A simple one sweep algorithm for optimal APP symbol decoding of linear block codes

Johansson, Thomas; Zigangirov, Kamil

Published in:
IEEE Transactions on Information Theory

DOI:
10.1109/18.737541

Published: 1998-01-01

Citation for published version (APA):
A Simple One-Sweep Algorithm for Optimal APP Symbol Decoding of Linear Block Codes

Thomas Johansson, Member, IEEE, and Kamil Zigangirov, Member, IEEE

Abstract—Soft-input/soft-output symbol decoding plays a significant role in iterative decoding. We propose a simple optimal soft-input/soft-output symbol decoding algorithm for linear block codes which requires one forward recursion using a trellis. For many codes the decoding complexity is lower than previous methods, such as the algorithm by Bahl et al. [1], and the decrease is shown at its most when decoding Hamming codes.

Index Terms—Linear block codes, soft-output symbol decoding, trellises.

I. INTRODUCTION

Recently, much interest has focused around iterative decoding (or turbo decoding) due to the impressive simulation results presented in [4]. The basic idea is to decode in steps, by transferring conditional probabilities, or “soft” information, between consecutive steps. In particular, [4] used a two-dimensional systematic feedback convolutional code including a large pseudorandom interleaver, and decoded iteratively. For an overview of iterative decoding, see [2].

A crucial part of the iterative decoding is the decoding algorithm, taking soft inputs and delivering soft outputs for each symbol. Such algorithms have been considered and dates back to [1]. These algorithms are referred to as soft-input/soft-output symbol decoding algorithms, or APP (a posteriori probability) symbol decoding algorithms.

For optimal APP symbol decoding, the Bahl, Cocke, Jelinek, Raviv algorithm applies to trellises, and hence to both convolutional codes and linear block codes [10]. The algorithm makes one forward and one backward recursion in the trellis, and requires storage of approximately $2KS$ real numbers, where $K$ is the number of information bits and $S$ is the number of states on one level in the trellis. For a binary $[N, K]$ linear block code, the trellis can contain $\min\{2^K, 2^{N-K}\}$ states, and for many good linear block codes this will be the case. If $K > N - K$ this algorithm requires storage of approximately $K\cdot 2^{N-K}$ real numbers, and does one forward and one backward recursion. Other optimal symbol-by-symbol APP decoding algorithms have been proposed. In [2], several methods are proposed, either by a straightforward implementation of the trellis, based on [7], or using the dual code as proposed in [6] and [7]. Summing up the results, both methods calculate the soft output by one forward recursion on a trellis of at most $2^K$ states each with a metric as a real number. Hence in many cases, it has a complexity that is lower than the optimal decoding methods mentioned above. Its low complexity is shown at its most when decoding Hamming codes, since then almost all information calculated in the algorithm will be efficiently used. This will be demonstrated by an example. Finally, we consider a generalization to the nonbinary case.

II. NOTATION AND PROBLEM FORMULATION

We model our communication system as follows. A source with alphabet $\mathcal{I} = \{0, 1, \ldots, I - 1\}$, where the symbols are chosen independently of each other with equal probability, feeds an encoder which in our case is a linear block encoder. The source symbols are divided into blocks of $K$ symbols, denoted $u = (u_1, u_2, \ldots, u_K)$, and the corresponding encoded symbols, denoted $v_n$, $1 \leq n \leq N$, are then transmitted over any memoryless noisy channel. We assume that the symbols are modulated into analog waveforms that are sent over the channel. Let $w = (v_1, v_2, \ldots, v_N)$ be the transmitted codeword, $v_n \in \mathcal{I}$.

On the receiver side, the output from the memoryless noisy channel is the analog waveforms interfered with noise, and we assume quantization of the channel output into a finite set of possible values from the output alphabet $\mathcal{J} = \{0, 1, \ldots, J - 1\}$. For example, if we have additive white Gaussian noise, this can be thought of as the output of a bank of matched filters. We suppose that the channel is defined by the set of transition probabilities

$$p_{ij} = P(j|i), \quad i = 1, 2, \ldots, I - 1, \quad j = 1, 2, \ldots, J - 1.$$  

The received vector, denoted $\mathbf{r} = (r_1, r_2, \ldots, r_N)$ with $r_n \in \mathcal{J}$ is hence regarded as a vector of discrete random variables. The generalization to the continuous case is omitted, but it is a straightforward procedure. Due to the memoryless channel,

$$P(w|\mathbf{v}) = \prod_{i=1}^{N} P(r_i|v_i).$$  

The vector $\mathbf{r}$ is the input to the decoder of the systematic linear block code, which is going to produce an estimate of the information symbols, using the extra information through the parity-check symbols. In our case, this estimate should be a a posteriori probability vector $\mathbf{d}_n = (d_n^{(0)}, d_n^{(1)}, \ldots, d_n^{(I-1)})$ on each information symbol $u_n$ expressing the probability that the $n$th source symbol was actually symbol $i$, $i = 0, 1, \ldots, I - 1$, conditioned on all the received channel information and the dependence within the codeword. Actually, the algorithm to be derived will produce the a posteriori probability for any codeword symbol, but at this moment we are only interested in the codeword symbols that are information symbols.

Continuing, we now consider the case $I = 2$ with $\mathcal{I} = \{0, 1\}$. The generalization to the nonbinary case is considered in the last section. Let $w = (v_1, v_2, \ldots, v_N) \in \mathbb{F}_2^N$ be a codeword of an $[N, K]$ linear binary block code $V$. Assume that the linear code $V$ has a generator matrix $G$ and that the corresponding parity-check matrix

rate at $0.67$ at bit-error rate (BER) of $10^{-4}$. Furthermore, good simulation results have been shown for very simple block codes, such as Hamming codes, as component codes, see [2].

The purpose of this correspondence is to derive an optimal soft-input/soft-output symbol-decoding algorithm for linear block codes. It will require only one forward recursion on a trellis of at most $2^{N-K}$ states each with a metric as a real number. Hence in many cases, it has a complexity that is lower than the optimal decoding methods mentioned above. Its low complexity is shown at its most when decoding Hamming codes, since then almost all information calculated in the algorithm will be efficiently used. This will be demonstrated by an example. Finally, we consider a generalization to the nonbinary case.

Manuscript received August 3, 1997; revised February 10, 1998.

The authors are with the Department of Information Technology, Lund University, S-221 00 Lund, Sweden.

Publisher Item Identifier S 0018-9448(98)06753-4.
Finally, for the received vector and distributed, which will be the case in iterative decoding. We will a priori case, namely, when all codewords are in each position of the codeword when the receiver has the soft-systematic this gives us.

From this notation we define the partial syndrome.

We start by introducing the notation

\[ s_n = v_{[1:n]} H_{[1:n]}^T \]  

and we call \( s_n \) the partial syndrome. Note that the partial syndrome is defined for any word \( v_{[1:n]} \), not necessarily a codeword. Continuing, we introduce the cosets of the code \( V \), denoted \( V_s \), as

\[ V_s = \{ v : H_{[1:n]}^T = s \}, \quad \forall s \in \mathbb{F}_2^{N-K}. \]

Finally, for the received vector \( r = (r_1, r_2, \ldots, r_N) \), we introduce \( r_n^- \) by

\[ r_n^- = (r_1, \ldots, r_{n-1}, r_{n+1}, \ldots, r_N) \]

i.e., \( r_n^- \) is the received vector \( r \) with the \( n \)th position removed.

We start the algorithm derivation. We consider the most simple case, namely, when all codewords are a priori equiprobable, i.e.,

\[ P(v|v \in V) = 2^{-K}, \quad \forall v \in V \]

and hence also

\[ P(v_n = 0|v \in V) = 2^{-K+1}, \quad \forall v \in V, v_n = 0. \]

Note that the algorithm to be derived is easily adopted to the case when the \( K \) independent information symbols are nonuniformly distributed, which will be the case in iterative decoding. We will in such a case use a slightly different metric in the trellis defined below. Using Bayes formula we get

\[ P(v_n = 0|r, v \in V) = P(r|v = 0) P(v | v \in V) \]

where \( P(v_n = 0|v \in V) = 1/2, \)

\[ P(r|v = 0) = \sum_{v \in V} P(r|v) P(v | v \in V) \]

is the probability of receiving \( r \), and finally,

\[ P(r|v_n = 0, v \in V) = \sum_{v \in V} P(r|v) P(v | v_n = 0, v \in V). \]

The calculation of \( P(r_n = 0|v, v \in V) \) reduces through (8) to calculation of two statistics, \( P(r|v \in V) \) and \( P(r|v_n = 0, v \in V) \), respectively.

For the given parity-check matrix \( H \), consider the following length \( N \) trellis diagram. The paths of this trellis diagram correspond to the sequences \( v_{[1:n]} \), \( n = 1, 2, \ldots, N \). Paths of length \( n \) will come to the same node (state) \( s \) on level \( n \) if they have the same partial syndrome as defined in (5). Since all partial syndromes are \( (N-K) \)-dimensional binary vectors, the total number of states at each level is upper-bounded by \( 2^{N-K} \). This trellis, introduced in [1], is known as the syndrome trellis. Furthermore, it is a minimal trellis.

By definition, the metric of node \( s \) on level \( n \) is

\[ \mu(s, n) = \sum_{v_{[1:n]} | v_{[1:n]} H_{[1:n]}^T = s} P(r_{[1:n]}|v_{[1:n]}). \]

Since \( s_n = s_{n-1} + v_n h_n \)

we see that, in general, to state \( s \) on level \( n \) there come two edges, one from state \( s \) at level \( n-1 \) associated with \( v_n = 0 \) and one from state \( s - h_n \) at level \( n-1 \) associated with \( v_n = 1 \). Calculation of the metrics for each node at each level is then done recursively by

\[ \mu(0, 0) = 1, \mu(s, 0) = 0, \forall s \neq 0, \text{ and then} \]

\[ \mu(s, n) = \mu(s, n-1) P(r_n|v_n = 0) + \mu(s - h_n, n-1) P(r_n|v_n = 1). \]

Since the trellis contains all states at the last level, the algorithm above will require slightly more computations than in a standard trellis [1], [8], which considers only paths merging to state zero at the last level.

It is easily verified that (11) holds for all nodes using the above calculation. From (11) it follows that

\[ \mu(0, N) = \sum_{v \in V} P(r|v) = \sum_{v \in V} P(r|v) \]

and, in general,

\[ \mu(s, N) = \sum_{v \in V} P(r|v) = \sum_{v \in V} P(r|v). \]

Consider the codeword symbol \( v_n \). Note that \( h_n \) is the partial syndrome caused by \( v_{[1:n]} = (0, 0, 0, \ldots, 0, 1) \), i.e.,

\[ h_n = (0, 0, 0, \ldots, 0, 1) H_{[1:n]}^T. \]

Introduce

\[ P(r_n^+|v_n = 0, v \in V) = \sum_{v_{[1:n]} \neq v_n} P(r_n^+|v) \]

\[ P(r_n^-|v_n = 1, v \in V) = \sum_{v_{[1:n]} \neq v_n} P(r_n^-|v). \]
The key observation is now that the following two equations in the two unknowns variables

\[ P(r_n^+|v_n = 0, \nu \in V) \]

and

\[ P(r_n^+|v_n = 1, \nu \in V) \]

respectively, hold

\[
\sum_{\nu \in V} P(\nu|\nu) = P(r_n|v_n = 0)P(r_n^+|v_n = 0, \nu \in V)
+ P(r_n|v_n = 1)P(r_n^+|v_n = 1, \nu \in V)
\]

(19)

\[
\sum_{\nu \in V} P(\nu|\nu) = P(r_n|v_n = 1)P(r_n^+|v_n = 0, \nu \in V)
+ P(r_n|v_n = 0)P(r_n^+|v_n = 1, \nu \in V).
\]

(20)

Recall that the left-hand-sides of the above two equations are given by the metrics \( \mu(0, N) \) and \( \mu(h, N) \), respectively. Hence we can solve for one of the unknown variables and get

\[
P(r_n^+|v_n = 0, \nu \in V) = \frac{P(r_n|v_n = 0)\mu(0, N) - P(r_n|v_n = 1)\mu(h, N)}{P(r_n|v_n = 0)^2 - P(r_n|v_n = 1)^2}
\]

(21)

if

\[ P(r_n|v_n = 0) \neq P(r_n|v_n = 1). \]

Furthermore, note that \( P(\nu|\nu \in V) = 2^{-K} \) and \( P(\nu|v_n = 0, \nu \in V) = 2^{-K+1} \). Therefore, (8)-(10) imply

\[
P(v_n = 0|\nu, \nu \in V) = \frac{\sum_{\nu_0 = 0, \nu \in V} P(\nu|\nu)2^{-K+1} \frac{1}{2}}{\sum_{\nu \in V} P(\nu|\nu)2^{-K}}
\]

(22)

and since

\[
\sum_{\nu_0 = 0, \nu \in V} P(\nu|\nu) = \sum_{\nu_0 = 0, \nu \in V} P(\nu_0^+|v_n = 0, \nu \in V) \cdot P(r_n|v_n = 0)
\]

(23)
and backward recursion. Following the ideas of Battail et al. [7] the soft output of all the information bits is calculated with $K$ forward recursions in a trellis that needs to be slightly modified for each recursion. In [6] and [2] the calculation is done using the dual code, which is an alternative requiring $K$ forward recursions in a trellis of size at most $2^{N-K}$.

The proposed algorithm requires only $2^{N-K}$ stored values, i.e., storage of one level in the trellis, and uses only one forward recursion. Hence, for some codes, the storage space is approximately a factor $N$ lower than that of the algorithm of Bahi et al. and the number of operations is approximately a factor 2 lower. Comparing with the other algorithms mentioned above, the storage space is about the same but the number of operations is approximately a factor $K$ lower for the proposed algorithm.

IV. AN EXAMPLE OF DECODING OF HAMMING CODES

To fully illustrate the decoding algorithm and to show that the reduced complexity is at its most when decoding Hamming codes, we give an example. Assume that we want to decode a [7, 4, 3] Hamming code given by the parity-check matrix (in transposed form)

$$
H^T = \begin{pmatrix}
0 & 1 & 1 \\
1 & 0 & 1 \\
1 & 1 & 0 \\
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{pmatrix}
$$

We assume that the first four symbols of $v$ are information symbols, i.e., the encoder is systematic. Consider a 4-ary output DMC with transition probabilities $P(r_n|v_n)$ given by the following table:

<table>
<thead>
<tr>
<th>$v_n$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.5</td>
<td>0.3</td>
<td>0.15</td>
<td>0.05</td>
</tr>
<tr>
<td>1</td>
<td>0.05</td>
<td>0.15</td>
<td>0.3</td>
<td>0.5</td>
</tr>
</tbody>
</table>

Assume that the received vector is

$$
r = (1, 0, 1, 0, 2, 0, 0).
$$

We note that the closest codeword is (0000000). Fig. 2 illustrates Steps 1 and 2 in the decoding algorithm by giving values for $\mu(s, n), n = 0, \cdots, N$ having eight entries of real numbers at each level.

Using Step 3 we finally get the soft-output values by

$$
P(u_1 = 0|v, v \in V) = \frac{P(r_1|v_1 = 0) \mu(001, 7)}{P(r_1|v_1 = 1) \mu(000, 7)} \frac{P(r_1|v_1 = 1)}{P(r_1|v_1 = 0)}.
$$

$$
= \frac{0.3 \times 0.00112}{0.3} = 0.85502
$$

etc., and performing all calculations in Step 3 gives the soft output vector

$$(0.85502, 0.94965, 0.85502, 0.90909, 0.78067, 0.90909, 0.93763).$$

V. GENERALIZATION TO THE NONBINARY CASE

The derivation from Section III generalizes straightforwardly to the nonbinary case. In this section we present the result and comment shortly on this.

For alphabet $I$ of size $I > 2$ we recall the enumeration of the elements by $I = \{0, 1, \cdots, I-1\}$. Assume that $(I, +, \cdot)$ form a ring. An information sequence $u \in I^K$ is chosen uniformly and mapped into a codeword $r, v \in V$ such that $vH^T = 0$.

Using the notation introduced in Section II, the output should be a posteriori probability vector $h_n = \left( b_n^{(0)}, b_n^{(1)}, \cdots, b_n^{(I-1)} \right)$, where $b_n^{(i)} = P(u_n = i|v, r \in V)$ for each codeword symbol.

To state $s$, where $s \in I^{N-K}$, on level $n$ there are now $I$ incoming edges, one from state $s$ at level $n - 1$ associated with $v_n = 0$, one from state $s - h_n$ at level $n - 1$ associated with $v_n = 1$, and so on, and, finally, one from state $s-(I-1) \cdot h_n$ at level $n - 1$ associated with $v_n = I - 1$. Calculation of the metrics for each node at each level is as before done recursively by $\mu(0, 0) = 1, \mu(0, 0) = 0, \forall s \neq 0$, and then

$$
\mu(s, n) = \sum_{i=0}^{I-1} \mu(s - i \cdot h_n, n - 1) P(r_n|v_n = i).
$$

Recall that in general

$$
\mu(s, N) = \sum_{v \in V|s \in V} P(r|v) = \sum_{v \in V|s \in V} \sum_{r \in V} P(r|v).
$$

Now the following $I$ equations in the $I$ unknown variables

$$
P(r_n|v_n = i, v \in V) = \sum_{v_{n+1}=1}^{I-1} P(r_{n+1}|v)\text{ for } i = 0, 1, \cdots, I-1
$$

hold.

$$
\sum_{v \in V|s \in V} P(r|v) = \sum_{i=0}^{I-1} P(r_n|v_n = i) \sum_{v_{n+1}=1}^{I-1} P(r_{n+1}|v).
$$
An important aspect of the above algorithm for the nonbinary case is that it can be applied to binary nonlinear codes that are linear over binary code. For example, the Bahl et al. algorithm would only need storage space of approximately $2^{K-n-k}$ words of storage, whereas the proposed algorithm would only need $2^{K-n-k}$ words of storage space and still requires approximately a factor 2 less operations. This is due to the fact that it only does one forward recursion. For the nonbinary case and maximum-distance-separable codes, the algorithm will be better than the Bahl et al. algorithm, since the trellis for such codes is maximal [11]. Finally, we want to point out the possibility to modify the proposed algorithm so that it applies to the dual code, using the approach introduced by Hartmann and Rudolph [6] and later used by many authors, see for example [2]. This will provide an efficient solution for the case $k < n - k$, and applies to codes like the Simplex code and first-order Reed–Muller code, which are the dual codes of the Hamming code and the extended Hamming code, respectively. More details on this as well as computer simulations using the proposed algorithm can be found in [12].

$$M_n = \begin{bmatrix}
    P(r_n|v_n = 0) & P(r_n|v_n = 1) & \cdots & P(r_n|v_n = I - 1), \\
    P(r_n|v_n = -1) & P(r_n|v_n = 0) & \cdots & P(r_n|v_n = I - 2), \\
    \vdots & \vdots & \ddots & \vdots \\
    P(r_n|v_n = -I + 1) & P(r_n|v_n = -I + 2) & \cdots & P(r_n|v_n = 0).
\end{bmatrix}$$  

(28)
ACKNOWLEDGMENT

The authors wish to thank V. R. Sidorenko and A. Trushkin for helpful comments.

REFERENCES


A Soft Output Hybrid Algorithm for ML/MAP Sequence Estimation

Gary D. Brushe, Member, IEEE, Robert E. Mahony, Member, IEEE, and John B. Moore, Fellow, IEEE

Abstract—The classical Viterbi algorithm (ML sequence estimation) can be computed using a forward-backward structure, similar to that of the classical hidden Markov model forward-backward algorithm (MAP state estimation). This similarity is exploited to develop a hybrid algorithm which provides a mathematical connection between ML sequence estimation and MAP state estimation.

Index Terms—Forward-backward algorithms, hidden Markov models, HMM’s, sequence, soft outputs, state estimation, Viterbi algorithm.

I. INTRODUCTION

The basic filter theory for hidden Markov models was first presented by Baum and his colleagues in a series of papers in the late 1960’s and early 1970’s [1]–[5]. These papers developed statistical estimation algorithms for a discrete-time Markovian process observed in noise. The model structure became known as a hidden Markov model (HMM) and since the mid-1980’s has become increasingly popular in many engineering applications (e.g., signal and speech processing). In the field of communications, the typical application is one where the signal statistics are known a priori and the goal is to estimate the transmitted state sequence from observed data. There are two natural measures of the most probable state sequence transmitted. First, at each separate time, one may consider the states which are individually most likely. This is equivalent to estimating the maximum a posteriori probability (MAP) (sometimes known as minimum variance or conditional mean) state estimates. These estimates can be determined using the HMM forward-backward algorithm (FBBA) [7]. Conversely, one may consider the most likely state sequence over all the data. This is equivalent to computing the maximum-likelihood (ML) state sequence for the full data stream. This estimate can be determined using the Viterbi algorithm (VA) [7].

In 1974, Bahl et al. [8] explored the use of MAP estimation in decoding linear block and convolutional codes in order to minimize the symbol- (or bit-) error rate. They concluded that the increased computational complexity of MAP estimation was not warranted as the performance of the VA and the MAP estimators were effectively identical in the applications they considered. More recently,

Manuscript received September 11, 1995; revised January 13, 1998. The work of the authors at the Cooperative Research Centre for Robust and Adaptive Systems was supported by the Australian Commonwealth Government under the Cooperative Research Centre Program. The material in this correspondence was presented in part at the ISSPA’96, Gold Coast, Australia, August 25–30, 1996.

G. D. Brushe is with the Signal Analysis Discipline, Communications Division, ESRL of the Defence Science and Technology Organization, Salisbury, SA 5108, Australia, and the Cooperative Research Centre for Robust and Adaptive Systems, c/- The Australian National University, Canberra, ACT, Australia.

J. B. Moore is with the Department of Systems Engineering, RSISE, The Australian National University, Canberra, ACT, Australia, and the Cooperative Research Centre for Robust and Adaptive Systems, c/- The Australian National University, Canberra, ACT, Australia.

R. E. Mahony is with the Cooperative Research Centre for Robust and Adaptive Systems, c/- The Australian National University, Canberra, ACT, Australia.

Publisher Item Identifier S 0018-9448/98/06901-6.