The Performance of Short Random Linear Fountain Codes under Maximum Likelihood Decoding

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

***Abstract*—In this paper, two particular instances of LT codes with short message blocklength k and maximum likelihood (ML) decoding over the binary erasure channel (BEC) are investigated, i.e., random linear fountain (RLF) codes and (nearly) check-concentrated LT codes. Both show an almost equally good performance. The focus of this paper will be on RLF codes, a type of LT codes whose generator matrices are constructed from independent Bernoulli trials and have a binomial check node degree distribution. A new simple expression for an upper bound on the bit erasure probability under ML decoding is derived for RLF codes with density $\Delta = 0.5$, i.e., with check node degree distribution $\Omega(x) = 2^{-k}(1+x)^k$. It is shown that RLF codes with a minimum density far less than 0.5 are equally well suited to achieve a certain bit erasure probability for a given reception overhead. Furthermore, a characteristic term from a general upper bound on the bit erasure probability under ML decoding is identified that can be used to optimise check node degree distributions. Its implications on the performance of LT codes are qualitatively analysed.**

I. Introduction

Fountain codes, also called rateless codes, are a class of 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 assuming any knowledge of the erasure probability ϵ. This feature is useful, e.g., in multicast scenarios, where different users experience different channel conditions and independent losses that are unknown to the transmitter. Using rateless codes, the transmitter is able to produce a potentially infinite number n_T of encoded symbols from a finite amount of k input symbols, consisting of m bits each. Since the size m can be any fixed number of bits and as this size has no influence on the performance of the codes, we will assume $m = 1$ and refer to the input or code symbols as input or code bits, respectively. Good rateless codes have the property that the receiver is able to decode the original k input bits from any $n_\mathrm{R} = k(1+\varepsilon_\mathrm{R})$ received code bits with high probability if the relative reception overhead $\varepsilon_\mathrm{R} \geq 0$. Practical rateless codes are sparse-graph codes, e.g., LT codes [2], Raptor codes [3] or Online codes [4] for which simple and efficient encoding and decoding algorithms exist.

If an application is delay-sensitive, the usage of short codes is mandatory. In this paper, we propose two types of LT codes for short message blocklength, i.e., $k \approx 100$, that show strong error correction properties under maximum likelihood (ML) decoding and that are easy to design. The standard decoding algorithm of LT codes is the computationally cheap, yet sub-optimal, belief propagation (BP) algorithm that performs well on properly designed codes, but only for a large blocklength. 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 codes the decoding cost is $\mathcal{O}(n_\mathrm{R}k)$ per input bit, but it decreases for less dense codes. The density Δ of an LT code is the ratio of the number of ones in the generator matrix to the total number of entries.

II. LT Codes

The generator matrix $\mathbf{G} \in \mathbb{F}_2^{[n_\mathrm{T}\times k]}$ of an LT code defines a graph connecting the set of k input bits to the set of n_T output bits, where n_T can be arbitrarily large. The input bits are associated to input nodes, whereas the output bits are associated to output nodes that are also called check nodes. In vector-matrix notation, encoding is performed by $\mathbf{y}^\mathrm{T} = \mathbf{G}\mathbf{u}^\mathrm{T}$, where $\mathbf{u} \in \mathbb{F}_2^{[1\times k]}$ and $\mathbf{y} \in \mathbb{F}_2^{[1\times n_\mathrm{T}]}$ are the input and output vector. 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 bit to which input bits it is connected, i.e., the matrix $\mathbf{G}$ is known. This can be achieved by synchronising identical pseudo-random processes that produce the underlying generator matrix.

The erasure correcting properties of LT codes are mainly defined by the so-called check node degree distribution $\Omega_0, \Omega_1, \ldots \Omega_k$ on $\{0, 1, \ldots k\}$, 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 input nodes. Typically, the degree distribution is given by its generating polynomial $\Omega(x) = \sum_{d=0}^{k} \Omega_d x^d$. In the generator matrix $\mathbf{G}$ the d ones in a row correspond to the connections of a check node to the d input bits. The encoder produces n_T output bits that are then transmitted over a BEC that randomly erases some of these bits. At the receiver, $n_\mathrm{R} \leq n_\mathrm{T}$ bits are collected from which the decoder tries to reproduce the original k input bits.

Having collected $n_\mathrm{R} \leq n_\mathrm{T}$ output bits, the decoder uses the n_R rows of $\mathbf{G}$ that are associated to the received, i.e, the collected, non-erased bits to make up a new matrix $\mathbf{G}'$ on

*Henning Schepker is now with the Department of Communications Engineering at University of Bremen, Bremen, Germany

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

which decoding is performed. Since $\mathbf{G}'$ consists of a set of n_R rows that is sampled at random from the original matrix $\mathbf{G}$ according to the erasures that occur on the BEC, $\mathbf{G}'$ follows the same degree distribution as $\mathbf{G}$. In this paper, we consider only ML decoding, due to the weak error correction properties of BP decoding for a short blocklength. For a more detailed description of LT codes, we refer the reader to the original paper of Luby [2].

III. Analysis of Random Linear Fountain Codes

So-called random linear fountain (RLF) codes or random LT codes as introduced in [5] and in [3] have the degree distribution $\Omega(x) = 2^{-k}(1+x)^k$. This degree distribution results from setting each entry in the generator matrix $\mathbf{G}$ to 0 or 1 according to the outcome of a Bernoulli trial, where the probability of choosing a 1 is $P_1 = 0.5$. Hence, the probability of generating a row of weight d is $\Omega_d = \binom{k}{d} P_1^d (1-P_1)^{(k-d)} = \binom{k}{d} 2^{-k}$. For arbitrary values of P_1, $0 < P_1 < 1$, RLF codes are characterised by a binomial check node degree distribution $\Omega(x) = \sum_{d=0}^{k} \binom{k}{d} P_1^d (1-P_1)^{(k-d)} x^d$. Therefore, we will synonymously utilise the term binomial $(k,\, P_1)$ LT codes and mark the resulting degree distributions with indices k and P_1, i.e., $\Omega^{[k,\,P_1]}(x)$. The density of RLF codes is $\Delta = P_1$. If setting $\Omega_0 = 0$, a normalisation of the other probabilities for $d > 0$ is necessary, i.e., $\Omega_d = \frac{1}{1-(1-P_1)^k} \binom{k}{d} P_1^d (1-P_1)^{(k-d)}$ in order to obtain $\sum_{d=1}^{k} \Omega_d = 1$. Even though $\Omega_0 = 0$ in practical systems (also in our simulations), we mostly use the unmodified binomial distribution in our analysis for reasons of simplicity and since the induced error is negligible if k or P_1 are not too small. In cases where the effect is not negligible, we also state a result for the modified distribution.

As ML decoding on a BEC is equivalent to solving a system of n_R linear equations in k unknowns, the probability that the system is solvable equals the probability that the matrix $\mathbf{G}'$ at the receiver has rank k. Hence, the frame erasure probability P_f^ML after ML decoding equals the probability that $\mathbf{G}'$ has not rank k. As shown in [5] and [3], an upper bound on P_f^ML is[1]

$$\overline{P}_\mathrm{f}^\mathrm{ML} = 2^{k-n_\mathrm{R}} = 2^{-\eta} \tag{1}$$

for a binomial $(k,\, 0.5)$ LT code, where $\eta = k\varepsilon_\mathrm{R}$ is the absolute reception overhead. The corresponding bit erasure probability P_b^ML is at most $\overline{P}_\mathrm{b}^\mathrm{ML} = 2^{-(\eta+1)}$ as will be shown in the following. As a basis we require Lemma 1 from [6] of which we will also restate the proof for a better understanding:

Lemma 1. *[6] For general LT codes of length k, with check node degree distribution $\Omega(x)$ and the inverse reception rate $\gamma_R = 1 + \varepsilon_R$, an upper bound on P_b^{ML} is*

$$\overline{P}_b^{ML} = \sum_{w=1}^{k} \binom{k-1}{w-1} \cdot \left[\sum_d \Omega_d \frac{\sum_{s=0,2,\ldots,2\left\lfloor \frac{d}{2} \right\rfloor} \binom{w}{s}\binom{k-w}{d-s}}{\binom{k}{d}} \right]^{k\gamma_R}. \tag{2}$$

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

Proof: The probability P_b^ML is equal to the probability that the ith bit cannot be determined by ML decoding for an arbitrary $i \in \{1,\, 2, \ldots k\}$

$$P_\mathrm{b}^\mathrm{ML} = \Pr\left\{ \exists \mathbf{x} \in \mathbb{F}_2^{[1\times k]},\, x_i = 1 :\ \mathbf{G}'\mathbf{x}^\mathrm{T} = \mathbf{0}^\mathrm{T} \right\} \tag{3}$$

$$\leq \sum_{\substack{\mathbf{x}\in\mathbb{F}_2^{[1\times k]},\\ x_i=1}} \Pr\left\{ \mathbf{G}'\mathbf{x}^\mathrm{T} = \mathbf{0}^\mathrm{T} \right\}. \tag{4}$$

The right-hand side of (3) is the probability of the ith column of matrix $\mathbf{G}'$ being linearly dependent on a non-empty set of columns, whereas the right-hand side of (4) is the probability of any possible set of columns of $\mathbf{G}'$ being linearly dependent on column i. The $k\gamma_\mathrm{R}$ rows of $\mathbf{G}'$ can be viewed as the outcomes of independent trials of a random variable $\mathbf{r} \in \mathbb{F}_2^{[1\times k]}$.

$$\Pr\left\{ \mathbf{G}'\mathbf{x}^\mathrm{T} = \mathbf{0}^\mathrm{T} \right\} = \left[\Pr\left\{ \mathbf{r}\mathbf{x}^\mathrm{T} = 0 \right\} \right]^{k\gamma_\mathrm{R}} \tag{5}$$

The weight of a binary vector is denoted $|\cdot|$. A row has weight $|\mathbf{r}| = d$ with probability Ω_d. The inner product $\mathbf{r}\mathbf{x}^\mathrm{T}$ amounts to zero, iff an even number of the k addends $r_i x_i$ are equal to one, where r_i and x_i are the ith elements of the binary vectors $\mathbf{r}$ and $\mathbf{x}$, respectively. Let $\mathbf{v} = (r_1 x_1,\, r_2 x_2, \ldots,\, r_k x_k)$, then

$$\begin{aligned} \Pr\left\{ \mathbf{r}\mathbf{x}^\mathrm{T} = 0 \,\middle|\, |\mathbf{r}| = d,\ |\mathbf{x}| = w \right\} &= \Pr\left\{ |\mathbf{v}| \ \text{ even} \,\middle|\, |\mathbf{r}| = d,\ |\mathbf{x}| = w \right\} \\ &= \frac{\sum_{s=0,2,\ldots,2\left\lfloor \frac{d}{2} \right\rfloor} \binom{w}{s}\binom{k-w}{d-s}}{\binom{k}{d}}. \end{aligned} \tag{6}$$

Weighting the term in (6) with degree distribution $\Omega(x)$, inserting it into (5) and marginalising over all $\binom{k-1}{w-1}$ choices of $\mathbf{x}$ of weight w with $x_i = 1$ concludes the assertion. □

Based on Lemma 1, we show next that for binomial $(k,\, 0.5)$ LT codes the upper bound in (2) reduces to $\overline{P}_\mathrm{b}^\mathrm{ML} = 2^{-(\eta+1)}$:

Lemma 2. *Given a binomial $(k,\, 0.5)$ LT code, i.e., with the degree distribution $\Omega^{[k,\,0.5]}(x) = 2^{-k} \sum_{d=0}^{k} \binom{k}{d} x^d$, and the absolute reception overhead $\eta = n_R - k = (\gamma_R - 1)k$, an upper bound on the bit erasure probability P_b^{ML} after ML decoding is $\overline{P}_b^{ML} = 2^{-(\eta+1)}$ for $\eta \geq 0$.*

Proof: The coefficients of $\Omega^{[k,\,0.5]}(x)$ are inserted into (2).

$$\overline{P}_\mathrm{b}^\mathrm{ML} = \sum_{w=1}^{k} \binom{k-1}{w-1} \Bigg[2^{-k} \underbrace{\sum_{d=0}^{k} \sum_{s=0,2,\ldots,2\left\lfloor \frac{d}{2} \right\rfloor} \binom{w}{s}\binom{k-w}{d-s}}_{\Gamma(k)} \Bigg]^{k\gamma_\mathrm{R}}$$

The upper limit of the inner summation in $\Gamma(k)$ is changed from $2\left\lfloor \frac{d}{2} \right\rfloor$ to $2\left\lfloor \frac{k}{2} \right\rfloor$ without affecting the result, since[2] the terms with $s > 2\left\lfloor \frac{d}{2} \right\rfloor$ amount to 0. The inner summation variable s is now independent of the outer summation variable d and thus the order of the two summations can be exchanged:

$$\Gamma(k) = \sum_{s=0,2,\ldots,2\left\lfloor \frac{k}{2} \right\rfloor} \binom{w}{s} \sum_{d=0}^{k} \binom{k-w}{d-s}.$$

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

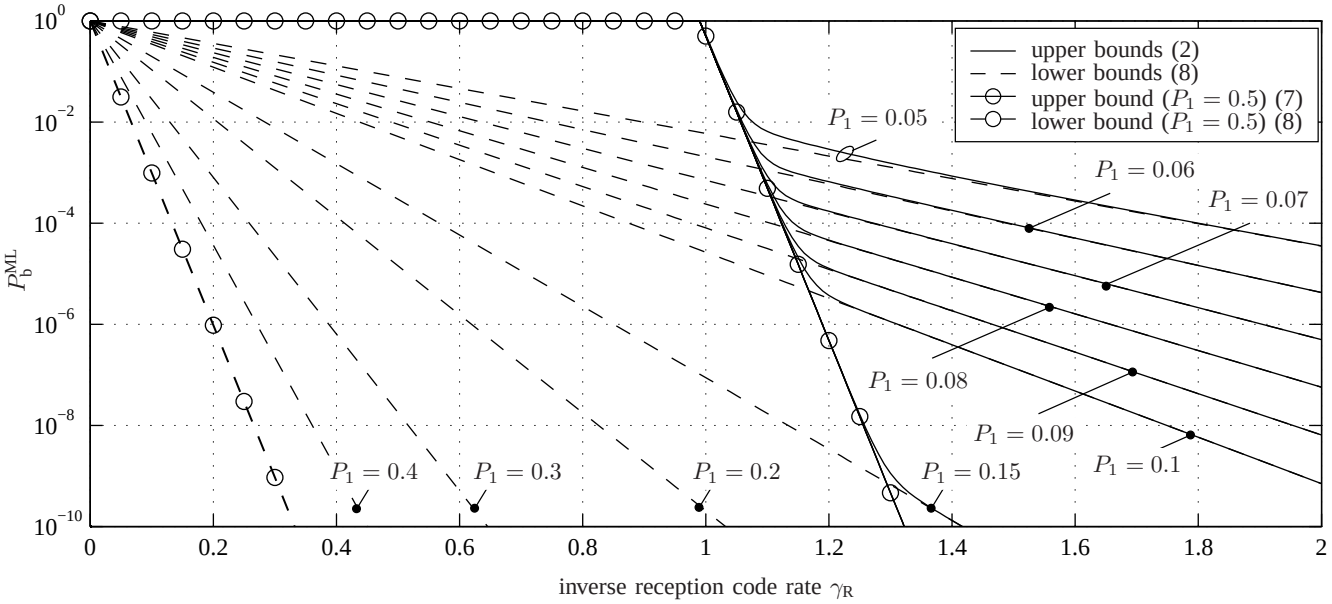


Fig. 1. Upper and lower bounds on the bit erasure probability P_b^ML after ML decoding of random linear fountain codes of blocklength $k = 100$.

The term $\binom{w}{s}$ restricts s to $0 \le s \le w$, such that

$$\sum_{d=0}^{k} \binom{k-w}{d-s} = \sum_{d=s}^{k-w+s} \binom{k-w}{d-s} = \sum_{d=0}^{k-w} \binom{k-w}{d} = 2^{k-w}.$$

Combining this term with the last expression for $\Gamma(k)$ yields

$$\Gamma(k) = 2^{k-w} \cdot \sum_{s=0,2,\ldots,2\left\lfloor \frac{k}{2} \right\rfloor} \binom{w}{s} = 2^{k-w} 2^{w-1} = 2^{k-1},$$

where we have used the identity $\sum_{\sigma \text{ even}} \binom{\omega}{\sigma} = 2^{\omega-1}$. With $\Gamma(k) = 2^{k-1}$ we now obtain

$$\begin{aligned} \overline{P}_\mathrm{b}^\mathrm{ML} &= \sum_{w=1}^{k} \binom{k-1}{w-1} \left[2^{-k}\Gamma(k)\right]^{k\gamma_\mathrm{R}} = 2^{-k\gamma_\mathrm{R}} \sum_{w=1}^{k} \binom{k-1}{w-1} \\ &= 2^{-k\gamma_\mathrm{R}} \sum_{w=0}^{k-1} \binom{k-1}{w} = 2^{-k\gamma_\mathrm{R}} 2^{k-1} = 2^{-(k(\gamma_\mathrm{R}-1)+1)} \\ &= 2^{-(\eta+1)}. \end{aligned} \tag{7}$$

□

Due to the high density ($\Delta = P_1 = 0.5$) of $\mathbf{G}'$, this remarkable exponentially decreasing decoding erasure probability has a rather high encoding and an even higher decoding cost. The encoding cost in general is proportional to the average check node degree $\bar{\Omega} = \sum_{d=1}^{k} d\Omega_d$, which amounts to $k/2$ in the case of binomial $(k,\, 0.5)$ LT codes, the cost of ML decoding using Gaussian elimination is $\mathcal{O}(n_\mathrm{R}k)$ per input bit. Thus, these costs are only affordable for a short blocklength. This is a motivation to examine the performance of binomial $(k,\, P_1)$ LT codes with $P_1 < 0.5$, such that the generator matrix is not so dense or even sparse.

In Fig. 1 the upper and lower bounds on P_b^ML are depicted for RLF codes of an exemplary blocklength $k = 100$ with different values[3] of P_1. The upper bounds are according to (2), simplified to (7) for $P_1 = 0.5$. Since the upper bound is very tight for RLF codes, as the simulation results at the end of the paper will show, it is well suited to compare RLF codes with different parameters. A lower bound on P_b^ML is given by the probability that an input node is not connected to any check node. According to [3] this lower bound is

$$\underline{P}_\mathrm{b}^\mathrm{ML} = \left(1 - \frac{\bar{\Omega}}{k}\right)^{k\gamma_\mathrm{R}}. \tag{8}$$

For RLF codes with $\Omega^{[k,\,P_1]}(x)$ this lower bound can be easily expressed in terms of P_1

$$\underline{P}_\mathrm{b}^\mathrm{ML} = (1 - P_1)^{k\gamma_\mathrm{R}}.$$

Using the modified binomial distribution, i.e, $\Omega_0 = 0$, the average check node degree is $\bar{\Omega} = \frac{kP_1}{1-(1-P_1)^k}$ and thus

$$\underline{P}_\mathrm{b}^\mathrm{ML} = \left(1 - \frac{P_1}{1-(1-P_1)^k}\right)^{k\gamma_\mathrm{R}}.$$

All lower bounds and the upper bound for $P_1 = 0.5$ that are depicted in Fig. 1 are straight lines in the semi-logarithmic plot. Except for the case $P_1 = 0.5$, the upper and lower bound pairs converge for increasing γ_R. For $\gamma_\mathrm{R} \ge 1$, all upper bounds for $P_1^* < 0.5$ follow initially the steep descent of the upper bound for $P_1 = 0.5$. An RLF code with P_1^* performs in its steep region as well as the code with $P_1 = 0.5$. The simple upper bound for $P_1 = 0.5$ can therefore be used to approximate the behavior in the steep region. Close to the intersection of the upper bound for $P_1 = 0.5$ with the lower bound for $P_1^* < 0.5$, the upper bound for P_1^* diverges from the upper bound for $P_1 = 0.5$ and converges to the corresponding lower bound for P_1^*. For higher γ_R, the upper bound for P_1^*

[3]Only $P_1 \le 0.5$ is considered. Values of $P_1 > 0.5$ just increase the complexity without improving the error correction properties.

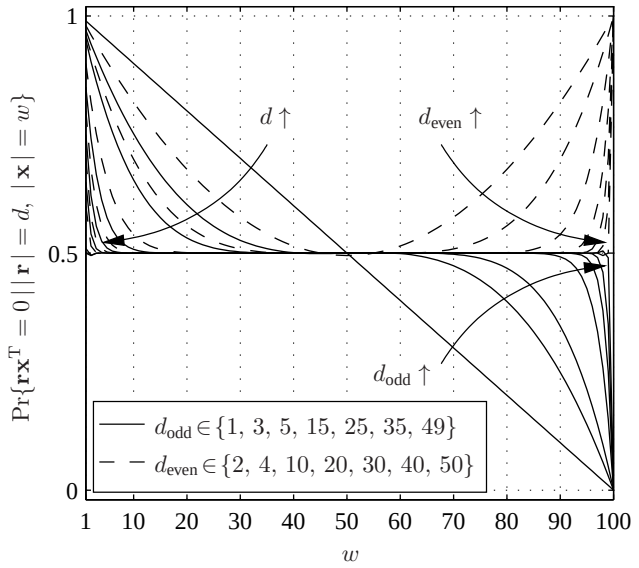


Fig. 2. $\Pr\left\{\mathbf{r}\mathbf{x}^{\mathrm{T}} = 0 \,\middle|\, |\mathbf{r}| = d,\ |\mathbf{x}| = w\right\}$ for $k = 100$ and $d \leq \frac{k}{2}$.

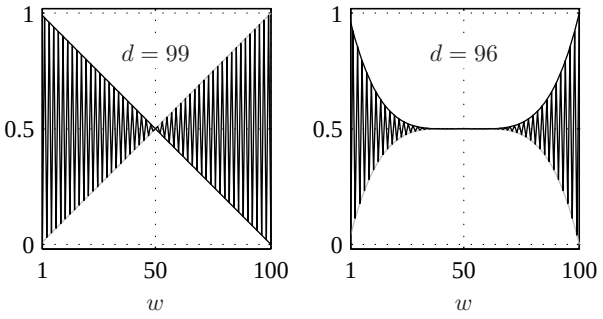


Fig. 3. $\Pr\left\{\mathbf{r}\mathbf{x}^{\mathrm{T}} = 0 \,\middle|\, |\mathbf{r}| = d,\ |\mathbf{x}| = w\right\}$ for $k = 100$ and $d > \frac{k}{2}$.

can be approximated by the corresponding lower bound. The slope of $\underline{P}_{\mathrm{b}}^{\mathrm{ML}}$ depends on $\bar{\Omega}$ or on P_1, respectively. The two linear (in log-domain) functions (7) and (8) can be used to design the steep as well as the shallow region of an RLF code. The parameters $\bar{\Omega}$ or P_1, respectively, define the beginning of the shallow region and also its slope, i.e., a high value of $\bar{\Omega}$ or P_1 leads to a low bit erasure probability $P_{\mathrm{b}}^{\mathrm{ML}}$ at a low relative reception overhead $\varepsilon_{\mathrm{R}} = \gamma_{\mathrm{R}} - 1$.

In the following, we will point out some aspects of the upper bound given in (2) that lead to good ML decoding properties of a code for an arbitrary but fixed blocklength k. For successful decoding with arbitrary high reception overhead, the term in square brackets from (2), i.e., $\Pr\{\mathbf{r}\mathbf{x}^{\mathrm{T}} = 0 \,|\, |\mathbf{x}| = w\}$ has to be strictly less than 1, the smaller it is the less overhead is required for $\overline{P}_{\mathrm{b}}^{\mathrm{ML}}$ to drop below a certain value, since this term is raised to the power of $k\gamma_{\mathrm{R}} = k(1+\varepsilon_{\mathrm{R}})$. The aforementioned term in (2) corresponds to the expression in (6) weighted with some distribution $\Omega(x)$. In order to be able to assess the contribution of (6) for all values of w and d, this term is depicted in Figs. 2 and 3 as a function of w for some degrees d. For increasing values of d, $d \leq k/2$ the graphs become flatter for w close to $k/2$. On the left $(w = 1)$, all characteristics stay below 1, while on the right $(w = k)$ the characteristics of the even degrees attain an ordinate-value of

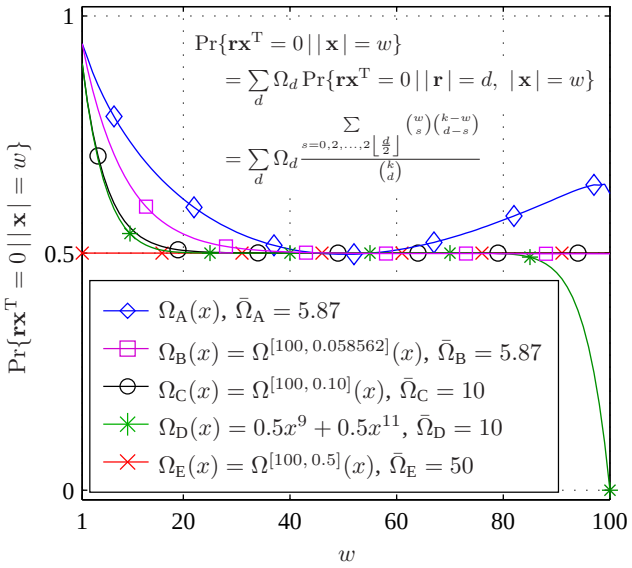
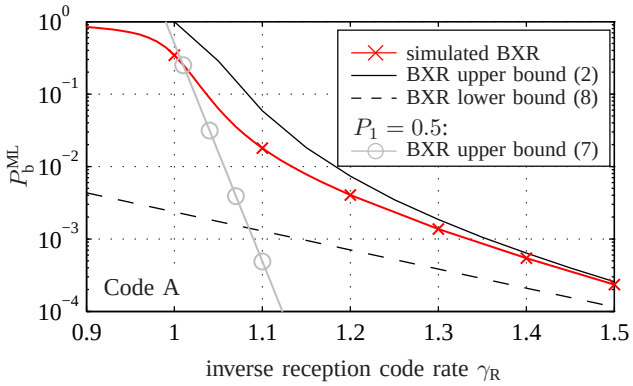


Fig. 4. $\Pr\left\{\mathbf{r}\mathbf{x}^{\mathrm{T}} = 0 \,\middle|\, |\mathbf{x}| = w\right\}$ for $k = 100$ and various check node degree distributions. Codes B, C, E are RLF codes with $\Omega^{[k,\, P_1]}(x)$.

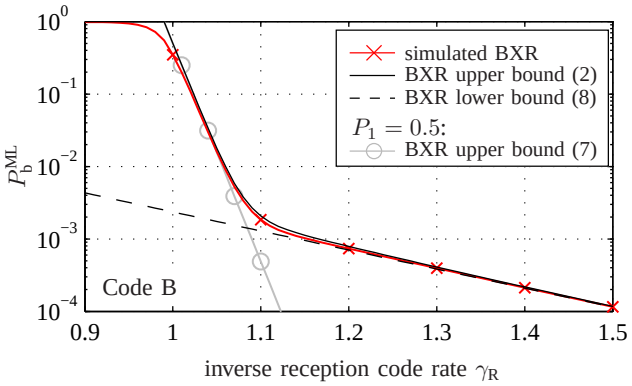
1. From the latter fact it becomes obvious, that a system of linear equations consisting only of rows of even degree cannot be solved. If $d > k/2$, the characteristics alternate between the characteristic of $d^* = k - d$ and the horizontally mirrored version thereof as can be seen in Fig. 3. A good degree distribution is one that weights these characteristics such that the sum is minimised especially for w close to $k/2$, since these resulting values are exponentiated by $k\gamma_{\mathrm{R}}$ and are then multiplied by $\binom{k-1}{w-1}$. The latter operation amplifies especially the values for w close to $k/2$. A good resulting characteristic is thus flat for w close to $k/2$ and attains a value very close or equal to 0.5.

Figure 4 depicts the resulting term $\Pr\{\mathbf{r}\mathbf{x}^{\mathrm{T}} = 0 \,|\, |\mathbf{x}| = w\}$ that is obtained by weighting (6) with different degree distributions $\Omega_{\mathrm{A}}(x)$ to $\Omega_{\mathrm{E}}(x)$. The distribution $\Omega_{\mathrm{A}}(x) = 0.007969x + 0.49357x^2 + 0.16622x^3 + 0.072646x^4 + 0.082558x^5 + 0.056058x^8 + 0.037229x^9 + 0.05559x^{19} + 0.025023x^{65} + 0.003135x^{66}$ is taken from [3] and has been optimised for BP decoding. $\Omega_{\mathrm{B}}(x)$ is the distribution of an RLF code with modified P_1 such that $\bar{\Omega}_{\mathrm{B}} = \bar{\Omega}_{\mathrm{A}}$. The characteristic of code B is much flatter and closer to 0.5 for w near $k/2$ which leads to a better upper bound. The simulated bit erasure rates (BXR) are plotted in Figs. 5(a) and 5(b). The BXR of code B approaches its upper bound closely and both converge to the corresponding lower bound at relatively low overheads, while $\overline{P}_{\mathrm{b}}^{\mathrm{ML}}$ of code A is not that tight. Furthermore, the convergence to the lower bound as well as the BXR is worse than of code B.

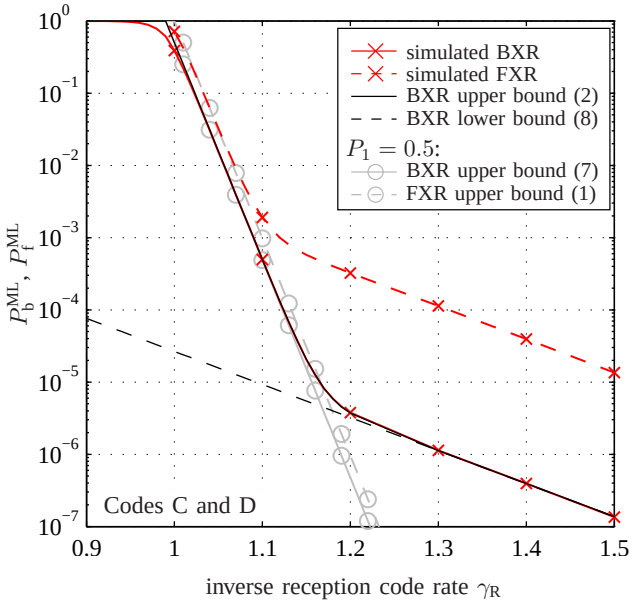
Code C is an RLF code with $\bar{\Omega}_{\mathrm{C}} = 10$, while code D is nearly check-concentrated, i.e., it has only degrees close to its average degree. Degrees of 10 are spared out, as a degree distribution with a high probability of even degrees leads to a high probability of producing rank deficient matrices. For simplicity, we have constructed $\bar{\Omega}_{\mathrm{D}} = 10$ from the two neighboring odd degrees 9 and 11. The characteristics of these two codes in Fig. 4 are flat and undistinguishable for medium



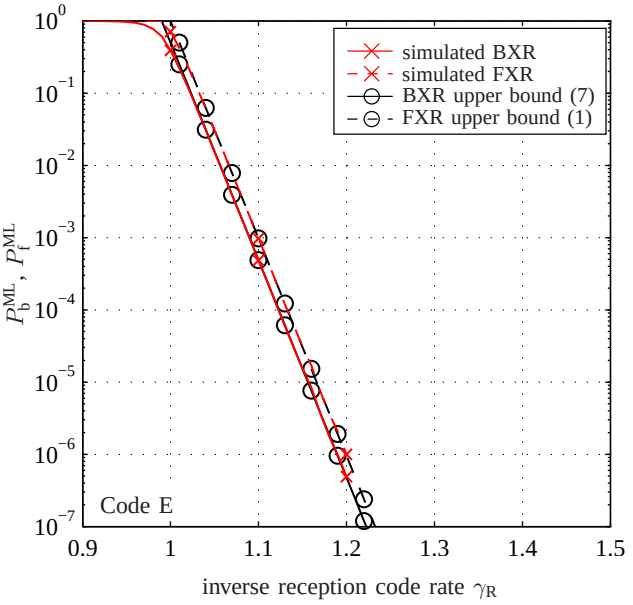
(a) $\Omega_A(x)$, $\bar{\Omega}_A = 5.87$.



(b) $\Omega_B(x) = \Omega^{[100,\,0.058562]}(x)$, $\bar{\Omega}_B = 5.87$.



(c) $\Omega_C(x) = \Omega^{[100,\,0.10]}(x)$ and $\Omega_D(x) = 0.5x^9 + 0.5x^{11}$, $\bar{\Omega}_C = \bar{\Omega}_D = 10$.



(d) $\Omega_E(x) = \Omega^{[100,\,0.5]}(x)$, $\bar{\Omega}_E = 50$

Fig. 5. Bit erasure rates (BXR) and frame erasure rates (FXR) of LT codes of blocklength $k = 100$ with different degree distributions.

values of w and differ for small and large values of w. Despite the latter differences, the BXR as well as the frame erasure rates (FXR) of the two codes are so similar that they are undistinguishable in Fig. 5(c).

Code E is the binomial $(k,\, 0.5)$ LT code with $\Omega^{[100,\,0.5]}(x)$ whose characteristic in Fig. 4 is totally flat and equals $0.5\ \forall w$. The simulation results in Fig. 5(d) illustrate the fast convergence of the simulation results to the respective bounds and the remarkable performance.

The flatness of the characteristics in Fig. 4 shows to be a good measure for the performance of the codes A to E. It may be useful to optimise degree distributions for ML decoding.

IV. Conclusion

We have analysed random linear fountain (RLF) codes and (nearly) check-concentrated LT codes that perform undistinguishably well under ML decoding if the average check node degree is equal. These two classes of codes show a very good ML decoding performance even at short blocklength and for a minimum density Δ far less than 0.5, while the encoding and decoding complexity still remains manageable. A simple expression for a tight upper bound on the bit erasure probability has been derived for RLF codes with $\Delta = P_1 = 0.5$ and a term from the general upper bound has been identified as a characteristic of the performance of LT codes. This characteristic may prove useful to optimise degree distributions for LT codes under ML decoding.

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

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

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

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

[6] 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.