Correction of Samplable Additive Errors

Kenji Yasunaga
Kanazawa University
yasunaga@se.kanazawa-u.ac.jp
April 5, 2017

Abstract

We study the correctability of efficiently samplable errors. Specifically, we consider the setting in which errors are efficiently samplable without the knowledge of the code or the transmitted codeword, and the error rate is not bounded. Assuming the existence of one-way functions, there are samplable pseudorandom distributions that are not correctable by efficient coding schemes. We show that there is an oracle relative to which there is a samplable flat distribution over \( \{0,1\}^n \) of entropy \( m \) that is not pseudorandom, but uncorrectable by efficient coding schemes of rate less than \( 1 - m/n - \omega(\log n/n) \). The result implies that correcting samplable additive errors is difficult even when they are not pseudorandom, and low-rate coding schemes are employed. We also show that the existence of one-way functions is necessary to derive impossibility results for coding schemes of rate less than \( 1 - m/n \) that correct flat distributions of entropy \( m \).

1 Introduction

In the theory of error-correcting codes, two of the most-studied channel models are probabilistic channels and worst-case channels. In probabilistic channels, errors are introduced through stochastic processes, and the most well-known one is the binary symmetric channel (BSC). In worst-case (or adversarial) channels, errors are introduced adversarially by considering the choice of codes and transmitted codewords under the restriction of the error rate. In his seminal work \([20]\), Shannon showed that reliable communication can be achieved over BSC if the coding rate is less than \( 1 - H_2(p) \), where \( H_2(\cdot) \) is the binary entropy function and \( p \) is the crossover probability of BSC. In contrast, it is known that reliable communication cannot be achieved over worst-case channels when the error rate is at least 1/4 unless the coding rate tends to zero \([19]\).

If we view the introduction of errors as computation of the channel, probabilistic channels perform low-cost computation with little knowledge about the code and the input, while worst-case channels perform high-cost computation with the full-knowledge. As intermediate channels between probabilistic channels and worst-case channels, Lipton \([16]\) introduced computationally-bounded channels, where errors are introduced by polynomial-time computation. He showed that reliable communication can be achieved at the coding rate less than \( 1 - H_2(p) \) in the shared randomness setting, where \( p < 1 \) is the error rate, which is the fraction of errors introduced by

*Preliminary version of parts of the work appeared in the Proceedings of the 2014 IEEE International Symposium on Information Theory.
the channel. Micali et al. [18] presented reliable coding schemes in the public-key infrastructure setting. Guruswami and Smith [10] showed reliable coding schemes without assuming the shared randomness or the public-key infrastructure. Note that these work [16, 18, 10] consider the settings in which channels are computationally-bounded and the error rate is bounded.

In this work, we also focus on computationally-bounded channels. In particular, we consider samplable additive channels, in which errors are sampled by efficient computation and added to the codeword in an oblivious way. More precisely, errors are sampled by a probabilistic polynomial-time algorithm, but the algorithm does not depend on the choice of the code or the transmitted codeword. This is stronger than the standard notion of obliviousness, where an oblivious channel can depend on the code, but not the codeword (cf. [15]).

Furthermore, in this work, we consider samplable additive channels with unbounded error rate. Namely, the error rate $p$ is not a priori bounded. Although most of the work in the literature focuses on bounded error-rate settings, this restriction might not be necessary for modeling errors generated by nature as a result of polynomial-time computation. We believe it is worth studying unbounded error-rate settings since exploring the correctability in unbounded error-rate settings can reveal what error structures can help to achieve error correction. In particular, the study on samplable additive errors can reveal what computational structures of errors are necessary to be corrected.

Samplable additive channels are relatively simple channel models since the error distributions are identical for every coding scheme and transmitted codeword. The binary symmetric channel is an example of samplable additive channels. Thus, we consider the setting in which coding schemes can be designed with the knowledge of the error distribution that is generated by an efficient algorithm. This setting is incomparable to previous notions of error correction against computationally-bounded channels. Our model is stronger because we do not restrict the error rate, but is weaker because the channel cannot see the code or the transmitted codeword.

1.1 Our Results

We would like to characterize samplable additive channels regarding the existence of efficient reliable coding schemes. We use the entropy of the error distributions as a criterion. The reason is that, if the entropy is zero, it is easy to achieve reliable communication since the error is a fixed string and this information can be used for designing a reliable coding scheme. On the other hand, if the error distribution has the full entropy, we could not achieve reliable communication since the truly random error will be added to the transmitted codeword. Thus, there seem to be bounds on the existence of efficient reliable coding schemes depending on the entropy of the underlying error distribution. When reliable coding schemes exist, an important quantity of the scheme is the information rate (or simply rate), which is the ratio of the message length to the codeword length. We investigate the bounds on the rate when reliable communication is achievable.

Let $Z$ be an error distribution over $\{0,1\}^n$ associated with a samplable additive channel, and $H(Z)$ the Shannon entropy of $Z$. Note that for a flat distribution, which is a uniform distribution over its support, $H(Z)$ is equal to the min-entropy of $Z$.

Basic observations. First, we observe several basic facts regarding the correctability of samplable additive errors.

Let consider flat distributions $Z$. It follows from a probabilistic argument that for any flat $Z$, there is a linear code that corrects $Z$ with error $\epsilon$ for rate $R \leq 1 - H(Z)/n - 2\log(1/\epsilon)/n$. 

2
The decoding complexity is $O(n^2 2^{H(Z)})$. Thus, if $H(Z) = O(\log n)$, the code can correct $Z$ in polynomial time. Conversely, by a simple counting argument, it holds that every flat distribution $Z$ is not correctable with error $\epsilon$ for rate $R > 1 - H(Z)/n + \log(1/(1 - \epsilon))/n$. In addition, we observe that it is difficult to construct a code that corrects the family of flat distributions with the same entropy. Specifically, we show that for every code of rate $k/n$ and every $m \leq k$, there is a flat distribution $Z$ with $H(Z) = m$ that is not correctable by the code.

A positive result can be obtained if we consider much more structured errors. If the error vectors form a linear subspace, there is an efficient coding scheme that corrects them by syndrome decoding with optimal rate $R = 1 - m/n$, where $m$ is the dimension of the linear subspace.

Regarding efficient coding schemes, we observe that if errors are pseudorandom (in the cryptographic sense), then efficient coding scheme cannot correct them. This implies that assuming the existence of one-way functions, there exist $Z$ with $H(Z) = n^\epsilon$ for $0 < \epsilon < 1$ that are not efficiently correctable.

**Errors with membership test.** To avoid the impossibility of correcting pseudorandom errors, we consider samplable distributions for which membership test can be done efficiently. Such distributions are not pseudorandom since the membership test can be used to distinguish them from the uniform distribution.

We show the existence of an uncorrectable distribution with membership test for low-rate codes. Specifically, we show that there is an oracle relative to which there exists a samplable distribution $Z$ of entropy $\omega(\log n)$ that is not correctable by efficient coding schemes of rate $R < 1 - H(Z)/n - \omega(\log n/n)$. The result complements the impossibility of correcting flat distributions for rate $R > 1 - H(Z)/n + O(1/n)$. Also, the entropy of $\omega(\log n)$ is optimal since, as in the above observations, there is a probabilistic construction of a code that corrects $Z$ in polynomial time if $H(Z) = O(\log n)$.

To derive this result, we use the technique of Wee [25], which is based on the reconstruction paradigm of Gennaro and Trevisan [8]. We use his technique for the problem of error correction. We show that if a samplable distribution with a sampler $S$ is efficiently correctable, then the function of $S$ has a short description, and thus, by a counting argument, efficient coding schemes cannot correct every samplable distribution with membership test.

This negative result seems counterintuitive. In general, constructing low-rate codes seems to be easier than high-rate codes. However, the result implies the impossibility of constructing low-rate codes. The reason for such a result is that the reconstruction paradigm crucially uses the fact that some function can be described shortly. In our case, we use the fact that functions for samplable errors can be described shortly if the errors are correctable by coding schemes with short descriptions. Since low-rate codes have short descriptions, the result can be applied to low-rate codes.

**Necessity of one-way functions.** Finally, we show that it is difficult to prove unconditional impossibility results for coding schemes of rate $R \leq 1 - H(Z)/n$. Specifically, we show that if one-way functions do not exist, then any samplable flat distribution $Z$ is correctable by an efficient coding scheme of rate $1 - H(Z)/n - O(\log n/n)$. Thus, it is necessary to assume the existence of one-way functions or oracle access to derive impossibility results for rate $R \leq 1 - H(Z)/n$.

The results are summarized in Table 1, where $R$ denotes the rate of coding schemes.
Table 1: Correctability of Samplable Additive Error(Z)

| $H(Z)$ | Correctabilities | Assumptions | References |
|--------|------------------|-------------|------------|
| $O(\log n)$ | Efficiently correctable with error $\epsilon$ for $R \leq 1 - \frac{H(Z)}{n} - \frac{2\log(1/\epsilon)}{n}$ | No | Proposition 3 |
| $\omega(\log n)$ | $\exists Z$ with membership test, not efficiently correctable for $R < 1 - \frac{H(Z)}{n} - \omega\left(\frac{\log n}{n}\right)$ | Oracle access | Corollary 1 |
| $n^\epsilon$ | $\exists Z$ not efficiently correctable for any $R$ | OWF | Proposition 7 |
| $1 \leq m \leq k$ | $\forall$ code with $R = k/n$, $\exists Z$ not correctable by the code | No | Proposition 5 |
| $\forall$ linear subspace $Z$ of dimension $m$, $\exists Z$ not correctable by the code | No | Proposition 6 |
| $\forall$ flat $Z$, $\exists$ (non-explicit) code correcting $Z$ with error $\epsilon$ for $R \leq 1 - \frac{H(Z)}{n} - \frac{2\log(1/\epsilon)}{n}$ | No | Proposition 3 |
| $\forall$ flat $Z$, (2) not correctable with error $\epsilon$ for $R > 1 - \frac{H(Z)}{n} + \frac{\log(1/(1-\epsilon))}{n}$ | No | Proposition 4 |
| $\forall$ flat $Z$ is efficiently correctable for $R \leq 1 - \frac{H(Z)}{n} - O\left(\frac{\log n}{n}\right)$ | No OWF | Theorem 3 |

1.2 Related Work

The notion of computationally-bounded channel was introduced by Lipton [16]. He showed that if the sender and the receiver can share secret randomness, then the Shannon capacity can be achieved for this channel. Micali et al. [18] considered a similar channel model in a public-key setting, and gave a coding scheme based on list-decodable codes and digital signature. Guruswami and Smith [10] gave constructions of capacity achieving codes for worst-case additive-error channel and time/space-bounded channels. In their setting of additive-error channel, the error rate is bounded, and the errors are only independent of the encoder’s random coins. They also gave strong impossibility results for bit-fixing channels, but their results can be applied to channels that use the information on the code and the transmitted codewords. In this work, we give impossibility results even for channels that do no use such information.

Samplable distributions were also studied in the context of data compression [9, 22, 25], randomness extractor [21, 24, 4], and randomness condenser [5]. Samplable distributions with membership test appeared in the study of efficient compressibility of samplable sources [9, 22, 25].

2 Preliminaries

For $n \in \mathbb{N}$, we write $[n]$ as the set $\{1, 2, \ldots, n\}$. For a distribution $X$, we write $x \sim X$ to indicate that $x$ is chosen according to $X$. We may use $X$ also as a random variable distributed according to $X$. The support of $X$ is $\text{Supp}(X) = \{x : \Pr_X(x) \neq 0\}$, where $\Pr_X(x)$ is the probability that $X$
assigns to \( x \). The Shannon entropy of \( X \) is \( H(X) = E_{x \sim X} \left[ -\log \Pr_X(x) \right] \). The min-entropy of \( X \) is given by \( \min_{x \in \text{Supp}(X)} \left( -\log \Pr_X(x) \right) \). It is known that the min-entropy of \( X \) is a lower bound on \( H(X) \). A flat distribution is a distribution that is uniform over its support. For flat distributions, the Shannon entropy is equal to the min-entropy. Thus, we simply say that a flat distribution \( Z \) has entropy \( m \) if its Shannon entropy is \( m \). For \( n \in \mathbb{N} \), we write \( U_n \) as the uniform distribution over \( \{0, 1\}^n \).

We define the notion of additive-error correcting codes.

**Definition 1.** (Additive-error correcting codes). For two functions \( \text{Enc} : \mathbb{F}^k \to \mathbb{F}^n \) and \( \text{Dec} : \mathbb{F}^n \to \mathbb{F}^k \), and a distribution \( Z \) over \( \mathbb{F}^n \), where \( \mathbb{F} \) is a finite field, we say \((\text{Enc}, \text{Dec})\) corrects (additive error) \( Z \) with error \( \epsilon \) if for any \( x \in \mathbb{F}^k \), we have that \( \Pr_{z \sim Z} [\text{Dec}(\text{Enc}(x) + z) \neq x] \leq \epsilon \). The rate of \((\text{Enc}, \text{Dec})\) is \( k/n \).

**Definition 2.** A distribution \( Z \) is said to be correctable with rate \( R \) and error \( \epsilon \) if there is a pair of functions \((\text{Enc}, \text{Dec})\) of rate \( R \) that corrects \( Z \) with error \( \epsilon \).

We call a pair \((\text{Enc}, \text{Dec})\) a coding scheme or simply code. The coding scheme is called efficient if \( \text{Enc} \) and \( \text{Dec} \) can be computed in polynomial-time in \( n \). The code is called linear if \( \text{Enc} \) is a linear mapping, that is, for any \( x, y \in \mathbb{F}^n \) and \( a, b \in \mathbb{F} \), \( \text{Enc}(ax + by) = a \text{Enc}(x) + b \text{Enc}(y) \). If \( |\mathbb{F}| = 2 \), we may use \( \{0, 1\} \) instead of \( \mathbb{F} \).

Next, we define syndrome decoding for linear codes.

**Definition 3.** For a linear code \((\text{Enc}, \text{Dec})\), \( \text{Dec} \) is said to be a syndrome decoder if there is a generator matrix \( G \in \mathbb{F}^{Rn \times n} \) and a function \( \text{Rec} : \mathbb{F}^{(n-Rn)} \to \mathbb{F}^n \) such that \( \text{Dec}(y) = (y - \text{Rec}(y \cdot H^T)) \cdot G^{-1} \), where \( \text{Enc}(x) = x \cdot G \) for all \( x \in \mathbb{F}^{Rn} \), \( G^{-1} \in \mathbb{F}^{n \times Rn} \) is a right inverse matrix of \( G \) \( \text{i.e.}, GG^{-1} = I \), and \( H \in \mathbb{F}^{(n-Rn) \times n} \) is a dual matrix of \( G \) \( \text{i.e.}, GH^T = 0 \).

We consider a computationally-bounded analogue of additive-error channels. We introduce the notion of sampleable distributions.

**Definition 4.** A distribution family \( Z = \{Z_n\}_{n \in \mathbb{N}} \) is said to be sampleable if there is a probabilistic polynomial-time algorithm \( S \) such that \( S(1^n) \) is distributed according to \( Z_n \) for every \( n \in \mathbb{N} \).

We consider the setting in which coding schemes can depend on the sampling algorithm of \( Z \), but not on its random coins, and \( Z \) does not use any information on the coding scheme or transmitted codewords. In this setting, the randomization of coding schemes does not help much.

**Proposition 1.** Let \((\text{Enc}, \text{Dec})\) be a randomized coding scheme that corrects a distribution \( Z \) with error \( \epsilon \). Then, there is a deterministic coding scheme that corrects \( Z \) with error \( \epsilon \).

**Proof.** Assume that \( \text{Enc} \) uses at most \( \ell \)-bit randomness. Since \((\text{Enc}, \text{Dec})\) corrects \( Z \) with error \( \epsilon \), we have that for every \( x \in \mathbb{F}^k \), \( \Pr_{z \sim Z, r \sim U_\ell} [\text{Dec}(\text{Enc}(x; r) + z) \neq x] \leq \epsilon \). By the averaging argument, for every \( x \in \mathbb{F}^k \), there exists \( r_x \in \{0, 1\}^\ell \) such that \( \Pr_{z \sim Z} [\text{Dec}(\text{Enc}(x; r_x) + z) \neq x] \leq \epsilon \). Thus, by defining \( \text{Enc}'(x) = \text{Enc}(x; r_x) \), the deterministic coding scheme \((\text{Enc}', \text{Dec})\) corrects \( Z \) with error \( \epsilon \). 

\( \square \)

The fact that the randomization does not help much is contrast to the setting of Guruswami and Smith [10], where the channels can use the information on the coding scheme and transmitted codewords, but not the random coins for encoding. They present a randomized coding scheme with optimal rate \( 1 - H_2(p) \) for worst-case additive-error channels, for which deterministic coding schemes are only known to achieve rate \( 1 - H_2(2p) \), where \( p \) is the error rate of the channels.
3 Basic Properties of Samplable-Additive Errors

We present several basic facts regarding the correctability of samplable additive errors. Although the claims in this section are elementary or folklore, we include the proofs for completeness.

3.1 Errors from Flat Distributions

For any flat distribution \( Z \), a random linear code can correct \( Z \) with high probability. Consider a random linear code of rate \( R \) such that the parity check matrix \( H \) is chosen uniformly at random from \( \mathcal{H}_R = \{0,1\}^{(n-Rn)\times n} \). The decoding is done in a brute-force way, namely, for a received word \( y \), find \( x \in \{0,1\}^{Rn} \) and \( z \in \text{Supp}(Z) \) such that \( y = x \cdot G + z \), and output \( x \), where \( G \) is a generator matrix for \( H \).

**Proposition 2.** For any flat distribution \( Z \) over \( \{0,1\}^n \), a random linear code from \( \mathcal{H}_R \) corrects \( Z \) with error \( 2^{-(n-Rn-H(Z))} \).

**Proof.** It is sufficient to show that, for a random \( H \) from \( \mathcal{H}_R \), every \( z \in \text{Supp}(Z) \) has a unique syndrome \( z \cdot H^T \) with high probability. For each \( z \in \text{Supp}(Z) \),

\[
\Pr_{H \in \mathcal{H}_R} \left[ \exists z' \in \text{Supp}(Z) \setminus \{z\} : z \cdot H^T = z' \cdot H^T \right] = \Pr_{H \in \mathcal{H}_R} \left[ \exists z' \in \text{Supp}(Z) \setminus \{z\} : \forall i \in [n-Rn], h_i \cdot (z-z') = 0 \right] \\
\leq \sum_{z' \in \text{Supp}(Z) \setminus \{z\}} \prod_{i \in [n-Rn]} \Pr_{h_i \in \{0,1\}^n} [h_i \cdot (z-z') = 0] \\
\leq 2^{-(n-Rn-H(Z))},
\]

where \( H^T = (h_1^T, \ldots, h_{n-Rn}^T) \) in (1), the last inequality follows from the fact that \( z-z' \neq 0 \) and \( |\text{Supp}(Z)| = 2^{H(Z)} \) for flat \( Z \). \( \square \)

By Proposition 2, for a \((1 - 2^{-(n-Rn-H(Z))})\)-fraction of \( H \) in \( \mathcal{H}_R \), the corresponding code corrects \( Z \) with error at most \( 2^{-(n-Rn-H(Z))}/2 \). Thus, we have the following proposition.

**Proposition 3.** Let \( Z \) be any flat distribution over \( \{0,1\}^n \) of entropy \( m \). There is a linear code of rate \( R \) that corrects \( Z \) with error \( \epsilon \) for \( R \leq 1 - m/n - 2\log(1/\epsilon)/n \). The decoding complexity is at most \( O(n^2 2^m) \).

**Proof.** The existence of such a code immediately follows from the above argument. Given a received word \( y \), the brute-force decoder checks if \((y-z) \cdot H^T = 0\) for all \( z \in \text{Supp}(Z) \), where \( H \) is the parity check matrix. If so, output \( x \) satisfying \( x \cdot G = y - z \). Thus, the decoding is done in time \( O(n^2) \cdot |\text{Supp}(Z)| \). \( \square \)

Proposition 3 implies that for any flat \( Z \) of entropy \( O(\log n) \), there is a code that corrects \( Z \) in polynomial time. Although the construction is not fully explicit, we can obtain such a code with high probability.

Conversely, we can show that the rate achieved in Proposition 3 is almost optimal.

**Proposition 4.** Let \( Z \) be any flat distribution over \( \{0,1\}^n \) of entropy \( m \). If a code of rate \( R \) corrects \( Z \) with error \( \epsilon \), then \( R \leq 1 - m/n + \log(1/(1-\epsilon))/n \).
Proposition 7. Assume that a one-way function exists. Then, for any $0 < \epsilon < 1$, there is a sampleable distribution $Z$ over $\{0,1\}^n$ such that $H(Z) \leq n^\epsilon$ and no polynomial-time algorithms $(\text{Enc}, \text{Dec})$ can correct $Z$.

Proof. If a one-way function exists, there is a pseudorandom generator $G : \{0,1\}^{n^\epsilon} \rightarrow \{0,1\}^n$ secure for any polynomial-time algorithm [12]. Then, a distribution $Z = G(U_{n^\epsilon})$ is not correctable by polynomial-time algorithms $(\text{Enc}, \text{Dec})$. If so, we can construct a polynomial-time distinguisher for pseudorandom generator by employing $(\text{Enc}, \text{Dec})$, and thus a contradiction follows. \square
4 Errors with Membership Test

Since pseudorandom distributions are not correctable by efficient schemes, we investigate the correctability of distributions that are not pseudorandom. For such distributions, we consider distributions for which the membership test can be done efficiently. A distribution $Z$ is called a distribution with membership test if there is a polynomial-time algorithm $D$ such that $D(z) = 1 \iff z \in \text{Supp}(Z)$.

Since the algorithm $D$ can distinguish $Z$ from the uniform distribution, $Z$ is not pseudorandom.

We show that there is an oracle relative to which there exists a samplable distribution with membership test that is not correctable by efficient coding schemes with low rate.

Let $N = 2^n$, $K = 2^k$, $M = 2^m$. Let $\mathcal{F}$ be the set of injective functions $f : \{0,1\}^m \rightarrow \{0,1\}^n$. For each $f \in \mathcal{F}$, define an oracle $O_f$ such that

$$O_f(b, y) = \begin{cases} O_f^S(y) & \text{if } b = 0, y \in \{0,1\}^m \\ O_f^M(y) & \text{if } b = 1, y \in \{0,1\}^n \\ \bot & \text{otherwise} \end{cases}$$

Let $\text{correct}_f$ be the set of functions $f \in \mathcal{F}$ for which there exist oracle circuits $(\text{Enc}, \text{Dec})$ that make $q$ queries to oracle $O_f$ and correct $f(U_m)$ with rate $k/n$. For each $f \in \mathcal{F}$ and the corresponding $(\text{Enc}, \text{Dec})$, we define

$$\text{invert}_f = \{ y \in \{0,1\}^m : \text{for any } x \in \{0,1\}^k, \text{ on input } \text{Enc}(x) + f(y), \text{ Dec queries } O_f^S \text{ on } y \},$$

$$\text{forge}_f = \{ y \in \{0,1\}^m : \text{for some } x \in \{0,1\}^k, \text{ on input } \text{Enc}(x) + f(y), \text{ Dec does not query } O_f^S \text{ on } y \}.$$

Note that $\text{invert}_f$ and $\text{forge}_f$ is a partition of $\{0,1\}^m$. We also define

$$\text{invertible} = \{ f \in \text{correct}_f : |\text{invert}_f| > \epsilon \cdot 2^m \},$$

$$\text{forgeable} = \{ f \in \text{correct}_f : |\text{forge}_f| \geq \delta \cdot 2^m \},$$

where $\epsilon$ and $\delta$ are any positive constants satisfying $\epsilon + \delta = 1$. Note that $\text{correct}_f = \text{invertible} \cup \text{forgeable}$.

Intuitively, if $f$ is in invertible, then there is a small circuit that inverts $f$. This is done by computing $\text{Enc}(x) + f(y)$ and monitoring oracle queries that $\text{Dec}(\text{Enc}(x) + f(y))$ makes to $O_f^S$. Since a random function is one-way with high probability, we can show that the size of invertible functions, i.e., invertible, is small. Similarly, if $f$ is in forgeable, then $\text{Dec}$ corrects $f(y)$ without querying $O_f^S$ on $y$. This means that $f(y)$ can be described using $\text{Dec}$ and $\text{Enc}(x) + f(y)$, and thus if $\text{Enc}(x) + f(y)$ has a short description, the size of forgeable is small.

To argue the above intuition formally, we use the reconstruction paradigm of [8]. Then, we show that both invertible and forgeable are small.

First, we show that $f$ in invertible has a short description.

**Lemma 1.** Take any $f \in \text{invertible}$ and the corresponding pair of oracle circuits $(\text{Enc}, \text{Dec})$ that makes at most $q$ queries to $O_f$ in total and corrects $f(U_m)$ with rate $k/n$. Then $f$ can be described using at most

$$\log \left( \binom{N}{c} \right) + \log \left( \binom{M}{c} \right) + \log \left( \binom{N-c}{M-c} (M-c)! \right)$$
bits, given \((\text{Enc}, \text{Dec})\), where \(c = \epsilon M / q\).

**Proof.** First, consider an oracle circuit \(A\) such that, on input \(z\), \(A\) picks any \(x \in \{0,1\}^k\) and simulates \(\text{Dec}\) on input \(\text{Enc}(x) + z\). Then, for any \(y \in \text{invert}_f\), on input \(f(y)\), \(A\) outputs \(y\) by making at most \(q\) queries to \(O_f\).

Next, we show that for any \(f \in \text{invertible}\), \(f\) has a short description given \(A\). Without loss of generality, we assume that \(A\) makes distinct queries to \(O^S_f\). We also assume that on input \(f(y)\), \(A\) always queries \(O^S_f\) on \(y\) before it outputs \(y\). We will show that there is a subset \(T \subseteq f(\text{invert}_f)\) such that \(f\) can be described given \(T\), \(B(T)\), \(f|_{\{0,1\}^m \setminus B(T)}\), where \(B(T) = \{y \in \{0,1\}^m : y \leftarrow A(z), z \in T\}\).

We describe how to construct \(T\) below.

**Construct-\(T\):**

1. Initially, \(T\) is empty, and all elements in \(T^* = f(\text{invert}_f)\) are candidates for inclusion in \(T\).
2. Choose the lexicographically smallest \(z\) from \(T^*\), put \(z\) in \(T\), and remove \(z\) from \(T^*\).
3. Simulate \(A\) on input \(z\), and halt the simulation immediately after \(A\) queries \(O^S_f\) on \(y\). Let \(y_1, \ldots, y_p\) be the queries that \(A\) makes to \(O^S_f\), where \(y_p = y\) and \(p \leq q\).
   - Remove \(f(y_1), \ldots, f(y_{p-1})\) from \(T^*\). (This means that these elements will never belong to \(T\), and in simulating \(A(z)\) in the recovering phase, the answers to these queries are made by using the look-up table for \(f\).)
   - Continue to remove the lexicographically smallest \(z\) from \(T^*\) until we have removed exactly \(q - 1\) elements in Step 3.
4. Return to Step 2.

Next, we describe how to reconstruct \(f\) from \(T\), \(B(T)\), and \(f|_{\{0,1\}^m \setminus B(T)}\). We show how to recover the look-up table for \(f\) on values in \(B(T)\).

**Recover-\(f\):**

1. Choose the lexicographically smallest element \(z \in T\), and remove it from \(T\).
2. Simulate \(A\) on input \(z\), and halt the simulation immediately after \(A\) queries \(O^S_f\) on \(y\) for which the answer does not exist in the look-up table for \(f\). Since the query \(y\) satisfies that \(y = f^{-1}(z)\), add the entry \((y, z)\) to the look-up table.
   
   In what follows, we explain why we can correctly simulate \(A(z)\).
   - Since \(B(T)\) and \(f|_{\{0,1\}^m \setminus B(T)}\) are given, we can answer all queries to \(O^M_f\).
   - For any query \(y'\) to \(O^S_f\), it must be either (1) \(y' \notin B(T)\), or (2) \(y'\) is the output of \(A\) on input \(z'\) such that \(z' \in W\) and \(z'\) is lexicographically smaller than \(z\). In either case, the look-up table has the corresponding entry, and thus we can answer the query.

3. Return to Step 1.

In each iteration in **Construct-\(T\)**, we add one element to \(T\) and remove exactly \(q\) elements from \(T^*\). Since initially the size of \(T^* = f(\text{invert}_f)\) is \(cM\), the size of \(T\) in the end is \(c = \epsilon M / q\).

The sets \(T\) and \(B(T)\), and the look-up table for \(f|_{\{0,1\}^m \setminus B(T)}\) can be described using \(\log(\binom{N}{c})\), \(\log(M!)\), and \(\log((\binom{N}{c})!)(M - c)!\), respectively. Therefore, the statement follows. \(\square\)
We show that the fraction of \( f \in \mathcal{F} \) for which \( f \in \text{invertible} \) and \( f(U_m) \) is correctable is small.

**Lemma 2.** If \( m > 3 \log s + \log n + O(1) \), then the fraction of functions \( f \in \mathcal{F} \) such that \( f \in \text{invertible} \) and \( f(U_m) \) can be corrected by a pair of oracle circuits \((\text{Enc}, \text{Dec})\) of total size \( s \) is less than \( 2^{-(sn \log s + 1)} \) for all sufficiently large \( n \).

**Proof.** It follows from Lemma 1 that, given \((\text{Enc}, \text{Dec})\), the fraction is

\[
\frac{|\text{invertible}|}{(N/M)!} \leq \frac{(N-M)!}{(M-c)!} \frac{M-c}{M}! = \frac{(M-c)!}{c!},
\]

where \( c = \epsilon M/(qK) \). By using the fact that \( q \leq s \) and the inequalities \( \binom{n}{k} < \left( \frac{en}{k} \right)^k \) and \( n! > \left( \frac{2e}{n} \right)^n \), the expression is upper bounded by

\[
\left( \frac{eM}{c} \right)^c \left( \frac{e}{c} \right)^c = \left( \frac{e^2 q^2}{e^2 M} \right)^{\epsilon M/q} \leq \left( \frac{1}{2} \right)^{ns \log s + 1}
\]

for all sufficiently large \( n \). The last inequality follows from the fact that

\[
e^2 q^2 \leq e^2 \Omega(s^3 n) < \frac{1}{2} \quad \text{and} \quad \frac{\epsilon M}{q} \leq \frac{\epsilon \Omega(s^3 n)}{q} > ns \log s + 1.
\]

Next, we show that forgeable has a short description.

**Lemma 3.** Take any \( f \in \text{forgeable} \) and the corresponding pair of oracle circuits \((\text{Enc}, \text{Dec})\) that make at most \( q \) queries to \( O_f \) in total and corrects \( f(U_m) \) with rate \( k/n \). Then \( f \) can be described using at most

\[
\log \left( \frac{M}{d} \right) + \log \left( \binom{N-d}{M-d} \right) + (\delta M/q)
\]

bits, given \((\text{Enc}, \text{Dec})\), where \( d = \delta M/q \).

**Proof.** First, consider an oracle circuit \( A \) such that, on input \( w \), \( A \) obtains \( x \) by simulating Dec on input \( w \), queries \( O_f^M \) on \( w - \text{Enc}(x) \), and outputs \( \bot \) if \( O_f^M(w - \text{Enc}(x)) = 0 \), and \( x \) otherwise. Then, \( A \) satisfies that, on input \( w \), \( A \) outputs \( \bot \) if \( w \notin \text{Enc}(0,1)^k \) or \( f(\{0,1\}^m) \), and Dec \( (w) \) otherwise.

Next, we show that for any \( f \in \text{forgeable} \), \( f \) has a short description given \( A \). Without loss of generality, we assume that \( A \) makes distinct queries to \( O_f^S \) and \( O_f^M \). We also assume that for \( x \in \{0,1\}^k \) and \( y \in \{0,1\}^m \), \( A(\text{Enc}(x) + f(y)) \) always queries \( O_f^M \) on \( f(y) \) before it outputs \( x \). Note that for \( y \in \text{forge}_f \), there is some \( x \in \{0,1\}^k \) such that, on input \( \text{Enc}(x) + f(y) \), \( A \) does not query \( O_f^S \) on \( y \).

We will show that there is a subset \( Y \subseteq \text{forge}_f \) such that \( f \) can be described given \( Y, f|_{\{0,1\}^m \backslash Y}, \) and \( \{(x,y,a_y,b_y) \in \{0,1\}^k \times [M] \times [q] : y \in Y\} \) of a set of advice strings. For \( x \in \{0,1\}^k \), we define \( D(x) = \{ \text{Enc}(x) + f(y) : y \in \{0,1\}^m \} \). Note that \( |D(x)| = M \) for any \( x \in \{0,1\}^k \).

We describe how to construct \( Y \) below.

**CONSTRUCT-Y:**
1. Initially, $Y$ is empty. All elements in $Y^* = \text{forge}_f$ are candidates for inclusion in $Y$. For every $x \in \{0,1\}^k$, set $D_x = \{\text{Enc}(x) + f(y) : y \in \text{forge}_f\}$. We write $D_k = \bigcup_{x \in \{0,1\}^k} D_x$.

2. Choose the lexicographically smallest $y$ from $Y^*$, put $y$ in $Y$, and remove $y$ from $Y^*$.

3. Choose the lexicographically smallest $w$ from the set of $\text{Enc}(x) + f(y) \in D_x$ such that $A$ does not query $O_f^y$ on $y$. If $w = \text{Enc}(x) + f(y)$, set $x_y = x$. Then, for every $x' \in \{0,1\}^k$, remove $\text{Enc}(x') + f(y)$ from $D_{x'}$. (This removal means that hereafter there are no elements in $D_k$ for which $A$ outputs some $x$ such that $f(y)$ is the error vector.) When $w$ is the lexicographically $t$-th smallest element in $D(x)$, set $a_y = t$ (so that we can recognize that the $a_y$-th element in $D(x)$ is $w$ in the recovering phase).

4. Simulate $A$ on input $w$, and halt the simulation immediately after $A$ queries $O_f^M$ on $f(y)$. Let $y'_1, \ldots, y'_p$ be the queries that $A$ makes to $O_f^y$, and $z'_1, \ldots, z'_r = f(y)$ be the queries that $A$ makes to $O_f^M$. Set $b_y = r$ (so that we can recognize that the $b_y$-th query that $\text{Dec}$ makes to $O_f^M$ is $f(y)$ in the recovering phase).

(a) For every $x' \in \{0,1\}^k$, remove $\text{Enc}(x') + f(y'_1), \ldots, \text{Enc}(x') + f(y'_p)$ from $D_{x'}$.

(b) For every $i \in [p]$, if $z'_i \in f(\text{forge}_f)$, then for every $x' \in \{0,1\}^k$, remove $\text{Enc}(x') + z'_i$ from $D_{x'}$, and otherwise, do nothing.

(c) Continue to remove the elements $\text{Enc}(x') + f(y)$ from $D_{x'}$ for every $x' \in \{0,1\}^k$ for the lexicographically smallest $w = \text{Enc}(x) + f(y) \in D_k$ until we have removed exactly $(q-1)K$ elements from $D_k$ in Step 4.

5. Return to Step 2.

Next, we describe how to construct $f$ from $Y$, $f|_{\{0,1\}^m \setminus Y}$, and $(x_y, a_y, b_y) \in \{0,1\}^k \times [M] \times [q] : y \in Y$. We show how to recover the look-up table for $f$ on values in $Y$.

**RECOVER-$f$:**

1. Choose the lexicographically smallest $y \in Y$, and remove it from $Y$. Then, choose the lexicographically $a_y$-th smallest element $w$ from $D(x_y)$.

2. Simulate $A$ on input $w$, and halt the simulation immediately after $A$ makes the $b_y$-th query to $O_f^M$. Since the $b_y$-th query is $f(y)$, add the entry $(y, f(y))$ to the look-up table.

In what follows, we explain why we can correctly simulate $A(w)$.

- For any query $y'$ to $O_f^y$, it must be either (1) $y' \notin Y$ or (2) $y'$ is lexicographically smaller than $y$. In case (1), we can answer the query by using $f|_{\{0,1\}^m \setminus Y}$. In case (2), since $y$ was chosen as the lexicographically smallest element such that $A$ does not query $O_f^y$ on $y$, the look-up table has the answer to the query.

- Consider any of the first $b_y - 1$ queries $z'$ to $O_f^M$. If $z' \in f(\{0,1\}^m)$, namely $z' = f(y')$ for some $y'$, then it must be either (1) $y' \notin Y$ or (2) $y'$ is lexicographically smaller than $y$. In either case, the look-up table has the entry $(y', z')$. If $z' \notin f(\{0,1\}^m)$, there is no entry for $z'$ in the look-up table. Thus, we can answer the query by saying “yes” if $z'$ is in the look-up table, and “no” otherwise.

3. Return to Step 1.

In each iteration in CONSTRUCT-$Y$, we add one element to $Y$ and remove exactly $qK$ elements from $D_k$. Since initially the size of $D_k$ is at least $\delta KM$, the size of $Y$ in the end is at least $d = \delta M/q$. 

11
The set $Y$, the look-up table for $f|_{\{0,1\}^m \setminus Y}$, the sets $\{(x_y, a_y, b_y) \in \{0,1\}^k \times [M] \times [q] : y \in Y\}$ can be described using $\binom{M}{d}$, $\log((\frac{N-d}{M-d})(M-d)!)$, and $d(k + m + \log q)$ bits respectively. Therefore, the statement follows.

We show that the fraction of $f \in \mathcal{F}$ for which $f \in \text{forgeable}$ and $f(U_m)$ is correctable is small.

**Lemma 4.** If $m > 3\log s + \log n + O(1)$ and $m < n - k - 2\log s - O(1)$, then the fraction of functions $f \in \mathcal{F}$ such that $f \in \text{forgeable}$ and $f(U_m)$ can be corrected by a pair of oracle circuits $(\text{Enc}, \text{Dec})$ of total size $s$ is less than $2^{-(sn\log s + 1)}$ for all sufficiently large $n$.

**Proof.** It follows from Lemma 3 that, given $(\text{Enc}, \text{Dec})$, the fraction is

$$
\frac{|\text{forgeable}|}{\binom{N}{M} M!} \leq \frac{\binom{M}{d}(\frac{N-d}{M-d})(M-d)!}{\binom{N}{M} M!} 2^{d(k + m + \log q)} = \frac{\binom{M}{d}}{\binom{N}{M} d!} (qKM)^d,
$$

where $d = \delta M / q$. By using the fact that $q \leq s$ and the inequalities $\binom{n}{k} < \left(\frac{en}{k}\right)^k$, $\binom{n}{k} > \left(\frac{n}{k}\right)^k$, and $n! > \left(\frac{n}{e}\right)^n$, the expression is upper bounded by

$$
\left(\frac{eM}{d}\right)^d \left(\frac{d}{N}\right)^d \left(\frac{e}{d}\right)^d (qKM)^d = \left(\frac{e^2q^2KM}{\delta N}\right)^{\delta M/q} < \left(\frac{1}{2}\right)^{ns\log s + 1}
$$

for all sufficiently large $n$. The last inequality follows from the fact that

$$
\frac{e^2q^2KM}{\delta N} < \frac{e^2q^2}{\delta \Omega(s^2n)} < \frac{1}{2} \quad \text{and} \quad \frac{\delta M}{q} > \frac{\delta \Omega(s^3n)}{q} > ns\log s + 1.
$$

We obtain the main result of this section.

**Theorem 1.** For any $m$ and $k$ satisfying $3\log s + \log n + O(1) < m < n - k - 2\log s - O(1)$, there exist injective functions $f : \{0,1\}^m \rightarrow \{0,1\}^n$ such that, given oracle access to $O_f$, (1) $f(U_m)$ is a samplable distribution with membership test of entropy $m$, and (2) $f(U_m)$ cannot be corrected with rate $k/n$ by oracle circuits of size $s$.

**Proof.** Since correct $f = \text{invertible} \cup \text{forgeable}$, it follows from Lemmas 2 and 4 that for a fixed $(\text{Enc}, \text{Dec})$ of size $s$, the fraction of functions $f \in \mathcal{F}$ such that $(\text{Enc}, \text{Dec})$ corrects $f(U_m)$ with rate $k/n$ is less than $2^{-(sn\log s)}$. Since there are at most $2^{sn\log s}$ circuits of size $s$, there are functions $f \in \mathcal{F}$ such that $f(U_m)$ cannot be corrected with rate $k/n$ by oracle circuits of size $s$. Given oracle access to $O_f$, $f(U_m)$ is samplable. Since $f$ is injective, $f(U_m)$ has entropy $m$.

The following corollary immediately follows.

**Corollary 1.** For any $m$ and $k$ satisfying $\omega(\log n) < m < n - k - \omega(\log n)$, there exists an oracle relative to which there exists a samplable distribution with membership test of entropy $m$ that cannot be corrected with rate $k/n$ by polynomial size circuits.
5 Necessity of One-Way Functions

We show that if one-way functions do not exist, then any samplable flat distribution of entropy \( m \) is correctable by an efficient coding scheme of rate \( 1 - m/n - O(\log n/n) \). For this, we use a technique used in the proof of [25, Theorem 6.3] that shows the necessity of one-way functions for separating pseudoentropy and compressibility. We observe that in its proof, a family of linear hash functions is used for giving an efficient compression function. Since a linear compression function is a dual object of a linear code that corrects additive errors, we can use a family of linear hash functions for constructing an efficient decoder.

Definition 5 ([13]). We say a function \( f \) is distributionally one-way if it is computable in polynomial time and there exists a constant \( c > 0 \) such that for every probabilistic polynomial-time algorithm \( A \), the statistical distance between \( (x, f(x)) \) and \( (A(f(x)), f(x)) \) is at least \( 1/n^c \), where \( x \sim U_n \).

Theorem 2 ([13]). If there is a distributionally one-way function, then there is a one-way function.

Theorem 3. If one-way functions do not exist, then any samplable flat distribution \( Z \) over \( \{0, 1\}^n \) of entropy \( m \) can be corrected with rate \( 1 - m/n - (c \log n)/n \) and error \( O(n^{-c}) \) for any constant \( c > 0 \) by polynomial-time coding schemes.

Proof. Let \( Z = f(U_m) \) for an efficiently computable function \( f \). Consider a family of linear universal hash functions \( \mathcal{H} = \{ h : \{0, 1\}^n \to \{0, 1\}^{n+2c \log n} \} \), where the universality means that for any distinct \( x, x' \in \{0, 1\}^n \), \( \Pr_{h \in \mathcal{H}}[h(x) = h(x')] \leq 2^{-(m+2c \log n)} \), and the linearity means that for any \( x, x' \in \{0, 1\}^n \) and \( a, b \in \{0, 1\} \), \( h(ax + bx') = ah(x) + bh(x') \). For each \( h \in \mathcal{H} \), we define \( C_h = \{ x \in \text{Supp}(Z) : \exists x' \in \text{Supp}(Z) \text{ s.t. } x' \neq x \land h(x) = h(x') \} \). Namely, \( C_h \) is the set of inputs with collisions under \( h \). By a union bound, it holds that for any \( x \in \text{Supp}(Z) \),

\[
\Pr_{h \in \mathcal{H}}[\exists x' \in \text{Supp}(Z) : x' \neq x \land h(x') = h(x)] \leq \frac{2^m}{2^{m+2c \log n}} = \frac{1}{n^{2c}}.
\]

Thus, \( E[|C_h|] \leq 2^m/n^{2c} \). We say \( h \in \mathcal{H} \) is good if \( |C_h| \leq 2^m/n^c \). By Markov’s inequality, we have that \( \Pr_{h \in \mathcal{H}}[|C_h| > 2^m/n^c] < 1/n^{c} \).

Consider the function \( g : \{0, 1\}^m \times \mathcal{H} \to \mathcal{H} \) given by \( g(y, h) = (h, h(f(y))) \). Note that \( g \) is polynomial-time computable. By the assumption that one-way functions do not exist, and thus distributionally one-way functions do not exist, there is a polynomial-time algorithm \( A \) such that the statistical distance between \( (y, h, g(y, h)) \) and \( (A(g(y, h)), g(y, h)) \) is at most \( n^{-c} \), where \( y \sim U_m \) and \( h \in \mathcal{H} \). Then, it holds that

\[
\Pr_{A, y, h}[g(A(g(y, h))) = g(y, h)] \geq 1 - \frac{1}{n^c},
\]

where the probability is taken over the random coins of \( A, y \sim U_m, \) and \( h \in \mathcal{H} \). Thus, we have that

\[
\Pr_{A, y, h}[g(A(g(y, h))) = g(y, h) \land h \text{ is good}] \geq 1 - \frac{2}{n^c}.
\]

By fixing the coins of \( A \) and \( h \in \mathcal{H} \), it holds that there are deterministic algorithm \( A' \) and \( h_0 \in \mathcal{H} \) such that \( h_0 \) is good and

\[
\Pr_y[g(A'(g(y, h_0))) = g(y, h_0)] \geq 1 - \frac{2}{n^c}.
\]
For \( y \in \{0, 1\}^m \) satisfying \( g(A'(g(y, h_0))) = g(y, h_0) \), we write \( A'(g(y, h_0)) = (y', h') \), where \( A'_1(g(y, h_0)) = y' \) and \( A'_2(g(y, h_0)) = h' \). Then, it holds that \( h' = h_0 \) and \( h_0(f(y)) = h_0(f(y')) \).

Furthermore, since \( h_0 \) is good, \( \Pr_y [f(y) \notin C_{h_0}] \geq 1 - 1/n^c \). Let \( H_0 \in \{0, 1\}^{(m+c \cdot \log n) \times n} \) be a matrix such that \( xH_0^T = h_0(x) \) for \( x \in \{0, 1\}^m \). (Such matrices exist since \( \mathcal{H} \) is a set of linear hash functions.) Consider a linear coding scheme in which \( H_0 \) is employed as the parity check matrix, and \( A'_1 \) is employed for recovering errors from syndromes. That is, \( \text{Enc}(x) = xG \) for a matrix \( G \in \{0, 1\}^{(n-m-c \cdot \log n) \times n} \) satisfying \( GH_0^T = 0 \), and \( \text{Dec}(y) = (y - f(A'_1(h_0, yH_0^T)))G^{-1} \), where \( G^{-1} \in \{0, 1\}^{n \times Rn} \) is a right inverse matrix of \( G \). Then, for any \( x \in \{0, 1\}^m \),

\[
\Pr_{y \sim U_r} [\text{Dec}(\text{Enc}(x) + f(y)) = x] = \Pr_{y \sim U_r} [\text{Enc}(x) + f(y) - f(A'_1(h_0, (\text{Enc}(x) + f(y))H_0^T)) = xG] = \Pr_{y \sim U_r} [f(A'_1(g(y, h_0))) = f(y)],
\]

where we use the property that \( GG^{-1} = I \), \( \text{Enc}(x) = xG \), \( GH_0^T = 0 \), and \( xH_0^T = h_0(x) \). Since the probability that \( g(A_0(g(y, h_0))) = g(y, h_0) \) is at least \( 1 - 2/n^c \), and for any \( y \in \{0, 1\}^m \) satisfying \( g(A_0(g(y, h_0))) = g(y, h_0) \), \( \Pr_y [f(y) \notin C_{h_0}] \geq 1 - 1/n^c \), we have that

\[
\Pr_{y \sim U_m} [f(A'_1(g(y, h_0))) = f(y)] \geq 1 - \frac{3}{n^c}.
\]

Hence the statement follows.

\[\square\]

6 Conclusions

In this work, we study the correctability of samplable additive errors with unbounded error-rate. We have considered a relatively simple setting in which the error distribution is identical for every coding scheme and codeword. The results imply that even when a distribution is not pseudorandom by membership test, it is difficult to correct every such samplable distribution by efficient coding schemes. Nevertheless, a positive result can be obtained if we consider much more structured errors such as errors from linear subspaces. We present some possible future work of this study.

Further study on the correctability. In this work, we have mostly discussed impossibility results. Thus, showing non-trivial possibility results is interesting. A possible direction is to consider more structured errors than samplable errors. One can consider \textit{computationally} structured errors such as errors computed by log-space machines, constant-depth circuits, or monotone circuits. Also, one can consider other types of structures, e.g., errors are introduced in a \textit{split-state} manner. Namely, an error vector is split into several parts, and each part is independently computed. This model has been well-studied in the context of leakage-resilient cryptography \([6, 17]\) and non-malleable codes \([7, 3, 1]\). BSC can be seen as an extreme of this type of channels in which each error bit is computed by the same biased-sampler.

Characterizing correctability. We have investigated the correctability of samplable additive errors using the Shannon entropy as a criterion. There may be another better criterion for characterizing the correctability of these errors, which might be related to efficient computability, to
which samplability is directly related. Since all the results in this paper deal with flat distributions, the results can be stated using other entropies such as the min-entropy. Since we have considered general distributions as error distributions, the information-spectrum approach [23, 11] may be more plausible.

**Acknowledgment**

This research was supported in part by JSPS/MEXT Grant-in-Aid for Scientific Research Numbers 25106509, 15H00851, and 16H01705. We thank anonymous reviewers for their helpful comments.

**References**

[1] D. Aggarwal, Y. Dodis, and S. Lovett. Non-malleable codes from additive combinatorics. In D. B. Shmoys, editor, *Symposium on Theory of Computing, STOC 2014*, pages 774–783. ACM, 2014.

[2] M. Cheraghchi. Capacity achieving codes from randomness conductors. In *IEEE International Symposium on Information Theory, ISIT 2009*, pages 2639–2643. IEEE, 2009.

[3] M. Cheraghchi and V. Guruswami. Non-malleable coding against bit-wise and split-state tampering. *J. Cryptology*, 30(1):191–241, 2017.

[4] A. De and T. Watson. Extractors and lower bounds for locally samplable sources. *TOCT*, 4(1):3, 2012.

[5] Y. Dodis, T. Ristenpart, and S. P. Vadhan. Randomness condensers for efficiently samplable, seed-dependent sources. In R. Cramer, editor, *Theory of Cryptography - 9th Theory of Cryptography Conference, TCC 2012*, volume 7194 of *Lecture Notes in Computer Science*, pages 618–635. Springer, 2012.

[6] S. Dziembowski and K. Pietrzak. Leakage-resilient cryptography. In *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008*, pages 293–302. IEEE Computer Society, 2008.

[7] S. Dziembowski, K. Pietrzak, and D. Wichs. Non-malleable codes. In A. C. Yao, editor, *Innovations in Computer Science - ICS 2010*, pages 434–452. Tsinghua University Press, 2010.

[8] R. Gennaro and L. Trevisan. Lower bounds on the efficiency of generic cryptographic constructions. In *41st Annual Symposium on Foundations of Computer Science, FOCS 2000*, pages 305–313, 2000.

[9] A. V. Goldberg and M. Sipser. Compression and ranking. *SIAM J. Comput.*, 20(3):524–536, 1991.

[10] V. Guruswami and A. D. Smith. Optimal rate code constructions for computationally simple channels. *J. ACM*, 63(4):35:1–35:37, 2016.

[11] T. S. Han. *Information-Spectrum Methods in Information Theory*. Springer, 2003. The original Japanese edition was published from Baifukan in 1998.
[12] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28(4):1364–1396, 1999.

[13] R. Impagliazzo and M. Luby. One-way functions are essential for complexity based cryptography (extended abstract). In *30th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 230–235, 1989.

[14] J. Justesen. Class of constructive asymptotically good algebraic codes. *IEEE Transactions on Information Theory*, 18(5):652–656, 1972.

[15] M. Langberg. Oblivious communication channels and their capacity. *IEEE Transactions on Information Theory*, 54(1):424–429, 2008.

[16] R. J. Lipton. A new approach to information theory. In P. Enjalbert, E. W. Mayr, and K. W. Wagner, editors, *STACS 94, 11th Annual Symposium on Theoretical Aspects of Computer Science*, volume 775 of *Lecture Notes in Computer Science*, pages 699–708. Springer, 1994.

[17] F. Liu and A. Lysyanskaya. Tamper and leakage resilience in the split-state model. In R. Safavi-Naini and R. Canetti, editors, *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference*, volume 7417 of *Lecture Notes in Computer Science*, pages 517–532. Springer, 2012.

[18] S. Micali, C. Peikert, M. Sudan, and D. A. Wilson. Optimal error correction for computationally bounded noise. *IEEE Transactions on Information Theory*, 56(11):5673–5680, 2010.

[19] M. Plotkin. Binary codes with specified minimum distance. *IRE Transactions on Information Theory*, 6(4):445–450, 1960.

[20] C. E. Shannon. A mathematical theory of communication. *Bell Systems Technical Journal*, 27:379–423,623–656, 1948.

[21] L. Trevisan and S. P. Vadhan. Extracting randomness from samplable distributions. In *41st Annual Symposium on Foundations of Computer Science, FOCS 2000*, pages 32–42, 2000.

[22] L. Trevisan, S. P. Vadhan, and D. Zuckerman. Compression of samplable sources. *Computational Complexity*, 14(3):186–227, 2005.

[23] S. Verdú and T. S. Han. A general formula for channel capacity. *IEEE Transactions on Information Theory*, 40(4):1147–1157, 1994.

[24] E. Viola. Extractors for circuit sources. In R. Ostrovsky, editor, *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011*, pages 220–229. IEEE Computer Society, 2011.

[25] H. Wee. On pseudoentropy versus compressibility. In *19th Annual IEEE Conference on Computational Complexity (CCC 2004)*, pages 29–41. IEEE Computer Society, 2004.