Counting Minimal Generator Matrices

Kim E. Lumbard Robert J. McEliece [1]
California Institute of Technology, Pasadena, CA 91125

Abstract — **Given a particular convolutional code C, we wish to find all minimal generator matrices $G(D)$ which represent that code. A standard form $S(D)$ for a minimal matrix will be defined, and then all standard forms for the code C will be counted (this is equivalent to counting special pre-multiplication matrices $P(D)$). It will then be shown that all the minimal generator matrices $G(D)$ are contained within the 'ordered row permutations' of these standard forms, and that all these permutations are distinct. Finally, the result will be used to place a simple upper bound on the possible number of convolutional codes.**

I. Definitions

Given any $k \times n$ polynomial matrix $G(D) = [g_{ij}(D)]$, define the *constraint lengths* ν_i of $G(D)$ as the maximum degree of any polynomial in row i, i.e. $\nu_i = \max_{j=1}^{n}\{\deg g_{ij}(D)\}$.

Define a *minimal* generator matrix $G(D)$ for C as does Forney [2, p. 494]. A minimal matrix $S(D)$ is in *standard form* if the row degrees ν_i are ordered $\nu_1 \le \nu_2 \le \ldots \le \nu_k$.

Note that the set $\{\nu_i\}_1^k$ of any minimal matrix $G(D)$ for a fixed $(n,\ k,\ m)$ convolutional code C is invariant. Call this set the *Forney Indices* $\{e_i\}_1^k$ of C, $e_1 \le e_2 \le \ldots \le e_k$.

Some of the Forney Indices may be equal; let s be the number of distinct indices. Label the distinct index values by β_j with multiplicities α_j for $j\ |_1^s\ (\equiv j = 1,\ 2,\ \ldots\ s)$. Note the β_j are strictly ordered $\beta_1 < \beta_2 < \ldots < \beta_s$.

II. Main Theorem

Given a particular (n, k, m) convolutional code C over GF(q) with Forney Indices $\{e_i\}_1^k$. The number of minimal generator matrices in standard form $S(D)$ for C is given by

$$\mathcal{S} = \prod_{i=1}^{s}\left[q^{\frac{\alpha_i(\alpha_i-1)}{2}}\prod_{h=1}^{\alpha_i}(q^h-1)\right]\prod_{j=1}^{i-1}(q^{\beta_i-\beta_j+1})^{\alpha_i\alpha_j} \qquad (1)$$

Furthermore, the total number of minimal generator matrices $G(D)$ for C is $\mathcal{KS}$, where $\mathcal{K}$ is the s-nomial coefficient

$$\mathcal{K} = \binom{k}{\alpha_1\ \alpha_2\ \ldots\ \alpha_s} = \frac{k!}{\alpha_1!\alpha_2!\ldots\alpha_s!} \qquad (2)$$

III. Proof of Main Theorem

Given two minimal matrices in standard form $S_1(D)$ and $S(D)$ representing the convolutional code C. We know

$$\exists P(D) \ni S_1(D) = P(D)S(D) \qquad (3)$$

where $P(D)$ is a unique $k \times k$ unimodular matrix of polynomials and $\det P(D) \neq 0$. Partition $P(D)$ naturally into smaller submatrices M_{ij}, where each M_{ij} is an $\alpha_i \times \alpha_j$ sized matrix. Within each M_{ij} the constraint lengths are all equal; the predictable degree property then yields

$$\deg m^{(ij)}(D) \le \beta_i - \beta_j \quad \text{for } i\ |_1^s \text{ and } j\ |_1^s \qquad (4)$$

where $m^{(ij)}(D)$ is any polynomial entry in the sub-matrix M_{ij}. $P(D)$ is seen to be a lower block diagonal matrix

$$P(D) = \left[\begin{array}{c|c|c|c} Q\{\alpha_1\} & 0 & \cdots & 0 \\ \hline R\{\alpha_2,\alpha_1\} & Q\{\alpha_2\} & \cdots & 0 \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline R\{\alpha_s,\alpha_1\} & R\{\alpha_s,\alpha_2\} & \cdots & Q\{\alpha_s\} \end{array}\right] \qquad (5)$$

where

$$\begin{aligned} \mathrm{Q}\{\alpha_i\} &= \alpha_i \times \alpha_i \text{ matrix of scalars of full rank } \alpha_i \\ \mathrm{R}\{\alpha_i,\alpha_j\} &= \alpha_i \times \alpha_j \text{ matrix of polynomials with degree} \le \beta_i - \beta_j \end{aligned}$$

Since $S(D)$ is basic, distinct $P(D)$ yield distinct $S_1(D)$; counting the standard form matrices $S_1(D)$ is thus equivalent to counting the pre-multiplication matrices $P(D)$. Let $N[A] \equiv$ "number of distinct matrices of type A". Then

$$\mathcal{S} = N[P(D)] = \prod_{i=1}^{s} N[Q\{\alpha_i\}]\prod_{j=1}^{i-1} N[R\{\alpha_i,\alpha_j\}] \qquad (6)$$

The $Q\{\alpha_i\}$ and $R\{\alpha_i,\alpha_j\}$ are easy to count, giving Eq (1).

Recall that our goal is to count minimal matrices. Given a particular minimal matrix $G(D)$, define an *ordered row permutation*(ORP) as one which preserves the sequential order of rows with equal constraint length. These ORPs form an equivalence relation on the set $\mathbf{G}$ of all minimal matrices $G(D)$ of a fixed convolutional code C. Thus $\mathbf{G}$ is the disjoint union of its equivalence classes.

The number of equivalence classes is equal to $\mathcal{S}$, the number of standard form matrices $S(D)$ (as there is exactly one $S(D)$ to every class). Each equivalence class also has the same size $\mathcal{K}$ {from Eq (2)}; thus $|\mathbf{G}| = \mathcal{KS}$.

IV. Simple Upper Bound

Consider the $k \times n$ matrices $W(D)$ with ordered $\{\nu_i\}_1^k$. Clearly, $N[W(D)] = q^{nm}(q^n-1)^k$, where $m = \sum_{i=1}^{k}\nu_i$. Any minimal matrix in standard form $S(D)$ for an $(n,\ k,\ m)$ convolutional code C with Forney Indices $\{e_i\}_1^k = \{\nu_i\}_1^k$ will be among these $W(D)$. Thus,

$$\begin{matrix}\text{Number of} \\ (n,\ k,\ m) \text{ codes} \\ C \text{ with } \{e_i\}_1^k\end{matrix} \le \left\lfloor \frac{N[W(D)]}{N[S(D)]} \right\rfloor \equiv \left\lfloor \frac{q^{nm}(q^n-1)^k}{\mathcal{S}} \right\rfloor \qquad (7)$$

This bound is fairly good for low rates.

References

[1] G. David Forney, Jr. "Convolutional Codes I: Algebraic Structure" *IEEE Trans. on IT*, Vol IT-16, pp. 720-738 (Nov 1970)

[2] G. David Forney, Jr. "Minimal Bases of Rational Vector Spaces, With Applications To Multivariable Linear Systems", *Siam J. Control*, Vol 13, No. 3, pp. 493-520 (May 1975)

[3] Thomas J. Shusta, "Enumeration of Minimal Convolutional Encoders" *IEEE Trans. on IT*, Vol IT-23, pp. 127-132 (Jan 1977)

[4] Bradley W. Dickinson, "A New Characterization of Canonical Convolutional Encoders" *IEEE Trans. on IT*, Vol IT-22, pp. 352-354 (May 1976)

[1] McEliece's contribution was supported in part by AFOSR Grant F49620-94-1-005 and in part by a grant from Pacific Bell.

0 - 7803-2015-8/94/$4.00