

$$N_v \geqslant \frac{r_v^2}{M} - \sum_x p_x^2 \geqslant \frac{1}{4M} - \frac{1}{K} \geqslant \frac{1}{8M}, \qquad N_v \leqslant \sum_{a:\ A_{v,a} \text{ retained}} w_{v,a}^2 \leqslant \frac{1+\theta}{M}.$$

Let $(X_v, X_v')$ be such an ordered pair, sampled with probability $p_x p_{x'}/N_v$. For $x$ in a retained fiber $A_{v,a}$, its first marginal has point mass

$$\Pr[X_v = x] = \frac{p_x(w_{v,a} - p_x)}{N_v} \leqslant \frac{8(1+\theta)}{K} \leqslant \frac{16}{K}.$$

By symmetry the same bound holds for $X_v'$; both marginals have min-entropy at least $k - 4$. The pair is sampled independently of $Y$.

Represent the conditional distribution $X_v' \mid X_v$ by a random fixed-point-free left map, sampled independently of $X_v$ and $Y$: at each point in the support of $X_v$, choose the image according to this conditional distribution, and at other points choose any different image. For each fixed map $f$, hypothesis (i) implies

$$\Pr[G(X_v, Y) = v, G(f(X_v), Y) = v] \leqslant D^{-1} \Pr[G(f(X_v), Y) = v] + \gamma.$$

Average this inequality over the maps. Since the *averaged* marginal of $X_v'$ has entropy at least $k - 4$, ordinary extraction in hypothesis (i) then gives

$$\Pr[G(X_v, Y) = G(X_v', Y) = v] \leqslant D^{-2} + 2\gamma. \tag{4.3}$$

The second marginal need not have high entropy for each *fixed* map; ordinary extraction is applied only after averaging. Independence from $Y$ holds throughout.

Expand the squares in (4.2). For each retained $v$, its off-diagonal contribution is $N_v$ times the probability in (4.3). Set $N_v = 0$ for discarded seeds and sum over all $D$ numerical seeds:

$$\begin{aligned} \mathcal{C}_Y(\mu) &\leqslant \frac{1}{K} + \sum_v N_v(D^{-2} + 2\gamma) \\ &\leqslant \frac{1}{K} + \frac{1+\theta}{DM} + \frac{2(1+\theta)D\gamma}{M}. \end{aligned}$$

Weighted Cauchy–Schwarz against the probability measure $P_Y \times U_{d+p}$, whose masses are $q_y/(DM)$, gives

$$\Delta(\mu, t_0(P_Y \times U_{d+p})) \leqslant \frac{1}{2}\sqrt{DM\mathcal{C}_Y(\mu) - t_0^2}.$$

The distances from $P$ to $\mu$ and from the full ideal distribution to $t_0$ times that ideal distribution cost a total of $1 - t_0 \leqslant \beta$. Finally,

$$t_0^2 = 1 - 2(1 - t_0) + (1 - t_0)^2 \geqslant 1 - 2\beta.$$

Combining this inequality with the collision bound and $DM/K = 2^{d+p-k}$ proves (4.1). The argument applies directly to the given source distributions and retains the original $Y$-marginal exactly. □

**Lemma 4.2** (XOR of two separately source-strong payloads)**.** Let $S = S(X, Y)$ be any $d$-bit function and let $A = E_L(X, S)$, $B = E_R(Y, S)$ each have $p$ bits. If $(Y, S, A)$ is $\xi_L$-close to $(Y, U_d, U_p)$ and $(X, S, B)$ is $\xi_R$-close to $(X, U_d, U_p)$, then $F = (S, A \oplus B)$ is separately source strong, with errors $\xi_L$ upon revealing $Y$ and $\xi_R$ upon revealing $X$.

*Proof.* For fixed numerical $(y, s)$, XOR with $E_R(y, s)$ is a permutation of $\{0,1\}^p$. Applying this deterministic permutation to the honest and ideal distributions preserves their distance, proving the first assertion. The second is the same argument with $X$ retained and $E_L(X, S)$ fixed. □

### 4.1.2 Theorem

**Theorem 4.3** (Near-total output from two independent sources)**.** There are absolute constants $C_0, C_1 > 0$ such that, for every fixed $0 < \delta \leqslant 1$, there are $b_\delta > 0$ and $n_\delta$ with the following property. For $n \geqslant n_\delta$, $\delta n \leqslant k \leqslant n$ integral, and

$$2^{-b_\delta n} \leqslant \varepsilon \leqslant \tfrac{1}{4},$$

there is a deterministic polynomial-time computable function

$$\mathrm{Ext}_{n,k,\delta,\varepsilon} : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}^m$$

such that, for independent $X, Y$ with $H_\infty(X), H_\infty(Y) \geqslant k$,

$$\Delta(\mathrm{Ext}_{n,k,\delta,\varepsilon}(X, Y), U_m) \leqslant \varepsilon, \qquad m \geqslant 2k - C_0 \log(1/\varepsilon) - C_1.$$

Its output has the form

$$\big(S, E_L(X, S), E_R(Y, S)\big), \qquad S = G(X, Y).$$

The two seeded outputs have unequal lengths, and the seed $S$ is retained. For each fixed $\delta$, construction and evaluation are polynomial in $n + \log(1/\varepsilon)$. The $2k$-scale output is not source strong at that length, as shown by Lemma 2.4; Corollary 4.9 separately gives $k - O(\log(1/\varepsilon) + 1)$ source-strong output.

### 4.1.3 Detailed deterministic construction and seed parameters

**Construction 4.1 Ordinary two-source output with additive entropy loss**

**Ingredients from earlier parts.** The one-sided sumset seed of Theorem 3.33 (Construction 3.5); the strong seeded extractors of Lemma 2.23; entropy-slack strongification, Lemma 2.5. Lemma 4.1 is the already proved collision interface used to analyze the first payload.

**Public parameters and fixed setup.** Fix $\delta > 0$, integer $\delta n \leqslant k \leqslant n$, and the error $\varepsilon$ in Theorem 4.3's range. Put $\sigma = \delta/4$, $s = \log(1/\varepsilon)$, and $\zeta = \varepsilon^4/2^{20}$. Instantiate $G_{\Sigma,\sigma}$ from Theorem 3.33 at rate $\sigma$, with at least $c_\sigma n$ output bits. With the absolute constants calibrated below, set

$$d = \left\lceil C_1 \left[ \log^2(n+2) + (s+1)\log\left(2 + \frac{n}{s+1}\right)\right]\right\rceil,$$
$$p = \lfloor k - d - 2s - 6 \rfloor, \qquad q = \lfloor k - A(s+1) \rfloor.$$

Instantiate $E_L, E_R$ from Lemma 2.23 at entropy threshold $k$ and error $\zeta$, with a common $d$-bit seed after ignored padding, and outputs truncated to $p$ and $q$ bits respectively. The parameter verification below ensures $p, q \geqslant 1$ and $d \leqslant c_\sigma n$. Here $q$ is a payload length, not a tampering count.

**Input.** The ordered pair $(x, y) \in \{0,1\}^n \times \{0,1\}^n$.

**Evaluation steps.**

1. Compute the internal seed $S = \mathrm{prefix}_d\, G_{\Sigma,\sigma}(x + y)$.
2. Compute the $p$-bit left payload $A_L = E_L(x, S)$.
3. Using the *same* seed, compute the $q$-bit right payload $A_R = E_R(y, S)$.
4. Return the concatenation $(S, A_L, A_R)$, including all $d$ seed bits.

**Output.** Exactly $m = d + p + q$ bits, with $m \geqslant 2k - (A+2)s - A - 8$ and error at most $\varepsilon$. Only the seed is sum-compatible; the final evaluator reads $x, y$ separately and is not asserted source strong at this output length.

**Not evaluated.** Hash-fiber trimming, collision partners, and the comparison experiment used to append the second payload. No additional random seed is sampled during evaluation.

The independent ordinary constant-rate construction in Section 3.1 is unchanged by this seed choice. A shortened full two-sided one-tampering seed would satisfy the same interface, but is not needed. The one-sided sumset seed supplies non-malleability, its honest marginal supplies ordinary extraction, and entropy slack supplies the required source strength.

### 4.1.4 Appending the second payload

**Corollary 4.4** (Ordinary concatenation from one-payload recycling)**.** Assume Lemma 4.1 for the left payload of length $p$, and let its distance bound be $\xi$. If $E_R$ is a strong seeded extractor for $Y$ with $q$ output bits and error $\zeta_R$, then

$$\Delta((S, E_L(X,S), E_R(Y,S)), U_{d+p+q}) \leqslant \xi + \zeta_R. \tag{4.4}$$

*Proof.* Apply $(y, s, a) \mapsto (s, a, E_R(y, s))$ to the comparison $(Y, S, E_L(X,S)) \approx_\xi (Y, U_d, U_p)$. This gives

$$(S, E_L(X,S), E_R(Y,S)) \approx_\xi (U_d, U_p, E_R(Y, U_d)).$$

The independent seed on the right permits strong extraction from $Y$; attach the independent $U_p$ and use the triangle inequality. □

**Corollary 4.5** (Common error calibration)**.** For $0 < \varepsilon \leqslant 1/4$, the one-payload error is at most $\varepsilon/4$ if

$$\theta = \varepsilon^2/64, \quad \zeta \leqslant \varepsilon^4/2^{20}, \quad \eta \leqslant \varepsilon^2/4096, \quad \gamma \leqslant \varepsilon^2/(512D^2), \quad DM/K \leqslant \varepsilon^2/64.$$

If also $\zeta_R \leqslant \varepsilon^4/2^{20}$, the concatenated output has error less than $\varepsilon$. The bound on $DM/K$ implies $K \geqslant 16M$.

*Proof.* Since $1 + \theta < 2$, the one-payload lemma has $\beta \leqslant \varepsilon^2/1024$. Its radicand is at most

$$\varepsilon^2(1/64 + 1/512 + 1/128 + 1/64) < \varepsilon^2/16.$$

Its distance is therefore at most $\varepsilon^2/1024 + \varepsilon/8 < \varepsilon/4$. Apply Corollary 4.4 for concatenation. □

### 4.1.5 Final parameter substitution and entropy accounting

**Corollary 4.6** (Short-output strongification)**.** If an ordinary $d$-bit two-source extractor works at component threshold $h$ with error $\eta_0$, then at component entropy $k > h$ its error strong in either original source is at most $2^d(\eta_0 + 2^{h-k})$.

*Proof.* This is Lemma 2.5 with zero comparisons. □

Fix any $0 < \delta \leqslant 1$ and an integer $\delta n \leqslant k \leqslant n$, and take $G_{\Sigma,\sigma}$ from Theorem 3.33 at the fixed rate $\sigma = \delta/4$. Write $a = e_\sigma$, $c = c_\sigma$, and $s = \log(1/\varepsilon)$ for the exponential-error and output-rate constants of this sum-compatible seed. Set $G(x, y) = \operatorname{prefix}_d G_{\Sigma,\sigma}(x + y)$. The seed theorem gives the required one-sided guarantee and ordinary extraction with $\gamma \leqslant 2^{-an}$, with no additional loss. For all sufficiently large $n$, $k - 4 \geqslant \sigma n$, as required for the collision-partner sources. Corollary 4.6 gives

$$\eta \leqslant 2^d(2^{-an} + 2^{\sigma n - k}) \leqslant 2^{d+1-a_* n}, \qquad a_* := \min\{a, \delta/2\}. \tag{4.5}$$

Use Lemma 2.23 at error $\zeta = \varepsilon^4/2^{20}$. After changing absolute constants, its seed length is at most $B\left\lceil \log^2(n+2) + (s+1)\log\left(2 + \frac{n}{s+1}\right)\right\rceil$ and its available output is at least $k - A(s+1)$. Choose

$$d = \left\lceil C_1 \left\lceil \log^2(n+2) + (s+1)\log\left(2 + \frac{n}{s+1}\right)\right\rceil\right\rceil$$

with a sufficiently large absolute $C_1$. This dominates the actual seeded extractor seed requirement, and we pad unused seed coordinates. Enlarge $C_1$ also to ensure that the left output below is an admissible truncation. Set

$$p = \lfloor k - d - 2s - 6 \rfloor, \qquad q = \lfloor k - A(s+1) \rfloor. \tag{4.6}$$

Both lengths will be positive in the range now chosen. In particular, $2^p \leqslant 2^k\varepsilon^2/(64 \cdot 2^d)$, as required by Corollary 4.5.

It is enough to ensure

$$d \leqslant cn, \qquad 2d + 2s + 14 \leqslant a_* n, \qquad p, q \geqslant 1. \tag{4.7}$$

Here $a_*, c$ are the already fixed positive constants of the sum-compatible seed, not functions of $s$. The condition $d \leqslant cn$ ensures that the output of $G_{\Sigma,\sigma}$ is long enough for the specified prefix. For $s \leqslant bn$, monotonicity gives

$$\frac{\left\lceil \log^2(n+2) + (s+1)\log\left(2 + \frac{n}{s+1}\right)\right\rceil}{n} \leqslant \frac{\log^2(n+2)}{n} + (b + 1/n)\log\left(2 + \frac{1}{b + 1/n}\right).$$

The right side tends to $b\log(2+1/b)$ as $n\to\infty$, and that expression tends to zero as $b\downarrow 0$. Choose a sufficiently small fixed $b_\delta>0$ to satisfy every linear budget in (4.7), including positivity of both output lengths. Then all budgets hold for large $n$, uniformly for $2\leqslant s\leqslant b_\delta n$.

Equation (4.5) and (4.7) imply the separate strength requirement $\eta\leqslant\varepsilon^2/4096$ and the one-sided error requirement $\gamma\leqslant\varepsilon^2/(512\cdot 2^{2d})$. Apply the collision wrapper and its calibration corollary. The output error is at most $\varepsilon$.

Finally, the retained seed cancels its own length charge:

$$d+p+q\geqslant 2k-(A+2)s-A-8. \tag{4.8}$$

The constants $A+2$ and $A+8$ are absolute seeded-extractor constants. This proves Theorem 4.3. No $\log n$ term remains in the output loss. The internal seed length is not claimed to be optimal. The one-sided sumset theorem supplies the seed. In particular Theorem 4.3 still asserts ordinary extraction, not non-malleability of its full long output.

### 4.1.6 All-error interpretation and evaluation

For a fixed $\delta$, choose $C_\delta$ larger than the constants in (4.8) and larger than $2/b_\delta+2$. When $s>b_\delta n$, the expression $2k-C_\delta(s+1)$ is nonpositive. Returning the empty string is then exactly uniform and satisfies the truncated all-error guarantee $m\geqslant\max\{0,\lfloor 2k-C_\delta(s+1)\rfloor\}$. Enlarge $C_\delta$ once more to cover the finite range $n<n_\delta$. For $n\geqslant n_\delta$ and $s\leqslant b_\delta n$, truncate the constructed output, when necessary, to the claimed nonnegative length. Statistical distance cannot increase under truncation.

For an arbitrary real accuracy request, it is enough to construct for $2^{-\lceil\log(1/\varepsilon)\rceil}$; the added entropy loss is an absolute constant. Thus the algorithm can take the accuracy exponent as an integer. Its seed evaluator consists of the fixed condenser, a constant number of field powers and traces, and a fixed elementary symmetric polynomial. Its second stages use Lemma 2.23. All work is polynomial in $n+\log(1/\varepsilon)$ for fixed rate. Colorings, representative tables, source pruning, and subsource selection occur only in the proof.

The final two-source wrapper is not asserted to preserve the seed's $O(n)$ character rank or special inner-product form. That property is used inside the seed construction, where its role has been proved explicitly.

## 4.2 Source-strong non-malleable output with additive entropy loss

Let $C\geqslant 0$ be fixed. We use the $(2C+1)$-tampering extractor of Theorem 3.45 at a smaller fixed entropy rate, shorten it using Lemma 2.5, and use the strong seeded extractor of Lemma 2.23, with its absolute constants $A,B$. The case $C=0$ means an empty comparison tuple; its short seed still uses one-comparison non-malleability. The centered recycling lemma below is a standalone implication from these seed and seeded-extractor interfaces.

### 4.2.1 Prerequisite with proof: centered recycling under actual leakage

We first prove a slightly more general statement allowing arbitrary source-local payload leakage selected by the comparison seeds. The large posterior distributions and collision graphs below are proof objects; they are never computed by the evaluator.

**Lemma 4.7** (Centered recycling with actual leakage)**.** Let $X,Y$ be independent flat sources on sets $\mathcal{A},\mathcal{B}$ of size $K=2^k$. Put

$$D=2^d,\qquad M=2^p,\qquad L=DM=2^m,\qquad m=d+p.$$

Suppose $k \geqslant h$ and $G : \{0,1\}^n \times \{0,1\}^n \to [D]$ is non-malleable against up to $R = 2C+1$ separate tamperings, with error $\eta$, strong in either source separately, whenever both source min-entropies are at least $h$. Fix admissible $(f_i, g_i)_{i=1}^C$, and write

$$S_0 = G(X,Y), \qquad \bar{S} = (G(f_i(X), g_i(Y)))_{i=1}^C.$$

For each numerical $\bar{s} \in [D]^C$ let $a_{\bar{s}} : \mathcal{A} \to [M]^C$ be arbitrary, and let

$$T = (\bar{S}, a_{\bar{S}}(X))$$

be the actual leakage tuple. Let $0 < \alpha, \beta < 1$. Suppose $E : \{0,1\}^n \times [D] \to [M]$ is a strong seeded extractor of error $\zeta$ at entropy

$$\kappa = k - Cm - \log \frac{1}{\alpha\beta}. \tag{4.9}$$

Then

$$\begin{aligned} &\Delta\big((Y,T,S_0,E(X,S_0)),(Y,T,U_d,U_p)\big) \\ &\quad \leqslant 2\beta + 3\alpha + 3\zeta + \frac{\eta}{2} + \frac{1}{2}\sqrt{\Delta}, \end{aligned} \tag{4.10}$$

where

$$\boxed{\Delta = (2C+1)\frac{L^{C+1}}{K} + \frac{2D^{C+2}L^C\,2^h}{\alpha^2 K} + \frac{4\eta D^{2C+2}}{\alpha^2}.} \tag{4.11}$$

All variables $Y, T$ on the ideal side have their original joint distribution.

**Posteriors and an independently seeded reference** Fix a numerical tail label $t = (\bar{s}, \bar{a})$. Define

$$A_t = \{x \in \mathcal{A} : a_{\bar{s}}(x) = \bar{a}\}, \qquad a_t = |A_t|.$$

For each fixed $\bar{s}$ these sets partition $\mathcal{A}$, so

$$\sum_t a_t = D^C K. \tag{4.12}$$

For $x \in A_t$ put

$$w_t(x) = \Pr_Y[\bar{S}(x,Y) = \bar{s}], \qquad \lambda_t = \Pr[T = t], \qquad N_t(y) = |\{x \in A_t : \bar{S}(x,y) = \bar{s}\}|.$$

Use $w_t(x) = 0$ outside $A_t$. The basic identities are

$$\sum_x w_t(x) = K\lambda_t, \qquad \Pr[X = x \mid T = t] = \frac{w_t(x)}{K\lambda_t}, \qquad \Pr[Y = y, T = t] = \frac{N_t(y)}{K^2}. \tag{4.13}$$

We omit zero-probability labels. Write $P_t$ for the posterior distribution $X \mid T = t$.

Let $P$ be the actual distribution of $(Y,T,S_0,E(X,S_0))$. Construct a reference distribution $\mathcal{R}$ by sampling the original $(X,Y,T)$, then an independent uniform $S \in [D]$, and outputting $(Y,T,S,E(X,S))$. Finally, let

$$Q(y,t,s,a) = \frac{\Pr[Y = y, T = t]}{DM} = \frac{N_t(y)}{K^2 L}.$$

Thus both $\mathcal{R}$ and $Q$ preserve the actual $(Y,T)$ marginal. The task is to compare $P$ first with $\mathcal{R}$.

Call $t$ good if

$$\lambda_t \geqslant \beta L^{-C}. \tag{4.14}$$

Bad labels have total mass at most $\beta$. On a good label,

$$\max_x P_t(x) \leqslant (K\lambda_t)^{-1} \leqslant 2^{-(k-Cm-\log(1/\beta))}.$$

In particular, $P_t$ has min-entropy at least $\kappa$. For a good $t$ define

$$\psi_t(y) = \mathbf{1}[N_t(y) \geqslant \alpha K \lambda_t]. \tag{4.15}$$

The actual mass of pairs with $N_t(y) < \alpha K \lambda_t$ is at most $\alpha$:

$$\sum_t \sum_{y: N_t(y) < \alpha K \lambda_t} \frac{N_t(y)}{K^2} \leqslant \sum_t \alpha \lambda_t = \alpha.$$

For every surviving $(y, t)$, the conditional distribution $X \mid (Y = y, T = t)$ is uniform on a set of size

$$N_t(y) \geqslant \alpha\beta K L^{-C} = 2^{\kappa}.$$

Strong seeded extraction therefore gives

$$\Delta(\mathcal{R}, Q) \leqslant \zeta + \alpha + \beta. \tag{4.16}$$

This step uses an independent seed and the actual tail fiber; it does not apply $G$ to a conditioned two-source distribution.

**Posterior trimming without a seeded-error multiplier** Discard a raw pair $(X, T)$ if

$$w_T(X) < \alpha D^{-C}. \tag{4.17}$$

This costs at most $\alpha$. Indeed, for each fixed $x$ there is only one possible $\bar{a} = a_{\bar{s}}(x)$ for each of the $D^C$ numerical seed tuples $\bar{s}$. Hence

$$\frac{1}{K} \sum_x \sum_{t: w_t(x) < \alpha D^{-C}} w_t(x) \leqslant \alpha.$$

The estimate is for the actual $(X, T)$ distribution, which is shared by $P$ and $\mathcal{R}$ before the honest seed is evaluated.

For good $t$ and numerical $s$ define the hash-fiber masses

$$r_{t,s}(a) = \Pr_{P_t}[E(X, s) = a].$$

Discard points with $r_{t,s}(E(x, s)) > 2/M$. For any distribution $r$ on $[M]$, the mass of its atoms exceeding $2/M$ is at most $2\Delta(r, U_M)$: on those atoms $r(a) - 1/M > r(a)/2$. Since $P_t$ has entropy at least $\kappa$, averaging over a uniform $s$ shows that this deletion has probability at most $2\zeta$ under $\mathcal{R}$, after summing over good $t$.

The same deletion under $P$ costs at most $2\zeta + \eta$. To see this, use the source-strong seed comparison retaining $X$:

$$(X, \bar{S}, S_0) \approx_\eta (X, \bar{S}, U_d).$$

Both $T = (\bar{S}, a_{\bar{S}}(X))$ and the heavy-fiber deletion test are deterministic functions of the retained variables and the honest seed. This is the only transfer needed for trimming. In particular, no factor $D^C$ multiplies $\zeta$.

For good $t$ set

$$\phi_{t,s}(x) = \mathbf{1}[x \in A_t]\, \mathbf{1}[w_t(x) \geqslant \alpha D^{-C}]\, \mathbf{1}[r_{t,s}(E(x,s)) \leqslant 2/M]. \tag{4.18}$$

Let $\mu \leqslant P$ and $\nu \leqslant \mathcal{R}$ be the subdistributions obtained by keeping good $t$, $\psi_t(y) = 1$, and $\phi_{t,s}(x) = 1$, using the actual honest seed for $\mu$ and the independent seed for $\nu$. The mass losses satisfy

$$b_P := 1 - \|\mu\|_1 \leqslant \beta + 2\alpha + 2\zeta + \eta, \tag{4.19}$$

$$b_R := 1 - \|\nu\|_1 \leqslant \beta + 2\alpha + 2\zeta. \tag{4.20}$$

The cutoffs defining $\phi_{t,s}$ are source local once $t, s$ are numerical. They use the posterior $P_t$, averaged over $Y$, not the posterior conditioned on a particular $Y = y$.

**The centered energy identity** Put

$$h_s(x,y) = \mathbf{1}[G(x,y) = s] - D^{-1}.$$

For good $t = (\bar{s}, \bar{a})$ and $a \in [M]$ define

$$B_{t,s,a}(y) = \sum_{\substack{x \in A_t \\ E(x,s)=a}} \phi_{t,s}(x)\, \mathbf{1}[\bar{S}(x,y) = \bar{s}]\, h_s(x,y).$$

Then, pointwise,

$$(\mu - \nu)(y,t,s,a) = K^{-2} \psi_t(y) B_{t,s,a}(y).$$

Consequently,

$$\mathcal{E} := \sum_{y,t,s,a} \frac{(\mu-\nu)(y,t,s,a)^2}{Q(y,t,s,a)} = \frac{L}{K^2} \sum_{t \text{ good}} \sum_{y: N_t(y) > 0} \frac{\psi_t(y)}{N_t(y)} \sum_{s,a} B_{t,s,a}(y)^2. \tag{4.21}$$

Zero-mass atoms are omitted. Weighted Cauchy–Schwarz gives

$$\frac{1}{2}\|\mu - \nu\|_1 \leqslant \frac{1}{2}\sqrt{\mathcal{E}}. \tag{4.22}$$

The reference is not uniform at this stage. Centering by $D^{-1}$ is what makes the large-graph term vanish under the non-malleable seed replacement.

**Diagonal and cross-input exceptions** Expand the squares in (4.21) as ordered pairs $(x, x')$. Call a pair exceptional if

$$x = x', \qquad \text{or} \qquad x' = f_i(x), \qquad \text{or} \qquad x = f_i(x') \quad \text{for some } i. \tag{4.23}$$

For every $x, x', y$,

$$\sum_s |h_s(x,y) h_s(x',y)| \leqslant \left(\sum_s h_s(x,y)^2\right)^{1/2} \left(\sum_s h_s(x',y)^2\right)^{1/2} = 1 - D^{-1} \leqslant 1. \tag{4.24}$$

The hash equality and $\phi$ factors can only reduce this absolute-value bound.

For each fixed $(y,t)$, the diagonal contributes at most $N_t(y)$ ordered pairs. The relation $x' = f_i(x)$ also contributes at most $N_t(y)$ pairs, by counting $x$; the relation $x = f_i(x')$ contributes at most $N_t(y)$ by counting $x'$. This remains true for noninjective $f_i$. There are at most $KL^C$ supported $(y,t)$. Thus the exceptional contribution, bounded in absolute value, is at most

$$\mathcal{E}_{\mathrm{exc}} \leqslant (2C+1)\frac{L^{C+1}}{K}. \tag{4.25}$$

The cross-input exceptions ensure that all subsequent composed comparison maps are admissible.

**Source-local collision graphs** For each good $t$ and numerical $s$, form the symmetric directed graph $\Gamma_{t,s}$ of ordered pairs $x, x' \in A_t$ satisfying

$$\phi_{t,s}(x) = \phi_{t,s}(x') = 1, \qquad E(x,s) = E(x',s),$$

with every exceptional pair in (4.23) removed. Let $J_{t,s} = |\Gamma_{t,s}|$.

Every retained hash fiber has cardinality at most

$$B_t := \frac{2D^C K\lambda_t}{\alpha M}. \tag{4.26}$$

Indeed, each surviving $x$ has $P_t(x) \geqslant \alpha/(D^C K\lambda_t)$, while the total $P_t$ mass of its retained fiber is at most $2/M$. Hence every vertex of $\Gamma_{t,s}$ has degree at most $B_t$, and

$$J_{t,s} \leqslant a_t B_t. \tag{4.27}$$

Call a graph small if $J_{t,s} < 2^h B_t$. On the retained $(y,t)$, $N_t(y)^{-1} \leqslant (\alpha K\lambda_t)^{-1}$. Using $|h_s h_s'| \leqslant 1$, the absolute contribution of one small graph to (4.21) is at most

$$\frac{LJ_{t,s}}{\alpha K^2\lambda_t} \leqslant \frac{2D^{C+1}2^h}{\alpha^2 K}.$$

There are at most $DL^C$ graph labels. Therefore

$$\mathcal{E}_{\mathrm{small}} \leqslant \frac{2D^{C+2}L^C\,2^h}{\alpha^2 K}. \tag{4.28}$$

No seed theorem is applied to these small graphs.

**Large graphs and admissible extra comparisons** For a large graph, sample $(V,V')$ uniformly from $\Gamma_{t,s}$, independently of the original $Y$. Its first marginal has maximum atom at most $B_t/J_{t,s} \leqslant 2^{-h}$. The second marginal has the same bound, although only the first is needed below.

Represent the conditional distribution $V' \mid V$ as a random deterministic table $v \mapsto \rho(v)$, sampled independently of $V, Y$. Each table chooses only neighbors of $v$ on the support of $V$. For every fixed table the honest pair $(V,Y)$ has the following $2C+1$ comparisons:

$$(\rho(V), Y), \qquad (f_i(V), g_i(Y)), \qquad (f_i(\rho(V)), g_i(Y)), \quad 1 \leqslant i \leqslant C. \tag{4.29}$$

The first comparison is distinct because $V' \neq V$. The middle comparisons satisfy the original admissibility condition. The last comparisons have $f_i(V') \neq V$ by (4.23). All maps are separate and are chosen independently of $Y$.

Apply strong non-malleability retaining $Y$, then average over the tables. It replaces $G(V,Y)$ by an independent uniform seed at distance at most $\eta$, while retaining

$$Y, \quad G(V',Y), \quad (G(f_i(V),g_i(Y)))_i, \quad (G(f_i(V'),g_i(Y)))_i.$$

All the following factors except $h_s(V,Y)$ are functions of these retained variables:

$$h_s(V',Y)\,\mathbf{1}[\bar{S}(V,Y)=\bar{S}(V',Y)=\bar{s}]\,\frac{\psi_t(Y)}{N_t(Y)}.$$

Set the quotient to zero where $N_t(Y)=0$. Its absolute value is at most $(\alpha K\lambda_t)^{-1}$. Under the independent replacement, the expectation of $h_s(V,Y)$ is zero. The standard bounded-test consequence of statistical distance therefore gives

$$\left|\mathbb{E}\left[h_s(V,Y)h_s(V',Y)\mathbf{1}[\bar{S}(V,Y)=\bar{S}(V',Y)=\bar{s}]\,\frac{\psi_t(Y)}{N_t(Y)}\right]\right| \leqslant \frac{2\eta}{\alpha K\lambda_t}. \tag{4.30}$$

This is where the previous main-term difficulty disappears. Neither the graph nor the random table is selected using $Y$.

Multiplying (4.30) by $KJ_{t,s}$ restores the sum over $y$ and ordered pairs. Hence

$$\mathcal{E}_{\text{large}} \leqslant \frac{2\eta L}{\alpha K^2}\sum_{t,s}\frac{J_{t,s}}{\lambda_t}.$$

By (4.12), (4.26), and (4.27),

$$\sum_{t,s}\frac{J_{t,s}}{\lambda_t} \leqslant \sum_{t,s}\frac{a_tB_t}{\lambda_t} \leqslant \frac{2D^{2C+1}K^2}{\alpha M}.$$

It follows that

$$\mathcal{E}_{\text{large}} \leqslant \frac{4\eta D^{2C+2}}{\alpha^2}. \tag{4.31}$$

Only the exponentially accurate seed error incurs this power of $D$.

**Completion of the centered lemma** Equations (4.25), (4.28), and (4.31) give $\mathcal{E}\leqslant\Delta$. Using half-$\ell_1$ distance also for subdistributions, the triangle inequality yields

$$\begin{aligned}\Delta(P,Q) &\leqslant \frac{b_P}{2}+\frac{1}{2}\|\mu-\nu\|_1+\frac{b_R}{2}+\Delta(\mathcal{R},Q)\\ &\leqslant 2\beta+3\alpha+3\zeta+\frac{\eta}{2}+\frac{1}{2}\sqrt{\Delta}.\end{aligned}$$

This proves Lemma 4.7. The final ideal distribution retains the original comparison marginal. Every deletion used in the intermediate subdistributions is included in the displayed error.

### 4.2.2 Main theorem and complete retained-seed XOR evaluator

**Theorem 4.8** (Source-strong endpoint)**.** For every fixed $\delta>0$ and integer $C\geqslant 0$ there is $b_{\delta,C}>0$ such that, for sufficiently large $n$, integer $\delta n\leqslant k\leqslant n$, and

$$2^{-b_{\delta,C}n}\leqslant\varepsilon\leqslant 1/4,$$

there is an explicit polynomial-time map $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$ with

$$m \geqslant \frac{k}{C+1} - O(\log(1/\varepsilon) + 1)$$

such that, for every independent min-entropy-$k$ pair and every admissible $C$-tuple,

$$(F(X,Y), (F(f_i(X), g_i(Y)))_{i=1}^C, Y) \approx_\varepsilon (U_m, (F(f_i(X), g_i(Y)))_{i=1}^C, Y), \tag{4.32}$$

$$(F(X,Y), (F(f_i(X), g_i(Y)))_{i=1}^C, X) \approx_\varepsilon (U_m, (F(f_i(X), g_i(Y)))_{i=1}^C, X). \tag{4.33}$$

The uniform variable is independent of everything else displayed. The same function satisfies both comparisons. The additive output-loss constants can be taken absolute; the error-range and running-time constants may depend on $\delta, C$.

**Construction 4.2 Source-strong $C$-tampering retained-seed XOR**

**Ingredients from earlier parts.** The fixed-comparison extractor of Theorem 3.45 (Construction 3.8); Lemma 2.5; the strong seeded extractor of Lemma 2.23; and the centered recycling interface of Lemma 4.7.

**Public parameters and fixed setup.** Fix $\delta > 0$, $C \geqslant 0$, integer $\delta n \leqslant k \leqslant n$, and target $\varepsilon$ in Theorem 4.8's range. First put $q = C+1$, $R = 2C+1$, and $\sigma = \delta/(8q)$. Instantiate a base extractor $G_0$ from Theorem 3.45 with $R$ *comparisons* at rate $\sigma$. Set

$$h_0 = \left\lceil \frac{\delta n}{8q} \right\rceil, \quad h = \left\lceil \frac{\delta n}{4q} \right\rceil, \quad u = \lceil \log(1/\varepsilon) \rceil + 10, \quad r_C = \lceil \log(2C+1) \rceil.$$

Using the constants $A, B$ of Lemma 2.23, with $A$ a positive integer, choose

$$\begin{aligned} d &= \left\lceil B \left\lceil \log^2(n+2) + (u+1) \log\left(2 + \frac{n}{u+1}\right) \right\rceil \right\rceil, \\ m &= \left\lfloor \frac{k - (A+4)(u+1) - r_C}{q} \right\rfloor, \\ p &= m - d, \qquad \kappa = k - Cm - 2u. \end{aligned}$$

Define $G = \mathrm{prefix}_d G_0$. Instantiate $E$ at entropy threshold $\kappa$ and error $2^{-u}$, pad its seed interface to $d$ bits, and truncate its output to $p$ bits. The bounds (4.36)–(4.38) certify that these calls fit. Strongification from threshold $h_0$ to $h$ changes only the guarantee, not the evaluation of $G$.

**Input.** $(x, y) \in \{0,1\}^n \times \{0,1\}^n$.

**Evaluation steps.**

1. Compute $S = G(x, y)$.
2. Compute $A_L = E(x, S)$ and $A_R = E(y, S)$, both of length $p$.
3. Return the retained seed concatenated with the bitwise XOR:

$$S = G(x,y), \qquad F(x,y) = \big(S, E(x,S) \oplus E(y,S)\big). \tag{4.34}$$

**Output.** Exactly $m = d + p$ bits. Theorem 4.8 gives error at most $\varepsilon$, $m \geqslant k/(C+1) - O(\log(1/\varepsilon) + 1)$, and strength in either source separately for this same function.

**Not evaluated.** The $2C+1$ auxiliary tamperings, actual-leakage posteriors, collision graphs, and source-dependent bijections. The evaluator makes one seed call and two seeded-extractor calls, not tampered-input calls.

For nonintegral $k \geqslant \delta n$, put $k' = \lfloor k \rfloor$ and invoke the theorem with rate parameter $\delta/2$, not $\delta$: for $n \geqslant 2/\delta$, one has $k' \geqslant (\delta/2)n$. Use its error-range constant $b_{\delta/2,C}$ and length cutoff. The output bound is $k'/(C+1) - O(\log(1/\varepsilon) + 1)$, so the rounding costs at most $1/(C+1)$ additional bit and is absorbed in the stated loss.

### 4.2.3 Returning to the symmetric evaluator

Let $F$ be (4.34). Suppose $Y = y$ is retained. For every output, honest or tampered, its seed is included in the output. Therefore the transformations

$$(s, z) \longmapsto (s, z \oplus E(y, s))$$

for the honest output and

$$(s_i, z_i) \longmapsto (s_i, z_i \oplus E(g_i(y), s_i))$$

for comparison $i$ are bijections determined by the retained $y$ and the displayed seeds. They transform the honest output to $(S_0, E(X, S_0))$ and the comparison tuple to

$$T = (\bar{S}, (E(f_i(X), S_i))_{i=1}^{C}).$$

This is precisely the leakage in Lemma 4.7, with $a_{\bar{s}}(x) = (E(f_i(x), s_i))_i$. The honest uniform distribution is preserved by the same bijection. Thus the lemma proves (4.32) with its displayed error.

To prove (4.33), exchange the two sources and their tampering maps. Apply the same lemma to $G^{\mathrm{op}}(x, y) = G(y, x)$, using the other source-strength guarantee of $G$. The evaluator remains exactly (4.34); only its analysis is exchanged.

For general independent sources of min-entropy at least integer $k$, decompose each into a convex combination of flat sources on $2^k$ points. Apply the bound to every product component with the same evaluator and maps, then average. The ideal distribution retains each component's actual source and comparison tuple, so averaging gives their original joint distribution. Admissibility persists on every component of positive weight.

### 4.2.4 Parameter calculation

**Obtaining the short source-strong seed** Use the atomwise entropy-slack strongification in Lemma 2.5.

Fix $q = C + 1$, $R = 2C + 1$, and choose Theorem 3.45 at rate $\sigma = \delta/(8q)$. Write its output and error constants as $c_0, a_0 > 0$, and put

$$h_0 = \left\lceil \frac{\delta n}{8q} \right\rceil, \qquad h = \left\lceil \frac{\delta n}{4q} \right\rceil, \qquad a = \min\left\{ a_0, \frac{\delta}{8q} \right\}.$$

Since $R + 1 = 2q$, Lemma 2.5 gives, for $d \leqslant c_0 n$,

$$\eta \leqslant D^{2q}(2^{-a_0 n} + 2^{h_0 - h}) \leqslant 2^{\,2+2qd-an}. \tag{4.35}$$

The same $G$ works at threshold $h$ for all comparisons needed in the centered lemma.

**Payload length and all three error terms** Set

$$s = \lceil \log(1/\varepsilon) \rceil, \qquad u = s + 10, \qquad \alpha = \beta = \zeta = 2^{-u}.$$

Enlarge $A$ to a positive integer and put

$$r_C = \lceil \log(2C+1) \rceil, \qquad m = \left\lfloor \frac{k - (A+4)(u+1) - r_C}{q} \right\rfloor, \qquad p = m - d.$$

Take $d$ to be the ceiling of the bound in (2.9), with $s = u$. Unused seeded-extractor seed bits can be ignored. Use $E$ at threshold

$$\kappa = k - Cm - 2u.$$

Its output is available because

$$\begin{aligned} \kappa - p &= k - qm + d - 2u \\ &\geqslant (A+4)(u+1) + r_C + d - 2u \geqslant A(u+1). \end{aligned}$$

Choose the positive error-range constant $b_{\delta,C}$ sufficiently small, then $n$ sufficiently large, to ensure

$$d \leqslant c_0 n, \qquad p \geqslant 1, \tag{4.36}$$

$$4qd + 4u + 4 \leqslant an, \tag{4.37}$$

$$k - Cm - (C+2)d - h \geqslant 4u + 1. \tag{4.38}$$

These choices are simultaneous. Indeed, for $u \leqslant b_{\delta,C} n + O(1)$, the seed-length bound divided by $n$ is at most

$$B\frac{\log^2(n+2)}{n} + B\left(b_{\delta,C} + O(1/n)\right) \log\left(2 + \frac{1}{b_{\delta,C} + O(1/n)}\right) + O(1/n),$$

which can be made arbitrarily small. Also, $k - Cm \geqslant k/q \geqslant \delta n/q$ and $h \leqslant \delta n/(4q) + 1$, leaving a fixed positive linear margin in (4.38). Finally $m/n$ stays bounded away from zero when $b_{\delta,C}$ is sufficiently small.

The three terms in (4.11) are each at most $2^{-2u}$. For the first,

$$(2C+1)2^{qm-k} \leqslant 2^{-(A+4)(u+1)} \leqslant 2^{-2u}.$$

For the second, (4.38) gives

$$2^{1+2u+(C+2)d+Cm+h-k} \leqslant 2^{-2u}.$$

For the third, (4.35) and (4.37) imply

$$\eta \leqslant 2^{-4u-2qd-2}, \qquad 4\eta\, 2^{2u+2qd} \leqslant 2^{-2u}.$$

Consequently Lemma 4.7 has error at most

$$8 \cdot 2^{-u} + \frac{\eta}{2} + \frac{\sqrt{3}}{2} 2^{-u} < 10 \cdot 2^{-u} < \varepsilon.$$

The symmetric argument has the identical bound, proving Theorem 4.8.

Since $r_C \leqslant C + 1 = q$, the output formula gives

$$m \geqslant \frac{k}{C+1} - \frac{(A+4)(u+1)}{C+1} - 2 = \frac{k}{C+1} - O(\log(1/\varepsilon) + 1),$$

with absolute additive-loss constants. Evaluation calls $G$ once and $E$ twice, hence is polynomial time.

## 4.3 Corollary: ordinary source-strong output with additive entropy loss

**Corollary 4.9** (The $C = 0$ specialization)**.** For every fixed $\delta > 0$, there is $b_{\delta,0} > 0$ such that, for sufficiently large $n$, integer $\delta n \leqslant k \leqslant n$, and $2^{-b_{\delta,0} n} \leqslant \varepsilon \leqslant 1/4$, an explicit deterministic polynomial-time two-source extractor has output

$$m \geqslant k - O(\log(1/\varepsilon) + 1)$$

and is strong in either source separately:

$$(F(X,Y), X) \approx_\varepsilon (U_m, X), \qquad (F(X,Y), Y) \approx_\varepsilon (U_m, Y).$$

The additive-loss constants are absolute, and the same function satisfies both comparisons.

**Construction 4.3 Ordinary source-strong additive-loss specialization**

**Ingredients from earlier parts.** Construction 4.2 and Theorem 4.8, specialized to $C = 0$.

**Public parameters and fixed setup.** Use the same rate and error inputs, but set $C = 0$, $q = 1$, $R = 1$, and $r_C = 0$. Thus $u = \lceil \log(1/\varepsilon) \rceil + 10$, $d = \lceil B \left[ \log^2(n+2) + (u+1) \log\left(2 + \frac{n}{u+1}\right) \right] \rceil$, $m = \lfloor k - (A+4)(u+1) \rfloor$, $p = m - d$, and $\kappa = k - 2u$. The internal seed still uses *one-comparison* non-malleability.

**Input.** $(x, y) \in \{0,1\}^n \times \{0,1\}^n$.

**Evaluation steps.**

1. Compute the $d$-bit seed $S$ by Construction 4.2 with these specialized public parameters.
2. Return $(S, E(x,S) \oplus E(y,S))$ using its $p$-bit payloads.

**Output.** $m = d + p \geqslant k - O(\log(1/\varepsilon)+1)$ bits, strong in either source separately, as in Corollary 4.9. This is not a new amplification routine; the final comparison tuple is empty, but the internal non-malleable seed is still needed.

*Proof.* Set $C = 0$ in Theorem 4.8. Then $q = 1$, $R = 1$, and $r_C = \lceil \log(2C+1) \rceil = 0$. The comparison tuple $T$ is empty; in the centered lemma it has one value, with $\lambda_t = w_t(x) = 1$ and $N_t(y) = K$. The exceptional pairs are precisely the diagonal. All other steps and parameter inequalities remain valid, and the energy bound specializes to

$$\Delta = \frac{L}{K} + \frac{2D^2\, 2^h}{\alpha^2 K} + \frac{4\eta D^2}{\alpha^2}.$$

The same evaluator retains $S$ and XORs its two seeded payloads, with $m = \lfloor k - (A+4)(u+1) \rfloor$ and $u = \lceil \log(1/\varepsilon) \rceil + 10$. This proves both strong comparisons with the asserted loss. □

## 4.4 Sumset output with additive entropy loss

### 4.4.1 Prerequisite: linear lossless condenser

**Theorem 4.10** (Strong linear lossless condenser)**.** *Reference.* [12, Definition 4.6 and Lemma 4.7]; see also [36, 19]. For every fixed $\alpha > 0$, $k \leqslant n$, and $0 < \zeta < 1/2$, there is an explicit strong linear lossless condenser $C : \mathbb{F}_2^n \times \mathbb{F}_2^{d_C} \to \mathbb{F}_2^v$ with error $\zeta$ and

$$d_C \leqslant (1 + 1/\alpha) \log(nk/\zeta) + O_\alpha(1), \qquad v \leqslant (1+\alpha)k + d_C + O_\alpha(1).$$

Thus, conditional on an independent uniform seed, the output is on average $\zeta$-close to a source with min-entropy at least $k$. For fixed seed the map is binary-linear. Evaluation is polynomial-time in $n + \log(1/\zeta)$ for fixed $\alpha$.

This is the strong linear formulation in [12, Definition 4.6 and Lemma 4.7], recording the GUV condenser and its linear implementation.

### 4.4.2 Prerequisite: sum-compatible recycling and its proof

Write $K = 2^k$, $D = 2^d$, and $M = 2^p$ for alphabet sizes.

**Lemma 4.11** (Entropy slack gives strength in a summand)**.** If an ordinary $d$-bit sumset extractor $G$ has component threshold $h$ and error $\gamma$, then for independent $X, Y$ with $H_\infty(X) \geqslant k > h$, $H_\infty(Y) \geqslant h$,

$$\Delta((X, G(X+Y)), (X, U_d)) \leqslant 2^d(\gamma + 2^{h-k}).$$

*Proof.* For each output value $u$, let $B_u = \{x : \Pr_Y[G(x+Y) = u] > 2^{-d} + \gamma\}$. If $\Pr[X \in B_u] \geqslant 2^{h-k}$, conditioning on $B_u$ preserves left entropy $h$ and independence of $Y$, contradicting extraction at the single atom $u$. Hence each $B_u$ has mass below $2^{h-k}$. Outside $B_u$ the positive atom excess is at most $\gamma$, and inside it at most one. Sum over the $2^d$ output atoms. This is the one-sided entropy-slack argument underlying Lemma 2.5. □

**Corollary 4.12** (Retained-seed sumset recycling)**.** Let $H_s : \mathbb{F}_2^n \to \mathbb{F}_2^p$ be linear for each $s$ and a strong seeded $(k, \zeta)$ extractor. Let $G$ be strong in the first summand at entropy $k$ with error $\eta$, and a left one-sided non-malleable sumset seed at threshold $k - 4$ with error $\gamma$, with the same ordinary extraction guarantee. If $K \geqslant 16M$, $0 < \theta < 1$, and $\beta = 3(1+\theta)\zeta/\theta + 2\eta < 1$, then for $S = G(X + Y)$,

$$\Delta((Y, S, H_S(X+Y)), (Y, U_{d+p})) \leqslant \beta + \tfrac{1}{2}\sqrt{\theta + 2\beta + 2(1+\theta)D^2\gamma + DM/K}. \tag{4.39}$$

The ordinary sumset conclusion follows by discarding $Y$.

*Proof.* Apply Lemma 4.1 to $\widetilde{G}(x, y) = G(x + y)$ and $E(x, s) = H_s(x)$. It compares $(Y, S, H_S(X))$ with $(Y, U_d, U_p)$ at the displayed error. Apply $(y, s, a) \mapsto (y, s, a + H_s(y))$. The real payload becomes $H_s(X + Y)$ by linearity; a fixed translation preserves uniformity of $U_p$ conditional on every $(y, s)$. No conditioning on $S$ is needed. □

**Corollary 4.13** (Sumset calibration)**.** For $0 < \varepsilon \leqslant 1/4$, the bound in (4.39) is at most $\varepsilon$ under the hypotheses of Corollary 4.5, in particular when $DM/K \leqslant \varepsilon^2/256$ and its other parameters are unchanged.

*Proof.* Apply the common calibration (the smaller diagonal term only helps). □

### 4.4.3 Prerequisite: polynomial shear and seed-fit linear hashing

A generic nonlinear strong seeded extractor cannot be substituted in Corollary 4.12: its proof uses $H_u(x + y) = H_u x + H_u y$. A full-input universal hash, although linear, need not fit in the available sumset seed. The following elementary family gives the parameter regime we need after lossless condenser.

**Lemma 4.14** (Polynomial shear hashing)**.** Let $E = \mathbb{F}_{2^t}$ and $b \geqslant 1$. For $u \in E$, define

$$\mathsf{Sh}_u(z_0, \dots, z_b) = (z_1 + uz_0, z_2 + u^2 z_0, \dots, z_b + u^b z_0).$$

For every distribution $Z \in E^{b+1}$ of min-entropy at least $k$, and an independent uniform $U \in E$,

$$\Delta((U, \mathsf{Sh}_U(Z)), U_{(b+1)t}) \leqslant \tfrac{1}{2}\sqrt{b\, 2^{bt-k}}. \tag{4.40}$$

Every fixed-seed map is binary-linear and surjective. The seed length is $t$, not $(b+1)t$.

*Proof.* Use the nondegenerate trace pairing to index characters of $E^{b+1}$. A nonzero output character $\lambda = (\lambda_1, \dots, \lambda_b)$ pulls back to

$$(\textstyle\sum_{i=1}^{b} \lambda_i u^i, \lambda_1, \dots, \lambda_b).$$

For fixed $\lambda \neq 0$ and fixed first coefficient $\eta$, the equation $\sum_i \lambda_i u^i = \eta$ has at most $b$ roots, since its left side minus $\eta$ is a nonconstant polynomial of degree at most $b$. If $\widehat{\mu}(\xi) = \mathbb{E}\chi_\xi(Z)$, then

$$\frac{1}{|E|} \sum_u \sum_{\lambda \neq 0} \left| \widehat{\mu}\left( \sum_i \lambda_i u^i, \lambda \right) \right|^2 \leqslant \frac{b}{|E|} \sum_\xi |\widehat{\mu}(\xi)|^2 \leqslant b\, 2^{bt-k}.$$

The last step is Parseval, $\sum_\xi |\widehat{\mu}(\xi)|^2 = 2^{(b+1)t} \operatorname{cp}(Z)$, and $\operatorname{cp}(Z) \leqslant 2^{-k}$. Fourier Cauchy–Schwarz bounds the distance for each fixed seed by half the square root of its nonzero-character sum. Average over seeds and use Jensen. Linearity is immediate; surjectivity follows by setting $z_0 = 0$. □

**Lemma 4.15** (Seed-fit linear extraction)**.** Fix $0 < \delta \leqslant 1$ and $0 < a < \delta/8$. There exists $b_{\delta,a} > 0$ such that, for all sufficiently large $n$, all integer $\delta n \leqslant k \leqslant n$, and all integers $2 \leqslant s \leqslant b_{\delta,a} n$, put

$$d = \lfloor an \rfloor, \qquad p = k - d - 2s - 8, \qquad \zeta = 2^{-4s-20}.$$

There is an explicit strong linear $(k, \zeta)$ seeded extractor with exactly $d$ seed bits and $p$ output bits. The constants and running time may depend on $\delta, a$, but $d + p = k - 2s - 8$ exactly.

**Construction 4.4 Seed-fit binary-linear payload extractor**

**Ingredients from earlier parts.** The strong linear lossless condenser of Theorem 4.10 and polynomial shear hashing, Lemma 4.14.

**Public parameters and fixed setup.** Fix $\delta > 0$, $0 < a < \delta/8$, integer $\delta n \leqslant k \leqslant n$, and integer $s$ in Lemma 4.15's range. Set $d = \lfloor an \rfloor$, $p = k - d - 2s - 8$, and $\zeta = 2^{-4s-20}$. Choose a fixed integer $b \geqslant \max\{2, 16/a\}$ and $\alpha = 1/(8b)$. Instantiate the linear condenser $\mathcal{C}$ at entropy $k$, parameter $\alpha$, and error $\zeta/2$; let its seed and output lengths be $d_C, v$. Put

$$w = 4s + 21, \quad \Lambda = 2w + \lceil \log b \rceil + 2, \quad t = \left\lfloor \frac{k - \Lambda}{b} \right\rfloor, \quad E = \mathbb{F}_{2^t}.$$

The proof below verifies $v \leqslant (b+1)t$, $d_C + t \leqslant d$, and $p \leqslant bt$. Fix the field's binary basis.

**Input.** $z \in \mathbb{F}_2^n$ and a $d$-bit numerical seed $S$.

**Evaluation steps.**

1. Parse the first $d_C$ seed bits as $S_C$, the next $t$ bits as $U \in E$, and ignore the remaining $d - d_C - t$ bits.
2. Compute $\mathcal{C}(z, S_C)$, append zeros to reach $(b+1)t$ bits, and parse the result as $(z_0, z_1, \ldots, z_b) \in E^{b+1}$.
3. Compute $(z_1 + Uz_0, z_2 + U^2 z_0, \ldots, z_b + U^b z_0)$, write the result as $bt$ bits, and return its first $p$ bits.

**Output.** $H_S(z) \in \mathbb{F}_2^p$ with exactly $d$ supplied seed bits. For every fixed $S$, the map in $z$ is binary-linear. Lemma 4.15 gives error $\zeta$ for an independent uniform seed. In the sumset wrapper below $S$ is generated internally, and Corollary 4.12, not an independence assumption, justifies that use.

*Proof.* Choose a fixed integer $b \geqslant \max\{2, 16/a\}$ and put $\alpha = 1/(8b)$. Apply Theorem 4.10 with error $\zeta/2$. Write its seed length and output length as $d_C, v$. There is a constant $A_b$ such that

$$d_C \leqslant A_b(\log(n+2) + s + 1), \qquad v \leqslant (1+\alpha)k + d_C + A_b.$$

Define the integers

$$w = \log(2/\zeta) = 4s + 21, \qquad \Lambda = 2w + \lceil \log b \rceil + 2, \qquad t = \left\lfloor \frac{k - \Lambda}{b} \right\rfloor.$$

Choose the positive constant $b_{\delta,a}$ sufficiently small. Since $\log n = o(n)$, uniformly over the specified $k, s$ and all sufficiently large $n$ we can ensure

$$d_C \leqslant an/4, \tag{4.41}$$

$$d_C + 2\Lambda + A_b + b + 1 \leqslant k/(2b), \tag{4.42}$$

$$d + 2s + 8 \geqslant \Lambda + b, \qquad p \geqslant 1. \tag{4.43}$$

To make this explicit as a choice order, first fix $b, \alpha, A_b$, then choose $b_{\delta,a}$ so that the coefficients of $s/n$ in these three inequalities fit with a strict margin, and finally increase the length threshold to absorb the logarithmic and constant terms. All required right-side margins are positive multiples of $n$; no parameter depends on the input source.

The native hash input length fits because

$$\begin{aligned}(b+1)t - v &\geqslant (1/b - \alpha)k - (1 + 1/b)\Lambda - (b+1) - d_C - A_b \\ &\geqslant 7k/(8b) - k/(2b) > 0.\end{aligned}$$

Pad the condenser output to $(b+1)t$ bits with zeros and apply Lemma 4.14 with an independent $t$-bit seed. Conditional on the condenser seed, its comparison source has min-entropy at least $k$. Since $bt \leqslant k - \Lambda$, the shear error is at most

$$\tfrac{1}{2}\sqrt{b}\,2^{-\Lambda/2} \leqslant \zeta/8.$$

The total error is less than $\zeta$. The combined map is linear for every fixed pair of seeds.

Its actual seed length obeys

$$d_C + t \leqslant an/4 + n/b \leqslant 5an/16 \leqslant \lfloor an \rfloor$$

for large $n$. Pad with ignored seed bits to reach exactly $d$. Its available output satisfies $bt \geqslant k - \Lambda - b \geqslant p$ by (4.43); truncate to $p$ bits. All maps are explicit and their field operations and condenser evaluation are polynomial-time for fixed $b, \alpha$. □

*Remark* 4.16 (Why a linear seed is an advantage here). For a constant error, the construction may retain $d = \Theta_\delta(n)$ seed bits and produce only $k - d - O(1)$ hash bits. This is not a loss: the seed itself is included in the output. No claim of an optimal $O(\log n + \log(1/\varepsilon))$ linear seed is used. Keeping $d$ fixed at a small linear fraction also gives enough room for the condenser and hash at every error exponent up to a sufficiently small linear fraction.

### 4.4.4 Theorem

**Theorem 4.17** (Near-optimal sumset output)**.** For every fixed $0 < \delta \leqslant 1$ there are $b_\delta > 0$ and $n_\delta$ such that, whenever $n \geqslant n_\delta$, $\delta n \leqslant k \leqslant n$ is an integer, and

$$2^{-b_\delta n} \leqslant \varepsilon \leqslant \tfrac{1}{4},$$

there is an explicit deterministic polynomial-time map

$$\mathrm{SumExt}_{n,k,\varepsilon} : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m, \qquad m = k - 2\lceil \log(1/\varepsilon) \rceil - 8,$$

whose output on $X + Y$ is $\varepsilon$-close to uniform for all independent $X, Y$ with $H_\infty(X), H_\infty(Y) \geqslant k$. In particular,

$$m \geqslant k - 2\log(1/\varepsilon) - 10.$$

The constants in the running time and the nontrivial error range may depend on $\delta$, but the displayed output-loss constants do not.

### 4.4.5 Complete sum-only retained-seed construction

**Construction 4.5 Sumset output with additive entropy loss**

**Ingredients from earlier parts.** The one-sided non-malleable sumset seed of Theorem 3.33 (Construction 3.5); Lemma 4.15 (Construction 4.4); and the retained-seed sumset recycling interface of Corollary 4.12.

**Public parameters and fixed setup.** Fix $\delta > 0$, integer $\delta n \leqslant k \leqslant n$, and error $\varepsilon$ in Theorem 4.17's range. Instantiate $G_0$ from Theorem 3.33 at rate $\delta/8$, with output and error constants $c, e > 0$. Fix $0 < a < \min\{c/4, e/16, \delta/64, 1/64\}$ and put

$$s = \lceil \log(1/\varepsilon) \rceil, \qquad d = \lfloor an \rfloor, \qquad p = k - d - 2s - 8.$$

Set $G = \mathrm{prefix}_d G_0$ and instantiate Construction 4.4 with these $n, k, \delta, a, s$. Its $d$-bit seed interface supplies $p$ payload bits and error $2^{-4s-20}$ under an independent uniform seed.

**Input.** Only $z \in \mathbb{F}_2^n$.

**Evaluation steps.**

1. Compute the $d$-bit seed $S = G(z)$.
2. Compute $H_S(z)$ by Construction 4.4, including its seed split, condenser, polynomial shear, and final truncation.
3. Return
$$\mathrm{SumExt}(z) = (S, H_S(z)), \qquad S = G(z). \tag{4.44}$$

**Output.** Exactly $d + p = k - 2\lceil \log(1/\varepsilon) \rceil - 8$ bits, with error at most $\varepsilon$ as in Theorem 4.17. The evaluator never receives either summand. Linearity of $H_S$ is with respect to $z$ for each *fixed* seed, not a claim that the whole seed-dependent evaluator is linear.

**Not evaluated.** Summands, the shift by $H_S(y)$, collision partners, and the independently seeded comparison experiment.

### 4.4.6 Final parameters and proof of the main theorem

*Proof of Theorem 4.17.* Fix $\delta > 0$ and use Theorem 3.33 at rate $\sigma = \delta/8$. Let its output and error constants be $c, e > 0$. Choose a positive rational

$$a < \min\{c/4, e/16, \delta/64, 1/64\}, \qquad d = \lfloor an \rfloor.$$

Let $G$ be the first $d$ seed bits. Truncation preserves the one-sided guarantee and its ordinary marginal, with $\gamma \leqslant 2^{-en}$. For all sufficiently large $n$, $k - 4 \geqslant \sigma n$. Lemma 4.11 gives strength in the first summand with

$$\eta \leqslant 2^d\big(2^{-en} + 2^{\sigma n - k}\big) \leqslant 2^{-(e-a)n} + 2^{-(7\delta/8 - a)n}.$$

Put $s = \lceil \log(1/\varepsilon) \rceil$ and $\varepsilon = 2^{-s} \leqslant \varepsilon$. Choose $b_\delta > 0$ sufficiently small that $s \leqslant 2b_\delta n$ lies in the range of Lemma 4.15 for large $n$, and that, throughout this range,

$$2^{-en} \leqslant 2^{-2s-9-2d}, \qquad 2^{-(e-a)n} + 2^{-(7\delta/8-a)n} \leqslant 2^{-2s-12}.$$

These inequalities have fixed positive linear margins by the choice of $a$; decreasing $b_\delta$ secures them uniformly. The extra one from the ceiling of $s$ is absorbed by taking $n$ sufficiently large.

Use Lemma 4.15 with error $\zeta = \varepsilon^4/2^{20}$ and payload length $p = k - d - 2s - 8$. With $K = 2^k, D = 2^d, M = 2^p$ we have exactly

$$DM/K = 2^{-2s-8} = \varepsilon^2/256.$$

All hypotheses of Corollary 4.13 hold. Therefore the sum-only evaluator (4.44) has error at most $\varepsilon \leqslant \varepsilon$. Its length is exactly

$$d + p = k - 2s - 8 \geqslant k - 2\log(1/\varepsilon) - 10.$$

This proves the theorem, uniformly over all $k$ in the stated interval. □

**Nontrivial error range and an all-error convention** The meaningful construction above covers $\varepsilon \geqslant 2^{-b_\delta n}$. It is not an assertion that every smaller requested error still permits the same nonzero output bound with coefficient two. If an all-error expression with rate-dependent constants is desired, choose $C_\delta \geqslant \max\{12, 1/b_\delta + 2\}$. For $\varepsilon < 2^{-b_\delta n}$, the bound $k - C_\delta(\log(1/\varepsilon) + 1)$ is nonpositive because $k \leqslant n$. Return the empty string, which is exactly uniform. Truncation of the main output in the nontrivial range and adjustment for finitely many short lengths give the conventional statement

$$m \geqslant \max\{0, \lfloor k - C_\delta(\log(1/\varepsilon) + 1)\rfloor\}$$

for all errors, without claiming a nonempty output below the proved linear-exponent range.

# 5 Decreasing entropy rates

The evaluated pipeline is: the all-pairs table (Construction 5.1), the head/advice/breaker short extractor (Construction 5.3), and the retained-seed XOR output extension (Construction 5.4). Regularization is used only to prove the properties of this pipeline.

Fix $0 < \vartheta < 1/2$ and a nonnegative integer tampering count $t$ independently of $n$. This section proves separately source-strong multiple-tampering extraction at entropy rate $C/\log n$, with output $k/(t+1) - O(\log(1/\varepsilon) + 1)$. The ordinary near-$k$ statement is its sole corollary. We first prove the growing-row ingredients, then construct and analyze the short non-malleable seed, and finally give the centered-recycling calibration and complete long-output evaluator.

## 5.1 Growing-row ingredients and their proofs

The following lemmas and quoted quantitative theorems are the prerequisites for the inverse-logarithmic construction. Their full parameter bounds are given here before the evaluated algorithm. Internal lemmas are proved below; imported primitives are identified by version-specific theorem references.

### 5.1.1 Cited primitives and their interfaces

We use the quantitative approximate-duality, linear-condenser, and affine somewhere-random inputs from Section 2. For the local notation of this section, let $a_1$ be a sufficiently large absolute constant in the affine somewhere-random input, and write $H(T) = (2T)^{a_1 \log(2T)}$. The following correlation-breaker interface is used to generate the short seed. For final entropy-efficient output we use the strong seeded extractor of Lemma 2.23 and the centered recycling lemma from Section 4.

**Theorem 5.1** (Quantitative affine correlation breaker)**.** *Reference.* [52, Lemma 3.16 and Section 3.6.2, Eq. (3.61)]; see also [49, Definition 3.4 and Theorem 3.5]. Let $M = h + 1 \geqslant 2$, $v = \lceil \log(2M) \rceil$, and let $u \geqslant m \geqslant 1$ be integers. For data length $N$ and advice length $a$, put $z =$

$u + \lceil \log(N+2) \rceil$. There is a uniformly explicit function $\mathrm{ACB} : \{0,1\}^N \times \{0,1\}^d \times \{0,1\}^a \to \{0,1\}^m$, with choices

$$d \leqslant C\big(Ma + Mv^3 z\big),$$
$$K \leqslant C\big(Ma + (M^2 + Mv^3)z\big),$$

having the following property. Let $b \geqslant 0$ be a seed-deficiency allowance. Suppose $A_j, B_j, Q_j \in \mathbb{F}_2^N$ and $R_j \in \mathbb{F}_2^d$ are random variables, with $Q_j = A_j + B_j$ for $0 \leqslant j \leqslant h$, and

$$(A_j)_{j=0}^h \;\perp\; ((B_j)_{j=0}^h, (R_j)_{j=0}^h), \qquad H_\infty(A_0) \geqslant K, \quad H_\infty(R_0) \geqslant d - b.$$

For fixed $\alpha_0, \ldots, \alpha_h \in \mathbb{F}_2^a$ with $\alpha_0 \neq \alpha_j$ for every $j > 0$, put $Z_j = \mathrm{ACB}(Q_j, R_j, \alpha_j)$. Then

$$(Z_0, (Z_j)_{j=1}^h) \approx_{256M^3 2^{b-u}} (U_m, (Z_j)_{j=1}^h).$$

The comparison tuple has its actual joint marginal, and $U_m$ is independent of that tuple. The conclusion allows arbitrary correlations within each displayed tuple and no entropy in comparison inputs. The parameter range here has $d, K \leqslant N$.

This is the quantitative form of [52, Lemma 3.16 and Section 3.6.2, Eq. (3.61)]. The loss $2^b$ for seed deficiency follows there by retaining the seed in the conditioning tuple and changing its marginal to uniform. The transformation underlying the breaker is also stated in [49, Definition 3.4 and Theorem 3.5]. We use this theorem as a cited quantitative ingredient. In particular, its independence requirement is on the residual $A$ part and the seed-determined $B$ part, not on the full data and seed tuples.

For clarity, the deficiency transfer uses the cited theorem with its conditioning tuple retained. Put $\mathcal{C} = ((B_j)_{j=0}^h, (R_j)_{j=0}^h)$. Replace the marginal of $R_0$ by $U_d$, preserve the conditional distribution of the rest of $\mathcal{C}$ given $R_0$, and keep the independent $A$ tuple unchanged. Define arbitrary conditional distributions at previously unsupported seed values. The original distribution is the new distribution reweighted by $w(r) = 2^d \Pr[R_0 = r] \leqslant 2^b$. The retained tuple in the uniform-seed theorem contains $R_0$, so reweighting both its real and ideal distributions recovers the original retained marginal and increases their half-$\ell_1$ distance by at most $2^b$. This proves the displayed weak-seed error without assuming that $R_0$ is independent of the other seeds or of the $B$ tuple.

### 5.1.2 Elementary conditioning and Fourier facts

**Lemma 5.2** (Flat-source decomposition)**.** For an integer $k$, every distribution with atoms at most $2^{-k}$ is a convex combination of uniform distributions on $2^k$-element sets.

*Proof.* Consider the polytope $0 \leqslant p_i \leqslant 2^{-k}$, $\sum_i p_i = 1$. A vertex cannot have two coordinates strictly between their bounds, since a small opposite perturbation preserves the constraints. It cannot have exactly one such coordinate, because the sum of all other coordinates is an integer multiple of $2^{-k}$. Every vertex is therefore uniform on exactly $2^k$ points. □

Decompose independent sources separately. The resulting component pairs are still independent; statistical distance averages by convexity. The tampering maps remain the original fixed maps on all components.

**Lemma 5.3** (Conditioning and truncation)**.** An event of probability $p$ costs at most $\log(1/p)$ bits of min-entropy. Deleting $b$ coordinates from a bit string costs at most $b$ bits. Conditioning independent flat sources on a product rectangle preserves their independence and flatness.

*Proof.* The first bound follows from $\Pr[X = x \mid E] \leqslant \Pr[X = x]/p$. For the second, each retained string has at most $2^b$ preimages. For the third, the conditional point probabilities factor into the two uniform distributions. □

**Lemma 5.4** (Fourier approximation on the output hull)**.** Let $P$ be supported on an affine subspace $V \subseteq \mathbb{F}_2^D$. If each ambient character nonconstant on $V$ has absolute expectation at most $2^{-v}$, then

$$\Delta(P, U_V) \leqslant 2^{\dim(V)/2-v-1} \leqslant 2^{D/2-v-1}.$$

*Proof.* Choose affine coordinates on $V$. Every nontrivial character in those coordinates extends to an ambient character, up to a fixed sign. For $d = \dim V$, Cauchy–Schwarz and Parseval give

$$\Delta(P, U_V) \leqslant \frac{1}{2}\left(\sum_{\lambda \neq 0} |\widehat{P}(\lambda)|^2\right)^{1/2} \leqslant \frac{1}{2}\sqrt{2^d - 1}\, 2^{-v}.$$

The zero-dimensional case has distance zero. □

### 5.1.3 Joint conversion through separate features

The common regularization theorem applies to arbitrary separately computed features, including tuples of original and tampered inputs. We record its normalization here so that the subsequent parameter substitutions retain their original symbols.

Let $\phi : \mathbb{F}_2^n \to \mathbb{F}_2^{p_L}$ and $\psi : \mathbb{F}_2^n \to \mathbb{F}_2^{p_R}$ be fixed maps, put $P = p_L + p_R$, and let $F(x, y) = \mathcal{B}(\phi(x), \psi(y)) \in \mathbb{F}_2^D$ for a fixed bilinear map $\mathcal{B}$. Constant feature coordinates may be included. The maps may be nonlinear, noninjective, and composed with arbitrary separate tamperings.

**Theorem 5.5** (Feature regularization)**.** There is an absolute constant $K_0$ such that the following holds. For independent flat sources $X, Y$, integers $R, u \geqslant 1$, and $v \geqslant 0, z \geqslant 1$, there is a finite deterministic product-rectangle partition with these properties.

(i) On every leaf $\tau$, the output distribution is within $2^{D/2-v-1}$ of uniform on its output affine hull.

(ii) Except on leaves of total mass at most $2^{1-z}$, each input loses at most

$$\mathcal{L} = K_0\left[\frac{P}{u} + \frac{P}{R}\left(2^u(v+1) + (u+1)\log(n+P+2)\right) + D(R+2) + z\right] \tag{5.1}$$

bits of min-entropy.

The partition is used only in the proof and is not computed by the extractor.

*Proof.* If $P = 0$, the output is constant and the assertion is immediate. Suppose first that $1 \leqslant R \leqslant P$. Pad the two feature spaces to a common dimension $P$ and apply Theorem 2.30 with $r_* = R$, $H = v$, and tail parameter $t = z$. The weighted duality bound is Lemma 2.29. Successful restrictions are charged to the sum of the feature-hull dimensions, and exact messages to the output-hull dimension. The two surprisal estimates give the displayed loss after increasing the absolute constant $K_0$. Every leaf is a product rectangle, and the Fourier error on its exact output affine hull is at most $2^{D/2-v-1}$.

For completeness, if $R > P$, compute each of the $D$ output bits by the low-rank protocol used in that theorem. Every bilinear part has rank at most $P$, so at most $D(P + 2)$ declared bits suffice in total. The table is constant on each resulting rectangle and is therefore exactly uniform on its

singleton affine hull. A transcript with at most $B_0 = D(P+2)$ declared bits has at most $2^{B_0}$ leaves. Leaves of probability below $2^{-B_0-z}$ have total mass at most $2^{-z}$; on all others the joint surprisal, and hence each side's entropy loss, is at most $B_0 + z \leqslant D(R+2) + z$. This also satisfies (5.1). Thus all permitted cutoffs are covered, including nonlinear and noninjective feature maps. □

### 5.1.4 The condenser table and joint affine regularization

**Construction 5.1 All-pairs field-inner-product condenser table**

**Ingredients from earlier parts.** The uniform linear somewhere condenser of Theorem 2.27 and the fixed finite-field conventions of Section 2.2.

**Public parameters and fixed setup.** Given input length $n$ and an admissible working threshold $k_0$, instantiate the condenser at that threshold, obtaining $\mathcal{C}_1, \dots, \mathcal{C}_L : \mathbb{F}_2^n \to \mathbb{F}_2^{B_0}$. Choose integer $1 \leqslant s \leqslant B_0$ and put $B = s\lfloor B_0/s \rfloor$, $T = L^2$, and $F = \mathbb{F}_{2^s}$. Fix a binary basis of $F$ and order pairs $(i,j) \in [L]^2$ lexicographically. In Proposition 5.8's regime, use $k_0 = k/4$ and $s = \lfloor n^{1/2-\vartheta/2} \rfloor$.

**Input.** $(x,y) \in \{0,1\}^n \times \{0,1\}^n$.

**Evaluation steps.**

1. Evaluate every condenser row on each input and retain its first $B$ bits. Parse each row into $B/s$ elements of $F$.
2. For *every* pair $(i,j) \in [L]^2$, compute
$$W_{ij}(x,y) = \sum_{e=1}^{B/s} \mathcal{C}_i(x)_e \, \mathcal{C}_j(y)_e \in F.$$
3. Return these $T$ field elements in the fixed pair order, each represented by $s$ bits. Flattening the table gives $Ts$ bits.

**Output.** The table $W(x,y) \in (\mathbb{F}_2^s)^T$; it is an intermediate object, not itself the final extractor. Unlike the many-good-row constant-rate constructions, this table retains all $L^2$ pairs.

**Not evaluated.** Joint affine regularization, affine hulls, a choice of good row, and the tampered table tuple. They certify the table's distribution but are not computed from $(x,y)$.

The table is binary bilinear in $x, y$, so its separate features have total dimension $P = 2n$, independently of $T$. For the proofs below, write the condenser's good-row rate as $1/2 + \beta$ and its error as $\varepsilon_c = 2^{-cB_0}$, with the constants of Theorem 2.27.

**Lemma 5.6** (Field inner-product character bound)**.** If independent sources $U, V$ on $B$ bits have entropies $h_U, h_V$, then every nontrivial binary character of their field inner product has absolute bias at most
$$2^{(B-h_U-h_V)/2}.$$

*Proof.* Each such character is a nondegenerate binary bilinear form on $\mathbb{F}_2^B \times \mathbb{F}_2^B$. The corresponding sign matrix has orthogonal rows of squared length $2^B$, and hence operator norm $2^{B/2}$. The two source probability vectors have Euclidean norms at most $2^{-h_U/2}$ and $2^{-h_V/2}$. Apply the operator-norm inequality. □

**Lemma 5.7** (Every sufficiently entropic rectangle has a full row)**.** Assume $s = o(B_0)$ and $B_0 \to \infty$. For all sufficiently large $n$, if both sides of a flat rectangle have entropy at least $k_0$, then some row

projection of $\operatorname{aff}(W(A,B))$ is all of $\mathbb{F}_2^s$.

*Proof.* Truncation costs fewer than $s$ entropy bits. Thus every designated good row in the ideal condenser mixture has entropy at least $(1/2+\beta/2)B$ for sufficiently large $n$. The two ideal condenser mixtures can be sampled independently, and their product distribution is within $2\varepsilon_c$ of the actual condenser product, where $\varepsilon_c = 2^{-cB_0}$.

Suppose every output row projection has a proper affine hull. For each row pair $(i,j)$ choose a nontrivial binary character constant, say equal to $b_{ij}$, on its actual output support. Let $\mathcal{E}$ be the event that all these chosen equations hold. Its actual probability is one.

In each product component of the ideal condenser mixtures, let $(i,j)$ be the designated good row pair. By Lemma 5.6, the probability of its selected equation is at most $(1+2^{-\beta B/2})/2$, after weakening constants. Thus the probability of $\mathcal{E}$ in every component is at most that quantity, regardless of dependence among other rows. Averaging and restoring the original distribution gives

$$1 \leqslant \frac{1+2^{-\beta B/2}}{2} + 2\varepsilon_c,$$

a contradiction for large $n$. □

**A reusable joint-conversion guarantee**

**Proposition 5.8** (Regularization parameters)**.** Fix $t$, and let $k$ be a working entropy threshold. Build the condenser at threshold $k/4$, and let $T = L^2$ be the number of field-product rows, each of length $s$. For $k = C_{\vartheta,t}n/\log n$, with a sufficiently large constant, take $s = \lfloor n^{1/2-\vartheta/2} \rfloor$ and $T = (\log n)^{O(1)}$. Then, for every product of flat sources whose side entropies are at least $k/2$, and every list of $t$ separate tamperings, the joint table distribution is $2^{-s}$-close to a mixture of jointly affine tuples $(Q^0,\dots,Q^t)$, where $Q^j \in (\mathbb{F}_2^s)^T$ and some row of $Q^0$ is exactly uniform. The good row may depend on the component.

*Proof.* For the $t+1$ executions, use separate features $(x, f_1(x),\dots,f_t(x))$ and $(y, g_1(y),\dots,g_t(y))$. Their total dimension is $P = 2(t+1)n$, and the output dimension is $D = (t+1)Ts$. Apply Theorem 5.5 with

$$v = D + 2s + 2, \qquad z = s + 2.$$

The total approximation and exceptional-leaf error is at most $2^{-s}$. It suffices to make its entropy loss $\mathcal{L} \leqslant k/4$. Then every good rectangle has side entropies at least $k/4$, and Lemma 5.7 supplies the uniform row in the honest affine projection. Replace exceptional leaves by any valid affine tuple before averaging.

Take $u = \lfloor (\vartheta/8)\log n \rfloor$ and $R = \lceil n^{1/2+\vartheta/4} \rceil$. In (5.1) the terms, apart from constant factors depending on $t, \vartheta$, are bounded by

$$\begin{aligned} P/u &= O_{\vartheta,t}(n/\log n), \\ (P/R)2^u(v+1) &\leqslant n^{1-5\vartheta/8+o(1)}, \\ (P/R)(u+1)\log(n+P+2) &\leqslant n^{1/2-\vartheta/4+o(1)}, \\ D(R+2) &\leqslant n^{1-\vartheta/4+o(1)}, \\ z &\leqslant n^{1/2-\vartheta/2+o(1)}. \end{aligned}$$

All but the first are $o(n/\log n)$. Increasing $C_{\vartheta,t}$ therefore gives $\mathcal{L} \leqslant k/4$. Here $s = o(B_0)$, as required by the full-row lemma. For the honest table alone, the same conclusion follows either directly or by discarding the comparison coordinates. □

### 5.1.5 Strong ordinary seeds and advice

We first make an ordinary seed strong with respect to either input separately; no independence from both inputs jointly is claimed.

**Lemma 5.9** (Two separate strong guarantees)**.** Suppose $E_0 : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^q$ is an ordinary two-source extractor with error $\varepsilon_0$ at entropy threshold $K$. If $X, Y$ are independent and each has min-entropy at least $K + b$, then $S = E_0(X, Y)$ satisfies

$$\Delta((S, X), (U_q, X)) \leqslant 2^q(\varepsilon_0 + 2^{-b}),$$
$$\Delta((S, Y), (U_q, Y)) \leqslant 2^q(\varepsilon_0 + 2^{-b}).$$

*Proof.* Fix an output value $s$ and put $p_s(x) = \Pr[E_0(x, Y) = s]$. Let $A_s = \{x : p_s(x) > 2^{-q} + \varepsilon_0\}$. If $\Pr[X \in A_s] > 2^{-b}$, the conditional source $X|A_s$ has entropy at least $K$ and is independent of $Y$. The probability of output $s$ on this rectangle is strictly greater than $2^{-q} + \varepsilon_0$, contrary to extraction. Thus $\Pr[X \in A_s] \leqslant 2^{-b}$. Consequently

$$\mathbb{E}_X \big(p_s(X) - 2^{-q}\big)_+ \leqslant \varepsilon_0 + 2^{-b}.$$

Sum over the $2^q$ output values to obtain the first inequality. Interchange the roles of $X, Y$ for the second. Uniformity of either source and any entropy condition on tampered sources are unnecessary. □

For an ordinary extractor with $q$ output bits and $\varepsilon_0 \leqslant 2^{-4q}$, taking entropy slack $b = 4q$ gives

$$\max\{\Delta((S, X), (U_q, X)), \Delta((S, Y), (U_q, Y))\} \leqslant 2^{1-3q}. \tag{5.2}$$

We will verify the required entropy slack for the seed used in Section 5.2.

**Polynomial fingerprints give separated advice** Fix a representation of $F = \mathbb{F}_{2^q}$, and let $h = \lceil n/q \rceil$. Pad an $n$-bit string $x$ with zeros to $hq$ bits, interpret its consecutive blocks as $x_0, \ldots, x_{h-1} \in F$, and define

$$P_x(T) = \sum_{j=0}^{h-1} x_j T^j \in F[T].$$

The map $x \mapsto P_x$ is injective. Thus $P_x - P_{x'}$ is a nonzero polynomial of degree at most $h - 1$ whenever $x \neq x'$. It has at most $h - 1$ roots in $F$. For $h = 1$ it has no roots.

**Theorem 5.10** (Advice generation from a two-sided strong seed)**.** Let $S = S(X, Y) \in F$ be a deterministic function of two independent sources and suppose

$$\Delta((S, X), (U_q, X)) \leqslant \varepsilon_s, \qquad \Delta((S, Y), (U_q, Y)) \leqslant \varepsilon_s.$$

Define a single deterministic advice function by

$$\mathrm{Adv}(x, y) = \big(S(x, y), P_x(S(x, y)), P_y(S(x, y))\big). \tag{5.3}$$

It has exactly $a = 3q$ bits. For any $t$ split-state tamperings $(f_j, g_j)$ such that $\Pr[(f_j(X), g_j(Y)) = (X, Y)] = 0$, its advice satisfies

$$\Pr\big[\exists j : \mathrm{Adv}(X, Y) = \mathrm{Adv}(f_j(X), g_j(Y))\big] \leqslant t\big(\varepsilon_s + (h - 1)2^{-q}\big). \tag{5.4}$$

This applies to arbitrary tampering functions, with no entropy requirement on their outputs. Evaluation is polynomial time if $S$ is polynomial time.

*Proof.* Fix a tampering $(f, g)$, and abbreviate $S' = S(f(X), g(Y))$. Independence of $X, Y$ gives

$$\Pr[f(X) = X,\ g(Y) = Y] = \Pr[f(X) = X] \Pr[g(Y) = Y].$$

Since this product is zero, one of the factors is zero. Suppose first that $\Pr[f(X) = X] = 0$. Equality of the advice strings implies $S = S'$ and then

$$P_X(S) = P_{f(X)}(S).$$

This implication is used without conditioning on the event $S = S'$. For every $x$ in the support of $X$, the set

$$B_x = \{s \in F : P_x(s) = P_{f(x)}(s)\}$$

has size at most $h - 1$. The strong-seed guarantee therefore gives

$$\begin{aligned}\Pr[\mathrm{Adv}(X, Y) = \mathrm{Adv}(f(X), g(Y))] &\leqslant \Pr[S \in B_X] \\ &\leqslant \Pr[U_q \in B_X] + \varepsilon_s \\ &\leqslant (h - 1)2^{-q} + \varepsilon_s.\end{aligned}$$

The case $\Pr[g(Y) = Y] = 0$ uses the third advice component and the strong guarantee with respect to $Y$. Sum the resulting bounds over $j \in [t]$. A field polynomial is evaluated with Horner's rule; field arithmetic and a representation of $\mathbb{F}_{2^q}$ can be implemented uniformly in polynomial time, as in the field-product construction. □

This is the standard fingerprinting principle underlying sampled-code advice. Its advantage here is a particularly transparent exact bound. The proof does not condition on equal seeds, does not assume that the tampered seed is uniform, and does not assume that it is independent of either honest source.

### 5.1.6 Joint affine conversion after fixing prefix-dependent advice

This is the conditioning step that permits the affine correlation breaker. It avoids both a feature expansion of the nonlinear advice and an independence assumption on the resulting execution tuples.

**Lemma 5.11** (Branchwise conversion with separate side information)**.** Let $W$ be the table in Proposition 5.8, and write $Q = (Q^0, \ldots, Q^t)$ for its joint executions. Let $\pi(Q) \in \{0, 1\}^b$ be a fixed linear projection. For each prescribed value $r \in \{0, 1\}^b$, let $L_r(x)$ and $R_r(y)$ be arbitrary separate functions, each with at most $c$ output bits. They may depend on the fixed tampering functions. Define the actual side information by

$$J = (L_{\pi(Q)}(X), R_{\pi(Q)}(Y)).$$

Suppose $X, Y$ are independent flat sources of entropy at least $k$, $c + 2s \leqslant k/2$, and $b \leqslant s/4$. Then $(Q, J)$ is within

$$\delta = 2^{b+2-s} \tag{5.5}$$

of a probability mixture with the following properties on each component: $J$ and $\pi(Q)$ are fixed, $Q$ is jointly affine, and some honest row has entropy at least $s - b$. More specifically, that row is the projection of a uniform $s$-bit row after at most $b$ affine constraints.

*Proof.* If $\delta = 2^{b+2-s} \geqslant 1$, take a uniform full table tuple, fix $\pi(Q) = 0$, and fix $J$ arbitrarily. The resulting affine distribution has an honest row of entropy at least $s - b$, and its distance from the actual distribution is at most $1 \leqslant \delta$. Hence assume $\delta < 1$.

Fix $r$ temporarily, without conditioning on $\pi(Q) = r$. Condition separately on the values of $L_r(X)$ and $R_r(Y)$. These are product rectangles. On the left, labels of probability less than $2^{-c-2s}$ have total mass at most $2^{-2s}$, because there are at most $2^c$ labels. Outside them the conditional entropy is at least $k - c - 2s \geqslant k/2$. The same holds on the right.

On each good label rectangle apply Proposition 5.8 to the entire tuple $Q$. On bad label rectangles use an arbitrary affine tuple having a uniform honest row. Retain the fixed label values in either case. We have constructed a probability distribution $\widehat{P}_r$ on $(Q, J_r)$, where $J_r = (L_r(X), R_r(Y))$, such that

$$\Delta(\mathcal{L}(Q, J_r), \widehat{P}_r) \leqslant 2^{-s} + 2^{1-2s} \leqslant 2^{1-s}.$$

Every component of $\widehat{P}_r$ has fixed labels and a uniform honest row.

Now restrict both distributions to the event $\pi(Q) = r$, without normalizing these restricted measures, and sum over all $r$. The true measures sum to the actual probability distribution of $(Q, J)$, since the prefix events partition the sample space. Call the sum of the approximate measures $\nu$ and its mass $w$. The half-$\ell_1$ distance from the actual distribution to $\nu$ is at most $2^{b+1-s}$. To bound its mass separately, write $P_r = \mathcal{L}(Q, J_r)$ and $E_r = \{\pi(Q) = r\}$. Since $P_r$ and $\widehat{P}_r$ are probability distributions before restriction,

$$|\widehat{P}_r(E_r) - P_r(E_r)| \leqslant 2^{1-s}.$$

The true event probabilities sum to one, so $|w - 1| \leqslant \sum_r |\widehat{P}_r(E_r) - P_r(E_r)| \leqslant 2^{b+1-s}$. The mass estimate thus uses the event-probability bound for the probability distributions before restriction; it is separate from the half-$\ell_1$ estimate for the restricted measures. Since $\delta < 1$, we have $2^{b+1-s} = \delta/2 < 1/2$ and $w > 0$. Normalize $\nu$ by its mass. The additional half-$\ell_1$ cost is $|w - 1|/2$, and the total is at most $\frac{3}{2}2^{b+1-s} \leqslant 2^{b+2-s}$.

Restricting a uniform affine distribution to $\pi(Q) = r$ gives a uniform affine distribution on a nonempty fiber. At most $b$ independent affine constraints were imposed, so the dimension of every projection decreases by at most $b$. In particular, the formerly uniform honest row retains entropy at least $s - b$. The component weights are renormalized, but their affine supports and their fixed labels are unchanged. □

The summation over $2^b$ choices is exclusively an analysis. The evaluated extractor computes just its actual prefix and actual advice. Thus no exponential running time is introduced.

### 5.1.7 Affine correlation breaking and row merging

**Lemma 5.12** (Decomposition relative to all seed rows)**.** Suppose $(V_0, \ldots, V_h, R_0, \ldots, R_h)$ is jointly affine. There is a representation $V_j = A_j + B_j$ such that

$$(A_0, \ldots, A_h) \perp (B_0, \ldots, B_h, R_0, \ldots, R_h),$$

and

$$H_\infty(A_0) = H(V_0 \mid R_0, \ldots, R_h) \geqslant H(V_0) - \sum_{j=0}^{h} |R_j|.$$

Here $H$ denotes Shannon entropy in bits. For a uniform affine distribution, its Shannon entropy and min-entropy both equal its affine dimension. All nonempty fibers of the seed projection have

the same direction space, so the displayed conditional entropy is their common affine dimension; $|R_j|$ denotes the bit length of the seed $R_j$.

*Proof.* Write the support as an affine translate of a vector space $V$. The seed projection is a linear map on $V$. Choose a complementary subspace to its kernel: $V = V_{\mathrm{ker}} \oplus V_{\mathrm{sec}}$. Independent uniform choices from these two subspaces generate the uniform distribution on $V$. Project the kernel choice onto all data coordinates to obtain $(A_j)_j$. Project the section choice, including the affine offset, onto the data to obtain $(B_j)_j$; the section choice also determines all seeds. These two collections are independent. The image of the kernel on the honest coordinate is exactly the common direction of $V_0$ conditioned on the seed tuple. The entropy bound follows from the dimension inequality for projection onto that tuple. □

**Lemma 5.13** (Advised affine somewhere-random merger)**.** Let $T \geqslant 1$ and $t \geqslant 0$ be integers with $(t+1)T \geqslant 2$. Let $Q^0, \ldots, Q^t \in (\mathbb{F}_2^s)^T$ be jointly affine, and suppose some row of $Q^0$ has entropy at least $s - b$, where $b \geqslant 0$. Let $\alpha_0, \ldots, \alpha_t$ be fixed $a_0$-bit strings with $\alpha_0 \neq \alpha_j$ for every $j > 0$. Put

$$N = Ts, \quad M = (t+1)T, \quad v = \lceil \log(2M) \rceil, \quad a = a_0 + \lceil \log T \rceil.$$

For desired output length $q \geqslant 1$, instantiate Theorem 5.1 with $M - 1$ comparisons and primitive exponent

$$u = q + b + \lceil \log(1024M^3) \rceil.$$

Let $d, K$ be its seed length and entropy threshold. If $d \leqslant s$ and

$$s - b - Md \geqslant K, \tag{5.6}$$

then the common function below has $t$-non-malleability error at most $2^{-q}/4$ on this tuple. For $i \in [T]$, define $\mathrm{bin}_T(i)$ to be the $\lceil \log_2 T \rceil$-bit binary encoding of $i - 1$, padded with leading zeros (the empty string when $T = 1$). Using $\|$ for string concatenation, set

$$\mathrm{Merge}(Q, \alpha) = \bigoplus_{i=1}^{T} \mathrm{ACB}(Q, \mathrm{prefix}_d(Q_i), \alpha \,\|\, \mathrm{bin}_T(i)). \tag{5.7}$$

Each table is flattened to $N$ bits. Every advice string in this formula has the prescribed common length $a$, and distinct row indices have distinct encodings.

**Construction 5.2 Advised affine somewhere-random merger**

**Ingredients from earlier parts.** The quantitative affine correlation breaker of Theorem 5.1. Lemma 5.12 supplies its independence decomposition only in the analysis.

**Public parameters and fixed setup.** Given $T, s, t, a_0, b$ and target output length $q$, put

$$N = Ts, \quad M = (t+1)T, \quad a = a_0 + \lceil \log T \rceil, \quad u = q + b + \lceil \log(1024M^3) \rceil.$$

Instantiate the breaker for data length $N$, advice length $a$, $M-1$ comparisons, output length $q$, and exponent $u$. Let $d, K$ be its seed length and entropy threshold. Use only parameters satisfying $d \leqslant s$ and $s - b - Md \geqslant K$.

**Input.** One table $Q = (Q_1, \dots, Q_T) \in (\mathbb{F}_2^s)^T$ and one $a_0$-bit advice string $\alpha$.

**Evaluation steps.**

1. Flatten the *entire* table $Q$ to an $N$-bit data word.
2. For each $i \in [T]$, take $R_i = \mathrm{prefix}_d(Q_i)$ and append the $\lceil \log_2 T \rceil$-bit encoding of $i-1$ to $\alpha$.
3. Compute $Z_i = \mathrm{ACB}(Q, R_i, \alpha \parallel \mathrm{bin}_T(i))$ for every $i \in [T]$, and return $\bigoplus_{i=1}^{T} Z_i$.

**Output.** $q$ bits. Lemma 5.13 states the non-malleability guarantee for jointly affine comparison tables and fixed distinct honest/comparison advice. The algorithm evaluates $T$ calls, although its analysis counts $M = (t+1)T$ calls across all executions.

**Not evaluated.** The good row and the kernel–section decomposition. No independence among rows is assumed by the evaluator.

*Proof.* Choose a good honest row $i_*$ in the analysis. There are $M$ breaker calls, indexed by $(j, i)$ with $0 \leqslant j \leqslant t$, $1 \leqslant i \leqslant T$. The selected honest call is $(0, i_*)$; all other $M-1$ calls are its comparisons, including other rows of the honest table. Its advice differs from every comparison advice: unequal row indices suffice, and for equal indices the given $\alpha$ strings are distinct.

The data and seed tuple is jointly affine. The honest $d$-bit prefix has entropy at least $d - b$, since deleting $s - d$ coordinates loses at most that many entropy bits. Apply Lemma 5.12 to all $M$ calls. The selected data coordinate $Q^0$ has entropy at least $s - b$, so its independent residual part has entropy at least $s - b - Md \geqslant K$. The affine correlation breaker applies, without assuming that the original data and seed tuples are independent. Its error is at most $256M^3 2^{b-u} \leqslant 2^{-q}/4$.

Thus the selected output is nearly uniform given every other breaker output. XORing it with the other honest row outputs preserves uniformity, and the comparison-table XORs are functions of the already retained outputs. This proves the claim. □

If the fixed advice strings sometimes coincide in a mixture of such components, discard those components. Their total probability adds to the error. No affine noncollision condition on $Q^0, Q^j$ is needed when the fixed advice strings already differ.

## 5.2 Short-output non-malleability: construction and proof

The construction in this subsection is available for every fixed positive comparison count $t$. In the final $t$-tampering theorem it will be instantiated with comparison count $2t+1$ and a smaller source threshold. The proofs here are independent of the later long-output theorem.

**Construction 5.3 Short non-malleable extractor at decreasing entropy rate**

**Ingredients from earlier parts.** The table in Construction 5.1 and Proposition 5.8; the affine somewhere-random extractor of Theorem 2.28; the polynomial fingerprints of Theorem 5.10; and the advised merger of Lemma 5.13 (Construction 5.2).

**Public parameters and fixed setup.** Fix $t \geqslant 1$, $0 < \vartheta < 1/2$, and a working entropy threshold $k$ in the regime of Proposition 5.8. Build the table with condenser threshold $k/4$ and $s = \lfloor n^{1/2-\vartheta/2} \rfloor$. Let $T = L^2$ be its row count. Put $N = Ts$, $M = (t+1)T$, and $v = \lceil \log(2M) \rceil$. With the fixed sufficiently large absolute constant $C_*$ used below, set

$$\ell = \left\lfloor \frac{s}{C_* M^3 v^3} \right\rfloor, \qquad q = \left\lfloor \frac{\ell}{8H(T)} \right\rfloor, \qquad b = M\ell, \tag{5.8}$$

where $H(T) = (2T)^{a_1 \log(2T)}$ comes from Theorem 2.28. Instantiate that extractor on $T$ rows of $\ell$ bits and truncate its output to $q$ bits. Instantiate Construction 5.2 with $a_0 = 3q$, deficiency allowance $b$, and output length $q$. In particular its breaker uses $M-1$ comparisons and $u = q + b + \lceil \log(1024M^3) \rceil$; denote its seed length by $d$. The estimates below ensure $q \geqslant 4\log(n+2)$, $\ell/H(T) \geqslant (2T)^4$, $(t+1)q + 2s \leqslant k/2$, $b \leqslant s/4$, and $s - b - Md \geqslant K$.

**Input.** $(x, y) \in \{0,1\}^n \times \{0,1\}^n$.

**Evaluation steps.**

1. **Compute the table.** Form $W(x, y)$ by Construction 5.1, retaining its fixed row order.
2. **Compute a short ordinary seed from the heads.** For each row take its first $\ell$ bits to form $\mathrm{Head}(W)$. Apply the chosen affine somewhere-random extractor and take its $q$-bit prefix, denoted $S = S(W(x, y))$.
3. **Compute advice from the full original inputs.** Over $\mathbb{F}_{2^q}$, pad $x, y$ to $\lceil n/q \rceil$ coefficients and form their polynomials $P_x, P_y$ as in Theorem 5.10. Interpret $S$ as a field element and set $\alpha = (S, P_x(S), P_y(S)) \in \{0,1\}^{3q}$.
4. **Run all breaker calls and XOR.** For every row $i$, use as data the full flattened $Ts$-bit table, as seed its row prefix $\mathrm{prefix}_d(W_i)$, and as advice $\alpha \,\|\, \mathrm{bin}_T(i)$. Return

$$E_{\mathrm{short}}(x, y) = \mathrm{Merge}(W(x, y), \alpha(x, y)). \tag{5.9}$$

**Output.** $q = n^{1/2-\vartheta/2-o(1)}$ bits in the inverse-logarithmic regime, with error at most $2^{-q/2}$ by Theorem 5.15. The head seed $S$ and the per-row breaker seeds are *different* objects. Only the XOR of breaker outputs is returned here.

**Not evaluated.** Enumeration of hypothetical heads, advice conditioning, regularization rectangles, and affine components. The evaluator computes only its actual table, actual head seed, and actual advice.

### Ordinary seed extraction and advice separation

**Lemma 5.14** (The seed and advice guarantees)**.** At source entropy $k/2$, $S(x, y)$ is an ordinary extractor with error at most $2^{-4q}$. At source entropy $k$, it is strong with respect to either original source separately, with error at most $2^{1-3q}$. For every admissible list of tamperings the advice collision probability is at most

$$\zeta = t\left(2^{1-3q} + (\lceil n/q \rceil - 1)2^{-q}\right). \tag{5.10}$$

*Proof.* By Proposition 5.8, the honest table on entropy-$k/2$ sources is $2^{-s}$-close to a mixture of affine tables with a uniform row. Their heads have a uniform $\ell$-bit row. The affine somewhere-random

extractor therefore gives error at most $2^{-\ell/H(T)} + 2^{-s} \leqslant 2^{-4q}$. This first argument extends from flat sources by convexity. Since $k/2 \geqslant 4q$ for large $n$, Lemma 5.9 with slack $4q$ gives the two strong guarantees. Theorem 5.10 now gives (5.10). □

**Advice is fixed before the final joint conversion** For fixed tamperings put $f_0 = g_0 = \mathrm{id}$ and $Q^j = W(f_j(X), g_j(Y))$. The concatenation of all $M$ row heads is a $b$-bit linear projection of the full table tuple; denote it by $r = \pi(Q)$. For a prescribed value $r$, all $q$-bit seeds $s_j = S(Q^j)$ are determined. Define separate functions

$$L_r(x) = (P_{f_j(x)}(s_j))_{j=0}^{t}, \qquad R_r(y) = (P_{g_j(y)}(s_j))_{j=0}^{t}.$$

Each has $c = (t+1)q$ output bits. The complete advice tuple is determined by $r, L_r(x), R_r(y)$.

Apply Lemma 5.11. It gives an approximation, of distance at most $\delta = 2^{b+2-s}$, to the joint distribution of all tables and all advice, in which every component has fixed advice, jointly affine tables, and an honest row of entropy at least $s - b$. Notice that the fingerprints did not have to be affine functions of the tables: after a prescribed head is fixed, they are separate functions of the original inputs, so their fixings precede the rectangle regularization.

**Checking the breaker's entropy inequalities** Let $a = 3q + \lceil \log T \rceil$ and $u = q + b + \lceil \log(1024M^3) \rceil$. The parameter conditions above imply

$$a = O(\ell), \qquad u + \log(N+2) = O(M\ell).$$

Theorem 5.1 therefore supplies

$$\begin{aligned} d &= O(M^2 v^3 \ell), \\ K &= O((M^3 + M^2 v^3)\ell). \end{aligned}$$

Consequently

$$b + Md + K \leqslant C_1 M^3 v^3 \ell \leqslant s$$

for an absolute $C_1$, by choosing $C_* \geqslant 2C_1$. This also gives $d \leqslant s$ and verifies (5.6). Increasing $C_*$ further, if necessary, absorbs all integer rounding.

**Theorem 5.15** (Short-output non-malleability)**.** The function (5.9) has $q$ output bits and $t$-non-malleability error at most

$$\zeta + 2^{-q}/4 + 3 \cdot 2^{b+2-s}. \tag{5.11}$$

For sufficiently large $n$ this is at most $2^{-q/2}$.

*Proof.* First take flat sources and use the joint approximation just constructed. Advice-collision probability in the ideal mixture is at most $\zeta + \delta$, because this event is determined by the retained advice tuple. On every other component apply Lemma 5.13. The componentwise error is at most $2^{-q}/4$. Returning the honest/tampered output tuple to its actual distribution costs $\delta$, and returning the ideal tail marginal to its actual distribution costs another $\delta$. This proves (5.11). Decompose arbitrary independent sources into flat sources separately and average; all maps remain the original fixed maps.

Since $q \geqslant 4\log(n+2)$, we have $\zeta \leqslant 2t\, 2^{-3q/4}$. Also $b \leqslant s/4$ and $q \leqslant s/8$ imply $2^{b+2-s} \leqslant 2^{2-6q}$. For fixed $t$ and sufficiently large $q$, their sum in (5.11) is at most $2^{-q/2}$. □

**The inverse-logarithmic parameter calculation** At rate $C_{\vartheta,t}/\log n$, $T = (\log n)^{O(1)}$ and

$$M^3 v^3 H(T) = 2^{O_{\vartheta,t}((\log\log n)^2)} = n^{o(1)}.$$

With $s = \lfloor n^{1/2-\vartheta/2} \rfloor$ this yields

$$q = n^{1/2-\vartheta/2-o(1)} \geqslant n^{1/2-\vartheta}$$

for all sufficiently large $n$. In particular $q \gg \log n$, $\ell/H(T) \geqslant (2T)^4$, and $(t+1)q + 2s = o(k)$. This verifies every size condition used above.

The evaluated algorithm computes one table, one ordinary seed, two fingerprints, and $T$ correlation-breaker calls. All numbers of rows, field sizes in bits, and subroutine input lengths are polynomially bounded. The quantitative breaker is uniformly polynomial time in its parameters. Neither regularization partitions nor the $2^b$ prescribed heads are enumerated by the algorithm.

## 5.3 Source-strong output with additive entropy loss

The short-output construction above is used only to generate a seed. We now apply the centered recycling lemma from Section 4. The resulting evaluator retains its seed and XORs two source-local payloads. In particular, the final source-strength claim retains all actual long comparison outputs, not merely prefixes of them.

### 5.3.1 Prerequisite: a finite-budget recycling statement

**Lemma 5.16** (Centered recycling with explicit budgets)**.** Let $t \geqslant 0$ be an integer, put $q = t+1$ and $\rho_t = \lceil \log(2t+1) \rceil$, and let $A, B \geqslant 1$ be absolute constants in Lemma 2.23, with $A$ an integer. For integers $n, k \geqslant 1$ and $u \geqslant 2$ with $k \leqslant n$, set

$$d = \left\lceil B \left[ \log^2(n+2) + (u+1)\log\left(2 + \frac{n}{u+1}\right)\right]\right\rceil + A(u+1), \tag{5.12}$$

$$m = \left\lfloor \frac{k - 4u - \rho_t}{q} \right\rfloor, \qquad p = m - d, \qquad \kappa = k - tm - 2u. \tag{5.13}$$

Suppose $1 \leqslant h \leqslant k$, $p \geqslant 1$, and a $d$-bit seed $G$ is separately source-strong against up to $2t+1$ separate tamperings at component entropy threshold $h$, with error $\eta$ satisfying

$$\eta \leqslant 2^{-2qd-4u-4}, \tag{5.14}$$

$$k - tm - (t+2)d - h \geqslant 4u + 2. \tag{5.15}$$

There is an explicit strong seeded extractor $E : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^p$, and the map

$$F(x,y) = \big(G(x,y), E(x, G(x,y)) \oplus E(y, G(x,y))\big) \tag{5.16}$$

is separately source-strong $t$-non-malleable on all independent min-entropy-$k$ inputs, with error less than $10 \cdot 2^{-u}$. The same evaluator satisfies both source-strength comparisons and retains the complete actual $t$-tuple of $m$-bit tampered outputs.

*Proof.* First check the seeded-extractor interface. The integer $\kappa$ obeys $0 < \kappa \leqslant k \leqslant n$, and

$$\kappa - p = k - qm + d - 2u \geqslant d + 2u + \rho_t \geqslant A(u+1).$$

Thus Lemma 2.23 at threshold $\kappa$ and error $\zeta = 2^{-u}$ can supply $p$ output bits using at most $\lceil B\left[\log^2(n+2) + (u+1)\log\left(2+\frac{n}{u+1}\right)\right]\rceil \leqslant d$ seed bits. Ignore unused seed coordinates and truncate the output as necessary. The added $A(u+1)$ seed coordinates in (5.12) are harmless padding; they ensure the payload fits without putting the seeded extractor's entropy-loss constant into the final output deficit.

Apply Lemma 4.7 with its tampering count $C = t$, $\alpha = \beta = \zeta = 2^{-u}$, and its threshold equal to $h$. Its three energy terms are, respectively,

$$\begin{aligned}\Delta_1 &= (2t+1)2^{qm-k} \leqslant 2^{-4u},\\ \Delta_2 &= 2^{1+2u+(t+2)d+tm+h-k} \leqslant 2^{-2u-1},\\ \Delta_3 &= 4\eta\, 2^{2qd+2u} \leqslant 2^{-2u-2}.\end{aligned}$$

For the first inequality use $2t+1 \leqslant 2^{\rho_t}$ and $qm \leqslant k - 4u - \rho_t$; the other two are exactly (5.15) and (5.14). In particular, $\Delta_1 + \Delta_2 + \Delta_3 \leqslant 3 \cdot 2^{-2u}$. The centered lemma's distance is at most

$$8 \cdot 2^{-u} + \frac{\eta}{2} + \frac{\sqrt{3}}{2}2^{-u} < 10 \cdot 2^{-u}.$$

For completeness, when $Y = y$ is retained, subtract $E(y,s)$ from the honest payload and $E(g_i(y), s_i)$ from comparison $i$. These are bijections determined by $y$ and the displayed seed values. They turn the honest output into $(S_0, E(X, S_0))$ and the comparison tuple into

$$T = (\bar{S}, (E(f_i(X), S_i))_{i=1}^{t}),$$

which is the actual source-local leakage allowed in Lemma 4.7. Undoing the bijections preserves the honest uniform distribution and restores the original comparison marginal. Exchanging the sources and applying the same argument to $G^{\mathrm{op}}(x,y) = G(y,x)$ proves the comparison retaining $X$; the evaluated map (5.16) does not change. The proof for flat sources extends by independent flat-source mixtures, preserving each component's actual comparison/source marginal. When $t = 0$ the comparison tuple is empty, but the seed still has one-comparison non-malleability. □

### 5.3.2 Prerequisite: calibrating the lower-entropy short seed

**Lemma 5.17** (Inverse-logarithmic source-strong seed calibration)**.** Fix $t \geqslant 0$ and $0 < \vartheta < 1/2$. There are constants $c_0, C_{t,\vartheta} > 0$ and an integer $n_0$ such that the following holds for all $n \geqslant n_0$, $C_{t,\vartheta} n/\log n \leqslant k \leqslant n$, and

$$2^{-n^{1/2-\vartheta}} \leqslant \varepsilon \leqslant 1/4.$$

Put $q = t+1$, $R = 2t+1$,

$$h_0 = \lceil c_0 n/\log n\rceil, \qquad h = 2h_0, \qquad u = \lceil \log(1/\varepsilon)\rceil + 12, \tag{5.17}$$

and choose $d, m, p, \kappa$ by (5.12)–(5.13). Instantiate the short-output construction at threshold $h_0$ and comparison count $R$. If its output length is $q_0$, then

$$G(x,y) = \mathrm{prefix}_d\, E_{\mathrm{short}}(x,y)$$

is well-defined and satisfies every seed and length hypothesis of Lemma 5.16, including both source-strength comparisons at threshold $h$.

*Proof.* Use Theorem 5.15 and its inverse-logarithmic parameter calculation with comparison count $R = 2t + 1$ and exponent parameter $\vartheta$. Choose $c_0$ large enough for that construction at threshold $h_0$. Its length and error satisfy

$$q_0 = n^{1/2-\vartheta/2-o(1)}, \qquad \gamma_0 \leqslant 2^{-q_0/2}. \tag{5.18}$$

All constants may depend on the fixed $t, \vartheta$ but not on $k$ or $\varepsilon$. This invocation is of the *short-output* theorem, not of the long-output theorem proved below.

Uniformly over the stated error range,

$$\begin{aligned} &u \leqslant n^{1/2-\vartheta} + 13, \\ &d = O\big(n^{1/2-\vartheta} \log n + \log^2(n+2)\big) = o(q_0). \end{aligned} \tag{5.19}$$

Also $q_0 = o(h_0)$, so $d = o(h_0)$ and in particular $d \leqslant q_0$. The strict exponent gap between $1/2 - \vartheta$ and $1/2 - \vartheta/2$ absorbs the factor $\log n$ in $d$ and all fixed comparison-count factors. For all sufficiently large $n$ we therefore have

$$\min\{q_0/2, h_0\} \geqslant 4qd + 4u + 5. \tag{5.20}$$

Apply Lemma 2.5 to the first $d$ bits of the $R$-tampering seed, raising its threshold from $h_0$ to $h = 2h_0$. Since $R + 1 = 2q$, both strong errors are at most

$$\begin{aligned} \eta &\leqslant 2^{2qd}\big(2^{-q_0/2} + 2^{-h_0}\big) \\ &\leqslant 2^{1+2qd-\min\{q_0/2,h_0\}} \leqslant 2^{-2qd-4u-4}. \end{aligned} \tag{5.21}$$

The estimate is uniform over all admissible $R$ comparisons and all independent sources with min-entropy at least $h$. Thus it also applies to the auxiliary graph marginals and composed comparisons in the centered recycling lemma; no entropy is required in their tampered images.

Choose $C_{t,\vartheta} \geqslant 16qc_0$ and enlarge $n_0$ to absorb the ceilings. Then $h \leqslant k/(4q)$. Moreover, $d + u = o(k)$ uniformly in $k$ and $\varepsilon$, and $m = k/q - O_t(u+1)$. Hence $p = m - d \geqslant 1$. Using $m \leqslant k/q$ gives

$$\begin{aligned} k - tm - (t+2)d - h &\geqslant \frac{k}{q} - (t+2)d - h \\ &\geqslant \frac{3k}{4q} - (t+2)d \geqslant 4u + 2 \end{aligned}$$

for all sufficiently large $n$. These are the remaining hypotheses of Lemma 5.16. All lower bounds on $n$ can be chosen before the particular $k, \varepsilon$, because the estimates above use their worst allowed values. □

### 5.3.3 Main theorem and complete retained-seed construction

**Theorem 5.18** (Source-strong entropy-efficient output at rate $C/\log n$)**.** Fix an integer $t \geqslant 0$ and $0 < \vartheta < 1/2$. There are constants $C_{t,\vartheta} > 0$ and $n_0$ such that, for every $n \geqslant n_0$, integer $C_{t,\vartheta} n/\log n \leqslant k \leqslant n$, and

$$2^{-n^{1/2-\vartheta}} \leqslant \varepsilon \leqslant 1/4,$$

there is an explicit polynomial-time $t$-non-malleable two-source extractor $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$ with

$$m \geqslant \frac{k}{t+1} - O\big(\log(1/\varepsilon) + 1\big).$$

The implied additive-loss constant is absolute. For every independent min-entropy-$k$ pair and every admissible $t$-tuple of separate tamperings, put $\mathbf{Z} = (F(f_i(X), g_i(Y)))_{i=1}^{t}$. The same function satisfies

$$(F(X,Y), \mathbf{Z}, Y) \approx_\varepsilon (U_m, \mathbf{Z}, Y), \tag{5.22}$$

$$(F(X,Y), \mathbf{Z}, X) \approx_\varepsilon (U_m, \mathbf{Z}, X). \tag{5.23}$$

The uniform word is independent of the entire displayed marginal, and $\mathbf{Z}$ consists of the actual $m$-bit comparison outputs. For $t = 0$ this is ordinary extraction strong in either original source separately. No claim is made for a growing tampering count or for the exact square-root error exponent with fixed constants.

**Construction 5.4 Source-strong low-rate output with additive entropy loss**

**Ingredients from earlier parts.** The short extractor of Theorem 5.15 (Construction 5.3); the seed calibration of Lemma 5.17; the strong seeded extractor of Lemma 2.23; and the explicit-budget recycling interface of Lemma 5.16.

**Public parameters and fixed setup.** Fix $t \geqslant 0$, $0 < \vartheta < 1/2$, integer $C_{t,\vartheta} n/\log n \leqslant k \leqslant n$, and $2^{-n^{1/2-\vartheta}} \leqslant \varepsilon \leqslant 1/4$. Fix the absolute constants $A, B$ and calibration constant $c_0$. First set

$$\begin{aligned} q &= t+1, & R &= 2t+1, & \rho_t &= \lceil \log(2t+1) \rceil, \\ h_0 &= \lceil c_0 n/\log n \rceil, & h &= 2h_0, & u &= \lceil \log(1/\varepsilon) \rceil + 12. \end{aligned}$$

Choose

$$\begin{aligned} d &= \left\lceil B \left\lceil \log^2(n+2) + (u+1)\log\left(2 + \frac{n}{u+1}\right) \right\rceil \right\rceil + A(u+1), \\ m &= \left\lfloor \frac{k - 4u - \rho_t}{t+1} \right\rfloor, \qquad p = m - d, \qquad \kappa = k - tm - 2u. \end{aligned} \tag{5.24}$$

Instantiate Construction 5.3 at threshold $h_0$ and comparison count $R$, not $t$; denote its output length by $q_0$ to distinguish it from $q = t+1$. Define $G = \mathrm{prefix}_d E_{\mathrm{short}}$. Lemma 5.17 gives $d \leqslant q_0$ and the required source-strength guarantee at threshold $h$. Instantiate $E$ at entropy $\kappa$, error $2^{-u}$, $d$ seed bits (after ignored padding), and $p$ output bits.

**Input.** $(x, y) \in \{0,1\}^n \times \{0,1\}^n$.

**Evaluation steps.**

1. Evaluate that lower-threshold, $R$-comparison short extractor once on $(x, y)$ and retain its first $d$ bits as $S$.
2. Compute the $p$-bit words $E(x, S)$ and $E(y, S)$.
3. Return
$$S = G(x, y), \qquad F(x, y) = \big(S, E(x, S) \oplus E(y, S)\big). \tag{5.25}$$

**Output.** Exactly $m = d + p$ bits with the two source-strength guarantees of Theorem 5.18. The output includes the generated seed and retains no intermediate table or advice. The error is at most $10 \cdot 2^{-u} < \varepsilon$ under the stated parameter range.

**Not evaluated.** Strongification, regularization, posteriors, collision graphs, and the auxiliary comparison executions. These certify the three evaluated calls and are not additional computations.

*Proof.* Lemma 5.17 verifies all the seed, length, and entropy hypotheses of Lemma 5.16. The latter proves both comparisons with error $10 \cdot 2^{-u} \leqslant (10/4096)\varepsilon < \varepsilon$. Since $\rho_t \leqslant t+1$, the explicit length

satisfies

$$m \geqslant \frac{k}{t+1} - \frac{4(\lceil \log(1/\varepsilon) \rceil + 12)}{t+1} - 2 = \frac{k}{t+1} - O(\log(1/\varepsilon) + 1),$$

with an absolute constant. All selected lengths are positive for the uniform sufficiently large $n$ in the calibration lemma. The short construction and the two seeded calls are deterministic polynomial-time for fixed $t, \vartheta$. No rank condition is needed for this final nonlinear composition. □

At $\varepsilon = 2^{-n^{1/2-\vartheta}}$ the theorem gives $m \geqslant k/(t+1) - O(n^{1/2-\vartheta}) = (1 - o(1))k/(t+1)$, with both full-output source-strength guarantees. This replaces the older asymmetric boost and its shorter-output source-strong companion. The retained seed cancels its own length charge: only $p = m - d$ bits are extracted in each payload, but all $d$ seed bits are returned.

### 5.3.4 The ordinary source-strong corollary

**Corollary 5.19** (Near-$k$ source-strong ordinary output at inverse-logarithmic rate)**.** For each fixed $0 < \vartheta < 1/2$, there is $C_\vartheta > 0$ such that, for every sufficiently large $n$, every integer $C_\vartheta n/\log n \leqslant k \leqslant n$, and every

$$2^{-n^{1/2-\vartheta}} \leqslant \varepsilon \leqslant 1/4,$$

there is an explicit ordinary two-source extractor, strong in either original source separately, with

$$m \geqslant k - 4\lceil \log(1/\varepsilon) \rceil - 56, \qquad \text{error at most } \varepsilon.$$

The same evaluator satisfies both source-strength comparisons.

**Construction 5.5 Ordinary source-strong low-rate specialization**

**Ingredients from earlier parts.** Construction 5.4 and Theorem 5.18, with $t = 0$.

**Public parameters and fixed setup.** Set $q = 1$, $R = 1$, $\rho_0 = 0$, and $u = \lceil \log(1/\varepsilon) \rceil + 12$. Keep the seed length $d$ and lower seed threshold $h_0$ from Construction 5.4, and set $m = k - 4u$, $p = m - d$, $\kappa = k - 2u$.

**Input.** $(x, y) \in \{0,1\}^n \times \{0,1\}^n$ in Corollary 5.19's parameter range.

**Evaluation steps.**

1. Compute $S$ from the one-comparison short seed at threshold $h_0$.
2. Return $(S, E(x, S) \oplus E(y, S))$ with these specialized lengths.

**Output.** Exactly $k - 4\lceil \log(1/\varepsilon) \rceil - 48$ bits before any optional fixed truncation. This implies the corollary's stated lower bound $k - 4\lceil \log(1/\varepsilon) \rceil - 56$. The same evaluator is strong in either source separately; the internal seed still handles one comparison.

*Proof.* Set $t = 0$ in Theorem 5.18. Its seed uses one comparison, its leakage tuple is empty, and $\rho_0 = 0$. The explicit output length in (5.24) is $k - 4\lceil \log(1/\varepsilon) \rceil - 48$, which is at least the stated bound; an additional fixed truncation is harmless. Both strong comparisons follow directly. There is no separate output-amplification or collision argument in this corollary. □

## References


[1] Divesh Aggarwal, Yevgeniy Dodis, and Shachar Lovett. Non-malleable codes from additive combinatorics. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, 2014.

[2] Omar Alrabiah, Jesse Goodman, Jonathan Mosheiff, and João Ribeiro. Low-degree polynomials are good extractors, 2025. arXiv:2405.10297v2; Theorem 9.

[3] Srinivasan Arunachalam, Davi Castro-Silva, Arkopal Dutt, and Tom Gur. Algorithmic polynomial freiman–ruzsa theorems. Technical Report TR25-130, Electronic Colloquium on Computational Complexity, 2025. Lemma 3.3 (restricted homomorphism testing).

[4] Boaz Barak, R. Impagliazzo, and Avi Wigderson. Extracting randomness using few independent sources. In *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science*, pages 384–393, 2004.

[5] Boaz Barak, Guy Kindler, Ronen Shaltiel, Benny Sudakov, and Avi Wigderson. Simulating independence: New constructions of condensers, Ramsey graphs, dispersers, and extractors. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pages 1–10, 2005.

[6] Boaz Barak, Anup Rao, Ronen Shaltiel, and Avi Wigderson. 2 source dispersers for $n^{o(1)}$ entropy and Ramsey graphs beating the Frankl-Wilson construction. In *Proceedings of the 38th Annual ACM Symposium on Theory of Computing*, 2006.

[7] Avraham Ben-Aroya, Dean Doron, and Amnon Ta-Shma. An efficient reduction from two-source to nonmalleable extractors: Achieving near-logarithmic min-entropy. *SIAM Journal on Computing*, 51(2):STOC17–31–STOC17–49, 2022.

[8] Eli Ben-Sasson, Shachar Lovett, and Noga Ron-Zewi. An additive combinatorics approach relating rank to communication complexity. *J. ACM*, 61(4):22:1–22:18, 2014.

[9] Eli Ben-Sasson and Noga Ron-Zewi. From affine to two-source extractors via approximate duality. *SIAM Journal on Computing*, 44(6):1670–1697, 2015.

[10] Abhishek Bhowmick, Zeev Dvir, and Shachar Lovett. New bounds for matching vector families, 2013. arXiv:1204.1367v2; Lemma 7.9 and its proof.

[11] Jean Bourgain. More on the sum-product phenomenon in prime fields and its applications. *International Journal of Number Theory*, 1:1–32, 2005.

[12] Eshan Chattopadhyay, Jesse Goodman, and Jyun-Jie Liao. Affine extractors for almost logarithmic entropy. In *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022*, pages 622–633. IEEE, 2021.

[13] Eshan Chattopadhyay, Vipul Goyal, and Xin Li. Non-malleable extractors and codes, with their many tampered extensions. In *Proceedings of the 48th Annual ACM Symposium on Theory of Computing*, 2016.

[14] Eshan Chattopadhyay and Xin Li. Explicit non-malleable extractors, multi-source extractors and almost optimal privacy amplification protocols. In *Proceedings of the 57th Annual IEEE Symposium on Foundations of Computer Science*, 2016.

[15] Eshan Chattopadhyay and Xin Li. Extractors for sumset sources. In Daniel Wichs and Yishay Mansour, editors, *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC, Cambridge, MA, USA, June 18-21, 2016*, pages 299–311. ACM, 2016.

[16] Eshan Chattopadhyay and Jyun-Jie Liao. Extractors for sum of two sources. In Stefano Leonardi and Anupam Gupta, editors, *STOC '22: 54th Annual ACM SIGACT Symposium on Theory of Computing, Rome, Italy, June 20 - 24, 2022*, pages 1584–1597. ACM, 2022.

[17] Eshan Chattopadhyay and David Zuckerman. Explicit two-source extractors and resilient functions. *Annals of Mathematics*, 189:653–705, 2019.

[18] Mahdi Cheraghchi and Venkatesan Guruswami. Non-malleable coding against bit-wise and split-state tampering. In *TCC*, pages 440–464, 2014.

[19] Mahdi Cheraghchi and Piotr Indyk. Nearly optimal deterministic algorithm for sparse Walsh–Hadamard transform. In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2016)*, pages 1036–1045. Society for Industrial and Applied Mathematics, 2016.

[20] Benny Chor and Oded Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM Journal on Computing*, 17(2):230–261, 1988.

[21] Eldon Chung, Maciej Obremski, and Divesh Aggarwal. Extractors: Low entropy requirements colliding with non-malleability. Technical report, arXiv, 2021.

[22] Gil Cohen. Local correlation breakers and applications to three-source extractors and mergers. In *Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science*, 2015.

[23] Gil Cohen. Making the most of advice: New correlation breakers and their applications. In *Proceedings of the 57th Annual IEEE Symposium on Foundations of Computer Science*, 2016.

[24] Gil Cohen. Two-source dispersers for polylogarithmic entropy and improved ramsey graphs. In Daniel Wichs and Yishay Mansour, editors, *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016*, pages 278–284. ACM, 2016.

[25] Gil Cohen. Two-source extractors for quasi-logarithmic min-entropy and improved privacy amplification protocols. Technical Report TR16-114, ECCC: Electronic Colloquium on Computational Complexity, 2016.

[26] Gil Cohen. Towards optimal two-source extractors and ramsey graphs. In Hamed Hatami, Pierre McKenzie, and Valerie King, editors, *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 1157–1170. ACM, 2017.

[27] Gil Cohen and Leonard Schulman. Extractors for near logarithmic min-entropy. In *Proceedings of the 57th Annual IEEE Symposium on Foundations of Computer Science*, 2016.

[28] Yevgeniy Dodis, Ariel Elbaz, Roberto Oliveira, and Ran Raz. Improved randomness extraction from two independent sources. In *RANDOM 2004*, pages 334–344, 2004.

[29] Yevgeniy Dodis, Xin Li, Trevor D. Wooley, and David Zuckerman. Privacy amplification and non-malleable extractors via character sums. *SIAM Journal on Computing*, 43(2):800–830, 2014.

[30] Yevgeniy Dodis and Daniel Wichs. Non-malleable extractors and symmetric key cryptography from weak secrets. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, pages 601–610, 2009.

[31] Dean Doron and Jesse Goodman. Low-error extractors. *Manuscript in preparation*, 2026.

[32] Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan. Extensions to the method of multiplicities, with applications to kakeya sets and mergers. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science*, 2009.

[33] Zeev Dvir and Avi Wigderson. Kakeya sets, new mergers and old extractors. *SIAM Journal on Computing*, 40(3):778–792, 2011.

[34] Stefan Dziembowski, Krzysztof Pietrzak, and Daniel Wichs. Non-malleable codes. In *ICS*, pages 434–452, 2010.

[35] W. T. Gowers, Ben Green, Freddie Manners, and Terence Tao. On a conjecture of marton. *Annals of Mathematics*, 201:515–549, 2025.

[36] Venkatesan Guruswami, Christopher Umans, and Salil Vadhan. Unbalanced expanders and randomness extractors from parvaresh–vardy codes. *Journal of the ACM*, 56(4):Article 20, 2009. Theorems 5.12 and 5.14; Remark 5.15.

[37] A. A. Karatsuba. On a certain arithmetic sum. *Soviet Mathematics Doklady*, 12:1172–1174, 1971. English translation of Doklady Akademii Nauk SSSR, 199(4):770–772, 1971.

[38] A. A. Karatsuba. Distribution of values of dirichlet characters on additive sequences. *Doklady Akademii Nauk SSSR*, 319(3):543–545, 1991. English translation: Doklady Mathematics, 44(1):145–148, 1992.

[39] Mark Lewko. An explicit two-source extractor with min-entropy rate near 4/9. *Mathematika*, 65(4):950–957, 2019.

[40] Xin Li. Improved constructions of three source extractors. In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity*, pages 126–136, 2011.

[41] Xin Li. A new approach to affine extractors and dispersers. In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity*, pages 137–147, 2011.

[42] Xin Li. Non-malleable extractors, two-source extractors and privacy amplification. In *Proceedings of the 53rd Annual IEEE Symposium on Foundations of Computer Science*, pages 688–697, 2012.

[43] Xin Li. Extractors for a constant number of independent sources with polylogarithmic min-entropy. In *Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science*, pages 100–109, 2013.

[44] Xin Li. New independent source extractors with exponential improvement. In *Proceedings of the 45th Annual ACM Symposium on Theory of Computing*, pages 783–792, 2013.

[45] Xin Li. Three source extractors for polylogarithmic min-entropy. In *Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science*, 2015.

[46] Xin Li. Improved two-source extractors, and affine extractors for polylogarithmic entropy. In *Proceedings of the 57th Annual IEEE Symposium on Foundations of Computer Science*, 2016.

[47] Xin Li. Improved non-malleable extractors, non-malleable codes and independent source extractors. In *Proceedings of the 49th Annual ACM Symposium on Theory of Computing*, 2017.

[48] Xin Li. Non-malleable extractors and non-malleable codes: Partially optimal constructions. In Amir Shpilka, editor, *34th Computational Complexity Conference, CCC 2019, July 18-20, 2019, New Brunswick, NJ, USA*, volume 137 of *LIPIcs*, pages 28:1–28:49. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

[49] Xin Li. Two source extractors for asymptotically optimal entropy, and (many) more. In *64th Annual Symposium on Foundations of Computer Science, FOCS 2023, Santa Cruz, CA, USA, November 6-9, 2023*, pages 1271–1281. IEEE, 2023.

[50] Xin Li and Yan Zhong. Explicit directional affine extractors and improved hardness for linear branching programs. In *39th Computational Complexity Conference (CCC 2024)*, volume 300 of *LIPIcs*, pages 10:1–10:14, 2024. Also available as arXiv:2304.11495v2 [cs.CC].

[51] Xin Li and Yan Zhong. Two-source and affine non-malleable extractors for small entropy. In *51st International Colloquium on Automata, Languages, and Programming (ICALP 24)*, volume 297 of *LIPIcs*, pages 108:1–108:18, 2024. Also available as arXiv:2404.17013 [cs.CC].

[52] Xin Li and Yan Zhong. Non-malleable affine extractors with small error and complexity lower bounds. Technical report, arXiv, 2026. arXiv:2610.02407v1.

[53] Mehdi Makhul and Arne Winterhof. Normality of the thue–morse function for finite fields along polynomial values. *Research in Number Theory*, 8:38, 2022. Lemma 1.

[54] Anup Rao. Extractors for a constant number of polynomially small min-entropy independent sources. In *Proceedings of the 38th Annual ACM Symposium on Theory of Computing*, 2006.

[55] Anup Rao. Extractors for low-weight affine sources. In *Proc. of the 24th CCC*, 2009.

[56] Ran Raz. Extractors with weak random seeds. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pages 11–20, 2005.

[57] Victor Shoup. New algorithms for finding irreducible polynomials over finite fields. *Mathematics of Computation*, 54:435–447, 1990.

[58] David Zuckerman. Linear degree extractors and the inapproximability of max clique and chromatic number. *Theory of Computing*, 3:103–128, 2007. Theorem 4.3, attributed there to Raz.



ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il