Reduced Complexity Bounded-Distance Decoding of the Leech Lattice

Ofer Amrani and **Yair Be'ery**, Tel-Aviv University Department of Electrical Engineering.
Alexander Vardy, IBM Research Division Almaden Research Center.

Abstract-**A new efficient algorithm for bounded-distance decoding of the Leech lattice is presented. The algorithm decodes correctly at least up to the guaranteed error-correction radius of the Leech lattice. The proposed decoder is based on projecting the points of the Leech lattice onto the codewords of the (6,3,4) quarternary code, — the *hexacode* H_6. Projection on the hexacode induces partition of the Leech lattice into four cosets of Q_{24}, beyond the conventional partition into two H_{24} cosets. This enables bounded-distance decoding of the Leech lattice with only 1127 real operations in the worst case, as compared to about 3600 operations for the maximum-likelihood decoding of [9]. The proposed algorithm is at least 30% more efficient than Forney's algorithm [5] in terms of computational complexity, while the coding gain loss is no more than 0.05 dB (over BER ranging from 10^{-1} to 10^{-6}).**

The *Leech lattice* Λ_{24} is one of the most interesting and well studied lattices [3]. Maximum-likelihood decoding of Λ_{24} was intensively investigated during the last few years. Conway and Sloane [2], Forney [4], Lang and Longstaff [6], Be'ery, Shahar, and Snyders [1], and Vardy and Be'ery [9] have devised various decoding algorithms with complexities ranging from 55968 down to 3595 operations. While the problem of maximum-likelihood decoding of Λ_{24} is interesting in its own right, in practice it may be rewarding to use a slightly suboptimal but more efficient bounded-distance decoding algorithm. One such algorithm was developed by Forney [5]. The computational complexity of the original Forney's algorithm is somewhat less than 2000 operations. However, since Forney's decoder is based on soft-decision decoding of the Golay code, utilizing the Golay decoder of [8] in Forney's bounded-distance algorithm yields a computational complexity of less than 1500 operations. In this paper we propose a more efficient bounded-distance decoding algorithm which requires only 1127 operations. The proposed algorithm is shown to decode correctly at least up to the guaranteed error-correction radius of the Leech lattice. Simulation results, which compare the coding gain obtained using the new algorithm with the coding gain of the Forney's algorithm, are also provided.

Our construction of the Leech-lattice involves the two-dimensional checkerboard lattice D_2. Partition D_2 into 16 subsets and arrange the labels of the 16 subsets in the following configuration:

$$\begin{matrix} A_{000} & B_{000} & A_{110} & B_{110} \\ B_{101} & A_{101} & B_{010} & A_{101} \\ A_{111} & B_{111} & A_{001} & B_{001} \\ B_{011} & A_{100} & B_{100} & A_{011} \end{matrix}$$

Tiling the entire space with nonoverlapping copies of scaled and rotated version of this 16-point configuration establishes a correspondence between the labels of the 16 subsets and the points of D_2. Let us represent the points of Λ_{24} by 2×6 arrays of D_2 points, such as :

$$\begin{bmatrix} A_{i_1j_1k_1} & A_{i_3j_3k_3} & \cdots & A_{i_{11}j_{11}k_{11}} \\ A_{i_2j_2k_2} & A_{i_4j_4k_4} & \cdots & A_{i_{12}j_{12}k_{12}} \end{bmatrix} \qquad (1)$$

The array in (1) is called type-A since it contains only A_{ijk} points. Similarly, type-B array will consist of only B_{ijk} points. Let $(A_{i_1j_1k_1}, A_{i_2j_2k_2})^t$ be a column of a type-A array and let $\underline{u} = (i_1, j_1, i_2, j_2)$ be the corresponding binary 4-tuple. If $\underline{u}$ contains an even number of nonzeros then the column is said to be *even*, otherwise the column is said to be *odd*. The index i_1 is called the *h-parity* of the column. The *overall h-parity* of the array is defined as the modulo-2 sum of the h-parities of the six columns. The *overall k-parity* of the array is the modulo-2 sum of the k subscripts of the 12 points. As in [8] any binary 4-tuple $\underline{u}$ is regarded as an *interpretation* of a character $x \in \{0, 1, \omega, \bar{\omega}\} = GF(4)$. Conversely any $x \in \{0, 1, \omega, \bar{\omega}\}$ may be regarded as the *projection* of four different binary 4-tuples $\underline{u}$, such that $x = (0, 1, \omega, \bar{\omega}) \cdot \underline{u}$. The *projection of the array* is a vector $\underline{x} \in GF(4)^6$ consisting of the projections of the six columns. Using the above notation the Leech lattice may be defined as follows [9]:

Definition 1. *The Leech lattice is the set of all the 2×6 arrays whose entries are points of D_2, such that each array satisfies the following conditions:*

i. *It is either type-A or type-B.*

ii. *It consists either of only even columns or only odd columns.*

iii. *The overall k-parity is even if the array is type-A, and odd otherwise.*

iv. *The overall h-parity is even if the columns are even, and odd otherwise.*

v. *The projection of the array is a codeword of H_6.*

Note that by restricting condition **i** of the foregoing definition, that is taking only the type-A arrays, the *Leech half-lattice* H_{24} is obtained. Further restricting condition **ii**, that is taking only even columns, produces the *Leech quarter-lattice* Q_{24}, as defined in [9]. The proposed decoding algorithm consists of four separate Q_{24} decoders operating concurrently. Basically the four decoders are identical. We therefore describe only the decoder for Q_{24}. This decoder operates on type-A arrays consisting of only even columns.

Precomputation: Let us assume an AWGN channel model, and let a sequence of 12 two-dimensional symbols $\{r(n)\}_{n=1}^{12}$ be observed at the channel output. For $n = 1, 2, \ldots 12$ find in each A_{ijk}-subset of D_2 a point $\hat{A}_{ijk}(n)$ which is closest to $r(n)$, and set this point as a representative of the entire subset.

Computation: For each $x \in GF(4)$ and for each of the six array locations, the decoder first finds the *preferable representation*, which is the column with the minimum squared Euclidean distance (SED) from the appropriate pair of received symbols. This SED is taken to be the metric of x. Using the acquired information the decoder finds the codeword of H_6 with the minimum metric. A type-A array with even columns is then reconstructed from this codeword of H_6. We show that this array is the closest to the received sequence of symbols. Next conditions **iv** and **iii** are checked, in this order. If either of these conditions is violated, correction is performed for condition **iv** and independently for condition **iii** using the "Wagner decoding rule" of [7].

The output of the Q_{24} decoder is a Leech quarter-lattice point accompanied by a corresponding metric. This point is not necessarily the closest to the received sequence of symbols due to the independent Wagner decoding. Finally we choose among the outputs of the four Q_{24} decoders the point with the minimal metric, and select this point as the output of our Leech lattice decoder.

Now let d_0 be the minimum distance between points in the checkerboard lattice D_2. The corresponding minimum SED between points in Λ_{24} is given by $d^2_{min} = 16d_0^2$. We have the following theorem.

Theorem 1. *Given a received vector of 12 two-dimensional symbols* $\mathbf{r} = \{r(n)\}_{n=1}^{12}$, *if there is a point* $\lambda \in \Lambda_{24}$ *such that* $\|\mathbf{r} - \lambda\|^2 < 4d_0^2$, *the proposed algorithm decodes* $\mathbf{r}$ *to* λ.

Theorem 1 implies that the proposed algorithm decodes correctly at least up to the guaranteed error correction radius of the Leech lattice $d_{min}/2 = 2d_0$. This correction capability is the same as that of the bounded-distance decoder of Forney [5]. A comprehensive computer simulation has been performed for both the proposed algorithm and the algorithm of Forney [5]. The simulation assumed a 64-QAM square constellation transmitted over an AWGN channel. Results show no more than 0.05 dB loss in the coding gain for our algorithm versus that of Forney, over the whole range of BER from 10^{-1} to 10^{-6}. This gain loss is due to an increase in the *effective error coefficient*, or the number of nearest neighbors, for the proposed algorithm. This issue will be further elaborated in the paper.

References

[1] Y. Be'ery, B. Shahar, and J. Snyders, "Fast decoding of the Leech lattice," *IEEE J. Select. Areas Comm.*, vol. SAC-7, pp. 959–967, 1989.

[2] J.H. Conway and N.J.A. Sloane, "Soft decoding techniques for codes and lattices, including the Golay code and the Leech lattice," *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 41–50, 1986.

[3] J.H. Conway and N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Veralg, New York, 1988.

[4] G.D. Forney, Jr., "Coset Codes II: Binary lattices and related codes," *IEEE Trans. Inform. Theory*, vol. IT-34, pp. 1152–1187, 1988.

[5] G.D. Forney, Jr., "A bounded distance decoding algorithm for the Leech lattice, with generalizations," *IEEE Trans. Inform. Theory*, vol. IT-35, pp. 906–909, 1989.

[6] G.R. Lang and F.M. Longstaff, "A Leech lattice modem," *IEEE J. Select. Areas Comm.*, vol. SAC-7, pp. 968–973, 1989.

[7] R.A. Silverman and M. Balser, "Coding for a constant data rate source," *IRE Trans. Inform. Theory*, vol. 4, pp. 50–63, 1954.

[8] A. Vardy and Y. Be'ery, "More efficient soft-decision decoding of the Golay codes," *IEEE Trans. Inform. Theory*, vol. IT-37, pp. 667–672, 1991.

[9] A. Vardy and Y. Be'ery, "More efficient maximum-likelihood decoding of the Leech lattice," to appear in *IEEE Trans. Inform. Theory.*