Coset Codes—Part II: Binary Lattices and Related Codes

G. DAVID FORNEY, JR., FELLOW, IEEE

Invited Paper

Abstract—**The family of Barnes–Wall lattices (including D_4 and E_8) of lengths $N = 2^n$ and their principal sublattices, which are useful in constructing coset codes, are generated by iteration of a simple construction called the "squaring construction." The closely related Reed–Muller codes are generated by the same construction. The principal properties of these codes and lattices, including distances, dimensions, partitions, generator matrices, and duality properties, are consequences of the general properties of iterated squaring constructions, which also exhibit the interrelationships between codes and lattices of different lengths. An extension called the "cubing construction" generates good codes and lattices of lengths $N = 3 \cdot 2^n$, including the Golay code and Leech lattice, with the use of special bases for 8-space. Another related construction generates the Nordstrom–Robinson code and an analogous 16-dimensional nonlattice packing. These constructions are represented by trellis diagrams that display their structure and interrelationships and that lead to efficient maximum likelihood decoding algorithms. General algebraic methods for determining minimal trellis diagrams of codes, lattices, and partitions are given in an Appendix.**

I. Introduction

A COMPANION PAPER [1] characterizes a large number of the coded modulation techniques that have been proposed for band-limited channels as coset codes, i.e., as sequences of cosets of a sublattice Λ' in a partition Λ/Λ' of a binary lattice Λ, where the cosets are selected by the outputs of a binary encoder.

The principal purpose of this paper is to give a unified development of the family of lattices that have proved to be most useful in constructing coset codes and of the properties of such lattices that are most important for such applications, e.g., their minimum squared distances, their partitions, and aspects of their structure that are useful in decoding.

This family of lattices is the sequence of 2^n-dimensional lattices called the Barnes–Wall lattices, and what we call their "principal sublattices." This family includes such important lattices as the Schläfli lattice D_4, the Gosset lattice E_8, and the infinite sequence $\Lambda_{16}, \Lambda_{32}, \cdots$ of Barnes–Wall lattices, whose fundamental coding gain [1] increases by a factor of $2^{1/2}$ (1.5 dB) for each doubling of dimension.

What may be obscured by the length of this paper is that the construction of these lattices is extremely simple. The only building blocks needed are the set $\boldsymbol{Z}$ of ordinary integers, with its infinite chain of two-way partitions $\boldsymbol{Z}/2\boldsymbol{Z}/4\boldsymbol{Z}/\cdots$, and an elementary construction that we call the "squaring construction," which produces chains of $2N$-tuples with certain guaranteed distance properties from chains of N-tuples. Iteration of this construction produces the entire family of lattices, determines their minimum squared distances, shows their partition (sublattice) structure, and gives general interrelationships between the lattices of different dimension. The construction also naturally points to structural decompositions that we illustrate by trellis diagrams and that lead to efficient maximum likelihood decoding algorithms. Other attributes of these lattices, such as their generator matrices, "code formulas" [1], and duality properties, may be easily derived from general properties of this simple construction.

Actually, the development makes it clear that the most natural starting point for the construction is the two-dimensional lattice $\boldsymbol{Z}^2$ of pairs of ordinary integers, with its infinite chain of two-way partitions $\boldsymbol{Z}^2/R\boldsymbol{Z}^2/2\boldsymbol{Z}^2/\cdots$ or, equivalently, the complex lattice $\boldsymbol{G}$ of Gaussian integers [1], with its partition chain $\boldsymbol{G}/\phi\boldsymbol{G}/\phi^2\boldsymbol{G}/\cdots$, where $\phi = 1 + i$.

These lattices are closely related to the family of Reed–Muller codes. Indeed, the Reed–Muller codes can be generated by the same construction, except that the starting point is the binary field GF(2), with the exhaustive two-way partition into its two elements. The two-by-two integer matrix $G_{(2,2)} = \{[10],[11]\}$ turns out to be a key tool in describing the application of the squaring construction to group partitions, and the m-fold Kronecker product of this matrix with itself, i.e., the $N \times N$ integer matrix $G_{(N,N)}$ that contains all the generators of all the Reed–Muller codes of length $N = 2^m$, turns out to be very helpful in characterizing the results of m-fold iterated squaring constructions (Lemma 2).

A construction that we call the "cubing construction," which is closely related to the twofold iteration of the squaring construction, produces groups of $3N$-tuples from groups of N-tuples. The principal use that we make of this construction is to construct the (24,12) Golay code and the

Manuscript received September 2, 1986; revised September 18, 1987. This paper was partially presented at the 1986 IEEE International Symposium on Information Theory, Ann Arbor, MI, October 8, and at the 1986 IEEE Communications Theory Workshop, Palm Springs, CA, April 28.

The author is with the Codex Corporation, 7 Blue Hill River Road, Canton, MA 02021.

IEEE Log Number 8824502.

0018-9448/88/0900-1152$01.00 ©1988 IEEE

24-dimensional Leech lattice. In addition to the cubing construction, we need to introduce special bases of 8-space to obtain the requisite distance properties.

Using these bases, we go on to construct the length-16 nonlinear Nordstrom–Robinson code, which is better than any comparable linear code, and an analogous 16-dimensional nonlattice packing, which falls just short of the density of the 16-dimensional Barnes–Wall lattice Λ_{16}. These constructions are closely related to each other and to those already described. Furthermore, they show that while coset code constructions may almost always be based on partitions that result from coset decompositions of groups (codes, lattices), the resulting constructions need not themselves be linear to have good distance properties (indeed, many of the best trellis codes are nonlinear [1]).

These constructions lead directly to unexpectedly simple and highly structured trellis diagrams for these codes and lattices. The trellis diagrams suggest maximum likelihood decoding algorithms for both codes and lattices that generally turn out to be improvements over the best previously known algorithms. For completeness, we give methods for systematic algebraic determination of minimal trellis diagrams for linear codes and lattices in an Appendix.

Relatively little in this paper is new. All of the codes and lattices are well-known (except for the 16-dimensional nonlattice packing, which was noticed earlier by Conway and Sloane but has not previously been published). Their constructions and properties have generally been derived earlier in various forms, some essentially equivalent to our constructions, which we have attempted to acknowledge appropriately. While we know of no readily accessible text on lattices, the recent book by Conway and Sloane [2] is an encyclopedic reference for practically everything here and far more. What we hope to have contributed is a unified treatment of the lattices that are most useful in applications, with a derivation of their principal properties, at a reasonably elementary mathematical level. We do believe that the structural properties exhibited in our trellis diagrams are generally new, as well as the decoding methods that they suggest.

The paper is organized as follows. In Section II we introduce the language and elementary results that we use for sets, set partitions, distance measures, and additive groups, particularly groups with orders equal to a power of two, with a few words on binary codes and lattices. Section III contains the general properties of the squaring construction and of iterated squaring constructions; then, in Section IV, the Reed–Muller codes and Barnes–Wall lattices are developed using these constructions, along with their principal properties. Similarly, Section V is devoted to the cubing construction, which then is used in Section VI to develop the Golay code and Leech lattice after the introduction of special bases for 8-space. In Section VII these bases are used to construct the Nordstrom–Robinson code and the analogous 16-dimensional nonlattice packing. In Section VIII we work out some examples of our decoding algorithms, for the (8,4) first-order Reed–Muller code (and the E_8 lattice), the Golay code, and the Leech lattice. Finally, in the Appendix we show how to determine the state spaces and trellis diagrams of codes, lattices, and partitions algebraically, using trellis-oriented generator matrices.

II. Preliminaries

This paper is about discrete sets on which a distance metric is defined, partitions of such sets, and set constructions based on such partitions. In this section we gather the elementary facts that we will need about such sets and partitions. These sets will almost always be algebraic groups, i.e., closed under some addition operation; however, the constructions do not essentially depend on group properties, and to emphasize this point, we defer the discussion of group properties for as long as possible.

A. Partitions

Let S be any discrete set with elements $s \in S$. An *M-way partition* of S is specified by a set of M disjoint subsets $T(a)$ whose union is S, where a is a *label* for the subset $T(a)$. We denote such a partition by S/T, and we say that the *order* of the partition is $|S/T| = M$. Ordinarily, in this paper, the order of a partition will be finite, even when the sets involved are infinite.

A *subset labeling* is any one-to-one map between the subsets and a set of M labels. Examples of labels which we shall use include: a subset index i, where, for example, $0 \le i \le M-1$; binary K-tuples $\boldsymbol{a}$, when $M = 2^K$; or a system of subset *representatives* $c \in S$, one from each subset. When S contains a zero element 0, we call the subset that contains 0 the *zero subset* $T(0)$, or simply T, and use 0 as its representative.

For example, there is a two-way partition of the set of ordinary integers $\boldsymbol{Z}$ into the even integers, $2\boldsymbol{Z}$, and the odd integers, $2\boldsymbol{Z}+1$. We say that $\boldsymbol{Z}/2\boldsymbol{Z}$ is a partition of order 2. The natural labels for the subsets are $\{0,1\}$, where $2\boldsymbol{Z}$ is the zero subset.

An *m-level partition chain* $S_0/S_1/\cdots/S_m$ is obtained by repeated partitioning of subsets; i.e., the set S_0 is first partitioned into $|S_0/S_1|$ subsets $S_1(a_0)$, then each subset $S_1(a_0)$ of S_0 is partitioned, and so forth. We shall require that the order of all subset partitions at any given level be the same; e.g., that all second-level partitions of the subsets $S_1(a_0)$ have the same order. Then we can say that the order $|S_j/S_{j+1}|$ is the common order of all jth-level partitions, and $|S_0/S_m|$ must then be the product of the orders $|S_j/S_{j+1}|$, $0 \le j \le m-1$.

It is natural to label an m-level partition by an *m-part label* $\boldsymbol{a} = (a_0, a_1, \cdots, a_{m-1})$, where a_j is one of a set of $|S_j/S_{j+1}|$ labels, $0 \le j \le m-1$. The subsets at the jth level may then be labeled by the first j parts of the label; e.g., $S_1(a_0)$, $S_2(a_0, a_1)$, and so forth. In other words, the same system of labels a_j is used for each partition $S_j(a_0,\cdots,a_{j-1})/S_{j+1}(a_0,\cdots,a_j)$. The final subsets $S_m(\boldsymbol{a})$ are labeled by the complete m-part label $\boldsymbol{a}$.

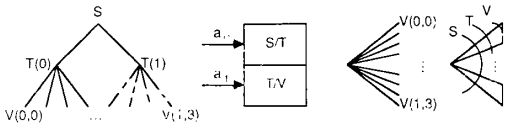


Fig. 1. Two-level partition $S/T/V$. (a) As partition trees. (b) As partition tower. (c) As partition trellis. (d) As schematic trellis.

Fig. 1 illustrates a two-level partition $S/T/V$ in three ways: as a tree, as a tower, and as a trellis. Let the orders of the partitions be $M = |S/T|$ and $N = |T/V|$, so that $|S/V| = MN$; in the figure, $M = 2$ and $N = 4$. Then the subsets $T(a_0)$ are labeled by an M-valued label a_0, and the subsets $V(\boldsymbol{a})$ are labeled by an MN-valued two-part label $\boldsymbol{a} = (a_0, a_1)$. The *partition tree* consists of an M-way branch at the first level, where each branch may be labeled by a label a_0, followed by N-way branches of each first-level subset at the second level, where each branch may be labeled by a label a_1. The *partition tower* represents the selection of a subset $T(a_0)$ of S in the partition S/T by a first label a_0, and then the selection of a subset $V(a_0, a_1)$ of $T(a_0)$ by a second label a_1. The *partition trellis* is a single-level representation of the partition tree with each of the MN branches representing a subset $V(\boldsymbol{a})$, and the branches grouped into M clusters of N branches, each cluster representing a subset $T(a_0)$. The final illustration is a generic *schematic trellis diagram* for a two-level partition with arbitrary orders $|S/T|$ and $|T/V|$.

The *dummy partition* S/S is a one-way "partition" of S into a single subset, namely S itself; partition chains can be arbitrarily extended by dummy partitions. If Z is a single-element subset (e.g., $Z = \{0\}$), then a partition chain can be extended all the way down to Z, yielding the *exhaustive partition* S/Z, whose order is the number of elements in S.

The *Cartesian product* S^N is defined as the set of all N-tuples $\boldsymbol{s} = (s_1, s_2, \cdots, s_N)$ of elements of S. If S/T is a partition of order $|S/T|$, then S^N/T^N is a partition of order $|S^N/T^N| = |S/T|^N$. The subsets of the partition S^N/T^N may be labeled by an N-tuple label $(a_1, a_2, \cdots, a_N)$, where $T^N(a_1, a_2, \cdots, a_N)$ is the subset of S^N consisting of N-tuples whose first component is in $T(a_1)$, whose second component is in $T(a_2)$, and so forth. If $S_0/S_1/\cdots/S_m$ is an m-level partition chain, then $S_0^N/S_1^N/\cdots/S_m^N$ is an m-level partition chain, and the $|S_0/S_m|^N$ subsets of S_0^N may be labeled by m-part, N-tuple labels $\boldsymbol{a} = \{a_{ij},\ 1 \le i \le N,\ 0 \le j \le m-1\}$, where $\boldsymbol{a}_i = \{a_{ij},\ 0 \le j \le m-1\}$ is an m-part label for the $|S_0/S_m|$ subsets of S_0 for each i, $1 \le i \le N$.

B. Distances

We are interested in discrete sets S on which a *distance metric* $d(s, s')$ is defined between pairs (s, s') of elements of S. We assume that $d(s, s')$ is zero if $s = s'$ and greater than zero if $s \neq s'$, and we define the *minimum distance* $d(S)$ of S as the minimum nonzero $d(s, s')$. (If S is a trivial set with only one element, we say $d(S) = \infty$.)

If S/T is a partition of S, the distance metric on S carries over to its subsets $T(a)$. We define the minimum distance $d(T)$ as the least minimum distance of any subset $T(a)$. Sometimes we say in shorthand that the partition S/T has distances $d(S)/d(T)$, where the slash is only a separation symbol. Generally, we are interested in partitions for which $d(T) > d(S)$.

If $T(a)$ and $T(a')$ are subsets of S, the *subset distance* $d(a, a')$ is defined as follows: a) if $a \neq a'$, $d(a, a')$ is the minimum distance between the elements of the distinct subsets $T(a)$ and $T(a')$; b) if $a = a'$, then $d(a, a')$ is the minimum distance between distinct elements of the subset $T(a)$, i.e., $d(a, a) = d(T(a))$.

In a single-level partition S/T, $d(a, a')$ is lower-bounded by $d(S)$ in general, but if $a = a'$, then $d(a, a') \ge d(T)$. In a two-level partition $S/T/V$ with a two-part label $\boldsymbol{a} = (a_0, a_1)$, $d(\boldsymbol{a}, \boldsymbol{a}')$ is lower-bounded as follows:

a) in all cases, $d(\boldsymbol{a}, \boldsymbol{a}') \ge d(S)$;
b) if $a_0 = a_0'$, then $d(\boldsymbol{a}, \boldsymbol{a}') \ge d(T)$, because $V(\boldsymbol{a})$ and $V(\boldsymbol{a}')$ are both subsets of the same first-level subset $T(a_0)$;
c) if $\boldsymbol{a} = \boldsymbol{a}'$, then $d(\boldsymbol{a}, \boldsymbol{a}') \ge d(V)$, by definition.

This lower bound thus depends only on whether the parts of the label are the same or different; i.e., on the Hamming distances between parts of the label, where the *Hamming distance* between two quantities is defined as zero if they are the same and one if they are different.

The general version of these observations is the essential distance property used in constructions based on set partitions, which we shall call the *partition distance lemma*: if $S_0/S_1/\cdots/S_m$ is an m-level partition chain with distances $d(S_0)/d(S_1)/\cdots/d(S_m)$ and $S_m(\boldsymbol{a})$ and $S_m(\boldsymbol{a}')$ are subsets with multipart labels $\boldsymbol{a}$ and $\boldsymbol{a}'$, respectively, then the subset distance $d(\boldsymbol{a}, \boldsymbol{a}')$ is lower-bounded by $d(S_j)$, where if $\boldsymbol{a} \neq \boldsymbol{a}'$, j is the smallest index such that $a_j \neq a_j'$, while if $\boldsymbol{a} = \boldsymbol{a}'$, j is equal to m.

If S^N is the N-fold Cartesian product of S with itself, then let the distance metric between two N-tuples $\boldsymbol{s}$ and $\boldsymbol{s}'$ be defined as the sum of the N componentwise distances $d(s_i, s_i')$, $1 \le i \le N$. Then $d(S^N) = d(S)$, since distinct N-tuples need not differ in more than one element. Distance metrics that naturally have this *additive property* include

a) Hamming distance: $d_H(\boldsymbol{s}, \boldsymbol{s}') = \sum_i d_H(s_i, s_i')$, where

$$d_H(s, s') \triangleq \begin{cases} 0, & \text{if } s = s' \\ 1, & \text{if } s \neq s' \end{cases};$$

b) squared Euclidean distance: $\|\boldsymbol{s} - \boldsymbol{s}'\|^2 \triangleq d_E(\boldsymbol{s}, \boldsymbol{s}') = \sum_i d_E(s_i, s_i')$, where $d_E(s, s') \triangleq |s - s'|^2$.

Thus if S/T is an M-way partition with distances $d(S)/d(T)$, then S^N/T^N is an M^N-way partition that also has distances $d(S)/d(T)$.

C. Group Partitions

Often we shall be interested in sets S which are groups, primarily because any subgroup T of a group S naturally

induces a partition of S into subsets, namely, the cosets of T. We recall the following facts from elementary group theory:

An (additive) *group* S is defined by a set of elements $\boldsymbol{s} \in S$ including $\mathbf{0}$, and an addition operation such that $(\boldsymbol{s}+\boldsymbol{s}') \in S$, $\boldsymbol{s}+\mathbf{0}=\boldsymbol{s}$, and $\boldsymbol{s}+\boldsymbol{s}'=\mathbf{0}$ has a solution $\boldsymbol{s}' \in S$ called $-\boldsymbol{s}$. Our groups will mostly be groups of N-tuples (vectors, points), and the addition operation will be some form of vector addition. (Thus we will use bold face for group elements $\boldsymbol{s}$.)

When S is a group, we assume that the distance metric $d(\boldsymbol{s}, \boldsymbol{s}')$ has the *group property*, $d(\boldsymbol{s}, \boldsymbol{s}') = d(\mathbf{0}, \boldsymbol{s}-\boldsymbol{s}') = \mathrm{wt}(\boldsymbol{s}-\boldsymbol{s}')$, where the last expression involves the *weight* $\mathrm{wt}(\boldsymbol{s}) \triangleq d(\mathbf{0}, \boldsymbol{s})$. Of course $\mathrm{wt}(\mathbf{0})=0$ and, assuming that the distance metric is symmetric, $\mathrm{wt}(\boldsymbol{s})=\mathrm{wt}(-\boldsymbol{s})$. The minimum distance $d(S)$ is then equal to the minimum nonzero weight of any element $\boldsymbol{s} \in S$. Both Hamming distance and squared Euclidean distance have the group property; the weight of $\boldsymbol{s}$ may be identified as the *norm* $\|\boldsymbol{s}\|^2$ in the latter case.

Any subgroup T of a group S naturally induces a partition of S as follows. Two elements $\boldsymbol{s}$ and $\boldsymbol{s}'$ are said to be *equivalent* (or *congruent*) *modulo* T if $(\boldsymbol{s}-\boldsymbol{s}') \in T$, and we may write $\boldsymbol{s} \equiv \boldsymbol{s}' (\mathrm{mod}\, T)$. Since $\boldsymbol{s} \equiv \boldsymbol{s}'$, $\boldsymbol{s} \equiv \boldsymbol{s}''$, implies $\boldsymbol{s}' \equiv \boldsymbol{s}''$, congruence modulo T is an equivalence relation and partitions S into disjoint equivalence classes; we denote this partition by S/T.

Let us label each class by taking one of its elements $\boldsymbol{c}$ as a representative. The equivalence class $T(\boldsymbol{c})$ that contains $\boldsymbol{c}$ is the set $\{\boldsymbol{t}+\boldsymbol{c}\colon\ \boldsymbol{t} \in T\}$, which we write as $T+\boldsymbol{c}$. Any set $T+\boldsymbol{c}$ is called a *coset* of T in S, and any such $\boldsymbol{c}$ is called a *coset representative*. The coset containing $\mathbf{0}$ is the *zero coset* $T+\mathbf{0}$, which is T itself, and we always use $\mathbf{0}$ as coset representative for the zero coset.

All cosets of T must have the same minimum distance $d(T)$, which is equal to the minimum nonzero weight within T itself. The subset distance $d(\boldsymbol{c}, \boldsymbol{c}')$ between the cosets $T+\boldsymbol{c}$ and $T+\boldsymbol{c}'$ is the minimum weight within the coset $T+(\boldsymbol{c}-\boldsymbol{c}')$; if we define $\mathrm{wt}(\boldsymbol{c})$ as the minimum weight within $T+\boldsymbol{c}$, then $d(\boldsymbol{c}, \boldsymbol{c}') = \mathrm{wt}(\boldsymbol{c}-\boldsymbol{c}')$.

Let $[S/T]$ denote any system of coset representatives $\boldsymbol{c}$, one for each equivalence class; then S is the union of the $|S/T|$ cosets $T+\boldsymbol{c}$, $\boldsymbol{c} \in [S/T]$, so every $\boldsymbol{s} \in S$ is equivalent to one such $\boldsymbol{c} \in [S/T]$, and thus every $\boldsymbol{s} \in S$ has a unique representation of the form $\boldsymbol{s}=\boldsymbol{t}+\boldsymbol{c}$ for some $\boldsymbol{c} \in [S/T]$ and $\boldsymbol{t} \in T$, namely, $\boldsymbol{t}=\boldsymbol{s}-\boldsymbol{c}$. Thus S is the direct sum of $[S/T]$ and T. This is called a *coset decomposition* of S and will be written here as $S=[S/T]+T$. (We reserve the symbol $\oplus$ for mod-2 addition.)

The sum of two cosets $T+\boldsymbol{c}$ and $T+\boldsymbol{c}'$ is defined as the coset $T+(\boldsymbol{c}+\boldsymbol{c}')$ which contains any sum of two elements, one taken from each coset. Under this definition of addition, the cosets form a group, called the *quotient group*, and also denoted as S/T. The order $|S/T|$ of this group is the number of cosets of T in S (also called the index of T in S), which is the same as the order of the partition S/T, so the notation and terminology are consistent.

If S is a finite group, then $|S|=|T||S/T|$; therefore, the order of any subgroup T divides $|S|$. While no multiplication operation need be defined on a group, it is always possible to multiply group elements by integers, since the product $\pm m\boldsymbol{s}$ of any integer $\pm m \in \boldsymbol{Z}$ with any group element $\boldsymbol{s} \in S$ is $\pm(\boldsymbol{s}+\boldsymbol{s}+\cdots)$ (m times). The set $[\boldsymbol{s}]$ of all such multiples is a subgroup of S. The order of the subgroup $[\boldsymbol{s}]$ is called the order of the element $\boldsymbol{s}$; the order of any element $\boldsymbol{s} \in S$ must therefore divide the order of S.

If S is a group with order $|S|=2^K$ for some K, we say that S is a *binary group*. Any subgroup of a binary group is a binary group, and all elements of a binary group have orders equal to powers of two. Any nontrivial binary group contains an element of order 2; for if $\boldsymbol{s}$ is any nonzero element, then the sequence $\boldsymbol{s}, 2\boldsymbol{s}, 4\boldsymbol{s}, \cdots$ eventually arrives at $\mathbf{0}$, and the last nonzero element of this sequence has order 2.

If S is a binary group with order $|S|=2^K$, then every element of S can be expressed as $s(\boldsymbol{a})=\sum_k a_k \boldsymbol{g}_k = \boldsymbol{a}G$, where $\boldsymbol{a}=(a_0, a_1, \cdots, a_{K-1})$ is an integer K-tuple such that $a_k \in \{0,1\}$, $0 \le k \le K-1$, and the *generators* $\boldsymbol{g}_k$ are a set $G=\{\boldsymbol{g}_k,\ 0 \le k \le K-1\}$ of group elements. The set G will be called a *generator matrix*, the parameter K (the binary logarithm of $|S|$) will be called the (binary) *dimension* of S, and the expression $s(\boldsymbol{a})=\boldsymbol{a}G$ will be called a *binary linear combination* of the generators. This may be shown by induction, as follows: choose $\boldsymbol{g}_{K-1}$ as any nonzero group element of order 2; then if T is the subgroup $[g_{K-1}] \triangleq \{\mathbf{0}, \boldsymbol{g}_{K-1}\} = \{a_{K-1}\boldsymbol{g}_{K-1}, a_{K-1} \in \{0,1\}\}$, S has the coset decomposition $S=[S/T]+T$, where the quotient group S/T of elements of S modulo T is another binary group, with order $|S/T|=2^{K-1}$. Repeating K times, we arrive at the desired expression.

A sequence $S_0, S_1, \cdots, S_m$ of groups S_j is said to be *nested* if S_{j+1} is a subgroup of S_j, $0 \le j \le m-1$. Then $S_0/S_1/\cdots/S_m$ is an m-level partition chain, and all partitions at the jth level have order $|S_j/S_{j+1}|$. The order of $|S_0/S_m|$ is the product of the orders of the $|S_j/S_{j+1}|$, $0 \le j \le m-1$. A coset of S_m in S_0 can be labeled by the m-part label $\boldsymbol{c}=(\boldsymbol{c}_0, \boldsymbol{c}_1, \cdots, \boldsymbol{c}_{m-1})$, where $\boldsymbol{c}_j$ is a coset representative in $[S_j/S_{j+1}]$, $0 \le j \le m-1$. This is a chain coset decomposition, $S_0=[S_0/S_1]+[S_1/S_2]+\cdots+S_m$. (The expression $s(\boldsymbol{a})=\sum_k a_k \boldsymbol{g}_k$ for elements of binary groups is an example of such a chain decomposition.) In this case the partition distance lemma is expressed as follows: the subset distance $d(\boldsymbol{c}, \boldsymbol{c}')$ between two cosets is lower-bounded by $d(S_j)$, the minimum distance between elements of S_j, where if $\boldsymbol{c} \ne \boldsymbol{c}'$, then j is the smallest index such that $\boldsymbol{c}_j \ne \boldsymbol{c}_j'$, while if $\boldsymbol{c}=\boldsymbol{c}'$, then j is equal to m.

If $|S_0/S_m|$ is some power of two, say 2^K, then we say that $S_0/S_1/\cdots/S_m$ is a *binary partition chain*. Because $|S_j/S_{j+1}|$ divides $|S_0/S_m|$, the order of each partition in the chain must be a power of two, say 2^{k_j}, and $K=\sum_j k_j$. Obviously, we can label the cosets of S_{j+1} in S_j by binary k_j-tuples $\boldsymbol{a}_j$ in any arbitrary way (but with the zero coset labeled by the all-zero k_j-tuple $\mathbf{0}$). Then an alternative m-part label for the cosets of S_m in S_0 is the binary K-tuple $\boldsymbol{a}=(\boldsymbol{a}_0, \boldsymbol{a}_1, \cdots, \boldsymbol{a}_{m-1})$. Because the partition distance lemma is based only on whether labels are the same or different, it continues to apply, however we label the cosets.

In a binary partition chain, at each level the quotient group S_j/S_{j+1} is a binary group, and therefore a set of k_j generators $G_j = \{\boldsymbol{g}_{jk}\}$ exists such that the elements of S_j/S_{j+1} are the binary linear combinations $\boldsymbol{a}_j G_j$ of the generators in the generator matrix G_j. In other words, we have a coset decomposition $S_j = S_{j+1} + \{\boldsymbol{a}_j G_j\}$, meaning that every $\boldsymbol{s}_j \in S_j$ has a unique representation of the form $\boldsymbol{s}_j = \boldsymbol{s}_{j+1} + \boldsymbol{a}_j G_j$ for some $\boldsymbol{s}_{j+1} \in S_{j+1}$ and some integer k_j-tuple $\boldsymbol{a}_j$ with $a_{jk} \in \{0,1\}$, $0 \le k \le k_j - 1$. Concatenating these representations, we arrive at a set of K generators $G = \{G_j, 0 \le j \le m-1\}$ that is a generator matrix for S_0/S_m; i.e., every $\boldsymbol{s}_0 \in S_0$ has a unique representation $\boldsymbol{s}_0 = \boldsymbol{s}_m + \boldsymbol{a}G$ for some $s_m \in S_m$ and some integer K-tuple $\boldsymbol{a} = (\boldsymbol{a}_0, \boldsymbol{a}_1, \cdots, \boldsymbol{a}_{m-1})$ with $a_k \in \{0,1\}$, $0 \le k \le K-1$. Obviously, this is a nice way of assigning labels to the cosets of S_m in S_0.

Note that if S_j and $S_{j'}$, $j' > j$, are any two groups in the partition chain, then the union of the generator matrices from G_j to $G_{j'-1}$ is a generator matrix for $S_j/S_{j'}$. This motivates the following definition of addition of generator matrices: the sum of two generator matrices is the union of their generators. Thus we may write, for example, $G = \sum_j G_j$. The empty set $\{\varnothing\}$ is the zero generator matrix under this notion of addition. However, there is no additive inverse or subtraction in this algebra.

Fig. 2 illustrates a binary partition chain $S_0/S_1/\cdots/S_m$ with $|S_0/S_m| = 2^K$ in three different ways. The first is as a partition tower (as in Fig. 1(b)) with vertical heights scaled proportionally to the dimensions k_j. The second is as a corresponding tower for a chain $T_0/T_1/\cdots/T_K$ of two-way partitions, where the subgroups T_k are defined recursively by $T_{k-1} = T_k + \{a_{k-1}\boldsymbol{g}_{k-1}\}$, starting with $T_K = S_m$, with the label $\boldsymbol{a}$ broken out into individual values $a_0, a_1, \cdots, a_{K-1}$. We can arrange this ordering so that all of the groups $S_0, S_1, \cdots, S_m$ appear in the chain $T_0/T_1/\cdots/T_K$. Finally, we give a chain representation of the chain $S_0/S_1/\cdots/S_m$, with the links of the chain labeled with the corresponding generator matrices G_j, and a similar representation of the chain $T_0/T_1/\cdots/T_K$, with the links labeled by the corresponding generators $\boldsymbol{g}_k$.

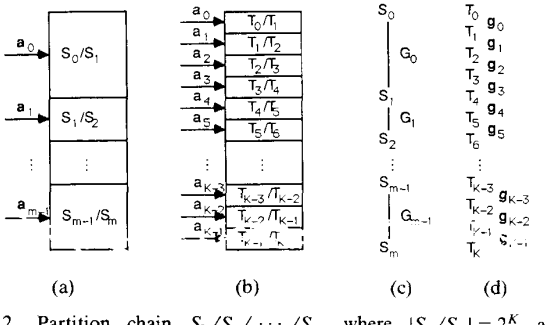


Fig. 2. Partition chain $S_0/S_1/\cdots/S_m$, where $|S_0/S_m| = 2^K$ and $|S_0/S_1| = 2^4$, $|S_1/S_2| = 2^2$, $|S_{m-1}/S_m| = 2^3$. (a) As partition tower. (b) As corresponding tower of two-way partitions $T_0/T_1/\cdots/T_K$. (c) As chain representation for $S_0/S_1/\cdots/S_m$, showing the generator matrices G_j for S_j/S_{j+1}. (d) As chain representation for $T_0/T_1/\cdots/T_K$, showing generators $\boldsymbol{g}_k$ for T_k/T_{k+1}.

D. Binary Codes and Lattices

The groups S_j that we are most interested in are binary codes and lattices.

A *binary* (N, K) *code* C is a set of 2^K binary N-tuples (*codewords*) that forms a group under mod-2 vector addition. The components of the codewords are usually thought of as belonging to the binary field GF(2), whose elements we shall write in bold face as $\{\mathbf{0}, \mathbf{1}\}$; however, they may equally well be thought of as ordinary integers restricted to the values $\{0,1\}$, since mod-2 vector addition and multiplication by a binary scalar lead to the same result in either case.

We use (vector) Hamming distance as a distance metric for codes. If we regard a codeword as an integer N-tuple, then the Hamming weight of a codeword $\boldsymbol{c}$ is equal to its norm $\|\boldsymbol{c}\|^2$. If the minimum Hamming distance between elements of the code C is $d_H(C) = d$, we may also use the notation (N, K, d) for the code C.

Since C is a binary group, from the discussion above, C has a generator matrix G_C consisting of K generators $\boldsymbol{g}_k$, where each $\boldsymbol{g}_k$ is a codeword in C, such that the code consists of the 2^K binary linear combinations $\boldsymbol{a}G_C$ of the generators, using mod-2 vector addition. (In fact, if we regard the codeword components as elements of GF(2), then C must be a vector space of dimension K over the field GF(2).) If C' is an (N, K') code that is a subcode of C, then G_C can be chosen to include a generator matrix $G_{C'}$ for C', and we may write $G_C = G_{C'} + G_{C/C'}$, meaning that the generator matrix for C is a union of a generator matrix for C' with a set of $K - K'$ generators $G_{C/C'}$ for C modulo C'. The set of $2^{K-K'}$ binary linear combinations $\boldsymbol{a}G_{C/C'}$ is a system of coset representatives $[C/C']$, and $C = C' + [C/C']$ is a coset decomposition of C corresponding to the decomposition $G_C = G_{C'} + G_{C/C'}$ of its generator matrix.

Any binary code C is a subcode of the (N, N) code of all binary N-tuples, so $(N, N)/C$ is a 2^{N-K}-way partition of the binary N-tuples into cosets of C, and there is a generator matrix $G_{(N,N)}$ for the (N, N) code that contains a generator matrix G_C for C plus $N - K$ additional generator $G_{(N,N)/C}$ that generate a system of coset representatives $[(N, N)/C]$ for the cosets of C.

A generator matrix $G_{(N,N)}$ for the (N, N) code is an $N \times N$ integer matrix that is a basis for binary N-space. Its (integer) determinant must be congruent to 1 modulo 2. If in fact the determinant is equal to ± 1, then we say that $G_{(N,N)}$ is a *universal basis* for any Cartesian product S^N, where S is any group, or a "universal basis for N-space"; for then (and only then) $G_{(N,N)}$ has an integer inverse $G_{(N,N)}^{-1}$, so that any element $\boldsymbol{s} \in S^N$ can be uniquely expressed as $\boldsymbol{s} = \boldsymbol{s}' G_{(N,N)}$ for some $\boldsymbol{s}' \in S^N$, namely $\boldsymbol{s}' G_{(N,N)}^{-1}$.

A (real) *binary lattice* Λ is defined as a set of integer N-tuples that forms a group under ordinary vector addition, and that has $2^m \boldsymbol{Z}^N$ as a sublattice for some m, where $\boldsymbol{Z}^N$ is the set of all integer N-tuples. The *2-depth* of a binary lattice is the least m for which $2^m \boldsymbol{Z}^N$ is a sublattice; a binary lattice with 2-depth 1 or 2 is called a *mod-2*

or *mod-4 lattice*, respectively (see [1]). We use squared Euclidean distance as a distance metric for lattices (although it is not a metric in a strict sense).

The cosets of Λ modulo $2^m\boldsymbol{Z}^N$ may be represented by N-tuples of integers modulo 2^m, and coset representatives may be added modulo 2^m. If Λ is a mod-2 lattice, there is thus an isomorphism between its cosets modulo $2\boldsymbol{Z}^N$ and the codewords of some binary (N, K) code C (see [1, lemma 3]). The (Euclidean) weight of a coset $2\boldsymbol{Z}^N + \boldsymbol{c}$, i.e., the minimum weight of any element of this coset, is equal to the Hamming weight of the codeword $\boldsymbol{c}$.

Since $\boldsymbol{Z}^N/\Lambda/2^m\boldsymbol{Z}^N$ is a partition chain and $|\boldsymbol{Z}^N/2^m\boldsymbol{Z}^N| = 2^{mN}$, the theory of binary partitions applies. The partition $\Lambda/2^m\boldsymbol{Z}^N$ has a generator matrix G_Λ comprising K coset representatives $\boldsymbol{g}_k$ of $2^m\boldsymbol{Z}^N$ modulo 2^m such that the 2^K binary linear combinations $\boldsymbol{a}G_\Lambda \pmod{2^m}$ are a system of 2^K coset representatives $[\Lambda/2^m\boldsymbol{Z}^N]$ for the cosets of $2^m\boldsymbol{Z}^N$ in Λ. If Λ' is a binary lattice that is a sublattice of Λ, then we can choose G_Λ so that it includes a generator matrix $G_{\Lambda'}$ for $\Lambda'/2^m\boldsymbol{Z}^N$, and $G_\Lambda = G_{\Lambda'} + G_{\Lambda/\Lambda'}$, where the binary linear combinations $\boldsymbol{a}G_{\Lambda/\Lambda'}$ are a system of coset representatives for the lattice partition Λ/Λ'. If $|\Lambda/2^m\boldsymbol{Z}^N| = 2^K$, then $|\boldsymbol{Z}^N/\Lambda| = 2^{mN-K}$, and there is a generator matrix $G_{\boldsymbol{Z}^N/2^m\boldsymbol{Z}^N}$ for $\boldsymbol{Z}^N/2^m\boldsymbol{Z}^N = (\boldsymbol{Z}/2^m\boldsymbol{Z})^N$ (the N-tuples of integers $\bmod 2^m$) that is the union of a generator matrix G_Λ plus a generator matrix $G_{\boldsymbol{Z}^N/\Lambda}$ for a system of coset representatives for the cosets of Λ in $\boldsymbol{Z}^N$.

The *Gaussian integers* are the set of complex numbers $\boldsymbol{G} = \{a + bi\colon\ a, b \in \boldsymbol{Z}\}$. A *complex binary lattice* Λ is defined as a set of Gaussian integer N-tuples that forms a group under complex vector addition and that has $\phi^\mu\boldsymbol{G}^N$ as a sublattice for some μ, where $\boldsymbol{G}^N$ is the set of all Gaussian integer N-tuples, and $\phi \triangleq 1 + i$ is the prime of least norm in $\boldsymbol{G}$. The *depth* (ϕ-depth) of Λ is the least such μ. Every property stated above for real binary lattices is true for complex binary lattices, if we substitute Gaussian integers for integers and the lattice chain $\boldsymbol{G}^N/\Lambda/\phi^\mu\boldsymbol{G}^N$ for $\boldsymbol{Z}^N/\Lambda/2^m\boldsymbol{Z}^N$.

The *fundamental coding gain* γ is the principal subject of [1]. For a lattice Λ of real $2N$-tuples or complex N-tuples, the coding gain is in general defined as $\gamma(\Lambda) \triangleq d^2_{\min}(\Lambda)/V(\Lambda)^{1/N}$, where $d^2_{\min}(\Lambda)$ is the minimum squared distance between points in Λ, and $V(\Lambda)$ is the fundamental volume of Λ. All of the lattices to be considered here may be regarded as complex binary lattices and have minimum squared distance equal to $d^2_{\min} = 2^\mu$, where μ is the depth of Λ. If $|\Lambda/2^\mu\boldsymbol{G}^N| = 2^K$, then $V(\Lambda) = |\boldsymbol{G}^N/\Lambda| = 2^{\mu N-K}$. Consequently, for such lattices $\gamma(\Lambda) = 2^{K/N} = |\Lambda/2^\mu\boldsymbol{G}^N|^{1/N}$.

III. Squaring Constructions

If S is any set and S/T is a partition of S, then the squaring construction is a simple method of generating a set U of pairs of elements of S with distance at least $\min[d(T), 2d(S)]$. In the next section we show that this simple 2-construction generates many good codes and lattices, notably the Reed–Muller codes and the Barnes–Wall lattices. As in Section II, we begin by considering set partitions S/T, then go on to group partitions, and finally to partitions of codes and lattices.

A. The Squaring Construction

If S is a union of M subsets T_i, $1 \le i \le M$, then the *squaring construction* is defined as the union U of all pairs (s_1, s_2) where s_1 and s_2 are in the same subset, i.e., as the union of the M sets T_i^2, $1 \le i \le M$. We denote U by $|S/T|^2$.

Fig. 3 illustrates the squaring construction by a trellis diagram. The trellis consists of two *sections* joined at M intermediate nodes, or *states*. Each section contains M *branches*, one corresponding to each subset T_i, and representing all elements of T_i. The union of all branches in a section thus represents the total set S, and the section thus represents the M-way partition S/T. The branches in each section corresponding to the same subset T_i are joined at a common state; thus each joined pair of branches represents a Cartesian product T_i^2. The set $U = |S/T|^2$ is represented by the set of all possible paths through the trellis from the initial node to the final node, i.e., by the union of the T_i^2, $1 \le i \le M$. The essential property of the squaring construction is that it guarantees a certain minimum distance between elements of $U = |S/T|^2$, which is in part a consequence of the partition distance lemma.

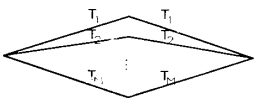


Fig. 3. Trellis diagram representing squaring construction $U = |S/T|^2$.

Lemma 1: If S/T is a partition with minimum distances $d(S)/d(T)$, then $U = |S/T|^2$ has minimum distance

$$d(U) = \min\left[d(T), 2d(S)\right].$$

Proof: a) If two distinct elements of U belong to the same set T_i^2 (correspond to the same path through the trellis), then they differ by at least $d(T)$ in one coordinate. b) If two distinct elements of U belong to different sets T_i^2 (correspond to different paths through the trellis), then they differ by at least $d(S)$ in both coordinates. c) If t_1 and t_2 are two elements in the same set T_i that differ by $d(T)$, then (t_1, t_1) and (t_2, t_1) are elements of U that differ by $d(T)$. d) If s_1 and s_2 are two elements of S that differ by $d(S)$, then (s_1, s_1) and (s_2, s_2) are elements of U that differ by $2d(S)$.

In view of Lemma 1, we shall be particularly interested in partitions S/T where $d(S)$ and $d(T)$ are in the ratio 1:2.

Suppose we arrange the branches in each section of the trellis so that they connect in any arbitrary order, i.e., let U be the union of M Cartesian product sets $T_i \otimes T_j$, where the M pairs (i, j) are ordered in any way such that both

indices run through all possible values. Another way of saying this is that there is a one-to-one map $j(i)$ from i to j. We call this a *twisted squaring construction*. Then assertions a) and b) of the proof of Lemma 1 still hold; c) holds with a minor modification; but d) need not necessarily hold. Thus the minimum distance is bounded by $d(T) \geq d(U) \geq \min[d(T), 2d(S)]$; i.e., the equality of Lemma 1 becomes a lower bound. We shall see later, in the construction of the Nordstrom–Robinson code and the analogous nonlattice packing, that twisted squaring constructions can indeed improve minimum distance.

A trellis diagram may be used as a recipe for decoding, provided that the decoding metric is a sum of independent contributions from each section of the trellis. More precisely, if the elements of a set (code) are represented by a trellis diagram with N sections, so that each codeword $\boldsymbol{c}$ is an N-tuple $(\boldsymbol{c}_1, \boldsymbol{c}_2, \cdots, \boldsymbol{c}_N)$ corresponding to some path through the trellis, and the decoder's objective is to find the codeword $\boldsymbol{c}$ that minimizes some additive distance metric $d(\boldsymbol{c}, \boldsymbol{r}) = \sum_i d(\boldsymbol{c}_i, \boldsymbol{r}_i)$, where $\boldsymbol{r} = (\boldsymbol{r}_1, \boldsymbol{r}_2, \cdots, \boldsymbol{r}_N)$ is some "received word," then a trellis diagram is a guide to an efficient search, as follows. First, for each branch in the trellis, find the element $\boldsymbol{c}_i$ in the subset $T(a)$ corresponding to that branch that minimizes $d(\boldsymbol{c}_i, \boldsymbol{r}_i)$ over $T(a)$. Thereafter, regard that branch as being labeled by the minimizing $\boldsymbol{c}_i$ and having the corresponding distance as its metric, or length. Second, find the minimum length path through the trellis by some orderly search that systematically compares the lengths of all possible paths between nodes and discards all but the best.

For example, the squaring construction trellis diagram of Fig. 3 specifies the following obvious decoding method. First, for each branch in each section, find the best element of the corresponding subset T_i. Then, for each of the M intermediate nodes, sum the metrics of the two branches connecting that node to the initial and final nodes, and compare the M sums to find the shortest of the M two-branch paths. The latter step involves M additions of two numbers and an M-way comparison, equivalent to $M-1$ two-way comparisons, so that the total number of binary operations (additions or comparisons of two numbers) is $2M-1$.

The construction of U exhibits it as a union of M subsets T_i^2, and U is a subset of S^2. S^2 is the union of M^2 subsets $T_i \otimes T_j$, where the indices (i, j) run through all possible values. Clearly, we can express S^2 as the union of M subsets U_i, where each U_i has the form of a twisted squaring construction, one of which (but only one) can be a true squaring construction. Fig. 4 is a trellis diagram illustrating such an M-way partition S^2/U. Now there are M final nodes, one corresponding to each U_i. The set S^2 is the set of all elements (s_1, s_2) corresponding to all possible paths through the trellis from the initial node to any final node. Fig. 4(a) illustrates the partition S^2/U for $M=4$, and Fig. 4(b) is a schematic representation of this kind of trellis.

Decoding a partition means finding the shortest path through the trellis from the initial node to each final node,

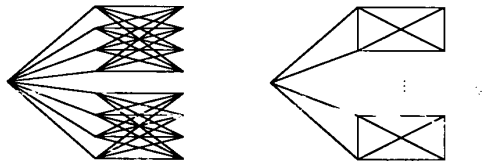
(a) (b)

Fig. 4. Trellis diagram for partition S^2/U, where $U = |S/T|^2$. (a) Illustration for case $M = |S^2/U| = |S/T| = 4$. (b) Schematic representation.

i.e., finding the least distance $d(\boldsymbol{c}, \boldsymbol{r})$ for each subset in the partition. Decoding an M-way partition is thus a set of M parallel computations. The trellis diagram for the M-way partition S^2/U suggests the following efficient decoding procedure. First, find the best element for each branch and the corresponding branch metric. Then, for each of the M final nodes, decode the corresponding squaring construction as before. The total decoding complexity after the first step is thus $M(2M-1)$ binary operations.

B. Two-Level Squaring Constructions

Now suppose that $S/T/V$ is a two-level partition chain: i.e., that there is a set of MN subsets V_{ij}, $1 \leq i \leq M$, $1 \leq j \leq N$, such that each T_i is the union of N subsets V_{ij}, and S is the union of the M sets T_i. Then, for each T_i, we can form a squaring construction W_i equal to the union of the N corresponding sets V_{ij}^2. However, W_i is a subset of T_i^2, which is a subset of $U = |S/T|^2$. In fact U is the union of the M sets T_i^2, while each T_i^2 is the union of N twisted squaring constructions of the type of W_i, so that there is an MN-way partition U/W, illustrated by the trellis diagram of Fig. 5. The trellis is the union of M subtrellises, one corresponding to each set T_i^2. Each subtrellis is an N-state trellis of the form of Fig. 4, representing a partition T_i/W_i. The set U corresponds to the union of all paths from the initial node to any of the MN final nodes, each such node representing one of the subsets of the type W_i.



(a) (b)

Fig. 5. Trellis diagram for partition U/W, where $U = |S/T|^2$, $W = |T/V|^2$. (a) Illustration for case $M = |S/T| = 2$, $N = |T/V| = 4$. (b) Schematic representation.

Comparing Fig. 5 to Fig. 1, we see that the first section is a partition trellis for the two-level partition $S/T/V$, while the nodes at the end of the second section represent the two-level partition $U/T^2/W$. Note that $|U/T^2| = |S/T| = M$, while $|T^2/W| = |T/V| = N$, so that there is the same number MN of nodes at the end of each of the two sections of a two-level partition trellis.

Decoding the partition $U/T^2/W$ involves decoding MN N-way squaring constructions, so the decoding complexity is $MN(2N-1)$ binary operations. Because U/W is a set

partition, we can iterate the squaring construction to arrive at a *two-level squaring construction* $|U/W|^2$. Alternatively, we denote a two-level squaring construction in terms of the original chain $S/T/V$ as the *4-construction*

$$|S/T/V|^4 \triangleq \|S/T|^2/|T/V|^2|^2.$$

In view of Lemma 1,

$$\begin{aligned} d(|S/T/V|^4) &= \min[d(W), 2d(U)] \\ &= \min[d(V), 2d(T), 4d(S)]. \end{aligned}$$

Thus we will be particularly interested in two-level partitions $S/T/V$ with distances $d(S)/d(T)/d(V)$ in the ratio $1:2:4$.

A trellis diagram for a two-level squaring construction $|S/T/V|^4$ is obtained by joining two trellises of the type of Fig. 5 back-to-back, as shown in Fig. 6. Every branch in this trellis represents a subset V_{ij}. The decoding complexity of such a trellis, given branch metrics, is $2MN(2N-1)$ to decode the partitions represented by the two halves of the trellis, plus MN additions and $MN-1$ binary comparisons to sum the left and right metrics to each of the MN center nodes, and finally to select the largest. The total decoding complexity is thus $4MN^2-1$ binary operations, given branch metrics.

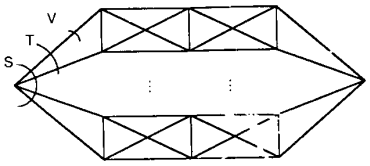


Fig. 6. Schematic trellis diagram for two-level squaring construction $|S/T/V|^4$.

Wei [3] and Ungerboeck [4] use the *branch complexity* of a trellis as a measure of decoding complexity, where the branch complexity is the number of branches per section. For the trellises of Fig. 5 and 6, the branch complexity is MN^2 in the most complicated section. Note that in all cases so far, our decoding complexity per section is closely approximated by the branch complexity.

C. Iterated Squaring Constructions

The squaring construction can be iterated indefinitely to produce 8-constructions $|S/T/V/W|^8$, 16-constructions, and so forth. The corresponding trellis diagrams become not only more complicated but also less regular, in that they do not have the same number of states at each boundary. Nonetheless, the decoding methods for the one- and two-level squaring constructions do generalize.

Let $S_0/S_1/\cdots/S_m$ be an m-level partition chain. We may apply the squaring construction to each partition of the chain to generate m sets $S_{1j} \triangleq |S_j/S_{j+1}|^2$, $0 \le j \le m-1$, which in turn form a partition chain $S_{10}/S_{11}/\cdots/S_{1,m-1}$, because each S_{1j} is a subset of S_j^2 and has S_{j+1}^2 as a subset. We may iterate up to m times, finally arriving at a 2^m-construction defined inductively by

$$\begin{aligned} &|S_0/S_1/\cdots/S_m|^N \\ &\quad \triangleq \|S_0/S_1/\cdots/S_{m-1}|^{N/2}/|S_1/S_2/\cdots/S_m|^{N/2}|^2 \end{aligned}$$

where $N=2^m$. By iteration of Lemma 1, we find that

$$\begin{aligned} &d\left(|S_0/S_1/\cdots/S_m|^N\right) \\ &\quad = \min\left[d(S_m), 2d(S_{m-1}), \cdots, 2^m d(S_0)\right]. \end{aligned}$$

A schematic trellis diagram for the partition $S_{10}/S_{11}/\cdots/S_{1,m-1}$ is shown in Fig. 7. The first section represents the m-level partition $S_0/S_1/\cdots/S_m$, with every branch representing one subset $S_m(\boldsymbol{a})$ in this partition. The nodes at the end of the second section represent the subsets $S_{1,m-1}(\boldsymbol{a}') = |S_{m-1}(\boldsymbol{a}')/S_m|^2$ in the partition $S_{10}/S_{11}/\cdots/S_{1,m-1}$. The total number of such nodes is equal to

$$\begin{aligned} &|S_{10}/S_{11}/\cdots/S_{1,m-1}| \\ &\quad = |S_0/S_1/\cdots/S_m|^2/(|S_0/S_{11}||S_{m-1}/S_m|). \end{aligned}$$

For each such node, there are $|S_{m-1}/S_m|$ merging branches, all originating from a common cluster of $|S_{m-1}/S_m|$ nodes at the end of the first section. The total number of branches in the second section (the branch complexity) is thus equal to

$$\begin{aligned} &|S_{m-1}/S_m||S_{10}/S_{11}/\cdots/S_{1,m-1}| \\ &\quad = |S_0/S_1/\cdots/S_m|^2/|S_0/S_1|. \end{aligned}$$

The diagram shows that the union of all $|S_{m-1}/S_m|$ nodes $S_{1,m-1}(\boldsymbol{a}')$ in a cluster at the end of the second section represents a set $S_{m-1}(\boldsymbol{a}')^2$, while the whole trellis, representing $S_{10} = |S_0/S_1|^2$, is the union of $|S_0/S_1|$ subtrellises, each representing a set $S_1(a)^2$.

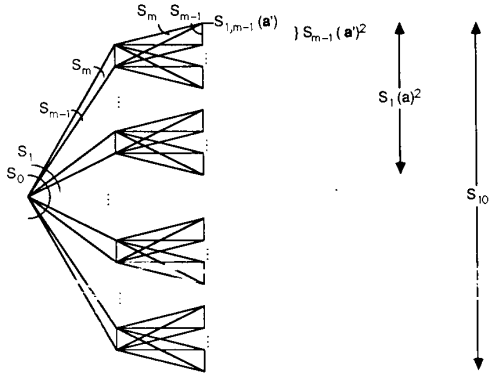


Fig. 7. Schematic two-section trellis diagram for partition $S_{10}/S_{11}/\cdots/S_{1,m-1} = |S_0/S_1|^2/\cdots/|S_{m-1}/S_m|^2$.

The decoding of an iterated squaring construction proceeds in stages. Given the best element for each subset and the corresponding subset metric in the partition $S_0/S_1/\cdots/S_m$, for each of the two sections illustrated in Fig. 7, we may determine the best element for each subset and the corresponding subset metric in the partition $S_{10}/S_{11}/\cdots/S_{1,m-1}$ by decoding $|S_{10}/S_{1,m-1}|$ (twisted) squaring constructions, each involving $|S_{m-1}/S_m|$ addi-

tions and $|S_{m-1}/S_m|-1$ binary comparisons, for a total of $(2|S_{m-1}/S_m|-1)|S_{10}/S_{1,m-1}|$ binary operations, or approximately twice the branch complexity. This operation is repeated m times to decode the whole 2^m-construction. Thus the strategy is to decode first 1-tuples, then 2-tuples, then 4-tuples, and so forth until we arrive at a final decoded 2^m-tuple. This strategy resembles that of other "fast" algorithms, such as the fast Fourier transform on 2^m points.

D. The Squaring Construction for Groups

Now let S be a group, T a subgroup, and S/T the group partition induced by T. Since each subset of S in this partition is a coset $T+\boldsymbol{c}$ for some coset representative $\boldsymbol{c}\in[S/T]$, the squaring construction for groups may be defined as the union U of all pairs $(\boldsymbol{t}_1+\boldsymbol{c}, \boldsymbol{t}_2+\boldsymbol{c})$, where $\boldsymbol{t}_1, \boldsymbol{t}_2 \in T$ and $\boldsymbol{c}\in[S/T]$. Thus U is the union of $|S/T|$ cosets of T^2, namely $T^2+(\boldsymbol{c},\boldsymbol{c})$ for $\boldsymbol{c}\in[S/T]$.

Since S/T remains a set partition, all of the properties of the squaring construction applied to set partitions continue to hold, in particular the expression for $d(U)$ of Lemma 1, as well as the trellis and associated decoding method. The chain $S^2/U/T^2$ is thus a set partition chain. However, S^2 and T^2 are groups, and it is easy to see that $U=|S/T|^2$ is also a group, because an element of $T^2+(\boldsymbol{c},\boldsymbol{c})$ plus an element of $T^2+(\boldsymbol{c}',\boldsymbol{c}')$ is an element of $T^2+(\boldsymbol{c}+\boldsymbol{c}', \boldsymbol{c}+\boldsymbol{c}')$. Thus $S^2/U/T^2$ is in fact a group partition chain.

The elements $(\boldsymbol{c},\boldsymbol{c})\in[S/T]^2$ form a natural set of $|S/T|$ coset representatives $[U/T^2]$ for U/T^2. As coset representatives for S^2/U, we may choose any $|S/T|$ elements of S^2 that are distinct mod U. Two natural choices are $[S^2/U]=\{(\boldsymbol{c},\boldsymbol{0})\colon\ \boldsymbol{c}\in[S/T]\}$ and $[S^2/U]=\{(\boldsymbol{0},\boldsymbol{c})\colon \boldsymbol{c}\in[S/T]\}$.

We shall find it convenient to express coset representatives of squaring constructions as Kronecker products. Define $\boldsymbol{g}_0$ as the integer 2-tuple [10], and $\boldsymbol{g}_1$ as [11]. Then the two-by-two integer matrix $G_{(2,2)} \triangleq \{\boldsymbol{g}_0, \boldsymbol{g}_1\}$ is a universal basis for any two-fold Cartesian product group, and in particular for $S^2/T^2=(S/T)^2$. We have

$$(\boldsymbol{c},\boldsymbol{0}) = \boldsymbol{g}_0\otimes\boldsymbol{c}$$

$$(\boldsymbol{c},\boldsymbol{c}) = \boldsymbol{g}_1\otimes\boldsymbol{c}$$

$$[S^2/U] = \boldsymbol{g}_0\otimes[S/T]$$

$$[U/T^2] = \boldsymbol{g}_1\otimes[S/T]$$

$$[S^2/T^2] = (\boldsymbol{g}_0+\boldsymbol{g}_1)\otimes[S/T]$$

where the sum in the last equation is the direct sum $[S^2/T^2]=[S^2/U]+[U/T^2]$. (Note that we could have equally well used $\boldsymbol{g}_0' \triangleq [01]$ in place of $\boldsymbol{g}_0$.) In the rest of the paper, we will usually write Kronecker products as ordinary products.

Now we may write the squaring construction as

$$|S/T|^2 = T^2 + \boldsymbol{g}_1[S/T]$$

and because $\boldsymbol{g}_1$ is a generator matrix $G_{(2,1)}$ for the binary (2,1) code, we may also write

$$|S/T|^2 = T^2 + G_{(2,1)}[S/T]$$

where the sum is a direct sum and the indicated products are Kronecker products in both cases.

Suppose now that S/T is a binary group partition, i.e., that the order of S/T is some power of two, say 2^K. Then, as shown in Section II, there is a generator matrix $G_{S/T}=\{\boldsymbol{g}_k,\ 0\le k\le K-1\}$, such that $[S/T]=\boldsymbol{a}G_{S/T}$, where the label $\boldsymbol{a}$ runs through all K-tuples of $\{0,1\}$-valued integers, i.e., such that the set of all binary linear combinations of the generators $\boldsymbol{g}_k$ in the matrix $G_{S/T}$ form a system of coset representatives for the partition S/T. The partitions S^2/U and U/T^2 are then also binary partitions of order 2^K, with generator matrices

$$G_{S^2/U} = \boldsymbol{g}_0\otimes G_{S/T} = \left[G_{S/T}, 0\right]$$

$$G_{U/T^2} = \boldsymbol{g}_1\otimes G_{S/T} = \left[G_{S/T}, G_{S/T}\right].$$

The (binary) dimensions of S^2/U and U/T^2 are equal to the dimension of S/T.

Let $S/T/V$ now be a two-level group partition. Because $|S/T|^2$ has T^2 as a subgroup and $|T/V|^2$ is a subgroup of T^2, $|T/V|^2$ is a subgroup of $|S/T|^2$ and $|S/T|^2/|T/V|^2$ is a group partition. A set of coset representatives $[|S/T|^2/|T/V|^2]$ is the direct sum $\boldsymbol{g}_1\otimes[S/T]+\boldsymbol{g}_0\otimes[T/V]$. The squaring construction applied to this partition yields

$$\begin{aligned}|S/T/V|^4 &\triangleq \||S/T|^2/|T/V|^2|^2\\ &= \left(|T/V|^2\right)^2 + \boldsymbol{g}_1\otimes\left(\boldsymbol{g}_1\otimes[S/T]+\boldsymbol{g}_0\otimes[T/V]\right)\\ &= V^4 + (\boldsymbol{g}_0+\boldsymbol{g}_1)\otimes\left(\boldsymbol{g}_1\otimes[T/V]\right)\\ &\quad + \boldsymbol{g}_1\otimes\left(\boldsymbol{g}_1\otimes[S/T]+\boldsymbol{g}_0\otimes[T/V]\right)\\ &= V^4 + (\boldsymbol{g}_0\boldsymbol{g}_1+\boldsymbol{g}_1\boldsymbol{g}_0+\boldsymbol{g}_1\boldsymbol{g}_1)[T/V] + \boldsymbol{g}_1\boldsymbol{g}_1[S/T].\end{aligned}$$

In the last expression we have written Kronecker products as ordinary products and used the fact that the associative law holds for Kronecker products.

The Kronecker product $\boldsymbol{g}_1\otimes\boldsymbol{g}_1$ is the integer 4-tuple [1111], while $\boldsymbol{g}_0\otimes\boldsymbol{g}_1=[1100]$, $\boldsymbol{g}_1\otimes\boldsymbol{g}_0=[1010]$. Because $\boldsymbol{g}_1\otimes\boldsymbol{g}_1$ is a generator matrix $G_{(4,1)}$ for the binary (4,1) repetition code, and $(\boldsymbol{g}_0\boldsymbol{g}_1+\boldsymbol{g}_1\boldsymbol{g}_0+\boldsymbol{g}_1\boldsymbol{g}_1)$ is a generator matrix $G_{(4,3)}$ for the binary (4,3) single-parity-check code, we may write

$$|S/T/V|^4 = V^4 + G_{(4,3)}[T/V] + G_{(4,1)}[S/T]$$

where Kronecker products are written as ordinary products.

If $S/T/V$ is a binary group partition, then S/T and T/V both have orders equal to a power of two, say 2^K and 2^{J-K}, respectively, and there are generator matrices $G_{S/T}=\{\boldsymbol{g}_k,\ 0\le k\le K-1\}$ and $G_{T/V}=\{\boldsymbol{g}_k,\ K\le k\le J-1\}$, respectively, such that $[S/T]=\boldsymbol{a}G_{S/T}$ and $[T/V]=\boldsymbol{a}'G_{T/V}$, where $\boldsymbol{a}$ and $\boldsymbol{a}'$ are $\{0,1\}$-valued integer K-tuples and $(J-K)$-tuples, respectively. Then if $U=|S/T/V|^4$, the partition U/V^4 has generator matrix

$$G_{U/V^4} = G_{(4,3)}G_{T/V} + G_{(4,1)}G_{S/T}$$

which can be written out as

$$G_{U/V^4} = \begin{bmatrix} G_{T/V} & G_{T/V} & 0 & 0 \\ G_{T/V} & 0 & G_{T/V} & 0 \\ G_{T/V} & G_{T/V} & G_{T/V} & G_{T/V} \\ G_{S/T} & G_{S/T} & G_{S/T} & G_{S/T} \end{bmatrix}.$$

The dimension of the partition $|S/T/V|^4/V^4$ is thus $3\dim[T/V]+\dim[S/T]$.

In summary, when we use squaring constructions or iterated squaring constructions with group partitions, we obtain groups comprising 2^m-tuples of elements of the original groups. Partitions involving 2^m-tuples can be expressed as direct sums of the products of integer $\{0,1\}$-valued 2^m-tuples with coset representatives of the original partitions, these integer 2^m-tuples being m-fold Kronecker products of the 2-tuples $\boldsymbol{g}_0$ and $\boldsymbol{g}_1$. When the group partitions are binary group partitions, then partitions involving 2^m-tuples are also binary group partitions and have generator matrices which are Kronecker products of integer $\{0,1\}$-valued 2^m-tuples with the generator matrices of the original partitions.

Note: When S/T is a group partition, an alternative form of the squaring construction is

$$U = \{(s, s+t): s \in S,\ t \in T\}$$

because the first element of $U = |S/T|^2$ can be any element of S, while the second must then be from the same coset $T+s$ of T. This is the $|u|u+v|$ construction of MacWilliams and Sloane [5, ch. 2, section 9]. The squaring construction can be defined whenever S/T is a partition, whether or not S and T are groups, and thus is fundamentally a geometric construction. The $|u|u+v|$ construction can be defined whenever the elements of S and T can be added, whether or not T is a subset of S, and thus is fundamentally an algebraic construction. The distance formula of Lemma 1, the trellis diagram, and the associated decoding method all depend on T being a subset of S, rather than on group structure, and we therefore feel that the squaring construction better expresses the basic construction principle. However, when S/T is a group partition, the results of the two constructions are identical.

E. The Squaring Construction for Group Partition Chains

Now let $S_0/S_1/\cdots/S_m$ be a group partition chain. From the previous section, $S_{10}/S_{11}/\cdots/S_{1,m-1}$ is also a group partition chain, where $S_{1j} \triangleq |S_j/S_{j+1}|^2$, $0 \le j \le m-1$; thus the squaring construction can be iterated on the new chain. Iterating m times, we arrive at an m-level iterated squaring construction of 2^m-tuples denoted by $|S_0/S_1/\cdots/S_m|^N$, where $N = 2^m$.

Let us define S_{nj}, $0 \le n \le m$, $0 \le j \le m-n$, as the jth group in the chain after n iterations. Thus $S_{0j} = S_j$, $0 \le j \le m$, and $S_{m0} = |S_0/S_1/\cdots/S_m|^N$. S_{nj} is a group of 2^n-tuples of elements of S. By iteration of Lemma 1,

$$d(S_{nj}) = \min\left[d(S_{j+n}), 2d(S_{j+n-1}), \cdots, 2^n d(S_j)\right].$$

From the previous section, a set of coset representatives for $S_{nj}/S_{n,j+1}$, $0 \le j \le m-n-1$, is

$$\left[S_{nj}/S_{n,j+1}\right] = \boldsymbol{g}_1 \otimes \left[S_{n-1,j}/S_{n-1,j+1}\right] + \boldsymbol{g}_0 \otimes \left[S_{n-1,j+1}/S_{n-1,j+2}\right]$$

where the indicated sum is again a direct sum.

When the group partition chain is a binary partition chain, it is convenient to deal with generator matrices. Let G_{nj}, $0 \le n \le m-1$, $0 \le j \le m-n-1$, be a generator matrix for the set of coset representatives given by the above formula, with $G_{0j} = G_j$ a generator matrix for $S_{0j}/S_{0,j+1}$, $0 \le j \le m-1$. Then we have the recursion

$$G_{nj} = \boldsymbol{g}_1 G_{n-1,j} + \boldsymbol{g}_0 G_{n-1,j+1}, \qquad 0 \le j \le m-n-1,$$

again writing Kronecker products as ordinary products.

The above recursions have the form of convolutions of a sequence $G_{n-1,j}$ or $[S_{n-1,j}/S_{n-1,j+1}]$, $0 \le j \le m-n-1$, with the sequence $(\boldsymbol{g}_0, \boldsymbol{g}_1)$, except for end effects. To avoid end effects, let us extend the original chain $S_0/S_1/\cdots/S_m$ with dummy partitions $S_0/S_0/\cdots/S_0$ and $S_m/S_m/\cdots/S_m$ at each end. The generator matrix for the coset representatives of a dummy partition is the empty set $\{\varnothing\}$, which serves as the zero element 0 in the addition of generator matrices, and the corresponding set of coset representatives is the trivial set $\{\boldsymbol{0}\}$. Thus in the extended chain, $G_{0j} = \{\varnothing\} = 0$, or $[S_j/S_{j+1}] = \{\boldsymbol{0}\}$, for $j < 0$ or $j \ge m$. Then the above recursion is true for all j.

Fig. 8 illustrates these definitions with a tableau of partition chains. The original chain $S_0/S_1/\cdots/S_m = S_{00}/S_{01}/\cdots/S_{0m}$ is extended in both directions by dummy partitions. The links of the chain are labeled with the coset representative generator matrices G_{0j}, where $G_{0j} = 0$ for $j < 0$ or $j \ge m$. The squaring construction then produces a second chain $S_{10}/S_{11}/\cdots/S_{1,m-1}$, extended at the top by dummy partitions $S_0^2 = |S_0/S_0|^2$, and at the bottom by dummy partitions $S_m^2 = |S_m/S_m|^2$. Note that S_0^2/S_{10} is not a dummy partition and has coset representatives generated

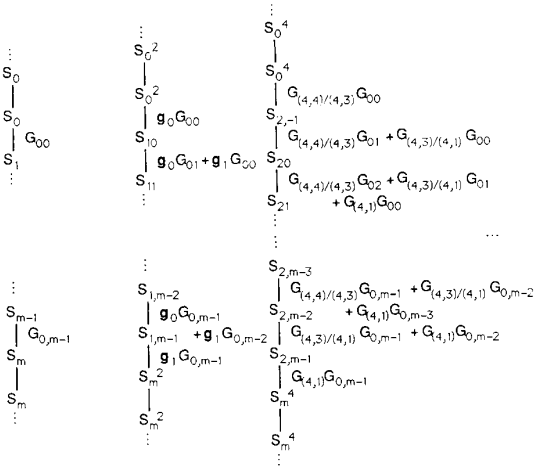


Fig. 8. Tableau of iterated squaring constructions for partition chains. $G_{(4,4)/(4,3)} = \{\boldsymbol{g}_0\boldsymbol{g}_0\}$; $G_{(4,3)/(4,1)} = \{\boldsymbol{g}_0\boldsymbol{g}_1, \boldsymbol{g}_1\boldsymbol{g}_0\}$; $G_{(4,1)} = \{\boldsymbol{g}_1\boldsymbol{g}_1\}$.

by $G_{1,-1} = \boldsymbol{g}_0 G_{00}$; neither is $S_{1,m-1}/S_m^2$, with generator matrix $G_{1,m-1} = \boldsymbol{g}_1 G_{0,m-1}$. Thus the nontrivial part of the tableau expands, rather than contracts, with increasing n. Nonetheless, after m iterations, the center element S_{m0} in the chain is the m-level iterated squaring construction $|S_0/S_1/\cdots/S_m|^N$, $N = 2^m$.

Generating functions are a convenient way of dealing with convolutions. Let us define formal power series in the indeterminate x as follows:

$$G_n(x) \triangleq \sum_j G_{nj} x^j$$

$$\boldsymbol{g}(x) \triangleq \boldsymbol{g}_1 + \boldsymbol{g}_0 x^{-1}.$$

(We could replace G_{nj} by $[S_{nj}/S_{n,j+1}]$ if we preferred to use systems of coset representatives rather than generator matrices.) Then the recursion is expressed as the generating function product

$$G_n(x) = \boldsymbol{g}(x) G_{n-1}(x)$$

where sums are direct sums and products are Kronecker products. Because the associative law applies to Kronecker products, we may iterate to obtain

$$G_n(x) = [\boldsymbol{g}(x)]^n G_0(x)$$

where the coefficients of $[\boldsymbol{g}(x)]^n$ are 2^n-tuples of $\{0,1\}$-valued integers which are n-fold Kronecker products of $\boldsymbol{g}_0$ and $\boldsymbol{g}_1$. If we define $G_{\partial \mathrm{RM}}(n,x) \triangleq [\boldsymbol{g}(x)]^n$, then

$$G_n(x) = G_{\partial \mathrm{RM}}(n,x) G_0(x).$$

Thus

$$G_{nj} = \sum_{0 \le r \le n} G_{\partial \mathrm{RM}}(r,n) G_{0,j+r}$$

where $G_{\partial \mathrm{RM}}(r,n)$ is the coefficient of x^{-r} in the polynomial $G_{\partial \mathrm{RM}}(n,x)$.

Because of the generality of this formula, it behooves us to examine the generating function $G_{\partial \mathrm{RM}}(n,x)$ more closely. It is a polynomial in x^{-1} with $n+1$ nonzero terms. The coefficient $G_{\partial \mathrm{RM}}(r,n)$ of x^{-r} in this polynomial is the set of all n-fold Kronecker products of $\boldsymbol{g}_0$ and $\boldsymbol{g}_1$ that comprise $\boldsymbol{g}_0$ r times and $\boldsymbol{g}_1$ $n-r$ times, in any order. The number of such products is the combinatorial coefficient $C_{nr} \triangleq (n!)/[(r!)(n-r)!)]$. If $\boldsymbol{v}$ is any vector, then the Hamming weight of the Kronecker product $\boldsymbol{g}_0 \otimes \boldsymbol{v}$ is the Hamming weight of $\boldsymbol{v}$, and that of $\boldsymbol{g}_1 \otimes \boldsymbol{v}$ is twice the Hamming weight of $\boldsymbol{v}$; thus, by induction, every such product has Hamming weight 2^{n-r}.

Another way of expressing these facts is to consider the n-fold Kronecker product $G_{(N,N)} \triangleq G_{(2,2)}^n$ of the two-by-two matrix $G_{(2,2)} = \{\boldsymbol{g}_0, \boldsymbol{g}_1\}$ with itself. $G_{(2,2)}, G_{(4,4)} = G_{(2,2)}^2$, and $G_{(8,8)} = G_{(2,2)}^3$ look like this:

$$G_{(2,2)} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \qquad G_{(4,4)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$G_{(8,8)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

The rows of $G_{(N,N)}$ are all 2^n n-fold Kronecker products of $\boldsymbol{g}_0$ and $\boldsymbol{g}_1$. A row corresponding to a product that includes $\boldsymbol{g}_0$ r times and $\boldsymbol{g}_1$ $n-r$ times has Hamming weight 2^{n-r}. The set of all such rows is the coefficient of x^{-r} in $G_{\partial \mathrm{RM}}(n,x)$, i.e., $G_{\partial \mathrm{RM}}(r,n)$. Any such matrix $G_{(N,N)}$ is a universal basis for N-space.

The Reed–Muller code $\mathrm{RM}(r,n)$ is a binary code of length 2^n which may be defined as the code generated by the generator matrix $G_{\mathrm{RM}}(r,n)$ that consists of all rows of $G_{(N,N)}$ of weight 2^{n-r} or greater. (In the next section, we will define it as the product of an iterated squaring construction; then we will show that such a construction leads to this generator matrix.) Then $G_{\partial \mathrm{RM}}(r,n)$, the matrix of the C_{nr} rows of weight exactly 2^{n-r}, can be identified as the generator matrix of the partition $\mathrm{RM}(r,n)/\mathrm{RM}(r-1,n)$. Thus $G_{\mathrm{RM}}(r,n) = \sum_{r' \ge r} G_{\partial \mathrm{RM}}(r',n)$. For example, the Reed–Muller codes of length 8 are $\mathrm{RM}(3,3) = (8,8)$, $\mathrm{RM}(2,3) = (8,7)$, $\mathrm{RM}(1,3) = (8,4)$, $\mathrm{RM}(0,3) = (8,1)$, and $\mathrm{RM}(-1,3) = (8,0)$; correspondingly, $G_{\partial \mathrm{RM}}(3,3)$ is the single row $G_{(8,8)/(8,7)}$ of weight 1 that generates $(8,8)/(8,7)$, $G_{\partial \mathrm{RM}}(2,3)$ is the set of three rows $G_{(8,7)/(8,4)}$ of weight 2 that generate $(8,7)/(8,4)$, and so forth.

The group S_{nj} is the direct sum $S_{nj} = S_n^N + \sum_{k \ge j} G_{nk}$, where $N = 2^n$, as can easily be seen from Fig. 8. Thus a generator matrix for S_{nj}/S_n^N can be obtained by summing the coefficients of x^k for $k \ge j$ in $G_n(x)$. Therefore, if we define the generating functions

$$S_n(x) \triangleq \sum_j S_{nj} x^j$$

$$u(x^{-1}) \triangleq 1 + x^{-1} + x^{-2} + \cdots,$$

then

$$S_n(x) = u(x^{-1}) G_n(x) = u(x^{-1}) G_{\partial \mathrm{RM}}(n,x) G_0(x).$$

There are two ways of expressing the S_{nj} in terms of the original partition chain, depending on how we group terms in the above expression. (We have this freedom since $u(x^{-1})$ commutes with $G_{\partial \mathrm{RM}}(n,x)$.) On the one hand, we have

$$S_n(x) = G_{\partial \mathrm{RM}}(n,x)[u(x^{-1}) G_0(x)]$$

$$= G_{\partial \mathrm{RM}}(n,x) S_0(x).$$

Thus

$$S_{nj} = \sum_{0 \le r \le n} G_{\partial \mathrm{RM}}(r,n) S_{0,j+r}$$

where $G_{\partial \mathrm{RM}}(r,n)$ is again the set of all rows in $G_{(N,N)}$ of

Hamming weight 2^{n-r}. For example,

$$\begin{aligned} S_{1j} &= G_{\partial \mathrm{RM}}(0,1)S_{0j} + G_{\partial \mathrm{RM}}(1,1)S_{0,j+1} \\ &= G_{(2,1)}S_j + G_{(2,2)/(2,1)}S_{j+1} \\ &= \boldsymbol{g}_1 S_j + \boldsymbol{g}_0 S_{j+1} \\ &= \{(\boldsymbol{s}+\boldsymbol{t},\boldsymbol{s}) : \boldsymbol{s} \in S_j, \boldsymbol{t} \in S_{j+1}\}, \end{aligned}$$

the $|u|u+v|$ construction. The two-level generalization of the $|u|u+v|$ construction is, for example,

$$\begin{aligned} S_{2j} &= G_{\partial \mathrm{RM}}(0,2)S_{0j} + G_{\partial \mathrm{RM}}(1,2)S_{0,j+1} + G_{\partial \mathrm{RM}}(2,2)S_{0,j+2} \\ &= G_{(4,1)}S_j + G_{(4,3)/(4,1)}S_{j+1} + G_{(4,4)/(4,3)}S_{j+2} \\ &= \boldsymbol{g}_1\boldsymbol{g}_1 S_j + (\boldsymbol{g}_0\boldsymbol{g}_1 + \boldsymbol{g}_1\boldsymbol{g}_0)S_{j+1} + \boldsymbol{g}_0\boldsymbol{g}_0 S_{j+2} \\ &= \{(\boldsymbol{s}+\boldsymbol{t}_1+\boldsymbol{t}_2+\boldsymbol{v}, \boldsymbol{s}+\boldsymbol{t}_1, \boldsymbol{s}+\boldsymbol{t}_2, \boldsymbol{s}) : \\ &\qquad \boldsymbol{s} \in S_j, \boldsymbol{t}_1, \boldsymbol{t}_2 \in S_{j+1}, \boldsymbol{v} \in S_{j+2}\}, \end{aligned}$$

a $||u|u+v||u+u'|u+u'+v+v'||$ construction.

Alternatively, we have

$$S_n(x) = \left[u(x^{-1})G_{\partial \mathrm{RM}}(n,x)\right]G_0(x).$$

However, observe that if we define the generating function

$$G_{\mathrm{RM}}(n,x) \triangleq \sum_r G_{\mathrm{RM}}(r,n)x^{-r},$$

then

$$G_{\mathrm{RM}}(n,x) = u(x^{-1})G_{\partial \mathrm{RM}}(n,x),$$

so that

$$S_n(x) = G_{\mathrm{RM}}(n,x)G_0(x).$$

Hence

$$S_{nj} = \sum_{r \geq 0} G_{\mathrm{RM}}(r,n)G_{0,j+r}.$$

When $r \geq n$, then $G_{\mathrm{RM}}(r,n) = G_{\mathrm{RM}}(n,n) = G_{(N,N)}$, so we can simplify this by using

$$\begin{aligned} \sum_{r \geq n} G_{\mathrm{RM}}(r,n)G_{0,j+r} &= G_{(N,N)} \sum_{r \geq n} G_{0,j+r} \\ &= G_{(N,N)}S_{0,j+n} \\ &= S^N_{0,j+n} \end{aligned}$$

where $N = 2^n$, since $G_{(N,N)} \otimes R = R^N$ for any group R, $G_{(N,N)}$ being a universal basis for N-space. Thus we have

$$S_{nj} = S^N_{0,j+n} + \sum_{0 \leq r \leq n-1} G_{\mathrm{RM}}(r,n)G_{0,j+r}.$$

This yields expressions such as

$$\begin{aligned} S_{1j} &= S^2_{0,j+1} + G_{\mathrm{RM}}(0,1)G_{0j} \\ &= S^2_{j+1} + G_{(2,1)}G_j \\ &= S^2_{j+1} + \boldsymbol{g}_1\left[S_j/S_{j+1}\right], \end{aligned}$$

the squaring construction, and

$$\begin{aligned} S_{2j} &= S^4_{0,j+2} + G_{\mathrm{RM}}(1,2)G_{0,j+1} + G_{\mathrm{RM}}(0,2)G_{0j} \\ &= S^4_{j+2} + G_{(4,3)}G_{j+1} + G_{(4,1)}G_j \\ &= S^4_{j+2} + (\boldsymbol{g}_1\boldsymbol{g}_1 + \boldsymbol{g}_0\boldsymbol{g}_1 + \boldsymbol{g}_1\boldsymbol{g}_0)\left[S_{j+1}/S_{j+2}\right] \\ &\quad + \boldsymbol{g}_1\boldsymbol{g}_1\left[S_j/S_{j+1}\right], \end{aligned}$$

the two-level squaring construction, such as were introduced in the previous section.

We summarize these results in the following lemma.

Lemma 2: Let $S_0/S_1/\cdots/S_m$ be an m-level group partition chain. Let S_{nj} be the n-fold iterated squaring construction $|S_j/S_{j+1}/\cdots/S_{j+n}|^N$, $N = 2^n$, $0 \leq j \leq m-n$. Then

$$S_{nj} = \sum_{0 \leq r \leq n} G_{\partial \mathrm{RM}}(r,n) \otimes S_{j+r};$$

also,

$$S_{nj} = S^N_{j+n} + \sum_{0 \leq r \leq n-1} G_{\mathrm{RM}}(r,n) \otimes \left[S_{j+r}/S_{j+r+1}\right],$$

where the sums are direct sums, $G_{\partial \mathrm{RM}}(r,n)$ is the set of all rows in $G_{(N,N)}$ of Hamming weight equal to 2^{n-r}, and $G_{\mathrm{RM}}(r,n)$ is the set of all rows in $G_{(N,N)}$ of Hamming weight greater than or equal to 2^{n-r}. Furthermore, if G_j is a generator matrix for S_j/S_{j+1}, $0 \leq j \leq m-1$, then

$$G_{nj} = \sum_{0 \leq r \leq n} G_{\partial \mathrm{RM}}(r,n) \otimes G_{j+r}$$

is a generator matrix for $S_{nj}/S_{n,j+1}$, $0 \leq j \leq m-n-1$, where the sum indicates a union of generator matrices. Finally, the minimum distance of the iterated construction is

$$\begin{aligned} &d\left(|S_j/S_{j+1}/\cdots/S_{j+n}|^N\right) \\ &\qquad = \min\left[d(S_{j+n}), 2d(S_{j+n-1}), \cdots, 2^n d(S_j)\right]. \end{aligned}$$

F. Duality

The sets generated by the squaring construction often have nice duality properties. Although these properties are not needed for our other results, it would be a shame not to mention them, at least briefly.

Let the set S consist of elements $\boldsymbol{s}$ from some space A such that the *inner product* $(\boldsymbol{s},\boldsymbol{s}')$ of elements of S with elements $\boldsymbol{s}'$ of some space B is defined. Here A and B will both be R^N, where R is some ring, and the inner product will be the sum of the products of the coordinates, an element of R.

Two elements of R^N are said to be *orthogonal* if their inner product is zero. They are *orthogonal mod r* if their inner product is congruent to zero mod r for some $r \in R$, where R is a principal ideal domain.

The *dual* $S^\perp$ to a set S is the set of all elements of R^N that are orthogonal (possibly mod r) to all elements of S.

Let T be a subset of S. Then $S^\perp$ is a subset of $T^\perp$. If S/T is a partition chain, $T^\perp/S^\perp$ is the dual partition chain. In general, the order $|T^\perp/S^\perp|$ is equal to $|S/T|$. If $S_0/S_1/\cdots/S_m$ is a partition chain, then $S_m^\perp/S_{m-1}^\perp/\cdots/S_0^\perp$ is the dual partition chain. If $S_0/S_1/\cdots/S_m$ is a chain of two-way partitions, with $\boldsymbol{g}_j$ the generator of S_j/S_{j+1}, then $S_m^\perp/S_{m-1}^\perp/\cdots/S_0^\perp$ is a chain of two-way partitions, and the generator $\boldsymbol{g}_k^\perp$ of $S_{k+1}^\perp/S_k^\perp$ is orthogonal to all elements of S_{k+1}, so $(\boldsymbol{g}_j, \boldsymbol{g}_k^\perp) = 0$ for $k < j$. (It is usually possible and desirable

to choose the generators $\boldsymbol{g}_k^{\perp}$ so that $(\boldsymbol{g}_j, \boldsymbol{g}_k^{\perp}) = 0$ for $k \neq j$.)

If S/T is a group partition and $U = |S/T|^2$, then $U^{\perp} = |\underline{T^{\perp}/S^{\perp}}|^2$, where the *dual squaring construction* is defined as

$$|\underline{S/T}|^2 \triangleq \{(\boldsymbol{t}_1 + \boldsymbol{c}, \boldsymbol{t}_2 - \boldsymbol{c}) : \boldsymbol{t}_1, \boldsymbol{t}_2 \in T, \boldsymbol{c} \in [S/T]\};$$

that is, $|\underline{S/T}|^2$ is the union of the cosets $T^2 + (\boldsymbol{c}, -\boldsymbol{c})$, $\boldsymbol{c} \in [S/T]$. Thus $|\underline{S/T}|^2$ is the very mildly twisted squaring construction in which the second coset representative is the additive inverse of the first (mod T). Alternatively, it is the squaring construction followed by a sign inversion of the second coordinate, if $T = -T$. Thus the distance expression $d(|\underline{S/T}|^2) = \min[d(T), 2d(S)]$ of Lemma 1 holds for the dual squaring construction.

The duality of $U^{\perp}$ follows because the inner product of an element $(\boldsymbol{t}_1 + \boldsymbol{c}, \boldsymbol{t}_2 + \boldsymbol{c})$ of $|S/T|^2$ with an element $(\boldsymbol{s}_1^{\perp} + \boldsymbol{c}^{\perp}, \boldsymbol{s}_2^{\perp} + \boldsymbol{c}^{\perp})$ of $|\underline{T^{\perp}/S^{\perp}}|^2$ is equal to the inner product of the coset representatives $(\boldsymbol{c}, \boldsymbol{c})$ and $(\boldsymbol{c}^{\perp}, -\boldsymbol{c}^{\perp})$, which is zero; and the orders of the partitions in the chains $S^2/|S/T|^2/T^2$ and $(T^{\perp})^2/|\underline{T^{\perp}/S^{\perp}}|^2/(S^{\perp})^2$ are both equal to $|S/T| = |T^{\perp}/S^{\perp}|$. These chains are thus dual partition chains.

The dual squaring construction $|\underline{S/T}|^2$ is actually equal Bto the squaring construction $|S/T|^2$ if and only if every element $\boldsymbol{c}$ of S/T has order 2, i.e., $2\boldsymbol{c} = \boldsymbol{c} + \boldsymbol{c} \equiv \boldsymbol{0}$ (mod T), for then and only then will the coset $T - \boldsymbol{c}$ equal $T + \boldsymbol{c}$ for all $\boldsymbol{c} \in [S/T]$. In this case we say that the squaring construction is *self-dual*. If $S_0/S_1/\cdots/S_m$ is a *self-dual partition chain*, i.e., if $S_j = S_{m-j}^{\perp}$, $0 \leq j \leq m$, and the squaring construction is self-dual for all partitions in this chain, then the result of applying the squaring construction to each partition in this chain is another self-dual partition chain.

IV. Binary Codes and Lattices of Length 2^n

It will not be a surprise at this point to note that the Reed–Muller codes themselves can be constructed by iterated squaring constructions, starting with the simple two-way exhaustive partition of the binary field. The general properties of the squaring construction lead immediately to the determination of the minimum distances of these codes, their duality properties, dimensions, generator matrices, trellis diagrams, and so forth, and give many interrelationships between them. The development shows that generalized Reed–Muller codes, with the same parameters as the binary Reed–Muller codes, can be defined over any group.

We shall also show that a notable sequence of dense lattices of lengths $N = 2^n$ can be constructed by iterated squaring constructions, starting with the simple two-way partition of the integers into even and odd. These are the sequence of Barnes–Wall lattices, which begin with the important lattices $\boldsymbol{Z}^2 \simeq \boldsymbol{G}$, D_4, and E_8, and their principal sublattices. We will see that the most natural starting point for this sequence is in two dimensions, where we have an infinite partition chain of two-way partitions with minimum squared distances $1/2/4/\cdots$. The general properties of the squaring construction lead immediately to the determination of the minimum distances of these lattices, their duality properties, dimensions, generator matrices, trellis diagrams, and so forth, and give many interrelationships between them, as well as with Reed–Muller codes.

A. Reed–Muller Codes

Consider the binary field $\mathrm{GF}(2) = \{\boldsymbol{0}, \boldsymbol{1}\}$, which may also be considered to be the (1,1) binary code. The trivial (1,0) binary code has one codeword $\boldsymbol{0}$, and the exhaustive partition of the field is the two-way partition $(1,1)/(1,0)$. The generator matrix for the (1,1) code, or for the coset representatives $[(1,1)/(1,0)]$ is the one-by-one integer matrix $G_{(1,1)}$ whose single generator is the 1-tuple 1.

Applying the squaring construction to the partition $(1,1)/(1,0)$, we arrive at a binary block code U of length 2 whose words are $(\boldsymbol{c}, \boldsymbol{c})$, where $\boldsymbol{c} \in \mathrm{GF}(2) = \{\boldsymbol{0}, \boldsymbol{1}\}$. Thus U is a (2,1) code (which may be regarded as either a repetition or parity-check code). From the general properties of the squaring construction, the (2,1) code is a union of two cosets of $(1,0)^2 = (2,0)$, is a subcode of $(1,1)^2 = (2,2)$, has minimum distance $d_H = 2$, has a generator matrix $G_{(2,1)}$ with the single generator $\boldsymbol{g}_1 = [11]$, and has a trivial two-section two-state trellis diagram.

A generator matrix $G_{(2,2)}$ for the (2,2) code that reflects the squaring construction and exhibits the coset decomposition $(2,2) = [(2,2)/(2,1)] + (2,1)$ is the matrix $G_{(2,2)} = G_{(2,2)/(2,1)} + G_{(2,1)} = \{\boldsymbol{g}_0, \boldsymbol{g}_1\} = \{[10], [11]\}$, where $G_{(2,2)/(2,1)} = \{\boldsymbol{g}_0\}$ is the generator matrix of a system of coset representatives $[(2,2)/(2,1)]$.

The (2,1) code is self-dual, and the (2,2) and (2,0) codes are each others' duals, so $(2,2)/(2,1)/(2,0)$ is a self-dual partition chain.

Applying the squaring construction to the two partitions $(2,2)/(2,1)$ and $(2,1)/(2,0)$, we arrive at two binary block codes of length 4, which may be seen to be the (4,3) parity-check code and the (4,1) repetition code. From the general properties of the squaring construction, there is a partition chain $(4,4)/(4,3)/(4,2)/(4,1)/(4,0)$ with distances $1/2/2/4/\infty$. A generator matrix for the (4,3) code is the set of three integer 4-tuples $G_{(4,3)} = \{\boldsymbol{g}_1\boldsymbol{g}_1 = [1111], \boldsymbol{g}_1\boldsymbol{g}_0 = [1010], \boldsymbol{g}_0\boldsymbol{g}_1 = [1100]\}$, corresponding to the rows of weights 4 and 2 in $G_{(2,2)}^2$, and $\boldsymbol{g}_1\boldsymbol{g}_1 = [1111]$ alone generates the (4,1) code. Both codes have two-section two-state trellis diagrams. Alternatively, we have the two-level constructions $(4,3) = |(1,1)/(1,1)/(1,0)|^4$ and $(4,1) = |(1,1)/(1,0)/(1,0)|^4$, leading to four-section two-state trellis diagrams. These two codes are duals of each other.

By continuing to iterate the squaring construction in this way, we can generate all Reed–Muller codes. The rth-order Reed–Muller code of length $N = 2^n$ is conventionally denoted by $\mathrm{RM}(r, n)$. We define an initial partition chain with $\mathrm{RM}(0,0)$ as the (1,1) code, and $\mathrm{RM}(-1,0)$ as the (1,0) code, and extend the chain with dummy partitions in both directions by defining $\mathrm{RM}(r,0)$ as the (1,1) code for

$r \geq 0$, and as the (1,0) code for $r < 0$. We then define $\mathrm{RM}(r,n)$ as the code obtained by the squaring construction

$$\mathrm{RM}(r,n) \triangleq |\mathrm{RM}(r,n-1)/\mathrm{RM}(r-1,n-1)|^2.$$

By the general properties of iterated squaring constructions, this definition produces a chain of nested codes of length $N = 2^n$ from the chain of codes of length $N/2$. By induction, $\mathrm{RM}(r,n)$ is the single-element $(N,0)$ code for $r < 0$, and $\mathrm{RM}(r,n)$ is the (N,N) code $[\mathrm{GF}(2)]^N$ of all binary N-tuples for $r \geq n$. By Lemma 1 and induction, the minimum Hamming distance of $\mathrm{RM}(r,n)$ is 2^{n-r} for $0 \leq r$.

If we define $M(r,n)$ as the dimension of $[\mathrm{RM}(r,n)/\mathrm{RM}(r-1,n)]$, then by the properties of the two-level squaring construction, $M(r,n) = M(r,n-1) + M(r-1, n-1)$, and $2^{M(r,n-1)}$ is the number of states in a two-section or four-section trellis diagram for

$$\mathrm{RM}(r,n) = |\mathrm{RM}(r,n-1)/\mathrm{RM}(r-1,n-1)|^2$$
$$= |\mathrm{RM}(r,n-2)/\mathrm{RM}(r-1,n-2)/\mathrm{RM}(r-2,n-2)|^4.$$

Solving this recursion with the initial conditions $M(r,0) = 1$ if $r = 0$ and $M(r,0) = 0$ otherwise, we obtain $M(r,n)$ equal to the combinatorial coefficient $C_{nr} \triangleq (n!)/[(r!)((n-r)!)]$, so the $M(r,n)$ array is the Pascal triangle. (The generating function for $M(r,n)$ is $M_n(x) = (1+x)^n$.) If we define $K(r,n)$ as the dimension of $\mathrm{RM}(r,n)$, or the dimension of $[\mathrm{RM}(r,n)/\mathrm{RM}(-1,n)]$, then $K(r,n)$ is the sum of $M(r',n) = C_{nr'}$ for $r' \leq r$. From the recursion for $M(r,n)$, we obtain the recursion $K(r,n) = K(r,n-1) + K(r-1,n-1)$. (The generating function for $K(r,n)$ is $K_n(x) = (1+x)^n u(x)$.)

Finally, every codeword $\boldsymbol{c}$ in a binary code has order 2, $\boldsymbol{c} + \boldsymbol{c} = \boldsymbol{0}$, so the squaring construction is self-dual for binary codes. The (1,1) and (1,0) codes are duals, so the initial partition chain is self-dual, and, by induction, all chains are self-dual; i.e., $\mathrm{RM}(r,n)^\perp = \mathrm{RM}(n-r-1,n)$. Note that the trellis diagrams for dual Reed–Muller codes have state spaces of the same size; in the Appendix we prove that this relationship holds in general for dual codes.

Fig. 9 is a tableau of the Reed–Muller codes of lengths up to $N = 32$, as generated by the squaring construction recursion defined above. The italicized codes are those corresponding to dummy partitions. The dimensions $M(r,n)$ are also shown in parentheses between $\mathrm{RM}(r,n)$ and $\mathrm{RM}(r-1,n)$, where they are nonzero; from these dimensions, we can see the numbers of states in the trellis diagrams for the partitions in the next chain.

Fig. 10 exhibits four-section trellis diagrams for Reed–Muller codes of lengths 8–32, with the associated two-level squaring construction $\mathrm{RM}(r,n) = |\mathrm{RM}(r,n-2)/\mathrm{RM}(r-1,n-2)/\mathrm{RM}(r-2,n-2)|^4$. There are surprisingly few states: only four for the (8,4) code, eight for the (16,11) and (16,5) codes, 16 for the (32,26) and (32,6) codes, and 64 for the (32,16) code. (The single-parity-check and repetition codes all have two-state trellis diagrams, as shown in [6].)

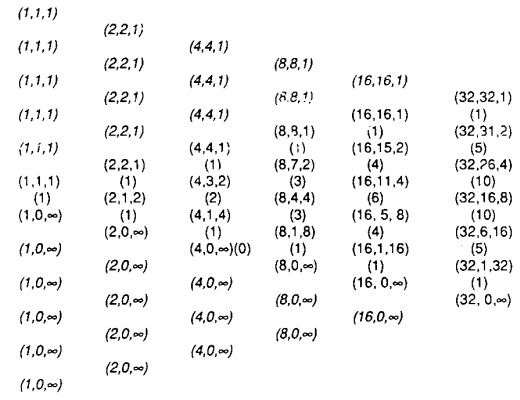


Fig. 9. Reed–Muller codes of lengths $N \leq 32$, as generated by squaring constructions.

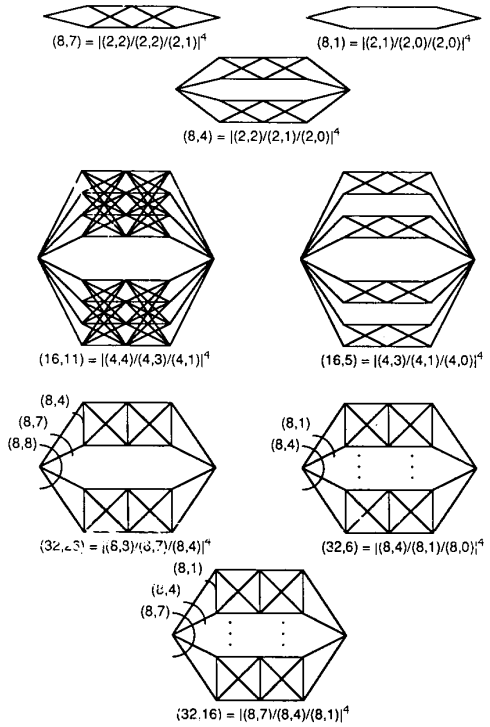


Fig. 10. Four-section trellises for Reed–Muller codes of lengths 8–32.

As we have noted, the total number of branches per section in a trellis diagram (the "branch complexity") is a more telling measure of complexity than the number of states. The number of branches in the middle sections of these four-section trellises is $2^{E(r,n)}$, where the exponent $E(r,n)$ is given by

$$E(r,n) = M(r,n-2) + 2M(r-1,n-2).$$

Using the fact that the generating function $M_n(x)$ equals $(1+x)^n$, we can determine the generating function $E_n(x)$ of $E(r,n)$ as $E_n(x) = (1+2x)(1+x)^{n-2}$. For example, $E(r,n)$ is one for repetition codes, two for single-parity-check codes, three for the (8,4) code, four and five for the

(16,5) and (16,11) codes, and five, seven, and nine for the (32,6), (32,26), and (32,16) codes, respectively.

What is the relation of this construction to the generating function formalism of Lemma 2, which involves the sets $G_{\mathrm{RM}}(r,n)$ and $G_{\partial\mathrm{RM}}(r,n)$ of $K(r,n)$ and $M(r,n) = C_{nr}$ of integer N-tuples? In the notation of that formalism, the original partition chain has elements S_{0_j} equal to the (1,1) code (or GF(2) = $\{\mathbf{0},\mathbf{1}\}$) for $j \le 0$ and to the (1,0) code (or the single-element set containing only $\mathbf{0}$) for $j > 0$. The generator matrix sequence G_{0_j} is nonzero only for $j = 0$, where it is the single generator 1. Thus the generating function $G_0(x)$ is the "unit impulse" 1, and the generating function $S_0(x)$ is the "unit step function" $u(x^{-1})$. Consequently, $G_n(x) = G_{\partial\mathrm{RM}}(n,x)G_0(x) = G_{\partial\mathrm{RM}}(n,x)$, and $S_n(x) = G_{\partial\mathrm{RM}}(n,x)S_0(x) = G_{\partial\mathrm{RM}}(n,x)u(x^{-1}) = G_{\mathrm{RM}}(n,x)$, where $G_{\partial\mathrm{RM}}(r,n)$ is the set of all rows of the $N \times N$ integer matrix $G_{(N,N)} = G_{(2,2)}^{n}$ with weight 2^{n-r}, and $G_{\mathrm{RM}}(r,n)$ is the set of all rows of $G_{(N,N)}$ with weight greater than or equal to 2^{n-r}. Thus Lemma 2 shows that the code $\mathrm{RM}(r,n)$ is equal to the set of all codewords generated by binary linear combinations of the set of generators $G_{\mathrm{RM}}(r,n)$, using mod-2 vector addition.

By substituting an arbitrary group S for GF(2), it is possible to show that codes with the parameters of the Reed–Muller codes can be constructed over any group S. Let Z be the trivial group containing only the single element $\mathbf{0}$ of S, and let S/Z be the exhaustive partition of S. The single generator 1 still generates a system of coset representatives $\{s\} = S$ for S/Z. By repeating the derivation of the previous paragraphs with S in place of GF(2), we arrive at a nested set of codes $\mathrm{RM}_S(r,n)$ which consist of all sums of N-tuples of the form $sG_{\mathrm{RM}}(r,n)$, where s is a $K(r,n)$-tuple of elements of S, using vector addition in S. If S is a field, $\mathrm{RM}_S(r,n)$ is a $K(r,n)$-dimensional vector space over S. The minimum Hamming distance between codewords in $\mathrm{RM}_S(r,n)$ is 2^{n-r}, even if S is not a field or S is not finite. The $N \times N$ integer matrix $G_{\mathrm{RM}}(n,n) = G_{(N,N)}$ is a basis for S^N, reflecting the fact that $G_{(N,N)}$ is a universal basis for N-space.

The binary Reed–Muller codes are the best binary codes of length $N = 2^n$ with minimum distances 2^{n-r} for $N \le 32$. At $N = 64$, the extended BCH codes with minimum distances 8 and 16 are superior and can themselves be improved upon [2, table 5.4]. Important special classes are

- $\mathrm{RM}(n,n) = (N,N,1)$: binary N-space $[\mathrm{GF}(2)]^N$;
- $\mathrm{RM}(n,n-1) = (N,N-1,2)$: single-parity-check codes;
- $\mathrm{RM}(n,n-2) = (N,N-n-1,4)$: extended Hamming codes;
- $\mathrm{RM}(n,(n-1)/2)) = (N,N/2,2(n+1)/2)$ (n odd): even self-dual codes;
- $\mathrm{RM}(n,1) = (N,n+1,N/2)$: first-order Reed–Muller codes;
- $\mathrm{RM}(n,0) = (N,1,N)$: repetition codes;
- $\mathrm{RM}(n,-1) = (N,0,\infty)$: the code whose single codeword is $\mathbf{0}^N$.

None of these codes (except the even self-dual codes) can be improved upon, for any N.

The nonbinary generalized Reed–Muller $(N,1,N)$ repetition code and $(N,N-1,2)$ generalized single-parity-check codes cannot be improved upon, in view of the Singleton bound, $d_H \le N-K+1$. (Because they meet this bound with equality, they are "maximum distance separable.") Thus the first generalized Reed–Muller code that can be improved upon is $\mathrm{RM}_S(1,3) = (8,4,4)$; indeed, when S is a finite field with more than seven elements, there is an (8,5,4) Reed–Solomon code over S [5].

Note that linearity was never used in any essential way in constructing the Reed–Muller codes or deriving their distance properties. This supports the view that these codes are fundamentally geometrical rather than algebraic constructs.

Notes: Reed–Muller codes were among the first to be constructed, and most of the properties derived here have been known for a long time. The first explicit iterative constructions of the Reed–Muller codes seem to be in [7], using a "product generator code" construction that is effectively the same as our iterated squaring construction, and in [8], using the $|u|u+v|$ construction. A close retrospective reading of Plotkin [9] reveals the same construction. The iterative construction using the squaring construction is also stated in [5, ch. 13, sec. 3, problem 6]. These are also special cases of the "generalized concatenated codes" of Blokh and Zyablov [10] and Zinov'ev [11].

The two-level constructions for the Reed–Muller codes, with their associated trellis diagrams, are believed to be new and unexpectedly simple. For example, Wolf [6] showed that an (N,K) code could be represented by a trellis diagram with no more than $\min[2^K, 2^{N-K}]$ states, giving, for example, a trellis for the (15,11) Hamming code with 16 states; our construction yields a regular eight-state trellis for the (16,11) extended Hamming code. (A complete trellis would have 16 states; see the Appendix.)

B. The Barnes–Wall Lattices and Their Principal Sublattices

Consider now the two-way partition $\boldsymbol{Z}/2\boldsymbol{Z}$ of the integers into even and odd integers. The set of coset representatives $[\boldsymbol{Z}/2\boldsymbol{Z}]$ is $\{0,1\}$, with generator 1. $\boldsymbol{Z}$ and $2\boldsymbol{Z}$ are both groups under addition and are therefore one-dimensional lattices.

Applying the squaring construction to the partition $\boldsymbol{Z}/2\boldsymbol{Z}$, we arrive at a two-dimensional set $U = |\boldsymbol{Z}/2\boldsymbol{Z}|^2 = \{2\boldsymbol{Z}^2 + (c,c),\ c \in \{0,1\}\}$, which is a subgroup of $\boldsymbol{Z}^2$ under vector addition, and thus is a two-dimensional lattice. Since U is the set of all integers which are either both even or both odd or, equivalently, the set of all integers with even norm, we identify U as the lattice $R\boldsymbol{Z}^2$ obtained earlier by applying the two-dimensional rotation operator R to $\boldsymbol{Z}^2$. From the general properties of the squaring construction, $R\boldsymbol{Z}^2$ has minimum squared distance $d_{\min}^2 = 2$, has a trivial two-section two-state trellis diagram, and is a union of two cosets of $2\boldsymbol{Z}^2$, while $\boldsymbol{Z}^2$ is a union of two cosets of $R\boldsymbol{Z}^2$; $R\boldsymbol{Z}^2/2\boldsymbol{Z}^2$ has a generator matrix with the single generator $\boldsymbol{g}_1 = [11]$, while $\boldsymbol{Z}^2/R\boldsymbol{Z}^2$ has a generator

matrix with the single generator $\boldsymbol{g}_0 = [10]$. Since $\boldsymbol{Z}^2$ and $2\boldsymbol{Z}^2$ may be regarded as each others' duals modulo 2, $R\boldsymbol{Z}^2$ is self-dual modulo 2.

Since $\boldsymbol{Z}^2/R\boldsymbol{Z}^2/2\boldsymbol{Z}^2$ is a chain of two-way partitions with generators $\boldsymbol{g}_0$ and $\boldsymbol{g}_1$ and distances 1/2/4, it follows that $2\boldsymbol{Z}^2/2R\boldsymbol{Z}^2/4\boldsymbol{Z}^2$ is a chain of two-way partitions with generators $2\boldsymbol{g}_0$ and $2\boldsymbol{g}_1$ and distances 4/8/16, and so forth. Therefore, there is an infinite chain of two-way partitions $\boldsymbol{Z}^2/R\boldsymbol{Z}^2/2\boldsymbol{Z}^2/2R\boldsymbol{Z}^2/4\boldsymbol{Z}^2/\cdots$ with minimum squared distances increasing by a factor of two at each partition, and with generators $\boldsymbol{g}_0, \boldsymbol{g}_1, 2\boldsymbol{g}_0, 2\boldsymbol{g}_1, \cdots$. (Note that $R\boldsymbol{g}_0 = \boldsymbol{g}_1$, $R\boldsymbol{g}_1 = 2\boldsymbol{g}_0$, and so forth.) As noted in [1], this chain can also be regarded as the one-dimensional chain $\boldsymbol{G}/\phi\boldsymbol{G}/\phi^2\boldsymbol{G}/\cdots$ of complex lattices $\phi^n\boldsymbol{G}$, where $\boldsymbol{G}$ is the lattice of Gaussian integers and ϕ is $1+i$, the prime of least norm in $\boldsymbol{G}$; the generators are then the 1-tuples $1, \phi, \phi^2, \cdots$. This is an ideal chain to which to apply the squaring construction.

Let us therefore extend the chain upwards with dummy partitions to obtain the chain $\cdots/\boldsymbol{Z}^2/\boldsymbol{Z}^2/\boldsymbol{Z}^2/R\boldsymbol{Z}^2/2\boldsymbol{Z}^2/\cdots$; i.e., we define the two-dimensional lattices $\Lambda(r,0)$ as $\boldsymbol{Z}^2$ for $r \geq 0$, and as $R^{-r}\boldsymbol{Z}^2$ for $r \leq 0$ (since $R^2 = 2$). The lattices $\Lambda(r,n)$ are then defined recursively by the squaring construction

$$\Lambda(r,n) \triangleq |\Lambda(r,n-1)/\Lambda(r-1,n-1)|^2.$$

By the general properties of iterated squaring constructions, this definition produces a chain of nested lattices of length $N = 2^{n+1}$ from the chain of lattices of length $N/2$. By induction, $\Lambda(r,n)$ is $\boldsymbol{Z}^N$ for $r \geq n$, and $\Lambda(r,n) = R^{-r}\Lambda(0,n)$ for $r \leq 0$ (since the rotation operator R commutes with the squaring construction). We shall see that $\Lambda(0,n)$ is the N-dimensional Barnes–Wall lattice, and we shall call the sequence $\Lambda(r,n)$, $0 \leq r \leq n$, its principal sublattices (although at this point we have shown only that $\Lambda(0,n)$ is a sublattice of $\Lambda(r,n)$ for $r \geq 0$). By Lemma 1 and induction, the minimum squared distance of $\Lambda(r,n)$ is 2^{n-r} for $0 \leq r \leq n$.

If we define $M_\Lambda(r,n)$ as the dimension of $[\Lambda(r,n)/\Lambda(r-1,n)]$, then by the properties of the two-level squaring construction, $M_\Lambda(r,n) = M_\Lambda(r,n-1) + M_\Lambda(r-1,n-1)$, and $M_\Lambda(r,n)$ is the binary logarithm of the number of states in a two-section or four-section trellis diagram representing $\Lambda(r,n) = |\Lambda(r,n-1)/\Lambda(r-1,n-1)|^2 = |\Lambda(r,n-2)/\Lambda(r-1,n-2)/\Lambda(r-2,n-2)|^4$. Solving this recursion with the initial conditions $M_\Lambda(r,0) = 1$ if $r \geq 0$ and $M_\Lambda(r,0) = 0$ if $r < 0$, we obtain $M_\Lambda(r,n)$ equal to $K(r,n)$, the dimension of $\mathrm{RM}(r,n)$, since $M_\Lambda(r,0) = K(r,0)$ and the recursion is the same.

Fig. 11 is a tableau of the Barnes–Wall lattices and their principal sublattices of lengths up to $N = 32$, as generated by the iterated squaring construction defined before. The italicized lattices are those corresponding to dummy partitions. We have preceded the initial chain $\Lambda(r,0)$ defined above with a one-dimensional chain $\cdots/\boldsymbol{Z}/\boldsymbol{Z}/\boldsymbol{Z}/2\boldsymbol{Z}/2\boldsymbol{Z}/4\boldsymbol{Z}/4\boldsymbol{Z}/\cdots$, as we may since $|m\boldsymbol{Z}/m\boldsymbol{Z}|^2 = m\boldsymbol{Z}^2$ and $|m\boldsymbol{Z}/2m\boldsymbol{Z}|^2 = mR\boldsymbol{Z}^2$. As we shall verify shortly, the Barnes–Wall lattices $\Lambda(0,1)$ and $\Lambda(0,2)$ are the Schläfli

$\boldsymbol{Z}$					
	$\boldsymbol{Z}^2$				
$\boldsymbol{Z}$		$\boldsymbol{Z}^4$			
	$\boldsymbol{Z}^2$		$\boldsymbol{Z}^8$		
$\boldsymbol{Z}$		$\boldsymbol{Z}^4$		$\boldsymbol{Z}^{16}$	
	$\boldsymbol{Z}^2$		$\boldsymbol{Z}^8$		$\boldsymbol{Z}^{32}(1)$
$\boldsymbol{Z}$		$\boldsymbol{Z}^4$		$\boldsymbol{Z}^{16}(1)$	(1)
	$\boldsymbol{Z}^2$		$\boldsymbol{Z}^8(1)$	(1)	$D_{32}(2)$
$\boldsymbol{Z}$		$\boldsymbol{Z}^4(1)$	(1)	$D_{16}(2)$	(5)
	$\boldsymbol{Z}^2(1)$	(1)	$D_8(2)$	(4)	$X_{32}(4)$
$\boldsymbol{Z}(1)$	(1)	$D_4(2)$	(3)	$H_{16}(4)$	(11)
(1)	$R\boldsymbol{Z}^2(2)$	(2)	$E_8(4)$	(7)	$H_{32}(8)$
$2\boldsymbol{Z}(4)$	(1)	$RD_4(4)$	(4)	$\Lambda_{16}(8)$	(15)
(0)	$2\boldsymbol{Z}^2(4)$	(2)	$RE_8(8)$	(8)	$\Lambda_{32}(16)$
$2\boldsymbol{Z}(4)$	(1)	$2D_4(8)$	(4)	$R\Lambda_{16}(16)$	(16)
(1)	$2R\boldsymbol{Z}^2(8)$	(2)	$2E_8(16)$	(8)	$R\Lambda_{32}(32)$
$4\boldsymbol{Z}(16)$	(1)	$2RD_4(16)$	(4)	$2\Lambda_{16}(32)$	(16)
(0)	$4\boldsymbol{Z}^2(16)$	(2)	$2RE_8(32)$	(8)	$2\Lambda_{32}(64)$
$4\boldsymbol{Z}(16)$	(1)	$4D_4(32)$	(4)	$2R\Lambda_{16}(64)$	(16)
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.

Fig. 11. Barnes–Wall lattices and principal sublattices of lengths $N \leq 32$, with minimum squared distances.

lattice D_4 and the Gosset lattice E_8, respectively. The lattices $\Lambda(0,3)$ and $\Lambda(0,4)$ are simply called the 16- and 32-dimensional Barnes–Wall lattices Λ_{16} and Λ_{32}, respectively. The lattices $\Lambda(n-1,n)$ are the checkerboard lattices D_N, and the lattices $\Lambda(1,n)$ are called H_N (for half-lattices) wherever not previously named. The last unnamed lattice $\Lambda(2,4)$ is called X_{32}. R^2 is replaced by 2 wherever possible. The dimensions $M_\Lambda(r,n)$ are also shown in parentheses between $\Lambda(r,n)$ and $\Lambda(r-1,n)$, where they are nonzero; from these dimensions, we can see the numbers of states in the trellis diagrams for the lattices in the next chain.

The Barnes–Wall lattices themselves are generated by the recursion

$$\Lambda(0,n) = |\Lambda(0,n-1)/R\Lambda(0,n-1)|^2,$$

since $\Lambda(-1,n-1) = R\Lambda(0,n-1)$. Thus $\Lambda(0,n-1)^2/\Lambda(0,n)/R\Lambda(0,n-1)^2$ is a lattice partition chain with distances $2^{n-1}/2^n/2^n$, where each partition has order $|\Lambda(0,n-1)/R\Lambda(0,n-1)|$. Since $R\Lambda(0,n) \triangleq |R\Lambda(0,n-1)/R^2\Lambda(0,n-1)|^2$, $R\Lambda(0,n-1)^2/R\Lambda(0,n)/R^2\Lambda(0,n-1)^2$ is also a lattice partition chain with the same partition orders. Thus the order of $\Lambda(0,n)/R\Lambda(0,n)$ is the square of the order of $\Lambda(0,n-1)/R\Lambda(0,n-1)$. Solving this recursion with the initial condition $|\Lambda(0,0)/R\Lambda(0,0)| = 2$, we find that $|\Lambda(0,n)/R\Lambda(0,n)| = 2^N = 2^{2^n}$, a Fermat power of two.

We also see that $\Lambda(0,n)$ and $R\Lambda(0,n-1)^2$ have the same minimum squared distance 2^n, but $\Lambda(0,n)$ has $|\Lambda(0,n-1)/R\Lambda(0,n-1)| = 2^{N/2}$ as many points per unit volume of 2^n-space as does $R\Lambda(0,n-1)^2$, so the coding gain $\gamma(n)$ of $\Lambda(0,n)$ is $|\Lambda(0,n-1)/R\Lambda(0,n-1)|^{1/N} = 2^{1/2}$ as large as that of $R\Lambda(0,n-1)^2$, which is the same as that of $\Lambda(0,n-1)$, namely $\gamma(n-1)$. Since $\gamma(0) = 1$,

$$\gamma(n) = 2^{n/2}.$$

Thus the coding gain of the Barnes–Wall lattices increases without limit.

Since D_4 and E_8 are mod-2 lattices isomorphic to the (4,3) and (8,4) Reed–Muller codes, respectively, their trellis diagrams are the same, and have two and four states, respectively. These lattices achieve coding gains of $2^{1/2}$ (1.5 dB) and 2 (3 dB). The Barnes–Wall lattices Λ_{16} and Λ_{32}, which achieve coding gains of $2^{3/2}$ (4.5 lB) and 4 (6 dB), have trellis diagrams with only 16 and 256 states, respectively, illustrated in Fig. 12. In general, since $\Lambda(0,n)/R\Lambda(0,n)$ is a partition of order 2^N, where $N=2^n$, a two-section or four-section trellis diagram for $\Lambda(0,n+1)$ has 2^N states. The trellis for $\Lambda(0,n)$ thus has $2^{2^{n-1}}$ states, and the number of states in the trellis for $\Lambda(0,n+1)$ is the square of the number of states in the trellis for $\Lambda(0,n)$. The first four numbers in this sequence, i.e., 2, 4, 16, and 256, are well behaved, but then a combinatorial explosion occurs: 65 536 states for Λ_{64}, which achieves a coding gain of $2^{5/2}$ (7.5 dB), and more than four billion states for Λ_{128}, which achieves a coding gain of eight (9 dB). This explosion might have been expected from capacity and R_0 considerations (Forney *et al.* [14]).

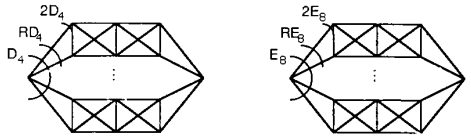


Fig. 12. Schematic trellis diagrams for $\Lambda_{16}=|D_4/RD_4/2D_4|^4$ and $\Lambda_{32}=|E_8/RE_8/2E_8|^4$.

The chain $\Lambda(r,n)$, $\forall r$, is obtained by applying the squaring construction n' times to the chain $\Lambda(r,n-n')$, $\forall r$. Thus we can express any lattice $\Lambda(r,n)$ by an n'-level iterated squaring construction on an n'-level lattice partition chain from the chain $\Lambda(r,n-n')$, namely,

$$\Lambda(r,n)=|\Lambda(r,n-n')/\cdots/\Lambda(r-n',n-n')|^{N'}, \qquad N'=2^{n'}.$$

From Lemma 2, therefore,

$$[\Lambda(r,n)/\Lambda(r-1,n)]=\sum_{0\le r'\le n'} G_{\partial \mathrm{RM}}(r',n') \cdot[\Lambda(r-r',n-n')/\Lambda(r-r'-1,n-n')]$$

$$\Lambda(r,n)=\sum_{0\le r'\le n'} G_{\partial \mathrm{RM}}(r',n')\Lambda(r-r',n-n')$$

$$\Lambda(r,n)=\Lambda(r-n',n-n')^{N'}+\sum_{0\le r'< n'} G_{\mathrm{RM}}(r',n') \cdot[\Lambda(r-r',n-n')/\Lambda(r-r'-1,n-n')].$$

In particular, if we let $n'=n$,

$$\Lambda(r,n)=|\Lambda(r,0)/\Lambda(r-1,0)/\cdots/\Lambda(r-n,0)|^N, \qquad =|\boldsymbol{Z}^2/\cdots/\boldsymbol{Z}^2/\cdots/R^{n-r}\boldsymbol{Z}^2|^N, \qquad 0\le r\le n,$$

where $N=2^n$, and we obtain

$$\Lambda(r,n)=\Lambda(r-n,0)^N+\sum_{0\le r'< n} G_{\mathrm{RM}}(r',n) \cdot[\Lambda(r-r',0)/\Lambda(r-r'-1,0)], \qquad N=2^n,$$

which, for $0\le r\le n$, is equal to

$$\Lambda(r,n)=R^{n-r}\boldsymbol{Z}^{2N}+\sum_{r\le r'< n} G_{\mathrm{RM}}(r',n)\left[R^{r'-r}\boldsymbol{Z}^2/R^{r'-r+1}\boldsymbol{Z}^2\right].$$

This shows that $R^{n-r}\boldsymbol{Z}^{2N}\simeq\phi^{n-r}\boldsymbol{G}^N$ is a sublattice of $\Lambda(r,n)$, but $R^{n-r+1}\boldsymbol{Z}^{2N}\simeq\phi^{n-r+1}\boldsymbol{G}^N$ is not, so the depth of $\Lambda(r,n)$ is $\mu=n-r$. Since $R^r\boldsymbol{Z}^2/R^{r+1}\boldsymbol{Z}^2\simeq\phi^r\boldsymbol{G}/\phi^{r+1}\boldsymbol{G}$, and $[\phi^r\boldsymbol{G}/\phi^{r+1}\boldsymbol{G}]$ is generated by ϕ^r, we arrive at the *complex code formula*

$$\Lambda(r,n)=\phi^{n-r}\boldsymbol{G}^N+\sum_{r\le r'< n}\mathrm{RM}(r',n)\phi^{r'-r}$$

where the expression $\mathrm{RM}(r',n)\phi^{r'-r}$ is to be interpreted as the set of all $2^{K(r',n)}$ codewords in $\mathrm{RM}(r',n)$, regarded as integer 2^n-tuples, multiplied by the Gaussian integer $\phi^{r'-r}$, and where the sum is a direct sum over all linear combinations of these generators. Thus the whole expression is a coset decomposition involving $2^{K^*(r,n)}$ cosets of $\phi^{n-r}\boldsymbol{G}^N$, where $K^*(r,n)=\sum_{r\le r'<n}K(r',n)$. Because of the symmetry of the sequence $K(r',n)$ around $N/2$, we have $K^*(0,n)=nN/2$, where $N=2^n$; therefore, the Barnes–Wall lattice $\Lambda(0,n)$ is the union of $2^{nN/2}$ cosets of $\phi^n\boldsymbol{G}^N$, which shows again that its coding gain is $\gamma(n)=2^{n/2}$. For example,

$$D_4=\Lambda(0,1)=\phi\boldsymbol{G}^2+(2,1,2);$$

$$D_8=\Lambda(1,2)=\phi\boldsymbol{G}^4+(4,3,2);$$

$$E_8=\Lambda(0,2)=\phi^2\boldsymbol{G}^4+\phi(4,3,2)+(4,1,4),$$

and so forth, since $\mathrm{RM}(0,1)=(2,1,2)$, $\mathrm{RM}(1,2)=(4,3,2)$, and $\mathrm{RM}(0,2)=(4,1,4)$. This means, for example, that E_8 is the lattice of all complex 4-tuples λ that are congruent to $\phi\boldsymbol{c}_1+\boldsymbol{c}_0$ modulo ϕ^2, where $\boldsymbol{c}_1$ and $\boldsymbol{c}_0$ are codewords in the (4,3,2) and (4,1,4) binary codes, respectively.

By going one step further back, we arrive at the one-dimensional chain $\cdots/\boldsymbol{Z}/\boldsymbol{Z}/\boldsymbol{Z}/2\boldsymbol{Z}/2\boldsymbol{Z}/4\boldsymbol{Z}/4\boldsymbol{Z}/\cdots$. In this chain, S_{0j} is $2^{j/2}\boldsymbol{Z}$ for j even, and $2^{(j-1)/2}\boldsymbol{Z}$ for j odd, so that the generator matrix G_{0j} is the single generator $2^{(j-1)/2}$ for j odd, and the empty set for j even. Consequently, in the general formula of Lemma 2 involving $G_{\mathrm{RM}}(r,n+1)$, every other term drops out, and we are left with the *real code formulas*

$$\Lambda(r,n)=2^{(n-r)/2}\boldsymbol{Z}^{2N}+\sum_{r+1\le r'\le n,\ n-r' \text{ even}}\mathrm{RM}(r',n+1)2^{(n-r')/2}, \qquad n-r \text{ even};$$

$$\Lambda(r,n)=2^{(n-r+1)/2}\boldsymbol{Z}^{2N}+\sum_{r+1\le r'\le n,\ n-r' \text{ even}}\mathrm{RM}(r',n+1)2^{(n-r')/2}, \qquad n-r \text{ odd},$$

where the expression $\mathrm{RM}(r',n+1)2^{(n-r')/2}$ is to be interpreted as the product of the codewords of $\mathrm{RM}(r',n+1)$, regarded as integer 2^{n+1}-tuples, with the integer $2^{(n-r')/2}$.

For example,

$$D_4 = \Lambda(0,1) = 2\mathbf{Z}^4 + (4,3,2)$$
$$E_8 = \Lambda(0,2) = 2\mathbf{Z}^8 + (8,4,4)$$
$$\Lambda_{16} = \Lambda(0,3) = 4\mathbf{Z}^{16} + 2(16,15,2) + (16,5,8)$$
$$\Lambda_{32} = \Lambda(0,4) = 4\mathbf{Z}^{32} + 2(32,26,4) + (32,6,16)$$

and so forth. Since R commutes with the squaring construction, we also have

$$R\Lambda(r,n) = 2^{(n-r+1)/2}\mathbf{Z}^{2N} + \sum_{r \le r' < n,\, n-r' \text{ odd}} \mathrm{RM}(r', n+1)2^{(n-r'-1)/2}, \quad n-r \text{ odd};$$

$$R\Lambda(r,n) = 2^{(n-r+2)/2}\mathbf{Z}^{2N} + \sum_{r \le r' < n,\, n-r' \text{ odd}} \mathrm{RM}(r', n+1)2^{(n-r'-1)/2}, \quad n-r \text{ even}.$$

For example,

$$RD_4 = \Lambda(-1,1) = 2\mathbf{Z}^4 + (4,1,4)$$
$$RE_8 = \Lambda(-1,2) = 4\mathbf{Z}^8 + 2(8,7,2) + (8,1,8)$$
$$R\Lambda_{16} = \Lambda(-1,3) = 4\mathbf{Z}^{16} + 2(16,11,4) + (16,1,16)$$
$$R\Lambda_{32} = \Lambda(-1,4) = 8\mathbf{Z}^{32} + 4(32,31,2) + 2(32,16,8) + (32,1,32),$$

and so forth. These code formulas exhibit the relationships between Reed–Muller codes and Barnes–Wall lattices that were developed in [12] and allow us to verify that indeed these are the Barnes–Wall lattices, including D_4 and E_8.

From these code formulas, it is easy to verify that $\Lambda(0,n)/R\Lambda(1,n)/\cdots/R^n\Lambda(n,n)$ is a lattice partition chain, because each lattice involves a subset of the generators for the previous lattice. For example,

$$E_8 = \Lambda(0,2) = \phi^2\mathbf{G}^4 + \phi(4,3,2) + (4,1,4),$$
$$RD_8 = R\Lambda(1,2) = \phi^2\mathbf{G}^4 + \phi(4,3,2);$$
$$R^2\Lambda(2,2) = \phi^2\mathbf{G}^4;$$
$$\Lambda_{16} = \Lambda(0,3) = \phi^3\mathbf{G}^8 + \phi^2(8,7,2) + \phi(8,4,4) + (8,1,8);$$
$$RH_{16} = R\Lambda(1,3) = \phi^3\mathbf{G}^8 + \phi^2(8,7,2) + \phi(8,4,4);$$
$$R^2D_{16} = R^2\Lambda(2,3) = \phi^3\mathbf{G}^8 + \phi^2(8,7,2);$$
$$R^3\Lambda(3,3) = \phi^3\mathbf{G}^8.$$

Note that every lattice in such a partition has the same minimum squared distance 2^{n-r}. The partition $\Lambda(r,n)/R\Lambda(r+1,n)$ has order $2^{K(r,n)}$, where $K(r,n)$ is the dimension of the code $\mathrm{RM}(r,n)$; the points in $\Lambda(r,n)$ are therefore $2^{K(r,n)}$ times as dense in 2^{n+1}-space as the points in $R\Lambda(r+1,n)$. This allows us to determine the coding gain of each of these lattices, which is given in [1, tables I and II]. The partition Λ_N/RH_N always has order 2, which is why H_N is called a half-lattice; the trellis diagram for Λ_N consists of two parallel subtrellises, each representing one of the two cosets of RH_N of which Λ_N is the union.

The duals $\Lambda(r,n)^\perp$ of these lattices may be defined by

$$\Lambda(r,n)^\perp \triangleq |\mathbf{G}/\phi\mathbf{G}/\cdots/\phi^{n-r}\mathbf{G}/\cdots/\phi^{n-r}\mathbf{G}|^N, \quad 0 \le r \le n,\ N = 2^n$$

where the notion of duality is as a complex lattice modulo ϕ^{n-r}, and the chain is the dual modulo ϕ^{n-r} to that which gives $\Lambda(r,n)$ in the expression $\Lambda(r,n) = |\mathbf{G}/\cdots/\mathbf{G}/\phi\mathbf{G}/\cdots/\phi^{n-r}\mathbf{G}|^N$. Then we arrive at the complex code formula

$$\Lambda(r,n)^\perp = \phi^{n-r}\mathbf{G}^N + \sum_{0 \le r' < n-r} \mathrm{RM}(r', n)\phi^{r'}.$$

For example,

$$D_4^\perp = \Lambda(0,1)^\perp = \phi\mathbf{G}^2 + (2,1,2) = D_4$$
$$D_8^\perp = \Lambda(1,2)^\perp = \phi\mathbf{G}^4 + (4,1,4)$$
$$E_8^\perp = \Lambda(0,2)^\perp = \phi^2\mathbf{G}^4 + \phi(4,3,2) + (4,1,4) = E_8$$

and so forth. Thus $\Lambda(0,n)$ is self-dual modulo ϕ^n, because the code formulas of $\Lambda(0,n)$ and $\Lambda(0,n)^\perp$ are the same; the depth of $\Lambda(r,n)^\perp$ is $\mu = n-r$, the same as the depth of $\Lambda(r,n)$; the minimum squared distance of $\Lambda(r,n)^\perp$ is $2^\mu = 2^{n-r}$, the same as that of $\Lambda(r,n)$; and the complex code formula for $\Lambda(r,n)^\perp$ involves the codes which are the duals of the codes in the complex code formula for $\Lambda(r,n)$.

(Note that $D_8^\perp$ has $\phi\mathbf{G}^4$ as a sublattice of order 2; $D_8^\perp$ is therefore a mod-2 lattice, with $2\mathbf{Z}^8$ as a sublattice of order 2^5, so $D_8^\perp$ must be isomorphic to some (8,5,2) code; but the real code formula $D_8^\perp = 2\mathbf{Z}^8 + (8,5,2)$ is not nearly as nice as the complex code formula. The lattice $RD_8^\perp$ is the mod-2 dual to D_8 and has real code formula $RD_8^\perp = 2\mathbf{Z}^8 + (8,1,8)$, which is dual to the real code formula for D_8.)

To display these dual sublattices, we may begin with the two-dimensional chain $\cdots/\mathbf{G}/\mathbf{G}/\mathbf{G}/\phi\mathbf{G}/\phi^2\mathbf{G}/\cdots/\phi^\mu\mathbf{G}/\phi^\mu\mathbf{G}/\phi^\mu\mathbf{G}/\cdots$, which is self-dual modulo ϕ^μ. Repeated application of the squaring construction to this chain results in a self-dual chain of $2^{\mu+1}$-dimensional depth-μ lattices. The $2^{\mu+1}$-dimensional lattices comprise, on the one hand, the lattices $\Lambda(r,\mu)$, $0 \le r \le \mu$, and, on the other hand, lattices $\phi^\mu\Lambda(r,\mu)^\perp$ which involve their duals $\Lambda(r,\mu)^\perp$, $0 \le r \le \mu$. Since the Barnes–Wall lattice $\Lambda(0,\mu)$ appears in the middle of this self-dual chain, it is self-dual. This construction is illustrated for $\mu = 4$ in Fig. 13. Note that this tableau illustrates the chain $\Lambda(0,\mu)^\perp/\phi\Lambda(1,\mu)^\perp/\cdots/\phi^\mu\Lambda(\mu,\mu)^\perp$, with distances $2^\mu/2^\mu/\cdots/2^\mu$, which is the dual chain to $\Lambda(\mu,\mu)/\Lambda(\mu-1,\mu)/\cdots/\Lambda(0,\mu)$, modulo 2^μ; there is also a chain $\Lambda(\mu,\mu)^\perp/\Lambda(\mu-1,\mu)^\perp/\cdots/\Lambda(0,\mu)^\perp$ with distances $1/2/\cdots/2^\mu$ which is dual to the chain $\Lambda(0,\mu)/\phi\Lambda(1,\mu)/\cdots/\phi^\mu\Lambda(\mu,\mu)$, modulo 2^μ. In [1, fig. 9] is an illustration of all of these chains in a single diagram.

It seems to us that these lattices are best regarded as complex lattices, for a number of reasons. The two-dimensional chain is a more natural starting point than the

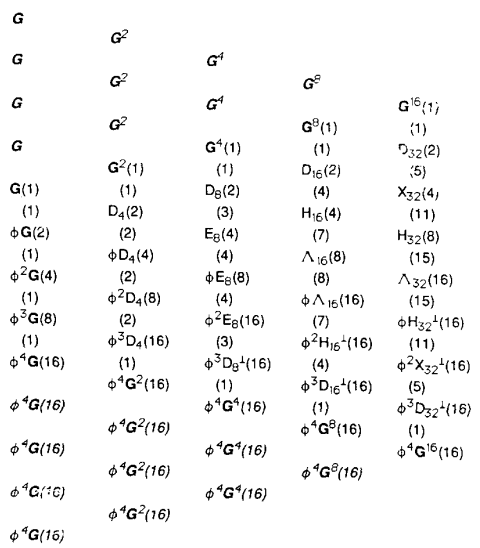


Fig. 13. Barnes–Wall lattices, principal sublattices, and dual principal sublattices of lengths $N \leq 32$ with minimum squared distances.

one-dimensional chain, and the two-dimensional chain is best regarded as a one-dimensional complex chain. Multiplication by a complex scalar ϕ is nicer than rotation by the 2×2 matrix R; for instance, it is easier to see that multiplication by ϕ commutes with the squaring construction. (Also, we avoid the abuse of notation that occurs when we operate with R on $2N$-dimensional vectors.) The complex code formulas are more regular than the real ones. The depth (ϕ-depth) seems a more significant structural parameter than the 2-depth. Duals are most naturally defined for the complex lattices modulo ϕ^{μ} and are naturally expressed by complex code formulas.

Notes: The infinite series of lattices $\Lambda(0, n)$ is due to Barnes and Wall [13], who essentially constructed them from rows of $G_{(N,N)}$. (The principal sublattices and their duals also appear in [13], although without special notice.) Their iterative construction by the squaring construction, their construction by the two-level construction with the associated four-section trellis diagrams, and the general multilevel constructions are believed to be new. Forney *et al.* [14] gave constructions for D_4, E_8, and Λ_{16} in terms of repeated binary partitions of a two-dimensional rectangular grid and gave a four-section trellis diagram for E_8. Cusack [15] derived a general construction for Barnes–Wall lattices equivalent to our complex code formula, using partitions from the two-dimensional chain $\boldsymbol{Z}^2/R\boldsymbol{Z}^2/2\boldsymbol{Z}^2/2R\boldsymbol{Z}^2/\cdots$ and Reed–Muller codes. The real code formulas that we derive from one-dimensional partitions, involving alternate Reed–Muller codes, amount to construction C of [12] or construction D of Barnes and Sloane [16]. There are also constructions involving nonbinary Reed–Solomon codes in [16] and [17] that turn out to be equivalent to our squaring construction and two-level constructions; this happens because the binary (2,1), (4,3), and (4,1) codes are "maximal distance separable," so that the Reed–Solomon code does not improve on the Reed–Muller or generalized Reed–Muller codes.

V. Cubing Constructions

We now give constructions that generate codes and lattices of length $3N$ from those of length N. These will be applied in the next section to yield codes and lattices of length $3\cdot 2^n$, notably the Golay code and Leech lattice, from those of length 2^n that have already been constructed.

A. Cubing Constructions for Two-Level Partitions

Let $S/T/V$ be a two-level partition chain, with $|S/T| = M$ and $|T/V| = N$. Then $S/T/V$ is represented by a partition trellis as in Fig. 1, with M clusters of N nodes each, each cluster corresponding to a subset T_i of S.

Let $U = |S/T|^2$ and $W_i = |T_i/V_i|^2$. We saw in Fig. 5(a) that the partition U/W is represented by a two-section trellis, also terminating in M clusters of N nodes each, each cluster corresponding to a subset T_i of S. It seems natural, therefore, to paste these two trellises together to arrive at the three-section trellis of Fig. 14. We respect the integrity of the clusters, but otherwise the clusters and the nodes within clusters may be pasted together (twisted) in any arbitrary way. We call such a construction a *cubing construction* $|S/T/V|^3$. It is closely related to the two-level iterated squaring construction $|S/T/V|^4$, whose trellis (Fig. 5(b)) is the same as that of Fig. 14, except with one more middle section.

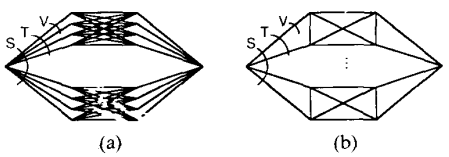


Fig. 14. Trellis diagrams for cubing construction $|S/T/V|^3$. (a) For $|S/T| = 2$, $|T/V| = 4$. (b) Schematic.

Decoding a cubing construction involves decoding the partition U/W, whose complexity is $MN(2N-1)$ binary operations, followed by decoding what is essentially an MN-state squaring construction, whose complexity is $2MN - 1$, for a total of $2MN^2 + MN - 1$ binary operations. The branch complexity in the middle section is MN^2, so that the decoding complexity per section approximates $2/3$ the branch complexity for large N.

From the trellis diagram, we obtain a lower bound on the minimum distance for any cubing construction, again using the partition distance lemma.

Lemma 3: If $S/T/V$ is a two-level partition chain with distances $d(S)/d(T)/d(V)$, and $U = |S/T/V|^3$, then

$$d(U) \geq \min\left[d(V), 2d(T), 3d(S)\right].$$

Proof: If two distinct elements of U correspond to paths in the trellis which are

a) the same—then at least one component differs by at least $d(V)$, so $d(U) \geq d(V)$;
b) distinct but in the same subtrellis (cluster)—then at least two components differ by at least $d(T)$, so $d(U) \geq 2d(T)$;

c) in different subtrellises—then all three components differ by at least $d(S)$, so $d(U) \geq 3d(S)$.

Elements corresponding to the same path always exist that differ by $d(V)$, so $d(U) \leq d(V)$. Whether or not there are elements that differ by $2d(T)$ or $3d(S)$ depends on the connection of the branches. If the cubing construction contains squaring constructions within two adjacent sections of a single subtrellis, however, then $d(U) \leq \min[d(V), 2d(T)]$, by Lemma 1.

As special cases of cubing constructions, we have the *repetition 3-construction* $|S/T/T|^3$, defined as the set of all 3-tuples of elements of S that all belong to the same coset of T, with a trellis diagram as shown in Fig. 15(a) or (b), and with minimum distance equal to $\min[d(T), 3d(S)]$; and the *parity-check 3-construction* $|S/S/T|^3$, defined as any cubing construction with a single subtrellis, as shown in Fig. 15(c) or (d) and with minimum distance lower-bounded by $\min[d(T), 2d(S)]$.

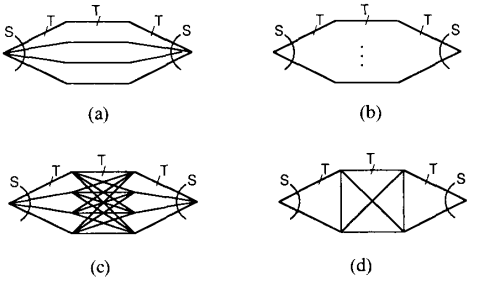


Fig. 15. Schematic trellis diagrams. (a) For repetition 3-construction $|S/T/T|^3$, if $|S/T| = 4$. (b) Same as (a), schematically. (c) Parity-check 3-construction $|S/S/T|^3$, if $|S/T| = 4$. (d) Same as (c), schematically.

B. The Cubing Construction for Group Partitions

Now let $S/T/V$ be a two-level group partition chain, with systems of coset representatives $[S/T]$ and $[T/V]$. As with the squaring constructions, we seek to define a cubing construction in terms of these coset representatives such that the resulting groups have desirable properties.

The squaring construction involves the integer matrix $G_{(2,2)} = \{\boldsymbol{g}_0, \boldsymbol{g}_1\}$, which is a basis for S^2, where S is any group. The two generators in $G_{(2,2)}$ generate all of the good binary codes of length 2.

Let us consider then the integer matrix $G_{(3,3)} \triangleq \{G_{(3,2)}, G_{(3,1)}\}$, where $G_{(3,2)}$ is the set of two integer 3-tuples {[110],[011]}, and $G_{(3,1)}$ consists of the single 3-tuple [111]. The two generators in $G_{(3,2)}$ generate the binary (3,2,2) code, and, in fact, as integer 3-tuples they generate a (3,2,2) code over any group S. The single generator in $G_{(3,1)}$ generates a (3,1,3) repetition code over any group. As a 3×3 integer matrix, $G_{(3,3)}$ has determinant 1, so $G_{(3,3)}$ is a universal basis for 3-space, i.e., a basis for S^3, where S is any group.

Because $G_{(3,2)}$ and $G_{(3,1)}$ together span 3-space, there are two distinct chains of partitions of the (3,3) code (or indeed of any S^3), illustrated in Fig. 16: $(3,3)/(3,2)/(3,0)$ and $(3,3)/(3,1)/(3,0)$. Thus $G_{(3,2)}$ is also a set of generators $G_{(3,3)/(3,1)}$ for the coset representatives $[(3,3)/(3,1)]$,

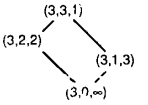


Fig. 16. Alternative partition chains $(3,3)/(3,2)/(3,0)$ and $(3,3)/(3,1)/(3,0)$.

and $G_{(3,1)} = G_{(3,3)/(3,2)}$ generates coset representatives for $[(3,3)/(3,2)]$. Note also that the generators in $G_{(3,2)}$ are dual to those in $G_{(3,1)}$ modulo 2, so that these two partition chains are dual to each other modulo 2.

We now define the following cubing construction, based on a two-level group partition $S/T/V$ with systems of coset representatives $[S/T]$ and $[T/V]$ and the generator matrices just defined:

$$\begin{aligned}|S/T/V|^3 &\triangleq G_{(3,3)}V + G_{(3,2)}[T/V] + G_{(3,1)}[S/T] \\ &= \{(\boldsymbol{v}_1 + \boldsymbol{c}_1 + \boldsymbol{d}, \boldsymbol{v}_2 + \boldsymbol{c}_1 + \boldsymbol{c}_2 + \boldsymbol{d}, \boldsymbol{v}_3 + \boldsymbol{c}_2 + \boldsymbol{d}): \\ &\qquad \boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3 \in V,\ \boldsymbol{c}_1, \boldsymbol{c}_2 \in [T/V],\ \boldsymbol{d} \in [S/T]\}\end{aligned}$$

where the second expression shows how to interpret the direct sum of Kronecker products denoted by the first expression. When we say *the cubing construction*, we mean this cubing construction.

The elements of $|S/T/V|^3$ corresponding to $\boldsymbol{c}_2 = \boldsymbol{d} = \boldsymbol{0}$ are the 2-tuples in the squaring construction $|T/V|^2$ followed by a 1-tuple in V. The elements $U(\boldsymbol{c}_2, \boldsymbol{d})$ of $|S/T/V|^3$ corresponding to fixed $\boldsymbol{c}_2$ and $\boldsymbol{d}$ are the coset $U(\boldsymbol{0},\boldsymbol{0}) + (\boldsymbol{d}, \boldsymbol{c}_2 + \boldsymbol{d}, \boldsymbol{c}_2 + \boldsymbol{d})$ of the elements $U(\boldsymbol{0},\boldsymbol{0})$ corresponding to $\boldsymbol{c}_2 = \boldsymbol{d} = \boldsymbol{0}$. Thus $|S/T/V|^3$ has a trellis diagram of the form of Fig. 14, where each set $U(\boldsymbol{c}_2, \boldsymbol{d})$ corresponds to all the paths going through a given node (which may be labeled $(\boldsymbol{c}_2, \boldsymbol{d})$) at the end of the second section, and the union of all such sets for a fixed $\boldsymbol{d}$ corresponds to a subtrellis. Similarly, the set of all elements of $|S/T/V|^3$ corresponding to fixed $\boldsymbol{c}_1$ and $\boldsymbol{d}$ correspond to all the paths going through a given node (which may be labeled $(\boldsymbol{c}_1, \boldsymbol{d})$) at the end of the first section.

It follows that this is indeed a cubing construction, and the lower bound on distance of Lemma 3 applies. Because the construction contains a squaring construction,

$$\begin{aligned}\min[d(V), 2d(T)] &\geq d(|S/T/V|^3) \\ &\geq \min[d(V), 2d(T), 3d(S)].\end{aligned}$$

If there is an element $\boldsymbol{d} \in [S/T]$ with $\mathrm{wt}(\boldsymbol{d}) = d(S)$, then the lower bound holds with equality; however, if there is no such element, then we may be able to improve on the lower bound, as we shall see in the construction of the Golay code and the Leech lattice in the next section.

As special cases of this construction, we have the *repetition 3-construction* $|S/T/T|^3$ and the $|T/T/V|^3$ *parity-check 3-construction* $|S/T/V|^3$. For these special cases, we have the distances

$$d(|S/T/T|^3) = \min[d(T), 3d(S)]$$

$$d(|T/T/V|^3) = \min[d(V), 2d(T)].$$

Equality holds in the first case because the repetition 3-construction contains all 3-tuples (s, s, s), $s \in S$.

It is easy to see that $|S/T/V|^3$ is a group. Also, $|S/T/V|^3$ is a subset of $|S/T/T|^3$, which is a subset of S^3; and V^3 is a subset of $|T/T/V|^3$, which is a subset of $|S/T/V|^3$. Consequently, $S^3/|S/T/T|^3/|S/T/V|^3/|T/T/V|^3/V^3$ is a group partition chain. The order of $S^3/|S/T/T|^3$ is the square of $|S/T|$, and the Kronecker product $G_{(3,2)}[S/T]$ generates a system of coset representatives for $S^3/|S/T/T|^3$ (since $S^3 = G_{(3,3)}(T+[S/T]) = G_{(3,3)}T + G_{(3,2)}[S/T] + G_{(3,1)}[S/T]$ and $|S/T/T|^3 = G_{(3,3)}T + G_{(3,1)}[S/T]$). The order of $|S/T/T|^3/|S/T/V|^3$ is $|T/V|$, and the Kronecker product $G_{(3,1)}[T/V]$ generates a system of coset representatives for $|S/T/T|^3/|S/T/V|^3$ (since $|S/T/T|^3 = G_{(3,3)}(V+[T/V]) + G_{(3,1)}[S/T]$, and $|S/T/V|^3 = G_{(3,3)}V + G_{(3,2)}[T/V] + G_{(3,1)}[S/T]$). Similarly, $|S/T/V|^3/|T/T/V|^3$ has order $|S/T|$ and generator matrix $G_{(3,1)}[S/T]$, while $|T/T/V|^3/V^3$ has order equal to the square of $|T/V|$ and generator matrix $G_{(3,2)}[T/V]$.

Now suppose that $S_0/S_1/\cdots/S_m$ is a group partition chain. The cubing partition may be applied to each two-level partition in this chain to yield groups $T_j = |S_j/S_{j+1}/S_{j+2}|^3$, $0 \le j \le m-2$. However, in general T_{j+1} is not a subgroup of T_j.

Fig. 17 shows the subgroup relationships that do exist, in general. These are based on the chain $S^3/|S/T/T|^3/|S/T/V|^3/|T/T/V|^3/V^3$ already noted, as well as the alternative central chain $|S/T/T|^3/T^3/|T/T/V|^3$ (since $T^3 = |T/T/T|^3$). We see that the subgroups can be arranged in a sort of double helix structure, with a periodicity corresponding to two levels in the original chain.

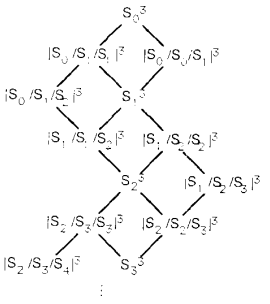


Fig. 17. Subgroup relationships for cubing constructions.

Using the generator matrix identity $G_{(3,3)} = G_{(3,2)} + G_{(3,1)}$, we have an alternative form for the cubing construction,

$$
\begin{aligned}
&|S/T/V|^3 \\
&\quad = G_{(3,2)}(V+[T/V]) + G_{(3,1)}(V+[S/T]) \\
&\quad = G_{(3,2)}T + G_{(3,1)}T^*, \quad \text{where } T^* \triangleq V+[S/T] \\
&\quad = \{(t_1+t^*, t_1+t_2+t^*, t_2+t^*) : t_1, t_2 \in T,\ t^* \in T^*\}.
\end{aligned}
$$

This is in the form of the $|a+x|b+x|a+b+x|$ construction mentioned in [5, ch. 18, sec. 7.4]. The direct sum of the coset representatives $[T/V]$ with the group T^*, defined as the direct sum $V+[S/T]$, is S; therefore, T^* is the intermediate group in an alternative partition $S/T^*/V$ to the partition $S/T/V$, as shown in Fig. 18. This shows that the cubing construction does not depend on the choice of

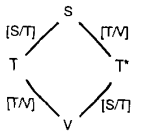


Fig. 18. Alternative partition chains $S/T/V$ and $S/T^*/V$.

coset representatives $[T/V]$; it does, however, depend on the choice of coset representatives $[S/T]$, or equivalently on T^*; thus, we shall indicate this choice explicitly when necessary.

Given T and T^*, an alternative definition of the cubing construction would therefore be the $|a+x|b+x|a+b+x|$ construction

$$
\begin{aligned}
&|T \nabla T^*|^3 \\
&\quad \triangleq G_{(3,2)}T + G_{(3,1)}T^* \\
&\quad = \{(t_1+t^*, t_1+t_2+t^*, t_2+t^*) : t_1, t_2 \in T,\ t^* \in T^*\}.
\end{aligned}
$$

We would then define V as the greatest common subgroup (intersection) of T and T^*, and S as the direct sum $V+[T/V]+[T^*/V]$, i.e., the least common supergroup of T and T^*. This definition has the advantage of completely specifying the construction, whereas the earlier definition needs to be augmented by a specification of $[S/T]$, and is the preferred form when there is a natural parallelism between T and T^*. On the other hand, the earlier definition is more natural for such constructions as $|(4,4)/(4,3)/(4,1)|^3$, where the set $T^* = (4,1)+[(4,4)/(4,3)]$ has no particular significance.

From this expression and Lemma 3, we have the distance bounds

$$
\begin{aligned}
&\min[d(V), 2d(T), 3d(T^*)] \\
&\qquad \ge d(|T \nabla T^*|^3) \ge \min[d(V), 2d(T), 3d(S)],
\end{aligned}
$$

so that if we want to improve on the lower bound, we will need to choose T^* (or $[S/T]$) so that $d(T^*) > d(S)$.

For the repetition and parity-check 3-constructions, the above form reduces to

$$
\begin{aligned}
|S/T/T|^3 &= G_{(3,2)}T + G_{(3,1)}(T+[S/T]) \\
&= G_{(3,2)}T + G_{(3,1)}S = |T \nabla S|^3 \\
|T/T/V|^3 &= G_{(3,2)}(V+[T/V]) + G_{(3,1)}V \\
&= G_{(3,2)}T + G_{(3,1)}V = |T \nabla V|^3,
\end{aligned}
$$

showing that in these cases the choice of coset representatives does not matter.

The cubing construction is not self-dual in general, when applied to binary groups; that is, it is not necessarily true that the dual of $|S/T/V|^3$ is $|V^\perp/T^\perp/S^\perp|^3$. In fact, if $\boldsymbol{u} \in G_{(3,2)}T + G_{(3,1)}(V+[S/T])$ and $\boldsymbol{u}' \in G_{(3,2)}T^\perp + G_{(3,1)}(S^\perp + [V^\perp/T^\perp])$ are elements of $|S/T/V|^3$ and $|V^\perp/T^\perp/S^\perp|^3$, respectively, then their inner product $(\boldsymbol{u}, \boldsymbol{u}')$ can be seen to be equal to $(\boldsymbol{d}, \boldsymbol{d}^\perp)$, if $\boldsymbol{d}$ and $\boldsymbol{d}^\perp$ are the elements of $[S/T]$ and $[V^\perp/T^\perp]$ that enter into the construction of $\boldsymbol{u}$ and $\boldsymbol{u}'$, respectively, when all elements of S/T and T/V are of order 2. Hence these two cubing

constructions are each others' duals when and only when it is possible to choose systems of coset representatives $[S/T]$ and $[V^{\perp}/T^{\perp}]$ such that every element of $[S/T]$ is orthogonal to every element of $[V^{\perp}/T^{\perp}]$. (However, it is true that $|T \nabla T^*|^3$ is the dual of $|T^{\perp} \nabla (T^*)^{\perp}|^3$, at least when all elements of S/T and T/V are of order 2; consequently, the repetition and parity-check 3-constructions are duals, $(|S/T/T|^3)^{\perp} = |T^{\perp}/T^{\perp}/S^{\perp}|^3$, or $(|T \nabla S|^3)^{\perp} = |T^{\perp} \nabla S^{\perp}|^3$.)

Examples: Let $(2,2)/(2,1)/(2,0)$ be the partition chain of binary length-2 codes considered earlier, and let $\boldsymbol{g}_0 = [10]$ be the generator for $(2,2)/(2,1)$, and $\boldsymbol{g}_1 = [11]$ the generator for $(2,1)$. The cubing construction applied to this partition chain yields a $(6,3)$ code with generator matrix $G_{(3,2)}\boldsymbol{g}_1 + G_{(3,1)}\boldsymbol{g}_0$ with minimum distance at least 3, and in fact since $G_{(3,1)}\boldsymbol{g}_0 = [101010]$, the minimum distance is three. Although the chain $(2,2)/(2,1)/(2,0)$ is self-dual, this $(6,3,3)$ code is not self-dual, because $(\boldsymbol{g}_0, \boldsymbol{g}_0) = 1$. However, if we construct another code $(6,3,3)^*$ by using the cubing construction on the same chain, but with the generator $\boldsymbol{g}_0' = [01]$ for $(2,2)/(2,1)$, then since $(\boldsymbol{g}_0, \boldsymbol{g}_0') = 0$, the $(6,3)$ and $(6,3)^*$ codes are duals. (The $(2,1,1)$ code generated by $\boldsymbol{g}_0$ is dual to the $(2,1,1)^*$ code generated by $\boldsymbol{g}_0'$.)

Secondly, let $(2,2)/(2,1)/(2,0)$ be the partition chain of length-2 generalized Reed–Muller codes over the field GF(4). Choose $\boldsymbol{g}_0 = [\omega \omega^*]$ as the generator for $(2,2)/(2,1)$, where ω and its conjugate ω^* are the elements of GF(4) other than zero and one, and again let $\boldsymbol{g}_1 = [11]$ be the generator for the $(2,1)$ code. The cubing construction applied to this partition chain yields a $(6,3)$ code with generator matrix $G_{(3,2)}\boldsymbol{g}_1 + G_{(3,1)}\boldsymbol{g}_0$ with minimum distance at least three. In fact, it is possible to show that all codewords must have even weight, so the minimum distance is four, and this is the $(6,3,4)$ hexacode over GF(4). Now, defining the inner product as the sum of products of the components of one vector with the conjugate of the components of the other, $\boldsymbol{g}_0$ is orthogonal to itself over GF(4), so the hexacode is self-dual. (Both the $(2,1,2)$ code generated by $\boldsymbol{g}_1$ and the $(2,1,2)^*$ code generated by $\boldsymbol{g}_0$ are self-dual.) Since $(2,2)/(2,1)/(2,0)$ is a chain of four-way partitions in this case, the hexacode has a 16-state three-section trellis diagram.

VI. Binary Codes and Lattices of Length $3 \cdot 2^n$

The constructions of Section V may be applied to the codes and lattices of Section IV to generate binary codes and lattices of length $N = 3 \cdot 2^n$. We shall briefly discuss the codes obtained for $N = 3$, 6, 12, and 24. We omit the corresponding lattice constructions.

The $(24,12)$ code obtained by the cubing construction $|(8,7)/(8,4)/(8,1)|^3$ has a minimum distance of only six if the standard coset representatives for the partition $(8,7)/(8,4)$ are used. We observe that there is an alternative choice of coset representatives that produces a $(24,12)$ code of minimum distance 8, namely the Golay code. Similarly, a nonstandard choice of coset representatives for the partition E_8/RE_8 in the cubing construction $|E_8/RE_8/2E_8|^3$ produces the 24-dimensional Leech lattice, which occupies an even more remarkable place among lattices than the Golay code does among binary codes. These constructions lead to three-section trellis diagrams for the Golay code and the Leech lattice that have only 64 and 256 states, respectively, and that in both cases lead to efficient maximum likelihood decoding algorithms.

A. Codes of Length $3 \cdot 2^n$

The $(3,1)$ and $(3,2)$ codes may be obtained from the Reed–Muller codes of length 1 by the trivial constructions $|(1,1)/(1,0)/(1,0)|^3$ and $|(1,1)/(1,1)/(1,0)|^3$, respectively, while even more trivially $(3,3) = (1,1)^3$ and $(3,0) = (1,0)^3$. Their nesting properties, minimum distances, $|a + x|b + x|a + b + x|$ representations, generator matrices, trellis diagrams, and duality properties are all determined as special cases of the general properties of their constructions. In particular, the $(3,1)$ and $(3,2)$ codes have minimum distances 3 and 2; they each have a two-state trellis diagram; and they are duals of each other.

Fig. 19 shows all codes of lengths 3, 6, 12, and 24 that can be derived in this way, with their minimum distances and their subcode relationships.

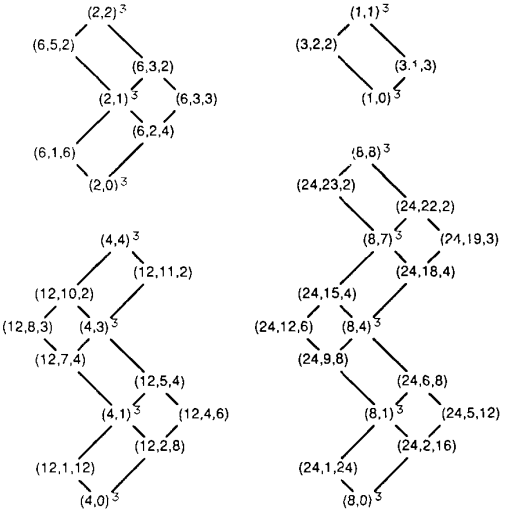


Fig. 19. Codes of lengths 3, 6, 12, and 24 generated by cubing construction.

We note that Fig. 19 illustrates the general properties of the constructions shown in Fig. 17. The codes of a given length that are formed by parity-check constructions form a partition chain, as do those formed by repetition constructions, but the codes formed by full cubing constructions are, in general, subcodes not of the next higher such code but of the code two levels higher.

Of these codes, the best with distances equal to powers of two are those constructed by parity-check constructions, while the best with distances equal to three times a power of two are those constructed by full cubing construc-

tions. The repetition construction nowhere produces the best code, except for the elementary cases $(3N,1) = |(N,1)/(N,0)/(N,0)|^3$. However, the repetition codes do serve as the duals of the parity-check codes.

The cubing construction codes have the right dimensions to be duals of each other but are not, as can be verified by examining inner products $(\boldsymbol{d}, \boldsymbol{d}^\perp)$. For example, we have already seen that the (6,3) code is not self-dual, but rather is dual to a closely related code $(6,3)^*$ that can also be expressed as $|(2,2)/(2,1)/(2,0)|^3$, but with a different coset representative for the partition $(2,2)/(2,1)$. In general, there do exist cubing construction codes of the dimensions shown here that are duals of each other, including self-dual codes of dimension half their length, but we must choose nonstandard coset representatives $[\mathrm{RM}(r,n)/\mathrm{RM}(r-1,n)]^*$ to obtain them. This will be illustrated in the next section for the (24,12) Golay code.

B. The (8,4)* Code and the Golay Code

The reason that the (24,12) code obtained by the cubing construction $|(8,7)/(8,4)/(8,1)|^3$ has a minimum distance of only six is that the standard system of coset representatives $[(8,7)/(8,4)]$, namely the words generated by the three rows $G_{(8,7)/(8,4)}$ of weight 2 in $G_{(8,8)} = G_{(2,2)}^3$, lead to codewords $G_{(3,1)}\boldsymbol{d} = (\boldsymbol{d}, \boldsymbol{d}, \boldsymbol{d})$ of weight 6. Furthermore, the reason that this code is not self-dual is that there are coset representatives in $[(8,7)/(8,4)]$ that are not orthogonal to each other modulo 2, e.g., [11000000] and [10100000].

Therefore, we introduce another basis $G_{(8,8)}^*$ for binary 8-space that has many attractive properties. In addition to the standard matrices $G_{(8,1)}$ and $G_{(8,4)/(8,1)}$, it includes nonstandard generator matrices $G_{(8,7)/(8,4)}^*$ and $G_{(8,8)/(8,7)}^*$, as follows:

$$G_{(8,8)}^* \triangleq \left\{ G_{(8,8)/(8,7)}^*, G_{(8,7)/(8,4)}^*, G_{(8,4)/(8,1)}, G_{(8,1)} \right\}$$

where

$$G_{(8,8)/(8,7)}^* \triangleq \begin{bmatrix} 1111 & 1110 \end{bmatrix}$$

$$G_{(8,7)/(8,4)}^* \triangleq \begin{bmatrix} 0111 & 1000 \\ 1001 & 1100 \\ 0101 & 0110 \end{bmatrix}$$

$$G_{(8,4)/(8,1)} = \begin{bmatrix} 1111 & 0000 \\ 1100 & 1100 \\ 1010 & 1010 \end{bmatrix}$$

$$G_{(8,1)} = \begin{bmatrix} 1111 & 1111 \end{bmatrix}.$$

Note that all generators are linearly independent, so that the complete set generates the (8,8) code; since all 8-tuples in $G_{(8,7)/(8,4)}^*$ have even weight, the last seven generators generate the (8,7,2) code. The four generators $\{G_{(8,1)}, G_{(8,7)/(8,4)}^*\}$ generate an (8,4) code, and since the columns of $G_{(8,7)/(8,4)}^*$ run through all 3-tuples, $G_{(8,7)/(8,4)}^*$ is a column permutation of $G_{(8,4)/(8,1)}$, so this is a permutation of the (8,4,4) code, which we shall denote as $(8,4,4)^*$. Fig. 20 illustrates alternative partition chains $(8,8)/(8,7)/(8,4)/(8,1)/(8,0)$ and $(8,8)/(8,7)/(8,4)^*/(8,1)/(8,0)$ that may be obtained with these generators.

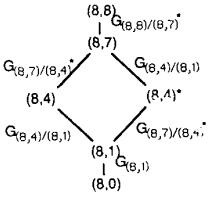


Fig. 20. Alternative partition chains $(8,8)/(8,7)/(8,4)/(8,1)/(8,0)$ and $(8,8)/(8,7)/(8,4)^*/(8,1)/(8,0)$.

(Note that $G_{(8,8)/(8,7)}^*$ has been chosen so that the seven generators $G_{(7,7)}^* \triangleq \{G_{(8,4)/(8,1)}, G_{(8,7)/(8,4)}^*, G_{(8,8)/(8,7)}^*\}$ generate all the good codes of length 7, including (7,6,2), (7,4,3), $(7,4,3)^*$, (7,3,4), $(7,3,4)^*$, and (7,1,7) codes, if we disregard the last component which is always zero.)

The generator matrix

$$G_{(8,7)}^* \triangleq \left\{ G_{(8,1)}, G_{(8,4)/(8,1)}, G_{(8,7)/(8,4)}^* \right\}$$

for the (8,7,2) code has the following nice properties, which characterize all of the inner products of the generators:

a) the weights of all seven generators are multiples of four;
b) all generators are orthogonal modulo 2, except for the pairs

$$\boldsymbol{g}_1 = 1111\ 0000 \qquad \boldsymbol{g}_1^* = 0111\ 1000$$
$$\boldsymbol{g}_2 = 1100\ 1100 \qquad \boldsymbol{g}_2^* = 1001\ 1100$$
$$\boldsymbol{g}_3 = 1010\ 1010 \qquad \boldsymbol{g}_3^* = 0101\ 0110.$$

Since $G_{(8,7)}^*$ is a generator matrix for the (8,7) code, any codeword $\boldsymbol{c}$ in that code can be uniquely represented as

$$\boldsymbol{c}(a_0, \boldsymbol{a}, \boldsymbol{a}^*) = a_0 G_{(8,1)} + \boldsymbol{a} G_{(8,4)/(8,1)} + \boldsymbol{a}^* G_{(8,7)/(8,4)}^* \pmod 2$$

so that $(a_0, \boldsymbol{a}, \boldsymbol{a}^*)$ is a 7-bit label for $\boldsymbol{c}$. In view of the inner product properties of the generators, the inner product of two (8,7) codewords satisfies

$$(\boldsymbol{c}_1, \boldsymbol{c}_2) \equiv (\boldsymbol{a}_1, \boldsymbol{a}_2^*) + (\boldsymbol{a}_1^*, \boldsymbol{a}_2) \pmod 2$$

where $\boldsymbol{c}_1 = \boldsymbol{c}(a_{01}, \boldsymbol{a}_1, \boldsymbol{a}_1^*)$ and $\boldsymbol{c}_2 = \boldsymbol{c}(a_{02}, \boldsymbol{a}_2, \boldsymbol{a}_2^*)$.

The codewords in the (8,4) code are the words in the (8,7) code with $\boldsymbol{a}^* = \boldsymbol{0}$, and those in the $(8,4)^*$ code are those with $\boldsymbol{a} = \boldsymbol{0}$. If $\boldsymbol{c}$ is an (8,4) codeword, then its weight $\|\boldsymbol{c}\|^2 = \sum_{jk} a_j a_k (\boldsymbol{g}_j, \boldsymbol{g}_k)$ contains diagonal terms which are multiples of four, plus twice the cross product terms, which are all multiples of two, so the weight of any (8,4) codeword is a multiple of four. Similarly, the weight of any $(8,4)^*$ codeword $\boldsymbol{c}^*$ is a multiple of four.

Now let $\boldsymbol{c} = \boldsymbol{c}(a_{01}, \boldsymbol{a}, \boldsymbol{0})$ be an (8,4) codeword, and let $\boldsymbol{c}^* = \boldsymbol{c}(a_{02}, \boldsymbol{0}, \boldsymbol{a}^*)$ be an $(8,4)^*$ codeword. The weight of their mod-2 sum $\boldsymbol{c} \oplus \boldsymbol{c}^*$ is governed by the following lemma.

Lemma 4: If $\boldsymbol{c}(a_{01}, \boldsymbol{a}, \boldsymbol{0}) \in (8,4)$ and $\boldsymbol{c}(a_{02}, \boldsymbol{0}, \boldsymbol{a}^*) \in (8,4)^*$, then the weight of their mod-2 sum $\|\boldsymbol{c} \oplus \boldsymbol{c}^*\|^2$ is congruent to $2(\boldsymbol{a}, \boldsymbol{a}^*)$ modulo 4.

Proof: If $\boldsymbol{c}$ and $\boldsymbol{c}^*$ are regarded as integer 8-tuples, then $\|\boldsymbol{c} \oplus \boldsymbol{c}^*\|^2$ is equal to the Euclidean distance

$$\|\boldsymbol{c} - \boldsymbol{c}^*\|^2 = \|\boldsymbol{c}\|^2 - 2(\boldsymbol{c}, \boldsymbol{c}^*) + \|\boldsymbol{c}^*\|^2.$$

However, $\|c\|^2$ and $\|c^*\|^2$ are both multiples of four, and $(c, c^*) \equiv (a, a^*) \pmod 2$.

The (8,7) code may be regarded as the union of 64 cosets $(8,1) + c(a, a^*)$ of the (8,1) code, where $c(a, a^*) = aG_{(8,4)/(8,1)} + a^*G^*_{(8,7)/(8,4)} \pmod 2$. Each coset thus consists of $c(a, a^*)$ and its complement. This implies that these 64 cosets fall into the following classes:

a) one class ($a = a^* = \mathbf{0}$) in which both weights are multiples of 8, i.e., 0 and 8;
b) $7 \times 4 = 28$ classes ($(a, a^*) \equiv 1 \bmod 2$) in which both weights are congruent to 2 modulo 4, i.e., 2 and 6;
c) 35 classes ($(a, a^*) \equiv 0 \bmod 2$, but not $a = a^* = \mathbf{0}$) in which both weights are congruent to 0 modulo 4, i.e., 4 and 4.

The following eight-by-eight map shows exactly where the numbers of these classes are located, where octal notation is used for a and a^*, and **0** indicates class a), 1 indicates b), and 0 indicates c):

	a^*							
a	0	1	2	3	4	5	6	7
0	**0**	0	0	0	0	0	0	0
1	0	1	0	1	0	1	0	1
2	0	0	1	1	0	0	1	1
3	0	1	1	0	0	1	1	0
4	0	0	0	0	1	1	1	1
5	0	1	0	1	1	0	1	0
6	0	0	1	1	1	1	0	0
7	0	1	1	0	1	0	0	1

The Golay code may now be defined by the cubing construction $|(8,7)/(8,4)/(8,1)|^3$, using as the system of coset representatives for $[(8,7)/(8,4)]$ the words generated by $G^*_{(8,7)/(8,4)}$ or, equivalently, by the $|a + x|b + x|a + b + x|$ construction

$$\begin{aligned}(24,12) &\triangleq |(8,4) \triangledown (8,4)^*|^3 \\ &= \{(c_1 + c^*, c_1 + c_2 + c^*, c_2 + c^*): \\ &\qquad c_1, c_2 \in (8,4),\ c^* \in (8,4)^*\},\end{aligned}$$

with addition modulo 2. (This is a "Turyn construction" [5, ch. 18, sec. 7.4] (see also Sloane *et al.* [18]).) The generator matrix corresponding to the cubing construction $|(8,7)/(8,4)/(8,1)|^3$ is

$$G_{(24,12)} = G_{(3,3)}G_{(8,1)} + G_{(3,2)}G_{(8,4)/(8,1)} + G_{(3,1)}G_{(8,4)^*/(8,1)}$$

where as always the expression is to be interpreted as a union of Kronecker products, and we have used the notation $G_{(8,4)^*/(8,1)}$ for $G^*_{(8,7)/(8,4)}$; the generator matrix can also be written as

$$G_{(24,12)} = G_{(3,2)}G_{(8,4)} + G_{(3,1)}G_{(8,4)^*},$$

corresponding to the $|(8,4) \triangledown (8,4)^*|^3$ form of the construction.

This (24,12) code has minimum distance 8, which may be proved as follows. Let $c = (c_1 + c^*, c_1 + c_2 + c^*, c_2 + c^*)$ be a codeword. Each of the 8-tuples is the mod-2 sum of an (8,4) codeword and an (8,4)* codeword. Using Lemma 4, therefore,

$$\begin{aligned}\|c\|^2 &\equiv 2(a_1, a^*) + 2(a_1 + a_2, a^*) + 2(a_2, a^*) \pmod 4 \\ &= 4(a_1 + a_2, a^*) \\ &\equiv 0 \pmod 4.\end{aligned}$$

Thus all weights are multiples of four. By the cubing construction lower bound of Lemma 3, however, the minimum distance is at least six; therefore, it must be eight. (Since each 8-tuple is an (8,7) codeword, minimum-weight codewords must have weights 2, 2, and 4 or 0, 0, and 8 in their three 8-tuple components.)

This (24,12) code is self-dual, because both the (8,4) and (8,4)* codes are self-dual. It is part of the self-dual partition chain $(24,15)/(24,12)/(24,9)$; i.e., it is a union of eight cosets of $(24,9) = |(8,4)/(8,4)/(8,1)|^3$, and $(24,15) = |(8,7)/(8,4)/(8,4)|^3$ is a union of eight cosets of (24,12).

Fig. 21 is a schematic trellis diagram for the Golay code, based on the cubing construction. It has 64 states (a, a^*) at each section boundary, where $aG_{(8,4)/(8,1)} \in [(8,4)/(8,1)]$ and $a^*G_{(8,4)^*/(8,1)} \in [(8,4)^*/(8,1)]$. It may be regarded as a union of eight subtrellises, each subtrellis representing a coset of the eight-state (24,9) code and having a coset representative (d^*, d^*, d^*), where $d^* = a^*G_{(8,4)^*/(8,1)}$. Each branch represents a coset of the (8,1) code and thus represents two 8-tuples which are binary complements of each other.

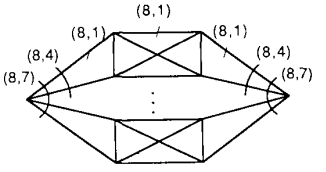


Fig. 21. Three-section 64-state trellis diagram for (24,12,8) Golay code.

C. R^*E_8 and the Leech Lattice

The Leech lattice is a 24-dimensional lattice that seems to be the most remarkable lattice of all. It is exceptionally dense for its dimension, it contains all good lattices of lower dimension, and it plays a pivotal role in the mathematical theory of lattices (and of finite groups).

In a development analogous to that of the previous section, we shall now show that the Leech lattice Λ_{24} is expressible as a cubing construction $|E_8/RE_8/2E_8|^3$, if we replace the standard coset representatives for E_8/RE_8 by another system $[E_8/RE_8]^*$.

In this case we introduce as our *deus ex machina* the following set of eight 8-dimensional generators. We may call them small miracle octad generators (SMOG's) in analogy to the well-known set of twenty-four 24-dimensional miracle octad generators that is often used for Leech lattice manipulations (Conway and Sloane [2]) and to which they are intimately related. In addition to the standard generators $G = \{G_{(8,1)}, 2G_{(8,7)/(8,4)}\}$ for $RE_8/2E_8$,

they include a nonstandard set G^* for E_8/RE_8, as follows:

$$G_{E_8/2E_8} \triangleq \{G^*, G\}$$

$$G^* = \begin{bmatrix} 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 2 & 0 & 0 & 0 \\ 1 & -1 & 2 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & -1 & 2 \end{bmatrix} \begin{matrix} \triangleq \boldsymbol{g}_0^* \\ \triangleq \boldsymbol{g}_1^* \\ \triangleq \boldsymbol{g}_2^* \\ \triangleq \boldsymbol{g}_3^* \end{matrix}$$

$$G \triangleq \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{matrix} \triangleq \boldsymbol{g}_0 \\ \triangleq \boldsymbol{g}_1 \\ \triangleq \boldsymbol{g}_2 \\ \triangleq \boldsymbol{g}_3 \end{matrix}.$$

That these are a generator matrix for $E_8/2E_8$ can be seen as follows. G is a standard generator matrix for $RE_8/2E_8$. $RE_8 + [\boldsymbol{g}_0^*]$ is the lattice $RD_8^{\perp} = 2\boldsymbol{Z}^8 + (8,1)$, because $\boldsymbol{g}_0^* = [11111111] - [02020200]$, and the latter 8-tuple with $2G_{(8,7)/(8,4)}$ generates $2\boldsymbol{Z}^8/2E_8$. The remaining three generators, $G_1^* = \{\boldsymbol{g}_1^*, \boldsymbol{g}_2^*, \boldsymbol{g}_3^*\}$, are congruent modulo 2 to the standard generators $G_{(8,4)/(8,1)}$ for $E_8/RD_8^{\perp}$. Thus the SMOG's generate a system of coset representatives for $E_8/2E_8$. They are linearly independent, thus a basis for 8-space. The generators G^* are in fact also generators for $E_8/2\boldsymbol{Z}^2$, since they are congruent to the standard generators modulo 2.

The lattice R^*E_8 is defined as $R^*E_8 \triangleq 2E_8 + \{\boldsymbol{a}G^*\}$, meaning (as usual) that R^*E_8 is the union of the 16 cosets of $2E_8$ whose representatives are the binary linear combinations of the generators in G^*. Then $E_8 = R^*E_8 + \{\boldsymbol{a}G\}$, so we have the alternative partitions illustrated in Fig. 22. We shall show shortly that $d^2_{\min}(R^*E_8) = 8$, the same as $d^2_{\min}(RE_8)$, so R^*E_8 has the same coding gain as RE_8 or E_8, and since E_8 is the unique eight-dimensional lattice with this coding gain [2], this implies that R^*E_8 must be a version of E_8.

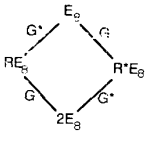


Fig. 22. Alternative partition chains $E_8/RE_8/2E_8$ and $E_8/R^*E_8/2E_8$.

The eight generators $\{G, G^*\}$ have the following nice properties, which characterize all of the inner products of the generators:

a) the weights of all generators are multiples of eight;
b) all generators are orthogonal modulo 4, except for the pairs $(\boldsymbol{g}_k, \boldsymbol{g}_k^*)$, $0 \le k \le 3$, whose inner products are congruent to 2 modulo 4.

Since $\{G, G^*\}$ is a generator matrix for $E_8/2E_8$, the 256 cosets $2E_8 + \boldsymbol{c}$ of $2E_8$ whose union is E_8 can be uniquely represented as

$$\boldsymbol{c}(\boldsymbol{a}, \boldsymbol{a}^*) \equiv \boldsymbol{a}G + \boldsymbol{a}^*G^* \pmod{2E_8},$$

so that $(\boldsymbol{a}, \boldsymbol{a}^*)$ is an 8-bit label for the coset $2E_8 + \boldsymbol{c}(\boldsymbol{a}, \boldsymbol{a}^*)$. In view of the inner product properties of the generators, the inner product of two elements of E_8 satisfies

$$(\boldsymbol{c}_1, \boldsymbol{c}_2) \equiv 2(\boldsymbol{a}_1, \boldsymbol{a}_2^*) + 2(\boldsymbol{a}_1^*, \boldsymbol{a}_2) \pmod 4$$

where $\boldsymbol{c}_1$ is an element of the coset $2E_8 + \boldsymbol{c}(\boldsymbol{a}_1, \boldsymbol{a}_1^*)$ and $\boldsymbol{c}_2$ is an element of the coset $2E_8 + \boldsymbol{c}(\boldsymbol{a}_2, \boldsymbol{a}_2^*)$, and we use the fact that any element of E_8 is orthogonal to any element of $2E_8$ modulo 4 (since $\boldsymbol{Z}^8/E_8/RE_8/2E_8/4\boldsymbol{Z}^8$ is a self-dual partition chain modulo 4).

The elements of RE_8 are the union of the 16 cosets of $2E_8$ with $\boldsymbol{a}^* = \boldsymbol{0}$, and those in R^*E_8 are those with $\boldsymbol{a} = \boldsymbol{0}$. The inner products of any two elements of RE_8 (resp. R^*E_8) are thus congruent to 0 modulo 4. Since the weights of all generators are eight, this suffices to show that the weight of any element of RE_8 (resp. R^*E_8) is a multiple of eight. In turn, this shows that $d^2_{\min}(R^*E_8) = 8$, as claimed.

Now let $\boldsymbol{c}$ be an element of RE_8 in some coset $2E_8 + \boldsymbol{c}(\boldsymbol{a}, \boldsymbol{0})$ of $2E_8$, and let $\boldsymbol{c}^*$ be an element of R^*E_8 in some coset $2E_8 + \boldsymbol{c}(\boldsymbol{0}, \boldsymbol{a}^*)$ of $2E_8$. Their squared distance is governed by the following lemma.

Lemma 5: If $\boldsymbol{c} \in 2E_8 + \boldsymbol{c}(\boldsymbol{a}, \boldsymbol{0})$ and $\boldsymbol{c}^* \in 2E_8 + \boldsymbol{c}(\boldsymbol{0}, \boldsymbol{a}^*)$, then $\|\boldsymbol{c} - \boldsymbol{c}^*\|^2$ is congruent to $4(\boldsymbol{a}, \boldsymbol{a}^*)$ modulo 8.

Proof: $\|\boldsymbol{c} - \boldsymbol{c}^*\|^2 = \|\boldsymbol{c}\|^2 - 2(\boldsymbol{c}, \boldsymbol{c}^*) + \|\boldsymbol{c}^*\|^2$; but $\|\boldsymbol{c}\|^2$ and $\|\boldsymbol{c}^*\|^2$ are both equal to multiples of eight, and $(\boldsymbol{c}, \boldsymbol{c}^*) \equiv 2(\boldsymbol{a}, \boldsymbol{a}^*) \pmod 4$.

This implies that the 256 cosets $2E_8 + \boldsymbol{c}(\boldsymbol{a}, \boldsymbol{a}^*)$ fall into the following classes:

a) one class ($\boldsymbol{a} = \boldsymbol{a}^* = \boldsymbol{0}$) in which all weights are multiples of 16;
b) $15 \times 8 = 120$ classes ($(\boldsymbol{a}, \boldsymbol{a}^*) \equiv 1 \bmod 2$) in which all weights are congruent to 4 modulo 8;
c) 135 classes ($(\boldsymbol{a}, \boldsymbol{a}^*) \equiv 0 \bmod 2$ but not $\boldsymbol{a} = \boldsymbol{a}^* = \boldsymbol{0}$) in which all weights are congruent to 0 modulo 8.

The Leech lattice may now be defined by the cubing construction $|E_8/RE_8/2E_8|^3$, using as the system of coset representatives for $[E_8/RE_8]$ the 16 8-tuples generated by G^* or, equivalently, by the $|a + x|b + x|a + b + x|$ construction

$$\Lambda_{24} \triangleq |RE_8 \triangledown R^*E_8|^3 = \{(\boldsymbol{c}_1 + \boldsymbol{c}^*, \boldsymbol{c}_1 + \boldsymbol{c}_2 + \boldsymbol{c}^*, \boldsymbol{c}_2 + \boldsymbol{c}^*): \boldsymbol{c}_1, \boldsymbol{c}_2 \in RE_8, \boldsymbol{c}^* \in R^*E_8\}$$

with ordinary vector addition. (This is a generalized Turyn construction; see [2, ch. 8, sec. 2] and the references therein.) The generator matrix corresponding to the cubing construction $|E_8/RE_8/2E_8|^3$ is

$$G_{\Lambda_{24}} = G_{(3,3)}G_{2E_8} + G_{(3,2)}G + G_{(3,1)}G^*$$

where, as usual, the expression is to be interpreted as a union of Kronecker products. Thus Λ_{24} is a union of 2^{12} cosets of $2E_8^3$, and E_8^3 is a union of 2^{12} cosets of Λ_{24}. The generator matrix can also be written as

$$G_{\Lambda_{24}} = G_{(3,2)}G_{RE_8} + G_{(3,1)}G_{R^*E_8},$$

corresponding to the $|RE_8 \triangledown R^*E_8|^3$ form of the construction.

The Leech lattice is self-dual modulo 4, because both RE_8 and R^*E_8 are self-dual modulo 4.

The Leech lattice has minimum squared distance 16, which may be proved as follows. Let $\lambda = (c_1 + c^*, c_1 + c_2 + c^*, c_2 + c^*)$ be a point in the lattice, where $c_1, c_2 \in RE_8$, $c^* \in R^*E_8$. Each of the 8-tuples is the sum of an element of RE_8 and an element of R^*E_8. Using Lemma 5, therefore,

$$\begin{aligned}\|\lambda\|^2 &\equiv 4(a_1, a^*) + 4(a_1 + a_2, a^*) + 4(a_2, a^*) \pmod 8 \\ &= 8(a_1 + a_2, a^*) \\ &\equiv 0 \pmod 8.\end{aligned}$$

Thus all weights are multiples of eight. By the cubing construction lower bound of Lemma 3, however, the minimum distance is at least 12; therefore, it must be 16. (Since each 8-tuple is an element of E_8, minimum-weight codewords must have weights 4, 4, and 8 or 0, 0, and 16 in their three 8-tuple components.)

Since $\boldsymbol{Z}^{24}/E_8^3/\Lambda_{24}/2E_8^3/4\boldsymbol{Z}^{24}$ is a chain of 2^{12}-way partitions, and $d^2_{\min}(\Lambda_{24}) = 16$, its coding gain is $\gamma(\Lambda_{24}) = 16 \cdot 2^{-24/12} = 4$ (6 dB). This is the same normalized density as is achieved in 32 dimensions by the Barnes–Wall lattice Λ_{32} and is very close to a sphere-packing bound called the Rogers bound [2]. Λ_{24} is exceptionally dense for its dimension.

Fig. 23 is a schematic trellis diagram for the Leech lattice based on the cubing construction. It has 256 states (a, a^*) at each section boundary, where $aG \in [RE_8/2E_8]$ and $a^*G^* \in [R^*E_8/2E_8]$. Each branch represents a coset of $2E_8$, and the 256 distinct branches in each section represent the cosets in the partition $E_8/RE_8/2E_8$. There are a total of 2^{12} paths through the trellis, representing the 2^{12} cosets of $2E_8^3$ of which Λ_{24} is the union. The trellis may be regarded as a union of 16 subtrellises, each subtrellis representing a coset of the 16-state lattice $|RE_8/RE_8/2E_8|^3$ whose code formula is $4\boldsymbol{Z}^{24} + 2(24,18,4) + (24,2,16)$ and having a coset representative (d^*, d^*, d^*), where $d^* = a^*G^*$. The trellis is identical in form to that for $\Lambda_{32} = |E_8/RE_8/2E_8|^4$, except that it has three sections rather than four.

The Leech lattice is more commonly encountered in the rotated form $R\Lambda_{24}$, defined as $R\Lambda_{24} = |RE_8/2E_8/2RE_8|^3 = |2E_8 \triangledown RR^*E_8|^3$ where we use the rotated SMOG's:

$$RG_{E_8/2E_8} = G_{RE_8/2RE_8} = \{RG^*, RG\}$$

$$RG^* = \begin{bmatrix} 0 & 2 & 0 & 2 & 0 & 2 & 2 & 0 \\ 2 & 0 & 0 & 2 & 2 & 2 & 0 & 0 \\ 0 & 2 & 2 & 2 & 2 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & -3 \end{bmatrix} \begin{matrix} = Rg_0^* \\ = Rg_1^* \\ = Rg_2^* \\ = Rg_3^* \end{matrix}$$

$$RG = \begin{bmatrix} 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 \\ 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 \\ 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{matrix} = Rg_0 \\ = Rg_1 \\ = Rg_2 \\ = Rg_3 \end{matrix}$$

The generators in RG are now the standard generators $\{2G_{(8,4)/(8,1)}, 4G_{(8,8)/(8,7)}\}$ for $2E_8/2RE_8$, while the generators in RG^* are a nonstandard set $\{2G^*_{(8,7)/(8,4)}, G^*_{(8,1)}\}$ for $RE_8/2E_8$, consisting of twice the generators $G^*_{(8,7)/(8,4)}$ for $(8,4)^*/(8,1)$ that we used earlier, plus a special generator Rg_3^*, which is the only one with odd components.

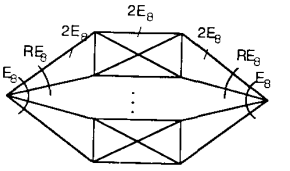


Fig. 23. Three-section 256-state trellis diagram for Leech lattice $\Lambda_{24} = |E_8/RE_8/2E_8|^3 = |RE_8 \triangledown R^*E_8|^3$.

In this representation, the rotated Leech lattice $R\Lambda_{24}$ has minimum squared distance 32 and is self-dual modulo 8. The generator matrix corresponding to the cubing construction $|E_8/RE_8/2E_8|^3$ is

$$G_{R\Lambda_{24}} = G_{(3,3)}G_{2RE_8} + G_{(3,2)}RG + G_{(3,1)}RG^*,$$

from which the miracle octad generators can easily be obtained, and the generator matrix corresponding to the $|2E_8 \triangledown RR^*E_8|^3$ construction is

$$G_{R\Lambda_{24}} = G_{(3,2)}G_{2E_8} + G_{(3,1)}G_{RR^*E_8}.$$

(The lattice RR^*E_8 is simply a rotated version of R^*E_8, $RR^*E_8 = 2RE_8 + \{aRG^*\}$.)

The lattices Λ_{24} and $R\Lambda_{24}$ are indecomposable [1], but we may nonetheless characterize them by code formulas under a broadened definition. Λ_{24} is the union of 2^{24} cosets of $4\boldsymbol{Z}^{24}$ whose representatives may be taken as the 2^{24} 24-tuples whose components are integers modulo 4 that are obtained by binary linear combinations of the 24 generators $\{2G_{(3,3)}G_{(8,4)}, G_{(3,2)}G, G_{(3,1)}G^*\}$, where the first 12 generators are simply the generators of $2E_8^3/4\boldsymbol{Z}^{24}$ in standard form, while the remaining 12 are the generators for $\Lambda_{24}/2E_8^3$, by the cubing construction. Of these 24 generators, 18 are multiples of two, namely, $2G_{(3,3)}G_{(8,4)} + 2G_{(3,2)}G_{(8,7)/(8,4)}$, which are the generators for the $(24,18,4)$ code $|(8,7)/(8,7)/(8,4)|^3$, multiplied by two. The remaining six generators are a set of six 24-tuples of integers modulo 4 whose binary linear combinations modulo 4 must all have weight at least 16, since all are Leech lattice vectors. Hence we may write

$$\Lambda_{24} = 4\boldsymbol{Z}^{24} + 2(24,18,4) + (24,6,16)'$$

where $(24,6,16)'$ is simply a notation for the 64 binary linear combinations (modulo 4) of the aforementioned set of six generators. Note that the generators of the $(24,6,16)'$ code are congruent to those of the binary $(24,6,8)$ code defined by $|(8,4)/(8,1)/(8,1)|^3$, which is dual to the $(24,18,4)$ code, and also a subcode of it.

Similarly, $R\Lambda_{24}$ is the union of 2^{24} cosets of $4R\boldsymbol{Z}^{24}$, or 2^{36} cosets of $8\boldsymbol{Z}^{24}$, whose representatives may be taken as the 2^{36} 24-tuples whose components are integers modulo 8 that are obtained by binary linear combinations of the 36 generators $\{G_{(3,3)}[4G_{(8,7)} + 2G_{(8,1)}], G_{(3,2)}RG, G_{(3,1)}RG^*\}$, where the first 24 generators are simply the generators of $2RE_8^3/8\boldsymbol{Z}^{24}$ in standard form. Of these 36 generators, 23 are multiples of four, namely $4G_{(3,3)}G_{(8,7)} + 4G_{(3,2)}G_{(8,8)/(8,7)}$, which are the generators for the $(24,23,2)$ code $|(8,8)/$

$(8,8)/(8,7)|^3$, multiplied by four. We then recognize a set of 12 generators which are those of the $(24,12,8)$ Golay code, multiplied by two, namely, $2G_{(3,3)}G_{(8,1)} + 2G_{(3,2)}G_{(8,4)/(8,1)} + 2G_{(3,1)}G_{(8,4)^*/(8,1)}$. The remaining generator $G_{(3,1)}R\boldsymbol{g}_3^*$ is a special "Leech generator" which we denote by $(24,1,32)'$. (Its weight is actually $16\times 3 = 48$, but there are elements in the coset $2RE_8 + (24,1,32)'$ of weight 32.) Hence we may write

$$R\Lambda_{24} = 8\boldsymbol{Z}^{24} + 4(24,23,2) + 2(24,12,8) + (24,1,32)'.$$

These code formulas show the existence of certain sublattices of Λ_{24} and $R\Lambda_{24}$ that can themselves be obtained by cubing constructions, as follows:

$$\begin{aligned} 2H_{24} &= 8\boldsymbol{Z}^{24} + 4(24,23,2) + 2(24,12,8) \\ &= |2D_8/2E_8/2RE_8|^3 \\ 2X_{24} &= 4\boldsymbol{Z}^{24} + 2(24,18,4) = |2D_8/2D_8/2E_8|^3 \\ 4D_{24} &= 8\boldsymbol{Z}^{24} + 4(24,23,2) = |4\boldsymbol{Z}^8/4\boldsymbol{Z}^8/4D_8|^3. \end{aligned}$$

(*Caution*: $R\Lambda_{24}$ is not a sublattice of Λ_{24}.) Thus there is a partition chain $\Lambda_{24}/RH_{24}/2X_{24}/2RD_{24}/4\boldsymbol{Z}^{24}$ of 24-dimensional lattices, all with minimum squared distances equal to 16, with partition orders 2, 2^5, 2^7, and 2^{11}.

A complex version of the Leech lattice can be defined by expressing the generators $\{G^*, G\}$ in complex form, using $\phi = 1+i$ and $\phi^* = 1-i$, as well as $\alpha = -1+2i$:

$$G^* = \begin{bmatrix} \phi^* & \phi^* & \phi^* & \phi \\ \phi & \phi^* & 2 & 0 \\ \phi^* & 2 & \phi & 0 \\ 1 & 1 & 1 & \alpha \end{bmatrix} \begin{matrix} = \boldsymbol{g}_0^* \\ = \boldsymbol{g}_1^* \\ = \boldsymbol{g}_2^* \\ = \boldsymbol{g}_3^* \end{matrix}$$

$$G = \begin{bmatrix} \phi & \phi & \phi & \phi \\ 2 & 0 & 2 & 0 \\ 2 & 2 & 0 & 0 \\ 2\phi & 0 & 0 & 0 \end{bmatrix} \begin{matrix} = \boldsymbol{g}_0 \\ = \boldsymbol{g}_1 \\ = \boldsymbol{g}_2 \\ = \boldsymbol{g}_3 \end{matrix}.$$

A complex code formula for Λ_{24} can be developed as follows. Λ_{24} is the union of 2^{24} cosets of $4\boldsymbol{G}^{12}$, whose representatives may be taken as the 2^{24} complex 12-tuples whose components are Gaussian integers modulo ϕ^4 (or modulo 4) obtained by binary linear combinations of the 24 generators $\{2G_{(3,3)}G_{(8,4)}, G_{(3,2)}G, G_{(3,1)}G^*\}$. The first 12 generators are the generators of $2E_8^3/4\boldsymbol{G}^{12}$ in standard form, which are obtainable from the code formula $2E_8 = 4\boldsymbol{G}^4 + 2\phi(4,3,2) + 2(4,1,4)$. Thus of the 24 generators, 11 are multiples of 2ϕ (or ϕ^3), namely, $2\phi(G_{(3,3)}G_{(4,3)} + G_{(3,2)}G_{(4,4)/(4,3)})$ which are the generators for the $(12,11,2)$ code $|(4,4)/(4,4)/(4,3)|^3$ multiplied by 2ϕ; seven are multiples of two (or ϕ^2), namely, $2(G_{(3,3)}G_{(4,4)/(4,3)} + G_{(3,2)}G_{(4,3)/(4,1)})$ which are the generators for the $(12,7,4)$ code $|(4,3)/(4,3)/(4,1)|^3$ multiplied by ϕ; five are multiples of ϕ, namely, $\phi(G_{(3,2)}G_{(4,1)} + G_{(3,2)}G_{(4,3)}^*)$ where $G_{(4,3)}^* = \{\boldsymbol{g}_0^*, \boldsymbol{g}_1^*, \boldsymbol{g}_2^*\}$, which we denote as $\phi(12,5,8)'$; and one final odd generator $G_{(3,1)}\boldsymbol{g}_0^*$, which we may denote as $(12,1,16)'$. (Again, these codes are congruent modulo 2 to the $(12,5,4)$ code $|(4,3)/(4,1)/(4,1)|^3$ and $(12,1,12)$ code $|(4,1)/(4,0)/(4,0)|^3$, respectively, which are the duals of the other codes in the code formula.) Hence we may write

$$\begin{aligned} \Lambda_{24} = 4\boldsymbol{G}^{12} &+ 2\phi(12,11,2) + 2(12,7,4) \\ &+ \phi(12,5,8)' + (12,1,16)'. \end{aligned}$$

Now the principal sublattices of the Leech lattice are simply defined as

$$\begin{aligned} H_{24} &= 2\phi\boldsymbol{G}^{12} + 2(12,11,2) + \phi(12,7,4) + (12,5,8)' \\ &= |D_8/E_8/RE_8|^3 \\ X_{24} &= 2\boldsymbol{G}^{12} + \phi(12,11,2) + (12,7,4) = |D_8/D_8/E_8|^3 \\ D_{24} &= \phi\boldsymbol{G}^{12} + (12,11,2) = |\boldsymbol{G}^4/\boldsymbol{G}^4/D_8|^3 \end{aligned}$$

and the existence and orders of the partition chain $\Lambda_{24}/\phi H_{24}/\phi^2 X_{24}/\phi^3 D_{24}/\phi^4\boldsymbol{G}^{12}$ follow immediately. The cubing construction expression shows that three-section trellis diagrams exist for these lattices with 128, 8, and 2 states, respectively. These are the same values as for their 32-dimensional relatives, except for X_{24}; this lattice achieves a coding gain of $\gamma(X_{24}) = 4\cdot 2^{-6/12} = 2^{3/2}$ (4.5 dB) with only eight states.

Notes: Much literature on the Leech lattice is available, and it is doubtful whether anything here is fundamentally new. In particular, an $|a+x|b+x|a+b+x|$ construction of Λ_{24} using two versions of E_8 is described as "well known" in [2, ch. 8, sec. 2]. We are not familiar with any previous use of the mod-4 SMOG's. The structure illustrated in the trellis diagram is also believed to be new.

VII. Nonlinear Constructions in Sixteen Dimensions

In general, for fewer than 32 dimensions, the best block codes are linear and the best packings are lattice packings. An exception occurs in 16 dimensions, where the best known binary block code with 256 codewords is the nonlinear Nordstrom–Robinson code, which has minimum Hamming distance 6 between codewords.

At one time, it was conjectured [19, pp. 336–337] that there might be an analogous nonlattice packing in 16 dimensions, consisting of 16 translates of the Barnes–Wall lattice Λ_{16} (in analogy to the Nordstrom–Robinson code, which can be expressed as eight translates of the $(16,5)$ first-order Reed–Muller code). This would imply numerous properties, including a coding gain that would be a factor of $3\cdot 2^{-3/2}$ (0.26 dB) greater than that of Λ_{16}. However, Conway and Sloane later showed in unpublished work that such a construction was possible with nine but no more than nine translates (see [2, ch. 7, th. 14]). This packing falls just short of the density of Λ_{16}. (If there were a construction consisting of ten translates, it would be denser.)

In this section, we first construct the Nordstrom–Robinson code using the nonstandard generators for two versions of the $(8,4)$ code that were used in the previous section in constructing the Golay code. We then give an analogous construction of a nine-translate nonlattice packing N_{16}, using the SMOG's for two versions of the E_8

lattice that were used in the previous section in constructing the Leech lattice. These constructions seem to fit naturally into the family of constructions that are the subject of this paper. In addition, it seems worthwhile to publish a construction for N_{16}; although N_{16} fails to improve on Λ_{16} in any known respect, it is somewhat surprising that it comes as close to matching Λ_{16} as it does, and it would seem to merit further study. These constructions also illustrate that twisted squaring constructions sometimes improve on squaring constructions and that we are really more interested in the distance properties of a coset code construction than in whether it is linear or not.

A. The Nordstrom–Robinson Code

The Nordstrom–Robinson code may be defined as the set of all 16-tuples consisting of two (8,7) codewords of the form

$$\boldsymbol{c} = \big(\boldsymbol{c}(a_1, \boldsymbol{a}, \boldsymbol{a}^*), \boldsymbol{c}(a_2, [\boldsymbol{a} + f(\boldsymbol{a}^*)], \boldsymbol{a}^*)\big)$$

where, as in the previous section,

$$\boldsymbol{c}(a_1, \boldsymbol{a}, \boldsymbol{a}^*) = a_1 G_{(8,1)} + \boldsymbol{a} G_{(8,4)/(8,1)} + \boldsymbol{a}^* G^*_{(8,7)/(8,4)}.$$

(This may be regarded as an $|a + x|a + b(x) + x|$ construction.) The function $f(\boldsymbol{a})$ is any one-to-one map from 3-tuples to 3-tuples with the properties

1) if $\boldsymbol{a} = \boldsymbol{0}$, $f(\boldsymbol{a}) = \boldsymbol{0}$;
2) if $\boldsymbol{a}_1 \neq \boldsymbol{a}_2$, the inner product $(\boldsymbol{a}_1 + \boldsymbol{a}_2, f(\boldsymbol{a}_1) + f(\boldsymbol{a}_2))$ is congruent to 1 modulo 2 (implying that if $\boldsymbol{a} \neq \boldsymbol{0}$, $(\boldsymbol{a}, f(\boldsymbol{a})) \equiv 1 \bmod 2$).

We shall shortly investigate what functions $f(\boldsymbol{a})$ satisfy these conditions.

The code thus consists of 64 translates of $(8,1)^2$ and has 2^8 codewords, labeled by the binary 8-tuples $(a_1, a_2, \boldsymbol{a}, \boldsymbol{a}^*)$. In fact, it is a twisted squaring construction, since the coset of (8,1) in the second section is a function of the coset of (8,1) in the first section. The set of $\boldsymbol{c}$ with $\boldsymbol{a}^* = \boldsymbol{0}$ is the squaring construction $|(8,4)/(8,1)|^2 = \{(\boldsymbol{c}(a_1, \boldsymbol{a}, \boldsymbol{0}), \boldsymbol{c}(a_2, \boldsymbol{a}, \boldsymbol{0}))\}$, which is the linear (16,5,8) first-order Reed–Muller code. This definition thus expresses the Nordstrom–Robinson code as a union of eight translates $(16,5) + (\boldsymbol{c}(0, \boldsymbol{0}, \boldsymbol{a}^*), \boldsymbol{c}(0, f(\boldsymbol{a}^*), \boldsymbol{a}^*))$ of the (16,5) code. It is therefore natural to express the construction as $|(8,7)/(8,4)/(8,1)|^2$, which is illustrated by the 64-state trellis diagram of Fig. 24. The trellis simply consists of the end sections of the trellis diagrams for the $(24,12,8) = |(8,7)/(8,4)/(8,1)|^3$ or $(32,16,8) = |(8,7)/(8,4)/(8,1)|^4$ codes, connected in a way specified by the function $f(\boldsymbol{a})$ that respects the integrity of the clusters.

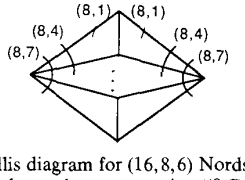


Fig. 24. 64-state trellis diagram for (16,8,6) Nordstrom–Robinson code based on twisted squaring construction $|(8,7)/(8,4)/(8,1)|^2$.

The minimum distance between codewords can be shown to be six, as follows. Since the code is nonlinear ($f(\boldsymbol{a}_1 \oplus \boldsymbol{a}_2) \neq f(\boldsymbol{a}_1) \oplus f(\boldsymbol{a}_2)$ in general), we must consider every possible pair of codewords $(\boldsymbol{c}_1, \boldsymbol{c}_2)$; their Hamming distance is the weight of their modulo 2 sum, which by Lemma 4 is

$$\begin{aligned}\|\boldsymbol{c}_1 \oplus \boldsymbol{c}_2\|^2 &\equiv 2(\boldsymbol{a}_1 + \boldsymbol{a}_2, \boldsymbol{a}_1^* + \boldsymbol{a}_2^*) + 2(\boldsymbol{a}_1 + \boldsymbol{a}_2 + f(\boldsymbol{a}_1^*) \\ &\quad + f(\boldsymbol{a}_2^*), \boldsymbol{a}_1^* + \boldsymbol{a}_2^*) \pmod 4 \\ &= 4(\boldsymbol{a}_1 + \boldsymbol{a}_2, \boldsymbol{a}_1^* + \boldsymbol{a}_2^*) \\ &\quad + 2(f(\boldsymbol{a}_1^*) + f(\boldsymbol{a}_2^*), \boldsymbol{a}_1^* + \boldsymbol{a}_2^*) \\ &\equiv \begin{cases} 0 \pmod 4, & \text{if } \boldsymbol{a}_1^* = \boldsymbol{a}_2^* \\ 2 \pmod 4, & \text{if } \boldsymbol{a}_1^* \neq \boldsymbol{a}_2^* \end{cases}\end{aligned}$$

from the properties of $f(\boldsymbol{a})$. Furthermore,

1) if $\boldsymbol{a}_1^* = \boldsymbol{a}_2^*$, then $\boldsymbol{c}_1 \oplus \boldsymbol{c}_2$ is a (16,5,8) codeword and has weight 0, 8, or 16;
2) if $\boldsymbol{a}_1^* \neq \boldsymbol{a}_2^*$, then $\boldsymbol{c}_1 \oplus \boldsymbol{c}_2$ is a 2-tuple of nonzero (8,7) codewords and thus has weight at least 4. However, since $\|\boldsymbol{c}_1 \oplus \boldsymbol{c}_2\|^2 \equiv 2 \bmod 4$, the weight must be at least six. (In fact, in this case the weight must be six or ten, four in one 8-tuple and two or six in the other.)

Thus the construction is a twisted squaring construction that pairs the 28 cosets of (8,1) in (8,7) that have weights congruent to 0 modulo 4 and are not in (8,4) with the 28 cosets of (8,1) in (8,7) that have weights congruent to 2 modulo 4, and vice versa.

We now consider the set of all possible $f(\boldsymbol{a})$ satisfying conditions 1) and 2). The function $f(\boldsymbol{a})$ may be specified by a table of $3 \times 8 = 24$ bits giving the value of $f(\boldsymbol{a})$ for each value of its argument. Condition 1) fixes three bits. Condition 2) gives a total of 28 inhomogeneous linear equations in the remaining 21 unknowns. These equations could have no solution, a unique solution, or a space of solutions. Happily, in this case there is a three-dimensional space of eight solutions, given in Table I. The table also gives two particular solutions $f_0(\boldsymbol{a})$ and $f_1(\boldsymbol{a})$; the total set of solutions consists of the two solutions that can be obtained as column permutations of $f_0(\boldsymbol{a})$, and the six solutions obtained in this way from $f_1(\boldsymbol{a})$.

TABLE I
SOLUTIONS FOR $f(a)$

a	$f(a)$	$f_0(a)$	$f_1(a)$
000	0,0,0	000	000
001	$\bar{a}, b, 1$	101	001
010	$c, 1, \bar{b}$	011	011
100	$1, \bar{c}, a$	110	111
011	$a + c, \bar{b}, b$	010	110
101	$a, b + c, \bar{a}$	001	100
110	$\bar{c}, c, a + b$	100	101
111	$a + \bar{c}, b + \bar{c}, a + \bar{b}$	111	010

The number of near neighbors and indeed the entire distance distribution is the same for each codeword (the code is distance-invariant) and is easily enumerated. For any codeword $\boldsymbol{c}$, the distance distribution within a subtrellis is that of the (16,5,8) code, namely 1 word at distance 0

(itself), 30 at distance 8, and 1 at distance 16 (its complement). The distances to the 32 words in any other subtrellis (coset of (16,5)) are equally divided between 6 and 10. Thus from any codeword there are $7\times16=112$ words at distance 6, 30 at 8, 112 at 10, and 1 at 16.

B. 16-Dimensional Nonlattice Packings

We now construct 16-dimensional nonlattice packings analogous to the Nordstrom–Robinson code. We shall denote any such packing as N_{16}. Its centers are the set of all 16-tuples consisting of two elements of E_8 of the form

$$c=(w_1+c(a,a^*),w_2+c([a+f(a^*)],a^*))$$

where w_1 and w_2 are elements of $2E_8$, a, a^*, and $f(a^*)$ are binary 4-tuples, the sum $a+f(a^*)$ may be taken modulo 2, and, as in the previous section,

$$c(a,a^*)=aG+a^*G^*.$$

The function $f(a)$ is a one-to-one map from a subset S of binary 4-tuples, including $\mathbf{0}$, to another subset $f(S)$, with the properties

1) $f(\mathbf{0})=\mathbf{0}$;
2) for all $(a_1,a_2)\in S^2$ such that $a_1\neq a_2$, the inner product $(a_1+a_2,f(a_1)+f(a_2))$ is congruent to 1 modulo 2.

We shall show shortly that these conditions cannot be met for the set of all 16 4-tuples but can be met for a large number of sets S of size $|S|=9$. Thus N_{16} consists of 144 translates of $2E_8^2$.

This construction is again a twisted squaring construction, since the coset of $2E_8$ in the second section is a function of the coset of $2E_8$ in the first section. The set of c with $a^*=\mathbf{0}$ is the squaring construction $|RE_8/2E_8|^2=2E_8^2+(c(a,\mathbf{0}),c(a,\mathbf{0}))$, which is a version $(R\Lambda_{16})$ of the Barnes–Wall lattice Λ_{16} with $d_{\min}^2=16$. This construction thus expresses N_{16} as a union of nine translates $R\Lambda_{16}+(c(\mathbf{0},a^*),c(f(a^*),a^*))$ of $R\Lambda_{16}$. We may therefore express the construction as $|E_8/RE_8/2E_8|^2$, which is illustrated by the 144-state trellis diagram of Fig. 25. The trellis consists of 9/16 of the end sections of the trellis diagrams for the $\Lambda_{24}=|E_8/RE_8/2E_8|^3$ or $\Lambda_{32}=|E_8/RE_8/2E_8|^4$ lattices, connected in a way specified by the function $f(a)$ that respects the integrity of the clusters.

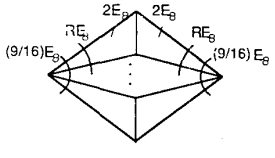


Fig. 25. 144-state trellis diagram for $N_{16}=|E_8/RE_8/2E_8|^2$.

There are nine times as many points of N_{16} per unit volume of 16-space as are in $R\Lambda_{16}$. We shall next show that the minimum squared distance between its points is 12. This implies that it is $3^{10}/2^{16}$ as dense as Λ_{16} in 16-space, with normalization for minimum distance, i.e., that its coding gain is $\gamma(N_{16})=3^{5/4}\cdot2^{-1/2}=2.792$ (4.46 dB), or 0.06 dB less than $\gamma(\Lambda_{16})=2^{3/2}=2.828$ (4.52 dB).

Again, we must consider the distance between every pair of centers (c_1,c_2) in N_{16}. Using Lemma 5 and the properties of $f(a)$, we have

$$\begin{aligned}\|c_1-c_2\|^2&\equiv 4(a_1+a_2,a_1^*+a_2^*)+4(a_1+a_2+f(a_1^*)\\&\quad+f(a_2^*),a_1^*+a_2^*)\pmod 8\\&=8(a_1+a_2,a_1^*+a_2^*)\\&\quad+4(f(a_1^*)+f(a_2^*),a_1^*+a_2^*)\\&\equiv\begin{cases}0\pmod 8, & \text{if } a_1^*=a_2^*\\ 4\pmod 8, & \text{if } a_1^*\neq a_2^*\end{cases}.\end{aligned}$$

If $a_1^*=a_2^*$, then c_1 and c_2 are in the same translate of $R\Lambda_{16}$, so that their minimum squared distance is in fact 16. (If $a_1=a_2$, then they are in the same translate of $2E_8^2$, whose minimum squared distance is 16. If $a_1\neq a_2$, then their difference consists of two nonzero elements of RE_8 and thus has weight at least $8+8=16$.)

If $a_1^*\neq a_2^*$, then the difference c_1-c_2 consists of two nonzero elements of E_8 and has weight at least $4+4=8$. However, since $\|c_1-c_2\|^2\equiv4\bmod8$, the weight of the difference must be at least 12. (When it is 12, the two 8-tuples of the difference must have weights 4 and 8.)

We now show that while the conjectured 16-translate packing fails, many nine-translate packings work. It is easy to show that condition 2) on $f(a)$ cannot be satisfied when S is the set of all 16 4-tuples; indeed, it is sufficient to consider any set including the four weight-1 4-tuples and the six weight-2 4-tuples, for which condition 2) gives a set of 55 equations in 44 unknowns which are inconsistent. However, for many sets S of size $|S|=9$, there are six-dimensional spaces of solutions to the set of 36 equations in 32 unknowns implied by condition 2). General and particular solutions for the sets $S_1=\{0000,0001,\cdots,1000\}$ and $S_2=\{$all 4-tuples of weight 0, 1, or 3$\}$ are given in Table II.

TABLE II
SOLUTIONS FOR $f(a)$

a	$f(a)$	$f_0(a)$	$f_1(a)$
0000	0,0,0,0	0000	0000
0001	$d,\bar{a},b,1$	0101	1101
0010	$e,c,1,\bar{b}$	0011	1011
0100	$f,1,\bar{c},a$	0110	1110
1000	$1,\bar{f},\bar{e},\bar{d}$	1111	1000
0011	$d+\bar{e},a+c,\bar{b},b$	1010	0010
0101	$d+\bar{f},a,b+c,\bar{a}$	1001	0001
0110	$e+\bar{f},\bar{c},c,a+b$	1100	0100
0111	$d+e+f,a+\bar{c},b+\bar{c},a+\bar{b}$	0111	1111
0000	0,0,0,0	0000	0000
0001	$d,\bar{a},b,1$	0101	1101
0010	$e,c,1,\bar{b}$	0011	1011
0100	$f,1,\bar{c},a$	0110	1110
1000	$1,\bar{f},\bar{e},\bar{d}$	1111	1000
0111	$d+e+f,a+\bar{c},b+\bar{c},a+\bar{b}$	0111	1111
1011	$d+e,a+c+f,\bar{b}+e,b+d$	0010	0101
1101	$d+f,a+f,b+c+e,\bar{a}+d$	0001	0110
1110	$e+f,\bar{c}+f,c+e,a+b+d$	0100	0011

Since the roles of a^* and $f(a^*)$ can be interchanged in the construction of N_{16}, the range $f(S)$ of any set S for which the construction works is another set of nine 4-tuples for which the construction works. Any column permutation applied to both a and $f(a)$ also gives a set S and a function $f(a)$ for which condition 2) is satisfied. Thus there are a large number of sets S of size $|S| = 9$ that work.

If there were a union of ten translates of $R\Lambda_{16}$ with $d^2_{\min} = 12$, its normalized density would be a factor of $10 \cdot (3/4)^8 = 65\,610/65\,536$ times that of $R\Lambda_{16}$. However, Conway and Sloane [2] state that no such ten-translate construction exists.

The number of near neighbors (kissing number) and indeed the entire distance distribution (theta series) is the same from each center and may be enumerated using the following facts about the 256 cosets of $2E_8$ in the quotient group $E_8/2E_8$, identified by the label (a, a^*):

1) the zero coset ($2E_8$ itself) has weight enumerator $1 + 240x^{16} + 2160x^{32} + \cdots$;
2) any of the 135 nonzero cosets with $(a, a^*) = 0 \bmod 2$ has weight enumerator $16x^8 + 128x^{16} + 448x^{24} + 1024x^{32} + \cdots$;
3) any of the 120 nonzero cosets with $(a, a^*) = 1 \bmod 2$ has weight enumerator $2x^4 + 56x^{12} + 252x^{20} + 688x^{28} + \cdots$.

(These are derived from the theta series for E_8 given in [19].) The weight/distance enumerator (theta series) for N_{16} is then computable as $1 + 4096x^{12} + 4320x^{16} + 147\,456x^{20} + 61\,440x^{24} + 1\,548\,288x^{28} + 522\,720x^{32} + 9\,011\,200x^{36} + \cdots$, the terms corresponding to weights congruent to 0 modulo 8 being those of $R\Lambda_{16}$ and being the distance enumerator within an $R\Lambda_{16}$ translate, and the remaining terms being the distance enumerator to the other eight translates. The kissing number of N_{16} is thus 4096, slightly less than the kissing number of Λ_{16}, which is 4320. (Again, if there were a ten-translate construction, the kissing number would be greater than that of Λ_{16}, namely, 4608.)

The facts that the nonlattice Nordstrom–Robinson packings N_{16} are just slightly less dense than the Barnes–Wall lattice Λ_{16} and have a slightly smaller kissing number are perhaps not too surprising since, whereas there is no very good (16,8) linear code, the Barnes–Wall lattice packing has excellent density for its dimension, better than the best packings known in nearby dimensions in the Leech normalization (see [2, fig. 1.5]). What may perhaps be regarded as remarkable is the existence of another packing with density even close to that of Λ_{16} in 16 dimensions.

The Barnes–Wall lattice Λ_{16} is not quite as good for covering; the square of its covering radius is three times the square of its packing radius, unlike D_4, E_8, and Λ_{24}, for which the ratio is two. Also, its mean-squared error as a quantizer is further away from a conjectured bound of Conway and Sloane than that of D_4, E_8, and Λ_{24} [2, fig. 2.9]. Is it possible that N_{16} (or perhaps a dual packing, of which Λ_{16} would be the union of nine translates) is superior to Λ_{16} for covering?

VIII. Decoding: Examples

As we have seen, the constructions of this paper give codes and lattices that can be represented by simple regular trellis diagrams with relatively few states. The general decoding methods suggested by these trellis diagrams have already been discussed. In this section we give a few concrete decoding algorithms for the (8,4) first-order Reed–Muller code (as well as the E_8 lattice), the (24,12) Golay code, and the Leech lattice Λ_{24}. In all cases the decoding algorithms improve on the best maximum likelihood decoding algorithms previously known, where we take as a benchmark the recent work of Conway and Sloane [20].

A. Decoding Binary Codes and Lattices

A *maximum likelihood decoding algorithm* for a code C or lattice Λ is an algorithm that, given an N-tuple $\boldsymbol{r} = \{r_j, 1 \le j \le N\}$, finds the closest N-tuple $\boldsymbol{c}$ in C or Λ to $\boldsymbol{r}$. We assume once more that the distance measure (*metric*) has the additive property $d(\boldsymbol{r}, \boldsymbol{c}) = \sum_j d(r_j, c_j)$.

Efficient maximum likelihood decoding algorithms, such as the general algorithms given earlier or the Viterbi algorithm, operate by successively determining the best partial sequences within sets of partial sequences, such that the ultimately decoded sequence must contain one of these best partial sequences, called *survivors*.

If C is a binary code, it is typically assumed that 0 and 1 are mapped into $+1$ and -1 for transmission, that the received level r_j is a real number, and that the symbol distance measure is $(r_j - 1)^2$ or $(r_j + 1)^2$ for 0 or 1, respectively; or, equivalently, that the metric is $-r_j$ for 0 and $+r_j$ for 1, the smaller (more negative) metric being better.

If Λ is a binary lattice with 2-depth m, then $2^m\boldsymbol{Z}^N$ is a sublattice of Λ, and Λ is a union of 2^K cosets of $2^m\boldsymbol{Z}^N$, with coset representatives that can be taken as N-tuples of integers $\bmod 2^m$. As a first step in decoding, therefore, we can find the closest integers i_{jk} to each coordinate r_j among the set of integers congruent to k modulo 2^m for $1 \le j \le N$, $0 \le k \le 2^m - 1$—i.e., the survivor of each coset of $2^m\boldsymbol{Z}$ in the partition $\boldsymbol{Z}/2^m\boldsymbol{Z}$—since the finally decided lattice point must have one of these integers as its jth coordinate (because any other integer congruent to k modulo 2^m could be replaced by i_{jk} to give another lattice point with improved metric). We shall assume that these integers and their metrics $d_{jk} \triangleq (r_j - i_{jk})^2$ are precomputed and available.

If Λ is a mod-2 binary lattice, then it is the set of all integer N-tuples that are congruent modulo 2 to codewords in some binary (N, K) code C; i.e., $\Lambda = 2\boldsymbol{Z}^N + C$. To decode a mod-2 lattice, we may first find the closest even and odd integers, i_{j0} and i_{j1}, to the received level r_j, and their metrics d_{j0} and d_{j1}. However, it is more convenient to use the metric $m_j \triangleq d_{j0} - d_{j1} = i^2_{j0} - i^2_{j1} - 2r_j(i_{j0} - i_{j1})$ for the closest even integer, and $-m_j$ as the metric for

the closest odd integer. (In fact, $m_j = 2|r_j - i_{j0}| - 1$, so no multiplication is required.) After this precomputation, we can proceed as though decoding the binary code C. For example, since $E_8 = 2\boldsymbol{Z}^8 + (8,4)$, it can be decoded by the method to be given now for the (8,4) code.

B. Decoding the (8,4) Code or E_8 Lattice

The (8,4) code is a case of a first-order Reed–Muller code, for which the fast Hadamard transform (Green machine) has been suggested [20] as an efficient decoding algorithm. Since $(8,4) = (8,1) + [(8,4)/(8,1)]$, the (8,4) code consists of the eight coset representatives in $[(8,4)/(8,1)]$ and their complements. The fast Hadamard transform computes the inner product of $\boldsymbol{r}$ with each of these eight coset representatives in $3 \times 8 = 24$ binary operations, as illustrated in Fig. 26. The sign of each inner product indicates whether the corresponding word or its complement is better; the magnitudes (absolute values) of the eight inner products are then compared to select the closest code word.

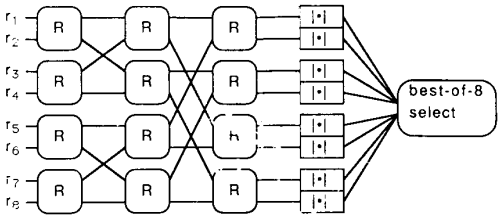


Fig. 26. Decoding (8,4) code or E_8 lattice via fast Hadamard transform. Operator R produces outputs $(x + y, x - y)$ from inputs (x, y); operator $|\cdot|$ takes absolute magnitude $|x|$ of its input x.

The general decoding algorithm for iterated squaring constructions given earlier, or the trellis for $(8,4) = |(4,\ 3)/(4,\ 1)|^2 = |(2,2)/(2,1)/(2,0)|^4 = |(1,1)/(1,1)/(1,0)/(1,0)|^8$, specifies an iterative decoding algorithm that can be put into very similar form as follows.

a) For each of the eight coordinates, and for each of the two cosets of (1,0) in the partition (1,1)/(1,0)—i.e., for each of the two bits 0 and 1—find the best element in that coset and its metric. Since there is only one element in each coset, this reduces to the trivial operation of letting $-r_j$ be the metric for 0 and $+r_j$ be the metric for 1. (In the case of the E_8 lattice, however, this step requires finding the best element in each coset of $2\boldsymbol{Z}$ in the partition $\boldsymbol{Z}/2\boldsymbol{Z}$—i.e., the closest even integer and the closest odd integer—and their metrics, as just discussed.)

b) For each of the four 2-tuples of coordinates, and for each of the four cosets of (2,0) in the partition (2,2)/(2,0)—i.e., for each of the four possible bit pairs—find the best element in that coset and its metric. Again, since there is only one element in each coset, no comparisons are required, and the metric of the pair is just the sum of the metrics of the two elements of the pair. Only the two metrics $r_1 \pm r_2$ need to be computed, the metrics of the complementary bit pairs being the negatives of these two metrics.

c) For each of the two 4-tuples of coordinates, for each of the four cosets of (4,1) in the partition (4,3)/(4,1), find the best element in that coset and its metric. Each coset consists of a (4,3) codeword and its complement. Only the four metrics $r_1 \pm r_2 \pm r_3 \pm r_4$ with an even number of minus signs need to be computed; the sign of the result indicates whether the corresponding codeword or its complement is better, so the negative of the absolute value of the result is the survivor metric.

d) Finally, to find the best 8-tuple, form four sums of survivor metrics from corresponding cosets of (4,1) in the two halves of the code, and choose the best.

This algorithm is illustrated in Fig. 27. We see that the first two operations are identical to those in Fig. 26 and amount to taking the fast Hadamard transform of each 4-tuple. The trellis-based algorithm then achieves a modest simplification: elimination of four binary operations (additions/subtractions), and replacement of a best-of-eight by a best-of-four select (equivalent to eliminating four binary operations). Similar modest improvements can be obtained for all first-order Reed–Muller codes. (The same simplification could have been achieved directly in Fig. 26 from the observation that $\max[|x + y|, |x - y|] = |x| + |y|$.)

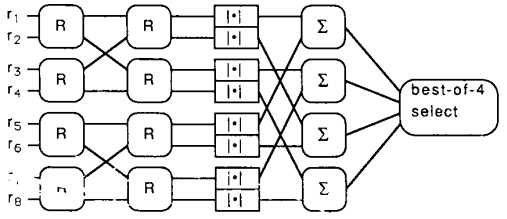


Fig. 27. Decoding (8,4) code or E_8 lattice via iterative trellis-based algorithm. Operator Σ produces sum $x + y$ of its inputs (x, y).

C. Decoding the Golay Code

The trellis diagram of the (24,12) Golay code (Fig. 21) is based on the cubing construction $|(8,7)/(8,4)/(8,1)|^3$ and displays it as the union of eight cosets of the (24,9) code, which has a simple eight-state trellis due to its parity-check construction $|(8,4)/(8,4)/(8,1)|^3$.

The first step in decoding is to compute all of the 8-tuple branch metrics, for each of the three sections, i.e., to decode the partition $(8,7)/(8,4)/(8,1)$. Since each branch represents a coset of (8,1) in the partition (8,7)/(8,1)—i.e., an (8,7) codeword and its complement—we need to find only the absolute values of 64 8-tuple inner products. These can be computed by the general method for decoding partition chains resulting from iterated squaring constructions, as follows.

1) For each 2-tuple, compute the metrics of the cosets of (2,0) in the partition (2,2)/(2,0) by computing (as above, using the fact that only one metric of a complement pair need be computed) $r_1 \pm r_2$, $r_3 \pm r_4$, $r_5 \pm r_6$, $r_7 \pm r_8$ (eight binary operations).

2) For each 4-tuple, compute the metrics of the cosets of (4,0) in the partition (4,4)/(4,0) by computing $r_1 \pm r_2 \pm$

$r_3 \pm r_4$, $r_5 \pm r_6 \pm r_7 \pm r_8$ by combinations of 2-tuple metrics (16 binary operations).

3) For each 8-tuple, compute the metrics of the cosets of (8,1) in the partition (8,7)/(8,1) by computing $r_1 \pm r_2 \pm r_3 \pm r_4 \pm r_5 \pm r_6 \pm r_7 \pm r_8$ for all combinations in which the number of minus signs is even by combinations of 4-tuple metrics (64 binary operations).

4) Take absolute values of each of these 64 sums. (Again, this accomplishes the comparison of the metric of a codeword and its complement.)

Thus decoding the 64-way partition requires 88 binary operations, and this must be done for each of the three sections. Now, with all needed metrics in hand, we can find the best codeword in each of the eight cosets of the (24,9) code—i.e., in each of the eight subtrellises—by use of the general method for cubing constructions, which is effectively the Viterbi algorithm. No merges occur, and thus no decisions are required until the end of the second section. At this point, for each of the eight states, metrics must be computed for each of eight competing paths, each metric requiring an addition of the metrics corresponding to the first and second 8-tuples. The best of these eight sums must then be selected. At the final node, eight competing metrics must again be computed, each requiring one addition, and the best selected. Thus the decoding of one (24,9) coset requires $9 \times 8 = 72$ additions and nine best-of-eight selects or, equivalently, $9 \times 7 = 63$ binary comparisons. This coset computation has to be done eight times, with one final best-of-eight select to choose the champion. In total, therefore, trellis decoding requires 1351 binary operations, namely,

1) $3 \times 88 = 264$ binary adds/subtracts to compute 8-tuple branch metrics;
2) $8 \times 72 = 576$ binary additions and $7 + 8 \times 63 = 511$ binary comparisons to find the best path in the three-section trellis.

While comparisons always depend to some extent on implementation technology, this method seems superior to either of the decoding techniques proposed in [20], one of which is based on regarding the Golay code as the union of 128 (24,5) cosets and takes 1584 steps, and the other of which is based on regarding it as the union of 512 (24,3) cosets and takes 1728 steps. Our algorithm uses the fact that the (24,12,8) code consists of eight cosets of the (24,9,8) code, which in turn consists of 64 cosets of the $(8,1)^3$ code via a parity-check 3-construction $|(8,4)/(8,4)/(8,1)|^3$ that yields an eight-state trellis diagram.

D. Decoding the Leech Lattice

The Leech lattice Λ_{24} is a mod-4 lattice and has the 256-state three-section trellis based on the cubing construction $|E_8/RE_8/2E_8|^3$ that is shown in Fig. 23. Decoding involves the following three stages.

a) Determine the metrics $d_{j0}, d_{j1}, d_{j2}, d_{j3}$ of each integer modulo 4 for each of the 24 coordinate positions. This step is highly implementation-dependent but has complexity of the order of only a small multiple of 96, so we shall not include the complexity of this stage when we add up the complexity of the whole algorithm below. We can normalize these metrics as follows: let i_j be the greatest integer not greater than r_j, and let $e_j = r_j - i_j$; then the normalized metrics $m_{jk} \triangleq d_{jk} - (r_j - i_j)^2$ have values $4 - 4e_j$, $1 - 2e_j$, 0, and $1 + 2e_j$; or, more symmetrically, if we define $e'_j = 1 - e_j$ and subtract e'_j from each value, the normalized metric values become $3e'_j$, $-e_j$, $-e'_j$, and $3e_j$.

b) For each of the three sections, decode the 256-way partition $E_8/2E_8$ to determine the metrics of the 2^8 distinct branches in that section. Since $E_8/RE_8/2E_8$ is a partition chain that results from an iterated squaring construction, i.e., $E_8/RE_8/2E_8 = |D_4/RD_4/2D_4/2RD_4|^2 = |\boldsymbol{Z}^2/R\boldsymbol{Z}^2/2\boldsymbol{Z}^2/2R\boldsymbol{Z}^2/4\boldsymbol{Z}^2|^4$, the general method can be applied, as follows.

1) For each 2-tuple, compute the metrics of the cosets of $4\boldsymbol{Z}^2$ in the 16-way partition $\boldsymbol{Z}^2/4\boldsymbol{Z}^2$ by computing all 16 possible 2-tuple metrics (16 binary additions per 2-tuple, or $4 \times 16 = 64$ total).

2) For each 4-tuple, compute the metrics of the cosets of $2RD_4$ in the 64-way partition $D_4/2RD_4$ by computing the 128 4-tuple metrics corresponding to the 128 possible branches $D_4/4\boldsymbol{Z}^4$, and then select the better of each complement pair to give the 64 4-tuple branch metrics (128 binary additions and 64 binary comparisons per 4-tuple, or $2 \times 192 = 384$ total binary operations)

3) For each 8-tuple, compute the metrics of the cosets of $2E_8$ in the 256-way partition $E_8/2E_8$ by computing the 1024 8-tuple metrics corresponding to the 1024 cosets of $2RD_4^2$ in E_8, and then, for each of the 256 cosets of $2E_8$, select the best of the four cosets of $2RD_4^2$ whose union is that coset ($256 \times 4 = 1024$ binary additions and $256 \times 3 = 768$ binary comparison, or 1792 total binary operations).

c) With all 8-tuple branch metrics in hand, find the best path through the trellis. For each of the 256 states at the end of the second section, 16 pairs of branch metrics must be summed and compared to find the best. At the final node, 256 paths must be compared, each path requiring a further binary addition to determine the metric. This stage thus requires $256 \times 16 + 256 = 4352$ binary additions and $256 \times 15 + 255 = 4095$ binary comparisons.

The computation of 256 8-tuple metrics requires $64 + 384 + 1792 = 2240$ binary operations per section, or 6720 in all. Finding the best of the 4096 paths through the trellis then requires 8447 binary operations. Given the initial normalized metrics, therefore, decoding requires a total of 15 167 binary operations. This would seem to be a substantial improvement over the method of Conway and Sloane [20] which requires 55 968 steps. While that algorithm is also based on a Turyn construction of the Leech lattice, and indeed on the recognition that with this construction $R\Lambda_{24}$ consists of 4096 cosets of $2RE_8^3$, it does not exploit (as ours does) the two-level decomposition of Λ_{24}, which consists of 16 cosets of the lattice $|RE_8/RE_8/2E_8|^3$, which in turn consists of $16 \times 16 = 256$ cosets of $2E_8^3$ via a parity-check 3-construction that leads

to a 16-state trellis diagram. Our main improvement, however, comes from the iterative method of computing 8-tuple metrics.

E. Notes

The notion of a trellis diagram was introduced by Forney [21] to show that Viterbi's "asymptotically optimum" decoding algorithm for convolutional codes [22] was actually optimum (equivalent to maximum likelihood decoding). Trellis decoding of block codes has been suggested before, e.g., in [6] where it is shown that an (N, K) code can be represented by a trellis of not more than $\min[2^K, 2^{N-K}]$ states. However, the trellises given here have fewer states and more regular structure than would have been expected; for instance, the Golay trellis has only 64 states, not $2^{12} = 4096$. (The appendix shows, however, that a complete trellis has 256 states at the center, and actually 512 states at the adjacent positions.) Solomon *et al.* [23], [24] have given a characterization of the Golay code as a 256-state convolutional code, but with 256 starting states connected to 256 final states; i.e., the trellis has a "tail-biting" form.

For lattices, the trellis representation and the associated decoding algorithms are essentially new, although simple trellis diagrams for D_4 and E_8 were given in [14] (where we also guessed, wrongly, that Λ_{16} would require a 64-state trellis, and Λ_{24} an 8192-state trellis). For partitions, the concept of a trellis diagram, as shown for example in Figs. 1, 4, 5, or 7, and the associated decoding methods are also new.

IX. Conclusion

The lattices developed in this paper are useful both in themselves, as lattice codes, and also as building blocks for more general coset codes, such as the trellis codes of [1]. They are all generated by rather simple constructions. We regard the constructions as more geometric than algebraic and have structured the development to reflect this emphasis. The binary codes to which they are closely related may be regarded as being contained in the corresponding lattices—e.g., the Barnes–Wall lattices contain all the binary Reed–Muller codes, and the Leech lattice contains the Golay code—so that these codes may be regarded as fundamentally geometric also.

The constructions have common character. We first partition a low-dimensional group of N-tuples—e.g., binary N-space, or an integer lattice $\mathbf{Z}^N$—into a sequence of subgroups of progressively increasing distance. For an N'-construction, we seek a universal basis for N'-space which can be partitioned in the same way. To construct a set of NN'-tuples, we then convolve one partition with the other (as in [7]). It seems to be desirable if one or both of these partition chains are self-dual in some sense; also, if there are alternative partition chains using the same generators, it is desirable that both have a favorable distance progression. In [25] we shall use similar construction principles to construct families of ternary codes and lattices, which include most of the remaining densest lattices in 24 or fewer dimensions.

The constructions are associated with simple, regular trellis diagrams that suggest efficient maximum likelihood decoding methods. In fact, the examples given all seem simpler than previously published decoding algorithms. The Appendix shows that the number of states shown in these diagrams is minimum (for the given coordinate ordering), so that there is some doubt whether these algorithms can be simplified further in any substantial way. There is always room for tricks such as Wagner decoding [6], doing comparisons by taking absolute magnitudes (as above), regrouping the coordinates or the order of the computations, and so forth. However, suboptimal bounded-distance decoding methods that effectively achieve the full minimum distance often can be found for constructions that are decomposable, and these are more likely candidates for substantial simplifications.

Acknowledgment

G. R. Lang introduced me to lattices, and his continued advocacy of communications applications of lattices led to my initial interest in finding a common framework for lattice codes and trellis-coded modulation. The multidimensional trellis codes discovered by L. F. Wei were the next major impetus to this work. Interaction with F. M. Longstaff on the implementation of Leech lattice decoding methods was also stimulating. A. R. Calderbank was helpful in pointing the way to the lattice/coset viewpoint. I am deeply indebted to N. J. A. Sloane for reprints and preprints, for guidance through the literature of codes and lattices, and for pointing out an error in my first attempt at a 16-dimensional nonlattice packing. Finally, in addition to those acknowledged in [1], I particularly wish to thank M. Rouanne for detailed comments on an earlier version of this paper.

Appendix
Algebraic Derivation of Trellis Diagrams

The trellis diagrams of the main text are obtained directly from our various constructions and depend only on the constructions and the set partitions to which they are applied, which need not even be groups. In fact, if the sets are groups of N-tuples, then trellis diagrams can be derived algebraically, as we shall show in this Appendix for codes, lattices, and partitions. Because the trellis diagrams obtained are minimal, they in some sense give lower bounds to the complexity of any maximum likelihood decoder.

A. The Trellis Diagram of a Code

Let C be a linear binary (N, K) block code, with coordinates arranged in a definite order. For any *position* N_p, let the first N_p coordinates be called the *past* and the remaining $N_f = N - N_p$ the *future*. Let C_p be the subcode consisting of all codewords whose *span* (the range between the first and last nonzero coordinates) lies within the past (i.e., which are all-zero in the future), and let C_f be the subcode of all codewords whose span lies in the

future; let the dimensions of these subcodes (which are easily seen to be linear vector spaces over the binary field) be K_p and K_f, respectively. We may regard these either as (N, K_p) and (N, K_f) codes or (N_p, K_p) and (N_f, K_f) codes, respectively.

We may obtain K generators for C by starting with K_p generators for C_p and K_f for C_f, and adding $K_s = K - K_p - K_f$ generators which must necessarily span both past and future. We say that K_s is the dimension of the state space (for this particular partition into past and future), and we may identify the $|\Sigma| = 2_s^K$ combinations of the state space generators as states.

(While a block code is a static construct, we prefer to continue using the dynamical terms past, future, and state because of their conceptual richness. Abstractly, the state is the past modulo the future; the states are the equivalence classes of past histories modulo future possibilities. In statistical terms, the states are sufficient statistics for the past with respect to prediction of future possibilities; the probability of a particular future given the entire past is the same as the probability of that future given the state.)

The code C may be described in terms of a trellis diagram (similar to a squaring construction trellis) that has an initial node, $|\Sigma|$ intermediate nodes (corresponding to the states), and a final node. The branch connecting the initial node to the zero state represents the code C_p (whose codewords may be considered to be parallel branches), and the other branches connecting the initial node to the other states represent cosets of C_p. Similarly, the branches connecting the states to the final node represent C_f and its cosets. The set of all paths through the trellis corresponds to all of the 2^K codewords. Clearly, any trellis diagram for C must have at least a state space of dimension K_s at this point, else there would be some past or future branch corresponding to more words than there are in C_p or C_f, which, by linearity, would be a contradiction to the definition of these subcodes.

From the trellis diagram, we see that the set C^p of all truncations of codewords to the past is an $(N_p, K_p + K_s)$ code, and the states correspond to the cosets of the partition C^p/C_p. Each truncated word has a set of extensions to the future which form a coset of C_f of dimension K_f, so that C^p is also isomorphic to C/C_f. C^p has dimension $K^p = K - K_f = K_p + K_s$. Similarly, the set C^f of all truncations of codewords to the future is an $(N_f, K_f + K_s)$ code, and the states correspond to the cosets of the partition C^f/C_f.

The past or future may be further subdivided, resulting in state spaces of computable dimension at each position selected as a partition boundary, which may be connected appropriately with branches to form a multisection trellis diagram. Since we can select boundary positions in any order, the dimension of the state space at a particular position cannot depend on the order of selection, and thus can be computed once and for all.

A *trellis-oriented generator matrix* is a useful tool for calculating and exhibiting state space dimensions. Let us first fix a set of positions for which we wish to exhibit states; this could be the positions between every adjacent pair of coordinates, or a subset of such positions, such as the positions corresponding to the boundaries of the sections in our few-section trellis diagrams in the main text. A generator matrix is called trellis-oriented if, at each position for which we wish to exhibit states, there are precisely K_s generators whose span covers that position, where K_s is the dimension of the state space at that position. Any generator matrix can always be brought into trellis-oriented form by elementary row operations.

Example: Let us compute state space dimensions for the (16,5) Reed–Muller code, with the coordinate order determined by the construction from $G_{(16,16)} = G_{(2,2)}^4$. Considering all 17 possible positions (including the trivial ones where the entire code is in the past or future), a standard generator matrix based on the construction $G_{(16,5)} = G_{(4,3)}G_{(4,1)} + G_{(4,1)}G_{(4,3)/(4,1)}$ and a trellis-oriented generator matrix are as follows:

1111	1111	0000	0000	**1111**	**1111**	0000	0000
1111	0000	1111	0000	0000	**1111**	**1111**	0000
1100	1100	1100	1100	0000	0000	**1111**	**1111**
1010	1010	1010	1010	00**11**	**0011**	**1100**	**1**100
1111	1111	1111	1111	0**101**	**0101**	**1010**	**101**0.

The spans of each generator in the trellis-oriented generator matrix have been highlighted. The dimensions K_p, K_f, and K_s for all 17 possible positions are then

K_p	0	0	0	0	0	0	0	0	1	1	1	1	2	2	3	4	5
K_f	5	4	3	2	2	1	1	1	1	0	0	0	0	0	0	0	0
K_s	0	1	2	3	3	4	4	4	3	4	4	4	3	3	2	1	0.

This is consistent with the trellis diagram of Fig. 9, which has $2^3 = 8$ states at positions 4, 8, and 12, although we now see that we have concealed 16-state state spaces at positions 5–7 and 9–11 (this seems fair enough, because there are no mergers or divergences at these positions).

Note that these sizes of the state spaces do depend on the ordering of the coordinates. For example, the (8,4)* code has a 16-state trellis (as large as it could have, given the bound of Wolf [6]), as opposed to four states for the (8,4) code.

We now show that a code C and its dual $C^\perp$ have state spaces of the same dimension, as expected.

Lemma 6: Let C and $C^\perp$ be dual codes; then C^p and $(C^\perp)_p$ are dual codes.

Proof: $(C^\perp)_p$ is the set of all codewords in $C^\perp$ that are zero in the future. Since words in $C^\perp$ are orthogonal to every word in C, every word in $(C^\perp)_p$ is orthogonal to the past portion of every word in C, i.e., to C^p. Hence $(C^\perp)_p \subseteq (C^p)^\perp$. Conversely, every word in the code $(C^p)^\perp$ dual to C^p, extended with zeros in the future, is orthogonal to all words in C; hence $(C^p)^\perp \subseteq (C^\perp)_p$.

Corollary: For any partition into past and future, the dimensions of the state spaces of C and $C^\perp$ are identical.

Proof: From the lemma, $(C^\perp)_p$ is dual to C^p, and $(C^\perp)^p$ is dual to C_p. Thus $(C^\perp)_p$ has dimension $N_p - K^p$, and $(C^\perp)^p$ has dimension $N_p - K_p$. The partitions C^p/C_p and $(C^\perp)^p/(C^\perp)_p$ thus both give state spaces of dimension $K_s = K^p - K_p = (N_p - K_p) - (N_p - K^p)$.

Example: The (16,11) Reed–Muller code is dual to the (16,5) code. A standard generator matrix based on the construction $G_{(16,11)} = G_{(4,4)}G_{(4,1)} + G_{(4,3)}G_{(4,3)/(4,1)} + G_{(4,1)}G_{(4,4)/(4,3)}$ and a trellis-oriented generator matrix are as follows:

1111	0000	0000	0000	**1111**	0000	0000	0000
1100	1100	0000	0000	00**11**	**1100**	0000	0000
1010	1010	0000	0000	0000	**1111**	0000	0000
1111	1111	0000	0000	0000	00**11**	**1100**	0000
1100	0000	1100	0000	0000	0000	**1111**	0000
1010	0000	1010	0000	0000	0000	00**11**	**1100**
1111	0000	1111	0000	0000	0000	0000	**1111**
1000	1000	1000	1000	0**101**	**1010**	0000	0000
1100	1100	1100	1100	0000	0**101**	**1010**	0000
1010	1010	1010	1010	0000	0000	0**101**	**1010**
1111	1111	1111	1111	000**1**	**0001**	**1000**	**1**000.

The dimensions K_p, K_f, and K_s for all 17 possible positions are then:

K_p	0	0	0	0	1	1	2	3	4	4	5	6	7	8	9	10	11
K_f	11	10	9	8	7	6	5	4	4	3	2	1	1	0	0	0	0
K_s	0	1	2	3	3	4	4	4	3	4	4	4	3	3	2	1	0.

This is consistent with both the result just obtained and the trellis of Fig. 9. Note that the maximum branch complexity of a 16-section trellis diagram is 32, the same as for the four-section trellis diagram, so that decoding on a sequential bit-by-bit basis with the Viterbi algorithm could in fact be as efficient as our iterative decoding procedure.

The generator matrix for the Golay code, from the cubing construction

$$G_{(24,12)} = G_{(3,3)}G_{(8,1)} + G_{(3,2)}G_{(8,4)/(8,1)} + G_{(3,1)}G_{(8,4)^*/(8,1)},$$

is

1111 1111 0000 0000 0000 0000
0000 0000 1111 1111 0000 0000
0000 0000 0000 0000 1111 1111
1111 0000 1111 0000 0000 0000
0000 0000 1111 0000 1111 0000
1100 1100 1100 1100 0000 0000
0000 0000 1100 1100 1100 1100
1010 1010 1010 1010 0000 0000
0000 0000 1010 1010 1010 1010
0111 1000 0111 1000 0111 1000
1001 1100 1001 1100 1001 1100
0101 0110 0101 0110 0101 0110.

If we put this into trellis-oriented form, we arrive at a matrix such as

1111 1111 0000 0000 0000 0000
0000 **1111 1111** 0000 0000 0000
0000 0000 **1111 1111** 0000 0000
0000 0000 0000 **1111 1111** 0000
0000 0000 0000 0000 **1111 1111**
00**11 0011 1100** 1100 0000 0000
0000 0000 00**11 0011 1100** 1100
0**110 0110 0110 0110** 0000 0000
0000 0000 0**110 0110 0110 0110**
000**1 0001 0001 1110 1000** 1000
0000 0**101 0011 1001 1010** 0000
0000 00**11 0110 1010** 1100 0000,

showing that the state space dimensions are

K_s 0 123 4 567 6 789 8 987 6 765 4 321 0.

This is consistent with the three-section trellis diagram of Fig. 21 but shows that that diagram conceals a state space of 256 states at the center of the code, and even 512 states one position away from the center (where, however, there are no mergers or divergences). This indicates the advantages of the decoding algorithm given in the main text over straightforward Viterbi decoding.

B. The Trellis Diagram of a Lattice

The analysis used for block codes may be extended to lattices (or any additive group of N-tuples). Let Λ be a lattice, and, given a partition of coordinates into past and future, let Λ_p and Λ_f be the sublattices consisting of elements of Λ that are zero in future and past, respectively. Then the state space Σ consists of the equivalence classes of Λ modulo the union of Λ_p and Λ_f: $\Sigma = \Lambda/(\Lambda_p \cup \Lambda_f)$. If Λ^p and Λ^f are the restrictions of Λ to past and future, respectively, then Σ is also isomorphic to Λ^p/Λ_p or to Λ^f/Λ_f. A trellis diagram for Λ (resembling a squaring construction) consists of $|\Sigma|$ past branches, each representing a coset of Λ_p in the partition Λ^p/Λ_p, concatenated with $|\Sigma|$ future branches, each representing a coset of Λ_f in the partition Λ^f/Λ_f.

For calculation, if Λ is a binary mod-2^m lattice, then it is convenient to use generators that are N-tuples of integers modulo 2^m.

For example, if Λ is Λ_{16}, and the past is the first 8-tuple, then Λ_p and Λ_f are each equal to RE_8 (in the respective 8-tuples where they are nonzero), and Λ^p and Λ^f are each equal to E_8, so the state space Σ is the set of equivalence classes in the partition E_8/RE_8, which has order 16. On the other hand, if we take the first 4-tuple as the past, then Λ_p is $2D_4$, while Λ^p is D_4, and the states are the cosets of the partition $D_4/2D_4$, which also has order 16. By using a trellis-oriented generator matrix for $R\Lambda_{16}$, we can compute the (binary) dimension K_s for each possible position:

Position	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
K_s	0	2	3	4	4	5	5	5	4	5	5	5	4	4	3	2	0

This could also be deduced by regarding the state space as the Cartesian product of the (16,11) and (16,1) [or (16,15) and (16,5)] state spaces.

A trellis-oriented generator matrix for the Leech lattice is

2222 0000 0000 0000 0000 0000
00**22 22**00 0000 0000 0000 0000
0000 **2222** 0000 0000 0000 0000
0000 00**22 22**00 0000 0000 0000
0000 0000 **2222** 0000 0000 0000
0000 0000 00**22 22**00 0000 0000
0000 0000 0000 **2222** 0000 0000
0000 0000 0000 00**22 22**00 0000
0000 0000 0000 0000 **2222** 0000
0000 0000 0000 0000 00**22 22**00
0000 0000 0000 0000 0000 **2222**
0**202 20**20 0000 0000 0000 0000
0000 0**202 20**20 0000 0000 0000
0000 0000 0**202 20**20 0000 0000
0000 0000 0000 0**202 20**20 0000
0000 0000 0000 0000 0**202 20**20
00**02 0002 20**00 2000 0000 0000
0000 0000 00**02 0002 2000** 2000
1111 1111 1111 1111 0000 0000
0000 0000 **1111 1111 1111 1111**
0000 00**02 $\bar{1}$111 1111** 2000 0000
0000 **1111 0002 $\bar{1}$111 1111** 0000
00**11 0011 02$\bar{1}$1 0011 1100** 1100
0101 0101 2$\bar{1}$01 0101 1010 1010,

where $\bar{\mathbf{1}}$ denotes $-\mathbf{1}$, showing that the state space dimensions are

K_s 0 246 6 888 8 −10− 10 −10− 8 888 6 642 0.

This is consistent with the three-section trellis diagram of Fig. 23, but shows that that diagram conceals a state space of 1024 states at the center position. The center sections of the last four generators are an alternative set of SMOG generators.

C. The Trellis Diagram of a Partition

Let S/T be a partition of a group S of N-tuples into M cosets of a subgroup T. A trellis diagram for such a partition has one initial node and M final nodes; the set of all paths from the

initial node to each final node represents the elements of each subset T, and the union of all these paths represents S. (Alternatively, of course, we could have M initial nodes and one final node.) Again, we are interested in the minimal state space at each intermediate position.

Again, let the first N_p coordinates be the past and the remainder the future. Let T_p be the subgroup of T which is nonzero only in the past, and let S^p be the group of all restrictions of S to the past. Then the state space at position N_p is the set of equivalence classes of S^p modulo T_p, and each past branch represents a coset of T_p in the partition S^p/T_p. Similarly, each future branch represents a coset of T_f in the partition S^f/T_f.

Example: Let us compute state space sizes for the eight-way partition $(8,7)/(8,4)$. For each N_p, let K^p be the dimension of $(8,7)^p$, and let K_p be the dimension of $(8,4)_p$; then $K_s = K^p - K_p$ is the dimension of the state space:

Position N_p	0	1	2	3	4	5	6	7	8
K^p	0	1	2	3	4	5	6	7	7
K_p	0	0	0	0	1	1	2	3	4
K_s	0	1	2	3	3	4	4	4	3

It is no coincidence that this is the same as the first eight positions of the (16,11) trellis, since $(16,11) = |(8,7)/(8,4)|^2$.

For a lattice example, take the 256-way partition $E_8/2E_8$ that occurs in Λ_{24} and Λ_{32}, with computation using mod-4 generators (as in the Leech lattice matrix):

Position N_p	0	1	2	3	4	5	6	7	8
K^p	0	2	4	6	7	9	10	11	12
K_p	0	0	0	0	1	1	2	3	4
K_s	0	2	4	6	6	8	8	8	8

This shows that there are four-way mergers not only at the position $N_p = 4$ but also at 6, 7, and 8, as we have already seen in the initial and final sections of the Leech lattice.

REFERENCES

[1] G. D. Forney, Jr., "Coset codes—Part I: Introduction and geometrical classification," *IEEE Trans. Inform. Theory*, this issue, pp. 1123–1151.

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

[3] L. F. Wei, "Trellis-coded modulation with multidimensional constellations," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 483–501, 1987.

[4] G. Ungerboeck, "Trellis-coded modulation with redundant signal sets. Part II: State of the art," *IEEE Commun. Mag.*, vol. 25, no. 2, pp. 12–21, 1987.

[5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. New York: North Holland, 1977.

[6] J. K. Wolf, "Efficient maximum likelihood decoding of linear block codes using a trellis," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 76–80, 1978.

[7] W. C. Gore, "Further results on product codes," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 446–451, 1970.

[8] N. J. A. Sloane and D. S. Whitehead, "A new family of single-error-correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 717–719, 1970.

[9] M. Plotkin, "Binary codes with specified minimum distances," *IEEE Trans. Inform. Theory*, vol. IT-6, pp. 445–450, 1960.

[10] E. L. Blokh and V. V. Zyablov, "Coding of generalized concatenated codes," *Problems Inform. Trans.*, vol. 10, pp. 218–222, 1974.

[11] V. A. Zinov'ev, "Generalized concatenated codes," *Problems Inform. Trans.*, vol. 12, pp. 5–15, 1976.

[12] J. Leech and N. J. A. Sloane, "Sphere packings and error-correcting codes," *Can. J. Math.*, vol. 23, pp. 718–745, 1971.

[13] E. S. Barnes and G. E. Wall, "Some extreme forms defined in terms of Abelian groups," *J. Australian Math. Soc.*, vol. 1, pp. 47–63, 1959.

[14] G. D. Forney, Jr., R. G. Gallager, G. R. Lang, F. M. Longstaff, and S. U. Qureshi, "Efficient modulation for band-limited channels," *IEEE J. Select. Areas Commun.*, vol. SAC-2, pp. 632–647, 1984.

[15] E. L. Cusack, "Error control codes for QAM signalling," *Electron. Lett.*, vol. 20, pp. 62–63, 1984.

[16] E. S. Barnes and N. J. A. Sloane, "New lattice packings of spheres," *Can. J. Math.*, vol. 35, pp. 117–130, 1983.

[17] A. Bos, J. H. Conway, and N. J. A. Sloane, "Further lattice packings in high dimensions," *Mathematika*, vol. 29, pp. 171–180, 1982.

[18] N. J. A. Sloane, S. M. Reddy, and C. L. Chen, "New binary codes," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 503–510, 1972.

[19] N. J. A. Sloane, "Tables of sphere packings and spherical codes," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 327–338, 1981.

[20] J. H. Conway and N. J. A. Sloane, "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.

[21] G. D. Forney, Jr., "Review of random tree codes," NASA Ames Res. Cen., Contract NAS2-3637, NASA CR 73176, Final Rep., Dec. 1967, Appx. A.

[22] A. J. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 260–269, 1967.

[23] R. W. D. Booth, M. A. Herro and G. Solomon, "Convolutional coding techniques for certain quadratic residue codes," in *Proc. 1975 Int. Telemetering Conf.*, pp. 168–177.

[24] G. Solomon and H. C. A. van Tilborg, "A connection between block and convolutional codes," *SIAM J. Appl. Math.*, vol. 37, pp. 358–369, 1979.

[25] G. D. Forney, Jr., "Coset codes III: Ternary codes, lattices, and trellis codes," in preparation.