# A Class of Sudan-decodable Codes

R. Refslund Nielsen
Department of Mathematics
Technical University of Denmark, Bldg. 303
DK-2800 Lyngby, Denmark.
E-mail: refslund@mat.dtu.dk

*Abstract*— **A new class of codes based on Reed-Solomon codes are defined and their properties are discussed. The minimum distance is generally bad, however, decoding can be done efficiently beyond half the minimum distance in well-defined cases. It is shown that the codes can be seen as non-linear MDS codes over a larger alphabet. Efficient decoding methods are presented for unique decoding and for list decoding. The construction is generalized to codes based on algebraic-geometry codes and the decoding algorithms are generalized.**

## I. Introduction

Reed-Solomon codes are often used in practice due to the fact that they can be decoded efficiently and have the optimal minimum distance for the lengths and dimensions where a Reed-Solomon code exists. During the last decades much effort has been put into the construction of codes with lengths and dimensions not obtainable for Reed-Solomon codes while maintaining a good minimum distance. The study of algebraic geometry codes has lead to very promising results.

However, the minimum distance is not the only measure of the usability of a code. For practical purposes it is important that there exist an efficient decoding method to make use of the error-correcting capability, and it is important that error-patterns which are likely to occur in the actual application are usually corrected by the decoder.

For example consider a $(n,k)$ Reed-Solomon code over $\mathbb{F}_{2^m}$. $\mathbb{F}_{2^m}$ can be seen as a vector space of dimension $m$ over $\mathbb{F}_2$, so the code can be seen as a $(mn, mk)$ code over $\mathbb{F}_2$. The minimum distance of the Reed-Solomon code is optimal over $\mathbb{F}_{2^m}$, but the minimum distance of the binary code could be considerably less than for other codes. This means that the Reed-Solomon codes might not correct as many random binary errors as for example a BCH-code. A reason why Reed-Solomon codes are still widely used even though the underlying communication channel is binary is that errors are often likely to happen in bursts, so a bit has higher probability of being erroneous if the previous bit was erroneous too, and a code over a larger alphabet handles this situation better than a binary code.

In this paper a new class of error-correcting codes is introduced. The codes are capable of correcting a set of error-patterns significantly different from the set corrected by previously known codes, so even though the codes generally have a bad minimum Hamming distance, they might perform better if suitable assumptions can be made on the distribution of error-patterns. To describe the set of error-patterns which can be corrected by the new codes a new distance function on vectors over finite sets is introduced.

## II. Construction

Let $\mathbb{F}_q$ denote a finite field with $q$ elements and suppose that

$$P := \{P_1, \dots, P_{n'}\} \subseteq \mathbb{F}_q \text{ with } |P| = n' \tag{1}$$

Consider a polynomial, $f \in \mathbb{F}_q[x]$, with $f = \sum_{j=0}^{\deg(f)} f_j x^j$. Given some $P_i \in P$ we can write

$$f(x) = \sum_{j=0}^{\deg(f)} f_{j,i}(x - P_i)^j$$

and it is seen by direct calculation that

$$f_{j,i} = \sum_{j'=j}^{\deg(f)} f_{j'} P_i^{j'-j} \binom{j'}{j} \tag{2}$$

It is useful to observe that

$$(x - P_i)^j | f(x) \Leftrightarrow \forall j' < j (f_{j',i} = 0) \tag{3}$$

*Definition 1:* Let $r$ be a positive integer and let $0 < k \leq rn'$. Then define the following error-correcting code:

$$C(P, r, k) = \{f(P, r) \mid \deg(f) < k\}$$

with $P$ being as in (1) and

$$f(P, r) := (f_{0,1}, \dots, f_{r-1,1}; f_{0,2}, \dots, f_{r-1,2}; \dots ; f_{0,n'}, \dots, f_{r-1,n'})$$

Notice that for $r = 1$ a Reed-Solomon code is obtained.

Furthermore, it is useful to notice that if $f(P, r) = (c_0, \dots, c_{n-1})$ then for any $i$ and $j$ with $1 \leq i \leq n'$ and $0 \leq j < r$ we have

$$f_{j,i} = c_{(i-1)r+j}$$

*Theorem 2:* $C(P, r, k)$ is a $\mathbb{F}_q$-linear code with length $n := rn'$ and dimension $k$.

## III. $r$-distance

The minimum distance of the code $C(P, r, k)$ is normally bad with respect to the usual Hamming distance. In this section a new distance which will be called $r$-distance is introduced and the properties of $C(P, r, k)$ with respect to the $r$-distance are analyzed.

Codewords of $C(P,r,k)$ consist of $n'$ chunks of $r$ field elements where each chunk corresponds to an element in $P$. This structure is reflected in the following definition of $r$-distance:

*Definition 3:* Let $r$ be a positive integer and let $u,v \in \mathbb{F}_q^n$ with $n = rn'$ for some integer $n'$. For $i \in \{1,\dots,n'\}$ define the $r$-similarity, $\mathbf{s}_r(u,v,i)$, and the $r$-distance, $\mathbf{d}_r(u,v,i)$, between $u$ and $v$ with respect to the $i$'th chunk as follows:

$$\begin{aligned}\mathbf{s}_r(u,v,i) &:= \max\{j \in \{0,\dots,r\} \mid u_{(i-1)r+j'} = v_{(i-1)r+j'} \\ &\qquad \text{for all } j' \text{ with } 0 \le j' < j\} \\ \mathbf{d}_r(u,v,i) &:= r - \mathbf{s}_r(u,v,i)\end{aligned}$$

Furthermore, define the $r$-similarity, $\mathbf{s}_r(u,v)$, and the $r$-distance, $\mathbf{d}_r(u,v)$, between $u$ and $v$:

$$\begin{aligned}\mathbf{s}_r(u,v) &:= \textstyle\sum_{i=1}^{n'} \mathbf{s}_r(u,v,i) \\ \mathbf{d}_r(u,v) &:= \textstyle\sum_{i=1}^{n'} \mathbf{d}_r(u,v,i)\end{aligned}$$

*Theorem 4:* $\mathbf{d}_r$ is a distance function on $\mathbb{F}_q^n$.

The following theorem gives the minimum $r$-distance of $C(P,r,k)$:

*Theorem 5:* If $u,v \in C(P,r,k)$ with $u \neq v$ then $\mathbf{d}_r(u,v) \geq n-k+1$ and $\mathbf{d}_r(w,0) = n-k+1$ for some $w \in C(P,r,k)$.

## IV. Decoding

In [1] V. Guruswami and M. Sudan presented an algorithm to decode Reed-Solomon codes beyond half the minimum distance by allowing the output to be a (small) list of codewords closest to the received word. In this section the method in [1] will be generalized to a list decoding method for $C(P,r,k)$. However, first some notation is needed.

Let $f(x,y) \in \mathbb{F}_q[x,y]\backslash\{0\}$ with $f = \sum_{\alpha,\beta} f_\alpha^{(\beta)} x^\alpha y^\beta$. Then the *weighted degree* of $f(x,y)$ is given by

$$\deg^{(a,b)}(f) := \max\{\alpha a + \beta b \mid f_\alpha^{(\beta)} \neq 0\}$$

where $a \in \mathbb{N}$ is called the weight of $x$ and $b \in \mathbb{N}$ is called the weight of $y$. For any choice of $a$ and $b$ we may define $\deg^{(a,b)}(0) := -\infty$. In general, $\deg^{(a,b)}(f)$ is called the weight of $f$.

Given a weighted degree, $\deg^{(a,b)}$, and a lexicographic order, $\leq_l$, a corresponding *weighted degree lexicographic order* can be defined on $M$ by

$$\begin{aligned}f \leq_w g \Leftrightarrow {} & \deg^{(a,b)}(f) < \deg^{(a,b)}(g) \vee \\ & (\deg^{(a,b)}(f) = \deg^{(a,b)}(g) \wedge f \leq_l g)\end{aligned}$$

for all $f,g \in M$.

The following lemma describes the weight of the monomials:

*Lemma 6:* Consider the polynomial ring $\mathbb{F}_q[x,y]$ with the weighted degree $\deg^{(1,k-1)}$ for some integer $k > 1$ and let the monomials be ordered by a corresponding $\leq_w$ order. Suppose that

$$m_0 \leq_w m_1 \leq_w m_2 \leq_w \dots$$

is an increasing list of all the monomials in $F_q[x,y]$. Then

$$\deg^{(1,k-1)}(m_j) = \left\lfloor \frac{j}{b} + \frac{(b-1)(k-1)}{2} \right\rfloor \tag{4}$$

where $b$ satisfies

$$\binom{b}{2} \leq \frac{j}{k-1} < \binom{b+1}{2}$$

The following definition turns out to be useful:

*Definition 7:* Let $w = (w_0,\dots,w_{n-1}) \in \mathbb{F}_q^n$ with $n = rn'$. Then define

$$w^{(i)}(x) := \sum_{j=0}^{r-1} w_{(i-1)r+j}(x-P_i)^j$$

Notice that for any $f(x) \in \mathbb{F}_q[x]$,

$$(x-P_i)^{\mathbf{s}_r(f(P,r),w,i)} | (f(x) - w^{(i)}(x)) \tag{5}$$

Furthermore, if $Q(x,y) = \sum_{\alpha=0}^{\deg_y(Q)} Q^{(\alpha)} y^\alpha$ then $Q$ can be written as follows:

$$Q(x,y) = \sum_{\alpha=0}^{\deg_y(Q)} Q^{(\alpha,i)}(y - w^{(i)}(x))^\alpha \ , \quad Q^{(\alpha,i)} \in \mathbb{F}_q[x]$$

*Algorithm 8:* As input take the code, $C(P,r,k)$, a received word, $w$, and a parameter, $s \geq 1$.

Let

$$\ell_s := \left\lfloor \frac{n\binom{s+1}{2}}{b_s} + \frac{(b_s-1)(k-1)}{2} \right\rfloor$$

where $b_s$ satisfies

$$\binom{b_s}{2} \leq \frac{j}{k-1} < \binom{b_s+1}{2}$$

Determine $Q(x,y) \in \mathbb{F}_q[x,y]\backslash\{0\}$ so that

$$\deg^{(1,k-1)}(Q) \leq \ell_s$$

and furthermore for $i \in \{1,\dots,n'\}$, $\alpha \in \{0,\dots,s-1\}$, and $j \in \{0,\dots,r(s-\alpha)-1\}$,

$$Q_{j,i}^{(\alpha,i)} = 0 \tag{6}$$

Next, let

$$\tau_s := n - \left\lfloor \frac{\ell_s}{s} \right\rfloor - 1$$

and find all factors of $Q$ of the form $y - f(x)$ with $\deg(f) < k$. If $\mathbf{d}_r(f(P,r),w) \leq \tau_s$ then include $f$ in the output list.

The claim is now that the output list contains all codewords, $c \in C(P,r,k)$, where $\mathbf{d}_r(c,w) \leq \tau_s$. To prove that the algorithm works, it must be proven that the polynomial $Q$ exists and that it has the right factors.

*Theorem 9:* $Q(x,y)$ satisfying the conditions above exists.

*Proof:* Equation 6 gives $n\binom{s+1}{2}$ homogeneous linear equation in the coefficients of $Q$. By Lemma 6 there are at least $n\binom{s+1}{2}+1$ monomials in $\mathbb{F}_q[x,y]$ with weighted degree at most $\ell_s$, so the system of equations has a non-zero solution. ■

*Lemma 10:* If $f(x) \in \mathbb{F}_q[x]$ with $\deg(f) < k$ then $(x - P_i)^{s\mathbf{S}_r(f(P,r),w,i)}$ divides $Q(x, f(x))$.

*Theorem 11:* If a codeword $f(P,r) \in C(P,r,k)$ has $\mathbf{d}_r(f(P,r),w) \leq \tau_s$ then $(y-f)|Q$.

The theorem below gives an idea of the size of $\tau_s$ in Algorithm 8 and corresponds to the result of [1].

*Theorem 12:* If $n$ and $s$ are sufficiently large then

$$\frac{\tau_s}{n} \approx 1 - \sqrt{\frac{k}{n}}$$

The following theorem gives an upper bound on the size of the output list:

*Theorem 13:* The number of codewords returned by Algorithm 8 is less than $b_s$.

The list decoding algorithm can easily be modified into an efficient algorithm for unique decoding of the code $C(P,r,k)$ up to half the minimum $r$-distance. This algorithm, which can be seen as a generalization of the Welch-Berlekamp algorithm for decoding of Reed-Solomon codes (see for example [2] or [3]), is given below:

*Algorithm 14:* As input take the code $C(P,r,k)$ and the received word, $w \in \mathbb{F}_q^n$.

Let $Q(x,y) = Q^{(0)}(x) + yQ^{(1)}(x) \in \mathbb{F}_q[x,y]\backslash\{0\}$ satisfy that

$$\deg(Q^{(0)}) \leq \left\lceil \frac{n+k}{2} \right\rceil - 1 \text{ and } \deg(Q^{(1)}) \leq \left\lfloor \frac{n-k}{2} \right\rfloor$$

and furthermore for each $1 \leq i \leq n'$ and $j < r$:

$$Q^{(0)}_{j,i} + \sum_{j'=0}^{j} w_{(i-1)r+j'} Q^{(1)}_{j-j',i} = 0 \qquad (7)$$

If there exists a codeword $f(P,r) \in C(P,r,k)$ with $\mathbf{d}_r(f(P,r),w) \leq \lfloor \frac{n-k}{2} \rfloor$ then $f = \frac{-Q^{(0)}}{Q^{(1)}}$.

The proof that this method works as promised is just a modification of the proof of Algorithm 8.

*Example 15:* Let $\mathbb{F}_q = \{\omega_0, \ldots, \omega_{q-1}\}$ and suppose that a vector in $\mathbb{F}_q^{rn'}$ is transmitted as $n'$ integers where a chunk $(\omega_{j_0}, \ldots, \omega_{j_{r-1}})$ is transmitted as $c := \sum_{\ell=0}^{r-1} j_\ell q^{r-1-\ell}$. What is received is $c + e$ where $|e|$ is a small integer. In this case errors are most likely to affect the right-most element, and in general if an element is erroneous then all the elements to the right of that element in the same chunk are almost always erroneous too. This means that the $r$-distance and the Hamming distance between a codeword and a received word are usually the same. So in this case using a $C(P,r,k)$-code corresponds to using a MDS-code og length $rn'$ which, however, does not exist if $n' = q$ and $r > 1$.

The code construction and the results mentioned here can all be generalized using the theory of algebraic function fields, in the same way that Reed-Solomon codes can be generalized to algebraic geometry codes.

## V. Conclusion

A new construction of error-correcting codes has been described. The codes does not have a good minimum distance with respect to the Hamming distance, but in situations where the error-patterns can be assumed to follow the so-called $r$-distance introduced in the text the codes perform better than previously known codes.

It is shown that the codes can be efficiently list decoded with respect to the $r$-distance using a variant of Sudan's algorithm. This can be specialized to a very efficient method for unique decoding.

## References

[1] Venkatesan Guruswami and Madhu Sudan: "Improved Decoding of Reed-Solomon and Algebraic-Geometric Codes" *Proc. 39th IEEE Symp. Foundations Comput. Sci.*, 1998.

[2] M. Morii and M. Kasahara: "Generalized Key-Equation of Remainder Decoding Algorithm for Reed-Solomon Codes" *IEEE Trans. Inform. Theory*, vol 38, no. 6, pp. 1801-1807, Nov. 1992.

[3] S. B. Wicker and V. K. Bhargava: "Reed-Solomon Codes and Their Applications" *IEEE Press*, section 5.3, p.87, 1994.