Abstract

Traditionally, data storage systems provide error-correction and data integrity techniques in an independent layer, with the goal of protecting all the data equally regardless of the application. In the context of machine learning systems, this strategy is not appropriate: errors in a few features may prove to be critically important (with respect to the algorithm output), while many errors may have little or no effect. This work takes a different direction: we allow ML algorithms to talk to error-correction schemes, with the goal of making algorithms robust to storage noise. We introduce several novel problems, provide an efficient solution to estimate the noise-induced change in the algorithm output for linear models, and show how to optimize error-correction codes to minimize error effects for fixed overhead.

1. Introduction

The standard approach to handling noise and faults in data storage systems is to provide a separate abstraction layer where error and fault correction techniques are applied to maintain the integrity of the data. The goal of this strategy is to ensure that all of the data is reliable; the correction layer is agnostic to the use of the data.

This solution may not be suitable for big data systems. Uniformly protecting the data is equivalent to minimizing the error rate measured at the input to some algorithm; this rate does not directly translate to the effect on the output. Even a very large number of errors may not have any impact on, for example, a classifier output. On the other hand, an error in a single feature (out of many) may have a dramatic impact, even though the input error rate remains very low.

This observation inspires us to consider a cross-layer approach for error-protection in machine learning systems, with the goal of reducing the effect of noise on the algorithm output. This novel problem bridges machine learning and the traditional fields concerned with the reliability of data, such as coding and information theory.

A general setting is shown in Figure 1. Noise can be found in the training data and labels \((X, Y)\) (left). The learned model \(F\) is affected by this noise, but can also be modified to be noise-aware by using the noise statistics \(\epsilon\). This model operates on noisy test data (right). The setting leads to the following hierarchy of problem settings, in increasing order of intractability:

1. Fixed model (learned from noiseless training data, i.e., \(\epsilon_{L,i} = 0\)) operating on noisy test data,
2. Noise-aware model (learned from noiseless training data and noise statistics \(\epsilon\)), produced to minimize expected noise loss on the output,
3. Noise-aware model learned from noisy training data.

\(1\)University of California Los Angeles, Los Angeles, California, USA. Correspondence to: Frederic Sala <fred-sala@ucla.edu>.

---

Don’t Fear the Bit Flips: Robust Linear Prediction Through Informed Channel Coding

Frederic Sala • Shahroze Kabir • Lara Dolecek • Guy Van den Broeck

Abstract

Traditionally, data storage systems provide error-correction and data integrity techniques in an independent layer, with the goal of protecting all the data equally regardless of the application. In the context of machine learning systems, this strategy is not appropriate: errors in a few features may prove to be critically important (with respect to the algorithm output), while many errors may have little or no effect. This work takes a different direction: we allow ML algorithms to talk to error-correction schemes, with the goal of making algorithms robust to storage noise. We introduce several novel problems, provide an efficient solution to estimate the noise-induced change in the algorithm output for linear models, and show how to optimize error-correction codes to minimize error effects for fixed overhead.

1. Introduction

The standard approach to handling noise and faults in data storage systems is to provide a separate abstraction layer where error and fault correction techniques are applied to maintain the integrity of the data. The goal of this strategy is to ensure that all of the data is reliable; the correction layer is agnostic to the use of the data.

This solution may not be suitable for big data systems. Uniformly protecting the data is equivalent to minimizing the error rate measured at the input to some algorithm; this rate does not directly translate to the effect on the output. Even a very large number of errors may not have any impact on, for example, a classifier output. On the other hand, an error in a single feature (out of many) may have a dramatic impact, even though the input error rate remains very low.

This observation inspires us to consider a cross-layer approach for error-protection in machine learning systems, with the goal of reducing the effect of noise on the algorithm output. This novel problem bridges machine learning and the traditional fields concerned with the reliability of data, such as coding and information theory.

A general setting is shown in Figure 1. Noise can be found in the training data and labels \((X, Y)\) (left). The learned model \(F\) is affected by this noise, but can also be modified to be noise-aware by using the noise statistics \(\epsilon\). This model operates on noisy test data (right). The setting leads to the following hierarchy of problem settings, in increasing order of intractability:

1. Fixed model (learned from noiseless training data, i.e., \(\epsilon_{L,i} = 0\)) operating on noisy test data,
2. Noise-aware model (learned from noiseless training data and noise statistics \(\epsilon\)), produced to minimize expected noise loss on the output,
3. Noise-aware model learned from noisy training data.

---

Training

\(X_1, Y_2, \ldots, X_n, Y_n, X'_1, Y'_2, \ldots, X'_n, Y'_n\)

Test

\(X_1, \ldots, X_n, X'_1, \ldots, X'_n\)

\(BSC(\epsilon_{L,1}), BSC(\epsilon_{L,2}), \ldots, BSC(\epsilon_{L,n})\)

\(BSC(\epsilon_{T,1}), BSC(\epsilon_{T,2}), \ldots, BSC(\epsilon_{T,n})\)

\(X'_1, Y'_2, \ldots, X'_n, Y'_n\)

\(\epsilon, L, F\)

Figure 1. Noisy system. Training phase (left) uses binary features and labels \((X, Y)\) passed through a noisy binary symmetric channel \(BSC(\epsilon)\): \(X'\) is equal to \(X\) with probability \(1 - \epsilon\) and equal to \(\bar{X}\) with probability \(\epsilon\). Algorithm \(L\) can use noise statistics \(\epsilon\) to produce a model \(F\) minimizing the impact of noise. Test phase (right) also operates on noisy features \(X'\) without observing the true values \(X\).
We largely concentrate on the first setting (which is quite challenging) while briefly discussing the other problems.

Given one of the problem settings, the first task is to evaluate the impact of the noise by measuring the loss (expected noise loss, or ENL) on the output compared to a noiseless version with the same features. For problems 2 and 3, we can modify $L$ to produce a model minimizing this loss. However, in all cases, we can modify the $\epsilon$’s through application of error-correcting codes. This is the key insight that enables us to bring together machine learning and coding theory. Naturally, forcing $\epsilon \rightarrow 0$ minimizes the loss; however, this may require an unacceptable amount of coding overhead. Instead, we focus on optimizing the code (with respect to the loss function) for a fixed overhead. We illustrate the main ideas with the following toy example:

### 2. Motivating Example

Consider a naive Bayes classifier with $n = 2$ features $X_1, X_2$, noisy versions $X'_1, X'_2$, and uniform prior on the class. The noise parameter is $\epsilon = 0.1$ by default. Let $p_i(x_j) := p(x_j = 0 | C = i)$. We allocate 4 additional redundancy bits for protection; uniform protection gives 2 such bits to each feature, while protection on $X_1$ alone grants all 4 bits to $X_1$ (the result of protection is a reduction of the $\epsilon_i$ noise parameter for feature $i$.)

In the first row of Table 1, $X_1$ contains more information about class $C$ compared to $X_2$. Observe that allocating all bits to $X_1$ yields a lower loss than equal protection or protection on $X_2$. Conversely, in the last row, even though $X_2$ contains more information about $C$, the loss is minimized by a uniform allocation of redundancy bits. The average loss between noisy and noiseless classifier output (equivalent to the probability of changing the classification) varies for different values of the $p_i(x_j)$’s and noise parameters. These observations imply that we cannot directly examine the conditional probabilities to decide how to allocate redundancy - we need an informed coding allocation strategy.

### 3. Related Work

There is a vast literature on robust machine learning algorithms. For example, Ramoni & Sebastiani (2001) considers missing training set data (missing features or labels) and is concerned with the impact on classifier accuracy. In Provost & Fawcett (2001), varying operative conditions and their effect on classifiers are studied. An experimental study of algorithms with synthetic noise corrupted datasets is performed by Kalapini et al. (2003). Deleted features are also tackled by Dekel & Shamir (2008) and Globerson & Roweis (2006); the latter proposes a game-theoretic approach to avoid over-reliance on a deleted feature.

Our approach (more detail in Mazooj et al. (2016) and Sala et al. (2017)) fundamentally differs from such works. In our problem, the noise occurs after feature generation (e.g., because the features are stored on noisy data storage devices). However, the system has the ability to protect the algorithm output with tailored error-correction strategies.

At the same time, our work stands in contrast to existing research on channel coding for data protection. The goal in these works is to preserve the data being stored without considering the application. That is, error-correction forms a separate abstraction layer. Works in this area propose error-correction for disk drives (Riggle & McCarth, 1998), write-once memories (Rivest & Shamir, 1982), RAID architectures (Blaum et al., 1995), non-volatile memories such as flash (Cassuto et al., 2010; Dolecek & Sala, 2016), solid-state drives (Zhao et al., 2013), and distributed storage (Weatherspoon & Kubiatowicz, 2002), (Dimakis et al., 2010).

### 4. Noise in Linear Models

We consider algorithms resulting in linear models in problem setting 1. For simplicity, we use binary features, although our results easily extend to non-binary features. Let $[n] := \{1, 2, \ldots, n\}$. Let $x = (x_1, x_2, \ldots, x_n)$ be a test point. Our running examples will be linear regression and linear classifiers; the classifier will be in the form of naive Bayes, though the results equivalently apply to logistic regression, other hyperplane-based classifiers, etc.

**Noise Model.** We employ a simple noise model: we define a noise parameter vector $\epsilon = (\epsilon_1, \epsilon_2, \ldots, \epsilon_n)$ with $0 \leq \epsilon_i \leq 1/2$ for $1 \leq i \leq n$. The binary feature $X_i$ is flipped to its opposite value $\overline{X_i}$ with probability $\epsilon_i$, and stays unchanged with probability $1 - \epsilon_i$. We express the resulting error vector as $E = (E_1, E_2, \ldots, E_n)$, where $E_i = 1$ if an error has occurred for feature $i$ and $0$ otherwise. If errors occur at positions in $S \subseteq [n]$ in $E$, then the probability of $E$ is given by $Pr(E) = \prod_{i \in S} \epsilon_i \prod_{i \notin S} (1 - \epsilon_i)$. We denote the algorithm operating on the noisy features as $F(x, E) = F(x \oplus E)$.

**Noise Loss Measures.** We examine the effect of the feature bit errors on the output of the algorithm. Let $\ell(F(e), F(x, e))$ be the noise loss between the output of the noiseless and noisy versions of the algorithms. We are interested in evaluating the expected noise loss (ENL)
\[
\mathbb{E}_E[\ell(F(X), F(X, E))].
\]
Conditioning on \(E\) and letting \(S_e\) be the positions \(i\) where \(e_i = 1\), the ENL can be written as
\[
\sum_{S \subseteq [n]} \ell(F(X), F(X, e)) \prod_{i \in S_e} e_i \prod_{i \not\in S_e} (1 - e_i). \tag{1}
\]
We are interested in the empirical ENL \(\mathbb{E}_E[\ell(F(x), F(x, E))].\) A natural choice for \(\ell\) is the \(L_1\) norm: \(\ell(F(x), F(x, E)) = |F(x) - F(x, E)|\). For classification problems, this 0/1 loss reduces to the classification change probability, that is, the probability that the noiseless point \(X\) and the noisy version \(X'\) have differing classification. For linear regression problems, the \(L_2\) norm is also of interest.

For linear models, the ENL can be written, for a function \(g\) determined by the algorithm, as the discrete integral
\[
\mathbb{E}_E[\ell(F(x), F(x, E))] = \sum_{S \subseteq [n]} \sum_{i \in S} D_i \prod_{i \in S} \epsilon_i \prod_{i \not\in S} (1 - \epsilon_i), \tag{2}
\]
for certain choices of \(D_i\). In linear regression, \(|F(x) - F(x, E)| = |\alpha^T x - \alpha^T (x \oplus E)|\), so that \(D_i = a_i(1-\epsilon_i)\) for \(1 \leq i \leq n\). Thus for linear regression, \(g(v) = |v|\). For Naive Bayes, set the loss term \(D_j\) to be the difference
\[
D_j = B_j - A_j = \log((1 - \alpha_j)/(1 - \beta_j)) - \log(\alpha_j/\beta_j),
\]
where \(\alpha_i = p(x_i | C = 0)\) and \(\beta_i = p(x_i | C = 1)\). Then, it can be shown that \(g(v) = 1\{v < T\}\), i.e., for linear classifiers
\[
\mathbb{E}_E[\ell(F(x), F(x, E))] = \sum_{S \subseteq [n]} 1\{\sum_{i \in S} D_i < T\} \prod_{i \in S} \epsilon_i \prod_{i \not\in S} (1 - \epsilon_i). \tag{3}
\]

5. Computing the Expected Noise Loss

Computing the ENL is a significant challenge. As a warm-up, we compute the ENL under the \(L_2\) norm for linear regression. It is not hard to show that
\[
\mathbb{E}_E[|a^T x - a^T x'|] = \text{Tr}(aa^T \text{Cov}(x - x')) + \mathbb{E}_E[x - x']^T aa^T \mathbb{E}_E[x - x'].
\]
It is easy to compute \(\mathbb{E}_E[x - x']\). If \(x_i = 0\), the expectation is \(-\epsilon_i\), while if \(x_i = 1\), it is \(\epsilon_i\), so that \(\mathbb{E}_E[x - x'] = \left[(-1)^{x_1+1} \epsilon_1, \ldots, (-1)^{x_n+1} \epsilon_n\right]^T\). Moreover, a similar solution can be found for Problem 2 for linear regression: it is possible to find the optimal coefficients \(\alpha\) that minimize the expected \(L_2\) loss as a function of the \(\epsilon\)'s.

Algorithm 1 Expected Noise Loss Approximation

**Input:** Loss terms \(D_1, D_2, \ldots, D_n\), Error probabilities \(\epsilon_1, \epsilon_2, \ldots, \epsilon_n\), Target \(T\) (in classification problems), Number of buckets in quantization scheme \(k\), Model function \(g\)

**Output:** Expected noise loss approximation \(\text{ENL}_{\text{app}}\)

**Initialize** \(S_1, \ldots, S_k\) to 0, \(\text{ENL}_{\text{app}}\) to 0

for \(j = 1\) to \(n\) do

if \(D_j \in [\text{Interval}_i\begin{array}{c} \text{begin} \\ \text{Interval}_i\end{array}^{\text{end}}]\) then

\(N_i \leftarrow N_i + 1\), \(\epsilon_i, N_i \leftarrow \epsilon_j\)

end if

end for

for \(i = 0\) to \(n\) do

\(\text{ENL}_{\text{app}} \leftarrow \text{ENL}_{\text{app}} + g_{i,j}(G[i,j])\)

end for

end for

Algorithm 2 Channel Code Optimization

**Input:** Test points \(x_1, x_2, \ldots, x_r\), Noise vector \(\epsilon = (\epsilon_1, \ldots, \epsilon_r)\), redundancy budget \(r\)

**Output:** Optimized redundancy allocation vector \(r^*\)

**Initialize** \(r(0)\) to 0

for \(j = 0\) to \(r - 1\) do

\(i \leftarrow \arg \min_{\ell} \frac{1}{k} \sum_{k=1}^{n} \text{ENL}_{\text{app}}(x_k, E^{(j+1)(i)})\)

\(r(j + 1) \leftarrow r(j) + 1(i)\)

end for

In contrast to the \(L_2\) loss, which offers the convenient factorization in above, the general problem and the \(L_1\) loss function version are difficult to compute:

**Proposition 1.** Expression (2) is \#P-hard to compute, even for an efficiently computable function \(g\).

**Proposition 2.** Expression (3) is \(NP\)-hard to compute.

To deal with this, we provide a lightweight, efficient approximation of the ENL relying on a discretization scheme. The key idea is to quantize the loss terms \(D_i\) into \(k\) intervals, for \(k\) a constant. By a clever choice of quantization, we induce a structure that enables us to approximate the ENL in no more than \(O(n^2 \log n)\) operations. The approximation is described in Algorithm 1. For linear regression, set \(g_{\ell,m}(v) = |\frac{m}{k-1} D_1 + \ell (D_{\text{min}} - D_1) | \times v\). For linear classifiers, set \(g_{\ell,m}(v) = 1\{m < T'\} | x v\) where \(T' = T - \ell \left(D_{\text{min}} - \frac{D_1}{k-1}\right)\). Details on how to perform the quantization are found in the longer version of this work (Sala et al., 2017). The key result is that the approximation can be performed efficiently:

**Theorem 1.** The ENL approximation in Algorithm 1 requires no more than \(O(k^2 n^2 \log(kn))\) computations of \(g\).
6. Optimized Channel Coding

Now that we can compute the ENL, the next step is to tailor an error-correction strategy to the characteristics of the features in order to minimize the ENL (reducing the harmful impact of the noise on the output of the algorithm).

**Repetition codes.** We rely on repetition coding. If the $j$th feature $x_j$, corrupted by a bit flip with probability $\epsilon$, is repeated $2r + 1$ times for some $r \geq 0$, the probability $\epsilon^{(r)}$ that the feature is decoded incorrectly is equal to the probability that the majority of votes are corrupted: $\epsilon^{(r)} = \sum_{i=r+1}^{2r+1} \binom{2r+1}{i} (1-\epsilon)^{2r+1-i} \epsilon^i$. Repetitions codes are useful due to the flexibility of per-bit independent encoding and decoding. Unlike in classical coding, we have found that such codes can be optimal in our setting.

**Coding optimization.** We use a total budget of $2r$ redundancy bits. Feature $i$ is represented by $1 + 2r_i$ copies, and has error probability $\epsilon^{(r_i)}$, for $1 \leq i \leq n$. The noise vector for all $n$ features is $\epsilon^{(r)} = (\epsilon^{(r_1)}, \epsilon^{(r_2)}, \ldots, \epsilon^{(r_n)})$. The corresponding error vector is written $E^{(r)}$. The values $r = (r_1, r_2, \ldots, r_n)$ are constrained by $r_1 + r_2 + \ldots + r_n = r$. The goal is to minimize the ENL over $r$ test points $x_1, \ldots, x_t$ with respect to $r$ and the resulting $\epsilon$ vector. We have the following optimization

$$\arg\min_r \frac{1}{t} \sum_{j=1}^{t} \text{ENL}(x_j, E^{(r)}) \text{ s.t. } n_i \geq 0.$$  \hspace{1cm} (4)

Consider the following greedy allocation algorithm, using the ENL approximation in Algorithm 1 and performed one redundancy unit (two repeated bits) at a time. After the $j$th step, we write the redundancy vector as $r(j) = (r_1(j), r_2(j), \ldots, r_n(j))$. In the $(j + 1)$st step, one of the $r_i(j)$ terms is selected and increased by 1. We write $1(i)$ for the vector $(0, 0, \ldots, 0, 1, 0, \ldots, 0)$ with a 1 in the $i$th position and 0’s elsewhere. Then, the $(j + 1)$st step is given by $\arg\min_i \frac{1}{t} \sum_{k=1}^{t} \text{ENL}(x_k, E^{r(j)+1(i)}) \text{ s.t. } 1 \leq i \leq n$. The complexity is reduced to that of performing $nt$ ENL computations per each of the $r$ steps. The procedure is given in Algorithm 2.

For linear classifiers, we found that the redundancy allocation function is submodular, and thus the greedy algorithm is close to optimal. This requires two properties: (i) monotonicity (which holds with high probability when the test and training distributions are the same) and (ii) the ‘diminishing returns’ property, which follows from monotonicity.

**Experiments.** We demonstrate the benefits of our scheme on several datasets: binary classification uses a voting dataset (Lichman, 2013) and a movie review dataset (Bekker et al., 2015), and linear regression uses a bike rental dataset (Gam, 2013). In all cases, we used $k = 50$ for the number of buckets in our ENL approximations. For the movie reviews set we used two sets of $n = 20$ features and 250 test data points. The $\epsilon$ parameter was 0.2 for the first 2 datasets (a very high amount of noise that can nevertheless be handled through channel coding). Table 2 shows the ENL for uniform and optimized assignment of redundancy bits given a budget of $2nR$ bits. For the classification setting, the values can be interpreted as the probability of switching the classification due to noisy test features; for regression, the values can be thought of as a type of distortion on the output. We also report the ratio of the ENL between the uniform and optimized coding strategies; this ratio represents the benefits of our coding strategy. We observe performance improvements of between 10% and 30% for various data sets.

7. Conclusion

We proposed a new class of problems where data protection is tailored to take advantage of the application. For the problem setting with linear models operating on noisy test data, we introduced an efficient scheme to evaluate the noise loss and an optimized coding scheme targeted at minimizing the noise loss based on submodular optimization. Our informed approach for redundancy allocation is among the first principled methods combining coding theory with machine learning. Several interesting problems remain for future work: non-linear models, other loss functions, and the general cases of Problems 2 and 3.

---

### Table 2. Expected Noise Loss (ENL) for classification and regression

<table>
<thead>
<tr>
<th>$R$</th>
<th>Uniform Optimal Ratio</th>
<th>Uniform Optimal Ratio</th>
<th>Uniform Optimal Ratio</th>
<th>Uniform Optimal Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.1263 0.1025 1.233</td>
<td>0.1011 0.0866 1.167</td>
<td>0.0564 0.0414 1.363</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0.0442 0.0303 1.459</td>
<td>0.0348 0.0302 1.152</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0.0147 0.0088 1.671</td>
<td>0.0115 0.0100 1.151</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0.0047 0.0026 1.903</td>
<td>0.0038 0.0033 1.154</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0.0016 0.0008 2.101</td>
<td>0.0012 0.0011 1.158</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>0.0005 0.0002 2.255</td>
<td>0.0004 0.0003 1.160</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0.0001 7.7E-05 2.398</td>
<td>0.0002 0.0001 1.162</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>6.3E-05 2.5E-05 2.539</td>
<td>4.9E-05 4.2E-05 1.164</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>2.2E-05 8.1E-06 2.672</td>
<td>1.7E-05 1.5E-05 1.165</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>7.4E-06 2.6E-06 2.811</td>
<td>5.8E-06 5.0E-06 1.165</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For future work: non-linear models, other loss functions, and the general cases of Problems 2 and 3.
Acknowledgements

This work is partially supported by the NSF (#IIS-1657613, #IIS-1633857, CAREER CCF-1150212, CCF-1527130), and DARPA (#N66001-17-2-4032).

References


