Proof of conjectures on the true dimension of some binary Goppa Codes

Pascal Véron

Designs, Codes and Cryptography, 36, 317–325, 2005

Proof of Conjectures on the True Dimension of Some Binary Goppa Codes*

P. VÉRON veron@univ-tln.fr
Groupe de Recherche en Informatique et Mathématiques (GRIM), Université de Toulon-Var, B.P. 132, 83957 La Garde Cedex, France

Communicated by: P. Wild

Received July 23, 2003; Revised April 20, 2004; Accepted May 7, 2004

Abstract. There is a classical lower bound on the dimension of a binary Goppa code. We survey results on some specific codes whose dimension exceeds this bound, and prove two conjectures on the true dimension of two classes of such codes.

Keywords: Goppa codes, trace operator, redundancy equation, parameters of Goppa codes

AMS Classification: 94B65

1. Introduction

Among the alternant codes [12], the class of Goppa codes (introduced in 1970 [8]) contains good codes over $\mathbb{F}_q$ which asymptotically meet the Varshamov–Gilbert bound. Binary Goppa codes can be specified through a polynomial $g(z)$ over $\mathbb{F}_{2^m}$ and a set $L \subset \mathbb{F}_{2^m}$ whose elements are not roots of $g(z)$.

Definition 1. Let $g(z) \in \mathbb{F}_{2^m}[z]$, $L = \{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{F}_{2^m}$ such that $\forall i, g(\alpha_i) \neq 0$. The Goppa code $\Gamma(L, g)$, of length n over $\mathbb{F}_2$, is the set of codewords, i.e. $n-tuples$ $(c_1, \ldots, c_n) \in \mathbb{F}_2^n$, satisfying

$$\sum_{i=1}^{n} \frac{c_i}{z - \alpha_i} \equiv 0 \pmod{g(z)}.$$

PROPOSITION 1. *The dimension k of $\Gamma(L, g)$ and its minimal distance d satisfy*

$$k \geq n - m \deg g(z)$$
$$d \geq \deg \bar{g}(z) + 1.$$

*Part of this work has been presented at the Sixth International Conference on Finite Fields and Applications, Oaxaca, Mexico, May 2001.

where $\bar{g}(z)$ is the lowest degree perfect square which is divisible by $g(z)$. Other basic definitions and properties of Goppa codes are to be found in [12].

The rest of the paper is organized as follows. Section 2 gives some well known properties of GRS and Goppa codes used in Sections 3 and 4. Sections 2 and 3 present two different strategies for computing polynomials giving Goppa codes whose dimension exceeds the classical lower bound, and present the known results obtained by these strategies (Theorems 1 and 2). The strategy of Section 3 is to use the link between the parity check matrix of a Goppa code and the parity check matrix of the associated GRS code. The strategy of Section 4 is to use Delsarte's theorem [6] which gives a "redundancy equation" [13,14], whose number of solutions is directly related to the dimension. Section 5 introduces three classes of Goppa polynomials amenable to treatment by Delsarte's theorem, and states previous conjectures on the true dimension of the corresponding Goppa codes. One of these conjectures has already been proved by the author [19]. Sections 6 and 7 are devoted to proving the other two conjectures. Section 7 is just an addendum to [19] since the proof is similar and does not bring any new mathematical material. The proof in Section 6 is quite different and uses some previous results [4,18] in order to prove a more general result than the original conjecture [14].

2. GRS Codes and Goppa Codes

Let $L=\{\alpha_1,\ldots,\alpha_n\}\subset\mathbb{F}_{2^m}$, and $g(z)\in\mathbb{F}_{2^m}[z]$. It is well known that a parity check matrix of the Goppa code $\Gamma(L,g)$ is

$$H=\begin{pmatrix} g(\alpha_1)^{-1} & \cdots & g(\alpha_n)^{-1} \\ \alpha_1 g(\alpha_1)^{-1} & \cdots & \alpha_n g(\alpha_n)^{-1} \\ \vdots & \vdots & \vdots \\ \alpha_1^{\deg g(z)-1} g(\alpha_1)^{-1} & \cdots & \alpha_n^{\deg g(z)-1} g(\alpha_n)^{-1} \end{pmatrix}$$

Although this matrix satisfies

$$\forall c\in\mathbb{F}_2^n,\quad c\in\Gamma(L,g)\Leftrightarrow Hc^t=0$$

it is not a "true" parity check matrix since its rows belong to $\mathbb{F}_{2^m}$ so they do not generate $\Gamma(L,g)^{\perp}$. The following result explains why H is used as a "parity check matrix" [13].

PROPOSITION 2. *$\Gamma(L,g)$ is the restriction to $\mathbb{F}_2$ of the Generalized Reed–Solomon code $GRS_{n-\deg g(z)}(\alpha,v)$ where $\forall i=1,\ldots,n$*

$$v_i=\frac{g(\alpha_i)}{\prod_{j\neq i}(\alpha_i+\alpha_j)}$$

Definition 2. Let $\alpha=(\alpha_1,\ldots,\alpha_n)$ be n distinct elements of $\mathbb{F}_{2^m}$, $v=(v_1,\ldots,v_n)$ a nonzero vector of $\mathbb{F}_{2^m}$, the Generalized Reed-Solomon code, denoted by $\mathrm{GRS}_k(\alpha,v)$ consists of all vectors

$$(v_1 F(\alpha_1), v_2 F(\alpha_2), \ldots, v_n F(\alpha_n))$$

where $F(z) \in \mathbb{F}_{2^m}[z]$ ranges over all polynomials of degree strictly less than k.

PROPOSITION 3. *A generator matrix of $GRS_k(\alpha, v)$ is*

$$\begin{pmatrix} v_1 & \cdots & v_n \\ \alpha_1 v_1 & \cdots & \alpha_n v_n \\ \vdots & \vdots & \vdots \\ \alpha_1^{k-1} v_1 & \cdots & \alpha_n^{k-1} v_n \end{pmatrix}$$

PROPOSITION 4. *The dual of a $GRS_k(\alpha, v)$ code is a $GRS_{n-k}(\alpha, v')$ code (for some $v' \in \mathbb{F}_{2^m} \setminus \{0\}$).*

It follows from the above results that:

- H is a generator matrix of a $\mathrm{GRS}_{\deg g(z)}(L, \gamma)$ code where $\gamma = (g(\alpha_1)^{-1}, \ldots, g(\alpha_n)^{-1})$,
- $\exists \lambda \in \mathbb{F}_{2^m}$ such that H be a parity check matrix of a $\mathrm{GRS}_{n-\deg g(z)}(L, \lambda)$ code,
- $\Gamma(L, g)$ is the restriction to $\mathbb{F}_2$ of $\mathrm{GRS}_{n-\deg g(z)}(L, \lambda)$.

3. Strategy 1

It is well known that a parity check matrix $\tilde{H}$ over $\mathbb{F}_2$ can be computed from H by replacing each element of H by the corresponding column vector (of length m) (when using any basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$). $\tilde{H}$ has $m \deg g(z)$ rows which generate $\Gamma(L, g)^{\perp}$. Since these rows are not necessarily independent, we can deduce that $k \geq n - m \deg g(z)$. Hence, a first hint to improve this latter bound is to find some polynomials and use a special basis, when computing $\tilde{H}$ from H, so as to easily find linear dependent rows. As an example, suppose that $\forall i$, $g(\alpha_i) \in \mathbb{F}_{2^t}$ where t divides m, then there exists a basis where $g(\alpha_i)$ can be expressed as a vector of length m whose $m - t$ latest coordinates are equal to 0 (so $m - t$ rows in $\tilde{H}$ are equal to 0). For such a polynomial we have $k \geq n - m \deg g(z) + m - t$.

THEOREM 1. *Let $g(z) \in \mathbb{F}_{2^m}[z]$ and $L = \mathbb{F}_{2^m} \setminus \{z \in F_{2^m} \mid g(z) = 0\}$. The following table sums up new lower bounds computed in [1–3, 5, 18] for specific polynomials, using strategy 1 ($\tilde{k}$ denotes the classical bound).*

Ref.	m	$g(z)$	k	*Remarks*
[1–3]	$2s$	$z^{2^s+1}+(\beta z)^{2^s}+\beta z+1$	$\tilde{k}+5s$	$\beta^{2^s+1}\neq 1$
[5]	$3s$	$z^{2^{2s}+2^s+1}+A$	$\tilde{k}+3s2^{s+2}-4s$	$A\in\mathbb{F}_{2^s}$
			$\tilde{k}+(j-1)s$	*any p and j*
[18]	js	$a(z)\mathrm{Tr}_{\mathbb{F}_{p^{js}}:\mathbb{F}_{p^s}}(b(z))$	$\tilde{k}+2s-1$	$j=2$
			$\tilde{k}+3s-1$	$p=j=2$

4. Strategy 2

Let $\mathscr{C}$ be a binary code of length n over $\mathbb{F}_{2^m}$ and consider the subset of codewords which belong to $\mathbb{F}_2^n$. A famous result due to Delsarte [6] states that for any such code $\mathscr{C}$:

PROPOSITION 5. *(Delsarte)* $(\mathscr{C}\,|\,\mathbb{F}_2)^{\perp}=T_m(\mathscr{C}^{\perp})$ *where*

$$\begin{aligned} T_m:\mathscr{C}^{\perp} &\longrightarrow \mathbb{F}_2^n \\ (c_1,\ldots,c_n) &\mapsto (\mathrm{Tr}_{\mathbb{F}_{2^m}:\mathbb{F}_2}(c_1),\ldots,\mathrm{Tr}_{\mathbb{F}_{2^m}:\mathbb{F}_2}(c_n)) \end{aligned}$$

Let $\Gamma(L,g)$ be a $[n,k]$ binary Goppa code defined over $\mathbb{F}_{2^m}$, there exists $\lambda\in\mathbb{F}_{2^m}^n$ such that $\Gamma(L,g)=\mathrm{GRS}_{n-\deg g(z)}(L,\lambda)\,|\,\mathbb{F}_2$. Moreover $\mathrm{GRS}_{n-\deg g(z)}(L,\lambda)^{\perp}=\mathrm{GRS}_{\deg g(z)}(L,\gamma)$ where $\gamma=(g(\alpha_1)^{-1},\ldots,g(\alpha_n)^{-1})$. Hence

$$\Gamma(L,g)^{\perp}=T_m(\mathrm{GRS}_{\deg g(z)}(L,\gamma))$$

Applying Delsarte's result, this gives a general formula for the dimension of any Goppa code:

$$k=n-m\deg g(z)+\dim_{\mathbb{F}_2}\ker(T_m)$$

In order to define codes with higher dimension than the classical bound, a strategy is to find polynomials $g(z)$ such that the kernel of the "trace map" T_m is large. Such an idea has been used in [13,14]. Authors have mainly focussed their attention on primitive Goppa codes, i.e. codes such that $z^{2^m}+z$ divides $g(z)\prod_{\beta\in L}(z+\beta)$. An important result given in [13] is that the dimension of the kernel of the trace map T_m is equal to the number of solutions of a modular equation referred to as the *redundancy equation*.

PROPOSITION 6. *The dimension of the kernel of* T_m *is equal to the number of polynomials* $a(z)\in\mathbb{F}_{2^m}[z]$ *(*$\deg a(z)<\deg g(z)$*) satisfying*

$$g(z)^{2^{m-1}+1}\,Tr_{\mathbb{F}_{2^m}:\mathbb{F}_2}\left(\frac{a(z)}{g(z)}\right)\equiv 0 \pmod{z^{2^m}+z}$$

THEOREM 2. *Let $m=2s$ and $g(z)^{2^s} \equiv g(z) \pmod{z^{2^{2s}+z}}$, the following table sums up the new lower bounds obtained in [13, 14] using strategy 2.*

k	*Remarks*
$\tilde{k}+s$	$\deg g(z)=2^s$
$\tilde{k}+3s$	$\deg g(z)\geq 2^s+1$

5. Three Conjectures

Among the class of polynomials which satisfy $g(z)^{2^s} \equiv g(z) \pmod{z^{2^{2s}+z}}$, authors of [14] have considered three special polynomials:

- $g_1(z)=z^{2^s}+z$,
- $g_2(z)=z^{2^s+1}+1$,
- $g_3(z)=g_1(z)/h(z)$ where $h(z)=z$ or $z+1$.

For these polynomials the lower bound on the dimension can be again improved and three new values have been computed (let L_i be $\mathbb{F}_{2^{2s}} \setminus \{z \in \mathbb{F}_{2^{2s}} \mid g_i(z)=0\}$):

- $\dim \Gamma(L_1, g_1) \geq n-2s \deg g_1(z)+3s-1$,
- $\dim \Gamma(L_2, g_2) \geq n-2s \deg g_2(z)+5s$,
- $\dim \Gamma(L_3, g_3) \geq n-2s \deg g_3(z)+s-1$.

Using a computer authors checked that these bounds were reached for $s=2$, 3, 4, 5. Till now it was an open problem to know if it was reached for all $s \geq 5$. It was recently proved in [19] that the true dimension of the code defined by $g_1(z)$ was effectively $n-2s \deg g_1(z)+3s-1$. The aim of this paper is to prove the other two conjectures.

We will first consider the polynomial $g_3(z)$ because the proof is quite different than those made for $g_1(z)$ and uses results stated in [4, 18]. We will furthermore prove a more general result by looking for polynomials equal to $g_1(z)/(z+\beta)$ for any $\beta \in \mathbb{F}_{2^s}$ (instead of $g_1(z)/z$ or $g_1(z)/(z+1)$).

6. True Dimension of $\Gamma(L_3, g_3)$

In this section we will prove a more general conjecture than the original one. Let $\beta \in \mathbb{F}_{2^s}$ and denote by $g_{3,\beta}$ the polynomial $(z^{2^s}+z)/(z+\beta)$, and let $L_{3,\beta}$ be the set $\{\beta, \alpha_1, \ldots, \alpha_n\}$ where $\{\alpha_1, \ldots, \alpha_n\} = L_1 = \mathbb{F}_{2^{2s}} \setminus \mathbb{F}_{2^s}$. With these notations, the conjecture stated in [14] concerns $g_{3,0}(z)$ and $g_{3,1}(z)$. In order to state the main result, we will first prove some intermediate results.

LEMMA 1. *All codes* $\Gamma(L_{3,\beta}, g_{3,\beta})$ *are equivalent to* $\Gamma(L_{3,0}, g_{3,0})$.

Let $\beta \in \mathbb{F}_{2^s}$, notice that $\Gamma(L_{3,\beta}, g_{3,\beta})$ is equivalent to $\Gamma(L', g_{3,\beta})$ where $L' = \{\beta, \alpha_1 + \beta, \ldots, \alpha_n + \beta\}$ since this set is a permutation of $L_{3,\beta}$. Now consider the mapping

$$\begin{aligned} \pi_\beta : L_{3,0} &\longrightarrow L' \\ x &\mapsto x + \beta \end{aligned}$$

Since π is an affine map, a well known result on equivalent Goppa codes [7] states that $\Gamma(L_{3,0}, g_{3,0})$ is equivalent to $\Gamma(L', g'_\beta)$ where $g'_\beta(z) = g_{3,0}(z+\beta)$. Now $g_{3,0}(z+\beta) = ((z+\beta)^{2^s} + z + \beta)/(z+\beta) = g_{3,\beta}(z)$ (since $\beta \in \mathbb{F}_{2^s}$).

LEMMA 2. *Let* $c = (c_0, c_1, \ldots, c_n) \in \mathbb{F}_{2^{n+1}}$ *and* $\omega(c)$ *be the Hamming weight of c, then*

$$\begin{array}{lcl} c \in \Gamma(L_{3,0}, g_{3,0}) & & c_0 = 0 \\ \textit{and} & \Longleftrightarrow & \textit{and} \\ \omega(c)\ \textit{even} & & (c_1, \ldots, c_n) \in \Gamma(L_1, g_1) \end{array}$$

The parity check matrix of $\Gamma(L_{3,0}, g_{3,0})$ can be expressed as

$$H = \begin{pmatrix} 1 & \\ 0 & \\ \vdots & H' \\ 0 & \end{pmatrix}$$

where

$$H' = \begin{pmatrix} g_{3,0}(\alpha_1)^{-1} & \cdots & g_{3,0}(\alpha_n)^{-1} \\ \alpha_1 g_{3,0}(\alpha_1)^{-1} & \cdots & \alpha_n g_{3,0}(\alpha_n)^{-1} \\ \vdots & \vdots & \vdots \\ \alpha_1^{2^s-2} g_{3,0}(\alpha_1)^{-1} & \cdots & \alpha_n^{2^s-2} g_{3,0}(\alpha_n)^{-1} \end{pmatrix}$$

is a parity check matrix of the code $\Gamma(L_1, g_{3,0})$. Let $c = (0, c_1, \ldots, c_n)$ such that $(c_1, \ldots, c_n) \in \Gamma(L_1, g_1)$. From [18] all codewords of $\Gamma(L_1, g_1)$ have even weight, hence $\omega(c)$ is even. Moreover it is clear that c satisfies $Hc^t = 0$, hence $c \in \Gamma(L_{3,0}, g_{3,0})$.

Conversely, let c be an even weight codeword of $\Gamma(L_{3,0}, g_{3,0})$. If $c_0 = 0$, since $Hc^t = 0$, we easily deduce that $H'(c_1, \ldots, c_n)^t = 0$, hence $(c_1, \ldots, c_n)$ belongs to $\Gamma(L_1, g_{3,0})$. Now it has been proved in [18] that $\Gamma(L_1, g_{3,0})$ and $\Gamma(L_1, g_1)$ are exactly the same code.

Suppose now that $c_0 = 1$ then using the first row of H, we have

$$\begin{aligned} & 1 + \textstyle\sum_{i=1}^n c_i (\mathrm{Tr}_{\mathbb{F}_{2^{2s}}:\mathbb{F}_{2^s}}(\alpha_i)/\alpha_i)^{-1} && = 0 \\ \Rightarrow\ & \mathrm{Tr}_{\mathbb{F}_{2^{2s}}:\mathbb{F}_{2^s}}\left(\textstyle\sum_{i=1}^n c_i \alpha_i \mathrm{Tr}_{\mathbb{F}_{2^{2s}}:\mathbb{F}_{2^s}}(\alpha_i)^{-1}\right) && = 0 \\ \Rightarrow\ & \textstyle\sum_{i=1}^n c_i && = 0 \end{aligned}$$

Hence $\omega(c_1, \ldots, c_n)$ is even which is a contradiction since $c = (1, c_1, \ldots, c_n)$ and $\omega(c)$ is even.

THEOREM 3. *$\forall \beta \in \mathbb{F}_{2^s}$, the dimension of the Goppa code $\Gamma(L_{3,\beta}, g_{3,\beta})$ is* $n - 2s \deg g_{3,\beta}(z) + s - 1$.

Let $\beta \in \mathbb{F}_{2^s}$, from Lemma 1, dim $\Gamma(L_{3,\beta}, g_{3,\beta})$=dim $\Gamma(L_{3,0}, g_{3,0})$. From Lemma 2, there is a one to one mapping between the set of even weight codewords of $\Gamma(L_{3,0}, g_{3,0})$ and $\Gamma(L_1, g_1)$. Moreover, from [4], we know that there exists odd weight codeword in $\Gamma(L_{3,0}, g_{3,0})$. Let us denote by $[n, k]$ the parameters of $\Gamma(L_{3,0}, g_{3,0})$, and by $[n', k']$ those of $\Gamma(L_1, g_1)$, we conclude that $k = k' + 1$ (and we already know that $n = n' + 1$). Now it has been proved in [19] that $k' = n' - 2s2^s + 3s - 1$. Hence

$$\begin{aligned} k &= n' - 2s2^s + 3s \\ &= n' + 1 - 2s(2^s - 1) + s - 1 \\ &= n - 2s \deg g_{3,0}(z) + s - 1 \end{aligned}$$

7. True Dimension of $\Gamma(L_2, g_2)$

The proof of the conjecture is quite long, boring and does not bring any new mathematical material since it follows exactly the same steps which allowed us to compute the true dimension of the Goppa codes defined by $g_1(z)$. Hence this section is to be considered as an addendum of [19].

We only give an outline of the proof, interested readers can find full details here: http://veron.univ-tln.fr/PAPERS/proof.pdf. We only have to show that $\dim \Gamma(L_2, g_2) \leq n - 2s \deg g_2(z) + 5s$ since from [14] we already know that $\dim \Gamma(L_2, g_2) \geq n - 2s \deg g_2(z) + 5s$. Now, remember that the dimension is linked to the number of solutions of the redundancy equation (cf. prop. 6). Hence, because of the properties of $g_1(z)$, we are searching how many polynomials $a(z)$ of degree less or equal than 2^s satisfy:

$$g(z)^{2^{s-1}+1} \mathrm{Tr}_{\mathbb{F}_{2^s}:\mathbb{F}_2}\left(\frac{a(z) + a(z)^{2^s}}{g(z)}\right) \equiv 0 \pmod{z^{2^{2s}} + z} \tag{1}$$

Let $a(z) = \sum_{j=0}^{2^s} a_j z^j$, we express this equation over $\mathbb{F}_{2^{2s}}[z]$ and search for monomials whose coefficient is one of the a_i's and not a linear combination of them. We can then state that:

PROPOSITION 7. *Let $a(z) = \sum_{j=0}^{2^s} a_j z^j$ be a polynomial of degree at most 2^s. If $a(z)$ satisfies the redundancy equation (1) then $a(z) = a_0 + a_1 z + a_{2^{s-1}} z^{2^{s-1}} + a_{2^{s-1}+1} z^{2^{s-1}+1} + a_{2^s} z^{2^s}$.*

From this canonical form of $a(z)$ and the redundancy equation, we can deduce some constraints on a_0, a_1, $a_{2^{s-1}}$, $a_{2^{s-1}+1}$, a_{2^s}.

PROPOSITION 8. *Let* $a(z)=a_0+a_1z+a_{2^{s-1}}z^{2^{s-1}}+a_{2^{s-1}+1}z^{2^{s-1}+1}+a_{2^s}z^{2^s}$. *If* $a(z)$ *satisfies equation (1), then* $a_0\in\mathbb{F}_{2^s}$, $a_{2^{s-1}+1}=a_{2^{s-1}}^{2^s}$ *and* $a_1+a_{2^{s-1}}^{2^{s+1}}+a_{2^s}^{2^s}=0$.

This shows that there are at most 2^{5s} polynomials $a(z)$ which satisfy the redundancy equation, hence:

THEOREM 4. *Let* $g(z)=z^{2^s+1}+1$, $L=\mathbb{F}_{2^{2s}}\setminus\{z\in\mathbb{F}_{2^{2s}}\mid g(z)=0\}$ *and* $n=card(L)$, *the dimension of the Goppa code* $\Gamma(L,g)$ *satisfies*

$$k=n-2s\deg g(z)+5s$$

Acknowledgments

The author wishes to warmly thank an anonymous referee for numerous suggestions which have helped in improving the presentation of these results.

References

1. S. V. Bezzateev, E. T. Mironchikov and N. A. Shekhunova, One subclass of binary Goppa codes, *Proc. XI Simp. po Probl. Izbit. v Inform. Syst.*, (1986) pp. 140–141.
2. S. V. Bezzateev and N. A. Shekhunova, On the subcodes of one class Goppa Codes, *Proc. Intern. Workshop Algebraic and Combinatorial Coding Theory ACCT-1* (1988) pp. 143–146.
3. S. V. Bezzateev, E. T. Mironchikov and N. A. Shekhunova, A subclass of binary Goppa code, *Problemy Peredachi Informatsii*, Vol. 25, No. 3 (1989) pp. 98–102.
4. S. V. Bezzateev and N. A. Shekhunova, Subclass of binary Goppa codes with minimal distance equal to the design distance, *IEEE Transactions on Information Theory*, Vol. 41, No. 2 (1995) pp. 554–555.
5. S. V. Bezzateev and N. A. Shekhunova, A subclass of binary Goppa codes with improved estimation of the code dimension, *Designs Codes and Cryptography*, Vol. 14, No. 1 (1998) pp. 23–38.
6. P. Delsarte, On subfield subcodes of modified Reed-Solomon codes, *IEEE Transactions on Information Theory*, Vol. IT-21 (1975) pp. 575–576.
7. J. K. Gibson, Equivalent Goppa codes and trapdoors to McEliece's public key cryptosystem, In *Advances in Cryptology—Eurocrypt'91*, LNCS No. 547, Springer-Verlag (1991) pp. 517–521.
8. V. D. Goppa, A new class of linear error correcting codes, *Problemy Peredachi Informatsii*, Vol. 6, (1970) pp. 24–30.
9. *Handbook of Coding Theory*, Vol. 1, V. S. Pless and W. C. Huffman (ed.), NorthHolland (1998).
10. J. M. Jensen, Subgroup subcodes, *IEEE Transactions on Information Theory*, Vol. 41, No. 3 (1995) pp. 781–785.
11. M. Loeloeian and J. Conan, A transform approach to Goppa codes, *IEEE Transactions on Information Theory*, Vol. IT-33 (1987) pp. 105–115.
12. F. J. Mac Williams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North Holland (1983).
13. A. M. Roseiro, The trace operator and generalized Goppa codes, Ph.D. Dissert., Dept. of Elect. Eng., Michigan State Univ., East Lansing, MI 48823 (1989).
14. A. M. Roseiro, J. I. Hall, J. E. Hadney and M. Siegel, The trace operator and redundancy of Goppa codes, *IEEE Transactions on Information Theory*, Vol. 38, No. 3 (1992) pp. 1130–1133.
15. H. Stichtenoth, On the dimension of subfield subcodes, *IEEE Transactions on Information Theory*, Vol. 36, (1990) pp. 90–93.
16. M. van der Vlugt, The true dimension of certain binary Goppa codes, *IEEE Transactions on Information Theory*, Vol. 36, No. 2 (1990) pp. 397–398.

17. M. van der Vlugt, On the dimension of trace codes, *IEEE Transactions on Information Theory*, Vol. 37, No. 1 (1991) pp. 196–199.
18. P. Véron, Goppa codes and trace operator, *IEEE Transactions on Information Theory*, Vol. 44, No. 1 (1998) pp. 290–295.
19. P. Véron, True dimension of some binary quadratic trace Goppa codes, *Designs Codes and Cryptography*, Vol. 24, No. 1 (2001) pp. 81–97.