Separation of Recursive Convolutional Codes into Sub-Codes using Galois Field Arithmetic

Thorsten Clevorn, Birgit Schotsch, Laurent Schmalen, Peter Vary, and Marc Adrat

***Abstract*— In this paper a novel interpretation of encoding and decoding of recursive convolutional codes is presented. By means of Galois field arithmetic a code is separated into sub-codes with a single delay operator. One of these simple sub-codes is sufficient for encoding and decoding with the equivalent Trellis diagram. This paper is not targeted at performance improvements but at new insights for the analysis of recursive convolutional codes resulting in novel, possibly less complex approaches for their implementation, e.g., on a chip.**

I. Separation of Recursive Convolutional Codes

We consider exemplarily a typical rate 1/2 recursive systematic convolutional (RSC) encoder with $L = 4$ memory elements, i.e., constraint length $L+1=5$. The method itself is applicable to all recursive convolutional codes. A systematic output bit y_1 and a non-systematic output bit y_2 are computed for each input bit x. With $z^{-1}=D$, the generator polynomial $\mathbf{G}_2$ for y_2 can be written as

$$\mathbf{G}_2(z)=\frac{G_2^{\mathrm{FF}}(z)}{G_2^{\mathrm{FB}}(z)}=\frac{1+D+D^2+D^4}{1+D^3+D^4}=\frac{1+z^2+z^3+z^4}{1+z+z^4}. \quad (1)$$

The denominator $G_2^{\mathrm{FB}}(z)$ of (1) is identical to the minimal polynomial $M(z) = z^4 + z + 1$ of the cyclotomic coset $\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$ in the GF(2^4) [1, 2]. For the GF(2^4) (with primitive polynomial $P(z)=z^4+z+1$) and the minimal polynomials we refer to, e.g., [1, 2]. Using the factorization of $M(z)$ into its respective conjugates, one (not unique) possibility to separate $\mathbf{G}_2(z)$ by partial fraction expansion is

$$\mathbf{G}_2(z) = 1 + \frac{\alpha^{11}}{z+\alpha} + \frac{\alpha^{7}}{z+\alpha^2} + \frac{\alpha^{14}}{z+\alpha^4} + \frac{\alpha^{13}}{z+\alpha^8} \quad . \quad (2)$$

Each of the partial fractions in (2) resembles an elementary filter and can be considered as a separate *sub*-generator polynomial $\mathbf{G}_2^{(g)}(z)$ with only a single non-binary delay operator $\mathcal{D}$ and the non-binary output $y_2^{(g)} \in \mathrm{GF}(2^4)$. We get

$$\mathbf{G}_2(z) = 1 + \sum_{g=0}^{3} \frac{(\alpha^{11})^{2^g}}{z+\alpha^{2^g}} \quad \text{and} \quad y_2 = x + \sum_{g=0}^{3} y_2^{(g)}. \quad (3)$$

Note, despite all of the *sub*-encoders operating in the GF(2^4), the output y_2 of (3) is still a single bit, i.e., $y_2 \in \{0, 1\} = \mathrm{GF}(2)$.

II. Complexity Reduction by Cyclotomic Cosets

For the chosen partial fraction expansion in (2) the numerators (or output coefficients) $\{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}$ as well as the denominators (or feedback coefficients) $\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$ of the sub-encoders $g=0...3$ in (2) and (3) each belong to the same cyclotomic coset $\mathbb{A}$ and are in their "natural" order[1]. It can be shown that this holds also for the states $v_0^{(g)}$ and $v_1^{(g)}$ and the output $y_2^{(g)}$ of all sub-encoders. Thus, it is sufficient to compute only the values for one sub-encoder, e.g., $\mathbf{G}_2^{(0)}$. The other values can be determined by using the consecutive elements of the respective $\mathbb{A}$ (with wrap-around). Furthermore, we only need the summed output $\Sigma_{\mathbb{A}}$ of the four sub-encoders $g=0...3$ and not the internal values. With $\mathbf{G}_2$ of (3) we get

$$\Sigma_{\mathbb{A}} = \sum_{g=0}^{3} y_2^{(g)} = \sum_{g=0}^{3} \left(y_2^{(0)}\right)^{2^g} = \sum_{g=0}^{3} \left(\alpha^{11} \cdot v_1^{(0)}\right)^{2^g} . \quad (4)$$

Thus, after determining the cyclotomic coset $\mathbb{A}$ of the sub-encoder output $y_2^{(0)}$, a simple mapping of $\mathbb{A}(y_2^{(0)})$ to $\Sigma_{\mathbb{A}}$ is sufficient. For each $\mathbb{A}$ of the GF(2^m), $m=4$, $\Sigma_{\mathbb{A}} \in \{0, 1\}$ is

$$\Sigma_{\mathbb{A}} = \sum_{1}^{m/|\mathbb{A}|} \sum_{\alpha^i \in \mathbb{A}} \alpha^i \quad . \quad (5)$$

The left sum to $m/|\mathbb{A}|$, with $|\mathbb{A}|$ being the number of elements in $\mathbb{A}$, ensures that also for cyclotomic cosets $\mathbb{A}$ containing less elements than sub-encoders, the correct number m of conjugates are summed up in the second sum. The complete mapping is given in Table I. The simplified encoder using only a single non-binary delay element $\mathcal{D}$ is depicted in Fig. 1.

TABLE I

Mapping of the Cyclotomic Cosets $\mathbb{A}$ to $\Sigma_{\mathbb{A}}$.

cyclotomic coset $\mathbb{A}$	$\Sigma_{\mathbb{A}}$
$\{0\}, \{1\}, \{\alpha, \alpha^2, \alpha^4, \alpha^8\}, \{\alpha^5, \alpha^{10}\}$	0
$\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}, \{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}$	1

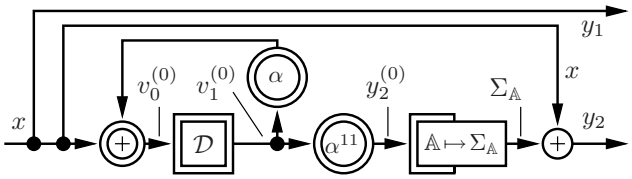

Fig. 1. Simplified RSC encoder with a single sub-encoder.

III. Summary

Using Galois field arithmetic we separated a recursive convolutional encoder into *sub*-encoders with only a single delay element. We showed that the complete code can be described by only a single *sub*-encoder with an appropriate mapping applied to the output. With the corresponding Trellis diagram for the simplified new encoder, easy decoding by well known algorithms is possible. Perhaps these new insights allow better encoder or decoder implementations on a chip or reveal unknown properties of convolutional codes.

References

[1] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*. Prentice-Hall, 1983.

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

T. Clevorn, B. Schotsch, L. Schmalen, and P. Vary are with the Institute of Communication Systems and Data Processing, RWTH Aachen University, Germany, clevorn@ind.rwth-aachen.de

M. Adrat is with FKIE/KOM, FGAN e.V., Wachtberg, Germany.

[1]By natural order we denote the generation by $\mathbb{A}=\{a, a^2, a^{2^2}, a^{2^3}, ...\}$ (possibly wrapped around depending on the start value $a=\alpha^i$).