Codes derived from binary GOPPA codes

Pierre LOIDREAU
Project CODES, INRIA Rocquencourt
Domaine de Voluceau, B.P. 105
78153 Le Chesnay Cedex France
e-mail : Pierre.Loidreau@inria.fr

Abstract

We present a new family of binary codes derived from the family of classical GOPPA codes. We generalize properties of GOPPA codes to this family and deduce bounds on the dimension and on the minimum distance, and the existence of a polynomial-time decoding algorithm up to a constructed error-correcting capability. Asymptotically these codes have the same parameters as GOPPA codes.

1 Introduction

GOPPA codes were introduced in [3]. They form a family of binary linear codes generated by the GOPPA polynomial $g(x)$ of degree t with coefficients taken in a finite field $\mathrm{GF}(2^m)$ and by the subset $L = \{\alpha_1, \ldots, \alpha_n\}$ over this field, whose elements α_i are not roots of $g(x)$. Lower bounds are known on their dimension and on their minimum distance as well as a fast (polynomial-time) decoding algorithm realizing the constructed distance of the code.

We start constructing a new family of codes by considering GOPPA codes with a special automorphism group. Namely, if the coefficients of the GOPPA polynomial belong to some subfield of the field $\mathrm{GF}(2^m)$, then the automorphism group of the code contains the group generated by the FROBENIUS automorphism. From the set of elements of the code that are invariant under the action of the FROBENIUS group we derive a code of smaller length which we call s-projected code.

For this new family of codes, we derive bounds on their dimension and minimum distance. We also transfer to it some known results for GOPPA codes. In particular we show that the bound on the dimension is reached in the case when the degree of the GOPPA polynomial is small. Moreover, by using the standard decoding algorithm for GOPPA codes, we build a polynomial time decoding procedure for s-projected codes correcting errors up to half the constructed minimum distance.

2 Binary GOPPA codes

GOPPA codes can be defined in various ways (see [7]). In this paper we consider the definition using the parity-check matrix of a generalized REED-SOLOMON code.

Let $g(x) \in \mathrm{GF}(2^m)[x]$ be a polynomial of degree t over the field $\mathrm{GF}(2^m)$. Let $L = \{\alpha_1, \ldots, \alpha_n\}$ be a subset of elements of $\mathrm{GF}(2^m)$ such that $g(\alpha_i) \neq 0$. We label the coordinates of the vector $\mathbf{a} \in (\mathrm{GF}(2^m))^n$ with the elements of L in the following way:

$$\mathbf{a} = (a_{\alpha_1}, \ldots, a_{\alpha_n}).$$

Definition 1 ([7]) *The* GOPPA *code* $\Gamma(L, g)$ *of generating polynomial* g *and generating set* $L = \{\alpha_1, \ldots, \alpha_n\}$ *is the set of binary vectors* $\mathbf{a} = (a_{\alpha_1}, \ldots, a_{\alpha_n})$ *such that*

$$H\mathbf{a}^t = 0,$$

where

$$H = \begin{pmatrix} \frac{1}{g(\alpha_1)} & \cdots & \frac{1}{g(\alpha_n)} \\ \frac{\alpha_1}{g(\alpha_1)} & \cdots & \frac{\alpha_n}{g(\alpha_n)} \\ \cdots & \ddots & \cdots \\ \frac{\alpha_1^{t-1}}{g(\alpha_1)} & \cdots & \frac{\alpha_n^{t-1}}{g(\alpha_n)} \end{pmatrix}.$$

The code $\Gamma(L, g)$ is by definition the subfield subcode over $\mathrm{GF}(2)$ of the generalized Reed-Solomon code with parity check matrix H.

Proposition 1 ([7]) *Let* $\Gamma(L, g)$ *be a* GOPPA *code with parameters* $[n,\ k,\ d]$. *Then we have*

- $k \geq n - mt$, *where* t *is the degree of* g;
- $d \geq 2\deg(\overline{g}) + 1$, *where* $\overline{g}$ *is the square-free polynomial of highest degree which divides* g;
- *there exists a polynomial-time decoding algorithm which corrects up to* $\deg(\overline{g})$ *errors.*

Theorem 1 ([8]) *Let* $g(x) \in \mathrm{GF}(2^m)[x]$ *be a square-free polynomial of degree* t *with no roots in* $\mathrm{GF}(2^m)$, *and let* $\Gamma(L, g)$ *be the corresponding* GOPPA *code of length* n *and dimension* k. *If* $t < 2^{m/2-1}$, *then* $k = n - mt$.

3 Construction of s-projected codes

The automorphism group of the GOPPA code, whose generating polynomial has coefficients in the subfield $\mathrm{GF}(2^s)$ of $\mathrm{GF}(2^m)$ contains the group generated by the FROBENIUS automorphism of $\mathrm{GF}(2^m)/\mathrm{GF}(2^s)$. The set of the

code vectors that are invariant under the action of the FROBENIUS automorphism is a subcode of the GOPPA code which is in one-to-one correspondence with a code of smaller length, called by us s-projected code.

Let $\mathbf{a} = (a_{\alpha_1}, \ldots, a_{\alpha_n})$ be a vector labeled by the elements of L, let π be a permutation of L. We define the action of π on the vector a by

$$\pi(\mathbf{a}) = (a_{\pi^{-1}(\alpha_1)}, \ldots, a_{\pi^{-1}(\alpha_n)}).$$

The vector $\mathbf{a}$ is an invariant of the group G if $\pi(\mathbf{a}) = \mathbf{a}$ for every $\pi \in G$.

Let us denote by $\sigma : z \mapsto z^{2^s}$ the FROBENIUS automorphism from the field $\mathrm{GF}(2^m)$ onto $\mathrm{GF}(2^s)$.

Lemma 1 *If $g(x) \in \mathrm{GF}(2^s)[x]$, then $\sigma(\mathbf{a}) \in \Gamma(L, g)$ for any vector $\mathbf{a}$ of $\Gamma(L, g)$, that is the automorphism group of the code $\Gamma(L, g)$ contains the group $< \sigma >$, generated by σ.*

Proof

The binary vector $\mathbf{a} = (a_{\alpha_1}, \ldots, a_{\alpha_n})$ belongs to the code $\Gamma(L, g)$ if and only if it satisfies the following parity check equations

$$\sum_{i=1}^{n} a_{\alpha_i} \frac{\alpha_i^j}{g(\alpha_i)} = 0$$

for $j = 0, \ldots, t-1$. Let us represent the vector $\sigma(\mathbf{a})$ in the form $(a_{\beta_1}, \ldots, a_{\beta_n})$, where $\beta_i^{2^s} = \alpha_i$. Since the coefficients of $g(x)$ belong to the field $\mathrm{GF}(2^s)$, then $g(\alpha_i) = g\left(\beta_i^{2^s}\right) = g(\beta_i)^{2^s}$. It follows that

$$\sum_{i=1}^{n} a_{\sigma^{-1}(\alpha_i)} \frac{\alpha_i^j}{g(\alpha_i)} = \sum_{i=1}^{n} a_{\beta_i} \frac{\alpha_i^j}{g(\alpha_i)} = \sum_{i=1}^{n} a_{\beta_i} \frac{(\beta_i^j)^{2^s}}{g(\beta_i)^{2^s}} = \left(\sum_{i=1}^{n} a_{\beta_i} \frac{(\beta_i^j)}{g(\beta_i)} \right)^{2^s} = 0$$

for $j = 0, \ldots, t-1$. Hence the vector $\sigma(\mathbf{a})$ is in the code $\Gamma(L, g)$, which completes the proof.

Lemma 1 implies if $\mathrm{GF}(2^s)$ is a strict subfield of $\mathrm{GF}(2^m)$, then the automorphism group of the GOPPA code is not trivial and its order is greater than m/s.

It is possible to show that for almost all GOPPA codes, whose generating vector $g(x)$ has coefficients in $\mathrm{GF}(2^s)$, the automorphism group is generated by the FROBENIUS automorphism, *i.e.* it is exactly the group $< \sigma >$ and is of order m/s.

Let $g(x) \in \mathrm{GF}(2^s)[x]$ and $L = \{\alpha_1, \ldots, \alpha_n\}$ be the set of elements of $\mathrm{GF}(2^m)$ that are not roots of g. Since the coefficients of $g(x)$ belong to $\mathrm{GF}(2^s)$, the set of the roots of $g(x)$ that are in $\mathrm{GF}(2^m)$ is invariant under

the action of the FROBENIUS group $< \sigma >$. Hence the set L can formally be written in the form

$$L = \cup_{i=1}^{N} \mathcal{O}_i$$

where the $\mathcal{O}_i$ are orbits of the elements of the field, that are not roots of $g(x)$, under the action of the group $< \sigma >$.

Let us denote by $I(L,g) = \{\mathbf{a} \in \Gamma(L,g) \mid \sigma(\mathbf{a}) = \mathbf{a}\}$ the set of the vectors of the GOPPA code $\Gamma(L,g)$ that are invariant under the action of σ.
For the code $I(L,g)$ we deduce the following properties:

1. $I(L,g)$ is a linear subcode of $\Gamma(L,g)$,
2. the support, *i.e.* the set of non zero coordinates (here equal to 1), of any vector $\mathbf{a} \in I(L,g)$ is a union of some orbits $\mathcal{O}_i$.

Now we pass to the construction of s-projected codes. Let $g(x) \in \mathrm{GF}(2^s)[x]$, and $\Gamma(L,g)$ the corresponding GOPPA code. We consider the subcode $I(L,g)$ formed with the vectors that are invariant under the action of the FROBENIUS automorphism σ. Let $\mathcal{O}_1, \ldots, \mathcal{O}_N$ be the orbits which form L under the action of $< \sigma >$. In every orbit $\mathcal{O}_i$, we take a representative $o_i \in \mathcal{O}_i$, and we consider the corresponding set $R = \{o_1, \ldots, o_N\}$. Since the support of any vector $\mathbf{a} = (a_{\alpha_1}, \ldots, a_{\alpha_n})$ of $I(L,g)$ is a union of orbits $\mathcal{O}_i$, the vector $\mathbf{a}$, whose coordinates are labeled by the elements of L, is in one-to-one correspondence with the vector $\widetilde{\mathbf{a}} \in \mathrm{GF}(2)^N$ by "projecting" every orbit $\mathcal{O}_i$ onto the corresponding point $o_i \in R$, that is

$$\begin{array}{rcl} [\ n,\ k_I,\ d_I] - \text{code } I(L,g) & \rightarrow & [\ N,\ k_I,\ d_{\widetilde{I}}] - \text{code } -\widetilde{I}(R,g) \\ \mathbf{a} = (a_{\alpha_1}, \ldots, a_{\alpha_n}) & \mapsto & \widetilde{\mathbf{a}} = (a_{o_1}, \ldots, a_{o_N}) \end{array}$$

The set $\widetilde{I}(R,g)$ thus deduced is a linear code of length $N \leq n$, and has the same dimension k_I as the code $I(L,g)$.

We notice that the code $\widetilde{I}(R,g)$ is independent of the choice of the representatives o_i in the orbits, *i.e.* the projection produces a unique code.

Conversely, any vector $\mathbf{a} = (a_{o_1}, \ldots, a_{o_N}) \in \widetilde{I}(R,g)$ can be lifted into an invariant vector $\overline{\mathbf{a}} \in I(L,g) \subset \Gamma(L,g)$ by duplicating each coordinate a_{o_i} exactly $|\mathcal{O}_i|$ times. This implies that this is a one-to-one mapping between the codes $\widetilde{I}(R,g)$ and $I(L,g) \subset \Gamma(L,g)$.

Definition 2 *The code $\widetilde{I}(R,g)$ is called s-projected code of parent code $\Gamma(L,g)$, and of generating set R.*

Example 1

Consider the polynomial $g(x) = x^3 + x + 1$ with coefficients in $\mathrm{GF}(2)$. *Since g is irreducible over* $\mathrm{GF}(2^4)$, *we take for L the whole field* $\mathrm{GF}(2^4)$.

Let α be a primitive element of $\mathrm{GF}(2^4)$*. We split the set L relatively to the orbits*

$$L = (\underbrace{0}_{\mathcal{O}_1}, \underbrace{1}_{\mathcal{O}_2}, \underbrace{\alpha, \alpha^2, \alpha^4, \alpha^8}_{\mathcal{O}_3}, \underbrace{\alpha^{12}, \alpha^3, \alpha^6, \alpha^9}_{\mathcal{O}_4}, \underbrace{\alpha^5, \alpha^{10}}_{\mathcal{O}_5}, \underbrace{\alpha^{11}, \alpha^{13}, \alpha^{14}, \alpha^7}_{\mathcal{O}_6})$$

A generating matrix of the Goppa *code $\Gamma(L, g)$ can be represented in the following form*

$$G_\Gamma = \left(\begin{array}{c|c|cccc|cccc|cc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right).$$

Then, a generating matrix of the subcode $I(L, g)$ of the vectors that are invariant under the action of the Frobenius *automorphism has the following form*

$$G_I = \left(\begin{array}{c|c|cccc|cccc|cc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right).$$

Thus by choosing $R = (0, 1, \alpha, \alpha^{12}, \alpha^5, \alpha^{11})$ we build the 1-projected code $\widetilde{I}(R, g)$ whose generating matrix is obtained by taking the columns of the matrix G_I that are labeled by the elements of R:

$$G_{\widetilde{I}} = \begin{array}{c} \begin{array}{cccccc} 0 & 1 & \alpha & \alpha^{12} & \alpha^5 & \alpha^{11} \end{array} \\ \left(\begin{array}{cccccc} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) \end{array}$$

4 Properties of s-projected codes

In this paragraph, we show that s-projected codes are the binary subcodes of some codes over $\mathrm{GF}(2^s)$ for which we exhibit a parity check matrix. Hence we deduce lower bounds on the dimension of s-projected codes. The main result concerns s-projected codes which have a square-free Goppa polynomial of comparatively low degree without roots in the field $\mathrm{GF}(2^m)$. In that case we calculate exactly the dimension of s-projected codes. The properties of the Goppa codes given in the property 1 can thus be extended to s-projected codes.

Proposition 2 *Let $\Gamma(L, g)$ be the $[n,\ k,\ d]$-Goppa code where $L \subset \mathrm{GF}(2^m)$, and where the degree of the* Goppa *polynomial $g(x) \in \mathrm{GF}(2^s)[x]$ is equal to t. Let $\widetilde{I}(R, g)$ be the corresponding s-projected code of length $N = |R|$, of dimension k_I and minimum distance d_I. Then we have the following properties:*

- $k_I \geq N - st$,
- $d_I > d\frac{s}{m}$,
- *any decoding algorithm of* GOPPA *codes can be adapted to decode* $\deg(\overline{g})\frac{s}{m}$ *errors in the* s*-projected codes,*
- *if the polynomial* $g(x)$ *is square free and has no roots in* $\mathrm{GF}(2^m)$*, and if its degree* $t < 2^{m/2} - 1$ *then* $k_I = N - st$.

We first prove the assertions dealing with the dimension of the s-projected codes. We show that a s-projected code is the subcode over the field $\mathrm{GF}(2)$ of some code over $\mathrm{GF}(2^s)$ whose parity check matrix is directly derived from the parity check matrix of the parent GOPPA code.

Consider the GOPPA code $\Gamma(L, g)$ such that its GOPPA polynomial $g(x) \in \mathrm{GF}(2^s)[x]$ has degree t. Let $\widetilde{I}(R, g)$ be the corresponding s-projected code, where $R = (o_1, \ldots, o_N)$, and let

$$H_I = \begin{pmatrix} \mathrm{Tr}_1\left(\frac{o_1}{g(o_1)}\right) & \cdots & \mathrm{Tr}_N\left(\frac{o_N}{g(o_N)}\right) \\ \vdots & \ddots & \vdots \\ \mathrm{Tr}_1\left(\frac{o_1^{t-1}}{g(o_1)}\right) & \cdots & \mathrm{Tr}_N\left(\frac{o_N^{t-1}}{g(o_N)}\right) \end{pmatrix}$$

where $\mathrm{GF}(2^s)(o_i)$ denotes the smallest field containing $\mathrm{GF}(2^s)$ and o_i, and $\mathrm{Tr}_i = \mathrm{Tr}_{\mathrm{GF}(2^s)(o_i)/\,\mathrm{GF}(2^s)}$ denotes the trace operator of $\mathrm{GF}(2^s)(o_i)/\,\mathrm{GF}(2^s)$. Then we have

Lemma 2 *For such a code, we have*

$$\widetilde{I}(R, g) = \{\widetilde{\mathbf{a}} \in \mathrm{GF}(2)^N \mid H_I \widetilde{\mathbf{a}}^t = 0\}.$$

Proof

Consider a word $\widetilde{\mathbf{a}} = (a_{o_1}, \ldots, a_{o_N})$ of the code $\widetilde{I}(R, g)$. Since there is a bijection between $\widetilde{I}(R, g)$ and the set of invariant points $I(L, g)$, the word $\widetilde{\mathbf{a}}$ can be "lifted" into a word $\mathbf{a} = (a_{\alpha_1}, \ldots, a_{\alpha_n})$ of $I(L, g)$.

Since $I(L, g) \subset \Gamma(L, g)$, $\mathbf{a}$ satisfies the following set of parity check equations

$$\sum_{i=1}^{n} a_{\alpha_i} \frac{\alpha_i^j}{g(\alpha_i)} = 0$$

for $j = 0, \ldots, t-1$. By summing over the orbits $\mathcal{O}_i$ we obtain the following set of parity check equations

$$\sum_{i=1}^{N} a_{o_i} \sum_{\beta \in \mathcal{O}_i} \frac{\beta^j}{g(\beta)} = 0$$

for $j = 0, \ldots, t-1$. Since the coefficients of $g(x)$ belong to $\mathrm{GF}(2^s)$, the polynomial $g(x)$ and the FROBENIUS automorphism σ commute. As a consequence, we obtain the equations

$$\sum_{\beta \in \mathcal{O}_i} \frac{\beta^j}{g(\beta)} = \mathrm{Tr}_i \left(\frac{o_i^j}{g(o_i)} \right),$$

and it follows that

$$\sum_{i=1}^{N} a_{o_i} \mathrm{Tr}_i \left(\frac{o_i^j}{g(o_i)} \right) = 0$$

for $j = 0, \ldots, t-1$. Thus $H_I \widetilde{\mathbf{a}}^t = 0$.

By choosing a basis of $\mathrm{GF}(2^s)$, considered as a vector space over $\mathrm{GF}(2)$, and by extending every element of H_I accordingly, we get a parity check matrix of $\widetilde{I}(R, g)$. Thus the lower bound on the dimension of $\widetilde{I}(R, g)$ can be immediately deduced. We say that a linear code is non-degenerated if its dimension is greater than zero.

Corollary 1 *Let $\Gamma(L, g)$ be a* GOPPA *code with $g(x) \in \mathrm{GF}(2^s)[x]$ of degree t and let $\widetilde{I}(R, g)$ be the corresponding s-projected code of length N and dimension k_I. Then*

$$k_I \geq N - st.$$

Corollary 2 *The s-projected code $\widetilde{I}(R, g)$ of parent* GOPPA *code $\Gamma(L, g)$ is non-degenerated provided $n - mt > 0$.*

Proof

The cardinality of the orbits $\mathcal{O}_i$ is less than m/s since the group generated by the FROBENIUS automorphism is of order m/s. Since $n = |L| = \sum_{i=1}^{N} |\mathcal{O}_i|$, we have $N \geq n\frac{s}{m}$ and $N - st \geq n\frac{s}{m} - st = \frac{s}{m}(n - mt) > 0$. Thus $k_I \geq N - st > 0$, which achieves the proof.

Corollary 1 can be used to estimate the dimension of the parent GOPPA code. Since obviously $k_I < k$ where k is the dimension of the parent GOPPA code, it implies that whenever $N - st > n - mt$, the lower bound $k \geq N - st$ is an improvement of the traditional lower bound $k \geq n - mt$ for the number k of information symbols of the GOPPA code.

We illustrate this observation with the example $L = \mathrm{GF}(2^{10})$, $m = 10$. The bound $k \geq n - mt$ ascertains that the GOPPA codes are non-degenerated provided $102 \geq t$. Now we show for the different possible values of s ($s = 1,\ 2,\ 5$) the range of t for which the lower bound $N - st$ is better than $n - mt$:

- for $s = 1$ then $N = 108$ and for $108 > t \geq 102$ the bound is tightened,
- for $s = 2$ then $N = 208$ and for $t = 103$ the bound is tightened,
- for $s = 5$ then $N = 528$ and for $105 > t \geq 100$ the bound is tightened.

As was shown in [8], the dimension of a GOPPA code attains the lower bound $k \leq n - mt$, if the degree of the GOPPA polynomial is small enough. Here we show that it is possible to transfer this result to s-projected codes.

Theorem 2 *Let $g(x) \in \mathrm{GF}(2^s)[x]$ be a square-free polynomial of degree t with no roots in the field $\mathrm{GF}(2^m)$, and let $\widetilde{I}(R, g)$ be the corresponding s-projected code of length N and dimension k_I. If $t < 2^{m/2-1}$ then $k_I = N - st$.*

To prove the theorem, we need the two following lemmas.

Lemma 3 *For $\widetilde{I}(R, g)^{\perp}$, the dual code of the s-projected code $\widetilde{I}(R, g)$, we have*

$$\widetilde{I}(R,g)^{\perp} = \left\{ \left(\mathrm{Tr}^{(1)}(z_1), \ldots, \mathrm{Tr}^{(N)}(z_N)\right) \mid f(x) \in \mathrm{GF}(2^s)[x], \deg(f) < t \right\},$$

where $\mathrm{Tr}^{(i)}(z) = \mathrm{Tr}_{\mathrm{GF}(2^s)(o_i)/\,\mathrm{GF}(2)}(z)$, and $z_i = f(o_i)/g(o_i)$.

Proof

In accordance with the lemma 2 the code $\widetilde{I}(R, g)$ is the binary subcode of the code over $\mathrm{GF}(2^s)$ with parity check matrix H_I where $R = (o_1, \ldots, o_N)$ and

$$H_I = \begin{pmatrix} \mathrm{Tr}_1\left(\frac{o_1}{g(o_1)}\right) & \cdots & \mathrm{Tr}_N\left(\frac{o_N}{g(o_N)}\right) \\ \vdots & \ddots & \vdots \\ \mathrm{Tr}_1\left(\frac{o_1^{t-1}}{g(o_1)}\right) & \cdots & \mathrm{Tr}_N\left(\frac{o_N^{t-1}}{g(o_N)}\right) \end{pmatrix}$$

with $\mathrm{Tr}_i = \mathrm{Tr}_{\mathrm{GF}(2^s)(o_i)/\,\mathrm{GF}(2^s)}$. Now we use a known theorem by DELSARTE [2] which asserts that for any linear code defined over an extension F of the field F_0, we have $(C|F_0)^{\perp} = \mathrm{Tr}_{F/F_0}(C^{\perp})$. From here follows that

$$\widetilde{I}(R,g)^{\perp} = \left\{ \left(\mathrm{Tr}_{\mathrm{GF}(2^s)/\,\mathrm{GF}(2)}\left[\mathrm{Tr}_i\left(\frac{f(o_i)}{g(o_i)}\right)\right] \right)_{i=1}^{N} \;\middle|\; \begin{array}{l} f(x) \in \mathrm{GF}(2^s)[x], \\ \deg(f(x)) < t. \end{array} \right\}$$

Now the proof of the lemma derives from the following property of the trace operator:

$$\mathrm{Tr}_{\mathrm{GF}(2^s)(o_i)/\,\mathrm{GF}(2)}(z) = \mathrm{Tr}_{\mathrm{GF}(2^s)/\,\mathrm{GF}(2)}(\mathrm{Tr}_i(z)),$$

that is $\mathrm{Tr}^{(i)}(z) = \mathrm{Tr}_{\mathrm{GF}(2^s)/\,\mathrm{GF}(2)}(\mathrm{Tr}_i(z))$.

Lemma 4 directly derives from the BOMBIERI's inequalities [1] (see [8]).

Lemma 4 (BOMBIERI) *Let $g(x) \in \mathrm{GF}(2^m)[x]$ be a polynomial of degree t with no roots in $\mathrm{GF}(2^m)$ and let $f(x) \in \mathrm{GF}(2^m)[x]$ be a non-zero polynomial of degree less than $t-1$. If*

$$\left| \sum_{\alpha \in \mathrm{GF}(2^m)} (-1)^{\mathrm{Tr}_{\mathrm{GF}(2^m)/\,\mathrm{GF}(2)}\left(\frac{f(\alpha)}{g(\alpha)}\right)} \right| > (2t-2)2^{m/2}$$

then the equation $Y^2 + Y = f/g$ has a solution in the field $\overline{\mathrm{GF}(2)}(x)$ where $\overline{\mathrm{GF}(2)}$ is the the algebraic closure of $\mathrm{GF}(2)$, and $\overline{\mathrm{GF}(2)}(x)$ is the fraction field of $\overline{\mathrm{GF}(2)}$. .

Proof of the theorem

Thanks to the linearity of the trace operator, it is enough to show that a non-zero polynomial $f(x) \in \mathrm{GF}(2^s)[x]$ of degree less that t does not give the zero vector in $\widetilde{I}(R,g)$. Thus the dimension of $\widetilde{I}(R,g)^{\perp}$ is not smaller than st. On the other hand, from the corollary 1, the dimension of $\widetilde{I}(R,g)^{\perp}$ is not greater than st. From this follows that this dimension is exactly equal to st.

We use contradiction arguments. We suppose that there exists a non-zero polynomial $f(x) \in \mathrm{GF}(2^s)[x]$ of degree less than t such that

$$\mathrm{Tr}^{(i)}\left(f(o_i)/g(o_i)\right) = 0,$$

where $i = 1, \ldots, N$, and $\mathrm{Tr}^{(i)}(z) = \mathrm{Tr}_{\mathrm{GF}(2^s)(o_i)/\,\mathrm{GF}(2)}(z)$. Since $\mathrm{Tr}_{\mathrm{GF}(2^m)/\,\mathrm{GF}(2)}(z) = \mathrm{Tr}_{\mathrm{GF}(2^m)/\,\mathrm{GF}(2^s)(o_i)}(1)\,\mathrm{Tr}_i(z)$, we also have

$$\mathrm{Tr}_{\mathrm{GF}(2^m)/\,\mathrm{GF}(2)}\left(f(o_i)/g(o_i)\right) = 0$$

for $i = 1, \ldots, N$. The polynomials f and g have coefficients in $\mathrm{GF}(2^s)$ thus they commute with the FROBENIUS automorphism $\sigma : x \mapsto x^{2^s}$. Moreover the trace operator also commutes with σ and since the set L labels the whole field $\mathrm{GF}(2^m)$, then for any element α of the field $\mathrm{GF}(2^m)$, we have

$$\mathrm{Tr}_{\mathrm{GF}(2^m)/\,\mathrm{GF}(2)}\left(f(\alpha)/g(\alpha)\right) = 0.$$

Thus we deduce that

$$\left| \sum_{\alpha \in \mathrm{GF}(2^m)} (-1)^{\mathrm{Tr}_{\mathrm{GF}(2^m)/\,\mathrm{GF}(2)}\left(\frac{f(\alpha)}{g(\alpha)}\right)} \right| = 2^m$$

We have $t < 2^{m/2} - 1$, hence $2^m > (2t-2)2^{m/2}$. Therefore

$$\left| \sum_{\alpha \in \mathrm{GF}(2^m)} (-1)^{\mathrm{Tr}_{\mathrm{GF}(2^m)/\,\mathrm{GF}(2)}\left(\frac{f(\alpha)}{g(\alpha)}\right)} \right| > (2t-2)2^{m/2}.$$

By applying the lemma 4, we deduce that there exists a rational function h with coefficients in $\overline{\mathrm{GF}(2)}$ such that

$$h^2 + h = f/g$$

Let $h(x) = v(x)/u(x)$, where $v(x)$ and $u(x)$ are prime together. Let $G(x) = g(x)/d(x)$ and $F(x) = f(x)/d(x)$, where $d(x) = (g(x), f(x))$ is the greatest common divisor of the polynomials $g(x)$ and $f(x)$. With this notations, the previous equation can be rewritten

$$G(v^2 + vu) = Fu^2.$$

Since $G(x)$ and $F(x)$ are prime together, then $G(x)$ divides u^2, and since $G(x)$ is square-free, then G divide u. If we take $U = u/G$, then the equation becomes

$$v^2 + vUG = FU^2G.$$

From here it follows that G divides v^2, thus G divides v. This contradicts the fact that $v(x)$ and $u(x)$ are prime together. Thus $h(x)$ is a polynomial satisfying the equation $Y^2 + Y = f/g$, and therefore f/g is also a polynomial. It follows that the degree of the polynomial $f(x)$ is not less than the degree of $g(x)$, that is t, which contradicts the hypothesis of the theorem.

The restriction $t < 2^{m/2-1}$ of the theorem can be practically increased. For example for $n = 1024$, that is $m = 10$, the theorem gives the exact value $k_I = N - st$ for $t < 16$, whereas experimental results show that this formula remains true for substantially higher values of t.

Now we derive an upper bound on the minimum distance of s-projected codes.

Proposition 3 *Let $\widetilde{I}(R, g)$ be the s-projected code of parent code $\Gamma(L, g)$ with $L \subset \mathrm{GF}(2^m)$ and of minimum distance d. If d_I denotes the minimum distance of $\widetilde{I}(R, g)$ then*

$$d_I \geq d\frac{s}{m}.$$

Proof

Consider a non-zero vector $\mathbf{a} \in \widetilde{I}(R, g)$. The vector $\mathbf{a}$ can be lifted into a vector $\overline{\mathbf{a}} \in I(L, g)$ by duplicating its coordinates, according to the cardinality of the corresponding orbits. Let $\mathrm{wt}(\mathbf{x})$ denote the HAMMING weight of the vector $\mathbf{x}$. Since in any orbit there is no more than m/s elements, then $\mathrm{wt}(\overline{\mathbf{a}}) \leq \mathrm{wt}(\mathbf{a})\frac{m}{s}$. Since $\overline{\mathbf{a}}$ lies in the GOPPA code then $\mathrm{wt}(\overline{\mathbf{a}}) > d$ and $d_I \geq d\frac{s}{m}$.

Code	$\Gamma(L,g)$	$\widetilde{I}(L,g)$
Length	$n = 128$	$N = 20$, Number of orbits.
Dimension	$k = 30$, $n - mt = 30$	$k_I = 6$, $N - t = 6$
Transmission rate	0.23	0.33
Correction	14 errors	$2 = 14/7$ errors

Table 1: Properties of $\Gamma(L,g)$ and of $\widetilde{I}(L,g)$ for the length $n = 128$

The decoding of s-projected codes is based on the principle of lifting the words into the parent GOPPA code. Thus the complexity of the decoding is roughly the same. However the computations can be done in the subfield $\mathrm{GF}(2^s)$ rather than in the field $\mathrm{GF}(2^m)$.

For more convenience we assume that the polynomial $g(x) \in \mathrm{GF}(2^s)[x]$ is of degree t and square-free. Then the minimum distance d of the GOPPA code is greater than $2t+1$, and known decoding algorithms correct t and less errors (see [7, 6]) in polynomial time. According to the proposition 3 the minimum distance of an s-projected code is $d_I \geq (2t+1)\frac{s}{m}$. By projection we get a decoding algorithm reaching this bound, that is correcting $t\frac{s}{m}$ errors, on the same model as any decoding algorithm for GOPPA codes correcting t errors.

Decoding algorithm

1. The receiver gets from the channel the vector $\mathbf{y} = \mathbf{x} + \mathbf{e}$ where $\mathbf{y} = (y_{o_i})_{i=1}^N$, $\mathbf{x} = (x_{o_i})_{i=1}^N \in \widetilde{I}(R,g)$ is the word to be decoded, and word $\mathbf{e} = (e_{o_i})_{i=1}^N$ an error vector of weight less than $t\frac{s}{m}$. The receiver lifts the vector $\mathbf{y}$ into the vector $\overline{\mathbf{y}} = (y_{\mathcal{O}_i})_{i=1}^N$ of length n, which takes the same value y_{o_i} on the coordinates belonging to the same orbit $\mathcal{O}_i$. The vector $\overline{\mathbf{y}}$ can be written $\overline{\mathbf{y}} = \overline{\mathbf{x}} + \overline{\mathbf{e}}$ where $\overline{\mathbf{x}} = (x_{\mathcal{O}_i})_{i=1}^N \in \Gamma(L,g)$ and $\overline{\mathbf{e}} = (e_{\mathcal{O}_i})_{i=1}^N$ are the analogous derived liftings of the vectors $\mathbf{x}$ and $\mathbf{e}$ respectively, and $\mathrm{wt}(\overline{\mathbf{e}}) \leq \mathrm{wt}(\mathbf{e})\frac{m}{s} \leq t$.

2. The receiver applies the decoding algorithm of the GOPPA code to the vector $\overline{\mathbf{y}}$ and recovers $\overline{\mathbf{x}} \in \Gamma(L,g)$, since the number of errors (weight of $\overline{\mathbf{e}}$) is less or equal than t.

3. By projection of $\overline{\mathbf{x}}$ onto R, the receiver recovers the transmitted word $\mathbf{x}$.

Example 2

Consider the polynomial $g(x) = x^{14} + x^3 + 1$ *with no roots in* $\mathrm{GF}(2^7)$ *and set* $L = \mathrm{GF}(2^7)$. *The relation between the corresponding* GOPPA *code and its* 1*-projected code can be found in the table 1.*

Code	GOPPA code	s-projected code
Length	n	N: Number of orbits $\approx n\frac{s}{m}$ when n grows
Dimension	$k \geq n - mt$	$k_I \geq N - st$
Transmission rate	$R = k/n$	$R_I = k_I/N \approx R$ when n grows
Constructed distance	$d \geq 2t + 1$	$d_I \geq (2t+1)\frac{s}{m}$

Table 2: Asymptotic comparison of the parameters of GOPPA codes and s-projected codes

This example shows that for small length, the GOPPA code and the s-projected code behave differently (the first being better). However this difference vanishes when the length of the codes increases. Consider the case when $\frac{m}{s}$ is a prime number and the GOPPA polynomial has no roots in the field $\mathrm{GF}(2^m)$. In this case, the number of orbits is

$$N = 2^s + (2^m - 2^s)\frac{s}{m} = n\frac{s}{m}\left(1 + 2^{s-m}\left(\frac{m}{s} - 1\right)\right),$$

where $n = 2^m$. Hence, when $\frac{m}{s} = \text{const}$ and when the length $n = 2^m$ of the GOPPA code increases, the s-projected code has length $N \approx n\frac{s}{m}$ and the parameters of the codes are proportional as indicated in the table 2.

5 Conclusion

In this paper we have built a new family of codes by using the binary GOPPA codes. These codes are obtained from the words that are invariant under the action of the FROBENIUS automorphism by "gluing" together (projecting) coordinates taken in the same orbit. This construction enables to transfer many properties of the GOPPA codes on the new codes. The properties of s-projected codes characterize in some way the parent GOPPA codes. However, we do not know if the subcode of the words invariant under the action of the FROBENIUS automorphism characterizes uniquely the GOPPA code, but this was verified in some numerical examples. When satisfied, this hypothesis enables to greatly reduce the complexity of structural attacks against the MCELIECE cryptosystem [5], in the case where the coefficients of the GOPPA polynomial are taken in a subfield [4].

References

[1] E. BOMBIERI , Exponential Sums in Finite Fields, *Am. J. Math.* **88**, pp.71-105, 1966.

[2] P. Delsarte, On Subfield Subcodes of Modified Reed-Solomon Codes, *IEEE Trans. Inform. Theory*, 1975, pp 575-576.

[3] V .D .Goppa, A New Class of Linear Correcting Codes, *Probl. Pered. Info.* **6**, no. 3, pp.24-30, 1970.

[4] P. Loidreau, N. Sendrier, Some weak keys in McEliece public-key cryptosystem, *ISIT 98'*, Boston MA., pp 382, 1998.

[5] R.J. McEliece , A Public-Key Cryptosystem Based On Algebraic Coding Theory , *JPL DSN Progress Report*, pp 114-116, 1978.

[6] N. J. Patterson, The Algebraic Decoding of Goppa Codes, *IEEE Trans. Inform. Theory*, **21**, No. 2, pp 203-207, 1975.

[7] F.J. McWilliams, N.J.A. Sloane, *The Theory of Error Correcting Codes*, North Holland Publishing Co. 1977.

[8] M. Van Der Vlugt, The True Dimension of Certain Binary Goppa Codes *IEEE Trans. Inform. Theory* **31**, no. 2, pp 397-398, 1990.