A Computational model for linear codes

Xiao Ma, Xinmei Wang,

National Key Lab of ISN
XiDian University, P. O. Box 119
Xi'an 710071
P. R. China
xmwang@xidian.edu.cn

Ping Li

Department of Electronics Engineering
City University of Hong Kong
Tat Chee Avenue, Kowloon
Hong Kong
liping@ee.cityu.edu.hk

Abstract: An algorithm for a linear code is described based on its factor graph. For small parameters, the algorithm can be utilized to compute its weight enumerating function (WEF) and input-redundancy weight enumerating function (IRWEF). For large parameters, the algorithm can be utilized to compute the minimum Hamming weight by passing incomplete messages over the factor graphs.

Introduction: Let $C[n,k]$ be a binary linear block code with length of *n* and dimension of *k*. Let $H=[H_1H_2...H_n]$ be its parity check matrix, where H_j's $(1\le j\le n)$ are n $(n-k)$-dimensional binary column vectors. Construct a factor graph [1] corresponding to this code, illustrated as Fig.1. In Fig.1, a variable node x_i (represented by the unfilled circle) takes on values from the binary integer set $S=\{0,1,...,2^{n-k}-1\}$. In particular, $x_0=x_n=0$. While the filled circles (called subset nodes), represent local functions with the joined variable nodes as the arguments. For $1\le i\le n$, define local functions $f_{i-1,i}: S^{n+1}$ $Z[W]$, where S^{n+1} is the Cartesian product induced by *S* and $Z[W]$ is the polynomial ring over the integer ring. Specificly, $f_{i-1,i}(x_{i-1},x_i)=1$ if $x_i=x_{i-1}$ and $f_{i-1,i}(x_{i-1},x_i)=W$ if $x_i=x_{i-1}+H_i$ (mod 2) and $f_{i-1,i}(x_{i-1},x_i)=0$ otrherwise. It should be noted that, in the equation $x_i=x_{i-1}+H_i$, x_i's are viewed as $(n-k)$-dimensional binary column vectors. Define a global function

$$g(x_0,x_1,...,x_{n-1},x_n)=\prod_{1\le i\le n} f_{i-1,i}(x_i,x_{i-1}).$$

Clearly, $g(x_0,x_1,...,x_{n-1},x_n)\neq 0$ if and only if the sequence of nodes $x_0,x_1,...,x_{n-1},x_n$ is related to a codeword in the code $C[n,k]$. Furthermore, $g(x_0,x_1,...,x_{n-1},x_n)=W^w$ means that the corresponding codeword has Hamming weight of *w*. Therefore the weight enumerating function (WEF) $A(W)$ can be calculated as $A(W)=\sum_{x_1x_2...x_{n-1}} g(x_0,x_1,...,x_{n-1},x_n)$. The problem can be solved by the sum-product algorithm (SPA) [1], which has been shown to be extended to an arbitrary semiring. It should be noted that the SPA over the factor graph is equivalent to the gerneralized Viterbi algorithm (GVA) [3] over the trellis graph. It is also pointed out by [3] that the GVA can be utilized to calculate the WEF of any given trellis codes.

Disscussions: For a code $C[n,k]$ with small *n* and *k*, the sum-product algorithm can be utilized for calculating out its WEF. In other cases, we are faced with computational difficulties. Messages transmitted along edges of the factor graph are polynomials, which perhaps include so many monomials and some monomials have so large integer cofficients that it is impossibe to store and process these messages on computers. However, we can calculate out the monomials with lower degree of the WEF by discarding the monomials with degrees greater than some integer $D_{\max}$. In this case, the messages transmitted are incomplete.

Generalizations: By introducing another dummy variable *Z* and modifying slightly the local functions, we also can calculate out the input-redundancy weight enumerating function (IRWEF) [2] of a code. The method can be also applied to convolutional codes and other trellis codes by properly defining the factor graph.

Examples: Consider the code $C[20,10]$ defined by

H = [1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 41, 35, 190, 900, 737, 364, 214, 686, 338, 912].

Its WEF is

$$A(W) = 1 + 8W^4 + 12W^5 + 30W^6 + 84W^7 + 114W^8 + 162W^9 + 204W^{10} + 168W^{11} + 112W^{12} + 64W^{13} + 38W^{14} + 20W^{15} + 5W^{16} + 2W^{17}$$

.

Its IRWEF is

$$A(W) = 1 + W(2Z^3 + 3Z^4 + 3Z^5 + 2Z^6) + W^2(3Z^2 + 2Z^3 + 5Z^4 + 15Z^5 + 10Z^6 + 8Z^7 + 2Z^8) + \ldots + W^{10}Z^3$$

.

Conclusions: An algorithm for computing the WEF (or IRWEF) of a given linear code is described on the factor graph. For large parameters, the algorithm can be utilized to calculate out the minimum Hamming weight.

Acknowledgment: Xiao Ma wishes to thank Dr. Tong Zhao of Shanghai Jiaotong University for her helps, and Dr. Jun Chen for his providing the reference 1. This paper is supported in part by NSFC no. 69972035.

References

1 FREY, B. J., KSCHISCHANG, F. R., LOELIGER, H.-A., and WIBERG, N. : 'Factor graphs and algorithms', in *Proceedings of the 35th ALLerton Conference on Communication, Control and Computing 1997.*

2 BENEDETTO, S. , and MONTORSI, G. : 'Unveiling turbo codes: Some results on parallel concatenated coding schemes', *IEEE Trans. Inf. Theory*, 1996, 42, (2), pp. 409-428

3 HEEGARD, C. , and WICKER, S. B. , *Turbo Coding*. Kluwer Academic Publishers: Boston/Dordrecht/London, 1999.

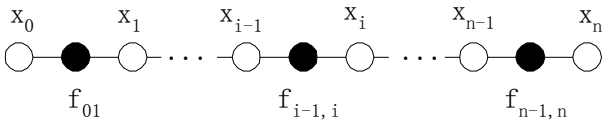

Fig1. A factor graph for the code C[n, k]