

# Maximum-Likelihood Soft Decision Decoding of BCH codes

Alexander Vardy

IBM Research Division, Almaden Research Center  
650 Harry Road, San Jose, CA 95120

Yair Be'ery

Tel-Aviv University, Department of Electrical Engineering  
Ramat-Aviv 69978, Tel-Aviv, Israel

**Abstract.** The problem of efficient maximum-likelihood soft decision decoding of binary BCH codes is considered. It is known that those primitive BCH codes whose designed distance is one less than a power of two, contain subcodes of high dimension which consist of a direct sum of several identical codes. We show that the same kind of direct-sum structure exists in all the primitive BCH codes, as well as in the BCH codes of composite block length. We also introduce a related structure termed the "concurring-sum", and then establish its existence in the primitive binary BCH codes. Both structures are employed to upper bound the number of states in the proper minimal trellis of BCH codes, and develop efficient algorithms for maximum-likelihood soft decision decoding of these codes.

In [2] Forney has shown that the binary Reed-Muller codes contain direct-sum subcodes of high dimension. It is well known that certain BCH codes, namely the primitive binary BCH codes with designed distance one less than a power of two, are supercodes of punctured Reed-Muller codes. Hence these BCH codes evidently share the direct-sum structure of the RM codes. This fact was used by Kasami et al. [3] to construct efficient trellis diagrams for the (64,24,16) and (64,45,8) extended BCH codes, and also several double-error correcting BCH codes. The following question, hence, arises: do other BCH codes also contain direct-sum subcodes of high dimension? We settle this question affirmatively for all the primitive BCH codes, and also for the BCH codes of composite block length. The direct-sum structure is in a sense a counterpart of the concept of "zero-concurring" codewords of [1, 4], obtained by substituting a code for each codeword. We also study a different structure, where we allow the constituent codes to overlap over a fixed set of coordinates. This *concurring-sum* structure is the corresponding counterpart of the "concurring" codewords of [1]. We show the existence of concurring-sum structures in all the primitive binary BCH codes. Both the direct- and the concurring-sum structures make it possible to set nontrivial upper bounds on the number of states in the minimal proper trellis of BCH codes, and provide a clue for efficient soft-decision decoding.

Let  $C$  be a binary BCH code of length  $n$  and dimension  $k$ , let  $\alpha$  be a primitive  $n^{\text{th}}$  root of unity, and let  $\mathcal{I}$  be a subset of  $\{0, 1, \dots, n-1\}$ . Denote by  $C[\mathcal{I}]$  the subcode of  $C$  which consists of all those codewords that are nonzero only on the positions contained in  $\mathcal{I}$ . Let  $C(\mathcal{I})$  be the code obtained from  $C[\mathcal{I}]$  by puncturing out all the positions not in  $\mathcal{I}$ .

**Proposition 1.** Let  $\mathcal{I}_1$  and  $\mathcal{I}_2$  be subsets of the set  $\{0, 1, \dots, n-1\}$ , such that for some  $a \in \{0, 1, \dots, n-1\}$  we have  $\{\alpha^i : i \in \mathcal{I}_2\} = \{\alpha^a \cdot \alpha^i : i \in \mathcal{I}_1\}$ . Then  $C(\mathcal{I}_1) = C(\mathcal{I}_2)$ .

Now assume that the block length of  $C$  is composite, say  $n = n_1 n_2$ , and let  $Z$  be the set of zero frequencies of  $C$ . Define  $S = \{s \equiv z \pmod{n_1} : z \in Z\}$ .

**Proposition 2.** Let  $\mathcal{I}_1 = \{0, n_2, 2n_2, \dots, (n_1-1)n_2\}$ . Then the code  $C(\mathcal{I}_1)$  is a BCH code of length  $n_1$  and dimension  $k_1 = n_1 - |S|$ . The zeros of  $C(\mathcal{I}_1)$  lie at  $\{\beta^s : s \in S\}$ , where  $\beta = \alpha^{n_2}$  is a primitive  $n_1^{\text{th}}$  root of unity.

In order to obtain direct-sum subcodes of high dimension in BCH codes of composite block length, it would now suffice to partition the set  $\{0, 1, \dots, n-1\}$  into  $n_2$  disjoint subsets satisfying the condition of Proposition 1 with respect to the set  $\mathcal{I}_1$  defined in Proposition 2. Note that the sets  $Z$  and  $S$  are unions of cyclotomic cosets modulo  $n$  and  $n_1$ , respectively. Thus the definition of  $S$  in conjunction with Proposition 2 induces "coset aliasing" between the cyclotomic cosets modulo  $n$  and modulo  $n_1$ . In particular, certain high frequencies of  $C$  alias as low frequencies in  $C(\mathcal{I}_1)$ . This is intuitively plausible since  $\mathcal{I}_1$  is just the "time-domain sampling" of  $C$ .

In the sequel we consider the primitive BCH codes. Henceforth let  $C$  denote an extended primitive narrow-sense BCH code of length  $n+1 = 2^m$ .

**Proposition 3.** Let  $\mathcal{I}_1$  and  $\mathcal{I}_2$  be subsets of the set  $\{0, 1, \dots, n-1, \infty\}$ , such that for some  $a \in \{0, 1, \dots, n-1\}$  we have  $\{\alpha^i : i \in \mathcal{I}_2\} = \{\alpha^a + \alpha^i : i \in \mathcal{I}_1\}$ . Then  $C(\mathcal{I}_1) = C(\mathcal{I}_2)$ .

Proposition 3 may be thought of as the "addition counterpart" of Proposition 1. Thus we can exhibit the existence of direct-sum subcodes in the extended primitive BCH codes by partitioning the set  $\{\alpha^0, \alpha^1, \dots, \alpha^{n-1}, \alpha^\infty\}$  into disjoint subsets satisfying the condition of Proposition 3 with respect to some given subset. Yet this set is just the field  $GF(2^m)$ . Thus it would suffice to regard  $GF(2^m)$  as a vector space, and partition it into a subspace and its cosets. Notably, Proposition 3 may be also employed for the derivation of the concurring-sum structure in the primitive binary BCH codes. For more details on this see [5].

We now indicate how the direct-sum and the concurring-sum structures may be employed for efficient maximum-likelihood soft decision decoding. Let  $s$  be the logarithm of the maximum number of states in the minimal proper trellis of a linear code  $C$ . This parameter governs the complexity of maximum-likelihood decoding of  $C$  using the trellis diagrams of [2]. It follows from the trellis construction of Wolf [6], that  $s \leq \min\{K, N-K\}$ , where  $N$  and  $K$  are the block length and the dimension of  $C$ . We employ the direct-sum and the concurring-sum structures of  $C$  to substantially improve upon this upper bound. Assume that  $C$  contains a subcode which is a direct-sum of  $h$  identical codes, each of dimension  $k$ . Then by arranging the coordinates of  $C$  in alignment with its direct-sum structure, it follows that  $s \leq K-(h-1)k$ . Substituting the parameters of the direct-sum structures, that we were able to find using the techniques described herein, into this expression yields upper bounds on  $s$  which are often tighter than the bound of Wolf. Arranging the coordinates of  $C$  in alignment with its concurring-sum structure also yields low values of  $s$  in all the primitive binary BCH codes. Some of the bounds on  $s$ , resulting from the direct- and concurring-sum structures, are listed in the table below. The table also lists the complexity of decoding the primitive binary BCH codes using the proposed techniques, as compared to the complexity of the conventional decoders (Viterbi decoding based on the trellis of Wolf [6] for high-rate codes, and Fast Hadamard Transform decoding [1] for low-rate codes). These figures are given in terms of the number of real operations per bit of information. The computational gain obtained reaches several orders of magnitude in many cases. For instance for the (64,30,14) extended BCH code the proposed techniques are about 1,000 times more efficient.

Code	Wolf bound	DS and CS structures	Lower bound	Conventional decoding	Proposed techniques
BCH[8,4]	4	3	3	16	6
BCH[16,11]	5	4	4	66	26
BCH[16,7]	7	6	5	128	42
BCH[16,5]	5	4	4	32	13
BCH[32,26]	6	5	5	160	66
BCH[32,21]	11	10	9	3413	1094
BCH[32,16]	16	9	9	20480	251
BCH[32,11]	11	10	9	2048	398
BCH[32,6]	6	5	5	64	27
BCH[64,57]	7	6	6	$3.48 \cdot 10^2$	$1.32 \cdot 10^2$
BCH[64,51]	13	12	11	$1.91 \cdot 10^4$	$6.76 \cdot 10^3$
BCH[64,45]	19	14	11	$9.67 \cdot 10^5$	$2.19 \cdot 10^4$
BCH[64,39]	25	20	11	$4.04 \cdot 10^7$	$8.81 \cdot 10^5$
BCH[64,36]	28	19	15	$2.16 \cdot 10^8$	$3.77 \cdot 10^5$
BCH[64,30]	30	21	16	$6.08 \cdot 10^8$	$6.06 \cdot 10^5$
BCH[64,24]	24	16	14	$1.68 \cdot 10^7$	$1.96 \cdot 10^4$
BCH[64,18]	18	17	16	$2.62 \cdot 10^5$	$3.37 \cdot 10^4$
BCH[64,16]	16	15	14	$6.55 \cdot 10^4$	$1.16 \cdot 10^4$
BCH[64,10]	10	9	9	$1.02 \cdot 10^3$	$4.61 \cdot 10^2$
BCH[64,7]	7	6	6	$1.28 \cdot 10^2$	$5.49 \cdot 10^1$

## References

- [1] Y. Be'ery and J. Snyders, "Optimal soft decision block decoders based on Fast Hadamard Transform," *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 355-364, 1986.
- [2] G.D. Forney, Jr., "Coset Codes II: Binary lattices and related codes," *IEEE Trans. Inform. Theory*, vol. IT-34, pp. 1152-1187, 1988.
- [3] T. Kasami, T. Takata, T. Fujiwara, and S. Lin, "Trellis diagram construction for some BCH codes," *IEEE Int. Symp. Inform. Theory and Appl.*, Hawaii, 1990.
- [4] A. Vardy and Y. Be'ery, "On the problem of finding zero-concurring codewords," *IEEE Trans. Inform. Theory*, vol. IT-37, pp. 180-187, 1991.
- [5] A. Vardy and Y. Be'ery, "Maximum-likelihood soft decision decoding of BCH codes," *IEEE Trans. Inform. Theory*, submitted for publication.
- [6] J.K. Wolf, "Efficient maximum-likelihood decoding of linear block codes," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 76-80, 1978.