The "Art of Trellis Decoding" is Computationally Hard – for Large Fields[1]

Kamal Jain Ion Măndoiu Vijay V. Vazirani
College of Computing, Georgia Institute of Technology, Atlanta, GA 30332
{kjain,mandoiu,vazirani}@cc.gatech.edu

Abstract — **The problem of minimizing the trellis complexity of a code by coordinate permutation is proven NP-hard for three different measures of trellis complexity, provided the field over which the code is specified is not fixed.**

I. Introduction

Every linear code admits a unique minimal trellis for a fixed coordinate permutation (see e.g. [2, 4]) which simultaneously minimizes (1) the number of states, (2) the number of edges, and (3) the maximum state complexity. Even though permuting the coordinates of the code changes none of its traditional properties, it can drastically change the size of the minimal trellis under all these measures. Indeed, the problem of minimizing the trellis complexity of a code by coordinate permutations has been called the "art of trellis decoding" by Massey [4]. This problem has attracted much interest recently; as stated by Vardy in a recent survey [5], "... seven papers in [1] are devoted to this problem. Nevertheless, the problem remains essentially unsolved." In this context, an important unresolved problem is determining the computational complexity of finding the optimal permutation. We prove NP-hardness for all three measures, provided the field over which the code is specified is not fixed; however, we are able to fix the characteristic of the field. We leave open the problem of dealing with the case of a fixed field. The related problem of finding a permutation that minimizes state complexity at a given time index was known to be NP-hard [3].

II. NP-hardness of minimizing the maximum state complexity

Minimizing the maximum state complexity by coordinate permutation is equivalent to minimizing width of the parity-check matrix (the *width* of matrix H is defined as $\max_i w_i$, where w_i is the dimension of intersection of the space spanned by the first i columns with the space spanned by the last $n-i$ columns of H).

Theorem II.1 *For any prime p, the following is NP-hard:*
Problem: *Finite Field Minimum Width (FFMW)*
Instance: *A $k \times 2k$ matrix H over $GF(p^{3(k-1)})$.*
Question: *Is there a matrix H' obtained by permuting columns of H such that the width of H' is less than k?*

This will follow from:

Theorem II.2 *For every prime p, the following is NP-hard:*
Problem: *Restricted MDS Code (RMDSC)*
Instance: *A $k \times 2k$ matrix H over $GF(p^{3(k-1)})$.*
Question: *Does H have a set of k dependent columns?*

[1] Work supported by NSF Grant CCR 9627308. The full version of this paper has appeared in *IEEE Trans. Inform. Theory*, vol. 44, pp. 1211-1214, 1998.

Proof sketch. First, we show that 3-Dimensional Matching (given three disjoint sets W, X, Y, each of cardinality r, and $M \subseteq W \times X \times Y$, decide whether M contains a matching, i.e. a subset $M' \subseteq M$ such that $|M'| = r$ and no two elements of M' agree on any coordinate) remains NP-hard even when restricted to instances in which $|M| = 2r+1$. Next, we prove that given $\alpha_1, \alpha_2, \ldots, \alpha_{2r+1}, \beta \in GF(p^{3r})$, it is NP-hard to decide whether β can be written as the sum of r of the α_i's. Finally, we reduce this problem to RMDSC using Vardy's construction [5]. We obtain an instance of RMDSC by taking $k = r+1$, and

$$H = \begin{bmatrix} 1 & 1 & \ldots & 1 & 0 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_{2r+1} & 0 \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_{2r+1}^2 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{r-2} & \alpha_2^{r-2} & \ldots & \alpha_{2r+1}^{r-2} & 0 \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \ldots & \alpha_{2r+1}^{r-1} & 1 \\ \alpha_1^{r} & \alpha_2^{r} & \ldots & \alpha_{2r+1}^{r} & \beta \end{bmatrix}.$$

It is easy to see that any set of r columns of H is independent: after removing the last row of H, any r columns will form a Vandermonde determinant. Since H has $r+1$ rows, any set of $r+2$ columns of H is dependent. It follows that the minimum number of dependent columns of H is either $r+1$ or $r+2$. The following lemma by Vardy distinguishes between these two cases. □

Lemma II.3 *(Vardy [5]) H has $r+1$ dependent columns iff $\alpha_{i_1} + \alpha_{i_2} + \ldots + \alpha_{i_r} = \beta$ for some $i_1, \ldots, i_r$.*

Proof of Theorem II.1. Let H be an instance of RMDSC. If every set of k columns of H is independent, the width of any matrix obtained by column permutations from H is k. On the other hand, if there exists a set of k dependent columns, then by listing these columns first and the remaining columns next, we obtain a permutation of width less than k. □

References

[1] J. FEIGENBAUM, G.D. FORNEY, B. MARCUS, R.J. MCELIECE, and A. VARDY, Special issue on "Codes and Complexity," *IEEE Trans. Inform. Theory*, vol. 42, November 1996.

[2] G. D. FORNEY and M. TROTT, The dynamics of group codes: state spaces, trellis diagrams, and canonical encoders, *IEEE Trans. on Inform. Theory*, vol. 39, pp. 1491-1513, 1993.

[3] G.B. HORN and F.R. KSCHISCHANG, On the Intractability of permuting a block code to minimize trellis complexity, *IEEE Trans. Inform. Theory*, vol. 42, pp. 2042-2048, 1996.

[4] J.L. MASSEY, Foundation and methods of channel encoding, *Proc. Int. Conf. on Information Theory and Systems*, vol. 65, NTG-Fachberichte, Berlin, 1978.

[5] A. VARDY, Algorithmic complexity in coding theory and the minimum distance problem, *Proc. 29th ACM Symposium on Theory of Computing*, pp. 92-109, 1997.