Subclass of non-binary cumulative Goppa codes

Sergey Bezzateev and Natalia Shekhunova

Saint Petersburg State University of Airspace Instrumentation
Saint-Petersburg, Russia
e-mail: bsv@aanet.ru, sna@delfa.net

Fq 9
THE 9TH INTERNATIONAL CONFERENCE ON
FINITE FIELDS AND THEIR APPLICATIONS
UCD, July 13-17 2009

Classical Goppa codes

A q-ary vector $a=(a_1,\ldots a_n)$ of length n is a codeword of the Γ(L,G) Goppa code if and only if

$$\sum_{i=1}^{n} a_i \frac{1}{x-\alpha_i} \equiv 0 \bmod G(x)$$

$G(x)$ is Goppa polynomial with the coefficients from $GF(q^m)$ and L is a locator set:

$$L=\{\alpha_1,\alpha_2,...,\alpha_n\},\ \alpha_i \in GF(q^m), G(\alpha_i)\neq 0,\ \alpha_i \neq \alpha_j\ \forall i \neq j.$$

Parameters of q-ary Goppa codes are :

Code length is $n \le q^m$,

Code redundancy is $r \le m \cdot \deg G(x)$,

Code dimension is $k \ge n - m \cdot \deg G(x)$,

Minimal distance is $d \ge \deg G(x)+1$.

Classification of Goppa codes

- Cumulative Γ(L,G)-code

$$G(x) = (x - \alpha)^l, \alpha \in \{GF(q^m) \setminus L\}$$

  - Cyclic Γ(L,G)-code

$$G(x) = x^l, L = \{\alpha^i, i = 1,..,n\}, \alpha^n = 1.$$

    Cyclic Goppa codes are BCH-codes.

- Separable Γ(L,G)-code

$$G(x) = \prod_{i=1}^{l} (x - \beta_i), \ \beta_i \notin L; \beta_i \neq \beta_j, \forall i \neq j; i, j = 1,..,l$$

  - Irreducible Γ(L,G)-code

    G(x) is irreducible polynomial over GF(q^m),

$$G(x) = \prod_{i=1}^{l} (x - \beta_i), \ \beta_i \notin GF(q^m), \beta_i \neq \beta_j, \forall i \neq j; \ i, j = 1,..,l$$

Cumulative Goppa codes

$$G(x)=(x-\alpha_j)^l, \alpha_j \in GF(q^m), L \subseteq GF(q^m)\setminus\{\alpha_j\}$$

Lemma 1 [F.J. Mac Williams, N.J.A Sloane]

Cumulative Goppa code with

$$G(x) = (x - \alpha_j)^l,\ L = GF(q^m)\setminus\{\alpha_j\}$$

is equivalent to cumulative Goppa code with

$$G(x) = x^l,\ L = GF(q^m)\setminus\{0\}$$

and it is equivalent to primitive q-ary BCH- code with length $n=q^m-1$ and parity check matrix

$$H = \begin{vmatrix} 1 & \alpha^{-\ell} & \dots & \alpha^{-(n-1)\ell} \\ 1 & \alpha^{-(\ell-1)} & \dots & \alpha^{-(n-1)(\ell-1)} \\ \dots & \dots & \dots & \dots \\ 1 & \alpha^{-1} & \dots & \alpha^{-(n-1)} \end{vmatrix}$$

Cumulative Goppa codes

Lemma 2 [F.J. Mac Williams, N.J.A Sloane]

Cumulative q-ary Goppa code with

$$G(x) = (x - \alpha_j)^q,\ L \subseteq GF(q^m) \setminus \{\alpha_j\}$$

is equivalent to cumulative Goppa code with

$$G^*(x) = (x - \alpha_j)^{q-1},\ L \subseteq GF(q^m) \setminus \{\alpha_j\}$$

Parameters of cumulative q-ary Goppa codes are :

Code length is $n \le q^m - 1$,

Code redundancy is $r \le m \cdot (\deg G(x) - \frac{\deg G(x)}{q})$

Code dimension is $k \ge n - m \cdot r$,

Minimal distance is $d \ge \deg G(x) + 1$.

Separable Goppa codes

G(x) is the separable polynomial with coefficients from GF(q^m)

$$G(x) = \prod_{i=1}^{l} (x - \beta_i),\ L \subseteq GF(q^m) \setminus \{\beta_1, \ldots, \beta_t\}$$

where t =deg G(x) and $\beta_j \neq \beta_i$ for all $j \neq i$.

Parameters of separable q-ary Goppa codes are:

Code length is $n \leq q^m$,

Code redundancy is $r \leq m \cdot \deg G(x)$,

Code dimension is $k \geq n - m \cdot r$,

Minimal distance is $d \geq \deg G(x) + 1$.

In binary case we have improved estimation for minimal distance of the code:

$d \geq 2\deg G(x) + 1$.

Main questions

To find codes with:

- Improved estimations of parameters: dimension and minimal distance;
- Good parameters (VG bound);
- Special structure (large permutation group, quasi-cyclic, etc.);

Historical background in special classes of binary separable Goppa codes

M. Loeloeian and J. Conan (1984) presented (55,16,19) Goppa code with
$G(x) = (x - \alpha^{9})(x - \alpha^{12})(x - \alpha^{30})(x - \alpha^{34})(x - \alpha^{42})(x - \alpha^{43})(x - \alpha^{50})(x - \alpha^{54})$,
where α is a primitive element of $GF(2^6)$. $d_{ds}=17 < d=19$.

S.Bezzateev and N. Shekhunova (1986) considered
$G(x) = x^{t+1} + V^t x^t + Vx + 1$, "Subfield subcodes", where $L \subset GF(t^2)$, $t=2^l$,
$V \in \{GF(t^2)\backslash\{1\}\}$,
$n = t^2 - t - 1$.
$k \geq \mathbf{t^2 - t - 1} - 2l(t - 3/2)$, $d \geq d_{ds}= 2t+3$.

M. Loeloeian and J. Conan (1987),
$G(x) = x^t + x$, where $L \subset GF(t^2)$ and
$n = t^2 - t$. $k \geq \mathbf{t^2 - t} - 2l(t - 3/2) - 1$, $d \geq d_{ds}= 2t+1$.

A.M.Roseiro, J.I.Hall, J.E.Adney and M.Siegel (1992)
By representation $G^t(x) = G(x) \bmod (x^{t^2} + x)$,
$k \geq \mathbf{t^2 - t} - 2l(t - 3/2) - 1$, $d \geq d_{ds}= 2t+1$.

Historical background in special classes of binary separable Goppa codes

S.Bezzateev and N. Shekhunova (1995) described codes with
$G(x) = x^{t-1} + 1$, $k \geq \mathbf{t^2 - t} - 2l(t - 3/2)$, and we have proved that $d = d_{ds} = 2t-3$

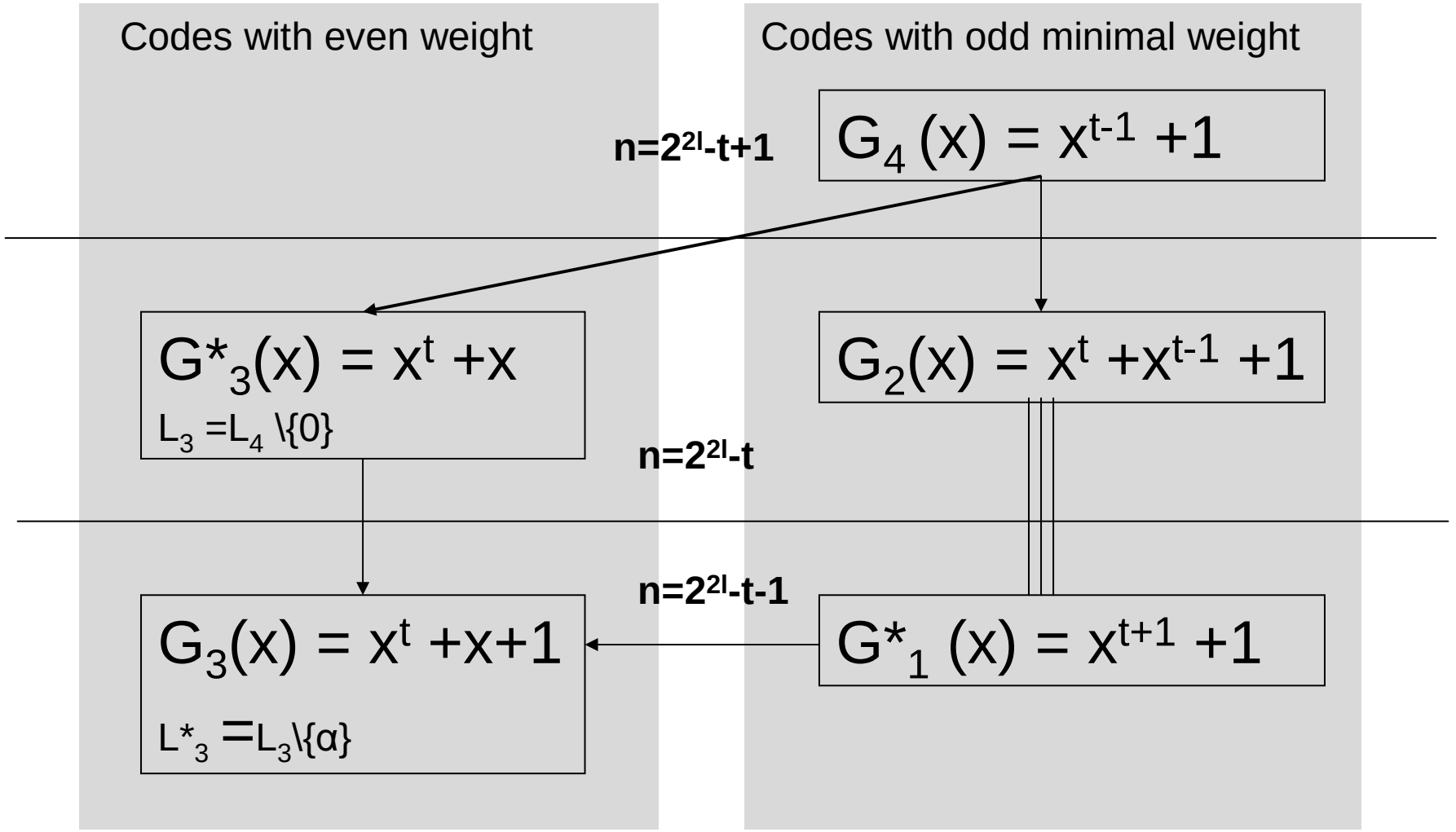
P. Veron (2001) $G(x) = x^t + x$ - “Quadratic trace Goppa codes”.
$k = \mathbf{t^2 - t} - 2l(t - 3/2) - 1$, $d \geq 2t+4$

P. Veron (2005) $G(x) = x^{t+1}+V^tx^t+Vx+1$.
$k = \mathbf{t^2 - t - 1} - 2l(t - 3/2)$
and $G(x) = x^{t-1} +1$, $k = \mathbf{t^2 - t +1} - 2l(t - 3/2) -1$

S.Bezzateev and N. Shekhunova (1995), P. Veron(1998), G. Bommer and F.Blanchet (2000) - all the forementioned codes are quasi-cyclic binary Goppa codes.

S.Bezzateev and N. Shekhunova (2008), Chain of Separable Binary Goppa Codes,

Code chain of binary separable codes



Special classes of non-binary separable codes

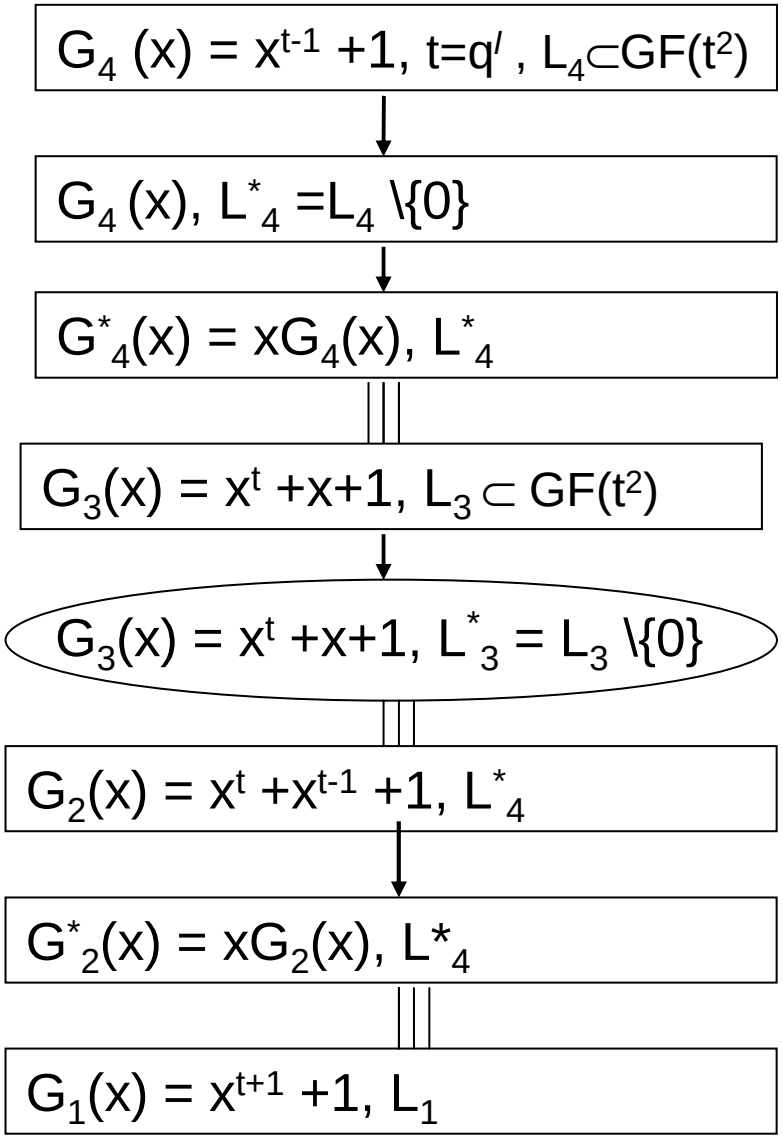
$G_4(x) = x^{t-1} + 1, \quad L_4 = \{GF(t^2) \setminus GF(t)\} \cup \{0\}, \; t = q^l,$

$G_3(x) = x^t + x + 1, \quad L_3 = GF(t^2) \setminus \{\alpha : G_3(\alpha) = 0\}, \; t = q^l,$

$G_2(x) = x^t + x^{t-1} + 1, \quad L_2 = GF(t^2) \setminus \{\alpha : G_2(\alpha) = 0\}, \; t = q^l,$

$G_1(x) = x^{t+1} + 1, \quad L_1 = GF(t^2) \setminus \{\alpha : G_1(\alpha) = 0\}, \; t = q^l,$

Code chain for non-binary separable Goppa codes



Estimation of Minimal distance

Theorem 1

The minimal distance of Γ (L_4; $G_4(x) = x^{t-1} + 1$) code is

$\boldsymbol{d_4} = \deg G_4(x) + 1 = t$.

Theorem 2

The minimal distance of Γ (L_1; $G_1(x) = x^{t+1} + 1$) code is

$\boldsymbol{d_1} = \deg G_1(x) + 1 = t+2$.

Theorem 3

The minimal distance of Γ (L_3; $G_3(x) = x^t + x + 1$) code is

$t+2 = \deg G_3(x) + 2 \leq \boldsymbol{d_3} \leq \deg G_3(x) + 3 = t+3$.

Estimation of Dimension

Theorem 4

The dimension of Γ (L_4; $G_4(x) = x^{t-1} + 1$) code is

$$k_4 \geq n_4 - (2\ell \deg G_4(x) - \ell + 1) .$$

Theorem 5

The dimension of Γ (L_3; $G_3(x) = x^t + x + 1$) code is

$$k_3 = k_4 - 1 .$$

“Cumulative-separable” non-binary Goppa codes

$$G(x) = \left(G_0(x)\right)^f, L \subseteq GF(q^m) \setminus \{\alpha : G_0(\alpha) = 0\}, f > 1,$$

where $G_0(x)$ is separable polynomial.

.

Consequence 1 (from **Lemma2**)
Goppa code with $G(x)=G_0(x)^q$ is equivalent to code with $G(x)=G_0(x)^{q-1}$.

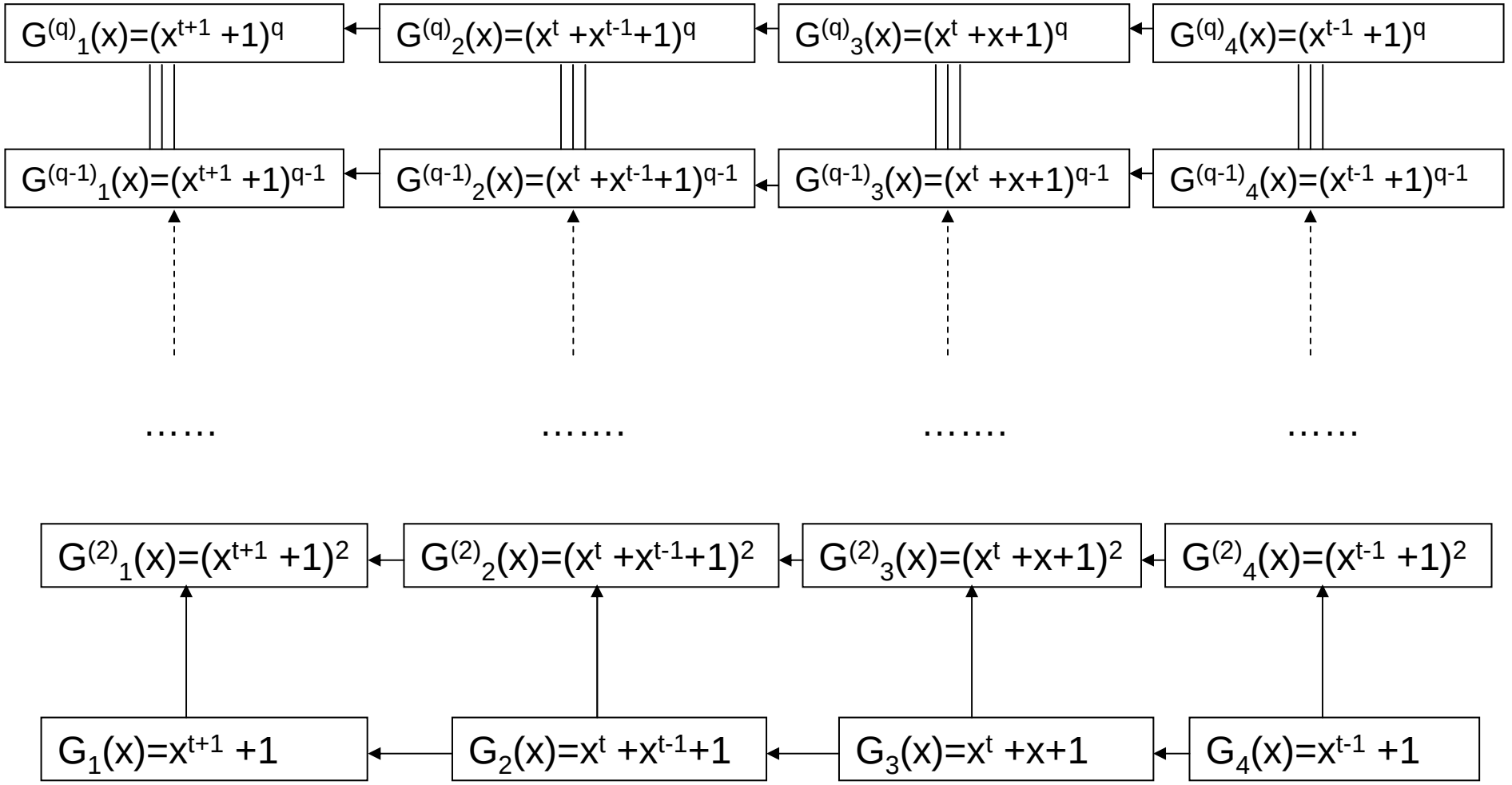
Lemma 3
Dimension k of “cumulative-separable” Goppa code with

$$G(x) = \left(G_0(x)\right)^q, L \subseteq GF(q^m) \setminus \{\alpha : G_0(\alpha) = 0\}$$

is estimated by inequality:

$$k \geq n - m(q-1)\deg G_0(x).$$

Chain structure for “cumulative-separable” codes



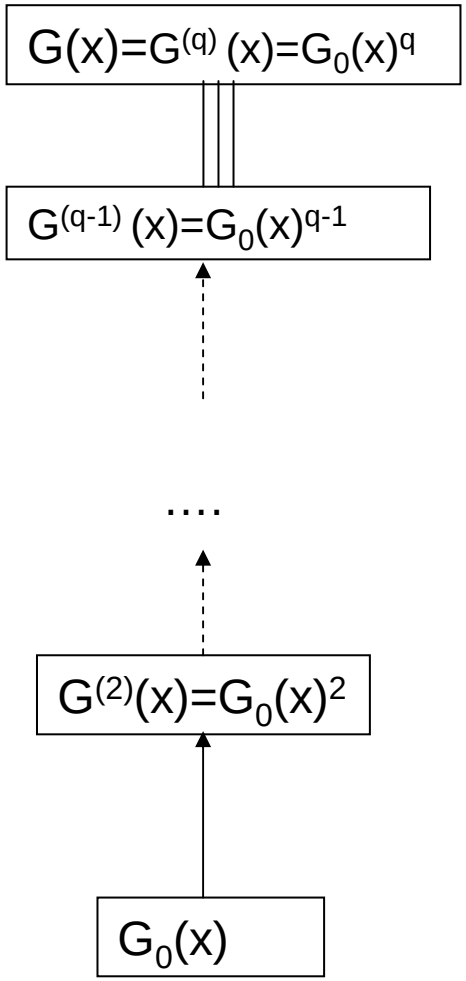
$t=q^{\ell}$, $L \subseteq GF(q^{2\ell})$

Parity check matrix for "cumulative–separable" Goppa code

$$G(x) = \left(G_0(x)\right)^q,\ L \subseteq GF(q^m) \setminus \{\alpha : G_0(\alpha) = 0\},\ \deg G_0(x) = \tau.$$

$$H_q = \begin{array}{|cccc|l|}
\hline
\frac{1}{G_0(\alpha_1)^{q-1}} & \frac{1}{G_0(\alpha_2)^{q-1}} & \cdots & \frac{1}{G_0(\alpha_n)^{q-1}} & \\
\frac{\alpha_1}{G_0(\alpha_1)^{q-1}} & \frac{\alpha_2}{G_0(\alpha_2)^{q-1}} & \cdots & \frac{\alpha_n}{G_0(\alpha_n)^{q-1}} & = h_{q-1} \\
\cdots & \cdots & \cdots & \cdots & \\
\frac{\alpha_1^{\tau-1}}{G_0(\alpha_1)^{q-1}} & \frac{\alpha_2^{\tau-1}}{G_0(\alpha_2)^{q-1}} & \cdots & \frac{\alpha_n^{\tau-1}}{G_0(\alpha_n)^{q-1}} & \\
\hline
\frac{1}{G_0(\alpha_1)^{q-2}} & \frac{1}{G_0(\alpha_2)^{q-2}} & \cdots & \frac{1}{G_0(\alpha_n)^{q-2}} & \\
\frac{\alpha_1}{G_0(\alpha_1)^{q-2}} & \frac{\alpha_2}{G_0(\alpha_2)^{q-2}} & \cdots & \frac{\alpha_n}{G_0(\alpha_n)^{q-2}} & = h_{q-2} \\
\cdots & \cdots & \cdots & \cdots & \\
\frac{\alpha_1^{\tau-1}}{G_0(\alpha_1)^{2}} & \frac{\alpha_2^{\tau-1}}{G_0(\alpha_2)^{2}} & \cdots & \frac{\alpha_n^{\tau-1}}{G_0(\alpha_n)^{2}} & \\
\hline
\frac{1}{G_0(\alpha_1)} & \frac{1}{G_0(\alpha_2)} & \cdots & \frac{1}{G_0(\alpha_n)} & \\
\frac{\alpha_1}{G_0(\alpha_1)} & \frac{\alpha_2}{G_0(\alpha_2)} & \cdots & \frac{\alpha_n}{G_0(\alpha_n)} & = h_1 \\
\cdots & \cdots & \cdots & \cdots & \\
\frac{\alpha_1^{\tau-1}}{G_0(\alpha_1)} & \frac{\alpha_2^{\tau-1}}{G_0(\alpha_2)} & \cdots & \frac{\alpha_n^{\tau-1}}{G_0(\alpha_n)} & \\
\hline
\end{array}$$

Embedded “cumulative-separable” q-ary Goppa codes



The parity check matrix for code with Goppa polynomial $G^{(i)}(x)$ is H_i .

Then parity check matrix for code with Goppa polynomial $G^{(i+1)}(x)$ is

$$H_{i+1}=\begin{vmatrix} h_{i+1} \\ H_i \end{vmatrix}$$

Estimation of Minimal distance

Theorem 8

The minimal distance of Γ (L_4; $G_4^{(q)}(x)$= (x^{t-1} $+1)^q$) code is

$\boldsymbol{d_4} \geq \deg G_4^{(q)}(x) + 1 = q(t-1)+1$.

Theorem 9

The minimal distance of Γ (L_1; $G_1^{(q)}(x)$= (x^{t+1} $+1)^q$) code is

$\boldsymbol{d_1} \geq \deg G_1^{(q)}(x) + 1 = q(t+1)+1$.

Dimension of the Goppa code with $G_1(x)=(x^{t+1}+1)^q$

Let us consider submatrix h_i of the parity check matrix H_{q-1} for the Goppa code with $G_1(x)$

$$h_i = \begin{vmatrix} \frac{1}{G_0(\alpha_1)^{q-1}} & \frac{1}{G_0(\alpha_2)^i} & \dots & \frac{1}{G_0(\alpha_{n-1})^i} & \frac{1}{G_0(\alpha_n)^i} \\ \frac{\alpha_1}{G_0(\alpha_1)^{q-1}} & \frac{\alpha_2}{G_0(\alpha_2)^i} & \dots & \frac{\alpha_{n-1}}{G_0(\alpha_{n-1})^i} & \frac{\alpha_n}{G_0(\alpha_n)^i} \\ \dots & \dots & \dots & \dots & \dots \\ \frac{\alpha_1^t}{G_0(\alpha_1)^i} & \frac{\alpha_2^t}{G_0(\alpha_2)^i} & \dots & \frac{\alpha_{n-1}^t}{G_0(\alpha_{n-1})^i} & \frac{\alpha_n^t}{G_0(\alpha_n)^i} \end{vmatrix}, \quad where\ \alpha_j \in GF(q^{2l}),\ j=1,..,n.$$

Theorem 9

In submatrix h_i it exists not more than $(t+1)\cdot 2l-\Delta_i$ linear independent q-ary rows.

$$\Delta_i = l + i\cdot 2l$$

Consequence

In matrix H_f, f<q-1 it exists not more than $f(t+1)\cdot 2l-\Delta$ linear independent q-ary rows

$$\Delta=\Delta_1+\Delta_2+\ldots+\Delta_f=(q-1)l+2l(1+2+\ldots+f)=(q-1)l+2l\frac{f(f+1)}{2}$$

Redundancy of the Goppa code with $G_1(x)=(x^{t+1}+1)^q$

Theorem 10

In submatrix h_{q-1} it exists not more than $(t+1)\cdot 2l-\Delta_{q-1}-\Delta^*_{q-1}$ linear independent q-ary rows.

$$\Delta_{q-1}=l+(q-1)\cdot 2l,\quad \Delta^*_{q-1}=(q-1)\cdot 2l.$$

Consequence

Redundancy of the Goppa code with $G_1(x)=(x^{t+1}+1)^q$, $t=q^l$, $n=t^2-t-1$ is

$$r\le 2l(q-1)(t+1)-2l\frac{(q-1)(q+3)}{2}=m\frac{q-1}{q}(d-2-\frac{q^2+3q-2}{2}),$$

$$d\ge q(t+1)+1,\ m=2l.$$

Therefore the redundancy coefficient is satisfied

$$c(q,d)\le\frac{q-1}{q}(d-2-\frac{q^2+3q-2}{2}).$$

Note: The extended BCH code obtained by adding the overall parity check has length q^m and redundancy coefficient

$$c_{BCH}(q,d)\le\frac{q-1}{q}(d-2).$$

Dimension of the Goppa code with $G_1(x)=(x^{t+1}+1)^q$

Dimension of this code is

$$k \geq n - 2l(q-1)(t - \frac{q+1}{2}),$$

$$where\ m = 2l,\ t = q^l,\ n = t^2 - t - 1.$$

Note: In case q=2 we obtain estimation for binary codes

$$k \geq n - m(t - \frac{3}{2}) \quad ,$$

$$where \quad m = 2l, t = 2^l, n = 2^{2l} - 2^l - 1.$$

Parameters of the Goppa codes with $G_1(x)=(x^{t+1}+1)^q$, $t=q^l$

q	$GF(q^{2l})$	$t=q^l$	$G_1(x)$	n	r estimation	r true	$d \geq q(t+1)+1$
3	l=2	9	$(x^{10}+1)^3$	71	56	55	31
	l=3	27	$(x^{28}+1)^3$	701	300	300	85
	l=4	81	$(x^{82}+1)^3$	6479	1264	1264	247
5	l=2	25	$(x^{26}+1)^5$	599	352	343	131
	l=3	125	$(x^{126}+1)^5$	15499	2928	2928	631
7	l=2	49	$(x^{50}+1)^7$	2351	1080	1055	351
11	l=2	121	$(x^{122}+1)^{11}$	14519	4600	4519	1343

Parameters of the Goppa codes with $G_4(x)=(x^{t-1}+1)^q$, $t=q^l$

q	$GF(q^{2l})$	$t=q^l$	$G_1(x)$	n	r estimation	r true	$d \geq q(t-1)+1$
3	l=2	9	$(x^8+1)^3$	73	57	56	25
	l=3	27	$(x^{26}+1)^3$	703	301	301	79
	l=4	81	$(x^{80}+1)^3$	6481	1265	1265	241
5	l=2	25	$(x^{24}+1)^5$	601	353	344	121
	l=3	125	$(x^{124}+1)^5$	15501	2929	2929	621
7	l=2	49	$(x^{48}+1)^7$	2353	1081	1056	337
11	l=2	121	$(x^{120}+1)^{11}$	14522	4601	4520	1331

Embedded codes * for ternary Goppa code with $G_1(x)=(x^{10}+2)^3$

$$G_1^{(i)}(x) = G_1(x)(x+2)^i$$

i	$G_1^{(i)}(x)$	n	k	d	$d_{\text{best known code}}$ http://www.codetables.de/
0	$(x^{10}+2)^3$	71	16	31	31
1	$(x^{10}+2)^3(x+2)$	71	15	33	32
4	$(x^{10}+2)^3(x+2)^4$	71	11	35	36
10	$(x^{10}+2)^3(x+2)^{10}$	71	7	42	42
13	$(x^{10}+2)^3(x+2)^{13}$	71	5	44	45

* Bezzateev S., Shekhunova N., On the subcodes of one class of Goppa codes, ACCT-1, Proceedings, Varna, 1988, pp. 143-146.

THANK YOU

FOR YOUR ATTENTION!

Fq 9
THE 9TH INTERNATIONAL CONFERENCE ON
FINITE FIELDS AND THEIR APPLICATIONS
UCD, July 13-17 2009