A NEW GENERALIZATION OF REED-MULLER CODES

Todd D. Vance

Abstract. An error-correcting code can be defined as a set of functions mapping P, called the set of *places*, to A, called the *alphabet*. With classical Generalized Reed-Muller Codes, P is an m-dimensional vector space F^m over a finite field F, and A is just the finite field F. Then, $C =$ GRM(ν, m) is defined to be the set of all functions from P to A which, when represented as a polynomial of minimal degree through Lagrange interpolation, (see [2], for example) has degree less than or equal to ν.

This procedure can be generalized. $C = A_\nu$ is taken to be an element of the filtration of some filtered F-algebra B. A is another F-algebra, and $P =$ HOM$_{ALG}$ (B, A). Then, $C = C_\nu(B, A)$ is the set of elements of B_ν viewed as functions from P to A via $b(x) := x(b)$ for $x \in P$ and $b \in B$.

1. Filtered Algebras.

Definition 1 (Algebra). Let A be a vector space over a field F. In addition, define a multiplication $\mu : A \times A \to A$ that makes A a ring with unity. Assume also that F is injected in the center of A via $f \mapsto f1$, where 1 is the identity of A. Then, A is an *F-algebra* or simply an *algebra*.

Definition 2 (Algebra Homomorphism). Let $f\colon B \to A$, where A and B are F-algebras, be a linear map of vector spaces that is also a ring homomorphism taking the unit of B to the unit of A. Then, f is called a *homomorphism* from B to A. The set of all homomorphisms from B to A will be denoted HOM$_{ALG}$ (A, B).

An example which motivates the remainder of the paper follows: let F be a field and X be any set. Then, we define the *polynomial algebra* with coefficients in F and indeterminates in X as the algebra $F[X]$: let $\hat{X}$ be the free Abelian monoid generated by X. Then, the underlying set of $F[X]$ is the vector space over F with standard basis $\hat{X}$. Multiplication is just the multiplication in $\hat{X}$ extended bilinearly to all of $F[X]$. For example, if $X = \{x_1, x_2, \ldots, x_n\}$, then $F[X] = F[x_1, x_2, \ldots, x_n]$ is just the set of all polynomials over F with variables $x_1, x_2, \ldots, x_n$ along with the standard polynomial addition and multiplication.

It can be shown that $F[X]$ is a free commutative F-algebra over the set X. This means that, given any set map $\phi : X \to A$, A any algebra, there is a unique algebra homomorphism $\phi^\sharp\colon F[X] \to A$ that extends the domain of ϕ as a set map. For example, if $X = \{x_1, x_2, \ldots, x_m\}$ is a finite set and $F[X]$ is the m-variable polynomial algebra over F, then let $A = F$ be the one-dimensional algebra. Then, a set map $\phi\colon F[X] \to F$ can be viewed as substitution of field elements for the variables. That is, each such ϕ is identified with an m-tuple $(a_1, a_2, \ldots, a_m) \in F^m$. Then, $\phi^\sharp$ is just the homomorphism from $F[X]$ to F that sends a polynomial f to $f(a_1, a_2, \ldots, a_m)$. In fact, all homomorphisms from $F[X]$ to F arise in this way (by restriction of the homomorphism to $X \subset F[X]$). Thus, we have the identification of sets $\mathrm{HOM}_{ALG}\ (F[X], F) = F^m$. More generally, for any X and any F-algebra A, we have $\mathrm{HOM}_{ALG}\ (F[X], A) = A^X$, where A^X is the set of all set maps from X to A.

Definition 3 (Filter). Let B be an F-algebra. Let $\mathbb{Z}^+$ be the set of non-negative integers, i.e. $\mathbb{Z}^+ = \{0, 1, 2, \ldots\}$. Suppose

$$B = \bigcup_{\nu \in \mathbb{Z}^+} B_\nu$$

where

$$B_0 \subset B_1 \subset B_2 \subset \cdots .$$

If, in addition, $B_\nu B_\mu \subset B_{\nu+\mu}$ for $\nu, \mu \in \mathbb{Z}^+$, then we say B is *filtered.* The list $\{B_0, B_1, \ldots\}$ is called a *filter* on B.

A filter is just a generalization of the degree of a polynomial. For example, if $B = F[x_1, \ldots, x_m]$ is the polynomial ring of m variables, then the standard filtering on B is

$$B_\nu = \{f \in B \mid \deg f \leq \nu\}.$$

More information about algebras and filtered algebras can be found in [4] and [5].

2. Algebraic Reed-Muller Codes.

Definition 4 (Code). Let A and P be sets. Let A^P be the set of all set maps $f\colon P \to A$. Then a *code* is a subset $C \subset A^P$. A is called the *alphabet* of the code and P is the set of *places.*

Most often P and A, and therefore C are finite. Also, A is often taken to be a field and C is taken to be a vector subspace of A^P, which has a vector space structure on it through pointwise addition and scalar multiplication of the functions. See [1] for more information about codewords defined as functions.

Let B be any filtered F-algebra (with filtration $\{B_0, B_1, \dots\}$) and A another algebra. Then, let $P = \text{HOM}_{ALG}\ (B, A)$. Then, we have a set map $\rho: B \to A^P$ defined as follows: for $b \in B$ and $x \in P$, $\rho(b): P \to A$ via $\rho(b)(x) = x(b)$. Note that more than one element of B can have the same image in A^P under ρ.

Definition 5 (Algebraic Reed-Muller Code). Let F be any field, and B, $\{B_\nu\}$, A, P, and ρ be as above. The code

$$C_\nu(B, A) = \{c \in A^P \mid \rho(b) = c \text{ for some } b \in B_\nu\}$$

is called the ν-th order *algebraic Reed-Muller code* in B and over A.

For example, if $A = F$ is a finite field and $A = F[x_1, \dots, x_m]$, then the $C_\nu(B, A)$ are just the classical generalized Reed-Muller codes which are well studied and often used in applications. Thus, we have a new generalization of Reed-Muller codes. (More information about classical generalized Reed-Muller codes can be found in [6], [3], and [1].)

Note that it is routinely shown that if $A = F$ is a finite field and B any filtered algebra, then the $C_\nu(B, A)$ are equivalent to classical generalized Reed-Muller codes with some coordinate positions deleted. On the other hand, if A is an algebra that is not a field, then we have a generalization of Reed-Muller codes to a large class of non-field alphabets.

References

1. E. F. Assmus and J. D. Key, *Designs and Their Codes*, Vol. 103 of *Cambridge Tracts in Mathematics*, Cambridge University Press, Cambridge, 1993.

2. C. de Boor, “Topics in Multivariate Approximation Theory,” *Topics in Numerical Analysis*, Vol. 965 *Lecture Notes in Mathematics*, Springer-Verlag, New York, 1982, 39–78.

3. P. Delsarte, J.-M. Goethals, and F. J. MacWilliams, “On Generalized Reed-Muller Codes and Their Relatives,” *Information and Control*, 16 (1970), 403–442.

4. N. Jacobson, *Basic Algebra II*, 2nd ed., W. H. Freeman and Company, New York, 1989.

5. C. Kassel, *Quantum Groups*, Vol. 155 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1995.

6. T. Kasami, S. Lin, and W. W. Peterson, "Generalized Reed-Muller Codes," *Electron. Commun. Japan*, 51 (1968), 96–104.

Todd D. Vance
HC 66, Box 55
Moorefield, WV 26836