# A Multivariate Weight Enumerator for Tail-biting Trellis Pseudocodewords 

Nigel Boston*<br>Departments of Mathematics, Electrical and Computer Engineering, University of Wisconsin, Madison, WI 53706, USA


#### Abstract

Tail-biting-trellis representations of codes allow for iterative decoding algorithms, which are limited in effectiveness by the presence of pseudocodewords. We introduce a multivariate weight enumerator that keeps track of these pseudocodewords. This enumerator is invariant under many linear transformations, often enabling us to compute it exactly. The extended binary Golay code has a particularly nice tail-biting-trellis and a famous unsolved question is to determine its minimal AWGN pseudodistance. The new enumerator provides an inroad to this problem.


Keywords: Tail-biting trellis; Binary Golay code; Pseudocodewords; Weight enumerators; Invariant theory

## Introduction

This paper makes headway into a longstanding problem, namely that of whether the Golay tail-biting trellis found by Calderbank, Forney, and Vardy [1] has any pseudocodewords of AWGN pseudoweight less than 8 . This problem was addressed by many experts in the field before being abandoned as being computationally too hard. We circumvent this issue by introducing a new kind of multivariate weight enumerator that is invariant under the action of a large group of matrices. This enumerator is not covered by the encyclopedic work of Nebe, Rains, and Sloane [2], but the method, dating back to Gleason [3], of using invariant theory so as to constrain drastically the form of the enumerator polynomial, works well. In particular, we show that there are no Golay pseudocodewords of period less than 5 and AWGN pseudoweight less than 8. Deeper explorations of these techniques should permit us to extend this result to periods of 5 and higher.

## Tail-biting Trellises

Definition: A tail-biting trellis $T=(V, E, A)$ of depth $n$ is a directed graph with vertex set $V$ and edge set $E$ such that each edge has a label taken from alphabet $A$ and with the following property: the set $V$ can be partitioned into $n$ subsets $V=V_{0} \cup V_{1} \cup \ldots \cup V_{n-1}$ such that every edge in $T$ either begins at a vertex of $V_{i}$ and ends at a vertex of $V_{i+1}$ for some i with $0 \leq i \leq n-2$ or begins at a vertex of $V_{n-1}$ and ends at a vertex of $V_{0}$.

The set of edge labels along a cycle in $T$ starting at a vertex in $V_{0}$ is an $n$-tuple in $A^{n}$. We say that $T$ represents a linear block code $\mathcal{C}$ over $A$ if $\mathcal{C}$ is precisely the set of all edge-label sequences in $T$.

Conventional trellises, corresponding to the case where $\left|V_{0}\right|=1$, have an older history dating back to the 60 's. Trellis representations of linear block codes provide efficient decoding algorithms such as the two-way, or BCJR, algorithm [4,5] and the Viterbi algorithm [6]. Their complexity depends on the state complexity $\sigma:=\max _{i}\left|V_{i}\right|$ and associated to each code is a minimal conventional trellis, unique up to isomorphism.

Tail-biting trellises date back to 1979 [7]. Their advantage is that they can have much lower state complexity (in fact $\sqrt{ }$ ) than that, $\sigma$, of the minimal conventional trellis associated to the code. Also, they are the simplest kind of factor graph with cycles. On the other hand, there are different notions of minimality [8] and so no uniqueness for minimal tail-biting trellises associated to a given code. Additionally, their construction can be hard, as in one famous case given next.

## The Extended Binary Golay Code

One of the most extraordinary binary linear codes is the [24, $12,8]$ extended binary Golay code. Muder [9] showed that the state complexity of its minimal conventional trellis is at least 256 and Forney [10] that this bound is met. It follows that any associated tail-biting trellis has state complexity at least 16 and in 1996 Forney issued the challenge of finding a tail-biting trellis meeting this bound. In 1999, Calderbank, Forney, and Vardy successfully answered this challenge [1].

The corresponding trellis-oriented generator matrix is
$\left(\begin{array}{llllllllllllllllllllllll}1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1\end{array}\right)$

## Pseudocodewords

Because of the local nature of iterative decoding algorithms they can decode to vectors that are not codewords of the original code but come from some 'covering' code instead. This is most commonly studied in the case of belief propagation algorithms on Tanner graphs of low density parity check codes, where since finite covers of Tanner

[^0]graphs are locally identical to the original graph, the algorithm can be misled by codewords associated to the cover. This leads to a theory of pseudocodewords for which advanced algebraic tools have already been developed by, for instance, Koetter, Li, Vontobel, and Walker [11]. Much work has also been carried out to define suitable pseudoweights for various channels and the minimum pseudoweight of a nonzero pseudocodeword becomes a better performance measure for the code than its minimum distance.

Tail-biting trellises also yield pseudocodewords. Namely, given $T=$ ( $V, E, A$ ) and any positive integer $m$, define tail-biting trellis $T^{m}:=\left(V^{m}\right.$, $\left.E^{m}, A\right)$ of depth $m n$ by letting $V_{i}^{m}$ be a copy of $V_{j}$ where $j=i(\bmod n)$ and letting the edges from $V_{i}^{m}$ to $V_{i+1}^{m}$ be those from $V_{i(\bmod n)}$ to $V_{(i+1)(\bmod n)}$. The edge-labels on cycles in $\mathrm{T}^{\mathrm{m}}$ starting at $V_{0}^{m}$ yield a code $C_{m}$ such that $C_{1}$ is the original code C represented by T .

Assume that $C$ is binary. If $\left(c_{0}, \ldots, c_{m n-1}\right)$ is in $C_{m}$, its associated pseudocodeword is defined to be $\mathbf{p}:=\left(p_{0}, \ldots, p_{n-1}\right)$ where $p_{j}$ counts the number of nonzero $c_{i}$ for $i(\bmod n)=j($ note that sometimes this is normalized by dividing each entry by $m$ ). We say that $\mathbf{p}$ is of period $m$. There are different kinds of pseudoweight-for example, the AWGN pseudoweight of $\mathbf{p}$ is defined to be $\left(\sum p_{i}\right)^{2} / \sum p_{i}^{2}$ [12].

In the case where $C$ is the extended Golay code, a trellis-oriented generator matrix for $C_{m}$ is given as follows. Let $M$ be the generator matrix given in section 2 . Let $A$ be the matrix obtained by zeroing out the ones in the bottom left hand corner of $M$ and $B=M-A$, i.e. the matrix obtained by zeroing out everything but the bottom left hand corner. Let $Z$ be the zero matrix of the same dimensions as $M$. Define $M_{m}$ to be the $12 m$-by- $24 m$ block matrix

$$
\left(\begin{array}{cccccc}
A & B & Z & Z & \ldots & Z \\
& Z \\
Z & A & B & Z & \ldots & Z \\
Z \\
Z & Z & A & B & \ldots & Z
\end{array}\right]
$$

Then $C_{m}$ is the $[24 m, 12 m, 8]$ binary linear code with generator matrix $M_{m}$. Note that in the limit as $m \rightarrow \infty, M_{m}$ yields the infinite recurring generator matrix for the Golay convolutional code.

Much work has been done on pseudoweights of pseudocodewords in this case, notably in Aji et al. [13] and Forney et al. [14]. The question of whether there exist nonzero pseudocodewords of AWGN pseudoweight less than 8 apparently became a major challenge but remains open to this day. There are many nontrivial near-misses - for example, there are pseudocodewords of period 2 with 2 in 2 positions, 1 in 8 positions, and 0 elsewhere, which therefore have AWGN pseudoweight $12^{2} / 16=9$, and pseudocodewords of period 3 with 3 in 2 positions, 2 in 2 positions, 1 in 6 positions, and 0 elsewhere, which therefore have AWGN pseudo weight $16^{2} / 32=8$.

This question motivated the current work. It is feasible to find all 224 codewords of $C_{2}$ and hence all corresponding pseudocodewords but to do the same with $C_{3}$ is already computationally intense. Resolving the question by brute force would require doing the same for all $C_{m}$ for $1 \leq m \leq 16$ since cycles can go around up to 16 times before necessarily returning to the same vertex of $V_{0}$.

## Pseudocodeword Weight Enumerators

Let $\mathbf{p}:=\left(p_{0}, \ldots, p_{n-1}\right)$ be a pseudocodeword of period m. Attach to $\mathbf{p}$ the monomial $x_{0}^{r_{0}} x_{1}^{r_{1}} \ldots x_{m}^{r_{m}}$ where $r_{i}$ is the number of occurrences
of $i$ in $\mathbf{p}$. Note that $r_{0}+r_{1}+\ldots+r_{m}=n$. For example, the two pseudocodewords referred to in the penultimate paragraph of section 3 yield monomials $x_{0}^{14} x_{1}^{8} x_{2}^{2}$ and $x_{0}^{14} x_{1}^{6} x_{2}^{2} x_{3}^{2}$ respectively. Note that the AWGN pseudoweight can be calculated from the corresponding monomial.

Next, define the pseudocodeword weight enumerator $W_{m}$ associated to pseudocodewords of period $m$ to be the sum of all these monomials as we run through the codewords of $C_{m}$. Note that $W_{m}$ is a polynomial in $m+1$ variables $x_{0}, \ldots, x_{m}$ with non-negative integer coefficients. So, for example, $W_{1}$ is the usual weight enumerator. For the extended Golay code,

$$
W_{1}=x_{0}^{24}+759 x_{0}^{16} x_{1}^{8}+2576 x_{0}^{12} x_{1}^{12}+759 x_{0}^{8} x_{1}^{16}+x_{1}^{24}
$$

As noted above, a brute force calculation of $W_{2}$ for the extended Golay code is feasible. We thereby obtain:

$$
\begin{aligned}
& W_{2}=x_{0}^{24}+294 x_{0}^{16} x_{1}^{8}+759 x_{0}^{16} x_{2}^{8}+9792 x_{0}^{14} x_{1}^{8} x_{2}^{2}+5152 x_{0}^{12} x_{1}^{12}+178248 x_{0}^{12} x_{1}^{8} x_{2}^{4} \\
& +2576 x_{0}^{12} x_{2}^{12}+340032 x_{0}^{10} x_{1}^{12} x_{2}^{2}+748608 x_{0}^{10} x_{1}^{8} x_{2}^{6}+24288 x_{0}^{8} x_{1}^{16}+2550240 x_{0}^{8} x_{1}^{12} x_{2}^{4} \\
& +1234980 x_{0}^{8} x_{1}^{8} x_{2}^{8}+759 x_{0}^{8} x_{2}^{16}+680064 x_{0}^{6} x_{1}^{16} x_{2}^{2}+4760448 x_{0}^{6} x_{1}^{12} x_{2}^{6}+748608 x_{0}^{6} x_{1}^{8} x_{2}^{10} \\
& +1700160 x_{0}^{4} x_{1}^{16} x_{2}^{4}+2550240 x_{0}^{4} x_{1}^{12} x_{2}^{8}+178248 x_{0}^{4} x_{1}^{8} x_{2}^{12}+680064 x_{0}^{2} x_{1}^{16} x_{2}^{6}+340032 x_{0}^{2} x_{1}^{12} x_{2}^{10} \\
& +9792 x_{0}^{2} x_{1}^{8} x_{2}^{14}+4096 x_{1}^{24}+24288 x_{1}^{16} x_{2}^{8}+5152 x_{1}^{12} x_{2}^{12}+294 x_{1}^{8} x_{2}^{16}+x_{2}^{24}
\end{aligned}
$$

Knowing $W_{2}$ is enough to establish that there are no nonzero pseudocodewords of period 2 with pseudoweight less than 8. Our strategy then will be to try to compute $W_{m}$ for all $m$ by using the fact that $W_{m}$ has some very nice transformation properties.

## Invariant Theory

In her 1962 Harvard PhD thesis [15], MacWilliams showed that the weight enumerator $W$ of the dual of a binary linear code $C$ is closely related to that of the code. In particular, $W$ is invariant under the transformation

$$
\binom{x_{0}}{x_{1}} \mapsto \frac{1}{\sqrt{2}}\left(\begin{array}{cc}
1 & -1 \\
1 & 1
\end{array}\right)\binom{x_{0}}{x_{1}}
$$

If the weights of all code words are divisible by 4 ( C is then called doubly even), then W is also invariant under the transformation

$$
\binom{x_{0}}{x_{1}} \mapsto\left(\begin{array}{cc}
1 & 0 \\
0 & \sqrt{-1}
\end{array}\right)\binom{x_{0}}{x_{1}}
$$

Thus, $W$ is invariant under all possible compositions of these two transformations, of which there are 192, forming what is called the Clifford-Weil group $G_{1}$.

In 1970, Gleason [3] observed that this imposes a strong restriction on the structure of W , since every homogeneous polynomial in $\mathrm{x}_{0}, \mathrm{x}_{1}$ invariant under $\mathrm{G}_{1}$ is a polynomial in the weight enumerators $W_{H}\left(=x_{0}^{8}+14 x_{0}^{4} x_{1}^{4}+x_{1}^{8}\right)$ of the extended [8, 4, 4] Hamming code and $W_{G}\left(=W_{1}\right.$ given in the previous section) of the extended Golay code. This permits quick computation of weight enumerators of large selfdual doubly even codes.

In the last four decades, hundreds of papers have appeared generalizing and applying Gleason's results, culminating in the book [2] by Nebe, Rains, and Sloane unifying these theories. They define the

Type of a self-dual code such that the weight enumerator of any code of that Type lies in the invariant ring of a certain Clifford-Weil group associated with that Type, and furthermore such that this invariant ring is spanned by weight enumerators of that Type. There are also fascinating algebra isomorphisms due to Broué and Enguehard between various rings of modular forms and rings of weight enumerators [16].

We are guided by a similar philosophy below, in seeking to compute the multivariate weight enumerators $W_{m}$ for the Golay case. This theory is new, not covered by the above book.

## Symmetric Power Invariance

Let $A$ be a 2-by-2 matrix. Then A acts on $x_{0}, x_{1}$ by linear transformations. Substituting these into $x_{0}^{m}, x_{0}^{m-1} x_{1}, x_{0}^{m-2} x_{1}^{2}, \ldots, x_{1}^{m}$, yields a linear transformation of those $m+1$ terms and hence produces an $m+$ 1-by- $m+1$ matrix, denoted $\operatorname{Sym}^{m}(A)$. For example, if $A=\frac{1}{\sqrt{2}}\left(\begin{array}{cc}1 & -1 \\ 1 & 1\end{array}\right)$ then $A\left(x_{0}\right)=\frac{1}{\sqrt{2}}\left(x_{0}-x_{1}\right)$ and so $A\left(x_{0}^{2}\right)=\left(\frac{1}{\sqrt{2}}\left(x_{0}-x_{1}\right)\right)^{2}=\frac{1}{2}\left(x_{0}^{2}-2 x_{0} x_{1}+x_{1}^{2}\right)$. Similarly one computes that $A\left(x_{0} x_{1}\right)=\frac{1}{2}\left(x_{0}^{2}-x_{1}^{2}\right)$ and $A\left(x_{1}^{2}\right)=\frac{1}{2}\left(x_{0}^{2}+2 x_{0} x_{1}+x_{1}^{2}\right)$. It follows that $A$ sends

$$
\left(\begin{array}{l}
x_{0}^{2} \\
x_{0} x_{1} \\
x_{1}^{2}
\end{array}\right) \mapsto \frac{1}{2}\left(\begin{array}{ccc}
1 & -2 & 1 \\
1 & 0 & -1 \\
1 & 2 & 1
\end{array}\right)\left(\begin{array}{l}
x_{0}^{2} \\
x_{0} x_{1} \\
x_{1}^{2}
\end{array}\right)
$$

The above 3-by-3 matrix is then $\operatorname{Sym}^{2}(A)$. Applying this to all 192 matrices in the Clifford-Weil group $G_{1}$ above yields 96 3-by-3 matrices (we say that the homomorphism Sym ${ }^{2}$ has a kernel of order 2). Each such matrix defines a linear transformation in $x_{0}, x_{1}, x_{2}$. One can check using a computer algebra system such as Magma that $W_{2}$ is invariant under all 96 of these transformations.

In fact $W_{2}$ is also invariant under the transformation $x_{0} \mapsto x_{0}, x_{1} \mapsto x_{1}, x_{2} \mapsto-x_{2}$. Compositions formed from this and the 96 transformations above yield a group $G_{2}$ of 384 3-by- 3 matrices, all leaving $W_{2}$ invariant.

If we had known a priori that $W_{2}$ is invariant under $G_{2}$, then we could have used Magma to compute all homogeneous degree 24 polynomials invariant under $G_{2}$ (it turns out that they are spanned by 6 such polynomials $I_{1}, \ldots, I_{6}$ ). The correct linear combination of those 6 polynomials (in fact $I_{1}+294 I_{6}$ ) could then be found by exploiting a computation of low weight codewords of $C_{2}$. This is the strategy we employ in section 7 below to calculate $W_{3}$ and $W_{4}$, which would otherwise have been out of reach. The main (nontrivial) point, proven in David Conti's upcoming University College Dublin PhD thesis, is that, for every $m, W_{m}$ is invariant under every matrix $\operatorname{Sym}^{m}(A)$ where $A$ is in $G_{1}$ and under certain diagonal matrices. This produces a typically large group $G_{m}$ of $(m+1)$-by- $(m+1)$ matrices leaving $W_{m}$ invariant.

The group $G_{2}$ is the group of 3-by-3 quasipermutation matrices which have exactly one nonzero entry, a 4th root of unity, in every row and every column. This makes it isomorphic to the wreath product $C_{4}$ 乙 $S_{3}$. It is also a complex reflection group, which makes its invariant theory particularly nice, leading to the following pretty formula. Let

$$
\begin{aligned}
& f\left(x_{0}, x_{1}, x_{2}\right):=x_{0}^{24}+x_{1}^{24}+x_{2}^{24}+759\left(x_{0}^{16} x_{1}^{8}+x_{0}^{16} x_{2}^{8}+x_{0}^{8} x_{1}^{16}+x_{0}^{8} x_{2}^{16}+x_{1}^{16} x_{2}^{8}+x_{1}^{8} x_{2}^{16}\right) \\
& +2576\left(x_{0}^{12} x_{1}^{12}+x_{0}^{12} x_{2}^{12}+x_{1}^{12} x_{2}^{12}\right)+3186 x_{0}^{8} x_{1}^{8} x_{2}^{8} \\
& \text { Then } W_{2}\left(x_{0}, x_{1}, x_{2}\right)=2^{12} f\left(\left(x_{0}+x_{2}\right) / 2, x_{1},\left(x_{0}-x_{2}\right) / 2\right)
\end{aligned}
$$

## Golay Pseudocodeword Enumerators

We move first to computing $W_{3}$. The above theory shows that $W_{3}$ is invariant under $\operatorname{Sym}^{3}(A)$ for A in $G_{1}$. This yields 192 transformations. In addition, $W_{3}$ is invariant under the transformation
$x_{0} \mapsto x_{0}, x_{1} \mapsto x_{1}, x_{2} \mapsto-x_{2}, x_{3} \mapsto-x_{3}$. All possible compositions of the above transformations yield a group $\mathrm{G}_{3}$ of 1152 4-by- 4 matrices leaving $W_{3}$ invariant.

Next, using Magma, we compute all homogeneous degree 24 polynomials in $x_{0}, x_{1}, x_{2}, x_{3}$ invariant under $G_{3}$. Magma produces 26 polynomials $I_{1}, \ldots, I_{26}$ that span this space. Using low weight codewords in $C_{3}$ yields a simple linear combination of them that must equal $\mathrm{W}_{3}$. Namely, $I_{1}+441 I_{14}+513 I_{18}+7560 I_{22}+288 I_{23}+11520 I_{25}+4608 I_{26}$, which gives:

$$
\begin{aligned}
& W_{3}=x_{0}^{24}+441 x_{0}^{16} x_{1}^{8}+513 x_{0}^{16} x_{2}^{8}+759 x_{0}^{16} x_{3}^{8}+7560 x_{0}^{14} x_{1}^{8} x_{2}^{2}+288 x_{0}^{14} x_{1}^{6} x_{2}^{2} x_{3}^{2} \\
& +14112 x_{0}^{14} x_{2}^{10}+11520 x_{0}^{13} x_{1}^{7} x_{2}^{3} x_{3}+2304 x_{0}^{13} x_{1}^{5} x_{2}^{3} x_{3}^{3}+4608 x_{0}^{12} x_{1}^{12}+792 x_{0}^{12} x_{1}^{10} x_{2}^{2}+\ldots \\
& \ldots+7560 x_{1}^{2} x_{2}^{8} x_{3}^{14}+33291 x_{2}^{24}+16371 x_{2}^{16} x_{3}^{8}+4608 x_{2}^{12} x_{3}^{12}+441 x_{2}^{8} x_{3}^{16}+x_{3}^{24} .
\end{aligned}
$$

There are 212 terms in $W_{3}$, too many to list here, but note that each monomial that appears corresponds to pseudocodewords that have pseudoweight at least 8.

As for $W_{4}$, we similarly obtain a group $G_{4}$ of 384 5-by- 5 matrices that leave $W_{4}$ invariant. The space of homogeneous degree 24 polynomials in $x_{0}, \ldots, x_{4}$ invariant under $G_{4}$ is spanned by 153 very lengthy polynomials which Magma gives explicitly. Of these 153 polynomials, 87 have the property that every monomial occurring in them corresponds to pseudocodewords of pseudoweight at least 8 . We show that $W_{4}$ is a span of these 87 polynomials by excluding the other 66 polynomials as follows. Every such polynomial contains a monomial that occurs in it and none of the remaining 152 polynomials. Examining these special monomials, we see that, for those 66 polynomials, if the special monomial were present, it would come from a codeword of $C_{4}$ of weight at most 24 . By analyzing low weight codewords of $C_{4}$, we can show that this does not happen. Thus, there are no nonzero pseudocodewords of period $\leq 4$ of pseudoweight less than 8 .

Likewise, for $\mathrm{m} \geq 5$, there is an explicitly given group $G_{m}$ of $m$ +1 -by- $m+1$ matrices leaving $W_{m}$ invariant. Unfortunately, both the computation of homogeneous degree 24 polynomials invariant under $G_{m}$ and the analysis of low weight code words of $C_{m}$ become computationally too expensive. It is clear that there are 147 m code words of $C_{m}$ of weight 8 , but beyond that patterns are hard to spot. For example, the codewords of $C_{m}$ of weight 12 correspond to pseudocodewords either consisting of 12 ones and 12 zeros or 2 twos, 8 ones, and 14 zeros, but there is no clear, even conjectural, formula for the number of either kind.

## Conclusions and Further Work

We have introduced new and useful multivariate polynomials attached to a tail-biting trellis. These keep track of what kinds of pseudocodewords exist and indeed how many there are of each kind. This can in turn be used to measure how good the code is as regards iterative decoding, with various formulae for pseudoweight being used, depending on the channel. It has been a longstanding question to determine whether the AWGN pseudo weight of a nonzero pseudocodeword for the tail-biting trellis of the extended binary Golay code is ever less than 8 . Our new invariant theory methods allow us to answer this question in the negative for all pseudocodewords of period $\leq 4$.

Pseudocodeword weight enumerators $W_{m}$ are defined for any tail-biting trellis. It is not true, however, that they are invariant under the same group $G_{m}$ as for the Golay code above. For example, for tailbiting trellises attached to the extended [8, 4, 4] Hamming code, the polynomials $W_{m}$ are invariant under slightly smaller groups than $G_{m}$. The author's PhD student, David Conti, is developing a theory that should hopefully clarify the notion of Type for a tail-biting trellis and allow one to define an analogue of the Clifford-Weil group for each Type.

## References

1. Calderbank AR, Forney GD, Vardy A (1999) Minimal tail-biting trellises: The Golay code and more. IEEE Transactions on Information Theory 45: 14351455.
2. Nebe G, Rains EM, Sloane NJA (2006) Self-Dual Codes and Invariant Theory. Springer-Verlag.
3. Gleason AM (1971) Weight polynomials of self-dual codes and the MacWilliams identities.Gauthiers-Villars, Paris 3: 211-215.
4. Bahl LR, Cocke J, Jelinek F, Raviv J (1974) Optimal decoding of linear codes for minimizing symbol error rate. IEEE Transactions on Information Theory 20: 284-287.
5. Gallager RG (1963) Low-density parity-check codes. MA, MIT Press, Cambridge.
6. Viterbi AJ (1967) Error bounds for convolutional codes and an asymptotically

Citation: Boston N (2015) A Multivariate Weight Enumerator for Tailbiting Trellis Pseudocodewords. J Generalized Lie Theory Appl S1: 004. doi:10.4172/1736-4337.S1-004

This article was originally published in a special issue, Algebra, Combinatorics and Dynamics handled by Editor. Dr. Natalia Iyudu, Researcher School of Mathematics, The University of Edinburgh, UK
optimum decoding algorithm. IEEE Transactions on Information Theory 13: 260-269.
7. Solomon G, van Tilborg HCA (1979) A connection between block and convolutional codes. SIAM Journal of Applied Mathematics 37: 358-369.
8. Koetter R, Vardy A (2003) The structure of tail-biting trellises: minimality and basic principles. IEEE Transactions on Information Theory 49: 1877-1901.
9. Muder DJ (1988) Minimal trellises for block codes. IEEE Transactons on Information Theory 34: 1049-1053.
10. Forney GD (1994) Dimension/length profiles and trellis complexity of linear block codes. IEEE Transactions on Information Theory 40: 1741-1752.
11. Koetter R, Li WCW, Vontobel PO, Walker JL (2007) Characterizations of pseudocode words of (low-density) parity-check codes. Advances in Mathematics 213: 205-229.
12. Wiberg N (1996) Codes depending on general graphs, Doctor of Philosophy Dissertation. Department of Electrical Engineering, University of Linkoping, Sweden.
13. Aji S, Horn G, McEliece R, Xu M (1998) Iterative min-sum decoding of tail-biting codes. Proc ITW workshop, Killarney.
14. Forney GD, Koetter R, Kschischang FR, Reznik A (1999) On the effective weights of pseudocodewords for codes defined on graphs with cycles, in Codes. The IMA Volumes in Mathematics and its Applications 123: 101-112.
15. MacWilliams FJ (1963) A theorem on the distribution of weights in a systematic code. Bell Syst Tech J 42: 79-94.
16. Solé P (2008) Codes, invariants, and modular forms, talk at Bonn MPIM.

## OMICS International: Publication Benefits \& Features

## Unique features:

- Increased global visibility of articles through worldwide distribution and indexing
- Showcasing recent research output in a timely and updated manner
- Special issues on the current trends of scientific research

Special features:

- 700 Open Access Journals
- 50,000 editorial team
- Rapid review process
- Quality and quick editorial, review and publication processing
- Indexing at PubMed (partial), Scopus, EBSCO, Index Copernicus and Google Scholar etc.
- Sharing Option: Social Networking Enabled
- Authors, Reviewers and Editors rewarded with online Scientific Credits
- Better discount for your subsequent articles

Submit your manuscript at: http://www.omicsonline.org/submission


[^0]:    *Corresponding author: Nigel Boston, Departments of Mathematics, and Electrical and Computer Engineering, University of Wisconsin, Madison, WI 53706, USA, Tel: 608263-4753; E-mail: boston@engr.wisc.edu
    Received July 21, 2015; Accepted August 03, 2015; Published August 31, 2015
    Citation: Boston N(2015) A Multivariate Weight Enumerator for Tail-biting Trellis Pseudocodewords. J Generalized Lie Theory Appl S1: 004. doi:10.4172/1736-4337.S1-004

    Copyright: © 2015 Boston N. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

