The Performance of Low-Density Random Linear Fountain Codes over Higher Order Galois Fields under Maximum Likelihood Decoding

Birgit Schotsch, Radu Lupoaie, and Peter Vary
Institute of Communication Systems and Data Processing (ind)
RWTH Aachen University, Aachen, Germany
{schotsch|vary}@ind.rwth-aachen.de

***Abstract*—Digital fountain codes over higher order Galois fields exhibit a better performance than their binary counterparts under maximum likelyhood (ML) decoding when transmitted over a symbol erasure channel (SEC). Especially random linear fountain (RLF) codes exhibit an excellent performance, though at the expense of a high computational complexity for decoding due to their high density generator matrix. For practical applications, we propose RLF codes with a reduced density over higher order Galois fields. Although the reduction of the density results in an error floor at higher reception overheads, the level of this error floor can be well controlled by two parameters. For error floor levels that are tolerable in practical applications, a significant density reduction and thus a reduction of the computational complexity can be achieved. Furthermore, we derive a general upper bound on the symbol erasure rate for Luby Transform (LT) codes over Galois fields $\mathbb{F}_q$ of order q. Finally, we propose a method to enhance decoding of $\mathbb{F}_q$-codes in the presence of bit erasures by using the binary images of the $\mathbb{F}_q$-elements, such that not complete $\mathbb{F}_q$-elements have to be discarded if their binary counterparts are impaired by bit erasures.**

I. Introduction

Fountain codes are a class of rateless erasure correcting codes that have been introduced in [1] for usage in packet-switched communication networks as an alternative solution to retransmission schemes such as automatic repeat request (ARQ) after packet losses. Rateless codes have been initially designed for the binary erasure channel (BEC) not requiring any knowledge of the erasure probability ϵ. In multicast scenarios, where different users experience different channel conditions and independent losses that are unknown to the transmitter, this feature is particularly useful. With rateless codes, the transmitter can produce a potentially infinite number n_{T} of encoded symbols $\mathbf{y} = (y_1, y_2, \ldots y_{n_{\mathrm{T}}})$ from a finite amount of k input symbols $\mathbf{u} = (u_1, u_2, \ldots u_k)$.

In the original proposal, binary codes have been considered, i.e. the input and output symbols u_i and y_j consist of l bits each, where $i \in \{1, 2, \ldots k\}$ and $j \in \{1, 2, \ldots n_{\mathrm{T}}\}$, and thus, $\mathbf{u} \in \mathbb{F}_2^{[l\times k]}$ and $\mathbf{y} \in \mathbb{F}_2^{[l\times n_{\mathrm{T}}]}$. Similar to low-density parity-check (LDPC) codes, rateless codes can also be defined over Galois fields $\mathbb{F}_q$ of order $q = 2^m$, where $m > 1$, see [2]–[4]. Accordingly, the symbols u_i or y_j represent a collection of l elements from $\mathbb{F}_q$ as depicted in Fig. 1. However, since the symbols u_i and y_j can contain any fixed number $l \in \mathbb{N}$ of elements from $\mathbb{F}_q$ (including the binary case $q = 2$) and as this number l has no influence on the erasure correction performance of the codes [5], we will assume $l = 1$ in the following, i.e. $\mathbf{u} \in \mathbb{F}_q^{[1\times k]}$ and $\mathbf{y} \in \mathbb{F}_q^{[1\times n_{\mathrm{T}}]}$ with $q \geq 2$. It should be noted though that the $\mathbb{F}_q$-elements have an equivalent binary representation which requires m bits per element. In order to deliver a fair comparison between codes over Galois fields of different orders, we fix the number $k = k_2$ of input *bits* and distribute them to $k_q = \lceil \frac{k_2}{\mathrm{ld}\, q} \rceil = \lceil \frac{k_2}{m} \rceil$ input *symbols*, such that the input size of a code over $\mathbb{F}_q$ with $q = 2^m$ is k_q.

Good rateless codes have the property that the receiver is able to decode the original k_q input symbols $\mathbf{u}$ from any $n_{\mathrm{R}} = k_q(1 + \varepsilon_{\mathrm{R}})$ received code symbols with high probability if $\varepsilon_{\mathrm{R}} \geq 0$, where ε_{R} is the relative reception overhead. Practical rateless codes are sparse-graph codes, e.g. LT codes [5], Raptor codes [6] or Online codes [7] for which simple and efficient encoding and decoding algorithms exist.

In this paper we consider random linear fountain (RLF) codes [6], [8], a type of LT codes with excellent error correcting performance under maximum likelihood (ML) decoding. Specifically, we analyse RLF codes with a low density (LDRLF codes) [9] over higher order Galois fields. We will show that the advantages of the binary codes from [9] also apply if these codes are generalised to higher order Galois fields.

The most popular decoding algorithm for LT codes is the computationally cheap, though suboptimal, belief propagation (BP) algorithm that performs well on properly designed codes, but only for large blocklengths. The optimal decoding algorithm (optimal in the sense of minimal bit erasure probability at a certain reception overhead) is ML decoding, which, in the case of the erasure channel, is equivalent to solving a consistent system of n_{R} linear equations in k unknowns by means of Gaussian elimination (GE). However, GE is computationally expensive for large blocklengths. For dense *binary* codes the decoding cost is $\mathcal{O}(n_{\mathrm{R}}k)$ per input bit, but

This work was supported by the UMIC Research Centre, RWTH Aachen University.

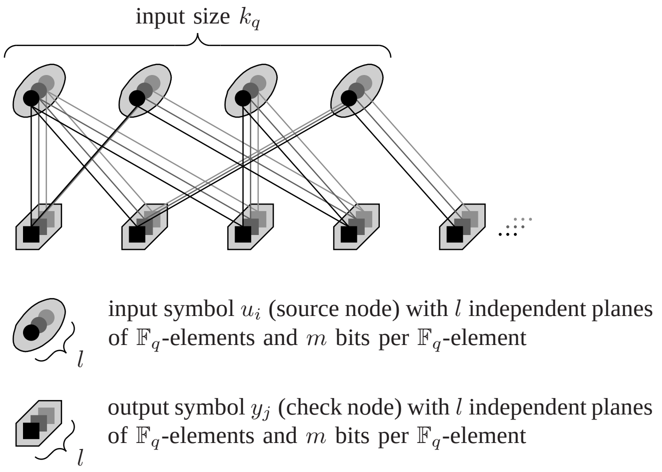

input size k_q
input symbol u_i (source node) with l independent planes of $\mathbb{F}_q$-elements and m bits per $\mathbb{F}_q$-element
l
output symbol y_j (check node) with l independent planes of $\mathbb{F}_q$-elements and m bits per $\mathbb{F}_q$-element
l

Fig. 1. General LT code graph with l independent planes of $\mathbb{F}_q$-elements and m bits per $\mathbb{F}_q$-element. Since l has no influence on the erasure correction performance of the codes [5], we assume $l = 1$ in this paper.

it decreases for less dense codes. The density Δ of an LT code over $\mathbb{F}_q$ is the ratio of the number of non-zero entries in the generator matrix to the total number of entries.

Considering delay sensitive applications, the usage of short codes is inevitable. Moreover, in such a case the ML decoding algorithm is the only decoding algorithm that shows a good performance and its complexity is also affordable for short codes.

Furthermore, we show that the excellent error correcting performance of RLF codes under ML decoding increases with the field order q. However, this performance gain is not as large as might be concluded from the results in [2] and [4]. In contrast to our setup, the number k of input *symbols* is kept constant in [2] and [4], while the number l of $\mathbb{F}_q$-elements per input symbol is adapted such that the number of equivalent input bits per source block is constant. However, increasing l is only an issue to save complexity and a means for a better parallelisation. The erasure correction performance of a code is independent of l [5]. Therefore, we claim that l should be kept constant for a fair comparison of the erasure correction performance and instead, the input size k_q of the code should be adapted as a function of the Galois field order $q = 2^m$ to ensure that the number of equivalent input bits per source block is constant. This allows a higher input size for codes over Galois fields of lower order by which their erasure correction performance is increased. It should be noted that by keeping l constant ($l = 1$ in this paper), it is required to consider the *relative* reception overhead in order to compare the erasure correction performance of codes over different Galois fields.

II. LT Codes over Higher Order Galois Fields

The generator matrix $\mathbf{G} \in \mathbb{F}_q^{[n_\mathrm{T} \times k_q]}$ of an LT code[1], with $q = 2^m$, defines a graph connecting the set of k_q input symbols $\mathbf{u} \in \mathbb{F}_q^{[1 \times k_q]}$ to the set of n_T output symbols $\mathbf{y} \in \mathbb{F}_q^{[1 \times n_\mathrm{T}]}$, where n_T can be arbitrarily large.

The input symbols are associated with input nodes, whereas the output symbols are associated with output nodes that are also called check nodes. In vector-matrix notation, encoding is performed by $\mathbf{y}^\mathrm{T} = \mathbf{G}\mathbf{u}^\mathrm{T}$. In contrast to traditional block codes, the matrix $\mathbf{G}$ is generated online and can differ for each data block. The decoder knows of each output symbol to which input symbols it is connected, i.e. the matrix $\mathbf{G}$ is known. This can be achieved by synchronising identical pseudo-random processes that produce $\mathbf{G}$.

The erasure correcting properties of LT codes are mainly defined by the so-called check node degree distribution $\Omega_0, \Omega_1, \dots \Omega_k$ on $\{0, 1, \dots k\}$, where a check node has degree d with probability Ω_d, i.e. it is connected to d distinct input nodes, chosen uniformly at random from the set of k_q input nodes. Typically, the degree distribution is described by its generating polynomial $\Omega(x) = \sum_{d=0}^{k_q} \Omega_d \, x^d$.

In the generator matrix $\mathbf{G}$ the d non-zero entries in a row correspond to the values of the d edges between a check node and d input nodes. The value of a check node is determined by adding up the product of each value of the d input nodes with the value of the corresponding connecting edge. The non-zero entries of $\mathbf{G}$ are sampled uniformly from the set of $q - 1$ non-zero $\mathbb{F}_q$-elements. The encoder produces n_T output symbols that are then transmitted over a symbol erasure channel (SEC) that randomly erases some of these transmitted Galois field symbols. At the receiver, $n_\mathrm{R} \leq n_\mathrm{T}$ symbols are collected from which the decoder tries to reproduce the original k_q input symbols.

Having collected $n_\mathrm{R} \leq n_\mathrm{T}$ output symbols, the decoder uses the n_R rows of $\mathbf{G}$ that are associated with the received, i.e, the collected, non-erased symbols to make up a new matrix $\mathbf{G}'$ on which decoding is performed. Since $\mathbf{G}'$ consists of a set of n_R rows sampled at random from the original matrix $\mathbf{G}$ according to the erasures that occur on the SEC, $\mathbf{G}'$ follows the same degree distribution as $\mathbf{G}$. Due to the weak erasure correction properties of BP decoding for a short blocklength, we consider only ML decoding in this paper.

III. Analysis of Low-Density Random Linear Fountain Codes over $\mathbb{F}_q$

So-called random linear fountain (RLF) codes or random LT codes have been introduced in [8] and [6] and have been extended to higher order Galois fields in [2]. We refer to these RLF codes as conventional RLF codes or sometimes simply as RLF codes in contrast to our proposed low-density RLF (LDRLF) codes. These codes have the degree distribution

$$\Omega(x) = q^{-k_q} \left(1 + (q-1)x\right)^{k_q} , \qquad (1)$$

where $q = 2$ in [8] and [6]. This degree distribution results from sampling each entry in the generator matrix $\mathbf{G}$ uniformly at random from the set of q Galois field elements, i.e. each element $a \in \mathbb{F}_q$ is chosen with probability $P_a = \frac{1}{q}$. Thus, an edge between an input and an output node is created as the outcome of a Bernoulli trial with probability $P_{\neg 0} = \frac{q-1}{q}$, where $P_{\neg 0}$ denotes the probability

[1] For a more detailed description of *binary* LT codes, we refer the reader to the original paper of Luby [5].

of occurrence of non-zero $\mathbb{F}_q$-elements. However, this construction leads to very dense LT matrices according to the field order q, as the probability $P_{\neg 0}$ of non-zero $\mathbb{F}_q$-elements is equal to the expected value of the density Δ of the code. The probability of generating a row of weight d is then[2] $\Omega_d = \binom{k_q}{d} P_{\neg 0}^d (1 - P_{\neg 0})^{(k_q - d)} = q^{-k_q} \binom{k_q}{d} (q-1)^d$.

ML decoding on an SEC is equivalent to solving a system of n_R linear equations in k_q unknowns. Thus, the probability that the system is solvable equals the probability that the matrix $\mathbf{G}'$ at the receiver has rank k_q. Hence, the frame erasure probability $P^\mathrm{ML}_{q,\mathrm{F}}$ after ML decoding equals the probability that $\mathbf{G}'$ has not rank k_q. It is given by (cf. e.g. [10])

$$P^\mathrm{ML}_{q,\mathrm{F}} = 1 - \prod_{i=1+\eta_{\mathrm{R,S}}}^{k_q+\eta_{\mathrm{R,S}}} \left(1 - q^{-i}\right), \tag{2}$$

where $\eta_{\mathrm{R,S}} = k_q \varepsilon_\mathrm{R}$ is the absolute symbol reception overhead. As shown in [2], tight upper and lower bounds[3] on the frame erasure probability $P^\mathrm{ML}_{q,\mathrm{F}}$ exist for conventional RLF codes that are independent of the input size k_q

$$\underline{P}^\mathrm{ML}_{q,\mathrm{F}} = q^{-(\eta_{\mathrm{R,S}}+1)} \leq P^\mathrm{ML}_{q,\mathrm{F}} < \frac{1}{q-1} q^{-\eta_{\mathrm{R,S}}} = \overline{P}^\mathrm{ML}_{q,\mathrm{F}}. \tag{3}$$

Also of great interest is the symbol erasure rate $P^\mathrm{ML}_{q,\mathrm{S}}$. In the following, we derive a general upper bound on $P^\mathrm{ML}_{q,\mathrm{S}}$ for LT codes with an arbitrary degree distribution $\Omega(x)$. And as a special case we show that $P^\mathrm{ML}_{q,\mathrm{S}}$ of conventional RLF codes is upper bounded by $\overline{P}^\mathrm{ML}_{q,\mathrm{S}} = q^{-(\eta_{\mathrm{R,S}}+1)}$. The derivation of this general upper bound follows closely the arguments from [11]. In particular, Lemma 1 from [11] is generalised for codes over higher order Galois fields.

Lemma 1. *Given an LT code of length k_q with generator matrix $\mathbf{G} \in \mathbb{F}_q^{[n_\mathrm{T} \times k_q]}$, following the check node degree distribution $\Omega(x)$, where the non-zero elements in $\mathbf{G}$ are chosen with equal probability, an upper bound on the symbol erasure probability $P^\mathrm{ML}_{q,\mathrm{S}}$ is*

$$\overline{P}^\mathrm{ML}_{q,\mathrm{S}} = \sum_{w=1}^{k_q} \binom{k_q - 1}{w - 1} (q-1)^{w-1} \cdot \left[\frac{1}{q} \sum_d \Omega_d \frac{\sum\limits_{s=0}^{d} \binom{w}{s} \binom{k_q - w}{d - s} \left[1 - (1-q)^{1-s}\right]}{\binom{k_q}{d}} \right]^{k_q \gamma_\mathrm{R}} \tag{4}$$

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

Proof: The probability $P^\mathrm{ML}_{q,\mathrm{S}}$ is equal to the probability that the ith $\mathbb{F}_q$-symbol cannot be determined by ML decoding for an arbitrary $i \in \{1, 2, \ldots k_q\}$

$$P^\mathrm{ML}_{q,\mathrm{S}} = \Pr\left\{ \exists \mathbf{u} \in \mathbb{F}_q^{[1 \times k_q]},\, u_i = a :\ \mathbf{G}'\mathbf{u}^\mathrm{T} = \mathbf{0}^\mathrm{T} \right\}, \tag{5}$$

with arbitrary but fixed $a \in \mathbb{F}_q \setminus \{0\}$. The right-hand side of (5) is the probability of the ith column of matrix $\mathbf{G}'$ being linearly dependent on a non-empty set of columns. This can be upper bounded by the probability of any possible set of columns of $\mathbf{G}'$ being linearly dependent on column i

$$P^\mathrm{ML}_{q,\mathrm{S}} \leq \overline{P}^\mathrm{ML}_{q,\mathrm{S}} = \sum_{\substack{\mathbf{u} \in \mathbb{F}_q^{[1 \times k_q]},\\ u_i = a}} \Pr\left\{ \mathbf{G}'\mathbf{u}^\mathrm{T} = \mathbf{0}^\mathrm{T} \right\}. \tag{6}$$

The $k_q \gamma_\mathrm{R}$ rows of $\mathbf{G}'$ can be viewed as the outcomes of independent trials of a random variable $\mathbf{r} \in \mathbb{F}_q^{[1 \times k_q]}$.

$$\overline{P}^\mathrm{ML}_{q,\mathrm{S}} = \sum_{\substack{\mathbf{u} \in \mathbb{F}_q^{[1 \times k_q]},\\ u_i = a}} \left[\Pr\left\{ \mathbf{r}\mathbf{u}^\mathrm{T} = 0 \right\} \right]^{k_q \gamma_\mathrm{R}} \tag{7}$$

The weight of a vector over $\mathbb{F}_q$ equals the number of non-zero elements and is denoted $|\cdot|$. Now, the probability $\Pr\left\{\mathbf{r}\mathbf{u}^\mathrm{T} = 0\right\}$ is determined, conditioned on $|\mathbf{r}| = d$ and $|\mathbf{u}| = w$. A row $\mathbf{r}$ has weight $|\mathbf{r}| = d$ with probability Ω_d and there are $\binom{k_q - 1}{w - 1} (q-1)^{w-1}$ choices of $\mathbf{u}$ of weight w with $u_i = a$. Let $\mathbf{v} = (v_1, v_2, \ldots, v_{k_q})$ with $v_i = r_i u_i$, where v_i, r_i and u_i are the ith elements of the vectors $\mathbf{v}$, $\mathbf{r}$ and $\mathbf{u}$, respectively, then

$$\overline{P}^\mathrm{ML}_{q,\mathrm{S}} = \sum_{w=1}^{k_q} \binom{k_q - 1}{w - 1} (q-1)^{w-1} \cdot \left[\sum_d \Omega_d \Pr\left\{ \mathbf{r}\mathbf{u}^\mathrm{T} = 0 \,\middle|\, |\,\mathbf{r}\,| = d,\ |\,\mathbf{u}\,| = w \right\} \right]^{k_q \gamma_\mathrm{R}} \tag{8}$$

with

$$\Pr\left\{ \mathbf{r}\mathbf{u}^\mathrm{T} = 0 \,\middle|\, |\,\mathbf{r}\,| = d,\ |\,\mathbf{u}\,| = w \right\} = \sum_{s=0}^{d} \Pr\left\{ |\,\mathbf{v}\,| = s \,\middle|\, |\,\mathbf{r}\,| = d,\ |\,\mathbf{u}\,| = w \right\} \cdot \Pr\left\{ \sum_{i=1}^{k_q} v_i = 0 \,\middle|\, |\,\mathbf{v}\,| = s \right\}. \tag{9}$$

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

$$\Pr\left\{ |\,\mathbf{v}\,| = s \,\middle|\, |\,\mathbf{r}\,| = d,\ |\,\mathbf{u}\,| = w \right\} = \frac{\binom{w}{s}\binom{k_q - w}{d - s}}{\binom{k_q}{d}}. \tag{10}$$

The last term in (9) is the number $N_0(s, q)$ of possibilities that s non-zero $\mathbb{F}_q$-elements add up to zero, taking the elements' order into account, divided by the number $N(s, q)$ of all possibilities to draw s times with replacement from the

[2] In practical systems and also in our simulations Ω_0 equals zero. Thus, a modification of the probabilities Ω_d for $d > 0$ is necessary, in order to obtain $\sum_{d=1}^{k_q} \Omega_d = 1$ and to keep the average check node degree constant. However, for not too small input sizes k_q or average check node degrees $\bar{\Omega}$, the induced error of considering $\Omega_0 \neq 0$ in the theoretical analyis is negligible. Therefore, we will not set $\Omega_0 = 0$ in the following derivations.

[3] For notational convenience, we will implicitly assume that probabilities and their bounds are limited from above by one, i.e. the operation $\min\{1, \cdot\}$ is omitted.

set of the $q-1$ non-zero $\mathbb{F}_q$-elements also taking the order into account:

$$\Pr\left\{\sum_{i=1}^{k_q} v_i = 0 \Big| \,|\,\mathbf{v}\,| = s\right\} = \frac{N_0(s,\,q)}{N(s,\,q)}. \tag{11}$$

The problem of determining $N_0(s,q)$ is equivalent to finding the number of closed walks of length s in a complete graph of size q of which a closed form expression can be found, e.g. in [12]

$$N_0(s,\,q) = \frac{1}{q}\left[(q-1)^s + (q-1)\,(-1)^s\right]. \tag{12}$$

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

$$\Pr\left\{\sum_{i=1}^{k_q} v_i = 0 \Big| \,|\,\mathbf{v}\,| = s\right\} = \frac{1}{q}\left[1-(1-q)^{1-s}\right]. \tag{13}$$

Finally, inserting (10) and (13) into (9) and the resulting expression into (8) concludes the assertion. □

Using Lemma 1 and some arguments similar to those in [9], it is shown in the following that for conventional RLF codes over $\mathbb{F}_q$ the upper bound (4) results in $\overline{P}_{q,\mathrm{S}}^{\mathrm{ML}} = q^{-(\eta_{\mathrm{R,S}}+1)}$, which is a generalisation of Lemma 2 in [9] to higher order Galois fields:

Lemma 2. *Given a conventional random linear fountain code over $\mathbb{F}_q$, i.e. an LT code over $\mathbb{F}_q$ with the degree distribution $\Omega(x) = q^{-k_q}\sum_{d=1}^{k_q}\binom{k_q}{d}(q-1)^d\,x^d$, and the absolute symbol reception overhead $\eta_{\mathrm{R,S}} = n_{\mathrm{R}} - k_q = (\gamma_{\mathrm{R}}-1)k_q$, an upper bound on the symbol erasure probability $P_{q,\mathrm{S}}^{\mathrm{ML}}$ after ML decoding is $\overline{P}_{q,\mathrm{S}}^{\mathrm{ML}} = q^{-(\eta_{\mathrm{R,S}}+1)}$ for $\eta_{\mathrm{R,S}} \geq 0$.*

Proof: Inserting the coefficients of $\Omega(x)$ into (4) yields (14) on the following page. In the term in (14) which is denoted by $\Gamma_q(k_q)$, the upper limit of the inner summation can be changed from d to k_q without affecting the result, since[4] the terms in which $s > d$ amount to zero. Now, the two summations can be exchanged as the inner summation variable s is independent of the outer summation variable d.

$$\Gamma_q(k_q) = \sum_{s=0}^{k_q}\binom{w}{s}\left[1-(1-q)^{1-s}\right]\sum_{d=0}^{k_q}\binom{k_q-w}{d-s}(q-1)^d$$

With

$$\begin{aligned}\sum_{d=0}^{k_q}\binom{k_q-w}{d-s}(q-1)^d &= \sum_{d=0}^{k_q-w}\binom{k_q-w}{d}(q-1)^{d+s}\\ &= (q-1)^s\,q^{k_q-w}\end{aligned}$$

the term $\Gamma_q(k_q)$ can be simplified to

$$\begin{aligned}\Gamma_q(k_q) &= q^{k_q-w}\sum_{s=0}^{k_q}\binom{w}{s}\left[(q-1)^s + (-1)^s\,(q-1)\right]\\ &= q^{k_q}.\end{aligned}$$

Inserting this result for $\Gamma_q(k_q)$ into (14) we obtain

$$\begin{aligned}\overline{P}_{q,\mathrm{S}}^{\mathrm{ML}} &= \sum_{w=1}^{k_q}\binom{k_q-1}{w-1}(q-1)^{w-1}\,q^{-k_q\gamma_{\mathrm{R}}}\\ &= q^{-k_q\gamma_{\mathrm{R}}}\sum_{w=0}^{k_q-1}\binom{k_q-1}{w}(q-1)^w\\ &= q^{-k_q\gamma_{\mathrm{R}}}q^{k_q-1} = q^{-k_q(\gamma_{\mathrm{R}}-1)-1} = q^{-k_q\varepsilon_{\mathrm{R}}-1} \qquad (15)\\ &= q^{-(\eta_{\mathrm{R,S}}+1)}. \qquad (16)\end{aligned}$$

□

A lower bound on $P_{q,\mathrm{S}}^{\mathrm{ML}}$ corresponds to the probability that an input node is not connected to any check node. Therefore, the bound which is known for binary codes [6] is also valid for other Galois fields:

$$\underline{P}_{q,\mathrm{S}}^{\mathrm{ML}} = \left(1-\frac{\bar{\Omega}}{k_q}\right)^{k_q\gamma_{\mathrm{R}}}, \tag{17}$$

where $\bar{\Omega} = \sum_{d=1}^{k_q} d\,\Omega_d$ is the average check node degree. For RLF codes of arbitrary density this lower bound can also be formulated in terms of the probability $P_{\neg 0}$ of non-zero $\mathbb{F}_q$-elements or even simpler in terms of the probability P_0 of the zero element

$$\underline{P}_{q,\mathrm{S}}^{\mathrm{ML}} = (1-P_{\neg 0})^{k_q\gamma_{\mathrm{R}}} = P_0^{k_q\gamma_{\mathrm{R}}}.$$

In Fig. 2(a) the upper bounds $\overline{P}_{q,\mathrm{S}}^{\mathrm{ML}}$ (16) of conventional RLF codes over different Galois fields are depicted as a function of the *absolute* symbol reception overhead $\eta_{\mathrm{R,S}}$. In this form, $\overline{P}_{q,\mathrm{S}}^{\mathrm{ML}}$ is independent of the input size k_q. Now, one has to be careful not to draw the wrong conclusion that by using higher order Galois fields, lower symbol erasure probabilities $P_{q,\mathrm{S}}^{\mathrm{ML}}$ could be reached much faster as is claimed in [2] and [4][5]. In Fig. 2(a) it is not taken into account that an $\mathbb{F}_2$-element consists of 1 bit, whereas an $\mathbb{F}_{256}$-element consists of 8 bits. Therefore, in Fig. 2(b) the upper bounds (15) are depicted in terms of the *relative* reception overhead ε_{R} for an RLF code of an exemplary equivalent input size of $k_2 = 840$ bits[6]. It should be noted that in contrast to Fig. 2(a) the upper bounds have a constant distance between each other and thus, the gain in terms of the relative reception overhead is constant between two codes over different fields as can be seen from (15).

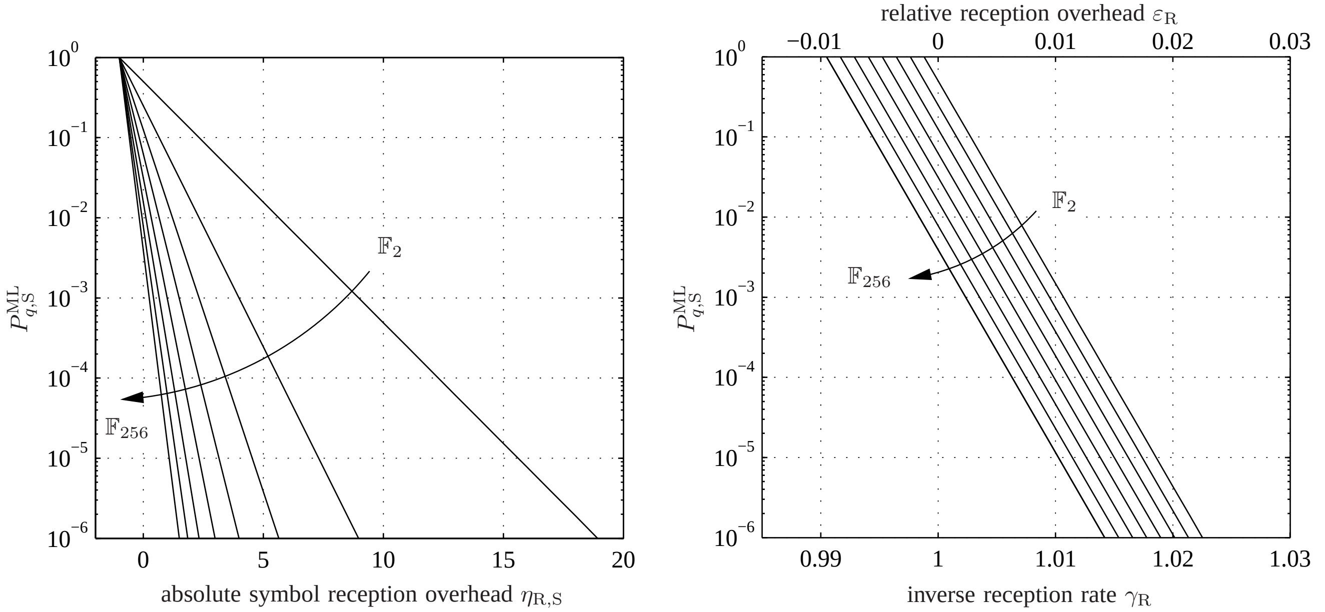
ML decoding over $\mathbb{F}_2$ has a complexity of $\mathcal{O}(k_2^3)$ per information word. Using higher order Galois fields while keeping the equivalent binary input size constant, the input size in terms of $\mathbb{F}_q$-elements decreases, so that less computation steps are necessary. However, these steps are computationally more complex, i.e. $\mathcal{O}((\beta_m k_q)^3)$ with $\beta_m > 1$.

[4] $\binom{\nu}{\kappa} > 0$ if $\nu,\,\kappa \in \mathbb{N}_0$ and $0 \leq \kappa \leq \nu$. In all other cases $\binom{\nu}{\kappa} = 0$ applies.

[5] The above reasoning is independent from the fact that [2] and [4] considered *frame* erasure probabilities.

[6] The equivalent binary input size of 840 bits is merely chosen since it is the least common multiple of $m \in \{1,\,2,\ldots 8\}$ and the codes in the different fields have *exactly the same* equivalent binary input size. Using arbitrary equivalent binary input sizes, the input sizes in terms of $\mathbb{F}_q$-elements are then $k_q = \lceil\frac{k_2}{\mathrm{ld}\,q}\rceil = \lceil\frac{k_2}{m}\rceil$.

$$\overline{P}^{\mathrm{ML}}_{q,\mathrm{S}} = \sum_{w=1}^{k_q} \binom{k_q-1}{w-1} (q-1)^{w-1} \cdot \left[q^{-(k_q+1)} \underbrace{\sum_{d=0}^{k_q} (q-1)^d \sum_{s=0}^{d} \binom{w}{s}\binom{k_q-w}{d-s} \left[1-(1-q)^{1-s}\right]}_{\Gamma_q(k_q)} \right]^{k_q\gamma_{\mathrm{R}}} \tag{14}$$



(a) Upper bounds (16) on $P^{\mathrm{ML}}_{q,\mathrm{S}}$ as a function of $\eta_{\mathrm{R,S}}$.

(b) Upper bounds (15) on $P^{\mathrm{ML}}_{q,\mathrm{S}}$ as a function of γ_{R} or ε_{R}, respectively, for input sizes of $k_q = \frac{840}{\mathrm{ld}\, q} = \frac{840}{m} \in \{840,\, 420, \ldots 105\}$.

Fig. 2. Upper bounds $\overline{P}^{\mathrm{ML}}_{q,\mathrm{S}}$ of conventional RLF codes over $\mathbb{F}_{2^m}$ with $m \in \{1,\, 2, \ldots 8\}$.

In [13] an optimised approach for multiplications over $\mathbb{F}_q$ is proposed. Since computer architectures are generally based on bytewise operations, we exemplarily consider a code over $\mathbb{F}_{256}$, i.e. $m = 8$. Using, e.g. the 'Log/Antilog Optimized' technique for the multiplications over $\mathbb{F}_{256}$ and assuming three table lookups and one add operation per multiplication (cf. [13, Table 1]), we coarsely estimate that $\beta_8 = 4$. With this assumption, the complexity for the code over $\mathbb{F}_{256}$ is $\mathcal{O}((4k_{256})^3) = \mathcal{O}(\frac{1}{8}k_2^3)$. Consequently, with optimised Galois field arithmetic implementations and eventually also smart ML decoding algorithms, the computational complexity per information word can be decreased with increasing field order q.

In Fig. 3 relative simulation times of the conventional RLF codes from Fig. 2(b) are depicted at an inverse reception overhead $\gamma_{\mathrm{R}} \approx 1.01$. The simulation times are given relative to that of the binary code. The dashed line ($t_{\mathrm{r}} = m^{-3}$) indicates the order of complexity, since the Gaussian elimination algorithm has a complexity of $\mathcal{O}(k_q^3)$ per information word. At least for our simulation, the complexity factor β is smaller than 4, i.e. our simulation time speedups are even better than estimated in the previous paragraph. However, the factor β strongly depends on the actual implementation.

In [9] binary RLF codes with reduced density have been analysed. These codes have been shown to have a good performance and can be used instead of their high density counterparts. This behaviour can also be seen with RLF codes over higher order Galois fields. The performance of two example code sets over $\mathbb{F}_2$ to $\mathbb{F}_{64}$ with $\bar{\Omega} = 10$ (code set A) and $\bar{\Omega} = 15$ (code set B) of equivalent binary input size $k_2 = 300$ is shown in Fig. 4 on the last page of this paper. In the large figure, the upper and lower bounds on the symbol erasure probabilities are depicted, while in the small subplot also the simulated symbol erasure rates (SXR) and the corresponding frame erasure rates (FXR) are shown for the codes with $\bar{\Omega} = 10$ over the fields $\mathbb{F}_2$, $\mathbb{F}_8$ and $\mathbb{F}_{64}$. For small input sizes the discrete nature of the codes becomes visible and only discrete points on the graphs (indicated by the round markers) are actually attainable. We will make statements on the performance mostly based on the upper bounds $\overline{P}^{\mathrm{ML}}_{q,\mathrm{S}}$, since these are very close to the simulated symbol erasure rates, as can be seen in the subplot of Fig. 4.

We denote RLF codes over different Galois fields with the same average check node degree $\bar{\Omega}$ and the same equivalent binary input size k_2 as a code set. The erasure correcting performance of codes from the same set is similar. So the size k_2

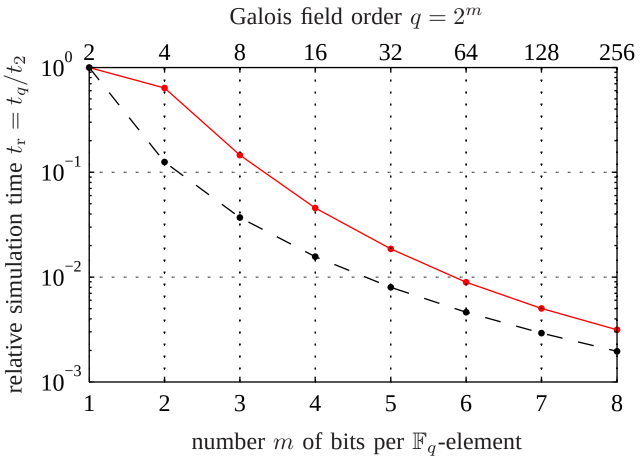


Fig. 3. Relative simulation times of the conventional RLF codes from Fig. 2(b) with input sizes of $k_q = \frac{840}{\mathrm{ld}\, q} = \frac{840}{m} \in \{840, 420, \ldots 105\}$ and $m \in \{1, 2, \ldots 8\}$ at an inverse reception rate $\gamma_\mathrm{R} \approx 1.01$. The simulation times are given relative to that of the binary code. The dashed line ($t_\mathrm{r} = m^{-3}$) indicates the order of complexity (the Gaussian elimination algorithm has a complexity of $\mathcal{O}(k_q^3)$ per information word).

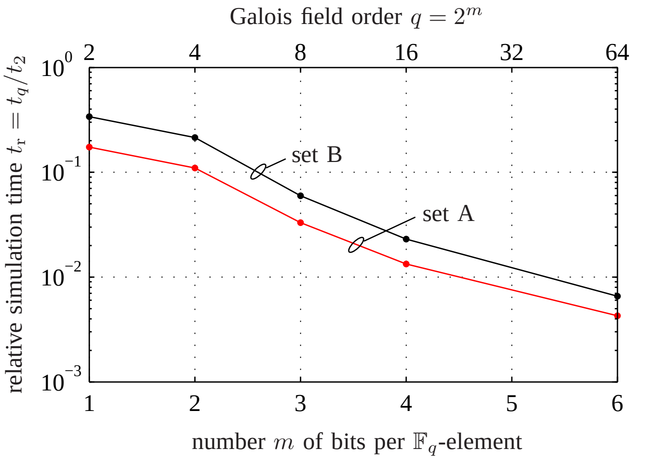


Fig. 6. Relative simulation times of the low-density RLF code sets A ($\bar{\Omega} = 10$) and B ($\bar{\Omega} = 15$) from Fig. 4 with input sizes of $k_q = \frac{300}{\mathrm{ld}\, q} = \frac{300}{m} \in \{300, 150, \ldots 50\}$ and $m \in \{1, 2, 3, 4, 6\}$ at an inverse reception rate $\gamma_\mathrm{R} = 1.04$. The simulation times are given relative to that of the binary code with density $\Delta = 0.5$.

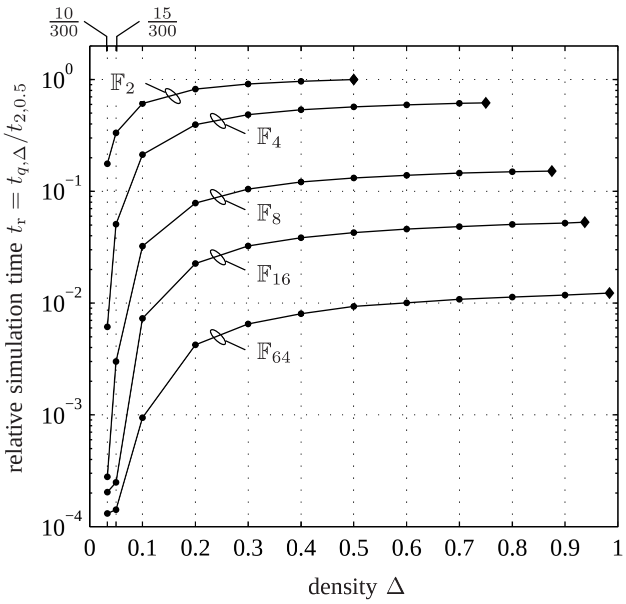


Fig. 5. Relative simulation times of (low-density) RLF codes with input sizes of $k_q = \frac{300}{\mathrm{ld}\, q} = \frac{300}{m} \in \{300, 150, \ldots 50\}$ and $m \in \{1, 2, 3, 4, 6\}$ (as in Fig. 4) at an inverse reception rate $\gamma_\mathrm{R} = 1.04$ as a function of the code density. The simulation times are given relative to that of the conventional binary RLF code, i.e. with density $\Delta = 0.5$. The diamond markers indicate the conventional RLF codes. These have the maximum considered density of $\Delta = 1 - 1/q$ for a Galois field of order q.

and the average degree $\bar{\Omega}$ are crucial parameters for defining the erasure correcting properties. The performance slightly increases with the Galois field order q. For a higher field order q the upper bound is shifted towards lower values of γ_R and also reaches lower values in the error floor region when approaching the corresponding lower bound. Compared to the conventional RLF codes, LDRLF codes apparently exhibit an error floor. However, this error floor can be well adjusted by the parameters k_2 and $\bar{\Omega}$. In addition, most applications do not need arbitrarily small erasure probabilities. Therefore, allowing an error floor leads to a reduced average degree and density, and thus to a reduced computational complexity. In the example code set A, the LDRLF code over $\mathbb{F}_{64}$ has a density $\Delta = 0.2$ and an average degree $\bar{\Omega} = 10$ instead of $\Delta = \frac{63}{64} \approx 0.984$ and $\bar{\Omega} = 49.22$ for a conventional RLF code of the same size and over the same field. Such a decrease of the density entails a remarkable complexity reduction which makes LDRLF codes over higher order Galois fields better suited for practical applications.

In Fig. 5 the relative simulation times are plotted for (low-density) RLF codes over $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_8$, $\mathbb{F}_{16}$ and $\mathbb{F}_{64}$ with input sizes $k_q = \frac{300}{\mathrm{ld}\, q} = \frac{300}{m} \in \{300, 150, \ldots 50\}$, where $m \in \{1, 2, 3, 4, 6\}$ at an inverse reception rate $\gamma_\mathrm{R} = 1.04$. The simulation times are given relative to that of the conventional binary RLF code, i.e. with density $\Delta = 0.5$. The diamond markers indicate the conventional RLF codes. These have the maximum considered density of $\Delta = 1 - 1/q$ for a Galois field of order q. By keeping the equivalent binary input size constant (here $k_2 = 300\,$bits), the relative simulation time can be significantly decreased by choosing a Galois field of higher order. Decreasing the density of the codes gives an additional speedup. However, one has to keep the erasure correction properties of the codes of different densities in mind. Therefore, in Fig. 6 we also show the relative simulation times of code sets A and B from Fig. 4 at an inverse reception rate $\gamma_\mathrm{R} = 1.04$, since the erasure correction performance within a set is very similar. And although codes over higher order Galois fields exhibit a slightly better erasure correction performance, their simulation time is significantly lower.

IV. A Comment on the Symbol Erasure Channel

In this paper we have considered a symbol erasure channel (SEC) in contrast to the binary erasure channel (BEC), since we assume that complete $\mathbb{F}_q$-elements (also denoted as $\mathbb{F}_q$-symbols) are erased. However, since in practice each element or symbol is transmitted in binary form, it may happen that even a single bit erasure leads to the erasure of a complete $\mathbb{F}_q$-element. If bit erasures are distributed among many $\mathbb{F}_q$-elements, it can have a very negative impact on the decodability of the received symbols. Therefore, in the corresponding scenarios, it might be useful to perform the decoding on the binary equivalent of the $\mathbb{F}_q$-code. Each non-zero $\mathbb{F}_q$-element is represented by a power of the so-called companion matrix [14]. The companion matrix corresponds to the primitive element α of $\mathbb{F}_q$ and is defined as the $m \times m$ matrix

$$\mathbf{M} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & \ddots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{m-1} \end{pmatrix}, \qquad (18)$$

where $a(x) = a_0 + a_1 x + \ldots + a_{m-1} x^{m-1} + x^m$ is a primitive polynomial of $\mathbb{F}_q$ with the coefficients $a_i \in \mathbb{F}_2$. The all-zero matrix of the same size corresponds to the zero element.

The binary equivalent of the generator matrix $\mathbf{G}$ is obtained by exchanging each $\mathbb{F}_q$-symbol α^λ, where $\lambda \in \{1, 2, \ldots, q-1\}$, by the corresponding power of the companion matrix, i.e. $\mathbf{M}^\lambda$. Analogously, the input and output symbols are converted to their binary images. If now bit erasures occur, the decoding can be performed as usual in the binary domain. However, the characteristics of the code are now different, i.e. the density decreases but the average degree increases (slightly, depending on m). The binary density of the non-zero $\mathbb{F}_q$-symbols can be determined as $\delta = \frac{2^{m-1}}{2^m - 1}$, i.e. the code with density Δ_q over $\mathbb{F}_q$ has now a density $\Delta_2 = \delta\,\Delta_q$, while the average degree changes from $\bar{\Omega}_q$ to $\bar{\Omega}_2 = m\,\delta\,\bar{\Omega}_q$. Using the binary image of a code over higher order Galois fields makes it possible to use partially received $\mathbb{F}_q$-symbols that contain bit erasures for decoding.

V. Conclusion

We have derived a formula for an upper bound on the symbol erasure probability under ML decoding for LT codes over higher order Galois fields $\mathbb{F}_q$ and have found a simple expression for the special case of random linear fountain (RLF) codes over $\mathbb{F}_q$ which have a density $\Delta = \frac{q-1}{q}$. Since this density is too high for practical implementations, low-density RLF (LDRLF) codes have been taken into consideration. Decreasing the density introduces an error floor, but most practical applications do not need arbitrarily small erasure probabilities. Thus, it is justifiable to decrease the density and thereby also the computational complexity of encoding and especially decoding. Furthermore, the level of the error floor can be controlled by means of the equivalent binary input size k_2 and the average check node degree $\bar{\Omega}$ of the LDRLF code. Referring to other publications, we have shown by a fair comparison that RLF codes over higher order Galois fields actually exhibit a performance gain compared to codes over lower order fields. A brief analysis of computational complexity reveals that the $\mathbb{F}_q$-codes can compete with or even outperform their binary counterparts if optimised Galois field arithmetic is used. Finally, binary images of LT codes over higher order Galois fields are introduced which provide a better decodability of received $\mathbb{F}_q$-symbols in the presence of bit erasures.

Acknowledgments

The first author would like to thank Bernd Geiser for many inspiring discussions.

References

[1] 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, 1998.

[2] 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.

[3] M. Luby, A. Shokrollahi, M. Watson, T. Stockhammer, and L. Minder, "IETF Internet Draft: RaptorQ Forward Error Correction Scheme for Object Delivery," 2011.

[4] QUALCOMM Incorporated, "RaptorQ$^{\text{TM}}$ Technical Overview," 2010. [Online]. Available: www.qualcomm.com/documents/files/raptorqtm-technical-overview.pdf

[5] M. Luby, "LT Codes," in *Proc. 43rd Annual IEEE Symposium on Foundations of Computer Science*, 2002, pp. 271–280.

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

[7] P. Maymounkov, "Online Codes," Secure Computer Systems Group, New York University, Tech. Rep. TR2002-833, Nov. 2002.

[8] D. MacKay, "Fountain Codes," *Communications, IEE Proceedings-*, vol. 152, no. 6, pp. 1062–1068, 2005.

[9] B. Schotsch, H. Schepker, and P. Vary, "The Performance of Short Random Linear Fountain Codes under Maximum Likelihood Decoding," in *IEEE International Conference on Communications (ICC)*, June 2011.

[10] R. Lidl, H. Niederreiter, and P. M. Cohn, *Finite fields*. Cambridge University Press, 1997.

[11] N. Rahnavard and F. Fekri, "Bounds on Maximum-Likelihood Decoding of Finite-Length Rateless Codes," in *Proc. of the 39th Annual Conference on Information Science and Systems (CISS'05)*, March 2005.

[12] R. P. Stanley, *Enumerative Combinatorics*, 2nd ed. Cambridge University Press, 2011, vol. 1, to appear. [Online]. Available: http://math.mit.edu/~rstan/ec/ec1.pdf

[13] K. M. Greenan, E. L. Miller, and T. J. E. Schwarz, "Optimizing Galois Field Arithmetic for Diverse Processor Architectures and Applications," in *IEEE International Symposium on Modeling, Analysis and Simulation of Computers and Telecommunication Systems MASCOTS*, 2008, pp. 1–10.

[14] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*. North-Holland, 1977.

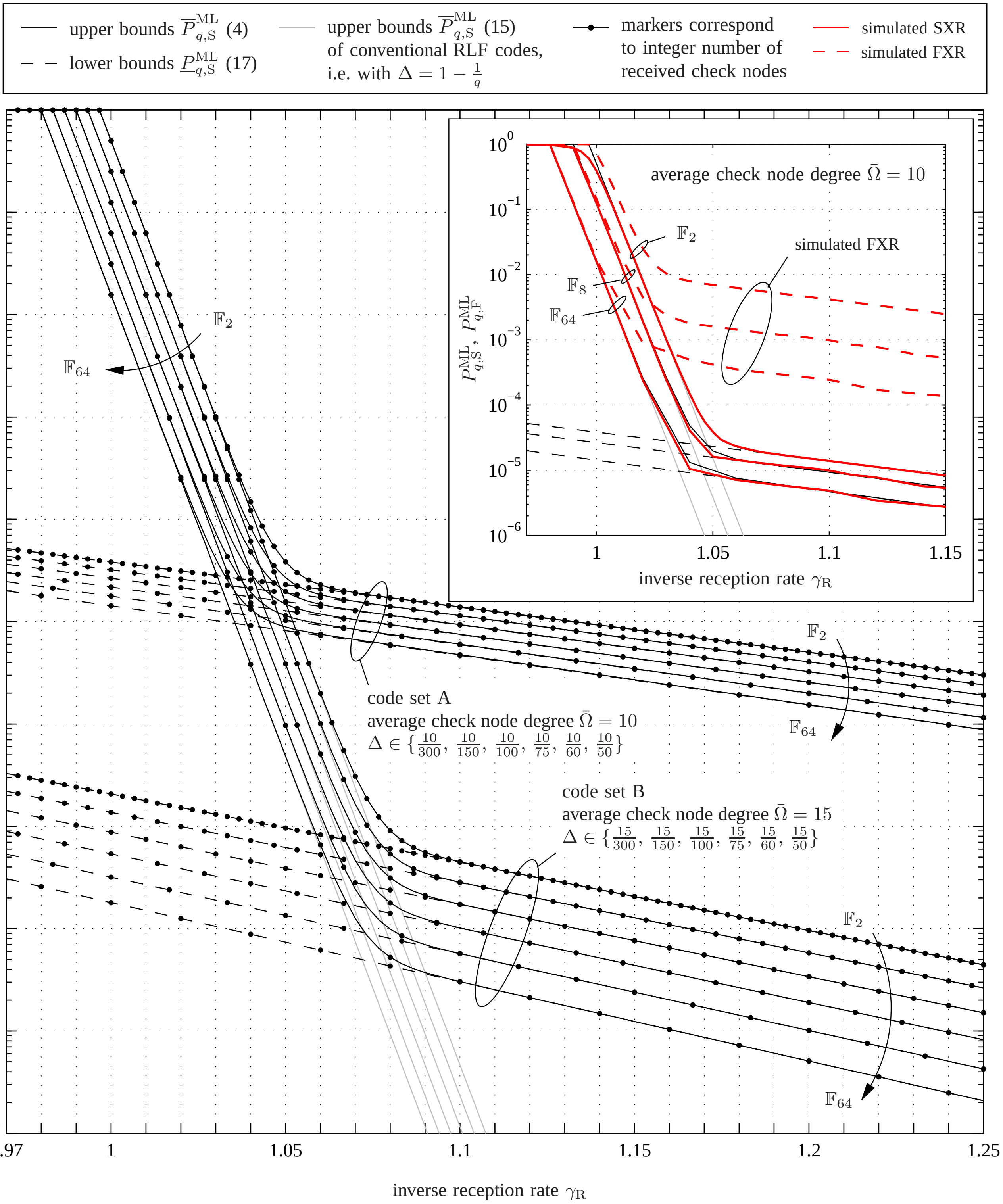


Fig. 4. Upper and lower bounds on the symbol erasure probabilities $P^{\mathrm{ML}}_{q,\mathrm{S}}$ after ML decoding of low-density random linear fountain codes of input sizes $k_q = \frac{300}{\mathrm{ld}\, q} = \frac{300}{m} \in \{300, 150, 100, 75, 60, 50\}$ over Galois fields $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_8$, $\mathbb{F}_{16}$, $\mathbb{F}_{32}$ and $\mathbb{F}_{64}$ with average check node degrees $\bar{\Omega} = 10$ and $\bar{\Omega} = 15$.

Upper right corner: Bounds for LDRLF codes over $\mathbb{F}_2$, $\mathbb{F}_8$ and $\mathbb{F}_{64}$ with $k_2 = 300$, $k_8 = 100$ and $k_{64} = 50$, respectively, for $\bar{\Omega} = 10$ together with corresponding simulated symbol erasure rates (SXR) and frame erasure rates (FXR). The discrete nature of the check nodes becomes visible in the piecewise linear characteristic of the upper bounds and the simulated results, which in the large plot is indicated by the round markers. Additionaly, due to the small deviation of the simulated SXRs from their respective upper bounds, it is justified to describe the codes' performance by means of their upper bounds $\overline{P}^{\mathrm{ML}}_{q,\mathrm{S}}$.