The "Art of Trellis Decoding" is Computationally Hard – for Large Fields *

Kamal Jain
Ion Măndoiu
Vijay V. Vazirani

College of Computing
Georgia Institute of Technology

Abstract

The problem of minimizing the trellis complexity of a code by coordinate permutation is studied. Three measures of trellis complexity are considered: the total number of states, the total number of edges, and the maximum state complexity of the trellis. The problem is proven NP-hard for all three measures, provided the field over which the code is specified is not fixed. We leave open the problem of dealing with the case of a fixed field, in particular $GF(2)$.

Index Terms– NP-hardness, trellis complexity, MDS codes, Vandermonde matrices.

1 Introduction

The most used and studied way of performing soft-decision decoding is via trellises. Clearly, in order to speed up decoding, it is important to minimize the *size* of the trellis for a given code. Several measures of trellis complexity have been proposed by researchers: the total number of states, the total number of edges, and the maximum state complexity of the trellis. It has been established that every linear code (in fact, every group code) admits a unique minimal trellis that simultaneously minimizes all these measures [2, 3, 7, 9], and much work has been done on obtaining efficient algorithms for constructing minimal trellises for linear codes as well as more general codes [6, 13].

It is easy to see that the seemingly trivial operation of permuting the coordinates of a code, which changes none of the traditional properties of the code, 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 [7]. This problem has attracted much interest recently; as stated by Vardy in a recent survey [11], "... 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

*Supported by NSF Grant CCR 9627308.

finding the optimal permutation. Horn and Kschischang [5] prove the NP-hardness of finding the permutation that minimizes the state complexity of the minimal trellis at a given time index, and conjecture that minimizing the maximum state complexity is NP-hard. In this paper, 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, in particular $GF(2)$.

Our proof uses several ideas from the recent breakthrough result of Vardy [12] showing the NP-hardness of the problem of computing the minimum distance of a binary linear code thus settling a conjecture of Berlekamp, McEliece and van Tilborg dating back to 1978. In particular, we use his ingenious construction for obtaining MDS codes using Vandermonde matrices. Vardy also proves the NP-hardness of determining whether a given linear code is MDS. We first show that this problem is NP-hard even if the parity check matrix is restricted to have dimensions $k \times 2k$. NP-hardness for all three measures follows easily from this problem.

2 Preliminaries

A *trellis* T, for an (n, k)-linear code $\mathcal{C}$ over $GF(q)$ is an edge-labeled directed layered graph. The vertices of T are partitioned into disjoint subsets $V_0, V_1, \ldots V_n$. The set V_i is referred to as the set of *states* at time index i. V_0 contains a unique start state v_0, and V_n contains a unique terminating state v_n. Edges of T are allowed to run only between states in successive time indices; the set of edges running from V_{i-1} to V_i is denoted by $E_{i-1,i}$. We require that each state must be useful, i.e. it must be on some path from v_0 to v_n. Notice that each path from v_0 to v_n has n edges. Edges of T are labeled with elements of $GF(q)$ in such a way that the set of n-tuples associated with the paths from v_0 to v_n is exactly $\mathcal{C}$.

A *proper (co-proper)* trellis is a trellis in which there is no state with two outgoing (incoming) edges having the same label. A trellis is called *biproper* if it is both proper and co-proper. If T is a biproper trellis, then V_i and $E_{i-1,i}$ can be seen as vector spaces over $GF(q)$ [2, 3]. Let $s_i = \dim(V_i)$ and $e_i = \dim(E_{i-1,i})$; then $(s_0, \ldots, s_n)$ and $(e_1, \ldots, e_n)$ are known as the *state* and *edge complexity profiles* of T, respectively.

A remarkable property of any biproper trellis is that it minimizes state and edge profiles, i.e., for each i, s_i and e_i are minimum [2, 9]. In particular, a biproper trellis minimizes the following quantities:

1. *maximum state complexity*, $s_{\max} = \max_i s_i$;
2. *total vertex complexity*, $|V| = \sum_{i=0}^{n} q^{s_i}$;
3. *total edge complexity*, $|E| = \sum_{i=1}^{n} q^{e_i}$.

It is easy to see that by permuting the coordinates of $\mathcal{C}$ the minimal trellis might change drastically with respect to above mentioned measures. So far, there is no general agreement on what is the best measure of trellis complexity (see [8] for a recent position in this matter). As we shall see, the intractability result of this paper holds for *any* choice of measure from the above list.

3 NP-hardness of Restricted MDS Code

Recently, Vardy [12] proved that it is NP-hard to find whether or not a given linear code is MDS. We show that the problem remains NP-hard even when restricted to $(2k, k)$-linear codes; this restricted version of the MDS Code problem will be used to derive the results of the next section.

Problem: Restricted MDS Code (RMDSC)

Let p be a fixed prime.

Instance: A $k \times 2k$ matrix H over $GF(p^{3(k-1)})$.

Question: Does H have a set of at most k dependent columns?

We will establish the NP-hardness of RMDSC in three steps. First, we prove that a restricted version of 3-Dimensional Matching is NP-hard. Then, we reduce it to a version of Finite Field Subset Sum (FFSS). Finally, this version of FFSS is reduced to RMDSC.

The restricted version of 3-Dimensional Matching (3DM) we will use is the following:

Problem: Restricted 3-Dimensional Matching (R3DM)

Instance: Three disjoint sets, W, X, Y, each of cardinality r, and a set $M \subseteq W \times X \times Y$ of cardinality $2r + 1$.

Question: Does M contain a matching, i.e. a subset $M' \subseteq M$ such that $|M'| = r$ and no two elements of M' agree on any coordinate?

Lemma 3.1 *Restricted 3-Dimensional Matching is NP-hard.*

Proof. We will reduce 3-Dimensional Matching [4] to R3DM – basically by adding elements to W, X, Y and M so that $|M| = 2|W| + 1$.

Let (M, W, X, Y) be an instance of 3DM, where W, X, Y are disjoint sets with r elements and $M \subseteq W \times X \times Y$. If $|M| = 2r + 1$ then (M, W, X, Y) is a valid instance of R3DM. If $|M| > 2r + 1$, add $k = |M| - (2r + 1)$ new elements to each of the sets W, X and Y, and add to M any k triples matching these new elements. Finally, if $|M| < 2r + 1$ we obtain an instance of R3DM by repeating $(2r + 1) - |M|$ times the following augmentation: add two new elements to each of the sets W, X and Y, while adding to M five of the eight triples that can be formed with the new elements.

Thus (M, W, X, Y) is converted in polynomial time to an instance of R3DM, and it is not difficult to check that the new instance has a matching if and only if (M, W, X, Y) has one □

Next we reduce this R3DM to the following version of Finite Field Subset Sum:

Problem: Restricted Finite Field Subset Sum (RFFSS)

Let p be a fixed prime.

Instance: A set of $2r + 1$ distinct elements $\alpha_1, \alpha_2, \ldots, \alpha_{2r+1} \in GF(p^{3r})$, an element $\beta \in GF(p^{3r})$.

Question: Is there a subset $\{\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_r}\}$ of $\{\alpha_1, \alpha_2, \ldots, \alpha_{2r+1}\}$ such that $\alpha_{i_1} + \alpha_{i_2} + \ldots \alpha_{i_r} = \beta$?

Lemma 3.2 *Restricted Finite Field Subset Sum is NP-hard.*

Proof. Let (M, W, X, Y) be an instance of R3DM with $|W| = |X| = |Y| = r$ and $|M| = 2r + 1$. The elements of $W \cup X \cup Y$ are numbered from 1 to $3r$ in some fixed order. Then a triple $(a, b, c) \in M$ is represented as the binary $3r$-tuple which has 1 at i, j and k^{th} position only, where a, b and c are i, j and k^{th} elements of $W \cup X \cup Y$ resp. Let $\alpha_1, \alpha_2, \ldots, \alpha_{2r+1} \in GF(2)^{3r}$ represent the $2r + 1$ elements of M.

Now consider the $3r$-tuple β consisting of all 1's. It is clear that there will exist a subset $\{\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_r}\}$ of $\{\alpha_1, \alpha_2, \ldots, \alpha_{2r+1}\}$ such that $\alpha_{i_1} + \alpha_{i_2} + \ldots \alpha_{i_r} = \beta$ if and only if M has a matching. By [10], these binary $3r$-tuples can be considered as elements of $GF(p^{3r})$. Hence RFFSS is NP hard □

We can now prove the NP-hardness of RMDSC:

Theorem 3.3 *For every prime p, Restricted MDS Code is NP-hard.*

Proof. We will reduce RFFSS to RMDSC using Vardy's construction [12]. Let $\alpha_1, \alpha_2, \ldots, \alpha_{2r+1}$, $\beta \in GF(p^{3r})$ be an instance of RFFSS. 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 3.4 *(Vardy [12]) H has $r + 1$ dependent columns iff $\alpha_{i_1} + \alpha_{i_2} + \ldots + \alpha_{i_r} = \beta$ for some $i_1, ..., i_r$.*

By Lemma 3.4, the answer to the instance of RFFSS is "no" iff every set of $r + 1$ columns of H is independent. Hence RMDSC is NP-hard □

4 NP-hardness of minimizing trellis complexity

Let H be an $m \times n$ matrix over $GF(q)$. Define w_i to be the dimension of the intersection of the space spanned by the first i columns with the space spanned by the last $n - i$ columns of H. The *width of* H is defined to be $\max_i\{w_i\}$.

Lemma 4.1 *(Horn and Kschischang [5]) If H is the parity-check (or generator) matrix of $\mathcal{C}$, then, for each i, the minimal trellis has $s_i = w_i$.*

Thus $s_{\max}$ is the width of the parity-check (or generator) matrix of the code, and the problem of finding a coordinate permutation minimizing the maximum state complexity can be rephrased as the the problem of finding a permutation that minimizes the width of the parity-check (or generator) matrix.

Problem: Finite Field Minimum Width (FFMW)

Let p be a fixed prime.

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?

We prove NP-hardness of FFMW by a reduction from RMDSC.

Theorem 4.2 *For any prime p, Finite Field Minimum Width is NP-hard.*

Proof. Let H be a $k \times 2k$ 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. Indeed, the first k columns and the last k columns of such a matrix generate the entire k-dimensional space. 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. Hence, H has k dependent columns if and only there exists a permutation of its columns for which the width is less than k. This proves that FFMW is NP-hard $\Box$

Corollary 4.3 *Finding a coordinate permutation that minimizes $s_{\max}$ is NP-hard.*

We will also reduce RMDSC to the problem of minimizing $|V|$ by coordinate permutations. Let H be an instance of the RMDSC problem, say H is a $k \times 2k$ matrix, and let $\mathcal{C}$ be the linear code generated by H. If no k columns of H are dependent, it is easy to see that $w_i = \min\{i, 2k - i\}$ for any permutation of the columns of H. So, the minimal trellis for any coordinate permutation of $\mathcal{C}$ has $(0, 1, 2, ..., k-1, k, k-1, ..., 2, 1, 0)$ as the state complexity profile. Hence, $|V|$ is a constant, K, over all coordinate permutations of $\mathcal{C}$. On the other hand, if there exist k dependent columns in H, by moving these columns in the first k positions we obtain a permutation such that $w_k < k$. Since $w_i \leq \min\{i, 2k - i\}$ for every i, it follows that the minimal trellis associated with this permutation has strictly less than K states. Hence we obtain:

Theorem 4.4 *Finding a coordinate permutation that minimizes $|V|$ is NP-hard.*

Similarly, we have:

Theorem 4.5 *Finding a coordinate permutation that minimizes $|E|$ is NP-hard.*

Proof. From the characterization of edge spaces given in [2, 3] it follows that the minimal trellis of the code generated by a $k \times 2k$ matrix H has e_i equal to the dimension of the intersection of the space spanned by the first i columns with the space spanned by the last $2k - i + 1$ columns of H (this differs from the definition of w_i in that the i^{th} column is included in both terms of the intersection).

We obtain a reduction of RMDSC to the problem of minimizing $|E|$ by coordinate permutations by observing that: (i) if no k columns of H are dependent, then, for any column permutation, the minimal trellis has $e_i = \min\{i, 2k - i + 1\}$ for every i, and (ii) if there exist k dependent columns, placing these columns in the first k positions gives a permutation with $e_k < k$ and $e_i \leq \min\{i, 2k - i + 1\}$ for every $i \neq k$ □

Remark. For purposes of decoding, it is better to consider a more compact form of trellises in which parallel edges are represented by a single edge labeled with a set of symbols (see [13] for instance). Note that in the proof of Theorem 4.5, if no k columns of H are dependent then the resulting minimal trellis has no parallel edges. Hence minimizing the number of edges for the compact form of trellises also remains NP-hard.

It is natural to ask whether or not minimizing trellis complexity becomes tractable for a fixed field. We concur with Horn and Kschischang [5] and Vardy [11, 12] in the belief that the answer is "no". In particular, we believe that the following problem is NP-hard:

Problem: Minimum Width

Let $GF(q)$ be a fixed field.

Instance: An integer $w > 0$ and an $m \times n$ matrix H over $GF(q)$.

Question: Is there a matrix H' obtained by permuting columns of H such that the width of H' is less than w?

We believe that this will be a challenging problem.

5 Acknowledgment

We wish to thank Alexander Vardy for several valuable comments, including pointing out that our proof gives NP-hardness for Restricted MDS Code.

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, Coset codes - part II: binary lattices and related codes, *IEEE Trans. Inform. Theory*, vol. 34, pp. 1152-1187, 1988.

[3] 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.

[4] M.R. GAREY and D.S. JOHNSON, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, Freeman, San Francisco, 1979.

[5] 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.

[6] F. R. KSCHISCHANG and V. SOROKINE, On the trellis structure of block codes, *IEEE Trans. Inform. Theory*, vol. 41, pp. 1924-1937, 1995.

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

[8] R.J. MCELIECE, On the BCJR trellis for linear block codes, *IEEE Trans. Inform. Theory*, vol. 42, pp. 11072-1092, 1996.

[9] D.J. MUDER, Minimal trellises for block codes, *IEEE Trans. Inform. Theory*, vol. 34, pp. 1049-1053, 1988.

[10] V. SHOUP, New algorithms for finding irreducible polynomials over finite fields, *Math. Computation*, vol.54, pp.435-447, 1990.

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

[12] A. VARDY, The intractability of computing the minimum distance of a code, *IEEE Trans. Inform. Theory,* vol.43, pp. 1757-1766, 1997.

[13] V.V. VAZIRANI, H. SARAN, and B. S. RAJAN, An efficient algorithm for constructing minimal trellises for codes over finite abelian groups, *IEEE Trans. Inform. Theory*, vol. 42, pp. 1839-1854, 1996.