Analysis of LT Codes over Finite Fields under Optimal Erasure Decoding

Birgit Schotsch, Giuliano Garrammone and Peter Vary

***Abstract*—The erasure correction performance of Luby transform (LT) code ensembles over higher order Galois fields is analysed under optimal, i.e. maximum likelihood (ML) erasure decoding. We provide the complete set of four bounds on the erasure probability after decoding on word as well as on symbol level. Especially the upper bounds are extremely close to the simulated residual erasure rates after decoding and can thus be used for code design instead of time-consuming simulations.**

***Index Terms*—Fountain codes, maximum likelihood decoding, random matrices, finite fields.**

I. Introduction

Luby transform (LT) codes [1] are the first practical realisation of digital fountain codes [2], a protocol devised for an efficient erasure resilient information transmission in packet-based communication networks, particularly in broadcast or multicast scenarios. Fountain codes are rateless codes, i.e. they allow to generate on the fly an arbitrary number[1] n_T of encoded symbols $\mathbf{y}_\mathrm{T}$ from a finite set of k input symbols $\mathbf{x}$ and in practice, decoding should be possible from any $n_\mathrm{R} = k(1+\varepsilon_\mathrm{R})$ received encoded symbols $\mathbf{y}_\mathrm{R}$, where ε_R is the small and non-negative relative reception overhead.

LT codes usually constitute the rateless component in a compound code, in which a high rate precode cleans up the erasure floor which is specific to LT codes. Though designed for belief propagation (BP) decoding which only performs well for large input sizes k, lately LT codes under maximum likelihood (ML) decoding[2] have received an increasing attention due to the superior erasure correction performance for practical, i.e. short to medium input sizes. Also the extension to higher order Galois fields $\mathbb{F}_q$ with $q = 2^m$ and $m \in \mathbb{N}$, has proven beneficial [3]–[5] in terms of erasure correction performance and in [5] also in terms of computational complexity.

We begin with a brief introduction to LT codes over higher order Galois fields in Sec. II. In [5] we have derived a pair of upper and lower bounds on the residual symbol erasure probability. In Sec. III, we now complete the picture by contributing a practically more relevant pair of bounds on the residual word erasure probability. Since especially the upper bounds are extremely close to the simulated residual erasure rates, these can be used for code design instead of performing time-consuming Monte Carlo simulations.

II. LT Code Ensembles over $\mathbb{F}_q$

LT codes are linear codes, i.e. an arbitrarily long codeword $\mathbf{y}_\mathrm{T} \in \mathbb{F}_q^{n_\mathrm{T}}$ is generated by $\mathbf{y}_\mathrm{T} = \mathbf{G}_\mathrm{T}\mathbf{x}$, where $\mathbf{x} \in \mathbb{F}_q^k$ is the information or input word and $\mathbf{G}_\mathrm{T} \in \mathbb{F}_q^{n_\mathrm{T}\times k}$ is an LT generator matrix at the transmitter taken from the ensemble G_T. Considering the equivalent bipartite LT code graph, the input symbols are denoted input nodes and the encoded symbols are called output nodes. The edges connecting the two types of nodes are defined by the generator matrix. Each matrix is created row-wise by a random process that first determines the row weight by means of a so-called output degree distribution. This distribution is usually given in terms of its generator polynomial $\Omega(\xi) = \sum_{d=0}^{k} \Omega_d\, \xi^d$, where Ω_d is the probability of creating a row with d non-zero entries. The d entries are chosen uniformly at random without repetition from the set of k possible entries and are assigned non-zero values chosen uniformly at random with repetition from $\mathbb{F}_q \setminus \{0\}$.

The codeword is transmitted symbol-wise over a q-ary erasure channel that randomly erases encoded symbols with a certain probability. At the receiver, only the non-erased encoded symbols are taken into account and are reassembled to $\mathbf{y}_\mathrm{R} \in \mathbb{F}_q^{n_\mathrm{R}}$. The rows of $\mathbf{G}_\mathrm{T}$ that are associated to the erased symbols are useless to the receiver and are not considered anymore, leading to a new matrix $\mathbf{G}_\mathrm{R} \in \mathbb{F}_q^{n_\mathrm{R}\times k}$, which however, has the same row weight distribution as $\mathbf{G}_\mathrm{T}$, i.e. if $\mathsf{G}_\mathrm{T} \sim \Omega(\xi)$, also $\mathsf{G}_\mathrm{R} \sim \Omega(\xi)$. ML decoding is performed, which in case of a transmission over an erasure channel is equivalent to solving $\mathbf{y}_\mathrm{R} = \mathbf{G}_\mathrm{R}\mathbf{x}_\mathrm{R}$, a system of n_R consistent linear equations in k unknowns. Besides Gaussian elimination, there exist several computationally more efficient ML decoding algorithms, e.g. [6], [7], that are preferred to stand-alone BP decoding in practical systems [4], [8] due to the superior erasure correction performance of ML decoding.

III. Bounds on the Word and Symbol Erasure Probability of LT Code Ensembles

In this section, we provide the complete set of four bounds on word as well as on symbol level under ML decoding.

B. Schotsch and P. Vary are with the Institute of Communication Systems and Data Processing at RWTH Aachen University, 52074 Aachen, Germany (e-mail: {schotsch | vary}@ind.rwth-aachen.de).

G. Garrammone is with the Institute of Communication and Navigation of the Deutsches Zentrum für Luft und Raumfahrt (DLR), 82234 Wessling, Germany (e-mail: Giuliano.Garrammone@dlr.de).

Supported in part by the UMIC Research Centre, RWTH Aachen University.

[1] In the fountain coding setup a receiver centric view is common that penalises a wasteful use of reception code rate $r_\mathrm{R} = k/n_\mathrm{R}$, but not the use of the channel by the transmitter [9]. Therefore, in order to clearly differentiate between transmitter or receiver related quantities, an index ”T” or ”R” is used if required. Moreover, we use the following notation: scalars are written in italic type (e.g. x). Boldfaced lower case letters denote column vectors (e.g. $\mathbf{x}$), while boldfaced capital letters denote matrices (e.g. $\mathbf{X}$). The corresponding random variables are set in sans serif font, e.g. x for random variables, $\boldsymbol{\mathsf{x}}$ for random vectors and $\boldsymbol{\mathsf{X}}$ for random matrices.

[2] Note that on erasure channels, optimal decoding is accomplished by means of ML decoding which is equivalent to MAP (maximum-a-posteriori) decoding independently of the priors.

We have derived bounds on the symbol erasure probability already in [5], of which the upper bound is a generalisation to higher order Galois fields of an expression from [10]. We include these bounds on symbol level for completeness. In the following, symbol erasures are marked by $\cancel{\mathcal{S}}$ and word erasures by $\cancel{\mathcal{W}}$, whereas upper and lower bounds on a certain probability P are denoted $\overline{P}$ and $\underline{P}$, respectively.

A. Upper Bounds

Theorem 1. Given an LT code ensemble $\mathbf{G}_\mathrm{R} \sim \Omega(\xi)$ over $\mathbb{F}_q$, an upper bound on the word erasure probability $P^{[\mathrm{ML}]}\left(\cancel{\mathcal{W}}\right)$ after ML decoding is[3]

$$\overline{P}^{[\mathrm{ML}]}\left(\cancel{\mathcal{W}}\right) = \sum_{w=1}^{k}\binom{k}{w}(q-1)^{w-1} \cdot \left[\frac{1}{q}\sum_{d}\Omega_d \frac{\sum\limits_{l=0}^{d}\binom{w}{l}\binom{k-w}{d-l}\left[1-(1-q)^{1-l}\right]}{\binom{k}{d}}\right]^{k\gamma_\mathrm{R}} \tag{1}$$

$$= \sum_{w=1}^{k}\binom{k}{w}(q-1)^{w-1}\left[\frac{1}{q}+\frac{q-1}{q}\sum_{d}\Omega_d\frac{\mathcal{K}_d(w;k)}{\mathcal{K}_d(0;k)}\right]^{k\gamma_\mathrm{R}} \tag{2}$$

with the inverse reception code rate $\gamma_\mathrm{R} = 1+\varepsilon_\mathrm{R} \geq 1$. The second, more compact variant comprises the well-known Krawtchouk polynomial[4] $\mathcal{K}_d(\,\cdot\,;\cdot\,)$.

Proof: The probability $P^{[\mathrm{ML}]}\left(\cancel{\mathcal{W}}\right)$ is equal to the probability that $\mathbf{G}_\mathrm{R}$ does not have full column rank

$$P^{[\mathrm{ML}]}\left(\cancel{\mathcal{W}}\right) = \Pr\left\{\mathrm{rank}(\mathbf{G}_\mathrm{R}) < k\right\},$$

i.e. the probability that the kernel of $\mathbf{G}_\mathrm{R}$ is non-trivial,

$$P^{[\mathrm{ML}]}\left(\cancel{\mathcal{W}}\right) = \Pr\left\{\exists \mathbf{x} \in \ker(\mathbf{G}_\mathrm{R}) \setminus \{\mathbf{0}\}\right\}. \tag{3}$$

This is equivalent to the probability that an arbitrary information word cannot be uniquely determined, since the solution of $\mathbf{G}_\mathrm{R}\mathbf{x} = \mathbf{y}_\mathrm{R}$ is a $(k - \mathrm{rank}(\mathbf{G}_\mathrm{R}))$-dimensional vector space. This probability can be upper bounded by the expected cardinality of the non-trivial kernel of $\mathbf{G}_\mathrm{R}$

$$P^{[\mathrm{ML}]}\left(\cancel{\mathcal{W}}\right) \leq \mathrm{E}\left\{|\ker(\mathbf{G}_\mathrm{R}) \setminus \{\mathbf{0}\}|\right\}.$$

However, this bound can be tightened by a factor of $q-1$, since we can exploit the fact that if some $\mathbf{x} \in \ker(\mathbf{G}_\mathrm{R}) \setminus \{\mathbf{0}\}$, then also $a\mathbf{x} \in \ker(\mathbf{G}_\mathrm{R}) \setminus \{\mathbf{0}\}$, $\forall a \in \mathbb{F}_q \setminus \{0\}$. And in order to bound (3) from above, it is sufficient to consider just one of the $q-1$ scaled versions of $\mathbf{x}$

$$P^{[\mathrm{ML}]}\left(\cancel{\mathcal{W}}\right) \leq \overline{P}^{[\mathrm{ML}]}\left(\cancel{\mathcal{W}}\right) = \frac{1}{q-1}\cdot \mathrm{E}\left\{|\ker(\mathbf{G}_\mathrm{R}) \setminus \{\mathbf{0}\}|\right\},$$

and w.l.o.g. we do so by counting only those vectors $\mathbf{x}$ that have been normalised w.r.t. their first non-zero entry, i.e. vectors $\mathbf{x}$ whose first non-zero entry is $x_i = 1$:

$$\overline{P}^{[\mathrm{ML}]}\left(\cancel{\mathcal{W}}\right) = \sum_{\substack{\mathbf{x}\in\mathbb{F}_q^k,\\ \mathbf{x}\neq\mathbf{0},\, x_i=1}} \Pr\left\{\mathbf{G}_\mathrm{R}\mathbf{x} = \mathbf{0}\right\}.$$

The $k\gamma_\mathrm{R}$ rows of $\mathbf{G}_\mathrm{R}$ can be viewed as the outcomes of independent trials of a random variable $\mathbf{r} \in \mathbb{F}_q^k$:

$$\overline{P}^{[\mathrm{ML}]}\left(\cancel{\mathcal{W}}\right) = \sum_{\substack{\mathbf{x}\in\mathbb{F}_q^k,\\ \mathbf{x}\neq\mathbf{0},\, x_i=1}} \left[\Pr\left\{\mathbf{r}^\mathsf{T}\mathbf{x} = 0\right\}\right]^{k\gamma_\mathrm{R}}.$$

The Hamming weight of a vector over $\mathbb{F}_q$ equals the number of its non-zero elements and is denoted $\|\cdot\|$. Now, the probability $\Pr\left\{\mathbf{r}^\mathsf{T}\mathbf{x} = 0\right\}$ is determined, conditioned on $\|\mathbf{r}\| = d$ and $\|\mathbf{x}\| = w$. A row $\mathbf{r}$ has weight $\|\mathbf{r}\| = d$ with probability Ω_d and there are $\binom{k}{w}(q-1)^{w-1}$ choices of $\mathbf{x}$ of weight $w > 0$ and a one as the first non-zero entry. Let $\mathbf{v} = (\mathsf{v}_1, \mathsf{v}_2, \ldots, \mathsf{v}_k)^\mathsf{T}$ with $\mathsf{v}_j = \mathsf{r}_j x_j$, where v_j, r_j and x_j are the jth elements of the vectors $\mathbf{v}$, $\mathbf{r}$ and $\mathbf{x}$, respectively, then

$$\overline{P}^{[\mathrm{ML}]}\left(\cancel{\mathcal{W}}\right) = \sum_{w=1}^{k}\binom{k}{w}(q-1)^{w-1} \cdot \left[\sum_{d}\Omega_d \Pr\left\{\mathbf{r}^\mathsf{T}\mathbf{x} = 0 \,\middle|\, \|\mathbf{r}\| = d,\ \|\mathbf{x}\| = w\right\}\right]^{k\gamma_\mathrm{R}} \tag{4}$$

with

$$\Pr\left\{\mathbf{r}^\mathsf{T}\mathbf{x} = 0 \,\middle|\, \|\mathbf{r}\| = d,\ \|\mathbf{x}\| = w\right\} = \sum_{l=0}^{d}\Pr\left\{\|\mathbf{v}\| = l \,\middle|\, \|\mathbf{r}\| = d,\ \|\mathbf{x}\| = w\right\} \cdot \Pr\left\{\sum_{j=1}^{k}\mathsf{v}_j = 0 \,\middle|\, \|\mathbf{v}\| = l\right\}. \tag{5}$$

The probability of occurrence of exactly l non-zero elements in $\mathbf{v}$ is

$$\Pr\left\{\|\mathbf{v}\| = l \,\middle|\, \|\mathbf{r}\| = d,\ \|\mathbf{x}\| = w\right\} = \frac{\binom{w}{l}\binom{k-w}{d-l}}{\binom{k}{d}}. \tag{6}$$

The last term in (5) is the number $N_0(l,q)$ of possibilities that l non-zero $\mathbb{F}_q$-elements add up to zero, taking the elements' order into account, divided by the number $N(l,q)$ of all possibilities to draw l times with replacement from the set of the $q-1$ non-zero $\mathbb{F}_q$-elements taking the order into account:

$$\Pr\left\{\sum_{j=1}^{k}\mathsf{v}_j = 0 \,\middle|\, \|\mathbf{v}\| = l\right\} = \frac{N_0(l,\,q)}{N(l,\,q)}. \tag{7}$$

The problem of determining $N_0(l,q)$ is equivalent to finding the number of closed walks of length l in a complete graph of size q from some fixed but arbitrary vertex back to itself of which a closed form expression can be found, e.g. in [12]

$$N_0(l,\,q) = \frac{1}{q}\left[(q-1)^l + (q-1)(-1)^l\right]. \tag{8}$$

[3] For notational convenience it is implicated that probabilities and their bounds are limited from above by one and the operation $\min\{1,\,\cdot\,\}$ is omitted.

[4] The Krawtchouk polynomial is defined as (cf. e.g. [11])

$$\mathcal{K}_\varsigma(\xi;\nu) = \sum_{i=0}^{\varsigma}(-1)^i(q-1)^{\varsigma-i}\binom{\xi}{i}\binom{\nu-\xi}{\varsigma-i},$$

for any positive integer ν and $\varsigma = 0, 1, \ldots, \nu$ as well as a prime power q and a non-negative indeterminate ξ.

With $N(l,q) = (q-1)^l$ we obtain

$$\Pr\left\{\sum_{j=1}^{k} \mathsf{v}_j = 0 \middle| \|\mathbf{v}\| = l\right\} = \frac{1}{q}\left[1-(1-q)^{1-l}\right]. \tag{9}$$

Finally, inserting (6) and (9) into (5) and the resulting expression into (4) gives the explicit variant of the upper bound in (1). By some simple transformations, the more compact version (2) can be obtained. ∎

Theorem 2 ([5])**.** Given an LT code ensemble $\mathbf{G}_{\mathrm{R}} \sim \Omega(\xi)$ over $\mathbb{F}_q$, an upper bound on the symbol erasure probability $P^{[\mathrm{ML}]}\left(\cancel{S}\right)$ after ML decoding is

$$\begin{aligned}\overline{P}^{[\mathrm{ML}]}\left(\cancel{S}\right) = &\sum_{w=1}^{k}\binom{k-1}{w-1}(q-1)^{w-1}\\ &\cdot\left[\frac{1}{q}+\frac{q-1}{q}\sum_{d}\Omega_d\cdot\frac{\mathcal{K}_d(w;k)}{\mathcal{K}_d(0;k)}\right]^{k\gamma_{\mathrm{R}}}\end{aligned} \tag{10}$$

with the inverse reception code rate $\gamma_{\mathrm{R}} = 1+\varepsilon_{\mathrm{R}} \geq 1$.

Proof: The probability $P^{[\mathrm{ML}]}\left(\cancel{S}\right)$ is equal to the probability that the ith input symbol cannot be determined by ML decoding for an arbitrary $i \in \{1, 2, \ldots, k\}$

$$P^{[\mathrm{ML}]}\left(\cancel{S}\right) = \Pr\left\{\exists \mathbf{x} \in \mathbb{F}_q^k \setminus \{\mathbf{0}\},\, x_i = a \,:\, \mathbf{G}_{\mathrm{R}}\mathbf{x} = \mathbf{0}\right\}$$

with arbitrary but fixed $a \in \mathbb{F}_q \setminus \{0\}$. This is also the probability that the ith column of matrix $\mathbf{G}_{\mathrm{R}}$ is linearly dependent on a non-empty set of columns, which can be upper bounded by the probability that any possible set of columns of $\mathbf{G}_{\mathrm{R}}$ is linearly dependent on column i

$$P^{[\mathrm{ML}]}\left(\cancel{S}\right) \leq \overline{P}^{[\mathrm{ML}]}\left(\cancel{S}\right) = \sum_{\substack{x\in\mathbb{F}_q^k,\\ x_i=a}} \Pr\left\{\mathbf{G}_{\mathrm{R}}\mathbf{x} = \mathbf{0}\right\}. \tag{11}$$

The remainder of this proof is along the same lines as the proof of Theorem 1 with the only difference that in contrast to the previous derivation, there are $\binom{k-1}{w-1}(q-1)^{w-1}$ choices of $\mathbf{x}$ of weight $w > 0$ with $x_i = a$. ∎

B. Lower Bounds

Lemma 3. Given an LT code ensemble $\mathbf{G}_{\mathrm{R}} \sim \Omega(\xi)$ over $\mathbb{F}_q$, the probability that i particular (fixed but arbitrary) input nodes (INs) are not connected to any of the $k\gamma_{\mathrm{R}}$ independent output nodes (ONs), i.e. the probability that i particular columns of $\mathbf{G}_{\mathrm{R}}$ are all-zero columns, is given by

$$\Pr\left\{\begin{matrix}i\ \text{particular INs not}\\ \text{connected to any ONs}\end{matrix}\right\} = \left(\sum_{d=1}^{k}\Omega_d\frac{\binom{k-i}{d}}{\binom{k}{d}}\right)^{k\gamma_{\mathrm{R}}}. \tag{12}$$

Proof: The probability that i particular input nodes, with $1 \leq i \leq k$, are not connected to an output node of degree d is

$$\frac{\binom{k-i}{d}}{\binom{k}{d}}, \tag{13}$$

while the probability that i particular input nodes are not connected to an output node of arbitrary degree is

$$\sum_{d=1}^{k}\Omega_d\frac{\binom{k-i}{d}}{\binom{k}{d}}. \tag{14}$$

Since there are $k\gamma_{\mathrm{R}}$ independent output nodes, the probability that i particular input nodes are not connected to any of them is given by (12). ∎

The latter derivation is similar to the one in [13] for the special case $i = 1$. This case constitutes a lower bound on the symbol erasure probability and is stated below without proof.

Theorem 4 ([13])**.** Given an LT code ensemble $\mathbf{G}_{\mathrm{R}} \sim \Omega(\xi)$ over $\mathbb{F}_q$, a lower bound on the symbol erasure probability $P^{[\mathrm{ML}]}\left(\cancel{S}\right)$ after ML decoding is

$$\begin{aligned}\underline{P}^{[\mathrm{ML}]}\left(\cancel{S}\right) &= \Pr\left\{\begin{matrix}1\ \text{particular INs not}\\ \text{connected to any ONs}\end{matrix}\right\}\\ &= \left(1-\frac{\bar{d}}{k}\right)^{k\gamma_{\mathrm{R}}},\end{aligned} \tag{15}$$

where $\bar{d} = \sum_{d=1}^{k} d\Omega_d$ is the average output node degree.

Theorem 5. Given an LT code ensemble $\mathbf{G}_{\mathrm{R}} \sim \Omega(\xi)$ over $\mathbb{F}_q$, a lower bound on the word erasure probability $P^{[\mathrm{ML}]}\left(\cancel{W}\right)$ after ML decoding is

$$\underline{P}^{[\mathrm{ML}]}\left(\cancel{W}\right) = \sum_{i=1}^{k}(-1)^{i+1}\binom{k}{i}\left(\sum_{d=1}^{k}\Omega_d\frac{\binom{k-i}{d}}{\binom{k}{d}}\right)^{k\gamma_{\mathrm{R}}}. \tag{16}$$

Proof: An information word cannot be reconstructed if at least one input node cannot be recovered. A lower bound on the word erasure probability $P^{[\mathrm{ML}]}\left(\cancel{W}\right)$ is therefore given by the probability that there exist input nodes that are not connected to any of the $k\gamma_{\mathrm{R}}$ independent output nodes

$$\begin{aligned}\underline{P}^{[\mathrm{ML}]}\left(\cancel{W}\right) &= \Pr\left\{\begin{matrix}\exists\ \text{INs not connected}\\ \text{to any ONs}\end{matrix}\right\} && (17)\\ &= \sum_{j=1}^{k}\Pr\left\{\begin{matrix}\text{exactly } j \text{ INs not con-}\\ \text{nected to any ONs}\end{matrix}\right\} && (18)\\ &= \sum_{j=1}^{k}\Pr\{j\}, && (19)\end{aligned}$$

where in the last line we have used the short-hand notation

$$\Pr\{j\} := \Pr\left\{\begin{matrix}\text{exactly } j \text{ INs not con-}\\ \text{nected to any ONs}\end{matrix}\right\}.$$

Although the summands in (18) or (19) are not given explicitly, they are available implicitly in another expression for (12)

$$\Pr\left\{\begin{matrix}i\ \text{particular INs not}\\ \text{connected to any ONs}\end{matrix}\right\} = \frac{\sum\limits_{j=i}^{k}\binom{j}{i}\Pr\{j\}}{\binom{k}{i}}. \tag{20}$$

In the following, the simple identity $\sum_{\varsigma=1}^{\nu}(-1)^{\varsigma+1}\binom{\nu}{\varsigma} = 1$ is used, as well as the fact that $\binom{\nu}{\varsigma} > 0$ if $\nu, \varsigma \in \mathbb{N}_0$ and $0 \leq \varsigma \leq \nu$, and that $\binom{\nu}{\varsigma} = 0$ in all other cases.

Multiplying (20) by $(-1)^{i+1}\binom{k}{i}$ and summing over i yields

$$\begin{aligned}
&\sum_{i=1}^{k}(-1)^{i+1}\binom{k}{i}\Pr\left\{\begin{matrix}i \text{ particular INs not}\\ \text{connected to any ONs}\end{matrix}\right\} \qquad (21)\\
&= \sum_{i=1}^{k}(-1)^{i+1}\sum_{j=i}^{k}\binom{j}{i}\Pr\{j\}\\
&= \sum_{i=1}^{k}\sum_{j=i}^{k}(-1)^{i+1}\binom{j}{i}\Pr\{j\}\\
&= \sum_{i=1}^{k}\sum_{j=1}^{k}(-1)^{i+1}\binom{j}{i}\Pr\{j\}\\
&= \sum_{j=1}^{k}\Pr\{j\}\sum_{i=1}^{k}(-1)^{i+1}\binom{j}{i}\\
&= \sum_{j=1}^{k}\Pr\{j\}\sum_{i=1}^{j}(-1)^{i+1}\binom{j}{i}\\
&= \sum_{j=1}^{k}\Pr\{j\} = \underline{P}^{[\mathrm{ML}]}\left(\cancel{W}\right).
\end{aligned}$$

Finally, inserting (12) into (21) yields (16) and concludes the assertion. ■

C. Numerical Evaluation and Comparison with Monte Carlo Simulations

In Fig. 1 the four bounds are depicted for an exemplary LT code ensemble, namely the expurgated sparse random linear fountain ensemble[4] [5] over $\mathbb{F}_2$ and $\mathbb{F}_{64}$ with the same number of input *bits*, i.e. $k = 300$ and $k = 50$, respectively, and average degree $\bar{d} = 10$. The respective upper bounds almost coincide with the included residual erasure rates obtained by Monte Carlo simulations. Each point marked by a red plus on the red curves is obtained from solving $2.5 \cdot 10^7$ ($\mathbb{F}_2$) and 10^9 ($\mathbb{F}_{64}$) systems of linear equations, where the matrices are taken from the just mentioned LT code ensemble.

IV. Conclusions

LT codes over higher order Galois fields and under ML decoding have excellent erasure correction properties. For this setup, we have derived tight upper and lower bounds on the residual word erasure probability. These bounds, together with the bounds on the residual symbol erasure probability which we have proposed in a previous work, now form a complete set of four bounds facilitating an efficient and accurate analysis of the erasure correction performance of LT code ensembles.

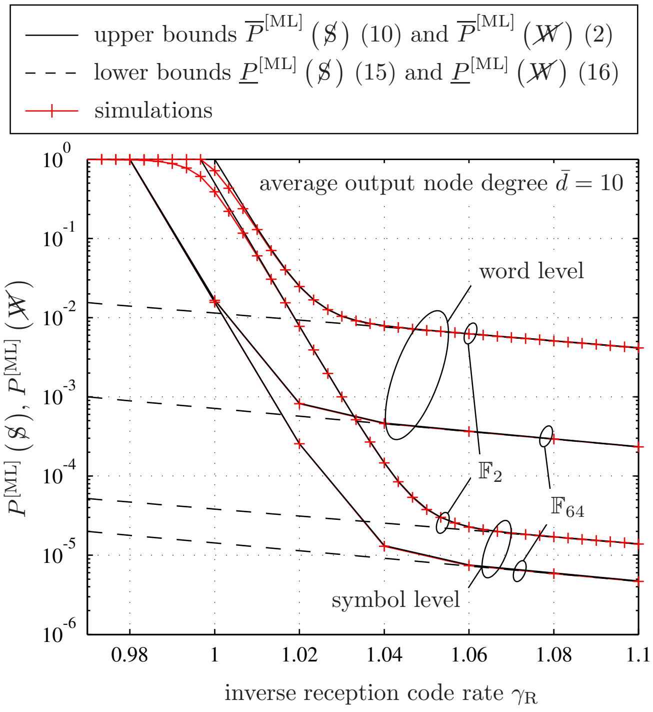

Fig. 1. Bounds on the word and symbol erasure probability after ML decoding as well as simulated residual erasure rates for the expurgated sparse random linear fountain ensemble [5] with the same number of input *bits*, namely 300, and average degree $\bar{d} = 10$. The code over $\mathbb{F}_{64}$ has thus an input size $k = 50$ of 6-bit symbols. The visible piecewise linearity of the latter code's curves arises from the discrete nature of the transmission process. An increase of γ_R by 0.02 corresponds to the reception of one additional encoded symbol.

References

[1] M. Luby, "LT Codes," in *IEEE Symposium on Foundations of Computer Science (FOCS)*, Vancouver, BC, Canada, November 2002, pp. 271–280.

[2] J. W. Byers, M. Luby, M. Mitzenmacher, and A. Rege, "A Digital Fountain Approach to Reliable Distribution of Bulk Data," *ACM SIGCOMM Computer Communication Review*, vol. 28, pp. 56–67, Oct. 1998.

[3] G. Liva, E. Paolini, and M. Chiani, "Performance versus Overhead for Fountain Codes over $\mathbb{F}_q$," *IEEE Communications Letters*, vol. 14, no. 2, pp. 178–180, 2010.

[4] M. Luby, A. Shokrollahi, M. Watson, T. Stockhammer, and L. Minder, "RaptorQ Forward Error Correction Scheme for Object Delivery," IETF RFC 6330, August 2011.

[5] B. Schotsch, R. Lupoaie, and P. Vary, "The Performance of Low-Density Random Linear Fountain Codes over Higher Order Galois Fields under Maximum Likelihood Decoding," in *Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, USA, September 2011, pp. 1004–1011.

[6] A. Shokrollahi, S. Lassen, and R. Karp, "Systems and Processes for Decoding Chain Reaction Codes Through Inactivation," U.S. Patent 6,856,263, February 2005.

[7] E. Paolini, G. Liva, B. Matuz, and M. Chiani, "Maximum Likelihood Erasure Decoding of LDPC Codes: Pivoting Algorithms and Code Design," *IEEE Transactions on Communications*, vol. 60, no. 11, pp. 3209–3220, 2012.

[8] QUALCOMM Incorporated, "RaptorQ$^{\mathrm{TM}}$ Technical Overview," 2010.

[9] S. Shamai, I. E. Telatar, and S. Verdú, "Fountain Capacity," *IEEE Transactions on Information Theory*, vol. 53, no. 11, pp. 4372–4376, 2007.

[10] N. Rahnavard, B. N. Vellambi, and F. Fekri, "Rateless Codes With Unequal Error Protection Property," *IEEE Transactions on Information Theory*, vol. 53, no. 4, pp. 1521–1532, 2007.

[11] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[12] R. P. Stanley, *Enumerative Combinatorics*, 2nd ed. Cambridge University Press, 2011, vol. 1.

[13] A. Shokrollahi, "Raptor Codes," *IEEE Transactions on Information Theory*, vol. 52, no. 6, pp. 2551–2567, 2006.

[4] Note that in [5] the expurgated sparse random linear fountain ensemble is called low-density random linear fountain code. By the additional term *expurgated* it shall be emphasised that in contrast to the element-wise random construction of the sparse (or low-density) random linear fountain ensemble, all-zero rows are removed, i.e. $\Omega_0 = 0$.