An Algebraic Approach for Decoding Spread Codes

E. Gorla ∗1, F. Manganiello2 and J. Rosenthal †2

1Mathematics Institute, University of Basel
2Mathematics Institute, University of Zürich

July 28, 2011

Abstract

We present a family of constant–dimension codes for random linear network coding called spread codes. This is a family of optimal codes with maximum minimum distance. A spread code is constructed starting from the algebra defined by the companion matrix of an irreducible polynomial. We give a minimum distance decoding algorithm that is particularly efficient when the dimension of the codewords is small. The decoding algorithm takes advantage of the structure of the algebra and it uses an original result on minors of a matrix and the factorization of polynomials over finite fields.

1 Introduction

Network coding is a branch of coding theory that arose in 2000 in the work by Ahlswede, Cai, Li and Yeung [ACLY00]. One is interested in multicast communication, i.e., a set of sources $S$ communicating with a set of sinks $R$, over a network which is represented by a directed multigraph. Multicast communication is used nowadays and it is often employed in Internet protocol applications of streaming media, digital television and peer–to–peer networking.

The goal of this communication is to achieve the maximal rate of communication, which, by words, corresponds to the maximal amount of messages per transmission, meaning per single use of the network. Li, Cai and Yeung in [LYC03] prove that this maximal rate of communication can be achieved in single–source multicast communication using linear network coding provided that the size of the base field is large.

The algebraic aspects of network coding emerged with the work by Kötter and Kschischang [KK08b]. The authors introduced a new setting for random linear network coding. Given the linearity of the combinations, the authors suggest to employ as codewords subspaces of a given vector space. Indeed, subspaces are invariant under taking linear combinations of their elements. Consider $\mathcal{P}(\mathbb{F}_q^n)$ to be the set of all subspaces of $\mathbb{F}_q^n$. This set, together with the subspace distance defined by

$$d(\mathcal{U}, \mathcal{V}) = \dim(\mathcal{U} + \mathcal{V}) - \dim(\mathcal{U} \cap \mathcal{V})$$

for all $\mathcal{U}, \mathcal{V} \in \mathcal{P}(\mathbb{F}_q^n)$,

∗The first author was supported by the Swiss National Science Foundation under grant no. 123393.
†The second and third authors were partially supported by the Swiss National Science Foundation under grant no. 126948.
is actually a metric space. Codes are defined to be subsets of $\mathcal{P}(\mathbb{F}_q^n)$. Constant–dimension codes are codes where codewords have all the same dimension. New notions of errors and erasures compatible with the metric space $(\mathcal{P}(\mathbb{F}_q^n), d)$ are introduced in [KK08b]. Besides, upper and lower bounds for network codes are contained in [KK08b, EV08].

We review here some of the results regarding constructions of constant–dimension codes. The first code construction was introduced by Kötter and Kschischang in [KK08b]. The codes are based on the evaluation of linearized polynomials over a subspace and it is easy to see that this is still a subspace. These codes are called Reed–Solomon like codes for their similarities with Reed–Solomon codes in classical coding theory. The authors present also a list–1 minimum distance decoding algorithm for these codes. In [MV10] the authors introduce codes based on the evaluation of two different linearized polynomials. The obtained codes are then decodable by a list decoding algorithm which was also presented in the same work.

A more general family of codes, which also contains Reed–Solomon like codes, is the subject of the paper [ES09]. The construction is based on binaryc constant–weight codes, Ferrer diagrams and rank–metric codes. A decoding algorithm in this case is on two levels. First one has to decode the constant–weight code and then apply a decoder for rank–metric codes. In [Ska10] the author presents a family of codes that is a sub–family of the one in [ES09]. Another family of codes, this one based on $q$–analog of designs, appears in [KK08a]. The authors were able to find, by computer search, constant–dimension codes based on designs with big cardinality. Spread codes were first introduced by the authors in [MGR08]. The family introduced in [ES09] contains spread codes and it constitutes a generalization of the codes defined in [KK08b], when their distance is maximal.

This work focuses on spread codes which are a family of constant–dimension codes first introduced in [MGR08]. Spreads of $\mathbb{F}_q^n$ are a collection of subspaces of $\mathbb{F}_q^n$, all of the same dimension, which partition the ambient space. Such a family of subspaces of $\mathbb{F}_q^n$ exists if and only if the dimension of the subspaces divides the dimension of the ambient space. The construction of spread codes can be based on the $\mathbb{F}_q$–algebra $\mathbb{F}_q[P]$ where $P \in GL_k(\mathbb{F}_q)$ is the companion matrix of a monic irreducible polynomial of degree $k$. In Definition 2.8 we define spread codes as

$$S = \{\text{rowsp} \ (A_1, \cdots, A_r) \in \mathfrak{S}_{\mathbb{F}_q}(k, n) \mid A_i \in \mathbb{F}_q[P] \forall i \in \{1, \ldots, r\}\}$$

where $\mathfrak{S}_{\mathbb{F}_q}(k, n)$ is the Grassmannian of all subspaces of $\mathbb{F}_q^n$ of dimension $k$.

Since spreads partition the ambient space, spread codes are optimal. More precisely, they have maximal minimum distance $k$ and have the largest possible number of codewords for a code with minumum distance $k$. Indeed, it is possible to check that they achieve the anticode bound presented in [EV08]. This family is closely related to the family of Reed–Solomon like codes introduced in [KK08b]. We discuss the relation in Section 2.1. In Lemma 2.13 we show that it is possible to extend to spread codes the existing decoding algorithms for Reed–Solomon like codes.

The structure of this special family of spreads, helps us in constructing a minimum distance decoding algorithm which is able to correct up to half the minimum distance of $S$. In Lemma 3.1 we reduce the decoding algorithm for a general spread code (i.e., where $n = rk$ with $r > 2$) to at most $r - 1$ instances of the decoding algorithm for the special case $r = 2$.

We focus then on a decoding algorithm for the spread code

$$S = \{\text{rowsp} \ (A_1, A_2) \in \mathfrak{S}_{\mathbb{F}_q}(k, 2k) \mid A_1, A_2 \in \mathbb{F}_q[P]\}.$$
The paper is structured as follows. In Section 2 we focus on the construction of spread codes, also giving their main properties. In Subsection 2.1 we explicitly show the connection between spread codes and Reed–Solomon like codes.

The main results of the paper are contained in Section 3. There we introduce a new minimum distance decoder for spread codes. We compute the complexity of our algorithm and compare it with the complexity of the algorithms in the literature. It turns out that the presented algorithm is more efficient than the one presented in [KK08b] as soon as $k < n^2(n - k)$ and the algorithm performs better than the one presented in [SKK08] as soon as $k^4 < (n - k)^2$. It follows that the algorithm is most suitable in case the dimension $k$ of the code words is small compared to the size $n$ of the ambient space.

2 Definition and first properties

**Definition 2.1** ([Hir98, Section 4.1]). A subset $S \subset \mathbb{S}_F_q(k, n)$ is a spread if it satisfies

- $U \cap V = \{0\}$ for all $U, V \in S$ distinct, and
- $F_n = \bigcup_{U \in S} U$.

**Theorem 2.2** ([Hir98, Theorem 4.1]). A spread exists if and only if $k \mid n$.

We give now a construction of spreads suitable for use in Random Linear Network Coding (RLNC) based on companion matrices.

**Definition 2.3.** Let $F_q$ be a finite field and $p = \sum_{i=1}^k p_i x^i \in F_q[x]$ a monic polynomial. We define the companion matrix of $p$ to be the matrix

$$
\begin{pmatrix}
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & 0 & 1 & \cdots \\
-p_0 & -p_1 & -p_2 & \cdots & -p_{k-1}
\end{pmatrix} \in F_q^{k \times k}.
$$

Let $n = rk$ with $r > 1$, $p \in F_q[x]$ a monic irreducible polynomial of degree $k$ and $P \in F_q^{k \times k}$ its companion matrix.

**Lemma 2.4.** The $F_q$-algebra $F_q[P]$ is a finite field, i.e., $F_q[P] \cong F_{q^k}$.

This is a well–known fact (see [LN94, page 64]).

**Lemma 2.5.** Let $\varphi : F_q^k \to F_q[P]$ be a ring isomorphism. Denoted by $\mathbb{P}^{r-1}(F_q^k) := (F_q^r \setminus \{0\})/\sim$ the projective space, where $\sim$ is the following equivalence relation

$$v \sim w \iff \exists \lambda \in F_q^* \text{ such that } v = \lambda w,$$

where $v, w \in F_q^r \setminus \{0\}$. Then, the map

$$\tilde{\varphi} : \mathbb{P}^{r-1}(F_q^k) \to \mathbb{S}_F_q(k, n)$$

$$[v_1 : \cdots : v_r] \mapsto \text{rowsp} (\varphi(v_1) \cdots \varphi(v_r)).$$

is injective.
Proof. Let \( v = [v_1 : \cdots : v_r], w = [w_1 : \cdots : w_r] \in \mathbb{P}^{r-1}(\mathbb{F}_q^k) \). If \( \tilde{\varphi}(v) = \tilde{\varphi}(w) \) there exists an \( M \in GL_k(\mathbb{F}_q) \) such that
\[
(\varphi(v_1) \cdots \varphi(v_r)) = M (\varphi(w_1) \cdots \varphi(w_r))
\]
\[
= (M \varphi(w_1) \cdots M \varphi(w_r))
\]
(1)
Let \( i_v, i_w \in \{1, \ldots, r\} \) be the least indices such that \( \varphi(v_{i_v}) \neq 0 \) and \( \varphi(w_{i_w}) \neq 0 \). From (1) it follows that \( i_v = i_w \). Since, without loss of generality, we can consider \( v_{i_v} = w_{i_w} = 1 \), it follows that \( \varphi(v_{i_v}) = \varphi(w_{i_w}) = 1 \) and consequently \( M = I \). Then, (1) becomes
\[
(\varphi(v_1) \cdots \varphi(v_r)) = (\varphi(w_1) \cdots \varphi(w_r))
\]
leading to \( v = w \).

\[\Box\]

**Theorem 2.6** ([MGR08, Theorem 1]). \( S := \tilde{\varphi}(\mathbb{P}^{r-1}(\mathbb{F}_q^k)) \) is a spread of \( \mathfrak{S}_{F_q}(k, n) \).

**Definition 2.7** ([MGR08, Definition 2]). We call spread codes of \( \mathfrak{S}_{F_q}(k, n) \) the subsets \( S \subset \mathfrak{S}_{F_q}(k, n) \) from Theorem 2.6.

In order to simplify the notations we consider the following equivalent definition of spread codes.

**Definition 2.8.** Let \( n, k \in \mathbb{N} \) with \( k > 0 \) and \( n = rk \) for some \( r \in \mathbb{N}, r > 1 \). Let \( p \in \mathbb{F}_q[x] \) be a monic irreducible polynomial of degree \( k > 0 \) and \( P \in GL_k(\mathbb{F}_q) \) its companion matrix. Then
\[
S = \{ \text{rowsp} (A_1 \cdots A_r) \in \mathfrak{S}_{F_q}(k, n) \mid A_i \in \mathbb{F}_q[P] \forall i \in \{1, \ldots, r\} \}
\]
is a spread code of \( \mathfrak{S}_{F_q}(k, n) \). Without loss of generality and in order to have a unique representation matrix of the elements of a spread code, we consider the matrices \( (A_1 \cdots A_r) \) to be in row reduced echelon form.

**Lemma 2.9** ([MGR08]). Let \( S \subset \mathfrak{S}_{F_q}(k, n) \) be a spread code. Then

1. \( d(U, V) = d_{\text{min}}(S) = 2k \), for all \( U, V \in S \) distinct, i.e., the code has maximal minimum distance, and
2. \( |S| = \frac{q^n - 1}{q^k - 1} \), i.e., the code has maximal cardinality with respect to the given minimum distance.

### 2.1 Relation with Reed–Solomon like codes

Reed-Solomon-like codes are a class of constant–dimension codes, i.e. codes on \( \mathfrak{S}_{F_q}(k, n) \), introduced in [KK08]. These codes are strictly related to maximal rank distance codes as introduced in [Gab85]. We give here an equivalent definition of these codes.

**Definition 2.10.** Let \( \mathbb{F}_q \subset \mathbb{F}_{q^n} \) be two finite fields. Fix some \( \mathbb{F}_q \)–linearly independent elements \( \alpha_1, \ldots, \alpha_k \in \mathbb{F}_{q^n} \). Let \( r \in \mathbb{N} \) with \( r < k \) and denote with \( L^r_{\mathbb{F}_{q^n}} \subset \mathbb{F}_{q^n}[x] \) the set of linearized polynomials of degree less than \( q^r \), i.e., \( f \in L^r_{\mathbb{F}_{q^n}} \) if and only if \( f = \sum_{i=0}^{r-1} f_i x^i \) for some \( f_i \in \mathbb{F}_{q^n} \). Let \( \psi : \mathbb{F}_{q^n} \to \mathbb{F}_q^n \) be an isomorphism of \( \mathbb{F}_q \) vector spaces. Then a Reed-Solomon-like (RSL) code is defined as
\[
RSL^r_{\mathbb{F}_{q^n}} := \left\{ \text{rowsp} \left( \begin{array}{c} \psi(f(\alpha_1)) \\ \vdots \\ \psi(f(\alpha_k)) \end{array} \right) \right\} \subset \mathfrak{S}_{F_q}(k, k + n).
\]
The following proposition establishes a relation between spread codes and RSL codes.

**Proposition 2.11.** Let \( n = rk, \mathbb{F}_q \subset \mathbb{F}_{q^k} \subset \mathbb{F}_{q^n} \) finite fields, and \( P \in GL_k(\mathbb{F}_q) \) the companion matrix of a monic irreducible polynomial \( p \in \mathbb{F}_q[x] \) of degree \( k > 0 \). Let \( \lambda \in \mathbb{F}_{q^k} \) be a root of \( p, \mu_1, \ldots, \mu_r \in \mathbb{F}_{q^n} \) a basis of \( \mathbb{F}_{q^n} \) over \( \mathbb{F}_{q^k} \). Moreover, let \( \psi : \mathbb{F}_{q^n} \to \mathbb{F}_{q^k}^n \) be the isomorphism of \( \mathbb{F}_q \)-vector spaces which maps the basis \((\lambda^1 \mu_j)_{0 \leq j \leq k-1}\) to the standard basis of \( \mathbb{F}_{q^n} \) over \( \mathbb{F}_q \).

Then for every choice of \( A_0, \ldots, A_{r-1} \in \mathbb{F}_q[P] \) there exists a unique linearized polynomial of the form \( f = ax \) with \( a \in \mathbb{F}_{q^n} \) such that

\[
(A_0 \cdots A_{r-1}) = \begin{pmatrix}
\psi(f(1)) \\
\psi(f(\lambda)) \\
\vdots \\
\psi(f(\lambda^{k-1}))
\end{pmatrix}.
\]

The constant \( a \) is of the form \( a = \psi^{-1}(v) \) where \( v \in \mathbb{F}_{q^k}^n \) is the first row of \( (A_0 \cdots A_{r-1}) \).

**Proof.** We first prove the proposition for \( r = 1 \). Let \( \lambda \in \mathbb{F}_{q^k} \) such that \( p(\lambda) = 0 \). Let \( \psi \) be the following map

\[
\psi : \mathbb{F}_q[\lambda] \to \mathbb{F}_{q^k}
v \mapsto (v_0, \ldots, v_{k-1})
\]

where \( v = \sum_{i=0}^{k-1} v_i \lambda^i \).

Let \( A = (a_{i,j})_{1 \leq i,j \leq k} \in \mathbb{F}_q[P] \). Since

\[
P = \begin{pmatrix}
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & & \ddots & & \vdots \\
0 & 0 & 0 & \cdots & 1 \\
-p_0 & -p_1 & -p_2 & \cdots & -p_{k-1}
\end{pmatrix}
\]

we obtain that \( PA = (\bar{a}_{i,j})_{1 \leq i,j \leq k} \) where

\[
\bar{a}_{i,j} = a_{i+1,j} \text{ for } i \in \{1, \ldots, k-1\}, \text{ and}
\]

\[
\bar{a}_{k,j} = -\sum_{i=1}^{k} a_{i,j} p_{i-1}.
\]

We now prove by induction that for every \( l \in \mathbb{N} \) the relation

\[
P^l = \begin{pmatrix}
\psi(\lambda^l) \\
\vdots \\
\psi(\lambda^{l+k-1})
\end{pmatrix}
\]

holds. For \( l = 0 \), we have that

\[
I = \begin{pmatrix}
\psi(1) \\
\vdots \\
\psi(\lambda^{k-1})
\end{pmatrix}.
\]
Consider the thesis true for \( P^{l-1} = (a_{i,j})_{1 \leq i,j \leq k} \). By \(^{3}\) we obtain that

\[
P^l = PP^{l-1} = \begin{pmatrix}
\psi(\lambda^l) \\
\vdots \\
\psi(\lambda^{l+k-2}) \\
\psi(v)
\end{pmatrix},
\]

where \( \psi(v) = (-\sum_{i=1}^ka_{i,1}p_{i-1}, \ldots, -\sum_{i=1}^ka_{i,k}p_{i-1}) \). By the definition of \( \psi \), it follows that

\[
v = \sum_{j=1}^k \left( -\sum_{i=1}^ka_{i,j}p_{i-1} \right) \lambda^{j-1} = -\sum_{i=1}^kp_{i-1} \left( \sum_{j=1}^ka_{i,j}\lambda^{j-1} \right)
= -\sum_{i=1}^kp_{i-1}\lambda^{l+i-2} = \lambda^{l-1} \left( -\sum_{i=1}^kp_{i-1}\lambda^{i-1} \right) = \lambda^{l+k-1}.
\]

We are now ready to prove the theorem for \( r = 1 \) using \(^{4}\). Let \( A \in \mathbb{F}_q[P] \), then there exists a polynomial \( g = \sum_{i=0}^{k-1} g_i x^i \in \mathbb{F}_q[x] \) such that \( g(P) = A \), then

\[
A = g(P) = \sum_{i=0}^{k-1} g_i P^i = \sum_{i=0}^{k-1} g_i \begin{pmatrix}
\psi(\lambda^i) \\
\vdots \\
\psi(\lambda^{i+k-1})
\end{pmatrix}
= \begin{pmatrix}
\sum_{i=0}^{k-1} g_i \psi(\lambda^i) \\
\vdots \\
\sum_{i=0}^{k-1} g_i \psi(\lambda^{i+k-1})
\end{pmatrix} = \begin{pmatrix}
\psi(\sum_{i=0}^{k-1} g_i\lambda^i) \\
\vdots \\
\psi(\sum_{i=0}^{k-1} g_i\lambda^{i+k-1})
\end{pmatrix}
= \begin{pmatrix}
\psi(\sum_{i=0}^{k-1} g_i\lambda^i) \\
\vdots \\
\psi(\sum_{i=0}^{k-1} g_i\lambda^{k-1})
\end{pmatrix} = \begin{pmatrix}
\psi(f(1)) \\
\vdots \\
\psi(f(\lambda^{k-1}))
\end{pmatrix}
\]

where \( f = ax \) and \( a = \sum_{i=0}^{k-1} g_i\lambda^i \). We deduce that the entries of the first row of \( A \) correspond to the coefficients of \( g \).

Let \( n = rk \) with \( r > 1 \). The map \( \psi \) defined in the theorem satisfies the following diagram

\[
\begin{array}{ccc}
\mathbb{F}_q^n & \xrightarrow{\psi} & \mathbb{F}_q^n \\
\psi_1 \downarrow & & \downarrow \psi_2 \\
\mathbb{F}_q^r & \xrightarrow{\psi} & \mathbb{F}_q^r
\end{array}
\]

where the maps \( \psi_1, \psi_2 \) are defined as follows:

- \( \psi_1(v) = (v_1, \ldots, v_r) \) where \( v = \sum_{i=1}^r v_i\mu_i \), and
- \( \psi_2((v_1, \ldots, v_r)) = (\tilde{\psi}(v_1), \ldots, \tilde{\psi}(v_r)) \), where \( \tilde{\psi} \) is the map \(^{2}\).
For any \( i \in \{1, \ldots, r\} \), since \( A_i \in \mathbb{F}_q[P] \), there exists an \( a_i \in \mathbb{F}_{q^k} \) such that

\[
A_i = \begin{pmatrix}
\tilde{\psi}(a_i) \\
\vdots \\
\tilde{\psi}(a_i \lambda^{k-1})
\end{pmatrix}.
\]

Let \( a \in \mathbb{F}_{q^n} \) be such that \( \psi(a) \) corresponds to the first row of the matrix \((A_1 \; \cdots \; A_r)\). By the \( \mathbb{F}_{q^k} \) linearity of \( \psi_1 \) we obtain that

\[
\begin{pmatrix}
\psi(a) \\
\vdots \\
\psi(a \lambda^{k-1})
\end{pmatrix} = \begin{pmatrix}
\psi_2(\psi_1(a)) \\
\vdots \\
\psi_2(\psi_1(a \lambda^{k-1}))
\end{pmatrix} = \begin{pmatrix}
\psi_2(a_1, \ldots, a_r) \\
\vdots \\
\psi_2(a_1 \lambda^{k-1}, \ldots, a_1 \lambda^{k-1})
\end{pmatrix} = \begin{pmatrix}
\tilde{\psi}(a_1) & \cdots & \tilde{\psi}(a_r) \\
\vdots & \ddots & \vdots \\
\tilde{\psi}(a_1 \lambda^{k-1}) & \cdots & \tilde{\psi}(a_r \lambda^{k-1})
\end{pmatrix} = (A_1 \; \cdots \; A_r).
\]

The following corollary shows the explicit relation between spread codes and RSL codes.

**Corollary 2.12.** Let \( \psi_1 : \mathbb{F}_q^{(r-i)k} \to \mathbb{F}_q^{(r-i)k} \) be isomorphisms of vector spaces that map the basis \((\lambda^j \mu_i)_{0 \leq j \leq k-1}^{1 \leq i \leq r-i}\) to the standard basis of \( \mathbb{F}_q^{(r-i)k} \), \( \mu_1, \ldots, \mu_{r-i} \) a basis of \( \mathbb{F}_q^{(r-i)k} \) over \( \mathbb{F}_q \). Then,

\[
S = \bigcup_{i=1}^r \left\{ \text{rowsp} \begin{pmatrix} 0 & \cdots & 0 & I & \cdots & \psi_i(f(1)) \end{pmatrix} \middle| f = ax, \ a \in \mathbb{F}_q^{(r-i)k} \right\}
\]

**Lemma 2.13.** Let \( S \) be a spread code, and \( \mathcal{R} = \text{rowsp} (R_1 \; \cdots \; R_r) \in \mathcal{G}_{\mathbb{F}_q} (k, rk) \). Assume there exists a \( C = \text{rowsp} (C_1 \; \cdots \; C_r) \in S \) such that \( d(\mathcal{R}, C) < \frac{d(S)}{2} = k \). Let \( i := \min \{ j \in \{1, \ldots, r\} \mid \text{rank}(R_j) > \frac{k-1}{2} \} \). It holds that

- \( C_j = 0 \) for \( 1 \leq j < i \),
- \( C_i = I \), and
- \( d(\text{rowsp} (R_1 \; R_{i+1} \; \cdots \; R_r), \text{rowsp} (I \; C_{i+1} \; \cdots \; C_r)) < k \).

Lemma 2.13 follows from Lemma 3.1, which we prove in the next section. This lemma allows us to decode spread codes using a decoding algorithm for RSL codes. Examples of decoding algorithms for RSL codes can be found in \[\text{Gab85}, \text{KK08b}, \text{SKK08}\].

Another interesting application of Lemma 2.13 allows to improve the efficiency of the decoding algorithm for the codes proposed in \[\text{Ska10}\]. For the relevant definitions, we refer the interested reader to the original article.

**Corollary 2.14.** There is an algorithm which decodes the codes from \[\text{Ska10}\] and has complexity \( O_{\mathbb{F}_q^{n-k}}(k(n-k)) \), i.e., it performs \( O(k(n-k)) \) field operations in \( \mathbb{F}_q^{n-k} \).
Proof. The algorithm is as follows. In order to decide the position of the identity matrix, thanks to Lemma 2.13, one computes the rank of the $k \times k$ blocks of the received matrix. Then one applies the decoding algorithm from [SKK08]. The complexity of computing the row reduced echelon forms is $O_{\mathbb{F}_q}(nk^2)$ and the complexity of the decoding algorithm by Silva, Kschischang, and Kötter is $O_{\mathbb{F}_q}(k(n-k)) = O_{\mathbb{F}_q}(k(n-k)^3)$. Since $n-k \geq k$, the complexity of the decoding algorithm is the dominant term. Therefore, we can decode the codes from [Ska10] with $O(k(n-k))$ operations over $\mathbb{F}_{q^{n-k}}$, or $O(k(n-k)^3)$ operations over $\mathbb{F}_q$. 

The algorithm from Corollary 2.14 is given in pseudocode in Algorithm 1.

**Algorithm 1:** Decoding algorithm for codes proposed in [Ska10].

```plaintext
input : $\mathcal{R} = \text{rowsp} \left( R_1 \, \cdots \, R_r \, \vec{R} \right) \in \mathfrak{S}_{\mathbb{F}_q}(k,n)$
where $R_j \in \mathbb{F}_q^{k \times k}$ and $\vec{R} \in \mathbb{F}_q^{k \times (n-rk)}$ where $r = \left\lfloor \frac{n}{k} \right\rfloor$.

output: $C \in S \subset \mathfrak{S}_{\mathbb{F}_q}(k,n)$ such that $d(\mathcal{R}, C) < k$, if such a $C$ exists.

$i := 1;\\
\text{while } \text{rank}(R_i) \leq \frac{k-1}{2} \text{ and } i \leq r \text{ do } i = i + 1;\\
\text{if } i \leq r \text{ then }\\
\quad \text{Find } C \in \mathbb{F}_q^{k \times n-ik} \text{ such that } d(\text{rowsp} \left( R_i \, \cdots \, R_r \, \vec{R} \right), \text{rowsp} \left( I \, C \right)) < k \text{ using a minimum distance decoder for } RSL_{\mathbb{F}_q}^{k \times n-ik}, \text{ if such a } C \text{ exists;}\\
\text{return } C := \text{rowsp} \left( 0 \, \cdots \, 0 \, I \, C \right) \in \mathfrak{S}_{\mathbb{F}_q}(k,n);\\
\text{else }\\
\quad \text{return there exists no } C \in S \text{ such that } d(\mathcal{R}, C) < k;\\
\text{end}
```

3 Decoding Algorithm

Throughout this section let $\mathbb{F}_q$ be a finite field, $p \in \mathbb{F}_q[x]$ a monic irreducible polynomial of degree $k > 0$ and $P \in GL_k(\mathbb{F}_q)$ its companion matrix. Let $S \in GL_k(\mathbb{F}_q^k)$ be a matrix diagonalizing $P$, i.e., $S^{-1}PS = \text{diag}(\lambda, \lambda^q, \ldots, \lambda^{q^{k-1}})$ with $\lambda \in \mathbb{F}_q^k$ a root of $p$.

In this section we provide a minimum distance decoding algorithm for spread codes. The following lemma shows how to reduce the minimum distance decoding algorithm in the general case, i.e., $n = rk$, to at most $r-1$ instances of the same procedure for $n = 2k$ that can be run in parallel.

**Lemma 3.1.** Let $S$ be a spread code, and $\mathcal{R} = \text{rowsp} \left( R_1 \, \cdots \, R_r \right) \in \mathfrak{S}_{\mathbb{F}_q}(k,rk)$. Assume there exists a $C = \text{rowsp} \left( C_1 \, \cdots \, C_r \right) \in S$ such that $d(\mathcal{R}, C) < k$. It holds

$$
C_i = 0 \iff \text{rank}(R_i) \leq \frac{k-1}{2}.
$$
Proof. ⇒ Let \( i \in \{1, \ldots, r\} \) be an index such that \( C_i = 0 \). By the construction of a spread code there exists a \( j \in \{1, \ldots, r\} \) with \( C_j = I \). It follows that
\[
\operatorname{rank}\left( \begin{array}{cc} 0 & I \\ R_i \\ R_j \end{array} \right) \leq \operatorname{rank}\left( \begin{array}{ccc} C_1 & \cdots & C_r \\ R_1 & \cdots & R_r \end{array} \right) < \frac{3k}{2} \Rightarrow \operatorname{rank}(R_i) < \frac{k}{2}.
\]

⇐ Let \( i \in \{1, \ldots, r\} \) be such that \( \operatorname{rank}(R_i) \leq \frac{k-1}{2} \) and assume by contradiction that \( C_i \in \mathbb{F}_q[P]^* \). It follows that
\[
\dim(C \cap R) \leq \dim(\text{rowsp}(C_i) \cap \text{rowsp}(R_i)) = \dim(\text{rowsp}(R_i)) \leq \frac{k-1}{2}
\]
which contradicts the assumption that \( d(C, R) = 2k - 2 \dim(C \cap R) < k \).

Algorithm 3 on page 23 is based on this lemma.

Lemma 2.13 now follows from Lemma 3.1 and from the observation that \( d(C, R) \geq d(\text{rowsp}(C_i) \cap \text{rowsp}(R_i), \text{rowsp}(R_1, \cdots, R_r)) \).

We can now focus on specifying a minimum distance decoding algorithm for the case where \( n = 2k \), i.e.,
\[
S = \{ \text{rowsp } (I \ A) \mid A \in \mathbb{F}_q[P] \} \cup \{ \text{rowsp } (0 \ I) \}
\]
where \( I \) and \( 0 \) are respectively the identity and the zero matrix of size \( k \times k \).

Since a minimum-distance decoding algorithm decodes uniquely up to half the minimum distance, we are interested in writing an algorithm with the following specifications.

**input:** \( R = \text{rowsp } (R_1 \ R_2) \in \mathcal{G}_{\mathbb{F}_q}(k, 2k) \),
\( P \in \text{GL}_k(\mathbb{F}_q) \) the companion matrix of \( p \in \mathbb{F}_q[x] \) and
\( S \in \text{GL}_k(\mathbb{F}_q) \) its diagonalizing matrix.

**output:** \( C \in S \subset \mathcal{G}_{\mathbb{F}_q}(k, 2k) \) such that \( d(R, C) < \frac{d(S)}{2} = k \), if such a \( C \) exists.

We now first give a membership criterion for spread codes.

**Lemma 3.2** (Membership Criterion). Let \( A \in \text{GL}_k(\mathbb{F}_q) \cup \{0\} \). Then the following statements are equivalent.
1. \( A \in \mathbb{F}_q[P] \).
2. \( S^{-1}AS \) is a diagonal matrix.
3. \( AP = PA \).

More specifically, \( S^{-1}AS = \text{diag}(\lambda_A, \lambda_A^q, \ldots, \lambda_A^{q^{k-1}}) \) for some \( \lambda_A \in \mathbb{F}_q \).

Based on this lemma we give a membership criterion.

**Corollary 3.3** (Membership Criterion). Let \( R = \text{rowsp } (R_1 \ R_2) \in \mathcal{G}_{\mathbb{F}_q}(k, 2k) \). Then \( R \in S \) if and only if either \( R_1 \in \text{GL}_k(\mathbb{F}_q) \) and \( S^{-1}R_1^{-1}R_2S \) is diagonal or \( R_1 = 0 \) and \( R_2 \in \text{GL}_k(\mathbb{F}_q) \).
Proof. \( \Rightarrow \) This implication is a direct consequence of the definition of a spread code and Lemma 3.2.

\( \Leftarrow \) If \( R_1 = 0 \) and \( R_2 \in GL_k(\mathbb{F}_q) \), it follows that \( \text{rowsp} \left( R_1 \quad R_2 \right) = \text{rowsp} \left( 0 \quad I \right) \in S \). If instead \( R_1 \in GL_k(\mathbb{F}_q) \), then

\[
\text{rowsp} \left( R_1 \quad R_2 \right) = \text{rowsp} \left( I \quad R_1^{-1}R_2 \right) \in S
\]

since by Lemma 3.2 \( R_1^{-1}R_2 \in \mathbb{F}_q[P] \) if and only if \( S^{-1}R_1^{-1}R_2S \) is a diagonal matrix.

\( \square \)

Definition 3.4. We say that a vector space \( R \in \mathcal{G}_{\mathbb{F}_q}(k, 2k) \) is uniquely decodable by the spread code \( S \subset \mathcal{G}_{\mathbb{F}_q}(k, n) \) if

\[
\text{there exists a } C \in S \text{ such that } d(R, C) < \frac{d(S)}{2} = k.
\] (5)

We can state the following corollary of Lemma 3.1.

Corollary 3.5. Consider \( R \in \mathcal{G}_{\mathbb{F}_q}(k, 2k) \) satisfying (5). The following are equivalent:

- \( \text{rank} \left( R_1 \right) \leq \frac{k-1}{2} \), and
- the output of a minimum distance decoder is \( \text{rowsp} \left( 0 \quad I \right) \).

A similar statement holds for \( R_2 \).

Therefore we can restrict our decoding algorithm to look for codewords of the form \( C = \text{rowsp} \left( I \quad A \right) \) where \( A \in \mathbb{F}_q[P] \). Since there is an obvious symmetry in the construction of a spread code we can without loss of generality assume that

\[
\text{rank}(R_1) \geq \text{rank}(R_2) > \frac{k - 1}{2}.
\]

With the following theorem we translate Condition (5) into a rank condition, and then into a greatest common divisor condition. Let \( M \) be a matrix of size \( k \times k \) and let \( J = (j_1, \ldots, j_s) \), \( L = (l_1, \ldots, l_s) \in \{1, \ldots, k\}^s \). We denote by \( (J; L)_M \) the minor of the matrix \( M \) corresponding to the submatrix \( (J; L)_M \) with row indices \( j_1, \ldots, j_s \) and column indices \( l_1, \ldots, l_s \). We skip the suffix \( M \) when the parent matrix is clear from the context. We are now ready to state the next result.

Theorem 3.6. Let \( R \in \mathcal{G}_{\mathbb{F}_q}(k, n) \) be a subspace with

\[
\text{rank}(R_1) \geq \text{rank}(R_2) > \frac{k - 1}{2}.
\]

The following are equivalent:

- \( R \) satisfies (5).
- Let \( \Delta(x) := \text{diag} \left( x, x^q, x^{q^2}, \ldots, x^{q^{k-1}} \right) \), then there exists a unique \( \mu \in \mathbb{F}_{q^k} \) such that

\[
\text{rank} \left( S^{-1}R_1S\Delta(\mu) - S^{-1}R_2S \right) \leq \frac{k - 1}{2}
\] (6)

Theorem 3.6.
• \(x - \mu = \gcd \left( \{ [J; L]_{S^{-1}R_1S\Delta(x)-S^{-1}R_2S} \mid J, L \in \{1, \ldots, k\}^{\frac{k+1}{2}} \} , x^{q^k} - x \right), \) for some \( \mu \in \mathbb{F}_{q^k} \).

Proof. The property that \( R \) satisfies \([\mathbf{x}] \) is equivalent to the existence of a unique matrix \( X \in \mathbb{F}_q[P] \) such that

\[
k - 1 \geq d(R, C) = 2 \text{rank} \begin{pmatrix} I & X \\ R_1 & R_2 \end{pmatrix} - 2k
\]

\[
= 2 \text{rank} \begin{pmatrix} I & X \\ 0 & R_1X - R_2 \end{pmatrix} - 2k = 2 \text{rank}(R_1X - R_2).
\]

Furthermore we get that \( \text{rank}(R_1X - R_2) = \text{rank}(S^{-1}R_1S\Delta(x) - S^{-1}R_2S) \) where \( \Delta(x) := S^{-1}XS = \text{diag}(x, x^q, \ldots, x^{q^{k-1}}) \) is a consequence of Lemma \(3.2 \). The existence of a unique solution \( X \in \mathbb{F}_q[P] \) is then equivalent to the existence of a unique \( \mu \in \mathbb{F}_{q^k} \) such that

\[
\text{rank}(S^{-1}R_1S\Delta(\mu) - S^{-1}R_2S) \leq \frac{k - 1}{2}.
\]

This is equivalent to the condition that all minors of size \( \frac{k+1}{2} \) of \( S^{-1}R_1S\Delta(\mu) - S^{-1}R_2S \) are zero. This leads to a nonempty system of polynomials in the variable \( x \) having a unique solution \( \mu \in \mathbb{F}_{q^k} \). Therefore

\[
x - \mu \mid \gcd \left( \{ [J; L]_{S^{-1}R_1S\Delta(x)-S^{-1}R_2S} \mid J, L \in \{1, \ldots, k\}^{\frac{k+1}{2}} \} , x^{q^k} - x \right).
\]

Equality follows from the uniqueness of \( \mu \).

As a corollary one gets the following decoding algorithm. First compute all \( \left( \frac{k}{\frac{k+1}{2}} \right)^2 \) minors of size \( \frac{k+1}{2} \) of \( S^{-1}R_1S\Delta(x) - S^{-1}R_2S \), then compute their greatest common divisor with \( x^{q^k} - x \). In order to decrease the complexity of this first approach we can focus on the factorization of only one non zero minor.

Remark 3.7. Fix \( J, L \in \{1, \ldots, k\}^{\frac{k+1}{2}} \) such that \( [J; L]_{S^{-1}R_1S\Delta(x)-S^{-1}R_2S} \neq 0 \). If \( \mu \in \mathbb{F}_{q^k} \) is the unique element satisfying the equivalent conditions of Theorem 3.6 then

\[
x - \mu \mid \gcd \left( [J; L]_{S^{-1}R_1S\Delta(x)-S^{-1}R_2S} , x^{q^k} - x \right).
\]

The greatest common divisor \( \gcd \left( [I; J]_{S^{-1}R_1S\Delta(x)-S^{-1}R_2S} , x^{q^k} - x \right) \) is in general non linear, leading to possible multiple solutions over \( \mathbb{F}_{q^k} \). In order to find the unique one satisfying the rank condition we compute

\[
\text{rank}(S^{-1}R_1S\Delta(\mu) - S^{-1}R_2S)
\]

for all \( \mu \in \mathbb{F}_{q^k} \) such that \( x - \mu \mid \gcd \left( [I; J]_{S^{-1}R_1S\Delta(x)-S^{-1}R_2S} , x^{q^k} - x \right) \).

We still can do more in order to reduce the complexity of the algorithm. In the sequel we will:

• eliminate the computation of the greatest common divisor, and
• polynomially bound the number of checks we have to perform.

The following subsection is devoted to finding a minor suitable for our purpose.
3.1 Existence of a suitable polynomial

We now introduce some operations on tuples that we will use later in this subsection. Let $I = (i_1, \ldots, i_s) \in \{1, \ldots, k\}^s$.

- $i \in I$ means that $i \in \{i_1, \ldots, i_s\}$.
- $L \subset I$ means that $L = (i_1, \ldots, i_l)$ for $1 \leq l_1 < \cdots < l_k \leq s$.
- $|I| := s$ is the length of the tuple.
- $I \cap J$ denotes the $L \subset I, J$ such that $|L|$ is maximal.
- If $J = (j_1, \ldots, j_r)$ then $I \cup J := (i_1, \ldots, i_s, j_1, \ldots, j_r)$, i.e., $\cup$ denotes the concatenation of tuples.
- If $J \subset I$ then $I \setminus J$ denotes the $L \subset I$ with $|L|$ maximal such that $J \cap L = \emptyset$ where $\emptyset$ is the empty tuple.
- $\min I = \min\{i \mid i \in I\}$, with the convention that $\min \emptyset > \min I$ for any $I$.

In this subsection we prove the following theorem.

**Theorem 3.8.** Let $\mathcal{R} = \text{rowsp}(R_1, R_2) \in \mathcal{G}_{\mathbb{F}_q}(k, 2k)$ satisfying $(\mathbb{F}_q^*)^k$ with $\text{rank}(R_1) \geq \text{rank}(R_2) > \frac{k-1}{2}$, $S \in \text{GL}_k(\mathbb{F}_q^k)$ a matrix diagonalizing $P$ and $M \in \text{GL}_k(\mathbb{F}_q^k)$ such that $MS^{-1}(R_1 R_2)S$ is in row reduced echelon form. Let $R(x) := MS^{-1}R_1S\Delta(x) - MS^{-1}R_2S$. Then, there exist $J, L \subset I := (1, \ldots, k)$ with $|J| = |L| = \left\lfloor \frac{k+1}{2} \right\rfloor - (k - \text{rank}(R_1))$ such that

$$[J; L]_R(x) = \mu \prod_{i \in K} (x^{q^i} - \mu_i),$$

where $K = J \cap L$, $\mu = [J \setminus K; L \setminus K]_{R(0)} \in \mathbb{F}_q^*$ and $\mu_i = [J \setminus \{i\}; L \setminus \{i\}]_{R(0)} \in \mathbb{F}_q$. In particular if $\mu \in \mathbb{F}_q^k$ is such that $\text{rank}(R(\mu)) \leq \frac{k-1}{2}$, then

$$\mu \in \left\{ \mu_i^{q^{k-i}} \mid i \in K \right\}.$$

Let $\mathbb{F}$ be a field and let $m \in \mathbb{F}[y_1, \ldots, y_s]$ be a polynomial of the form $m = \sum_{U \subseteq \{1, \ldots, s\}} a_U y_U$ where $y_U := \prod_{u \in U} y_u$, $a_{\{1, \ldots, s\}} \neq 0$.

**Lemma 3.9.** The following are equivalent:

1. The polynomial $m$ decomposes in linear factors, i.e.,

$$m = a_{\{1, \ldots, s\}} \prod_{u \in \{1, \ldots, s\}} (y_u + \mu_u)$$

where $\mu_u = \frac{a_{\{1, \ldots, s\}}(u)}{a_{\{1, \ldots, s\}}} \in \mathbb{F}$. 

12
2. It holds that
\[ a_U a_V = a_{U \cap V} a_{(1, \ldots, s)} \]
for all \( U, V \) such that \(|V| = s - 1 \) and
\[ \min((1, \ldots, s) \setminus V) < \min((1, \ldots, s) \setminus U). \]

**Proof.** We proceed by induction on \( s \).

\( \Rightarrow \) If \( s = 1 \), \( m \) is a linear polynomial. Let us now suppose the thesis true for \( s - 1 \). Then
\[ a_{(1, \ldots, s)} \prod_{u \in (1, \ldots, s)} (y_u + \mu_u) = a_{(1, \ldots, s)}(y_s + \mu_s) \left( \sum_{U \subseteq (1, \ldots, s-1)} \tilde{a}_U y_U \right) \]
where \( \tilde{a}_{(1, \ldots, s-1)} = 1 \) and the coefficients \( \tilde{a}_U \) with \( U \subseteq (1, \ldots, s - 1) \) satisfy by hypothesis condition (7). The coefficients of \( m \) are \( a_U = \tilde{a}_{U \setminus \{s\}} \) if \( s \in U \), and \( a_U = \mu_s \tilde{a}_U \) otherwise. Therefore we only need to prove that (7) holds for \( U \in (1, \ldots, s - 1) \). The equality is \( a_{(1, \ldots, s)} a_U = a_U a_{(1, \ldots, s)} \) hence it is trivial.

\( \Leftarrow \) The thesis is trivial for \( s = 1 \). Let us assume that the thesis holds for \( s - 1 \). We explicitly show the extraction of a linear factor of the polynomial.

\[ m = \sum_{U \subseteq (1, \ldots, s)} a_U y_U = \sum_{U \subseteq (1, \ldots, s)} \left( a_U y_U + a_{U \setminus \{1\}} y_U \setminus \{1\} \right) = \]
\[ = \sum_{U \subseteq (1, \ldots, s)} \left( a_U y_U \setminus \{1\} + a_U \frac{a_{(2, \ldots, s)}}{a_{(1, \ldots, s)}} y_U \setminus \{1\} \right) = \]
\[ = (y_1 + \frac{a_{(2, \ldots, s)}}{a_{(1, \ldots, s)}}) \cdot \left( \sum_{U \subseteq (1, \ldots, s)} \frac{a_U y_U \setminus \{1\}}{1 \in U} \right). \]

The thesis is true by induction.

Let \( \mathbb{F}[x_{i,j}]_{1 \leq i, j \leq k} \) be a ring of multivariate polynomials where \( k \in \mathbb{N} \). We consider the following matrix
\[ M := \begin{pmatrix} x_{1,1} & \cdots & x_{1,k} \\ \vdots & \ddots & \vdots \\ x_{k,1} & \cdots & x_{k,k} \end{pmatrix}. \]
We are now interested in some particular relations among the minors of \( M \).

**Lemma 3.10.** Let \( J = (j_1, \ldots, j_k), L = (l_1, \ldots, l_k) \in \{1, \ldots, k\}^k \), \( J_s = (j_1, \ldots, j_s) \) and \( L_s = (l_1, \ldots, l_s) \). Then,
\[ [J_s; L_s][J; L] = \sum_{t=s+1}^k (-1)^{t+s+1} [J_s \cup (j_t); L_s \cup (l_{s+1})][J \setminus (j_t); L \setminus (l_{s+1})]. \]
Proof. Notice that if we consider as convention that \([\emptyset; \emptyset] = 1\), i.e., when \(s = 0\), we get the determinant formula.

We proceed by induction on \(s\). Let us consider the case when \(s = 1\), i.e., \([J_1; L_1] = (x_{j_1,l_1})\). Then,

\[
(x_{j_1,l_1})[I; I] = \sum_{t=1}^{k} (-1)^{t+2} x_{j_1,l_1} x_{j_1,l_2} [J \setminus (j_1); L \setminus (l_2)]
\]

\[
= -x_{j_1,l_1} x_{j_1,l_2} [J \setminus (j_1); L \setminus (l_2)]
\]

\[
+ \sum_{t=2}^{k} (-1)^{t+2} ([j_1, j_2] + x_{j_1,l_1} x_{j_2,l_2}) [J \setminus (j_2); L \setminus (l_2)]
\]

\[
= \sum_{t=2}^{k} (-1)^{t+2} [(j_1, j_2); (l_1, l_2)] [J \setminus (j_2); L \setminus (l_2)]
\]

\[
+ x_{j_1,l_2} [J; (l_1, l_1, l_2, \ldots, l_k)].
\]

For \(s = 1\) the thesis is true because \([J; (l_1, l_1, l_3, \ldots, l_k)] = 0\) since column \(l_1\) appears twice.

Assume that the thesis is true for \(s - 1\).

\[
[J_s; L_s][J; L] = \sum_{t=1}^{k} (-1)^{t+s+1} x_{j_t,l_{t+1}} [J_s; L_s][J \setminus (j_t); L \setminus (l_{t+1})].
\]

Let us now focus on the factor \(x_{j_r,l_{s+1}} [J_s; L_s]\) for \(r \geq s + 1\), we get

\[
x_{j_r,l_{s+1}} [J_s; L_s] = [J_s \cup (j_r); L_s \cup (l_{s+1})] + \sum_{t=1}^{s} (-1)^{t+s} x_{j_t,l_{t+1}} [J_s \setminus (j_t) \cup (j_r); L_s].
\]

By substitution it follows that

\[
[J_s; L_s][J; L] = \sum_{t=s+1}^{k} (-1)^{t+s+1} [J_s \cup (j_t); L_s \cup (l_{s+1})][J \setminus (j_t); L \setminus (l_{s+1})] +
\]

\[
+ \sum_{t=s+1}^{s} (-1)^{t+s+1} x_{j_t,l_{t+1}} [J_s \setminus (j_t); L_s][J \setminus (j_t); L \setminus (l_{s+1})]
\]

\[
= \sum_{t=s+1}^{k} (-1)^{t+s+1} [J_s \cup (j_t); L_s \cup (l_{s+1})][J \setminus (j_t); L \setminus (l_{s+1})] +
\]

\[
+ \sum_{t=1}^{s} (-1)^{t+s+1} x_{j_t,l_{t+1}} ([J_s \setminus (j_t); L_s \setminus (l_s)][J; \bar{L}])
\]

where \(\bar{L} = (l_1, \ldots, l_s, l_s, l_{s+2}, \ldots, l_k)\). The repetition of column \(l_s\) twice in \(\bar{L}\) implies that \([J; \bar{L}] = 0\). The last equality follows from the induction hypothesis.
Denote by $\mathcal{I}_{s+1} \subset \mathbb{F}[x_{i,j}]_{1 \leq i,j \leq n}$ the ideal generated by all minors of size $s + 1$ of $M$ not involving entries on the diagonal, i.e.,

$$\mathcal{I}_{s+1} := ([J,L] \mid J,L \in \{1, \ldots, k\}^{s+1}, J \cap L = \emptyset).$$

The following is an easy consequence of Lemma 3.10.

**Corollary 3.11.** Let $J, L \subset I = (1, \ldots, k)$ such that $J \cap L = \emptyset$. Then

$$[J,L][I,I] - [J \cup (i); L \cup (i)][I \setminus (i); I \setminus (i)] = \sum_{l \in I \setminus (J \cup (i))} h_l[J \cup (i), L \cup (l)] \in \mathcal{I}_{s+1},$$

with $h_l \in \mathbb{F}[x_{i,j}]_{1 \leq i,j \leq k}$ for any $l \in I \setminus (J \cup (i))$.

We now investigate the minors of a matrix $S^{-1}NS$ where $N \in \mathbb{F}_q^{k \times k}$ and $S$ is a particular matrix diagonalizing $P$. We start by giving such a matrix $S$.

**Lemma 3.12.** Let $P \in \text{GL}_k(\mathbb{F}_q)$ to be the companion matrix of a monic irreducible polynomial $p \in \mathbb{F}_q[x]$ of degree $k > 0$, and let $\lambda \in \mathbb{F}_q^k$ be a root of $p$. Then the matrix

$$S := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \lambda & \lambda^q & \lambda^{q^2} & \cdots & \lambda^{q^{k-1}} \\ \lambda^2 & \lambda^{2q} & \lambda^{2q^2} & \cdots & \lambda^{2q^{k-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda^{k-1} & \lambda^{(k-1)q} & \lambda^{(k-1)q^2} & \cdots & \lambda^{(k-1)q^{k-1}} \end{pmatrix} \quad (8).$$

diagonalizes $P$.

**Proof.** The eigenvalues of the matrix $P$ correspond to the roots of the irreducible polynomial $p \in \mathbb{F}_q[x]$. If $\lambda \in \mathbb{F}_q^k$ is an element such that $p(\lambda) = 0$, then $p = \prod_{i=0}^{k-1}(x - \lambda^q)$ by [LN94, Theorem 2.4]. It is enough to show that the columns of $S$ correspond to the eigenvectors of $P$. Let $i \in \{0, \ldots, k-1\}$, then

$$P \begin{pmatrix} 1 \\ \lambda^q \\ \vdots \\ \lambda^{(k-1)q^i} \end{pmatrix} = \begin{pmatrix} \lambda^q \\ \lambda^{2q} \\ \vdots \\ - \sum_{j=0}^{k-1} P_j \lambda^{jq} \end{pmatrix} = \begin{pmatrix} \lambda^{q^i} \\ \lambda^{2q^i} \\ \cdots \\ \lambda^{(k-1)q^i} \end{pmatrix} = \lambda^{q^i} \begin{pmatrix} 1 \\ \lambda^q \\ \cdots \\ \lambda^{(k-1)q^i} \end{pmatrix}.$$

We now investigate the properties of $S$.

**Lemma 3.13.** The matrices $S$ and $S^{-1}$ defined by (8) satisfy the following properties:
1. the entries of the first column of $S$ (respectively, the first row of $S^{-1}$) form a basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$, and

2. the entries of the $(i+1)$-th column of $S$ (respectively, row of $S^{-1}$) are the $q$-th power of the ones of the $i$-th column (respectively, row) for $i = 1, \ldots, k-1$.

**Proof.** The two properties for the matrix $S$ come directly from its definition. By [LN94, Definition 2.30] we know that there exists a unique basis $\{\gamma_0, \ldots, \gamma_{k-1}\}$ of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ such that

$$\text{Tr}_{\mathbb{F}_q^k/\mathbb{F}_q}(\lambda^i \gamma_j) = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases},$$

where $\text{Tr}_{\mathbb{F}_q^k/\mathbb{F}_q}(\alpha) := 1 + \alpha + \cdots + \alpha^{q^k-1}$ for $\alpha \in \mathbb{F}_{q^k}$. We have

$$S^{-1} = \begin{pmatrix} \gamma_0 & \gamma_1 & \cdots & \gamma_{k-1} \\ \gamma_0^q & \gamma_1^q & \cdots & \gamma_{k-1}^q \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_0^{q^{k-1}} & \gamma_1^{q^{k-1}} & \cdots & \gamma_{k-1}^{q^{k-1}} \end{pmatrix}.$$

**Theorem 3.14.** Let $r \leq k$ and let $N \in \mathbb{F}_q^{r \times k}$ and $S \in \mathbb{F}_q^{k \times r}$ be two matrices satisfying the following properties:

- $N$ has full rank,
- the entries of the first column of $S$ form a basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$, and
- the entries of the $(i+1)$-th column of $S$ are the $q$-th power of the ones of the $i$-th column, for $i = 1, \ldots, r-1$.

Then $NS \in GL_r(\mathbb{F}_{q^k})$.

**Proof.** Let $N := (n_{ij})_{1 \leq i, j \leq r}$ and $NS = (t_{ij})_{1 \leq i, j \leq r}$.

Let $S := (s_{ij})_{1 \leq i, j \leq k}$ where $s_1, \ldots, s_k \in \mathbb{F}_{q^k}$ form a basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. Then:

$$t_{ij} := \sum_{l=1}^k n_{il} s_{lj} = \sum_{l=1}^k n_{il} s_{lj}^{q^{j-1}} = \left( \sum_{l=1}^k n_{il} s_l \right)^{q^{j-1}},$$

since the entries of $N$ are in $\mathbb{F}_q$. Let $\tau_i := \sum_{l=1}^k n_{il} s_l \in \mathbb{F}_{q^k}$, then

$$NS = \begin{pmatrix} \tau_1 & \tau_1^q & \cdots & \tau_1^{q^{r-1}} \\ \tau_2 & \tau_2^q & \cdots & \tau_2^{q^{r-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \tau_r & \tau_r^q & \cdots & \tau_r^{q^{r-1}} \end{pmatrix}.$$
The elements $\tau_1, \ldots, \tau_r \in \mathbb{F}_q^k$ are linearly independent over $\mathbb{F}_q$. Indeed, the linear combination
\[ \sum_{i=1}^{k} \alpha_i \tau_i = \sum_{i=1}^{r} \alpha_i \sum_{l=1}^{k} n_{il} s_l = \sum_{l=1}^{k} \left( \sum_{i=1}^{k} \alpha_i n_{il} \right) s_l \]

is zero only when $\sum_{i=1}^{r} \alpha_i n_{il} = 0$ for $l = 1, \ldots, r$. Since $N$ has full rank it follows that $\alpha_1, \ldots, \alpha_r$ must all be zero, leading to the linear independence of $\tau_1, \ldots, \tau_r$.

Now let $a_0, \ldots, a_{r-1} \in \mathbb{F}_q^k$ be such that
\[ NS \begin{pmatrix} a_0 \\ \vdots \\ a_{r-1} \end{pmatrix} = 0, \]

and consider the linearized polynomial $f = \sum_{i=0}^{r-1} a_i x^{q^{-i}}$. The elements $\tau_1, \ldots, \tau_r$ are by assumption roots of $f$. Since $f$ is a linear map, the kernel of $f$ contains the subspace $\langle \tau_1, \ldots, \tau_r \rangle \subset \mathbb{F}_q^k$. Therefore $f$ is a polynomial of degree $q^{-1}$ with $q^{-1}$ different roots, then $a_0 = \cdots = a_{r-1} = 0$.

**Corollary 3.15.** Let $S \in GL_k(\mathbb{F}_q)$ be the matrix specified in (8) and $N \in \mathbb{F}_q^{k \times k}$. Then, for any $J, L \subset \{1, \ldots, k\}$ tuples of consecutive indices and with $|J| = |L| = \text{rank}(N)$, it follows $[J; L]_{S^{-1}NS} \neq 0$.

**Proof.** Let $r := \text{rank}(N)$ and $J, L \subset \{1, \ldots, k\}$ with $|J| = |L| = r$, $H := (1, \ldots, r)$ . Let $N_1 \in \mathbb{F}_q^{k \times r}$ and $N_2 \in \mathbb{F}_q^{r \times k}$ be matrices with full rank such that $N = N_1 N_2$. One has
\[ [J, L]_{S^{-1}NS} = [J, L]_{S^{-1}N_1} N_2 S = [J, H]_{S^{-1}N_1} [H, L]_{N_2 S}. \]

We can now focus on the characterization of the maximal minors of the matrix $N_2 S$. The following considerations will also work for the matrix $S^{-1} N_1$ considering its transpose.

The minor $[H, L]_{N_2 S}$ is the determinant of a square matrix obtained by multiplying $N_2$ with the submatrix consisting of the columns of $S$ indexed by $L$. Let $L$ contain consecutive indices. By Lemma 3.14 the submatrix of $S$ that we obtain together with $N_2$ satisfy the conditions of Theorem 3.14. It follows that $[H, L]_{N_2 S} \neq 0$.

As a consequence we have that $[J, L]_{S^{-1}NS} \neq 0$ when both $J$ and $L$ are tuples of consecutive indices. \hfill \square

Before proving Theorem 3.8 we first give a further definition.

**Definition 3.16.** Let $N \in \mathbb{F}_q^{k \times k}$. We define the non diagonal rank of $N$ as follows
\[ \text{ndrank}(N) := \min \{ r \in \mathbb{N} \mid [J, L]_{N} = 0 \ \forall J, L \in \{1, \ldots, k\}^{\tau}, \ J \cap L = \emptyset \} - 1. \]

**Proof.** [Theorem 3.8] We first focus on the form of the matrix $R(x)$. Let $r_i := \text{rank}(R_i)$ for $i = 1, 2$. We deduce by Corollary 3.15 that the pivots of the matrix $MS^{-1}(R_1 R_2)S$ are contained in the first $r_1$ columns and in a choice of $k-r_1$ of the first $r_2$ columns of $MS^{-1}R_2 S$. The following picture depicts the matrix $MS^{-1}(R_1 R_2)S$. 

---

17
As a consequence, \( R(x) \) has the following form

\[
\begin{bmatrix}
\begin{array}{c}
\text{diag}(x, \ldots, x^{r_1 - 1}) \\
\text{a matrix with entries in } \mathbb{F}_{q^k}
\end{array}
\end{bmatrix}
\]

where \((l_1, \ldots, l_{k-r_1}) \subset I\) is the tuple of indices of the columns corresponding to the pivots of \( MS^{-1} R_2 S \). Hence, for all \( i \in \{1, \ldots, k-r_1\} \) the entries of columns \( l_i \) of \( R(x) \) are all zero except for the entry \( l_i \), which is \( x^{q^{l_i-1}} \), and the entry \( r_1 + i \), which is 1.

Now consider the square submatrix \( R'(x) \) of \( R(x) \) of size \( 2r_1 - k \) defined by the rows and columns indexed by

\[
I' := I \setminus (l_1, \ldots, l_{k-r_1}, r_1 + 1, \ldots, k).
\]

The matrix \( R'(x) \) is a matrix containing unknowns only in the diagonal entries.

Let \((J; L)_{R'(x)}\) be a submatrix of \( R'(x) \) such that \( J \cap L = \emptyset \) and \( s := |J| = |L| \). We can extend \((J; L)_{R'(x)}\) to the submatrix \((J \cup (r_1 + 1, \ldots, k); L \cup (l_1, \ldots, l_{k-r_1}))_{R(x)}\) of \( R(x) \) for which it holds that

\[
[J, L]_{R'(x)} = [J \cup (r_1 + 1, \ldots, k), L \cup (l_1, \ldots, l_{k-r_1})]_{R(x)}.
\]

We obtain that

\[
\text{ndrank}(R'(x)) \leq \text{ndrank}(R(x)) - (k - r_1) \\
\leq \frac{k - 1}{2} - (k - r_1) = \frac{2r_1 - k - 1}{2}.
\]

(9)
Let $\mu \in \mathbb{F}_{q^k}$ be the unique element satisfying condition (9), it holds that $\text{rank}(R'(\mu)) \leq \frac{k-1}{2} - (k-r_1)$. This implies that $\mu$ is a root of all $[J, L]_{R'(x)}$ such that $|J| = |L| = \frac{k+1}{2} - (k-r_1)$.

Consider $J', L' \subset I'$ to be tuples of indices such that

$$J' \cap L' = \emptyset, \quad [J', L']_{R'(x)} \neq 0, \quad \text{and} \quad [J' \cup (j), L' \cup (l)]_{R'(x)} = 0 \text{ for any } j \neq l \in I' \setminus (J' \cup L').$$

The existence of a couple of tuples satisfying these conditions is ensured by the definition of $\text{ndrank}(R'(x))$.

Let $K \subset I' \setminus (J' \cup L')$ with $|K| = \lfloor \frac{k+1}{2} \rfloor - (k-r_1) - s$. $K$ is non empty since by (11)

$$|K| \geq \left\lfloor \frac{k+1}{2} \right\rfloor - (k-r_1) - \frac{2r_1-k-1}{2} - \left\lfloor \frac{k+1}{2} \right\rfloor - \frac{k-1}{2} > 0.$$

Define $J := J' \cup K$ and $L := L' \cup K$.

Combining conditions (10) and Corollary 3.11 we obtain that

$$[J, L][I', I'] = [J \cup (i), L \cup (i)][I' \setminus (i), I' \setminus (i)] = 0$$

for $i \in K$. It follows by Lemma 3.9 that the polynomial $[J, L]$ factors as follows

$$[J, L]_{R(x)} = [J \setminus K, L \setminus K]_{R(0)} \prod_{i \in K} \left(x^{q^i} - \mu_i \right).$$

with $\mu_i = \frac{[J \setminus (i), L \setminus (i)]_{R(0)}}{[J \setminus K, L \setminus K]_{R(0)}}$ and $\mu \in \left\{ \mu_i^{q^{k-1}} \mid i \in K \right\}$.

Algorithm 2 in section 4 shows an efficient way to find tuples satisfying (11).

### 3.2 The non singular case

We focus on the case where the received word $R = \text{rowsp} \left(R_1, R_2\right) \in \mathfrak{G}_{\mathbb{F}_{q^k}}(k, n)$ satisfies $R_1 \in GL_k(\mathbb{F}_{q^k})$. We show that in this case we simplify the decoding algorithm.

The following is a reformulation of Corollary 3.15 for small rank matrices.

**Corollary 3.17.** Let $N \in \mathbb{F}_{q^k}^{k \times k}$ be a matrix such that $\text{rank}(N) \leq \frac{k-1}{2}$ and $S \in GL_k(\mathbb{F}_{q^k})$ defined as in (8). Then for any choice of $J, L \subset (1, \ldots, k)$ of consecutive indices with $|J| = |L| = \text{rank}(N)$,

$$[J, L]_{S^{-1}NS} \neq 0.$$

In particular $\text{ndrank}(S^{-1}NS) = \text{rank}(N)$.

Under this hypothesis, an alternative form of Theorem 3.6 holds.

**Proposition 3.18.** Let $R \in \mathfrak{G}_{\mathbb{F}_{q}}(k, n)$ be a subspace with

$$\frac{k-1}{2} < \text{rank}(R_2) \leq \text{rank}(R_1) = k.$$

The following are equivalent:

- $R$ satisfies (10).
There exists a unique \( \mu \in \mathbb{F}_{q^k} \) such that
\[
\text{rank}(\Delta(\mu) - S^{-1}R_1^{-1}R_2S) = \text{ndrank}(S^{-1}R_1^{-1}R_2S)
\]
where \( \Delta(x) \) was defined in Theorem 3.6.

Proof. By Theorem 3.6 it is clear the equivalence between the first statement and the existence of a unique \( \mu \in \mathbb{F}_{q^k} \) such that
\[
\text{rank}(\Delta(\mu) - S^{-1}R_1^{-1}R_2S) \leq \frac{k-1}{2}.
\]
Let \( A = S\Delta(\mu)S^{-1} \), then by Corollary 3.17 it holds
\[
\text{rank}(A - R_1^{-1}R_2) = \text{ndrank}(\Delta(\mu) - S^{-1}R_1^{-1}R_2S) = \text{ndrank}(S^{-1}R_1^{-1}R_2S).
\]

The following corollary is the main result of this subsection.

**Corollary 3.19.** Let \( \mathcal{R} = \text{rowsp}(R_1 \ | \ R_2) \in \mathfrak{S}_F(k, n) \) satisfying (15) with \( k = \text{rank}(R_1) \geq \text{rank}(R_2) > \frac{k+1}{2} \) and \( S \in \text{GL}_k(\mathbb{F}_{q^k}) \) a matrix diagonalizing \( P \). Let \( R(x) := \Delta(x) - S^{-1}R_1^{-1}R_2S \). Then, for any choice of tuples of consecutive indices \( J, L \subset \{1, \ldots, k\} \) such that \( J \cap L = \emptyset \) and \( |J| = |L| = \text{ndrank}(S^{-1}R_1^{-1}R_2S) \) it holds that for any \( i \in \{1, \ldots, k\} \setminus (J \cup L) \)
\[
\text{rank}\left( R\left( \left[ \begin{array}{c}
\left[ J \cup (i), L \cup (i) \right]_{S^{-1}R_1^{-1}R_2S} \\
\left[ J, L \right]_{S^{-1}R_1^{-1}R_2S}
\end{array} \right]^{q^{k-i}} \right) \right) \leq \frac{k-1}{2}.
\]

Hence the unique \( \mu \in \mathbb{F}_{q^k} \) from Proposition 3.18 is
\[
\mu = \left( \left[ J \cup (i), L \cup (i) \right]_{S^{-1}R_1^{-1}R_2S} \right)^{q^{k-i}}
\]
for any choice of \( i \in \{1, \ldots, k\} \setminus (J \cup L) \).

Proof. By Proposition 3.18 there exists a unique \( \mu \) for which
\[
\text{rank}(R(\mu)) = \text{ndrank}(S^{-1}R_1^{-1}R_2S) \leq \frac{k-1}{2}.
\]
Hence it suffices to consider minors of \( R(x) \) of size \( \text{ndrank}(S^{-1}R_1^{-1}R_2S) + 1 \).

By Corollary 3.17 the minor
\[
\left[ J \cup (i), L \cup (i) \right]_{R(x)} = \left[ J, L \right]_{S^{-1}R_1^{-1}R_2S} x^q - \left[ J \cup (i), L \cup (i) \right]_{S^{-1}R_1^{-1}R_2S}
\]
is not identically zero. Hence the root
\[
\mu = \left( \left[ J \cup (i), L \cup (i) \right]_{S^{-1}R_1^{-1}R_2S} \right)^{q^{k-i}}
\]
makes \( \text{rank}(R(\mu)) = \text{ndrank}(S^{-1}R_1^{-1}R_2S) \). By Proposition 3.18 \( \mu \) yields the unique solution to the decoding problem.

\( \blacksquare \)
4 Algorithms and complexity

We first give an algorithm that, given a non diagonal matrix, returns disjoint tuples $I, J \subset \{1, \ldots, k\}$ for which the related minor is nonzero and such that every bigger minor containing it and not involving entries of the diagonal is zero. The algorithm uses only row operations.

**Lemma 4.1.** Algorithm 4 on page 23 works as desired.

**Proof.** The algorithm eventually terminates since $|I|$ strictly decreases after every cycle of the while loop. Moreover, its complexity is bounded by the complexity of the Gaussian elimination algorithm which computes the row reduced echelon form of a matrix of $\mathbb{F}_q^{n \times n}$ in $O(n^3)$ operations.

We have to prove that the returned tuples $J, L \subset \{1, \ldots, k\}$ satisfy the output conditions.

First of all, the non diagonal condition of matrix $M$ implies that, once terminated the procedure, $J, L \neq \emptyset$. The emptiness of $J \cap L$ follows from the fact that $J, L$ are initialized to $\emptyset$ and each time we modify them, we get $J \cup (j)$ and $L \cup (l)$ where $j \neq l$ are not elements of $J \cup L$.

In order to continue we have to characterize the matrix $N$. The matrix changes as soon as we find coordinates $j, l \in I$ with $i \neq j$ for which $n_{jl} \neq 0$. The multiplication $PN$ consists of the following row operations

- the $i$-th row of $PN$ is the $i$-th row of $N$ for $i \leq j$, and
- the $i$-th row of $PN$ is the $i$-th row of $N$ minus $\frac{n_{ij}}{n_{jl}}$ times the $j$-th row of $N$, where $N = (n_{jl})_{1 \leq j, l \leq k}$ for $i > j$.

It follows that the entries of the $l$-th column of $PN$ are zero as soon as the row index is bigger than $j$.

We state that after each cycle of the while loop it holds that $[J, L]_N \neq 0$. We prove it by induction on the cardinality of $J$ and $L$. Since the matrix $M$ is not diagonal, the while loop will eventually produce tuples $J = (j)$ and $L = (l)$ with $j \neq l$ such that $[J, L]_M \neq 0$. Now suppose that we have $J, L$ such that $J, L \neq \emptyset$, $J \cap L = \emptyset$ and $[J, L]_N \neq 0$ and there exist, following the algorithm, entries $j, l \in I$ with $j \neq l$ such that $n_{jl} \neq 0$. From the previous paragraph, the only nonzero entry of the row with index $j$ of $(J \cup (j); L \cup (l))_N$, which by construction is the last one, is $n_{jl}$, hence

$$[J \cup (j), L \cup (l)]_N = n_{jl}[J, L]_N \neq 0.$$

In order to conclude that $[J, L]_M \neq 0$ it is enough to point out the row operations bringing $(J; M)_M$ to $(J; M)_N$ are rank preserving.

The property of maximality by containment of the minor $[J, L]_M$ is a direct consequence of the structure of the algorithm.

Algorithm 4 on page 23 represents the decoding algorithm for spread codes in $\mathcal{G}_{\mathbb{F}_q}(k, 2k)$ based on the previous section. Algorithm 3 on page 23 instead represents the decoding algorithm for spread codes in $\mathcal{G}_{\mathbb{F}_q}(k, rk)$ where $r > 2$ and it is a consequence of Lemma 3.1.
Complexity of the decoding algorithm

The complexity of Algorithm 4 is bounded by some operations on matrices which are performed on the field $\mathbb{F}_{q^k}$. The most expensive of the operations is the computation of the rank of matrices of size $k \times k$, which can be performed with the help of the Gaussian elimination algorithm. We give the complexities as follows.

- The complexity of step 4. is $O_{\mathbb{F}_{q^k}}(k^3)$ which corresponds to the computation of $\text{rank}(R(\mu))$.
- The complexity of step 5. is $O_{\mathbb{F}_{q^k}}(k^4)$ which corresponds to the computation of $\text{rank}(R(\mu_i))$ for all $i \in K$, where $|K| \leq \lfloor \frac{k-1}{2} \rfloor$.

The final complexity of Algorithm 4 is then $O_{\mathbb{F}_{q^k}}(k^4)$ which implies that the complexity of Algorithm 3 is $O_{\mathbb{F}_{q^k}}((n-k)k^3)$. Note, that the computation of the rank of the matrices $R_i$ has complexity $O_{\mathbb{F}_{q^k}}((n-k)k^2)$ which is dominated by $O_{\mathbb{F}_{q^k}}((n-k)k^3)$.

As already explained in Subsection 2.1 thanks to Lemma 2.13, any decoding algorithm for Reed–Solomon like codes can be adapted to spread codes. We compare our decoding algorithm with the ones contained in [KK08b] and [SKK08]. The complexity of the decoding algorithm contained in [KK08b] is $O_{\mathbb{F}_{q^n-k}}(n^2)$. Since the complexity of the two algorithm is based on operations on different fields, we consider that the complexity of the operations on an extension field $\mathbb{F}_{q^s} \supseteq \mathbb{F}_{q}$ is $O_{\mathbb{F}_q}(s^2)$. With this assumption we conclude that the decoding algorithm for spread codes presented in this work has lower complexity than the one contained in [KK08b] if $k^5 < n^2(n-k)$. In comparison, the complexity of the decoding algorithm contained in [SKK08] is $O_{\mathbb{F}_{q^n-k}}(k(n-k))$. Consequently, the spread decoding algorithm has lower complexity if $k^4 < (n-k)^2$.

Since $k \ll n$ is a natural assumption, we conclude that the illustrated decoding algorithm constitutes usually a faster option for decoding spread codes.

Acknowledgment

The authors are grateful to Heide Gluesing-Luerssen for the useful discussions and the help in the proof of Theorem 3.14.
Algorithm 2: Modified Gaussian elimination

**input:** $M \in \mathbb{F}_q^{k \times k}$ non diagonal matrix.

**output:** $J, L \subset \{1, \ldots, k\}$ such that $J, L \neq \emptyset$, $J \cap L = \emptyset$, $[J, L] \neq 0$ and $[J \cup (j), L \cup (l)] = 0$ for any $j \neq l \in (1, \ldots, k) \setminus (J \cup L)$.

$J = L = \emptyset$, $I = (1, \ldots, k)$, $j = 1$ and $N = (n_{j,l})_{1 \leq j,l \leq k} = M$;

while $I \neq \emptyset$ do

$t := 0$;

for $l \in I$ and $l \neq j$ do

if $n_{j,l} \neq 0$ and $t = 0$ then

$J = J \cup (j), L = L \cup (l)$ and $I = I \setminus (j, l)$;

$P = (p_{j',l'})_{1 \leq j', l' \leq k}$ such that $p_{i,i} = 1$ for any $i \in \{1, \ldots, k\}$, $p_{j,l} = -\frac{n_{j,l}}{n_{j,l}}$ for any $i \in I$ with $i > j$ and $p_{j',l'} = 0$ otherwise;

$N = PN$;

$t = 1$;

end

end

if $t = 0$ then $I = I \setminus (j)$;

$j = \min I$;

end

return $J, L$;

---

Algorithm 3: Decoding spread codes: case $n = rk, r > 2$

**input:** $\mathcal{R} = \text{rowsp} \left( R_1 \cdots R_r \right) \in \mathfrak{S}_{\mathbb{F}_q}(k; rk)$, $r > 2$, $P \in GL_k(\mathbb{F}_q)$ the companion matrix of $p \in \mathbb{F}_q[x]$ and $S \in GL_k(\mathbb{F}_q)$ its diagonalizing matrix.

**output:** $C \in S \subset \mathfrak{S}_{\mathbb{F}_q}(k, rk)$ such that $d(\mathcal{R}, C) < k$, if such a $C$ exists.

Let $r_i = \text{rank}(R_i)$ for $i = 1, \ldots, r$;

if $r_i \leq \frac{k-1}{2}$ for all $i \in \{1, \ldots, r\}$ then

return there exists no $C \in S$ such that $d(\mathcal{R}, C) < k$

end

Let $j = \min \{i \in \{1, \ldots, r\} \mid r_i > \frac{k-1}{2}\}$;

for $i \in \{1, \ldots, r\}$ and $r_i \leq \frac{k-1}{2}$ do

$C_i = 0 \in \mathbb{F}_q^{k \times k}$;

end

for $j < i \leq r$ and $r_i > \frac{k-1}{2}$ do

Apply Algorithm 4 with input $\mathcal{R} = \text{rowsp} \left( R_j \right)$, $P$, and $S$;

if Algorithm 4 returns no $C$ then

return there exists no $C \in S$ such that $d(\mathcal{R}, C) < k$;

else let $C_i \in \mathbb{F}_q[P]$ such that $C = \text{rowsp} \left( I \ C_i \right)$;

end

end

return $C = \text{rowsp} \left( C_1 \cdots C_r \right)$.
Algorithm 4: Decoding spread codes: case $n = 2k$

**input**: $\mathcal{R} = \text{rowsp}(R_1, R_2) \in \mathcal{G}_{F_q}(k, 2k)$, 
$P \in GL_k(F_q)$ the companion matrix of $p \in F_q[x]$ and 
$S \in GL_k(F_q)$ its diagonalizing matrix.

**output**: $\mathcal{C} \subseteq S \subseteq \mathcal{G}_{F_q}(k, n)$ such that $d(\mathcal{R}, \mathcal{C}) < k$, if such a $\mathcal{C}$ exists.

Let $r_i := \text{rank}(R_i)$ for $i = 1, 2$.

1. if either $r_1 = k$ and $S^{-1}R_1^{-1}R_2S$ is diagonal or $r_1 = 0$ and $r_2 = k$ then 
   return $\mathcal{R} \in \mathcal{S}$; 
   end

2. if either $r_1 \leq \frac{k-1}{2}$ or $r_2 \leq \frac{k-1}{2}$ then go to 3. 
   else if either $r_1 = k$ or $r_2 = k$ then go to 4. 
   else go to 5.

3. Case $r_1 \leq \frac{k-1}{2}$ // the case $r_2 \leq \frac{k-1}{2}$ is similar. 
   $\text{return \ rowsp}(0, I)$;
   end

4. Case $r_1 = k$ // the case $r_2 = k$ is similar. 
   $R(x) := \Delta(x) - S^{-1}R_1^{-1}R_2S$; 
   $s := \text{rank}((1, \ldots, \frac{k-1}{2}); (k - \frac{k-1}{2} + 1, \ldots, k))_{R(0)}$; 
   $\mu := \frac{[(1,\ldots,s+1),(1,k-s-1)]_{R(0)}}{[(2,\ldots,s+1),(k-s-1)]_{R(0)}}$; 
   if $\text{rank}(R(\mu)) \leq \frac{k-1}{2}$ then 
   $\text{return \ rowsp}(I, S\Delta(\mu)S^{-1}) \in \mathcal{S}$; 
   else return there exists no $\mathcal{C} \in \mathcal{S}$ such that $d(\mathcal{R}, \mathcal{C}) < k$; 
   end

5. Case $\frac{k-1}{2} < r_2 \leq r_1 < k$ // the case $r_1 \leq r_2$ is similar. 
   Find $M \in GL_k(F_q^s)$ such that $MS^{-1}(R_1, R_2)S$ is in row reduced echelon form; 
   $R(x) := MS^{-1}R_1S\Delta(x) - MS^{-1}R_2S$; 
   Let $l_1, \ldots, l_{k-r_1} \in \{1, \ldots, k\}$ the columns of the pivots of $MS^{-1}R_2S$; 
   Let $I' := \{1, \ldots, k\} \setminus (l_1, \ldots, l_{k-r_1}, r_1 + 1, \ldots, k)$; 
   Apply Algorithm 2 on $(I'; I')_{R(x)}$ to find $J, L \subset I'$ and set $s := |J|$; 
   Let $K \subset I' \setminus (J \cup L)$ with $|K| = \frac{k+s}{2} - k + r_1 - s$; 
   $\mu_i := \frac{[J_{\cup l}(i)]_{R(0)}}{[l_i]_{R(0)}}$ $q^{k-i}$ for $i \in K$; 
   if there exists an $i \in K$ such that $\text{rank}(R(\mu_i)) \leq \frac{k-1}{2}$ then 
   return $\text{rowsp}(I, S\Delta(\mu_i)S^{-1})$; 
   else return there exists no $\mathcal{C} \in \mathcal{S}$ such that $d(\mathcal{R}, \mathcal{C}) < k$; 
   end
References


