Characteristic vector and weight distribution of a linear code

Stefka Bouyuklieva

Faculty of Mathematics and Informatics,
St. Cyril and St. Methodius University of Veliko Tarnovo, Bulgaria

stefka@ts.uni-vt.bg

Abstract. An algorithm for computing the weight distribution of a linear $[n, k]$ code over a finite field $\mathbb{F}_q$ is developed. The codes are represented by their characteristic vector with respect to a given generator matrix and a generator matrix of the k-dimensional simplex code $\mathcal{S}_k$.

We propose an algorithm for computing the weight distribution without listing all codewords. The linear codes here are represented by their characteristic vector χ. We obtain a vector whose coordinates are all non-zero weights in the code, by multiplying a special (recursively constructed) integer matrix by χ^{T}. The complexity for this multiplication is $O(kq^k)$, where k is the dimension of the considered code. The multiplication can be realized by a butterfly algorithm which is very fast in a parallel realization. The proposed algorithm is effective especially for codes with large length.

In the binary case, our approach is related to the Walsh-Hadamard transform, and so one can compute the weight distribution by using algorithms for fast Walsh transform which are easy for implementation. For codes over prime field with $p > 2$ elements we use an integer matrix of size $\theta(p, k) \times \theta(p, k)$ where $\theta(p, k) = \frac{p^k-1}{p-1}$. The weight distribution in this case can also be obtained by applying the generalized Walsh transform but then one has to use a $p^k \times p^k$ matrix. For codes over composite fields with $q = p^m$, $m > 1$, elements we use the trace map and take their images over the prime field $\mathbb{F}_p$.

We implemented the presented algorithm in a C/C++ program without special optimizations. Input data were randomly generated linear codes with lengths 300, 3000, 30000 and different dimensions over finite fields with 2, 3, 4, 5, and 7 elements. The results of our experiments show that the presented approach is faster for codes with large length. For example, calculating the weight distribution of codes with length 30000 with the presented algorithm is between 4 and 100 times faster (depending on the field) than the same calculation with the Magma software system.

Joint work with Iliya Bouyukliev and Paskal Piperkov (Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Veliko Tarnovo, Bulgaria) and Tatsuya Maruta (Department of Mathematical Sciences, Osaka Prefecture University, Sakai, Osaka 599-8531, Japan)
Partially funded by grant number DN 02/2/13.12.2016