Introducing Three Best Known Binary Goppa Codes

Jan L. Carrasquillo–López[1] , Axel O. Gómez–Flores[2], Christopher Soto[3]

[1]Department of Mathematics, University of Puerto Rico at Cayey
[2]Department of Mathematics, University of Puerto Rico at Río Piedras
[3]Department of Mathematics, Queens College of the City University of New York

Abstract

The current best known $[239, 21]$, $[240, 21]$, and $[241, 21]$ binary linear codes have minimum distance 98, 98, and 99 respectively. In our research, we introduce three binary Goppa codes with Goppa polynomials $(x^{17}+1)^6, (x^{16}+x)^6$, and $(x^{15}+1)^6$. The Goppa codes are $[239, 21, 103]$, $[240, 21, 104]$, and $[241, 21, 104]$ binary linear codes respectively. These codes have greater minimum distance than the current best known codes (according to (2)) with the respective length and dimension. Thus, they have better error-correction capability. In addition, with the techniques of puncturing, shortening, and extending, we find more codes with a better minimum distance than the current best known codes with the respective length and dimension. Our codes are related to the Goppa codes described by M. Loeloeian and J. Conan in (1).

Background

Definition 1. Given a linear code C with length n, let A_w denote the number of codewords whose weight equals w. Then, the vector $[A_0, A_1, ..., A_n]$ is called the weight enumerator of C. The weight enumerator polynomial of C is defined by

$$W(C;x,y)=\sum_{w=0}^{n} A_w x^w y^{n-w}.$$

The lowest positive weight w such that $A_w \neq 0$ is the minimum distance of the code.

Definition 2. Let p be a prime and let $q = p^m$. Let $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a subset of $\mathbb{F}_q$. Let $g(x)$ be a polynomial such that $g(\alpha_i) \neq 0$, for $\alpha_i \in L$. The *p–ary Goppa code* is defined as

$$C(L,g) := \left\{ (c_1, c_2, \ldots, c_n) \in \mathbb{F}_p^n \;\middle|\; \sum_{i=1}^{n} \frac{c_i}{x-\alpha_i} \equiv 0 \mod g(x) \right\}.$$

Results

We have used the Coding Theory library of the SageMath programming language to determine the parameters of our codes. In particular, we used SAGE's own Goppa Codes constructor and its method to compute the weight distribution of each Goppa code.

Construction of [239,21,103] code

We computed that the binary Goppa code $C\left(L,(x^{17}+1)^6\right)$ is a $[239, 21, 103]$ code. This linear code has a higher minimum distance than the current best known $[239, 21, 98]$ binary code. Its weight enumerator polynomial is given by:

$$\begin{aligned} &x^{239}+62244x^{136}y^{103}+81396x^{135}y^{104}+190519x^{128}y^{111}+217736x^{127}y^{112}\\ &+496680x^{120}y^{119}+496680x^{119}y^{120}+217736x^{112}y^{127}+190519x^{111}y^{128}\\ &+81396x^{104}y^{135}+62244x^{103}y^{136}+y^{239}.\end{aligned}$$

By puncturing the $[239, 21, 103]$ code 12 times we get best known codes with the following parameters:

$[238, 21, 102]$, $[237, 21, 101]$, $[236, 21, 100]$, $[235, 21, 99]$,
$[234, 21, 98]$, $[233, 21, 97]$, $[232, 21, 96]$, $[231, 21, 95]$,
$[230, 21, 94]$, $[229, 21, 93]$, $[228, 21, 92]$, and $[227, 21, 91]$.

Construction of [240,21,104] code:

The binary Goppa code $C\left(L,(x^{16}+x)^6\right)$ is a $[240, 21, 104]$ code. This linear code has a higher minimum distance than the current best known $[240, 21, 98]$ binary code. Its weight enumerator polynomial is given by:

$$\begin{aligned} &x^{240}+143640x^{136}y^{104}+408255x^{128}y^{112}+993360x^{120}y^{120}\\ &+408255x^{112}y^{128}+143640x^{104}y^{136}+y^{240}.\end{aligned}$$

By shortening our $[240, 21, 104]$ code we get a $[239, 20, 104]$ code. By puncturing this one 7 times we get codes with the following parameters:

$[238, 20, 103]$, $[237, 20, 102]$, $[236, 20, 101]$, $[235, 20, 100]$,
$[234, 20, 99]$, $[233, 20, 98]$, and $[232, 20, 97]$.

Construction of [241,21,104] binary code:

The binary Goppa code $C\left(L,(x^{15}+1)^6\right)$ is a $[241, 21, 104]$ code. This linear code has a higher minimum distance than the current best known $[241, 21, 99]$ binary code. Its weight enumerator polynomial is given by:

$$\begin{aligned} &x^{240}y+143640x^{136}y^{105}+408255x^{128}y^{113}+993360x^{120}y^{121}\\ &+408255x^{112}y^{129}+143640x^{104}y^{137}+y^{241}.\end{aligned}$$

By extending the $[241, 21, 104]$ code to further lengths we get codes with following parameters:

$[242, 21, 104]$, $[243, 21, 104]$, $[245, 21, 104]$,
$[246, 21, 104]$, and $[247, 21, 104]$.

Other Best Known Codes

We are very grateful to M. Grassl for pointing out the following two constructions of new best known binary codes derived from the $[240, 21, 104]$ binary Goppa code.

With the technique from (3) it is actually possible to puncture the code at suitably chosen positions to obtain best known binary codes of parameters $[208, 21, 81]$, $[210, 21, 82]$, $[213, 21, 84]$, $[215, 21, 85]$, $[218, 21, 87]$, $[220, 21, 88]$, $[223, 21, 90]$, $[226, 21, 92]$, $[229, 21, 94]$, and $[229, 21, 94]$, but the very positions depend on the choice of the ordering of the elements of $\mathbb{F}_{256}$ when constructing the Goppa code in first place.

Applying Construction X (4) to the $[240, 21, 104]$ binary Goppa code, we can also find a best known $[249, 21, 106]$ binary code and a best known $[254, 22, 106]$ binary code.

Acknowledgements

Thanks to our mentor Dr. Fernando L. Piñero González for his mentorship and guidance throughout the entire project. We would also like to thank Dr. Anant Godbole for organizing the Puerto-Rico/East Tennessee REU with Dr. Piñero González and the National Science Foundation for supporing this work through their NSF-DMS REU-1852171 grant.

References

[1] M. Loeloeian and J. Conan, "A [55,16,19] binary Goppa code (Corresp.)", in IEEE Transactions on Information Theory, vol. 30, no. 5, pp. 773-773, September 1984, doi: 10.1109/TIT.1984.1056946.

[2] G. Markus, "Bounds on the minimum distance of linear codes and quantum codes", Online available at http://www.codetables.de, Accessed on 2020-10-09.

[3] M. Grassl and G. White, "New Good Linear Codes by Special Puncturings", in Proceedings 2004 IEEE International Symposium on Information Theory (ISIT 2004), Chicago, USA, June/July 2004, p. 454. DOI: 10.1109/ISIT.2004.1365491

[4] C. Tjhai, M. Tomlinson and M. Grassl, "Chains of cyclic codes, Construction X and incremental redundancy", 2008 IEEE Information Theory Workshop, Porto, 2008, pp. 323-327, doi: 10.1109/ITW.2008.4578678.

[5] J. Carrasquillo-López, A. Gómez-Flores, C. Soto, F. Piñero Introducing Three Best Known Goppa Codes, 2020, arXiv:2010.07278.