Words of Minimal Weight and Weight Distribution of Binary Goppa Codes

Matthieu Finiasz
INRIA Rocquencourt
78153 Le Chesnay Cedex, France

Abstract — **Little is known about the weight distribution of binary Goppa codes, however it is sure that it is close to a binomial distribution [5]. That is, the number of words of weight w in a code of length n is approximately $\binom{n}{w} \times 2^{k-n}$. This is true when w is not too small, but when w is close to 0 the distribution is not the same: for instance, for any weight from 1 to $2t$ the number of words is 0.**

Using an algorithm to find words of minimal weight we were able to perform some statistics on the small weights distribution and show that even for weights close to the minimal weight bound, the distribution is still binomial-like.

I. Words of Minimal Weight

Suppose we have a binary Goppa code Γ constructed over the field $\mathbb{F}_{2^m}$ with a polynomial g of degre t. This code will correct up to t errors, so our aim is to find words of weight $2t+1$.

We have an algorithm able to decode up to t errors [1], so if we try to decode a word of weight $t+1$ and the decoding works, it will give us a word of weight between 1 and $2t+1$. As there is no word of weight 1 through $2t$ in Γ we will necessarily have a word of weight $2t+1$. However this will only work if the decoding succeeds. If we call N_{2t+1} the number of words of minimal weight, the average number of tries before a decoding succeeds will be: $\binom{n}{t+1} / (N_{2t+1} \binom{2t+1}{t+1})$.

In [3] the case of decoding a random syndrome in a Goppa code is studied. It is shown that for a binary Goppa code correcting t errors, the ratio of decodable syndromes is approximately $1/t!$. This means that a random word has an average probability of $1/t!$ of being at a distance less or equal to t of a code word. This is true for a random word, but in our algorithm we only consider words of weight $t+1$ for which the average probability could be quite different.

However, if this ratio was respected, we would get $N_{2t+1} \simeq \frac{n^{t+1}}{(2t+1)!} \simeq \binom{n}{2t+1} \frac{1}{n^t}$ which is exactly the binomial distribution.

II. Known Values

In [2], Goppa codes correcting 3 errors are studied. They are classified and for each class the exact number of minimal weight words can be computed. The following table compares the obtained results to those expected if our asumption is true.

n	exact number	expected number
32	128	208
64	$\sim$ 2 640	3 328
128	47 616	53 261
256	$\sim$ 806 000	852 176
512	13 264 896	13 634 817

This table shows that when the length of the code increases our approximation gets closer to the real value. The error even decreases exponentially: 62%, 26%, 12%, 5.7%, 2.7%...

III. Experimentation

To be able to evaluate more precisely the quality of our estimation we compared it to experimental results: for each pair n and t shown in the following table we generated 50 random Goppa codes and decoded 20 words of weight $t+1$ for each of them. The numbers presented are the average number (calculated amoung the 1000 words) of attempts before a decoding succeeds. The "Theory" line is the number corresponding to what should be expected, that is $t!$

n \ t	5	6	7	8	9
512	146	866	5 903	45 491	–
1 024	138	755	5 308	44 172	425 400
2 048	125	721	4 892	44 827	367 767
4 096	119	769	4 773	38 685	368 646
8 192	120	750	5 235	41 036	383 443
16 384	123	732	5 470	39 351	374 139
32 768	120	662	5 193	42 309	357 590
65 536	116	693	5 372	39 643	360 973
Theory	120	720	5 040	40 320	362 880

IV. Conclusion

From these experiments and known results we can say that there is a good probability that, for codes of great length, the number of words of minimal weight tends to be what we expected: $N_{2t+1} = \frac{n^{t+1}}{(2t+1)!}$. However, for codes of smaller length, as we can see in the tables, the number of minimal weight words is a little smaller.

Performing the same experiment on words of weight $t+\alpha$ we obtain the same density of decodable words and deduce $N_{2t+\alpha} = \frac{n^{t+\alpha}}{(2t+\alpha)!}$ which is once again the binomial distribution.

The computational time required to make some statistics on codes correcting more errors is huge and we therefore cannot really check that our assumption remains true for a larger t, however it seems reasonable to believe that it will. Hence, it is possible to say that as long as t remains small compared to n, the weight distribution of binary Goppa codes is binomial-like, even for words of small weight.

References

[1] E. R. Berlekamp. "Goppa codes" In *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 590-592, 1973.

[2] A. Canteaut. *PHD Thesis* : "Attaques de cryptosystèmes à mots de poids faible et construction de fonctions t-Résilientes" chapter 2, example 2.14.

[3] N. Courtois, M. Finiasz, and N. Sendrier. "How to achieve a McEliece-based digital signature scheme" In *ASIACRYPT 2001*, Springer-Verlag, 2001.

[4] V. D. Goppa. "A new class of linear error-correcting codes" In *Probl. Inform. Transm.*, vol. 6, pp. 207-212, 1970.

[5] F. Levy-dit-Vehel and S. Litsyn. "Parameters of Goppa Codes Revisited" In *IEEE Transactions on Information Theory*, vol. 43, no. 6, November 1997.