Necessary field size and probability for MDP and complete MDP convolutional codes

Julia Lieb

Abstract
It has been shown that maximum distance profile (MDP) convolutional codes have optimal recovery rate for windows of a certain length, when transmitting over an erasure channel. In addition, the subclass of complete MDP convolutional codes has the ability to reduce the waiting time during decoding. Since so far general constructions of these codes have only been provided over fields of very large size, there arises the question about the necessary field size such that these codes could exist. In this paper, we derive upper bounds on the necessary field size for the existence of MDP and complete MDP convolutional codes and show that these bounds improve the already existing ones. For some special choices of the code parameters, we are even able to give the exact minimum field size. Moreover, we derive lower bounds for the probability that a random code is MDP respective complete MDP.

Keywords Convolutional codes · Maximum distance profile · Superregular matrices · Finite fields

Mathematics Subject Classification 94B10

1 Introduction
Convolutional codes play an important role for digital communication. These codes are a generalization of the classical block codes and when considering sliding window decoding over an erasure channel, which is the most used channel in multimedia traffic, they can in many cases correct more erasures than block codes; see [15].

Besides the classical free distance, convolutional codes possess a different notion of distance, called column distance. The column distances of a convolutional code are limited by an upper bound, which was proven in [13]. Convolutional codes attaining these bounds, i.e. convolutional codes whose column distances increase as rapidly as possible for as long as possible are called maximum distance profile (MDP) codes. These codes were introduced...
in [4] and are especially suitable for the use in sequential decoding algorithms. In [15], the authors showed that MDP convolutional codes can correct the maximum possible number of errors in some sliding window of a certain length (depending on the code parameters). Moreover, they considered reverse MDP convolutional codes, which have the advantage that optimal error correction is possible with forward and backward decoding algorithms. Finally, complete MDP convolutional codes, which are again a subclass of reverse MDP convolutional codes, have the additional benefit that they can correct even more error patterns than reverse MDP convolution codes, e.g. there is less waiting time when a large burst of erasures occurs and no correction is possible for some time [15].

The existence (and genericity) of reverse MDP convolutional codes for all code parameters has been proven in [15]. In [8], it has been shown that for the existence of a complete MDP convolutional code with rate \( k/n \) and degree \( \delta \), it is necessary to have \( (n - k) \mid \delta \) and that complete MDP convolutional codes exist (and are generic) for all code parameters fulfilling this condition. The case \( (n - k) \nmid \delta \), in which a complete MDP convolutional code cannot exist, is also much more involved when considering just MDP convolutional codes, see [11]. There are some general constructions for MDP [2,4] and complete MDP [8] convolutional codes. However, all of these constructions have the disadvantage that they only work over base fields of very large size. This is especially unfavourable as decoding of convolutional codes over the erasure channel could be basically done using only simple linear algebra [15], but this is infeasible with too big field sizes.

This provokes the question for the minimal field size such that an MDP respective complete MDP convolutional code could exist. For the case of MDP convolutional codes, there is something done to solve this problem in [7], where the authors provide an upper bound on the necessary field size. In [7] as well as in [4], where an - until now unproven - conjecture about a bound on the necessary field size is raised, superregular Toeplitz matrices are used, i.e. the question is connected to the problem of determining the necessary field size for the existence of such superregular Toeplitz matrices. In this paper, we improve these bounds by other means than using superregular Toeplitz matrices. For complete MDP convolutional codes, the so far only result on the necessary field size could be derived from the constructions in [8] but this is leading to very weak bounds. In this paper, we also present bounds for the necessary field size for complete MDP convolutional codes.

Since constructions - especially over fields of possibly small size - have been found to be very hard to obtain, it is an interesting question, how large the probability for an MDP respective complete MDP convolutional code is, when choosing the code randomly. In this paper, we give lower bounds for this probability for MDP as well as for complete MDP convolutional codes.

The paper is structured as follows. In Sect. 2, we start with some preliminaries about MDP convolutional codes. In Sect. 3, we consider convolutional codes of high rates \( (n - 1)/n \). First we give the exact minimum field size for \((n, 1, 1)\) and \((n, n - 1, 1)\) MDP, reverse MDP and complete MDP convolutional codes as well as the corresponding probabilities, then we present what is known about the necessary field size for \((n, n - 1, 2)\) MDP convolutional codes and finally, we show with the help of tables of examples that former bounds on the field size for \((n, n - 1, \delta)\) MDP convolutional codes lead to incredibly big field sizes, which we will improve in the further sections. In Sect. 4, we show upper bounds for the necessary field size for MDP convolutional codes and lower bounds for the probability that a convolutional code is MDP. In Sect. 5, we generalize the results of Sect. 4 to complete MDP convolutional codes. Section 6 provides an improved bound on the field size for MDP convolutional codes in the case \( \delta < \max\{k, n - k\} \). In Sect. 7, we show that except for very few choices of (small) parameters, the new bounds for the field size of this paper are better than all bounds existing up to now.
2 MDP convolutional codes

In this section, we summarize the basic definitions and properties concerning MDP convolutional codes. One way to define a convolutional code is via polynomial generator matrices.

Definition 1 A convolutional code \( \mathcal{C} \) of rate \( k/n \) is a free \( \mathbb{F}[z] \)-submodule of \( \mathbb{F}[z]^n \) of rank \( k \). There exists \( G(z) \in \mathbb{F}[z]^{n \times k} \) of full column rank such that

\[
\mathcal{C} = \{ v(z) \in \mathbb{F}[z]^n \mid v(z) = G(z)m(z) \text{ for some } m(z) \in \mathbb{F}[z]^k \}.
\]

\( G(z) \) is called a generator matrix of the code and is unique up to right multiplication with a unimodular matrix \( U(z) \in \text{GL}_k(\mathbb{F}[z]) \).

The degree \( \delta \) of \( \mathcal{C} \) is defined as the maximal degree of the \( k \times k \)-minors of \( G(z) \). Let \( \delta_1, \ldots, \delta_k \) be the column degrees of \( G(z) \). Then, \( \delta = \delta_1 + \cdots + \delta_k \) and if \( \delta = \delta_1 + \cdots + \delta_k \), \( G(z) \) is called a minimal generator matrix and \( \max_{i \in \{1, \ldots, n\}} \delta_i \) is the memory of \( \mathcal{C} \).

We refer to a convolutional code with rate \( k/n \) and degree \( \delta \) as \((n, k, \delta)\) convolutional code.

There is a generic subclass of convolutional codes that could not only be described by an image representation via generator matrices but also by a kernel representation via the so-called parity-check matrices, which will be introduced in the following. Therefore, we need the notion of right prime and left prime polynomial matrices.

Definition 2 Let \( \overline{\mathbb{F}} \) denote the algebraic closure of \( \mathbb{F} \). A polynomial matrix \( G(z) \in \mathbb{F}[z]^{n \times k} \) with \( k < n \) is called right prime if it has full column rank for all \( z \in \overline{\mathbb{F}} \). For \( k > n \), it is called left prime if it has full row rank for all \( z \in \overline{\mathbb{F}} \).

Definition 3 A convolutional code \( \mathcal{C} \) is called non-catastrophic if one and therefore, each of its generator matrices is right prime.

Definition 4 If \( \mathcal{C} \) is non-catastrophic, there exists a so-called parity-check matrix \( H(z) \in \mathbb{F}[z]^{(n-k) \times n} \) of full rank, such that

\[
\mathcal{C} = \{ v(z) \in \mathbb{F}[z]^n \mid H(z)v(z) = 0 \in \mathbb{F}[z]^{n-k} \}.
\]

Clearly, a parity-check matrix of \( \mathcal{C} \) is not unique and it is possible to choose it left prime and row proper. In this case, the sum of the row degrees of \( H(z) \) is equal to the degree \( \delta \) of \( \mathcal{C} \) [12].

\( H(z) \) has generic row degrees if \( v = \left[ \frac{\delta}{n-k} \right] \) and the first \( \delta - (n-k)(v-1) \) row degrees of \( H(z) \) are equal to \( v \) and the remaining \( (n-k)v - \delta \) row degrees are equal to \( v - 1 \).

Throughout this paper we assume all convolutional codes to be non-catastrophic.

Definition 5 Let \( \mathcal{C} \) be an \((n, k, \delta)\) convolutional code with generator matrix \( G \in \mathbb{F}[z]^{n \times k} \) and parity-check matrix \( H \in \mathbb{F}[z]^{(n-k) \times n} \). The dual code is defined as \( \mathcal{C}^\perp := \{ w \in \mathbb{F}[z]^n \mid wv^\top = 0 \text{ for all } v \in \mathcal{C} \} \). It holds that \( H \) is a generator matrix of \( \mathcal{C}^\perp \) and \( G \) is a parity-check matrix of \( \mathcal{C}^\perp \) and hence \( \mathcal{C}^\perp \) is an \((n, n-k, \delta)\) convolutional code.

Remark 1 Allowing permutation of the entries of the codeword \( v(z) \) respective of the columns of the parity-check matrix \( H(z) \), each non-catastrophic convolutional code has a unique parity-check-matrix of the form \( H(z) = [P(z) \; Q(z)] \), where \( P \) and \( Q \) are left coprime, \( Q \) is of Kronecker-Hermite form, i.e., \( q_{ii} \) is monic, \( \deg(q_{ji}) < \deg(q_{ii}) \) for \( j \neq i \), \( \deg(q_{ii}) < \deg(q_{ij}) \) for \( j < i \) and \( \deg(q_{ji}) \leq \deg(q_{ii}) \) for \( j > i \), and the row degrees of \( P \) are at most equal to the row degrees of \( Q \).

Springer
We will need the representation by parity-check matrices to define complete MDP convolutional codes. But first of all, we want to introduce MDP convolutional codes, for which we have to consider distances of convolutional codes.

**Definition 6** The **Hamming weight** \(\text{wt}(v)\) of \(v \in \mathbb{F}^n\) is defined as the number of its nonzero components. For \(v(z) \in \mathbb{F}[z]^n\) with \(\deg(v(z)) = \gamma\), write \(v(z) = v_0 + \cdots + v_{\gamma}z^\gamma\) with \(v_t \in \mathbb{F}^n\) for \(t = 0, \ldots, \gamma\) and set \(v_t = 0 \in \mathbb{F}^n\) for \(t \geq \gamma + 1\). Then, for \(j \in \mathbb{N}_0\), the **\(j\)-th column distance** of a convolutional code \(C\) is defined as

\[
d_{cj}(C) := \min_{v(z) \in C} \left\{ \sum_{i=0}^{j} \text{wt}(v_t) \mid v_0 \neq 0 \right\}.
\]

Moreover, \(d_{\text{free}}(C) := \min_{v(z) \in C} \left\{ \sum_{i=0}^{\deg(v(z))} \text{wt}(v_t) \mid v(z) \neq 0 \right\}\) is called the **free distance** of \(C\). It holds \(d_{\text{free}}(C) = \lim_{j \to \infty} d_{cj}(C)\).

There exist upper bounds for the free distance and for the column distances of a convolutional code.

**Theorem 1** [4,13] Let \(C\) be a convolutional code with rate \(k/n\) and degree \(\delta\). Then, it holds:

(a) \(d_{cj}(C) \leq (n-k)(j+1) + 1\) for \(j \in \mathbb{N}_0\)
(b) \(d_{\text{free}} \leq (n-k) \left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1\) (generalized Singleton bound)

We are interested in convolutional codes whose column distances increase as rapidly as possible for as long as possible, i.e. which reach the bounds of part (a) of the preceding theorem for \(j = 0, \ldots, L\), where \(L\) should be as large as possible. Due to the generalized Singleton bound, one knows \(L \leq \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor\).

**Definition 7** [6] A convolutional code \(C\) of rate \(k/n\) and degree \(\delta\) has **maximum distance profile** (MDP) if

\[
d_{cj}(C) = (n-k)(j+1) + 1 \quad \text{for} \quad j = 0, \ldots, L := \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor
\]

According to [4], it is sufficient to have equality for \(j = L\) in Theorem 1 to get an MDP convolutional code.

In the following, we will provide criteria to check whether a convolutional code has a maximum distance profile. Therefore, we need the notion of trivially zero determinants.

**Definition 8** (i) Let \(n \in \mathbb{N}\) and \(A \in \mathbb{F}^{n \times n}\) be a matrix with the property that each of its entries is either fixed to zero or is a free variable from \(\mathbb{F}\). Its determinant \(\det(A)\) is called **trivially zero** if it is zero for all choices for the free variables in \(A\).

(ii) An \(n \times n\) Toeplitz matrix of the form

\[
\begin{pmatrix}
a_1 & 0 \\
\vdots & \ddots \\
a_n & \ldots & a_1
\end{pmatrix}
\]

minors that are not trivially zero are nonzero.

**Theorem 2** [4] Let the \((n,k,\delta)\) convolutional code \(C\) be generated by a right prime minimal polynomial matrix \(G(z) = \sum_{i=0}^{\mu} G_i z^i \in \mathbb{F}[z]^{n \times k}\) and have the left prime and row proper parity-check matrix \(H(z) = \sum_{i=0}^{\nu} H_i z^i \in \mathbb{F}[z]^{(n-k) \times n}\). As before set \(L := \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor\). The following statements are equivalent:
(a) $\mathcal{C}$ is a maximum distance profile convolutional code.

(b) $G_L := \begin{bmatrix} G_0 & 0 \\ \vdots & \ddots \\ G_L & \ldots & G_0 \end{bmatrix}$, where $G_i = 0$ for $i > \mu$, has the property that every full size minor that is not trivially zero, i.e. zero for all choices of $G_1, \ldots, G_L$, is nonzero.

(c) $H_L := \begin{bmatrix} H_0 & 0 \\ \vdots & \ddots \\ H_L & \ldots & H_0 \end{bmatrix}$, where $H_i = 0$ for $i > \nu$, has the property that every full size minor that is not trivially zero is nonzero.

**Remark 2** The not trivially zero full size minors of $H_L$ are exactly those which are formed by columns with indices $1 \leq j_1 < \cdots < j_{(L+1)(n-k)} \leq (L+1)n$ which fulfil $j_s(n-k) \leq sn$ for $s = 1, \ldots, L$.

The following duality result for MDP convolutional codes will be important at many points of this paper.

**Theorem 3** [4] An $(n, k, \delta)$ convolutional code is MDP if and only if its dual code, which is an $(n, n-k, \delta)$ convolutional code, is MDP.

Next, we introduce reverse MDP convolutional codes, which are advantageous for use in forward and backward decoding algorithms [15].

**Definition 9** [5] Let $\mathcal{C}$ be an $(n, k, \delta)$ convolutional code with right prime minimal generator matrix $G(z)$, which has entries $g_{ij}(z)$ and column degrees $\delta_1, \ldots, \delta_k$. Set $g_{ij}(z) := z^{\delta_j} g_{ij}(z^{-1})$. Then, the code $\overline{\mathcal{C}}$ with generator matrix $\overline{G}(z)$, which has $\overline{g_{ij}(z)}$ as entries, is also an $(n, k, \delta)$ convolutional code, which is called the reverse code to $\mathcal{C}$.

It holds: $v_0 + \cdots + v_d z^d \in \overline{\mathcal{C}} \iff v_d + \cdots + v_0 z^d \in \mathcal{C}$.

**Definition 10** [15] Let $\mathcal{C}$ be an MDP convolutional code. If $\overline{\mathcal{C}}$ is also MDP, $\mathcal{C}$ is called reverse MDP convolutional code.

**Remark 3** [15] Let $\mathcal{C}$ be an $(n, k, \delta)$ MDP convolutional code with $(n-k) | \delta$. Furthermore, let $H(z) = H_0 + \cdots + H_v z^v$ be a left prime and row proper parity-check matrix of $\mathcal{C}$. Then the reverse code $\overline{\mathcal{C}}$ has parity-check matrix $\overline{H}(z) = H_v + \cdots + H_0 z^v$. Therefore, $\mathcal{C}$ is reverse MDP if and only if every full size minor of the matrix

$$\delta_L := \begin{bmatrix} H_v & \cdots & H_{v-L} \\ \vdots & \ddots \\ 0 & \cdots & H_v \end{bmatrix}$$

formed from the columns with indices $j_1, \ldots, j_{(L+1)(n-k)}$ with $j_{s(n-k)+1} > sn$, for $s = 1, \ldots, L$ is nonzero.

Next, we introduce complete MDP convolutional codes, which are even more advantageous for decoding than reverse MDP convolutional codes as there is less waiting time when a large burst of erasures occurs and no correction is possible for some time [15].
Definition 11 [15] Let \( H(z) = H_0 + H_1 z + \cdots + H_v z^v \in \mathbb{F}[z]^{(n-k)\times n} \) be a parity-check matrix of the convolutional code \( \mathcal{C} \) of rate \( k/n \) and degree \( \delta \). Set \( L := \lfloor \frac{\delta}{n-k} \rfloor + \lfloor \frac{\delta}{k} \rfloor \). Then

\[
\mathcal{S}_j := \begin{pmatrix}
H_v \cdots H_0 & 0 \\
\cdot & \cdot & \cdot \\
0 & H_v \cdots H_0 
\end{pmatrix} \in \mathbb{F}^{(L+1)(n-k)\times (v+L+1)n}
\]

is called partial parity-check matrix of the code. Moreover, \( \mathcal{C} \) is called complete MDP convolutional code if for any of its parity-check matrices \( H(z) \), every full size minor of \( \mathcal{S}_j \) which is not trivially zero is nonzero.

Remark 4
(i) Every complete MDP convolutional code is a reverse MDP convolutional code.

(ii) A complete MDP convolutional code exists over a sufficiently large base field if and only if \( (n-k) \mid \delta \). [8]

As for \( H_L \) - when considering MDP convolutional codes - and additionally for \( \mathcal{S}_j \) - when considering reverse MDP convolutional codes - one could describe the not trivially zero full size minors of the partial parity-check matrix \( \mathcal{S}_j \) by conditions on the indices of the columns one uses to form the corresponding minor.

Lemma 1 [15] A full size minor of \( \mathcal{S}_j \) formed by the columns \( j_1, \ldots, j_{(L+1)(n-k)} \) is not trivially zero if and only if

(i) \( j_{(n-k)s+1} > sn \)

(ii) \( j_{(n-k)s} \leq sn + vn \)

for \( s = 1, \ldots, L \).

This is equivalent to \( j_1 \in \{1, \ldots, vn + k + 1\}, \ldots, j_{n-k} \in \{n - k, \ldots, (v + 1)n\}, j_{n-k+1} \in \{n+1, \ldots, (v+1)n+k+1\}, \ldots, j_{(n-k)(L+1)} \in \{(L+1)n - k, \ldots, (v+1+L)n\} \).

As one of the aims of this paper is to improve the existing bounds for the necessary field size for MDP convolutional codes, we now present what was already known before concerning this field size. The following theorem gives the only bound up to now that is valid for all code parameters.

Theorem 4 [7] Let \( B_\gamma := \frac{1}{2} \left( \frac{1}{\gamma} \binom{2(\gamma-1)}{\gamma-1} + \binom{\gamma-1}{\frac{\gamma-1}{2}} \right) \) and \( \mathbb{F} \) be a finite field with \(|\mathbb{F}| > B_\gamma \).

Then, there exists a \( \gamma \times \gamma \) superregular Toeplitz matrix over \( \mathbb{F} \).

Let \( r \) be the remainder of \( \delta \) on division by \( n-k \). Let \( \mathbb{F} \) be a finite field with \(|\mathbb{F}| > B_{(L+1)(n-1)} \) or \(|\mathbb{F}| > B_{(L+1)(n-1)+k+r-1} \) as \( r = 0 \) or \( r \neq 0 \), respectively.

Then, an \((n, k, \delta) \) MDP convolutional code exists over \( \mathbb{F} \).

This theorem as well as the following conjecture use in the same way square superregular Toeplitz matrices to construct MDP convolutional codes.

Conjecture 1 [4,7] For \( \gamma \geq 5 \), there is a \( \gamma \times \gamma \) superregular Toeplitz matrix over \( \mathbb{F}_{2^{\gamma-2}} \).

Let \( r \) be the remainder of \( \delta \) on division by \( n-k \). Let \( \mathbb{F} \) be a finite field with \(|\mathbb{F}| \geq 2^{(L+1)(n-1)-2} \) or \(|\mathbb{F}| \geq 2^{(L+1)(n-1)+k+r-3} \) as \( r = 0 \) or \( r \neq 0 \), respectively. Then, an \((n, k, \delta) \) MDP convolutional code exists over \( \mathbb{F} \).
Table 1 Minimum field size for superregular matrices

| Size of superregular Toeplitz matrix | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 |
|-------------------------------------|----|----|----|----|----|----|----|----|
| Minimum required field size         | 3  | 5  | 7  | 11 | 17 | 31 | 59 | ≤ 127 |

The preceding conjecture would yield a better bound than $B_γ$ (see [7]) but would not be sharp as Table 1 [7] shows.

At the end of this paper, we will compare these field sizes with our newly obtained results.

Throughout this paper, we will use the following notations:

**Definition 12** For a finite field $F$, we define the reverse field size as $t := \vert F \vert^{-1}$.

Moreover, we say that a real valued function $f(t)$ in the variable $t$ has the property $O(t^n)$, i.e., we write $f(t) = O(t^n)$, for some $n \in \mathbb{N}$ if $\lim_{t \to 0} t^n f(t) \leq C$ for some constant $C \in \mathbb{R}$.

Moreover, the following definition and theorem will be used frequently throughout this paper:

**Definition 13** Let $f \in F[z_1, z_2, \ldots, z_r]$ be a polynomial in $r$ variables, i.e., $f$ is a sum of terms of the form $f_{i_1, i_2, \ldots, i_r} z_1^{i_1} z_2^{i_2} \cdots z_r^{i_r}$ with $f_{i_1, i_2, \ldots, i_r} \in F$ and $i_1, i_2, \ldots, i_r \in \mathbb{N}_0$. The (total) degree of $f$ is defined as $\deg(f) := \max_{f_{i_1, i_2, \ldots, i_r} \neq 0} \sum_{j=1}^r i_j$ if $f \neq 0$ and $\deg(f) := -\infty$ if $f \equiv 0$.

**Theorem 5** (Schwartz-Zippel) [14, Corollary 1]

(a) For $r \in \mathbb{N}$, consider $f \in F[z_1, \ldots, z_r]$ with total degree $d \geq 0$. Then, $f$ has at most $d \cdot \vert F \vert^{n-1}$ zeros.

(b) Let $f \in F[z_1, \ldots, z_r]$ be a nonzero polynomial of total degree $d$. Moreover, let $v_1, \ldots, v_r$ be selected at random independently and uniformly from $F$. Then, the probability that $(v_1, \ldots, v_r)$ is a zero of $f$ is at most $d \cdot t$.

We will start our considerations with high rate convolutional codes, which are also from the point of view of applications of particular interest.

### 3 Results for high rate convolutional codes

All codes considered in this section have rate $(n-1)/n$ for some $n \in \mathbb{N}$. For degree $\delta = 1$, it is quite easy to obtain exact results for the necessary field sizes, what will be done in the first subsection. For $\delta = 2$ and the case that $n$ is an exponent of 2, the exact minimum field size has been given in [3]. For further cases, the only upper bounds for the field size that were known before, are those presented in Theorem 4 and Table 1.

#### 3.1 Results for $(n, n-1, 1)$ convolutional codes

As a starting point, in this section, we want to consider unit memory convolutional codes of high rate, i.e., $\delta = 1$ and $k = n - 1$. According to Theorem 3, these codes are dual to the $(n, 1, 1)$ convolutional codes, which should therefore also be treated in this section. With this choice of parameters one has $L = \lceil \frac{\delta}{k} \rceil + \lfloor \frac{\delta}{n-k} \rfloor = 1 + \lfloor \frac{1}{n-1} \rfloor$. Hence, $L = 1$ for $n \geq 3$ and $L = 2$ for $n = 2$. 

![Springer]
3.1.1 Results for \((2, 1, 1)\) convolutional codes

**Theorem 6** [9, Theorem 84] A \((2, 1, 1)\) convolutional code is MDP if and only if it holds for its generator matrix \(G(z) := \sum_{i=0}^{\delta} g_i z^i = g_0 + g_1 z\) with \(g_0 = \begin{pmatrix} g_{0,1} \\ g_{0,2} \end{pmatrix}\), \(g_1 = \begin{pmatrix} g_{1,1} \\ g_{1,2} \end{pmatrix}\) \(\in \mathbb{F}^2\) that \(0 \notin \{g_{0,1}, g_{0,2}, g_{1,1}, g_{1,2}\}\) and \(g_{1,1} g_{0,2} - g_{1,2} g_{0,1} \neq 0\). Consequently, the probability that a random polynomial matrix \(G(z) \in \mathbb{F}[z]^2\) with \(\text{deg}(G(z)) = 1\) generates a \((2, 1, 1)\) MDP convolutional code is \(\frac{1-t^2(1-2t)}{1+t}\) where the reverse field size \(t\) is defined as in Definition 12.

From this theorem it follows that the number of \(G(z) \in \mathbb{F}[z]^2\) with \(\text{deg}(G(z)) = 1\) that generate a \((2, 1, 1)\) MDP convolutional code over \(\mathbb{F}\) is \((|\mathbb{F}| - 1)^3 \cdot (|\mathbb{F}| - 2)\). Since two such generator matrices generate the same code if and only if they differ by a factor from \(\mathbb{F} \setminus \{0\}\), the number of \((2, 1, 1)\) MDP convolutional codes over \(\mathbb{F}\) is \((|\mathbb{F}| - 1)^2 \cdot (|\mathbb{F}| - 2)\). In particular, there exists a \((2, 1, 1)\) MDP convolutional code over \(\mathbb{F}\) if and only if \(|\mathbb{F}| \geq 3\).

Next, we want to investigate reverse and complete MDP convolutional codes with these parameters.

**Remark 5** The dual of a \((2, 1, 1)\) convolutional code is again a \((2, 1, 1)\) convolutional code and it is easy to see that one could formulate the criterion for the MDP property in the same way if using the parity-check matrix: If the code has parity-check matrix \(H(z) = \sum_{i=0}^{\delta} h_i z^i = h_0 + h_1 z\) with \(h_0 = [h_{0,1}, h_{0,2}], h_1 = [h_{1,1}, h_{1,2}] \in \mathbb{F}^{1 \times 2}\), the code is MDP if and only if \(0 \notin \{h_{0,1}, h_{0,2}, h_{1,1}, h_{1,2}\}\) and \(h_{1,1} h_{0,2} - h_{1,2} h_{0,1} \neq 0\).

**Corollary 1** A \((2, 1, 1)\) convolutional code is MDP if and only if it is complete MDP. Thus, the statements of the preceding theorem are also true for \((2, 1, 1)\) reverse convolutional codes and \((2, 1, 1)\) complete MDP convolutional codes.

**Proof** It is easy to see that the conditions on the parity-check matrix of the preceding remark are also sufficient to get a complete (and hence also a reverse) MDP convolutional code. \(\square\)

At the end of this subsection, we want to compute the probability of a \((2, 1, 1)\) MDP convolutional code under the condition that the code is non-catastrophic.

**Corollary 2** The probability that a non-catastrophic \((2, 1, 1)\) convolutional code is MDP, reverse MDP or complete MDP is \(\frac{(1-t)(1-2t)}{1+t}\) where the reverse field size \(t\) is defined as in Definition 12.

**Proof** The conditions on the generator matrix \(G(z) = \begin{pmatrix} g_1(z) \\ g_2(z) \end{pmatrix}\) with \(g_1(z) = g_{0,1} + g_{1,1} z\) and \(g_2(z) = g_{0,2} + g_{1,2} z\) to get an MDP, reverse MDP or complete MDP convolutional code imply \(\text{deg}(g_1) = \text{deg}(g_2) = 1\) and that the zero of \(g_1\) is different from the zero of \(g_2\). This means that the entries of \(G(z)\) are coprime. Thus, each \((2, 1, 1)\) MDP convolutional code is non-catastrophic. Consequently, to obtain the conditional probability (under the condition that the code is non-catastrophic), one has just to divide the probability of the first theorem by the probability of non-catastrophicity, which is \(1 - t\); see [10]. \(\square\)

3.1.2 Results for \((n, 1, 1)\) and \((n, n - 1, 1)\) convolutional codes for \(n \geq 3\)

Since the aim of the whole section is to investigate high rate convolutional codes, we are more interested in the case of \((n, n - 1, 1)\) convolutional codes. But as the \((n, 1, 1)\) convolutional
codes are dual to these codes, the two types of codes should be considered together. We start examining the case of \((n, 1, 1)\) convolutional codes.

For codes with these parameters, we consider generator matrices of the form \(G(z) = \sum_{i=0}^{\delta} g_i z^i = g_0 + g_1 z\) with \(g_0, g_1 \in \mathbb{F}_n^\ast\).

**Theorem 7** [9] For \(n \geq 3\), the probability that \(G(z) \in \mathbb{F}[z]^n\) with \(\deg(G(z)) = 1\) generates an \((n, 1, 1)\) MDP convolutional code is

\[
(1 - t^n)^{-1} (1 - t)^{n+1} \prod_{i=2}^{n-1} (1 - it)
\]

where the reverse field size \(t \) is defined as in Definition 12.

**Remark 6** According to the proof of the preceding theorem, for \(n \geq 3\), the number of \((n, 1, 1)\) MDP convolutional codes over \(\mathbb{F}\) is \(\lvert\mathbb{F}\rvert(\lvert\mathbb{F}\rvert - 1)^{n+1} \prod_{i=2}^{n-1} (\lvert\mathbb{F}\rvert - i)\), i.e. such a code exists if and only if \(\lvert\mathbb{F}\rvert \geq n\), and one can construct a generator matrix of such a code as follows: choose all entries of \(g_0\) arbitrary but nonzero, choose the first entry of \(g_1\) arbitrary and then choose entry \(i\) of \(g_1\) such that \(\begin{pmatrix} g_0, i \\ g_1, i \end{pmatrix}\) is linear independent to \(\begin{pmatrix} g_0, j \\ g_1, j \end{pmatrix}\) for \(j \in \{1, \ldots, i - 1\}\).

One could see that all MDP codes with these parameters are reverse MDP: For \(j = 1, \ldots, n\), it holds \(\overline{g}_j(z) = \begin{cases} g_j(z), & g_{1,j} = 0 \\ g_1, j + g_{0,j} z, & g_{1,j} \neq 0 \end{cases}\). Therefore, \(\overline{g}_{0,j} \neq 0\) and it is easy to see that the other conditions are also fulfilled for \(\overline{G}\).

However, since \(n - 1 \geq 2 > \delta\) and thus \((n - k) \nmid \delta\), a complete MDP convolutional code with these parameters cannot exist [8].

As in the preceding subsection, we finally consider the probability for MDP convolutional codes under the condition that the code is non-catastrophic.

**Theorem 8** The probability that a non-catastrophic \((n, 1, 1)\) convolutional code is MDP or reverse MDP is \((1 - t^n)(1 - t^{n-1}))^{-1}(1 - t)^{n+1} \prod_{i=2}^{n-1} (1 - it)\) where the reverse field size \(t\) is defined as in Definition 12.

**Proof** That \(\begin{pmatrix} g_0, i \\ g_1, i \end{pmatrix}\) is linear independent to \(\begin{pmatrix} g_0, j \\ g_1, j \end{pmatrix}\) for \(j \in \{1, \ldots, i - 1\}\) implies that the entries of \(G(z)\) are coprime and hence each \((n, 1, 1)\) MDP convolutional code is non-catastrophic. Thus, to get the conditional probability, one just has to divide the formula of the preceding theorem by the probability of non-catastrophicity, which is \(1 - t^{n-1}\); see [10].

By the duality between \((n, n - 1, 1)\) MDP convolutional codes and \((n, 1, 1)\) MDP convolutional codes, we easily get all \((n, n - 1, 1)\) MDP convolutional codes and know that they exist if and only if \(\lvert\mathbb{F}\rvert \geq n\). For the construction, we just replace the conditions on the generator matrix \(G\) by the same conditions on the parity-check matrix \(H\). The following theorem considers \((n, n - 1, 1)\) reverse and complete MDP convolutional codes.

**Theorem 9** The number of \((n, n - 1, 1)\) reverse and complete MDP convolutional codes is both \((\lvert\mathbb{F}\rvert - 1)^{n+1} \prod_{i=2}^{n} (\lvert\mathbb{F}\rvert - i)\). Hence, the minimal field size for which an \((n, n - 1, 1)\) reverse or complete MDP convolutional code could exist is \(n + 1\).

**Proof** To get reverse or complete MDP convolutional codes with these parameters, one has the additional condition that all entries of \(h_j\) have to be nonzero. Thus, there are \((\lvert\mathbb{F}\rvert - 1)^{n+1} \prod_{i=2}^{n} (\lvert\mathbb{F}\rvert - i)\) such convolutional codes, which could be constructed with the same technique as mentioned before.
3.2 Results for \((n, n - 1, 2)\) convolutional codes

The following theorem gives the exact minimum field size for MDP convolutional codes with these parameters if \(n\) is an exponent of 2.

**Theorem 10** \([3]\)** Form \(\mathbb{F} > 2\) an \((2^m - 1, 2^m - 1, 2)\) MDP convolutional code exists if and only if \(|\mathbb{F}| \geq 2^m\).

In this paper, we won’t present special formulas for the case of \((n, n - 1, 2)\) convolutional codes. However, the cases not covered by the preceding theorem, namely if \(n\) is not an exponent of 2 (as well as complete MDP convolutional codes and probabilities), could be treated with the formulas for general parameters, which we will present later in the sequel of this paper.

3.3 Example values of former bounds for the field size of \((n, n - 1, \delta)\) MDP convolutional codes

For general code parameters the only known result giving an upper bound for the necessary field size for MDP convolutional codes is \(B_\gamma\) from Theorem 4. It uses superregular Toeplitz matrices and therefore, in this theorem, the necessary field size for an MDP convolutional code is equivalent to the necessary field size for a superregular Toeplitz matrix of a certain size \(\gamma\).

For rates \(\frac{n-1}{n}\), one has \((n - k) \mid \delta\) and therefore, needs the existence of a superregular Toeplitz matrix of size \(\gamma = (L + 1)(n - 1)\).

Moreover, for small \(\gamma \leq 9\), the exact field size necessary for the existence of a \(\gamma \times \gamma\) superregular Toeplitz matrix from Table 1 could be used. However, for larger values of \(\gamma\), up to now there was only the estimation \(B_\gamma\) available.

Lower bounds on the necessary field size have not been considered very much in the literature. The following theorem presents such a bound for particular code parameters.

**Theorem 11** \([3]\)** Assume \(\delta < n - 1\). For the existence of an \((n, n - 1, \delta)\) MDP convolutional code over \(\mathbb{F}\), it is necessary to have \(|\mathbb{F}| \geq \delta(n - 1) + 1\).

Next, we prove a weak but quite easily obtained lower bound for the same rates \(\frac{n-1}{n}\) but arbitrary degree.

**Theorem 12** For the existence of \((n, n - 1, \delta)\) MDP convolutional codes, it is necessary to have \(|\mathbb{F}| \geq n\).

**Proof** If an \((n, n - 1, \delta)\) convolutional code is MDP and has parity-check matrix \(H(z) = \sum_{i=0}^{\nu} H_i z^i\) with \(H_i \in \mathbb{F}^{1 \times n}\), one knows that all not trivially zero fullsize minors of \(H_L := \begin{bmatrix} H_0 & 0 \\ \vdots & \ddots \\ H_L & \ldots & H_0 \end{bmatrix}\), where \(H_i = 0\) for \(i > \nu\), are nonzero. Consider the not trivially zero fullsize minors formed by two of the first \(2n\) columns of \(H_L\) and \(L + 1\) of the remaining columns of \(H_L\). One gets that all not trivially zero fullsize minors of \(\begin{bmatrix} H_0 & 0 \\ H_1 & H_0 \end{bmatrix}\) have to be nonzero. That is only possible if \(|\mathbb{F}| \geq n\); see Sect. 2.1.3.

In the following, we will present tables that illustrate for some typical code values these known results, which should be improved in this paper. As the lower bound from Theorem 12...
Table 2  Minimum field size for rate 1/2

| n  | 2 | 2 | 2 | 2 |
|------------------|----|----|----|----|
| δ  | 3 | 4 | 5 | 6 |
| γ  | 7 | 9 | 11| 13|
| Minimum field size | 17 ($2^5$) | 59 ($2^6$) |
| $B_γ$ | 76 ($2^7$) | 750 ($2^{10}$) | 8524 ($2^{14}$) | 104468 ($2^{17}$) |

Table 3  Minimum field size for rate 2/3

| n  | 3 | 3 | 3 | 3 |
|------------------|----|----|----|----|
| δ  | 3 | 4 | 5 | 6 |
| γ  | 10| 14| 16| 20|
| $B_γ$ | 2494 ($2^{12}$) | 372308 ($2^{19}$) | $\approx 4 \cdot 85 \cdot 10^6$ | $\approx 8 \cdot 84 \cdot 10^8$ |

Table 4  Minimum field size for rate 3/4

| n  | 4 | 4 | 4 | 4 |
|------------------|----|----|----|----|
| δ  | 3 | 4 | 5 | 6 |
| γ  | 15| 18| 21| 27|
| $B_γ$ (approx.) | $1,34 \cdot 10^6$ | $6,48 \cdot 10^7$ | $3,28 \cdot 10^9$ | $9,18 \cdot 10^{12}$ |

Table 5  Minimum field size for large rates

| n  | 10| 10| 16|
|------------------|----|----|----|
| δ  | 3 | 5 | 3 |
| γ  | 36| 54| 60|
| $B_γ$ (approx.) | $1,56 \cdot 10^{15}$ | $5,81 \cdot 10^{28}$ | $2,03 \cdot 10^{32}$ |
| $\delta(n - 1) + 1$ | 28 | 46 | 46 |

equals $n$, it is present in the following tables. Where applicable, i.e. if $\delta < n - 1$, we also include the lower bound from Theorem 11. This shows the enormous gap between lower and upper bounds.

Table 2 gives for rate 1/2 and degree $\delta = 3, \ldots, 6$, the smallest possible field size for which the existence of an MDP convolutional code is known. For $\delta \in \{3, 4\}$, one has $γ \leq 9$ and could use the exact values for the minimum field size for superregular Toeplitz matrices. For $\delta \in \{5, 6\}$, this is not possible and we have to use $B_γ$ as upper bound for the field size. Moreover, the values in brackets give the smallest binary field over which the existence of such a code is proven.

Table 3 considers rate 2/3. For $\delta \geq 5$, the values of $B_γ$ are given only approximately as they are very large.

In Table 4 one can find examples for rate 3/4 MDP convolutional codes.

Finally, we present some values for higher rates to show the extremely large values of $B_γ$ obtained in these cases (Table 5).

In the following sections, we prove results that reduce many of these gaps and at the end of the paper we will evaluate the amount of the improvement we could achieve.
4 Sufficient field size and probability for MDP convolutional codes with arbitrary parameters

4.1 Sufficient field size

The goal of this subsection is to estimate what field size one needs such that it is possible to construct an MDP convolutional code with given but arbitrary parameters \( n, k \) and \( \delta \).

**Theorem 13** Let \( g \) be the polynomial that is formed by the product of all not trivially zero fullsize minors of \( H_L \) and has the entries of the coefficient matrices of \( H \) as variables. Then, an \((n, k, \delta)\) MDP convolutional code exists if \(|F| > \deg(g)\).

**Proof** It is sufficient to show the existence of an MDP convolutional code with generic row degrees, i.e. \( \nu = \lceil \frac{\delta}{n-k} \rceil \) and consider only matrices \( H \) of the form of Remark 1. This means \( H_{\nu} \) and \( H_{\nu-1} \) are of the forms \( H_{\nu} = \begin{pmatrix} I_{\delta-(n-k)(\nu-1)} & 0 & * \\ 0 & 0_{(n-k)\nu-\delta} & 0 \end{pmatrix} \) and \( H_{\nu-1} = \begin{pmatrix} * \\ 0_{((n-k)\nu-\delta)\times(\delta-(n-k)(\nu-1))} & I_{(n-k)\nu-\delta} & * \end{pmatrix} \), respectively. In this way, one can ensure that the generated code has really the given degree \( \delta \).

According to Theorem 5 (a), a polynomial \( g \) over \( F \) with \( m \) variables (and \( \deg(g) \geq 0 \)) has at most \( \deg(g) \cdot |F|^m \) zeros. Altogether, there are \(|F|^m \) tuples of points. Therefore, for having at least one of them being not a zero, it is sufficient that \(|F|^m > \deg(g) \cdot |F|^m \), i.e. \(|F| > \deg(g)\).

We apply this result to the polynomial \( g \) formed by the product of all not trivially zero fullsize minors of \( S_L \).

Since some of the entries of \( H_{\nu} \) and \( H_{\nu-1} \) are fixed zeros or ones, one has less variables than the number of entries of the coefficient matrices of \( H \) but this has no influence on the result (note that if \( \nu > L \), i.e. \( \nu = L + 1 \), and \( \lfloor \frac{\delta}{n-k} \rfloor = 0 \), for which case we give a better bound in a later section, all entries of \( H_{\nu} \) do not occur in the polynomial on which we apply the Schwartz-Zippel lemma). What influences the Schwartz-Zippel lemma is not the number of variables but the degree of the polynomial \( g \). This degree is in all cases at most \((L + 1)(n - k)\) times the number of not trivially zero fullsize minors of \( S_L \).

It remains to estimate the degree of the polynomial \( g \) from the preceding theorem to get an explicite bound for the field size.

**Theorem 14** If \(|F| > \min\{M_1, M_2, M_3\}\) with

\[
M_1 := (L + 1)(n - k) \left( \frac{(L + 1)n}{(L + 1)(n - k)} \right) \\
M_2 := (L + 1)(n - k) \left( \frac{n}{n - k} \right) \left( \frac{n + k}{n - k} \right) \cdots \left( \frac{n + Lk}{n - k} \right) \\
M_3 := (L + 1)(n - k) \sum_{i=n-k}^{n} \left( \frac{i - 1}{n - k - 1} \right) \left( \frac{2n - i}{n - k} \right) \cdots \left( \frac{2n + (L - 1)k - i}{n - k} \right)
\]

then there exists an \((n, k, \delta)\) MDP convolutional code over \( F \).

**Proof** To show that \(|F| > M_i\) for some \( i \in \{1, 2, 3\} \) is sufficient, one has to show that the factor after \((L + 1)(n - k)\) in the formulas is an upper bound for the number of not trivially
zero fullsize minors of \( \mathcal{H}_L \). For \( M_1 \) this is clear because there we use just the formula for all fullsize minors.

For \( M_2 \), we use the condition that we have to choose \( n - k \) columns from the first \( n \) columns, then \( n - k \) columns from the first \( 2n \) columns without the \( n - k \) columns we have already chosen and so on until we end up with choosing \( n - k \) columns from \( (L + 1)n \) columns without the \( (n - k) \) columns we have already chosen.

For \( M_3 \), we denote by \( i \in \{ n - k, \ldots, n \} \) the index of the \((n - k)\)-th column we choose. Thus, one has to choose \( n - k - 1 \) columns with smaller index than \( i \), i.e. out of the first \( i - 1 \) columns of \( \mathcal{H}_L \). After that, one proceeds like for \( M_2 \), i.e. next one has to choose \( n - k \) columns out of \( 2n \) but not the first \( i \), then \( n - k \) out of \( 3n \) without the first \( i \) and without the \( n - k \) chosen in the preceding step and so on. \( \square \)

**Remark 7** It depends on the parameters of the code, which of the bounds is best. In the following, we give some examples:

1. Case \( L = 0 \): \( M_1 = M_2 = M_3 \) (in this case there are no trivially zero minors)
2. Case \( k = 1 \): \( M_3 = M_2 = \left( \frac{1}{n} + \frac{n-1}{(n-1)} \right) \)
   
   (a) \( L \geq 1 \): \( M_3 < M_2 \)
   
   (b) \( L = 1 \) (\( \Rightarrow \delta = 1, n \geq 3 \)): \( M_3 = (3n^2 - n)(n - 1) < M_1 = (4n^2 - 2n)(n - 1) < M_2 = (n^3 + n^2)(n - 1) \)

   (c) \( (2, 1, 1) \): \( M_3 = 18 \cdot 3 < M_1 = 20 \cdot 3 < M_2 = 24 \cdot 3 \)

   (d) \( (2, 1, \delta) \) with \( \delta \geq 2 \): \( M_1 < M_3 < M_2 \)

   It holds \( L \geq 4 \), which implies \( M_3 < M_2 \) according to (a), and for \( L = 4 \), \( M_1 = 252 \cdot 5 < 3 \) \( M_3 = 480 \cdot 5 < M_2 = 720 \cdot 5 \). Moreover, \( M_3 \) is increasing more than \( M_1 \), when \( L \) increases (to \( L + 1 \)). This is true since \( M_1/(L + 1) = \left(\frac{2(L+1)}{L+1}\right) \)

   with factor \( \left(\frac{2(L+3)}{(L+4)(L+2)}\right) < 4 \) and \( M_3/(L + 1) = (L + 2)! \cdot \left(\frac{1}{2} + \frac{1}{L+2}\right) \)

   increases with factor \( (L + 2)\frac{L^2 + 7L + 10}{L^2 + 7L + 12} > 5 \) for \( L \geq 4 \).

### 4.2 Probability

In this subsection, we want to compute the probability that a non-catastrophic convolutional code with arbitrary parameters is MDP. Therefore, we assign to each code the unique parity-check matrix from Remark 1. This is possible since permutation of the columns of the parity-check matrix does not influence the MDP property. With these definitions/settings, one gets the following theorem:

**Theorem 15** Let \( \mathbb{F} \) be finite with cardinality \( |\mathbb{F}| = t^{-1} \). If \( |\mathbb{F}| > \min\{M_1, M_2, M_3\} \), the probability for an MDP convolutional code is lower bounded by

\[
(i) \quad 1 - \frac{(L + 1)(n - k)\binom{L+1}{L+1}(n-k)}{1 - t^k + O(t^{k+1})} \cdot t \\
(ii) \quad 1 - \frac{(L + 1)(n - k)\binom{n}{n-k}\binom{n+k}{n-k}\cdots\binom{n+Lk}{n-k}}{1 - t^k + O(t^{k+1})} \cdot t \\
(iii) \quad 1 - \frac{(L + 1)(n - k)\sum_{i=n-k}^{n-1}(\binom{2n-i}{n-k}\cdots\binom{2n+(L-1)k-i}{n-k})}{1 - t^k + O(t^{k+1})} \cdot t
\]
Proof For MDP (in contrast to complete MDP) it is not necessary that \( H \) has generic row degrees. Therefore, one has to make the following considerations for all possible values of the row degrees. However, we will see that this does not matter.

Again, we assume that \( H = [P \ Q] \) has the form of Remark 1. If the row degrees of \( Q \) are fixed, one knows for each entry of \( H \) either its degree or an upper bound on its degree. Hence, when considering the entries of the coefficient matrices of \( H \) as variables, we know how many variables we have and could apply Theorem 5 (b) to the polynomial \( g \) that is formed by the product of the non-trivially fullsize minors of \( \mathcal{H}_L \). Note that this polynomial is not the zero polynomial (since the existence of MDP convolutional codes has been shown for \(|\mathbb{F}| > \min\{M_1, M_2, M_3\}\)).

It has already been shown that \( M_1, M_2 \) and \( M_3 \) are upper bounds for \( \deg(g) \).

By the Schwartz-Zippel lemma, the probability that the variables do not fulfill the condition for MDP is upper bounded by \( \deg(g) \cdot t \).

One has to consider conditional probability with the condition that \( Q \) and \( P \) are left coprime. Therefore, the overall probability is upper bounded by the absolute probability divided by the probability of the condition, which is \( 1 - t^k + O(t^{k+1}) \); see [10]. \( \square \)

5 Sufficient field size and probability for complete MDP convolutional codes

In this section, we want to do the same considerations for complete MDP convolutional codes that were done for MDP convolutional codes in the preceding section.

5.1 Sufficient field size

Theorem 16 Let \( f \) be the polynomial that is formed by the product of all not-trivially zero fullsize minors of the partial parity-check matrix \( \mathcal{J}_\delta \) (as defined in (1)) and has the entries of the coefficient matrices of \( H \) as variables. Then, for \( (n - k) \mid \delta \), an \((n, k, \delta)\) complete MDP convolutional code exists if \(|\mathbb{F}| > \deg(f)\).

Proof One uses the Schwartz-Zippel lemma and proceeds completely analogous to the preceding subsection. \( \square \)

Again, we have to estimate the degree of the polynomial \( f \) from the preceding theorem to get an explicite bound for the field size.

Theorem 17 If \((n - k) \mid \delta \) and \(|\mathbb{F}| > \min\{N_1, N_2\}\) with

\[
N_1 := (L + 1)(n - k) \left( \frac{L + 1 + \delta}{n - k} \right)^n \]

(2)

\[
N_2 := (L + 1)(n - k) \left( \frac{\delta n}{n - k} + k + 1 \right)^{(n-k)(L+1)} \]

(3)

then there exists an \((n, k, \delta)\) complete MDP convolutional code over \( \mathbb{F} \).

Proof Each fullsize minor of \( \mathcal{J}_\delta \) is a polynomial of degree \((L + 1)(n - k)\). Moreover, the number of not-trivially zero fullsize minors of \( \mathcal{J}_\delta \) is upper bounded by \( \left( \frac{L+1+n-k}{L+1} \right)^{n-k} \), which is the number of all fullsize minors, as well as by \( \left( \frac{\delta n}{n-k} + k + 1 \right)^{(L+1)(n-k)} \) since the index of each chosen column has to lie in an interval with \( \frac{\delta n}{n-k} + k + 1 \) elements (see Lemma 1). \( \square \)
Remark 8  
(i) It depends on the parameters of the code, which of the two bounds \( N_1 \) or \( N_2 \) is better, i.e. smaller. For example for \( k = n - 1 \), the second bound is better for \( n = 2 \), for \( n = 3 \) the bounds are identical, and for \( n \geq 4 \) the first bound is better.
(ii) For complete MDP, one has \( v = \frac{\delta}{n-k} \) and hence \( L \geq v \geq 1 \), which implies \( \binom{vn+k}{\lfloor (L+1)/(n-k) \rfloor} \cdot ((n-k)(L+1))^{1/2(n-k)(L+1)} \geq \binom{vn+k}{\lfloor (L+1)/(n-k) \rfloor} \cdot (n-k)(L+1) \geq (L+1)(n-k)(\frac{\delta}{n-k}+k+1)^{(n-k)(L+1)} \) if \( (n, k, \delta) \neq (2, 1, 1) \). This shows that - unless \( (n, k, \delta) = (2, 1, 1) \) - the bound on the field size presented here is better than the bound obtained by the construction in [8], which is clearly very weak (which is due to the fact that it provides a general construction) but up to now there did not exist better bounds. For \( (2, 1, 1) \), we have already seen that the minimal possible field size is 3, i.e. much smaller than all these bounds.

5.2 Probability

We want to compute the probability that a non-catastrophic convolutional code with \( (n-k) \parallel \delta \) and generic row degrees \( v = \frac{\delta}{n-k} \) is complete MDP. Therefore, we assign again to each code the unique parity-check matrix from Remark 1. This is possible since permutation of the columns of the parity-check matrix does not influence the property to be complete MDP. With these definitions/settings, one gets the following theorem:

**Theorem 18**  
If \(|F| > \min\{N_1, N_2\}\), the probability for an \((n, k, \delta)\) complete MDP convolutional code is lower bounded by

\[
\begin{align*}
(i) \quad 1 - & \frac{(L+1)(n-k)(\frac{\delta}{n-k}+k+1)^{(n-k)(L+1)} \cdot t}{1 - t^k + O(t^{k+1})} \\
(ii) \quad 1 - & \frac{(L+1)(n-k)(\frac{\delta}{n-k}+k+1)^{(n-k)(L+1)} \cdot t}{1 - t^k + O(t^{k+1})}
\end{align*}
\]

where \( t \) denotes again the reverse field size.

**Proof**  
The proof is completely analogue to the proof for the probability of MDP convolutional codes. \( \square \)

6 Sufficient field size for MDP convolutional codes with
\( \delta < \max\{k, n-k\} \)

In this section, we show a better bound on the necessary field size for MDP convolutional codes for the case that \( \delta < \max\{k, n-k\} \). Because of duality arguments, we mainly have just to solve the case \( \delta < k \).

6.1 The case \( \delta < k \)

To derive an upper bound for the required field size, one could assume that \( H \) has generic row degrees since the existence of an MDP convolutional code with generic row degrees over \( F \) obviously implies the existence of an MDP convolutional code over \( \overline{F} \). The genericity of the row degrees implies \( v = \lceil \frac{\delta}{n-k} \rceil \) and therefore \( L = \lfloor \frac{\delta}{n-k} \rfloor \leq v \). If \( (n-k) \parallel \delta \), i.e. \( L = v \), all row degrees of \( H \) are equal to \( v \) and hence \( H_L = H_v \) does not contain fixed zeros. If
\((n-k) \dagger \delta\), i.e. \(L = \nu - 1\) and all row degrees of \(H\) are either equal to \(\nu - 1\) or equal to \(\nu\), \(H_L\) does not contain fixed zeros, too.

**Theorem 19** There exists an \((n, k, \delta)\) MDP convolutional code with \(\delta < k\) over \(\mathbb{F}\) if either

1. \(|\mathbb{F}| > (L+1)n-1\) or
2. in the case \(L \geq 1\), \(|\mathbb{F}| > S(n, k, \delta)\) with

\[
S(n, k, \delta) := \sum_{j=n-k+1}^{(n-k)L-1} \binom{n-1}{j-1} \binom{\frac{j}{n-k}}{n} n \left( \binom{\frac{j}{n-k}+1}{n-k} n \right) \cdots \left( \binom{L}{n-k} \right) + \sum_{j=\max\{\delta, L, n-k+1\}}^{(n-k)(L+1)-1} \binom{n-1}{j-1} \binom{L}{j+L-1} + \binom{n-1}{L+1(n-k)-1}
\]

**Proof** For \(y \in \{1, \ldots, (L+1)(n-k)\}\), define \(\mathcal{H}_L^{(y)}\) as the matrix consisting of the first \(y\) rows of \(H_L = \begin{bmatrix} H_0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ H_L & \cdots & H_0 \end{bmatrix} \).

We prove via induction with respect to \(y\) that if \(\mathbb{F}\) fullfills condition 1 or 2, then it is possible to find values for \(H_0, \ldots, H_L\) over \(\mathbb{F}\) such that every fullsize minor of \(\mathcal{H}_L^{(y)}\) that is not trivially zero is nonzero.

For \(y = 1\), all entries in the first row of \(H_0\) have to be nonzero, what is possible if \(|\mathbb{F}| > 1\), which is implied by both condition 1 and condition 2 (but true for any field anyway).

Assume that the statement is valid for \(1, \ldots, y\). For the step to \(y + 1\), consider the last row of \(\mathcal{H}_L^{(y+1)}\). First, we show that for each \(i \in \{1, \ldots, n\}\), if all entries of \(\mathcal{H}_L^{(y+1)}\) but the \(i\)-th entry of the last row of \(\mathcal{H}_L^{(y+1)}\), named by \(\mathcal{H}_{L,i}\), are fixed (such that the statement is valid for \(1, \ldots, y\)), there is a possibility to choose \(\mathcal{H}_{L,i}\) from \(\mathbb{F}\) such that the statement is valid for \(y + 1\).

To do this, we consider all not trivially zero fullsize minors of \(\mathcal{H}_L^{(y+1)}\) that contain the \(i\)-th column of this matrix.

For each of these minors, one has to show that it is possible to choose \(\mathcal{H}_{L,i}\) such that the minor is nonzero.

Denote by \(M \in \mathbb{F}^{(y+1) \times (y+1)}\) the submatrix of \(\mathcal{H}_L^{(y+1)}\) that corresponds to the considered fullsize minor and let \(\hat{M}\) be constructed out of \(M\) by deleting the row and the column that contain \(\mathcal{H}_{L,i}\).

Hence, in the case \(\det(\hat{M}) = 0\), one has to show \(\det(M) \neq 0\), independent of the choice of \(\mathcal{H}_{L,i}\).

Since \(\hat{M}\) is a fullsize minor of \(\mathcal{H}_L^{(y)}\), it follows by induction that it has to be trivially zero. Because of the structure of \(\mathcal{H}_L\) this implies that there exists \(s \in \{1, \ldots, L\}\) such that column \(s(n-k)\) of \(\hat{M}\) is a column of \(\mathcal{H}_L^{(y)}\) with index at least \(sn + 1\). Moreover, it follows that this column is column \(s(n-k) + 1\) of \(M\) and its first \(s(n-k)\) entries are zeros since it is not from the first \(s\) blocks of \(\mathcal{H}_L\).

Consequently, \(M\) is of the following form: 

\[
\begin{bmatrix} A_{s(n-k) \times (y+1-s(n-k))} & B \\ \ast & \end{bmatrix} \in \mathbb{F}^{(y+1) \times (y+1)}.
\]

Hence \(A\) and \(B\) are square matrices with \(\det(M) = \det(A) \cdot \det(B)\). Moreover, \(A\) and \(B\) are fullsize submatrices of 

\[
\begin{bmatrix} H_0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ H_{s-1} & \cdots & H_0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} H_0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ H_{L-s} & \cdots & H_0 \end{bmatrix},
\]

respectively.
Since the columns of $M$ are chosen such that $\det(M)$ is not trivially zero, $\det(A)$ and $\det(B)$ are not trivially zero, too. By induction it follows that $\det(A)$ and $\det(B)$ are nonzero and therefore also $\det(M)$ is nonzero.

To show that one can find such $\mathcal{H}_{L,i}$ over $\mathbb{F}$ if condition 1 or 2 is fulfilled, we count the maximum number of values that have to be excluded for $\mathcal{H}_{L,i}$, where without restriction, one could assume $i = n$ (note that $\hat{M}$ is independent of $\mathcal{H}_{L,i}$ as well as $\det(M)$ in the case $\det(\hat{M}) = 0$). This number is upper bounded by the number of not trivially zero fullsize minors of $\hat{M}$ with $r_j = n$ for some $j \in \{1, \ldots, (L+1)(n-k)\}$ since all these minors are at most linear in $H_{L,n}$. For the bound of condition 1, we just count the number of all fullsize minors with $r_j = n$ no matter if they are trivially zero or not. Surely, it is sufficient if $\mathbb{F}$ has more elements as the number of these minors.

For condition 2, which takes into account that some minors are trivially zero, one could assume $L \neq 0$ and neglect the case $j \leq n - k$. Since $r_{j+1} > n$, the minor would be trivially zero if $j < n - k$. If $j = n - k$, one chooses exactly $n - k$ columns from the first block of $\mathcal{H}_L$ and the minor is nonzero if and only if the corresponding $n - k$ columns of $H_0$ are linearly independent and the matrix (for the minor) without the first $n - k$ columns and rows has full rank. But these conditions are independent of $H_L$ and hence, do not lead to values for $H_{L,n}$ that have to be excluded.

For $j \geq n - k + 1$, there are at most $\binom{n-1}{j-1}$ possibilities to choose $r_1, \ldots, r_{j-1}$ since one has the condition $1 \leq r_1 < r_2 < \cdots < r_{j-1} < r_j = n$. For $r_j$ with $l > j$, one has to consider the condition $r_{s(n-k)} \leq s n$ for $s = 1, \ldots, L$. $r_j = n$ implies that this condition is already fulfilled for $s = 1, \ldots, \lfloor \frac{j}{n-k} \rfloor$. To fulfill this condition for $s = \lceil \frac{j}{n-k} \rceil + 1$, we need to choose $(\lfloor \frac{j}{n-k} \rfloor + 1)(n-k) - j$ columns from the first $(\lfloor \frac{j}{n-k} \rfloor + 1)n$ columns but not from the first $n$ columns of $\mathcal{F}_L$, i.e. we have to choose $(\lfloor \frac{j}{n-k} \rfloor + 1)(n-k) - j$ columns out of $(\lfloor \frac{j}{n-k} \rfloor)n$ columns. For $s \geq \lceil \frac{j}{n-k} \rceil + 2$, we have to choose $n - k$ columns out of at most $s n - n$ columns. Summing over all possible values for $j$, one gets the formula from condition 2.

To ensure that the degree of the code is equal to $\delta = v_1 + \cdots + v_{n-k}$, one has to ensure the $H$ is row proper, i.e. that the highest row rank coefficient matrix is invertible. This is true if the first $\delta - (n - k)(v-1)$ rows of $H_v$ and the last $(n - k)v - \delta$ rows of $H_{v-1}$ are linearly independent. When choosing the entries of $\mathcal{H}_L$ row by row as done in this proof, the number of values that has to be excluded for each entry of a coefficient matrix increases in each step. Moreover the condition that the highest row degree coefficient matrix is invertible, i.e. that the above mentioned rows are linearly independent, could be fulfilled by the first $n - k$ columns of $H_{v-1}$ and $H_v$. Therefore, one has no additional condition on $H_{L,n}$ because of that and thus, no additional value has to be excluded. (Note that for $(n-k) \nmid \delta$, i.e. $v > L$, $H_v$ is not contained in $\mathcal{H}_L$ and the only thing that has to be regarded when choosing the values for $H_v$ is that $H$ has to be column proper).

It would be possible to adopt condition 2 such that is valid also for $L = 0$ (in principle, the difference would be that then, one had to take $j = n - k$ as lower bound for the first sum since the case $j = n - k$ cannot be neglected for $L = 0$). But for $L = 0$ one has no trivially zero fullsize minors in $\mathcal{H}_L = H_0$ and therefore, it would equal the bound of condition 1 for $L = 0$, anyway.
Corollary 3  Bound 1 of the preceding theorem can be upper bounded by the following expression, which is independent of $k$:

$$\binom{(L+1)n-1}{(L+1)(n-k)-1} \leq \binom{(L+1)n-1}{n-2}.$$ 

Proof  Per definition, $L = \lfloor \frac{\delta}{n-1} \rfloor + \lfloor \frac{\delta}{n-2} \rfloor = \lfloor \frac{\delta}{n-1} \rfloor$ as $k > \delta$. Hence $L \leq \frac{\delta}{n-1}$, i.e. $L(n-k) \leq \delta$. It follows $(L+1)(n-k)-1 = L(n-k)+n-k-1 \leq \delta + n-k-1 \leq n-2$ since $k > \delta$. Moreover for $L \geq 1$, one has $2(n-2)+1 \leq 2n-3 < (L+1)n-1$ and thus, $\binom{(L+1)n-1}{(L+1)(n-k)-1} \leq \binom{(L+1)n-1}{n-2}$. \hfill \square

Remark 9  For $k = n-1$, i.e. $(n, n-1, \delta)$ convolutional codes with $\delta \leq n-2$, one has $L = \delta$ and the bound of condition 2 equals

$$\delta-1 \sum_{j=2}^{\delta} \binom{n-1}{j-1} \binom{j}{1} \binom{(j+1)n}{1} \cdots \binom{(n-1)}{1} \binom{n-1}{1} \binom{n-1}{\delta} = \delta \cdot n \sum_{j=1}^{\delta} \delta \binom{j-1}{j} \binom{n-1}{j} \binom{n-1}{\delta} < \delta \cdot n^\delta (e-1)$$

as

$$\delta \sum_{j=1}^{\delta} \binom{n-1}{j} \binom{n-1}{j} = (1+1/n)^{n-1} - 1 < e - 1.$$ 

Setting also $\delta = 1$ (for which one needs $n \geq \delta + 2 = 3$), one gets $n - 1$. This implies that the bound is sharp in that case; see Sect. 3.

6.2 The case $\delta < n - k$

For this case, we could use again that the MDP property is invariant under duality.

Theorem 20  If $\delta < n - k$ and $|\mathbb{F}| > S(n, n-k, \delta)$ or $|\mathbb{F}| > \binom{(L+1)n-1}{(L+1)k-1}$, there exists an $(n, k, \delta)$ MDP convolutional code over $\mathbb{F}$.

Proof  The result follows from the preceding subsection and Theorem 3. \hfill \square

Corollary 4  Analogous to the preceding subsection, one gets for $\delta < n - k$ that

$$\binom{(L+1)n-1}{(L+1)(n-k)-1} \leq \binom{(L+1)n-1}{n-2}.$$ 

6.3 The case $\delta < \min\{k, n-k\}$

In this subsection, we consider the case that the conditions of both preceding subsections are fulfilled, resulting in $L = 0$.

Theorem 21  If $\delta < \min\{k, n-k\}$ and $|\mathbb{F}| > \min \left\{ \binom{n-1}{n-k-1}, \binom{n-1}{k-1} \right\}$, there exists an $(n, k, \delta)$ MDP convolutional code over $\mathbb{F}$.

Proof  The result follows from the results of the preceding subsections. \hfill \square
Remark 10  (i) For $\delta < \min \{k, n-k\}$, i.e. $L = 0$, one has $H_L = H_0$ and the corresponding code is MDP if and only if $\begin{pmatrix} I_k & H_0 \end{pmatrix}$ is the generator matrix of an $[n, k]$ MDS block code.

Therefore, the bound of the preceding theorem is a bound for the necessary field size for the existence of an $[n, k]$ MDS block code.

(ii) $n-k > \delta$ implies that $n-k$ cannot divide $\delta$ and therefore, there exists no complete MDP convolutional code with these parameters. However, one could show that for a reverse MDP convolutional code with $L = 0$, the bound for MDP codes is also sufficient: $G_1, \ldots, G_\mu$ do not influence the property to be MDP. Thus, one could choose them arbitrary without affecting the MDP property. If one chooses column $j$ of $G_\delta j$ equal to column $j$ of $G_0$, one gets $G_0 = G_0$ and therefore, the code is also reverse MDP.

(iii) For an $(n, n-2, 1)$ convolutional code, the bound of the preceding theorem is equal to $n-1$. One could easily see that the construction $H_0 = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & 1 & \cdots & n-1 \end{pmatrix}$ reaches this bound. But as we will see in the next section, constructions over fields of smaller size are possible.

7 Comparison of bounds

The aim of this section is to show that in nearly all cases, the bounds on the necessary field size for the existence of MDP convolutional codes presented in this paper could improve all bounds that were proven before.

Now, we want to compare the new bounds of this paper with the already existing bounds (but the bound in [3] since that bound is optimal anyway) and start with the case $L = 0$.

7.1 Comparison of bounds for $L = 0$

Theorem 22  The bound for $L = 0$ from Theorem 21 is the best, i.e. the smallest, upper bound on the necessary field size for MDP convolutional codes that is known up to now. In particular, it is smaller than the bound $B_H$ from Theorem 4, smaller than the bound from Conjecture 1 and better than using exact values for superregularity for small matrices from Table 1.

Proof  $L = 0$ implies $n-k > \delta$, i.e. $n-k$ does not divide $\delta$ and thus $r \geq 1$. Hence, $\binom{n-k-1}{k-1} < 2^{n-1} \leq 2^{n-k+2}$ shows that the new bound is better than the conjecture, which implies that it is better than using the bound $B_H$. The first inequality follows from the Stirling formula and the second since $k > \delta \geq 1$.

Exact values for the existence of superregular matrices are only known if $n+k+r-2 \leq 10$. Computing all cases in which this inequation as well as $\min \{n-k, k\} > \delta$ is fullfilled, which implies $r = \delta$, one sees that the new bound is always smaller.

We want to show with some small examples that there are cases in which $L = 0$ and our bound is not optimal (even if it is the best of the existing bounds).

Example 1  1. According to Theorem 21, an $(4, 2, 1)$ MDP convolutional code exists if $|\mathbb{F}| \geq 4$. But $H_L = H_0 := \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix}$ yields an MDP convolutional code with these parameters over $\mathbb{F}_3$. 

\[ Springer \]
2. According to Theorem 21, (6, 3, 1) and (6, 3, 2) MDP convolutional codes exist if \( |F| \geq 1 \). But \( \mathcal{H}_L = H_0 := \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 2 \\ 0 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 & 3 & 3 \end{pmatrix} \) yields MDP convolutional codes with these parameters over \( F_5 \).

7.2 Comparison of bounds for \( L \geq 1 \) and \( \delta < \max\{k, n - k\} \)

**Theorem 23**

(i) Bound 2 from Theorem 19 is always better than \( B_2 \) from Theorem 4 and better than Conjecture 1. It is also better than using exact values for superregularity for small matrices - except for (5, 3, 2) codes, where bound 2 yields the existence of MDP codes if \( |F| > 34 \) and using the table for existence of superregular matrices, one gets that \( |F| \geq 31 \) is sufficient.

(ii) Bound 1 from Theorem 19 is for nearly all cases the next best bound after bound 2, exceptions are only (15, 8, 7), (13, 7, 6), (11, 6, 5), (9, 5, 4), (7, 4, 3), (6, 4, 2), (5, 3, 2), (3, 2, 1). For (3, 2, 1), using \( B_2 \) from Theorem 4, which is here identical with the exact minimal value for superregularity, yields a bound between 2 and 1. For (6, 4, 2) using the exact value for superregularity yields a bound between 2 and 1. In the other cases, Conjecture 1 yields a bound between 2 and 1 but the conjecture has not been proven.

**Proof**

**Step 1: Bound 2 is always better than bound 1**

In bound 2, for each \( j \in \{n - k + 1, \ldots, (n - k)(L + 1)\} \), one chooses altogether \( (L + 1)(n - k) - 1 \) elements from at most \( (L + 1)n - 1 \) elements (for \( n - k + 1 \leq j < L(n - k) \), this is true since \( (L - \lfloor \frac{j}{n-k} \rfloor n)(n-k) + (\lfloor \frac{j}{n-k} \rfloor + 1)(n-k) + 1 = (L+1)(n-k) - 1 \) and \( (L - \lfloor \frac{j}{n-k} \rfloor n + n - 1 \leq (L + 2 - \lfloor \frac{n-k+1}{n-k} \rfloor)n - 1 \leq (L+1)n - 1 \). Hereby, one has certain conditions for this choice. Bound 2 computes all possibilities without any restrictions to choose \( (L + 1)(n - k) - 1 \) elements from \( (L + 1)n - 1 \) elements and is therefore larger.

**Step 2: We use the upper bound for bound 1 from Corollary 3 and Corollary 4**

According to Corollary 3 and Corollary 4, it is sufficient to show that \( \binom{(L+1)n-1}{n-2} \) is always smaller than the conjecture.

**Step 3: For \( L = 2 \), bound 1 is better than Conjecture 1 (and therefore, also better than \( B_2 \))**

Bound 1 is at most \( \binom{3n-1}{n-2} < \frac{2^{3n-1}}{\sqrt{\pi}\sqrt{\binom{3n-1}{n-2}}} \) by the Stirling formula and the conjecture is equal to at least \( 2^{3n-5} \). For \( n \leq 6 \), one could compute directly that \( \binom{3n-1}{n-2} \) is smaller than \( 2^{3n-5} \). For \( n = 7 \), one could compute that \( \frac{2^{3n-1}}{\sqrt{\pi}\sqrt{\binom{3n-1}{n-2}}} \) is smaller than \( 2^{3n-5} \). Since \( 2^{3n-5} \) is increasing more rapidly than \( \frac{2^{3n-1}}{\sqrt{\pi}\sqrt{\binom{3n-1}{n-2}}} \) when \( n \) increases, this is true for \( n \geq 7 \) (in other words for \( n \geq 7 \), \( \sqrt{\pi}\sqrt{\binom{3n-1}{n-2}} < 2^4 \) and therefore, \( \binom{3n-1}{n-2} < \frac{2^{3n-1}}{\sqrt{\pi}\sqrt{\binom{3n-1}{n-2}}} < 2^{3n-5} \).

**Step 4: For \( L \geq 2 \), bound 1 is better than Conjecture 1 (and therefore, also better than \( B_2 \))**

From the preceding step, we know that for \( L = 2 \) and arbitrary \( n \), \( \binom{(L+1)n-1}{n-2} < 2^{(L+1)(n-1)-2} \). It remains to show that the right hand side of this inequality increases more rapidly than the left hand side when \( L \) increases (and \( n \) is fixed). When increasing
L to \( L + 1 \) the left hand side increases by the factor

\[
\frac{((L + 2)n - 1)! \cdot (Ln + 1)!}{((L + 1)n - 1)! \cdot ((L + 1)n + 1)!} = \frac{(L + 1)n \cdot \cdots \cdot (L + 2)n - 1)}{(Ln + 2) \cdot \cdots \cdot ((L + 1)n + 1)} < (1.5)^n. \tag{4}
\]

This inequality is true since \( 2(Ln + 2) = (L + 1)n + (L - 1)n + 4 \) and hence \( \frac{(L + 1)n}{Ln + 2} = 2 - \frac{(1-L)n + 4}{Ln + 2} < 2 - \frac{L - 1}{L} = 1 + \frac{1}{L} \leq 1, 5. \) This implies \( \frac{(L + 1)n + i}{Ln + 2 + i} < 1, 5 \) for \( i \in \{0, \ldots, n-1 \} \) and (4) follows.

However, when increasing from \( L \) to \( L + 1 \), the right hand side increases by the factor \( 2^{n-1} > (1.5)^n \) for \( n \geq 3 \).

Step 5: The case \( L = 1 \)

5.1: The case \( n - k \not| \delta \)

If \( n - k \not| \delta \), the bound of the conjecture is \( 2^{n-2+k+r-1} \geq 2^{n-2} \). Furthermore, \( \left( \frac{2^{n-1}}{n-2} \right)^{2n-1} < 2^{n-2} \) for \( n \geq 3 \).

5.2: The case \( n - k \mid \delta \) and \( k > \delta + 1 \)

\( L = 1 \) and \( n - k \mid \delta \) imply \( n - k = \delta \). If \( k \geq \delta + 1 \), one has \( 2(n-k) - 1 \leq n - 3 \) and hence \( \left( \frac{2^{n-1}}{2(n-k)-1} \right)^{2n-1} \leq \left( \frac{2^{n-1}}{2(n-k)-1} \right)^{2n-1} \). When \( n \) increases to \( n + 1 \), the right hand side of this inequality increases by the factor \( \frac{(2n+1)! \cdot (n-3)! \cdot (n+2)!}{(n-2)! \cdot (n+3)! \cdot (2n-1)!} = \frac{(2n+1)! \cdot 2n \cdot 2n \cdot 2n \cdot 2}{(n-1)! \cdot (n+1)! \cdot (2n-1)!} < 4^n \). The conjectured bound, which is in this case equal to \( 2^{n-4} \), increases by the factor 4. It holds \( \frac{4n^2 + 2n}{n^2 + n - 6} < 4 \iff n \geq 12 \). Moreover, one could compute directly that \( \left( \frac{2^{n-1}}{n-3} \right)^{2n-4} \) for \( n \in \{3, \ldots, 12 \} \). Consequently, bound 1 is smaller than the conjectured bound for all \( n \geq 3 \).

5.3: The case \( n - k \mid \delta \) and \( k = \delta + 1 \)

Since here \( n = \delta + k = 2 \delta + 1 \), one has only to consider odd values for \( n \). For \( n = 3 \), one has \( \left( \frac{2^{n-1}}{n-2} \right)^{2n-1} < 2^{n-4} \) and the left hand side is increasing by the factor \( \frac{2n+1)! \cdot (n-2)! \cdot (n+1)!}{(n-1)! \cdot (n+2)! \cdot (2n)!} = \frac{2n+1)! \cdot 2n \cdot 2n \cdot 2n \cdot 2}{(n-1)! \cdot (n+1)! \cdot (2n)!} < 4^n \). Thus, it only remains to consider \( (n, n + 1)/2, (n - 1)/2 \) convolutional codes for \( n \in \{3, 5, 7, 9, 11, 13, 15 \} \). Since for \( n = 3 \), one has \( \gamma = 4 < 5 \), the conjecture does not hold for this parameter. For the other values, one could compute directly that bound 1 is in all cases larger than the conjectured bound but bound 2 is always smaller than the conjectured bound.

Step 6: Comparison with \( B_\gamma \) for the cases in which bound 1 is larger than the bound from Conjecture 1

We have to consider \( (n, n + 1)/2, (n - 1)/2 \) convolutional codes for \( n \in \{3, 5, 7, 9, 11, 13, 15 \} \). For \( n = 3 \), \( B_\gamma = 4 \), bound 1 is equal to 5 and bound 2 is equal to 2. For \( n = 5 \), \( B_\gamma > \frac{1}{2} \cdot (2n - 2)^2 \cdot (n^2 - 3) \) is larger than bound 1 and since it is growing more rapidly in \( n \) than \( n \), it is larger than bound 1 for \( n \geq 5 \) (it is growing with factor \( \frac{2n+1)! \cdot (n-3)! \cdot (n+2)!}{(n-2)! \cdot (n+4)! \cdot (2n+1)!} = \frac{2n+1)! \cdot 2n \cdot 2n \cdot 2n \cdot 2}{(n-2)! \cdot (n+4)!} > \frac{2n+1)! \cdot 2n \cdot 2n \cdot 2n \cdot 2}{(n-2)! \cdot (n+4)!} \), which is the growing factor of bound 1).

Step 7: Comparison with exact minimal values for superregularity

Relevant are codes whose parameters fulfill \( (L + 1)(n + 1) + k + r - 1 \leq 10 \) and \( L \geq 1 \) (since the case \( L = 0 \) was already considered before). Hence one has to investigate the cases \( (3, 2, 1), (4, 3, 2), (5, 3, 2), (5, 4, 1), (6, 5, 1) \) and \( (6, 4, 2) \). For \( (5, 3, 2) \), the exact minimal value for superregularity yields \( \int F \geq 31 \), bound 1 yields \( \int F \geq 37 \), the conjectured bound yields \( \int F \geq 67 \), bound 2 yields \( \int F \geq 87 \) and \( B_\gamma \) yields \( \int F \geq 233 \). For \( (3, 2, 1) \), the exact minimal value for superregularity yields \( \int F \geq 5 \), which is the
bound as using $B_γ$. As seen in the preceding step, bound 1 yields here $|F| \geq 7$ and bound 2 gives $|F| \geq 3$, which is optimal (the conjecture cannot be applied here since $γ = 4 < 5$). For $(4, 3, 2), (5, 4, 1)$ and $(6, 5, 1)$ bound 1 is better than using the minimal value for superregularity. Finally, for $(6, 4, 2)$, the minimal value for superregularity lies between bound 2 and bound 1.

\[\square\]

**Remark 11** For $(n, n - 1, δ)$ with $δ \leq n - 2$, even the bound $(e - 1) \cdot n^δ \cdot δ!$ is smaller than the conjectured bound $2^{(δ + 1)(n - 1) - 2}$.

**Proof** For a given degree $δ$, the smallest possible value for $n$ fulfilling the restrictions is $n = δ + 2$. In this case and as long as $δ \geq 2$ (for $δ = 1$, the problem is solved anyway), $(e - 1) \cdot n^δ \cdot δ! = (e - 1) \cdot (δ + 2)^δ \cdot δ!$ is smaller than $2^{(δ + 1)(n - 1) - 2} = 2^{δ(δ + 2) - 1}$. This is true since for $δ = 2$, one has $(e - 1) \cdot 32 < 2^7$ and the bound increases with factor $(δ + 1)(δ + 2) \left(\frac{δ + 3}{δ + 2}\right)^δ$ when $δ$ increases by 1, while the conjecture increases with factor $2^{2δ+4}$, which is larger because $2^δ > \left(\frac{δ + 3}{δ + 2}\right)^δ$ and $8 \cdot 2^δ > (δ + 1)(δ + 2)$.

Since the conjectured bound increases with factor $2^{δ+1}$ when $n$ increases, and our new bound only with factor $(1 + 1/n)^δ$, the new bound is better for all $2 \leq δ \leq n - 2$. \[\square\]

### 7.3 Comparison of bounds for arbitrary parameters

In this subsection, we only consider cases where $\max(k, n - k) \leq δ$ since the other cases were already considered before. Using again the duality result from Theorem 3, for $B_γ$ as well as for the bounds of Theorem 14, one could take the minimum of the values for $(n, k, δ)$ and $(n, n - k, δ)$ to get the best possible bound.

**Theorem 24** For all parameters with $δ \geq \max\{k, n - k\}$ but

- $(2, 1, δ)$ with $δ$ arbitrary,
- $(3, k, δ)$ with $k \in \{1, 2\}$, $δ \in \{2, 3, 4, 5\}$,
- $(4, 2, δ)$ with $δ \in \{2, 4\}$,
- $(5, k, 3)$ with $k \in \{2, 3\}$

the bounds of Theorem 14 are able to improve $B_γ$.

**Proof** Using (amongst others) the Stirling formula, one gets

$$B_γ > 1/2 \cdot \frac{1}{2(L + 1)(n - 1)} \cdot \frac{2^{2((L+1)(n-1)-1)}}{\sqrt{π((L + 1)(n - 1) - 1)}} > \frac{2^{2((L+1)(n-1)-1)}}{4\sqrt{π((L + 1)(n - 1) - 1)}^{3/2}}$$

and

$$\left(\frac{(L + 1)n}{(L + 1)(n - k)}\right)^{(L + 1)(n - k)} < (L + 1)(n - k) \cdot \frac{2^{(L+1)n}}{\sqrt{π((L + 1)(n - 1))/2}} \leq \sqrt{2(L + 1)(n - 1)} \cdot \frac{2^{(L+1)n}}{\sqrt{π}}$$

Therefore, in order to get $M_1 < B_γ$, it is sufficient if

$$\sqrt{2} \cdot 2^{L+5}((L + 1)(n - 1))^2 \leq 2^{(L+1)(n-1)}.$$

It is sufficient to consider the case $L \geq 2$, which is implied by $n - k \leq δ$ and $k \leq δ$. 

\[\square\]
For \( n = 2 \), it is clear that above inequality is not fulfilled for all \( L \geq 2 \).
For \( n = 3 \), it is fulfilled for \( L \geq 14 \) (and not for \( L \leq 13 \)) (Mathematica).
For \( n = 4 \), it is fulfilled for \( L \geq 6 \) (and not for \( L \leq 5 \)) (Mathematica).
For \( n = 5 \), it is fulfilled for \( L \geq 4 \) (and not for \( L \leq 3 \)) (Mathematica).
For \( n = 6 \), it is fulfilled for \( L \geq 3 \) (and not for \( L \leq 2 \)) (Mathematica).
For \( n \geq 7 \), it is fulfilled for all \( L \geq 2 \) (Mathematica).

(One can show with Mathematica that it is fulfilled for \( L \geq 2 \) and \( n = 7 \). When switching from \( n \) to \( n + 1 \) the left hand side is growing by the factor \( \left( \frac{n}{n-1} \right)^2 \leq 4 \), while the right hand side is growing by the factor \( 2^{L+1} \geq 8 \). Therefore, the inequality is fulfilled for \( L \geq 2 \) and \( n \geq 7 \).)

Since the inequality is only sufficient, it is possible that \( M_1 \) is better than \( B_\gamma \) also in other cases than those mentioned above. We check this in the following by computing the bounds directly with Mathematica:

For \( n = 2 \), \( B_\gamma \) is better then \( M_1 \).
For \( n = 3 \) and \( L \geq 9 \), \( M_1 \) is better and for \( L \leq 7 \), \( B_\gamma \) is better (\( L = 8 \) is not possible with \( n = 3 \)).
For \( n = 4 \) and \( L = 5 \), \( M_1 \) is better than \( B_\gamma \). For \( n = 4 \) and \( L = 4 \), \( B_\gamma \) is better than \( M_1 \) if \( k = 2 \) and \( \delta = 4 \) and \( M_1 \) is better in the other cases. \( L = 3 \) is not possible with \( n = 4 \) and for \( n = 4 \) and \( L = 2 \), \( B_\gamma \) is better for \( \delta = 2 \) and \( M_1 \) is better for \( \delta = 3 \).
For \( n = 5 \) and \( L = 3 \), \( M_1 \) is better than \( B_\gamma \), and for \( n = 5 \) and \( L = 2 \), \( B_\gamma \) is better then \( M_1 \).
For \( n = 6 \) and \( L = 2 \), \( M_1 \) is better than \( B_\gamma \).

In all cases for which \( B_\gamma \) is better than \( M_1 \) it is also better than \( M_2 \) and \( M_3 \) (Mathematica). Thus, for the following code parameters we are not able to improve \( B_\gamma \) with the above new bounds (only cases were \( \max(k, n - k) \leq \delta \), other case was already considered before):

\[
(2, 1, \delta) \text{ with } \delta \text{ arbitrary},
(3, k, \delta) \text{ with } k \in \{1, 2\}, \delta \in \{2, 3, 4, 5\},
(4, 2, \delta) \text{ with } \delta \in \{2, 4\},
(5, k, 3) \text{ with } k \in \{2, 3\}
\]

Finally, we will again have a look on some of the examples for MDP convolutional codes of rate \( (n-1)/n \) from the end of Sect. 3 to see to what extend improvement has been possible. To this end, we denote by \( B \) the best bound that we could obtain for given code parameters.

One could see that the factor by which we are able to improve the upper bound for the necessary field size for MDP convolutional codes increases rapidly with the size of the code parameters. Especially, if \( \delta < n - 1 \) and we could use the stronger bounds from Sect. 6, the improvement is enormous (Table 6).

### 8 Conclusion

In this paper, bounds for the probability and the necessary field size for MDP and complete MDP convolutional codes have been shown. Moreover, it has been proven that these bounds on the field size are able to improve the already existing bounds. However, it is clear that these bounds are not optimal and they do not lead to concrete constructions of codes. Hence, this paper could be considered as one step forward towards solving the big problem of determining...
the exact minimum field size for the existence of MDP and complete MDP convolutional codes and providing constructions of these codes over fields of possibly small size.

References

1. Almeida P.J., Napp D., Pinto R.: Superregular matrices and applications to convolutional codes. Linear Algebra Appl. 499, 1–25 (2016).
2. Almeida P.J., Napp D., Pinto R.: A new class of superregular matrices and MDP convolutional codes. Linear Algebra Appl. 439, 2145–2157 (2013).
3. Barbero A., Ytrehus O.: Rate \((n − 1)/n\) systematic memory maximum distance separable convolutional codes. IEEE Trans. Inf. Theory 64(4), 3018–3030 (2018).
4. Gluesing-Luerssen H., Rosenthal J., Smarandache R.: Strongly-MDS convolutional codes. IEEE Trans. Inf. Theory 52(2), 584–598 (2006).
5. Hutchinson R.: The existence of strongly MDS convolutional codes. SIAM J. Control Optim. 47, 2812–2826 (2008).
6. Hutchinson R., Rosenthal J., Smarandache R.: Convolutional codes with maximum distance profile. Syst. Control Lett. 54, 53–63 (2005).
7. Hutchinson R., Smarandache R., Trumpf J.: On superregular matrices and MDP convolutional codes. Linear Algebra Appl. 428, 2585–2596 (2008).
8. Lieb J.: Complete MDP convolutional codes. J. Algebra Appl. arXiv:1712.08767 (2018).
9. Lieb J.: Counting Polynomial Matrices over Finite Fields. Matrices with Certain Primeness Properties and Applications to Linear Systems and Coding Theory (Dissertation), Wuerzburg University Press. (2017). https://www.bod.de/buchshop/counting-polynomial-matrices-over-finite-fields-julia-lieb-9783958260641.
10. Lieb J.: The probability of primeness for specially structured polynomial matrices over finite fields with applications to linear systems and convolutional codes. Math. Control Signals Syst. 29, 8 (2017). https://doi.org/10.1007/s00498-017-0191-z.
11. Napp D., Smarandache R.: Constructing strongly MDS convolutional codes with maximum distance profile. Adv. Math. Commun. 10(2), 275–290 (2016).
12. Rosenthal J.: Connections between linear systems and convolutional codes. In: Marcus B., Rosenthal J. (eds.) Codes, Systems and Graphical Models IMA, vol. 123, pp. 39–66 (2001).
13. Rosenthal J., Smarandache R.: Maximum distance separable convolutional codes. Appl. Algebra Eng. Commun. Comput. 10, 15–32 (1999).
14. Schwartz J.T.: Fast probabilistic algorithms for verification of polynomial identities. J. ACM 27(4), 701–717 (1980).
15. Tomas V., Rosenthal J., Smarandache R.: Decoding of convolutional codes over the erasure channel. IEEE Trans. Inf. Theory 58(1), 90–108 (2012).
Publisher’s Note  Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.