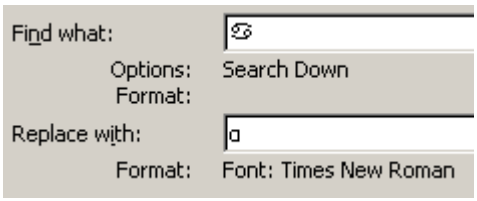
Scramblers Edit Log PhL 5.23.13

Following instructions for format conversion outlined in "plan for updating Galois". First copied over all styles. Then: There were 2887 subscripts that got converted. Then 1243 superscripts replaced. But I needed to open field codes first because a lot of my sums are that way. Another 106 subscripts. Then another 480 subscripts. Then close fields again. All this went very quickly.

Next is Greek letters. Around page 36 I have α and β stuff in Galois section. It is easy to select the ole α and replace it with a new α but you have to specify TNR font:



I replaced 87 alphas in this way. Then I replaced 66 betas.

I guess the next phase is to manually go through and fix equations which have problems. First problem on page 19 where it does not know my ⇒ type symbols. These are in the hard copy, so I can just manually put them in. Am at p 25, going OK. At page 39 OK. At page 71 OK. At p 86 OK, slow going. The big matrix equations are a pain. I am also correcting marked spelling errors. Page 101 and done!

I did a replace to remove extra spaces after periods. Probably there will be side effects of my global replacement. Also replaced flipflop with flip-flop.

Plan. I think I will read the whole thing for content only, no grammar/style edits as usual. I want to see what this thing is about, and whether it is worth publishing.

Chapter 1

1.1	ok	
1.2		
	symbols	ok
	Analysis of Figure 1	ok, not so bad
1.3		ok

Comments: I guess I always thought that the flip-flips contained the remainder, but here I am either avoiding saying that, or it is not true. We shall see.

1.4 ok, but I am confused by various claims being made, remainder, etc. Also, math not sharp.

1.5 ok, but not easy to understand, and what am I going to do with my fancy figures!!!

Comments: the idea is to explain how the two division circuits "work". I really need to ponder a way to draw the circuits and the division on the same page, otherwise hopeless to understand. But keep on reading. The pictures need an element j somewhere in the middle. My math steps are too big!

1.6 ok

1.7 ok I am not following the details very well.

1.8 ok the summary box is there.

1.9 ok

Appendix 1.1 ok a set of very tough questions I would say.

So far I have read 22 pages and it is a tough ride, AND my figures need scanning maybe.

So Chapter 1 was about hardware circuits to do poly mult and divide. Each circuit was analyzed in painful detail. We played in both time and z domain. At least I understand what the chapter was about!

Chapter 2 is next when back from Torrey. Well, here is a little head start.

Chapter 2 // resuming here June 9, 2013

2.1 ok
2.2 Galois mentioned briefly for first time
This is a long section with a lot of detail, but I basically follow it.
It leans heavily on the Galois Fields document!
Major issue: what is the period of a shift register generator with some h(x) ?
2.3 more heavy duty stuff based on Galois
2.4 I am up to page 50, need to take a break.
2.5 autocorrelation
2.6 spectral power density of a scrambler
two appendices occur here

Chapter 3 the matrix approach
3.1 review of earlier chapters
3.2 matrix solution of Fig 1
3.3 matrix solution of Fig 2
3.4 shift register generators revisited
3.5 the output of a scrambler (including a review of Leeper)
3.6 spectral density of a scrambler output
3.7 the NRZI mini-scrambler (and a scrambler summary)
3.8 matrix analysis of poly multiplier in fig 7
3.9 same for poly multiplier in Fig 8
3.10 proof that scramble/descramble really works
3.11 the Kill Sequence
another appendix
END

OK, this concludes my first very rough reading. The paper is 101 pages long. There is no overview section.

The Theory of Polynomial Processors, Shift Register Generators and Scramblers

Pondering a possible better title.

I adjusted all equation numbers to the right then removed internal contents so only the TOC at the front. subsections are 2.2, 2.3 etc, unlike all my other docs which use (a), (b) etc. Equation numbers all have three digits like (1.2.3). I will leave all this stuff AS IS, not worth changing the entire notation!

June 10 I read the first 3 entire chapters of my Galois doc, since this is the basis of the scrambler one. This gives me a chance to proof the entire Galois, and I have already found some small errata. I will continue this effort tomorrow. Then I have to adjust all the links into Galois from Scrambler.

June 11: Finished my reading of Galois (skipping 3 appendices), and made a list of about 30 errata which I will handle soon. I am now current on the Galois stuff again, and am ready to go back to Scramblers tomorrow.

June 12: How should I handle references to my documents in Scrambler? There are many of them. In my sun-earth doc, I used numbers like this

[6] P. Lucht, *Rotating Frames of Reference* (http://user.xmission.com/~rimrock/ , 2012) . This paper uses names Frame S and S', basis vectors $\mathbf{e}_n$ and $\mathbf{e}'_n$, origin-connecting vector **b**, and other notations which have been utilized in the current paper. Its Appendix A has information on spherical coordinates.

[7] D. di Cicco, "Exposing the Analemma" (Sky and Telescope, June 1979, pp536-540).
D. di Cicco, "Photographing the Analemma" (Sky and Telescope, March 2000, pp135-140).
Dennis di Cicco apparently took the first-ever solar analemma strobe photo. His imaginary club of analemma photographers is slowly increasing its membership.

As shown in Ref [6] Appendix A (A.13.c), at some arbitrary poi
vectors are given in terms of the spherical unit vectors according to

With this method, I don't repeat my own name many times, and I don't need to define terms like Galois and Spectral as referring to papers.

Also, how can I make my references more generic. My xmission time may end, and the stuff can move again. The "Phil Lucht Documents" search trick works pretty well IO think. So how about this

[6] P. Lucht, *Rotating Frames of Reference* (web "phil lucht documents", 2012).

Then maybe I start off my references with these two for right now

[31] P. Lucht, *Galois Fields and Cyclic Codes* (web "phil lucht documents", 2013).

[32] P. Lucht, *Fourier Transforms and their Application to Pulse Amplitude Modulated Signals* (web "phil lucht documents", 2013).

I can change the numbers later by replacing [32] for example.

Now let's go through all of Scrambler and cement each reference to the above two papers.

Starting Over in Scrambler.

1.1. Changed Ref. The last equation is wrong because extra terms are needed. This equation is used a few times later on, so let's mark in red and continue for now.

1.2. Right away I don't like the fact that the picture has no generic i^{th} flip-flop which I can refer to in equations. This picture probably needs to be redrawn somehow.

My Symbols subsection is OK, it took me a while to catch on. I have read this section several times, there is a lot to it. I am trying to make symbols be as general as possible.

As of 5 PM, I have battled my way only through the opening two sections 1.1 and 1.2. I really has been a battle, the material needed extra words, it was I think too hard for a new reader.

1.3 I am mildly OK with this section and the hidden remainder discussion.
1.4 ok
1.5 ok

I have concluded the section on polynomial dividers. It was non-trivial to say the least, especially in regard to my fancy separate drawings. I hope the reader will feel he has gotten his money's worth out of this poly divider section with its two implementations. I have gone through 13 of 97 pages!

June 13. Resuming with poly multipliers. Today I got all the way through the end of Chapter 1, it was good progress. Did not find any big errors or problems. The Appendix 1.1 is a bit strange, it has questions people don't normally ask. So this puts me at page 33 which is in fact about 1/3 through Scrambler. I have reviewed Galois a few days ago, so Chapter 2 I hope will go as smoothly.

June 14. Starting Chapter 2. Things are now falling apart a bit. I drew Fig 1 and Fig 2 in Visio and made a few improvements. But we have a problem. I speak of this circuit as a polynomial divider but that does not work right. H(z) is a polynomial, but I(z) is not really a polynomial since it has only negative powers. This is all very confusing and needs to be cleaned up. // I spent this entire session clarifying this point with more text and more examples and I think the result is OK. I also got rid of the confusing "relabeling" of the o_n coefficients in one place. So now I am ready to start into Section 1.4 again, which already has its new picture. I do think I made things better today.

June 15. Reviewing from the very start again. Section 1.1 is fine. // OK, I have now reviewed all the way up to the start of Section 1.4. This took quite a while, I did more edits and fleshed out the examples a bit

more and added continuity text. I think this little pass was worth it. The doc is now much better than it was at the start!

Section 1.4 passes muster! I started into section 1.5 and then ran aground in the CRC section and had to completely rewrite it. In doing so, I found two large errors in Galois which I have now added to the errata. These both concern the CRC stuff and how good the correction is.

I am now done with Section 1.5 and am ready to start multipliers (once again)

Section 1.6 is OK, but I don't know how to label those descrambler figures without goofing up my whole basic scheme. I will figure out something later on.

Starting 1.7 now. I get down to my pencil drawings and now I think they are just terrible! They are impossible to understand. There must be a better set of drawings one can make to explain how these circuits work. I guess that will be the task for tomorrow.

June 16. Today I drew all new pictures and descriptions to explain how the four basic circuits work. These will replace my hand-drawn work of an earlier era. It was definitely non-trivial! Balls dinner!

June 17. Well, I had to change figure numbers, and I will now use scrambler-style and standard-form as my descriptors, rather than Figure numbers. They are now Fig 1.X for Chapter 1, so I am then flexible if these numbers have to keep changing as I add more figures later. So I have now gone through all of Chapter 1 and made these Fig changes. The last two sections 1.8 and 1.9 just became 1.10 and 1.11. Chapter 1 is 41/109 pages so a major chunk of this doc. It now needs to be reviewed yet again. I am trying to get it to stabilize and be clear. The hand drawings are now all gone, thank goodness.

This is all quite painful, lots of cosmetic changes and introducing lots of bad cross references no doubt. So a whole new pass through chapter 1 is now needed.

Chapter 1

Opening text and figures: OK

1.1 Z transform, OK. I did not check the Fourier reference, but everything else.

1.2. Type A divider.

Symbols. OK

Analysis of the Type A Divider in the z-domain. OK

Interpretation of Polynomial Division

1.3 More Interpretation of Polynomial Division

opening text OK

finite division

The Hidden Remainder

Impulse Response

1.4 The Type B Polynomial Divider

opening figure and text OK

Analysis of the Type B Divider in the z-domain OK

1.5 How Polynomial Dividers Actually Work

Operation of the Type B Divider OK

Operation of the Type A Divider OK

1.6. The Type A Polynomial Multiplier

opening text and figure 1.8 OK

Analysis of the Type A Multiplier in the z-domain OK

Interpretation of Polynomial Multiplication OK

1.7 The Type B Polynomial Multiplier OK continuing here on **June 18**
1.8 How Polynomial Multipliers Actually Work
Operation of the Type A Polynomial Multiplier OK
Operation of the Type B Polynomial Multiplier OK
1.9 Polynomial Processors in the Time Domain opening text OK
The Type A Multiplier in the Time Domain OK
The Type A Divider in the Time Domain OK
Convolution Theorem Approach OK, cleaned up some.
1.10 Simultaneous Polynomial Multiply and Divide
opening text OK, made a new version of the Figure 1.13
Analysis of the simultaneous multiply/divide circuit in the z-domain OK
1.11 Application: Cyclic Redundancy Check -- a little rocky, but it is OK, just a quick reader view

I think my Appendix 1.1 should be omitted from this paper! It is an interesting subject to me, but it is just too far afield from my main topic. A reader would be put off I think about all this discussion of rings Z and poly(z,Z_n) etc, while we are trying to do practical hardware stuff. So let's just can it! I will move it off into a storage file right now. Also, this appendix is not well-written, I think I could do a much more direct approach, but again, it just isn't too interesting to a reader interested in the rest of this paper.

Pause: OK, I have reviewed Chapter 1. All by itself it is a monograph on these mysterious circuits that I think lots of people "wonder about". I don't think they appear in a lot of books, but maybe I just don't have the right books. Web scans have not shown up much under "hardware polynomial multiplier" and things like that, so I think this Chapter 1 has value just for that sole reason.

How does this relate to the notion of a "hardware multiplier" ? Is it really just the same thing? Maybe that is the real subject of the appendix I am omitting. It does seem that "z is the base" in the connection. I guess this really is a question I need to answer in this paper !!

June 19: Did battle with first appendix comparing numbers and polys. ended with a paradox.

June 20: Resolved the paradox, and now have something reasonable to say in that appendix. But I just ran into a bug. It seems that Mod(10) = Z_{10} has an inverse for every non-zero element 1,2,3,4,5,6,7,8,9 . That would seem to make Z_{10} be a field. But I thought Z_p was only a field if p is a prime number! In fact I think I state this somewhere. Well wrong. For Mod(10), there exists no 2^{-1}. Just form the • table and there is no 1 in this row. They are all even.

This means that if my example had a 2 instead of a 3, my whole argument fails. Suppose my example was this

$$(2z + 2 + 1z^{-1} + 6z^{-2}) / (2 + 3z^{-1} + 2z^{-2}) = ????????$$

Multiplying top and bottom by z^2, our division example above becomes (we redefine I and H),

$$(2z^3 + 2z^2 + 1z + 6) / (2z^2 + 3z + 2) = I(z) / H(z)$$

This can be regarded as the following recursion relation,

$h_2 o_{n+2} = i_n - h_0 o_n - h_1 o_{n+1}$

or

$o_{n+2} = (i_n/h_2) - (h_0/h_2) o_n - (h_1/h_2) o_{n+1}$

or

$o_{n+2} = a\, i_n - b o_n - c o_{n+1}$ $\quad a \equiv (1/h_2)$ $\quad b \equiv (h_0/h_2)$ $\quad c \equiv (h_1/h_2)$

$a = (1/2)$ $\quad b = (2/2)=1$ $\quad c = (3/2)$

Now I am dead in the water! But surely the long division must work right

$$
\begin{array}{ll}
 & z + (-1/2) + \ldots \\
2z^2 + 3z + 2 & 2z^3 + 2z^2 + 1z + 6 \\
 & \underline{2z^3 + 3z^2 + 2z} \\
 & \quad -z^2 - 9z + 6 \\
 & \underline{-z^2 - (3/2)z + 1}
\end{array}
$$

Well, the quotient has this coefficient (9/2) sitting right there which you cannot replace with a digit.

Status: As of 6:30 PM, I have Appendix A written and I think it is saying what I originally wanted it to say. Meanwhile, some guy wants to pick up my washer.

I think I am now ready for a close review & edit reading of Chapter 2. So far I only did a very fast reading of this stuff.

June 21: I keep referring to the Fig 1.5 circuit by that name rather than Type B divider. Is this what I want?

Chapter 2

2.1. The Maximum Period of a Shift Register Generator OK

2.2 The State Vector Sequence of a Shift Register Generator opening text OK

The Type B Shift Register Generator Iteration Equation OK after lots of math work!

A note on Symbols -- our symbols are all going to lie in GF(p) as a simplification

Galois Field Review -- painfully edited and now I think it is OK. Had to make solid connection to Galois doc.

The Figure 1.5 Galois Iterator -- an important section. Why do I use N and not n ?

The non-terminating Remainder in polynomial division. // stopping here for the day

June 22: (Sat) continuing on the above edit pass:

The non-terminating Remainder in polynomial division. // stopping here for the day

Well I didn't get far. I got confused by the notion of a remainder sequence in a Type B divider. I rewrote my section on how dividers work and got this clarified. I was trying to show that if you clock in an extra 0 input symbol, you multiply your input polynomial by z and this gives a new division problem with a new

remainder. This fact gets used in the section I am now reviewing, but I could not understand how that power was arising. On each clock, you have a new division problem. Various pieces of this doc have to agree on this issue, I will try more tomorrow.

June 23 Sun. OK, I will try to resolve the Chapter 2 issue and then come back and update comments earlier in the doc about remainders.

As of 1:30 PM I have completed a rather extensive rewrite of Section 1.3 on Division Interpretation. A lot got added, a lot got deleted. I think I will reread all that stuff right now before going on. But first, I read the poly interp portion of Section 1.2 and it is OK, so on to 1.3.

OK, I have now reread section 1.4 and done more edits. There are a whopping 22 equations now in this section, and I have verified the correct numbering sequence.

I next installed my revamped Section 1.5 from temp11.doc into scrambler doc. So let's now do a reading of all of Section 1.5. // OK, I am now happy with all of Section 1.5 which explains how both kinds of divider circuits work.

I am now going to NOT proof the remaining sections of Chapter 1. Instead, I will now resume where I left off in the proofing/editing of Chapter 2 with the section The Figure 1.5 Galois Iterator. I want to make sure I finally have created the supporting horsepower for this section. Earlier I felt it was vague, the iterator notation was fuzzy. But of course I am now out of time on the day, the Kay deal is pending.

June 24 Mon. After much fiddling, I have now rewritten the beginning of Chapter 2 (e) on The non-terminating Remainder in polynomial division. I also added letters for previously un-indicated subsections (but not if it begins with the word Example). I then redid the equation numbers in section 2.2 so that all the Facts have numbers, just as in Galois. I then redid all references just using GA as my Galois paper, and FT as the Fourier one.

OK, I finally got through the end of Section 2.2 and I can now continue the pass:

2.3 The Output Sequence of a Shift Register Generator

Well, this is really my first attentive reading of this section. I am not fully with it, but think another reading could clinch things.

I am back on the move again, I got over the hump of " The non-terminating Remainder in polynomial division". There is still a lot to go. I am amazed at how much STUFF exists in this scrambler doc.

June 25 Tues. I will now do another review of Section 2.2

2.2 The State Vector Sequence of a Shift Register Generator -- opening text OK

(a) The State Iteration Equation for a Type B Divider -- OK

(b) A note on Symbols -- very short and OK, we limit register to be a p-ary flip-flop

(c) Galois Field Review -- very good, it flies, no problems

(d) The Galois Iterator for Fig 1.5 -- this is finally in good shape.

(e) The non-terminating Remainder in polynomial division

Unfortunately, section (e) has just collapsed on me again, I thought I had it nailed down. I say all this stuff about some polynomial called $i_n(z)$, but I still don't really know what that polynomial is! What exactly is the point of section (e) ? I made changes and will now take another shot:

(e) The non-terminating Remainder in polynomial division -- OK, now in excellent shape

2.3 The Output Sequence of a Shift Register Generator

I have gotten down to Fact 4, all is just fine, but now I have to do Appendix 2.1 for a proof of Fact 4. so I now digress to handle this appendix. // First pass was a bit rough.

OK, as of 5:30 PM I have completely nailed this appendix in every way. I will now install it from my temp1 file and we are done with it! I can now continue onward from Fact 4 (2.3.8).

Now at 7:30 PM I have made it all the way through **Section 2.3**, it was a long haul. There are still a few details I have to fix. I think this is an excellent section IIDSSM.

June 26 Weds.

Starting off with Section 2.4, will fix previous things later if not referenced.

Stop, bug found. How do we know that Type A and Type B really have the same output sequence? My analysis is only for Type A. In this case, the initial o_j values can be specified as the initial register values.

I have now backed up and reviewed Section 2.2 again, being careful to specify whether a Fact is valid for Type B only, or both Type A and Type B. This was vague before.

I have now clarified that most of Section 2.3 applies to Type A and Type B, and this confusion to me seems to have gone away at least for the moment.

I keep getting thrown back into Section 2.3, did various repairs, and will try once again on Section 2.4.

Status 9 PM. After much work, I got through the proof of Fact 4 in Section 2.4. The proof of this Fact is very complicated and I had to redo some earlier stuff so I could quote things in the proof.

Maybe I should put an equation number on the Fact about weight above 2.4.5. I think Section 2.4 has bad equation numbers anyway. Manana. There is still a very long way to go, I am about half way.

June 27 Thurs.

Scanning question: where is my little Fact concerning the value of "n" being the order of something? I first introduce order above (2.2.12). It is not mentioned again really until beyond (2.2.24).

The *period* n of h(x) is what I really want. I define this integer n above (2.3.34). It is the (x^n-1) think, and it is the n which is the number of coefficients of c(x) code word. I do a long example below (2.3.10). I use a polynomial h(x) that is not primitive and which has order 5. Maybe that is the wrong word! Well maybe in that example I mean that the order of α^3 is 5 since $(\alpha^3)^5 = \alpha^{15} = 1$. But what do we know about the period of the three h(x) shown?

OK, my GF(16) example was completely wrong because I used n = 15 instead of n = 5. It is all fixed.

I think I will now read through all of Chapter 2 again for continuity purposes, after a feeding.

2.1 OK, did many edits though.
2.2 (a) OK (b) OK (c) OK (d) OK (e) OK
2.3

Well, I got distracted and at the end of the day wrote an overview of Sections 2.1, 2.2 and 2.3. They are so complex that I need these summaries just to remember what was happening.

Tomorrow I will read the Ch 2 overview and then start proofing Section 2.3 and try to keep forward motion going.

June 28 Fri.

I am now starting with 2.3. As part of that, I reviewed Appendix B and made a few edits. I get down to Fact 9 (2.3.13) and I have a **major new problem**: the proof seems completely wrong. You cannot form every code word from a given one by doing rotations of that one code word! You can only form some of the code words this way. I just got done showing this in my little example with n = 5.

I am now repairing this by adding Example B for GF(16). A new question arises: in this case, how do I know that all 15 rotations of a starting code word are DIFFERENT code words?

I think this is true, and it should appear somewhere in my Cyclic Codes chapter of Galois, it seems like an important fact to get stated.

Status: I wrote up a new section Chapter 8 (k) to be installed in Galois doc on my next pass there. This confirms that when h(x) is primitive, you exhaust all code words with rotations. This is critical to one of my main theorems. Thus took a lot of work and I guess I now have to start proofing one more time on good old section 2.3. It is now 6 PM already.

2.3

Fact 1 ok
Fact 2 ok
Fact 3 ok
Fact 4 ok
Fact 5 ok
Fact 6 ok
Example A ok
Example B ok
Fact 7 NOT OK

I think Fact 7 is not true and worse, I use it later in the proof of Fact 8. // I had to redo Fact 7 and Fact 8 completely. This is done and I now continue

Fact 7 ok
Fact 8 ok
Fact 9 ok, did small edits.
Fact 10 ok

Sift List
Fact 11 ok

Finally and once again, I reach the end of Section 2.3. It has certainly been recalcitrant and had various totally incorrect items before I did my rounds of edits. Proof steps were missing, and so on.

Tomorrow I will write an overview of 2.3 and then start once again in to Section 2.4.

June 30 Sun

I think I am ready to do an edit pass on Galois before continuing with Scrambler, there is so much new stuff. So today was entirely spent doing Galois proofs. I did pretty well in several areas.

July 12 Fri

I did a Galois update and it took the full 12 days seen between the two dates above! I did a LOT of new stuff in Galois, and am now ready to resume here with Scrambler.

Let's now reread 2.3 and try to get back into things. I just read Facts 1-6 and seems OK.

I am staring now at (2.3.11) which is a complicated quote from P&W about some min polys of GF(2^4). Here it is:

According to the Peterson and Weldon Appendix C, here are some candidate h(x) polynomials, and α is a primitive element.

1	23_8	$h(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)$			α has order 15 ($\alpha^{15} = 1$)	
		$23_8 = 010,011$	⇒	$h(x) = 1 + x + x^4$ = primitive	h(x) has period 15	
3	37_8	$h(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9)$			α^3 has order 5	
		$37_8 = 011,111$	⇒	$h(x) = 1 + x + x^2 + x^3 + x^4$	h(x) has period 5	
5	07_8	$h(x) = (x - \alpha^5)(x - \alpha^{10})$			α^5 has order 3	
		$07_8 = 000,111$	⇒	$h(x) = 1 + x + x^2$		(2.3.11)

I think it would be lot simpler if I just quote GA 6.21 which is this

GF(2^4)

$p_1(x)$	$= (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)$	$= x^4 + x + 1$	10011	15
$p_7(x)$	$= (x - \alpha^7)(x - \alpha^{14})(x - \alpha^{13})(x - \alpha^{11})$	$= x^4 + x^3 + 1$	11001	5
$m_3(x)$	$= (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9)$	$= x^4 + x^3 + x^2 + x + 1$	11111	
$m_5(x)$	$= (x - \alpha^5)(x - \alpha^{10})$	$= x^2 + x + 1$	111	3 (6.21)

It is cleaner, includes all the min polys. In GA I never said anything about the order of these conjugate sets and thus of the resulting min poly.

Well, the haziness about period and order and where they are coming from led me to make another round of changes in Galois doc, already on day 1! I then did some edits in scrambler and will now try to continue my review!

I start again at (2.3.11) and proceed from there:

- OK through (2.3.12), that took a long time!
- finished 2.3 and had no disasters. Can continue now.

2.4 Characteristic Sequences

- got through proof of (2.4.4).

Bug: The proof of Fact 6 just fell apart, and I wonder now if it is really true? No it is not! Here:

Now we add some new facts which apply only to binary characteristic sequences:

Fact 6: A string of (k-1) 1's appears exactly once in a binary characteristic sequence.

Proof: The state vector 01111..11 must appear somewhere, having (k-1) 1's. If the bit string on the right of it begins with a 0, then we have found our string of (k-1) 1's, and we have also located the state vector 1111..110. If the bit string on the right begins with a 1, then we have found the single allowed occurrence of k 1's (see Fact 3') and we then have 01111..1110... In this case we look for the state vector 11111...110 . Then this must have a 0 on the left to avoid a second occurrence of k 1's. Then this is our occurrence of (k-1) 1's.

The above theorem is not true, and the proof is bad as well. For example consider

c = {1,1,1,1,0,1,0,1,1,0,0,1,0,0,0}{1,1,1,1,0,1,0,1,1,0,0,1,0,0,0}

You see here a string of k = 4 1's and a string of 3 zeros. You do NOT see a string of 3 1's!!!! And in the big k = 9 case, you see a string of 9 1's and you see a string of 8 0's and you see no string of 8 1's! Hopefully I never use this fact.

Example: Consider again GF(512). The characteristic sequence has length 511, as noted above. The number of 1's in this sequence is 256, the number of 0's is 255. The largest string of consecutive 0's is 8. The largest string of consecutive 1's is 9, and there is another string of 8 1's. delete

_____-

I will just delete this Fact from the document!

I am now "OK" to "the product of two shifted....". This is the first time I have gotten this far.
This is a rather tough read but I think I have it right.

```
1   {1,1,1,1,0,1,0,1,1,0,0,1,0,0,0}
2    0,0{1,1,1,1,0,1,0,1,1,0,0,1,0,0,0}
3    1,1,0,0,1,0,0,0,1,1,1,1,0,1,0
4    0,0,0,0,1,0,0,0,0,1,1,0,0,0,0
```

n_1 = number of $\begin{pmatrix} 0 \\ 0 \end{pmatrix} = 3$

n_2 = number of $\begin{pmatrix} 0 \\ 1 \end{pmatrix} = 4$

n_3 = number of $\begin{pmatrix} 1 \\ 0 \end{pmatrix} = 4$

n_4 = number of $\begin{pmatrix} 1 \\ 1 \end{pmatrix} = 4$

Sunday July 14, 2013

OK I have improved the discussion of the fancy chart and am to "Prob of strings of 1's and 0's"

After consulting the web, I changed from "characteristic sequence" to "MLS sequence" globally with a comment on the name where it is first introduced. **DONE**

Have now finished Section 2.4 for the first time! And am on the move quickly, to page 84 after first plot of the famous white autocorrelation function.

Reached the end of Section 2.5 ! I have not carefully checked equations however. I will do another pass on this after I see where the last chapter goes.

Reached end of Chapter 2, but have work still to do, but it all makes complete sense I thnk.
I see what it is doing, getting the MLS spectrum.

3.1 seems OK

Comment: In the GF(p^m) = R/(f(x)) structure, in Galois we said that the only requirement was that f(x) be monic and irreducible in GF(p). However, once we say it is of degree m, then it must be a minimum polynomial according to Fig 5.5.

3.1 Review of earlier Chapters OK
3.2 Matrix Solution of the Type B Divider OK
3.3 Matrix Solution of the Type A Divider OK
3.4 Shift Register Generators Revisited OK
I swapped matrices A and B so they match the Type of the divider they go with !!!!
3.5 added a definition of a scrambler with some fancy extra comments

Holding now for a break on page 97 of 137. Got into Cod airfare stuff, nw 8:30 PM, done for today.

****** work in comment about meaning of α and β *****

Monday July 15, 2013

I have moved ahead, at 10:30 AM an up to the Leeper review section. There are some small unresolved things however that I will go back and address when I get through the paper.

• I just finished revamping the start of section 2.5. It used to be restricted to GF(2) symbols which was an unnecessary restriction and prevented me from using the equations in my later (-1,1) situation. Also, I managed to "work in" the four symbols α,β,μ and σ and the term "correlated". I then wrote down the autocorrelation drawing AND the spectrum for the uncorrelated case, quoting from FT.

Tues July 16, 2013

I reread from the start of Sec 2.5 where I do α and β and quote the power density for an uncorrelated pulse train from FT. I think I want to say that MLS is not quite uncorrelated. Reading now thru temp333 where i tried to update the following stuff. Bug: (2.5.13) is wrong for N = 2 ! Fixed it up.

I replaced the auto corr picture for white signal. This section is a little out of place, it does relate only to GF(2) however and it does use exactly the formulas above

I finished Case 1, and now start Case 2.

I will now insert this temp33 stuff into scrambler doc, I think it is a great improvement.

Chapter 2.6. I now return to the subject of MLS sequences, so let's just read on here. // OK, I have improved the structure of things pretty much.

Question: I am about to roll out the PSD formulas based on α and β.
(1) Is that even valid for MLS since it is correlated? NO it is not! so my quotes are all wrong!

(2) I should be using Khitchinte whatever since I know the autocorrelation and that should give PSD as I dimly recall.

Let's first look into the latter thing.

$$R_x(\omega) = |X(\omega)|^2 \, . \tag{32.8}$$

$$\mathcal{P}(\omega) \equiv \frac{\mathcal{E}(\omega)}{T} = \frac{|X(\omega)|^2}{2\pi T}$$

Where is my ensemble here? I am confused. This does show getting $\mathcal{P}(\omega)$ from $R_x(\omega)$ which is the FT of the autocorrelation *function*. I have to re-derive this I guess for an auto corr sequence.

My infinite pulse train formula direct is this:

$$\mathcal{P}(\omega) = T_1 \, \mathcal{P}_{pulse}(\omega) \, (1/T) \sum_{n=-\infty}^{\infty} \sum_{m=-\infty}^{\infty} a_m^* \, a_n \, e^{i\omega(m-n)T_1} \tag{34.14}$$

I do have a general formula for a "repeating sequence" that I have never confirmed anywhere:

$$\mathcal{P}(\omega) = \mathcal{P}_{pulse}(\omega) \frac{1}{M^2} \left| \sum_{k=0}^{M-1} A_k e^{-ik\omega T_1} \right|^2 \omega_1 \sum_{m=-\infty}^{\infty} \delta(\omega - m\omega_1/M) \, . \tag{34.30}$$

where I would have to take the A_k = MLS so I guess then M = P if numbered 1,2....P.

OK, I have unearthed some very major problems in Chapter 2 of Scrambler. I claim in 2.6 to have MLS spectra, but I don't!

My problems start in Chapter 2.6, think I am OK before that.

Question: In (2.6.1) I find by direct calculation that $\langle a_m a_n \rangle = (1/4)(1+1/P)$ and this does not depend on the m,n indices, so perhaps OK to call it α. On the other hand, I know I am uncorrelated, so $\langle a_m a_n \rangle \neq \langle a_n \rangle^2$, and I have shown how that inequality is really true. Similary $\langle a_n^2 \rangle$ is independent of n so OK to call it β. Is it possible that my PSD formula applies in this case, even though uncorrelated?

That last question is a good one, and I have an idea for an answer. I have been off working in temp44 on this and related issues. Will resume tomorrow, now 8:30 PM.

Weds July 17, 2013

In temp 44 I made my "idea" work and I now know the spectrum of MLS. I now need to reorganize the end of Chapter 2 somehow, it is just a mess right now.

I think my first mods will be in Section 2.4. I need more reference labels on things!

Bug: there are two equations (2.3.12). So starting at Fact 8, I have to shift numbers down one in the rest of section 2.3. Now numbers go to (2.3.18). So I will first renumber, then update all references. So did this renumbering and added more items, but I see a new problem. I need overviews because even I am lost in this thing!

I just wrote my detailed overview for Section 1. This is fairly stand-alone stuff. The only links are:

- GF(p) symbols GA
- Z transform FT
- convolution theorem FT

Since the cross links are so few and minor, I don't think changes I made to GA have any effect on Chapter 1, so I won't reread that now.

Replaced all Figure 1.1 stuff with Fig 1.1, whole doc. **DONE**

Chapter 1 equation number check: **DONE**
(1.1.1) to (1.1.4)
(1.2.1) to (1.2.9)
(1.3.1) to (1.3.22)
(1.4.1) to (1.4.4)
(1,5,1) to (1.5.9)
(1.6.1) to (1.6.9)
(1.7.1) to (1.7.5)
(1.8.1) to (1.8.3)
(1.9.1) to (1.9.8)

Paginate Chapter 1: **DONE**. This took a lot of work since huge divide things need to be on a single page and so on.

How should Figure labeling be done? I have so many done, I will just keep it that way. For example

Fig 1.2: Type A divider with k = 2

This is different from my other docs I know. I leave some white space above the Figure label, do this uniformly please even though wastes space.

I am now happy with Chapter 1's formatting. It has
Fig 1.1 to Fig 1.13

Review of Section 2.1. I added reference numbers to definitions and facts. All OK.

Applied std format to all equation numbers in Chapter 1 **DONE**

Section 2.2. This is a much larger section.
Equation number format : **DONE**
Figures: Tried to label them, one number was missing.

Section 2.2

(a) OK

(b) OK

(c) OK

(d) stop just before An Example GF(2^9). Did major repair here regarding φ(q-1). this section (d) is a little rough. It has several facts, and then a long Example which is now in the TOC.

(e) is OK, but reader is confused about what he knows at this point.

Ouch (2.2.27) is missing. Starting with 2.2.28 I will back up the equations by 1 and then do a global check. **DONE**.

Section 2.3. I think I will *not* review this now since I spent so much time on it recently. Broke out the three examples as headings. I am done with this section, it is OK.
But let's do equation numbers. DONE and OK, all tabbed right now.

Section 2.4. Equation numbers were a mess. I need to go through this entire section and clean it up before even starting to rewrite Section 2.5. I am OK thru (2.4.11). // OK, I finished 2.4.

It makes the first mention of a "white sequence" in a sort of passing fashion.

Go look up "white sequence" and make sure I am using the term right. I added a bit on this, no precision, no formal definition. Related to white noise and a flat spectrum. Of course a white NRZ has a flat spectrum times the box spectrum, so I don't want to digress on all of that.

As I approach Section 2.5, I am not sure the autocorrelation is really necessary for me to get the MLS spectrum, but I do like seeing the plots of the AF. I will continue with Section 2.5 tomorrow, but look at the Overview of Sections 2.1 through 2.4 first!

Thurs July 18, 2013

I updated the Overview through Section 2.4 as noted above. Now suppose I try to do things with no mention of autocorrelation. How would that go?

First problem: what does the word "uncorrelated" mean? I have not mentioned the correlation object. Maybe I should.

I have rewritten my little probability section to incorporate ALL the basic stuff and how it applies to a sequence. We are on much more solid ground now. I have added a lot, and now I am going to take out a lot. Those moments are irrelevant. What I really want to get to is the spectrum.

Big news: I created Appendix F for FT which has a proof of something I earlier just conjectured. This will play a major role in scrambler very soon.

Friday July 19, 2013

In temp55 I am doing the statistics, spectrum, and autocorrelation stuff, a full rewrite of 2.5.

Sat July 20, 2013

Resuming on temp55, ready to install autocorrelation plots. DONE.

Question: Why does every doc I write have a separate section on statistics? I have just added such a section to scrambler doc. Appendix D of FT has some stuff, but it seems less complete than what I am now putting in scrambler. But it has the same topics. Galois has no statistics section.

Added equation numbers to section (a) on Probability Theory. I think it is good. Got rid of the word statistics.

Section (b) proofed, and also good. Only 3 equation numbers here.

Section (c) lays out the steps of the plan to compute $\mathcal{P}(\omega)$. Two equation numbers.

OK, I have spent all day on this stuff, and I started making plots. But after doing all that, I found a simpler way to view the spectrum and I made new plots. The problem now is that these two plot methods don't give the same line amplitudes, so I now have some deeply buried bug I have to hunt for, locate, and then fix. That will probably take 4 hours, so breaking at 4:30 PM for a while. // Full Buff run, now 6 PM resume. // Found the bug. I omitted a multiply * symbol in Maple.

At 9 PM I have done this: (1) rewrote ending of FT Appendix F (in sep doc) to show lots of alternate forms for the repeated P spectrum. Then I can pick out the ones I want in Scrambler. (2) I then once again reorganized Scrambler Section 2.5, with new linkages into Appendix F. I did a lot of Maple work today but never got what I really wanted to see. Will do that manana.

Sun July 21, 2013

After a morning of fiddling, I think I finally have Section 2.5 finished. I guess I will proof the whole thing now including equation numbers.

equations number sequence OK
equation number positions: OK, done
figure numbers: The last Figure in Section 2.3 is Fig 2.7 so I continue from there: DONE.
(a) done.
(b) done
(c) done
(d) done
(e) done
(f) done
(g) done
(h) done
visual spelling check: done

As of 2 PM, this monster 2.5 is finally ready to install.

STOP! HOLD THE PRESSES!

I was trying to do a little W-K theorem adder for section 2.5 when I realized a goof. I have been writing things like this

$r_0 = \langle a_n^2 \rangle$
$r_s = \langle a_n a_{n+s} \rangle \qquad s \neq 0$

But for repeating subsequence situations this really is

$r_0 = \langle a_n^2 \rangle$
$r_s = \langle a_n a_{n+s} \rangle \qquad s \neq NP$

That means the autocorrelation function peaks up again periodically. None of my plots shows this and I should at least comment on that fact. But I fear there are worse problems that this mistake is doing to create. Maybe Appendix F is wrong again. I have to review many things in light of this error!

Doing a rewrite now of App F.
Section (a) needs no changes.
Nothing else needs any changes
I was lucky because I get down to the "reduced set" before talking about α and β. But added a few comments on this fact.

Now look at earlier in Scrambler doc before section 2.5. Done, nothing up to 2.5

Now look at temp55 which holds Section 2.5. Surely there will be issues here.
(a) OK
(b) the <..> notation is here, but no α and β yet. I mention $\langle a_n a_m \rangle$.

Change: I am removing m≠n from (2.5.19) bottom two lines? No, it is correct. A sequence with repeats is NOT uncorrelated!!!!! So I think when I write uncorrelated in that table, I rule out repeaters.
So (b) is OK.

(c) Here I quote (F.12) which already has the limited range! Then α and β in (2.5.21) are OK! Once we are in the smaller world, all is OK. Then (2.5.24) is also OK within Small World.
(d) is OK too.

Question: Is there any confusion about MLS sequence in (d) ? In the abutting stuff, I am only thinking in terms of one subsequence of length P. Yes, we assume wrap around when abutting things. But in the comparison, both compared sequences are just of length P.

(e) is OK too, just different values for α and β
(f) it is OK, need to assume m-n < s in the tables, after commenting earlier reader will know that.

(g) on autocorrelation. Here I have to pay full attention, I suspect trouble.

(2.5.33) suggests we are using the finite sequence, here numbered 1 to P (differs from App F). But the infinite thing is lurking right there. And here is my ambiguity note.

Now, stare at r_s as defined in (2.5.34): $r_s = \langle a_n a_{n+s} \rangle$. What I say is true if I limit to s < P. I have added notations that s < P just to state it clearly.

But does this really fly? I am defining r_s only for s < P ?? I think I should instead define it for any integer s I want. Then I make my first change just below (2.5.34). OK, I have made the required changes,, but (2.5.36) stays as is with a little qualifier comment above it. Fine.

Comment #1 issue. It is not true that $\langle a_m a_n \rangle$ for MLS is independent of m and n! That is only true when they differ < P. This comment now bailed out.

Comment #2 is OK as is. I added a comment about the plots peaking off the screen.

(h) Now I am using the Appendix F stuff which is restricted to the small MLS subsequence, so no problems with α and β. Added a comment at the end of (d)

(i) also OK.

OK, put down the fire extinguishers, I have remedied this problem with discreet comments in the right places. Now back to my W-K idea.

Hurray! I was able to make W-K work. It started as just a dim idea a few days ago, and now there it is in full detail and it really does give the MLS spectrum!

So how run a few checks on these last two (j) and (k) sections

(j) only 3 numbered equations, spell OK

(k) done

OK, NOW I am ready to install temp55 into scrambler doc. But I guess first I want to continue to peruse my various docs just to make sure some other problem is not spotted, or something else needs to be added. Manana!

What about a Z transform W-K that is more general and makes no use of "P" ? This would be something maybe to add to FT, and maybe it should all go there?

Mon July 22, 2013

About a general Z transform WK? It is done!! Now I have a big problem of deciding where to put what in Spectral! Right now I have that Appendix F idea, but maybe that whole thing is not needed!

My first idea is to add the "Z Transform WK theorem" as a little add-on at the very end of Section 32. That theorem I would state as $R''(z) = \frac{T_1}{T} | Y''(z) |^2$ and just let it lie for a while. At that time, I have not even talked about things like $\mathcal{P}(\omega)$. So that would be my first quiet addition.

Now lets have a little review of what happens next in FT:

33. Spectral power density of a Simple Pulse Train

(a) Infinite Simple Pulse Train

I brute force my way here to get this result for the infinitesimple pulse train

$$\frac{|X(\omega)|^2}{[2\pi\delta(0)]} = |X_{\mathbf{pulse}}(\omega)|^2 \sum_{m=-\infty}^{\infty} 2\pi\delta(\omega T_1 - 2\pi m)$$

(b) Finite Simple Pulse Train

Here I repeat the above to get

$$\frac{|X(\omega)|^2}{(2N+1)} = |X_{\mathbf{pulse}}(\omega)|^2 \; 2\pi\,\delta_6(\omega T_1, N) \qquad \text{finite} \qquad \textit{(33.18)}$$

So I have just done it "both ways"

(c) Spectral Power Density of a Simple Pulse Train

Here I combine the two ways and I then write these as

$$\mathcal{P}(\omega) \equiv \mathcal{P}_{\mathbf{pulse}}(\omega) \sum_{m=-\infty}^{\infty} 2\pi\delta(\omega T_1 - 2\pi m) \qquad \text{joules} \qquad \text{infinite}$$

$$\mathcal{P}(\omega) \equiv \mathcal{P}_{\mathbf{pulse}}(\omega)\; 2\pi\,\delta_6(\omega T_1, N) \qquad \text{joules} \qquad \text{finite} \qquad (33.25)$$

I then rewrite this as

$$\mathcal{P}(\omega) = \sum_{m=-\infty}^{\infty} |c_m|^2 \; \delta(\omega - m\omega_1). \qquad (33.27)$$

$$\mathcal{P}(\omega) = a_0^2\,\delta(\omega) + (1/2) \sum_{m=1}^{\infty} (a_m^2 + b_m^2)\; \delta(\omega - m\omega_1) \quad . \qquad (33.30)$$

All interesting facts to get down in writing.

(d) Average Power P of a Simple Pulse Train

Very short, conclusion is

$$P = \sum_{m=-\infty}^{\infty} |c_m|^2 = a_0^2 + (1/2) \sum_{m=1}^{\infty} (a_m^2 + b_m^2)\,. \qquad (33.32)$$

Now we start the more serious stuff here

34. Spectral power density of a General Pulse Train

(a) General Pulse Train results and connection with the Autocorrelation Function

This is where I have my boxed results that are completely general. Should I add something to this box? Perhaps a single line which says

$$R''(z) = \frac{T_1}{T} |\, Y''(z) \,|^2 \qquad (32.18)$$

$$\mathcal{P}(\omega) = \mathcal{P}_{pulse}(\omega)\, R''(z) \qquad (32.20)$$

But I don't have this last result anywhere! It needs to be derived in some logical location. How about a quiet addition in Section 34 (b). I can shuffle equations around a bit.

STOP. I really have to go get FT updated, it has too many moving parts right now. So right now I am starting a new Spectral folder to deal with this update. This will take a long time, and only then can I resume on scrambler. I see now way to avoid this big delay.

Weds July 24, 2013. OK, I have finished the above task (I think) and can resume on scrambler. I put all the spectral derivation details into FT App F, so I will now be removing lots of details from scrambler on that subject. Of course right now it is all in temp55. I think this needs major work, it is Section 2.5 yet again. Right off the bat at the start of (b) I quietly write $\langle a_n \rangle \equiv E(A_n) = \Sigma_n a_n\, p(a_n)$ but I don't mention ensemble. What is this average anyway? It could be either horizontal or vertical! But a specific sequence has specific a_n, there is no $p(a_n)$ through you could compute it as

$$\langle a_n \rangle_1 = (1/N) \sum_{n=1}^{N} a_n$$

I am not sure how to start (b). I am interested in the specific MLS sequence, not an ensemble. In a single MLS sequence, there is indeed some $p(a_n)$ that a bit is 1. We just do our sum of 1's/total bits ratio.

STOP. I am led back to Appendix D of FT which does probability. What exactly is meant by the term "random variable" ? My Proakis source start a little too late for this definition I think. I downloaded a Chap 2 of his book, and later I found the whole book ($220 amazon, yikes).

I spent this entire day looking at many sources on random variables. Tomorrow I think I can integrate this into a good presentation and put that right into Scrambler. There was a lot that I did not know, that I never knew. I don't think at L3 I did anything beyond Proakis.

Weds July 31, 2013.

I spent the last entire week updating FT. I added the random variable stuff there as Appendix G. It seemed that FT is the right place since it discusses pulse trains and that is what Y_n Y_m and $\langle y_m y_n \rangle$ are all about. So now I have much more support stuff in FT.

Right now I am confused about Section 2.5. I guess it is parked right now in temp55a.doc.

Now noon, it has been a battle, I need a new formula regarding r_s that should go into FT, I need it in order to make the connection between FT App G result and the MLS situation. I will work this in next thing.

Switched over to the FT Update log on Aug 1. This resulted in a solid week of FT updating.

Thu Aug 8, 2013.

Returning now to the Scrambler log to see if things have improved!!! We shall soon know.

I need now to look at temp55b.doc which is my pending rewrite of Section 2.5 on the MLS power spectrum.

(a) OK, readjusted a Sec 35 eq ref to the summary box
(b) repairs have been done, it is now OK, and all FT references are good.
(c) verified good
(d) very similar to (c)
(e) made changes, computed MLS correlation, much better, all done

So, temp55b.doc for Section 2.5 is stable and is ready to install in Scrambler!! The connections to FT are all clean, no further FT work is required. So I now return to the FT world to try and put out an Update!

I have just released an updated FT and am ready to resume now with scrambler. I will install temp55b.doc right now after a few checks.

equations numbers: done, aligned, all OK
figure numbers: adjustment made, 2.8 through 2.10.
spell check OK

There is text in red in scrambler doc, it is not finished. I can at least resume now with a full document to look at! The FT digression was very major.

Fri Aug 9, 2013.

It is 7:30 AM, will open by reading my Overview through section 2.4.

I read and slightly edited the Chapter 1 overview. It is just fine, quite detailed, and I think I can stay out of this Chapter 1, it is "done".

I read the Chap 2 reviews which exist through Section 2.4, and that also seems OK. So lets right now read Section 2.5 and then add an overview for it.

(a) OK, made small edits, it is about a white pulse train spectrum.

(b) basically quotes the repeated-P theorem and states its spectrum, but MLS is not there yet/
(c) very good, this is the major payoff for 2 months work (more or less). We have the MLS spectrum and we see how it goes to white for large P.
(d) repeats previous section for {1,-1}. These two symbols sets were in the original scrambler doc.
(e) OK, I changed the title.

I will now produce an overview of 2.5. Done. My formatting in the overview is inconsistent but I think OK for now.

Conclusion: I am done with Chapter 1 and Chapter 2.

Chapter 3 has been idle for 2 months or so and I expect will take some effort to beat into shape. Maybe get Scrambler into the Chapter 3 title.

Sat Aug 10, 2013.

Starting 7 PM. Looked for red text items and dealt with them prior to Chapter 3, there were 2 items.

I will just start reading Chapter 3.

Section 3.1 OK I claim things will be remedied
Section 3.2 OK, I produce a matrix version of the Galois iterator equation for Type B only
Section 3.3 OK, A equation is parallel to the B equation of the previous chapter

Break. The above sections are totally clean and require not work, assuming cross references are OK/

Section 3.4 OK, very clean, lots of cross references though. We learn that each register does MLS.

Section 3.5 long comment needed repair, it is very interesting I think.

Stop. I posed the question: is it possible for $[C^j]_{ab} = 0$ for some particular ab for all powers j? That does not conflict with h(C) = 0. Look at (3.3.5). If off diagonal, the bracket $[..]_{ab} = 0$. But q_n won't have some always vanishing element, so I see no problem there either.

What happens as you take powers of the matrix in 3.3.2 (which is a companion matrix) ? Does it "fill in" so you cannot have an element remain 0 for all powers of the matrix?

In a generator can some register just always remain 0 ? Not in Type B certainly since then the output would be 0.

Same question; In a GF matrix representation, can some element in every matrix be 0 ? I think it cannot, but after pondering for a while, I see now way to prove that fact. It is true in the representation examples I show.

This 3.5 is a MUCH harder section for me to get through. I will not check this off, but will continue
Leeper: this makes a lot of sense, but needs some rewriting.

Section 3.6. Needs repair. I suddenly jump from the MLS spectrum with finite P to the white noise spectrum. That jump is OK, but I have to state it somewhere. In my original paper, I claimed that the MLS spectrum WAS white noise! See (2.6.2) of the original paper. Again, this can be justified for large P, but I need to say that somewhere.

I do like the conclusions I am getting here, however. The scrambler converts a potential line spectrum input signal into the continuum.

3.7 the Mini scrambler. did a fast read through. I like the list of facts.
3.8 fast read
3.9 fast read
3.10 fast read

Stopping at 8:45. I have probably a solid week of work (or more) to get Section 3 in good shape, so forget about any pre-Cod release of this paper! I was not sure of that fact until this evening as I go through all this stuff quickly.

What about re-issuing tensor analysis as a single document? **********

Sun Aug 11, 2013.

I messaged Section 2.5 a bit to work in the phrase "effective continuum" for large P. I added the general dense arrows plot from FT and put in the general repeated-P section and made the point there about the effective continuum. I think the tie-in to FT is quite clean now, it used to be a complete mess in older times (a month ago).

Now back to Chapter 3 and it is 8:30AM Sunday, day before Cod flight. Once again I am completely happy with everything up to the start of Section 3.5.

Section 3.5. Once again, happy through "Exercise for the Reader". Eventually I will probably solve that little mystery, but don't want to do that right now.

I am now marching down chunk at a time with my ok to here marking, I had to renumber all equations and facts in this section 3.5.

I am now down to the Leeper section.

I have now finished Section 3.5 and I think my Leeper review is good, and I added its reference and found that BSTJ is all online!

Section 3.6. Did major edits here, made it much better, done at 5 PM. All done!

Section 3.7 on Mine-Scrambler. All done, did a few passes here, only 3 eq numbers.

Starting now into Section 3.8. Got one paragraph in only! It is time to shut down for Cape Cod trip, it is 8 PM Sun Aug 11. I will resume when I get back with Section 3.8 and try to see what I am doing here! Why

do we need a matrix analysis, I already have time domain stuff and I think it would be easy to prove that things work right without matrices! Maybe I didn't have time domain in the original paper?

Mon Aug 26, 2013.

15 days have elapsed and I am now getting back here. I better back up and start at the start of Chapter 3, but first I will read the Chapter 1 and 2 summaries.

Perhaps rename things so they are not all Fact 1 **********

Chapter 1 overview: done and fine.
Chapter 2 overview: done and fine, did tiny edits in the overview.
Chapter 3.1 -- the review of all that went before, it is OK
Chapter 3.2 -- Galois iterator for Type B divider in matrix form, companion matrix B.
Chapter 3.3 -- Galois iterator for Type A divider in matrix form, companion matrix A.
Chapter 3.4 -- shows that each register in Type A or Type B does the MLS sequence.
Chapter 3.5 -- I start talking about scrambler spectrum and the Leeper paper, it is all OK/
Chapter 3.6 -- this is pretty good I think, comparing square wave and scrambler spectra
Chapter 3.7 -- I am happy with this scrambler summary

I feel I am caught up pretty much and tomorrow AM will dig into Section 3.8 which I know is tricky.

Tues Aug 27, 2013.

Chapter 3.8 -- Did various edits here, it was too dense to follow, added more math lines.
Chapter 3.9 -- I am NOT happy with this section. But let's go on.

I do all this matrix work and I just don't see the payoff. The transient stuff never matters.

Comment: the time domain equation for the divider does not give a "solution", it is instead a difference equation you have to solve. But the matrix approach gives an actual solution, that is the payoff.

Well, I have read 3.8 several times and it is still OK. But the multiplier was not the difference equation issue, so we have now both a time domain solution and a matrix solution.

I have edited 3.9 to more clearly show which terms are active as a function of time n.

4:15PM. I have further edited Sections 3.8 and 3.9, making them more parallel all the time. Fixed some significant errors.

Now I come to Section 3.10.

As of 7:30 PM I have battled my way through Section 3.10. It uses the Type A divider as a scrambler, and this is the usual thing people use. I made no attempt to do a time domain analysis for the Type B scrambler.

Section 3.11 initial look. Made it through, but lots of cleanup needed. Then we are done, have only the appendix to deal with.

Weds Aug 28, 2013.

Will start with another pass through Section 11 on kill vectors. It was a little hazy the first time, and it seems disconnected from previous sections. // I know understand the N+k argument and agree with it.

I have now redone the video examples, my old stuff no longer even applies. And I added a book reference by Fisher where reader could go learn more.

10:30 AM. I am now happy with Section 11 and am done with it. It makes no use of anything that came before really. There is no reference to the A or B matrix stuff, for example. It is a stand-alone section.

I think I should now look at Appendix 3.1. but I will call it Appendix D and put it at the end.

I am how happy with Appendix D, I improved a few details such as the minus sign.

2:40 starting now on section 3.10. I revamped things a bit, and am now OK through the Z domain proof. Now at 4:30 I have made a full pass through Section 3.10, updated the pictures and equation formats. It is getting better.

New reading of Section 3.10. // Formatted equation numbers in Section 3 and part of Section 2 and in appendix B and D. //

I think I am finally done with Chapter 3 and its associated Appendix D. Let's try for a Chapter 3 overview. But first:

Question: What role has Galois Theory played in this scrambler doc. I say big things, but what are they?

Nothing before Chapter 2 certainly, Galois is not even mentioned. In Chapter 2, I first ge my little iterator equation, I go off and review Galois Theory, then I come back to that iterator equation above (2.2.13). I am able then to interpret that iterator equation in terms of GF elements

$$q'(x) = x\, q(x) - o\, h(x) + i \quad . \qquad (2.2.4)$$

$$\{q'(x)\} = \{x\} \bullet \{q(x)\} + \{i\} \quad . \qquad (2.2.13)$$

$$\beta' = \alpha \bullet \beta + i1 = \alpha\, \beta + i\, 1 \quad .$$

I associate polynomials with GF elements. I think I am able to show thaqt if h(x) is prim, then p^k-1 is the period, THAT is where we need Galois! We exhaust all the non-zero field elements! So that is at least something. How else would you show this? I am studying the period of the state vector and of the output at this point. You want a long period and Galois tells you how to do that!

I then don't really mention Galois until we get to Chapter 3 where I think it plays a different role. I start off with my little abstract iterator thing 2.2.16 quoted. But then in Section 3.2 I so my matrix thing for the Type B divider. I get a vector/matrix recursion relation $\mathbf{q'} = B\,\mathbf{q} + i\,\mathbf{1}$ and I solve it to get

$$\mathbf{q_n} = B^n\, \mathbf{q_0} + [\; i_0\, B^{n-1} + i_1\, B^{n-2} + ... + i_{n-2}\, B + i_{n-1}\, I \;]\, \mathbf{1} \qquad (3.2.5)$$

I could have gotten this result never mentioning Galois. But I then claim that matrix B is a field element in some matrix representation of GF(p^k). But what good does that do? Well, if h is a prim poly, then B is a prim element. So far I just make a comparison between my abstract Galois iterator. But I just don't say much, there is a similarity:

$$\beta_n = \alpha^n \beta_0 + [i_0 \alpha^{n-1} + i_1 \alpha^{n-2} + ... + i_{n-2} \alpha + i_{n-1} 1] 1 \qquad (2.2.16)$$

$$\mathbf{q}_n = B^n \mathbf{q}_0 + [i_0 B^{n-1} + i_1 B^{n-2} + ... + i_{n-2} B + i_{n-1} I] \mathbf{1} \qquad (3.2.5)$$

So don't I want to somehow associate $\mathbf{q}_n$ with a matrix? Something seems to be missing here!

In Sec 3.3 I digress to do the Type A Divider with its matrix A.
In Sec 3.4 I call upon the h(C) = 0 equation in 3.4.3.
In Sec 3.5 I show that each element of a matrix representation cycles through MLS, which is a new concept, and I show this in an example. I have my unanswered question there. I am then off to doing the spectrum stuff.
In Sec 3.8 I matricise the multipliers, still no Galois used
My proof doesn't use Galois either that descrambler undoes scrambler except I do use that 3.5.2 thing and it comes from 3.4.3 and it comes from h(C) = 0 and that comes from the little companion theory. I am more just making a linkage to Galois rather than using any Galois results.

I really should understand how 3.2.5 is part of a matrix equation to make the parallel closer. Is 3.2.5 the first column of a larger matrix equality?

But: $\mathbf{q}_0$ is a vector of values the register can hold, so it is an m-tuple element of GF(p^k)! So in that sense, $\mathbf{q}_0$ is a field element. But B is a field element that is a *matrix*. So how can a field element be both a vector and a matrix?? My equation (3.2.5) seems to be mixing together these two different kinds of elements.

Thurs Aug 29, 2013.

I pondered the above issue for a while and finally came up with some words to add in Section 3.2 about this being a mixed representation of the abstract equation. I am happy with this issue now and can move on. It is now time for a Chapter 3 overview.

Fri Aug 30, 2013.

Got a **Chapter 3 overview** written! I then decided to write a separate Overview from the Summary, and my cowgirl on here two horses gets mentioned. I emphasize GA and FT as planned.

Let's clean up the **References** now. This reference was not used, I just store it here

[TA] P. Lucht, *Tensor Analysis and Curvilinear Coordinates* (2012), http://user.xmission.com/~rimrock/. This document is segmented into two PDF files, the second containing a set of Appendices. If not there, search on "Phil Lucht Documents".

OK, references now generally have first two letters of author's last name.

Overview **spelling check**: done.

Install **overview stuff**: done. Oops, I need to add summary of the four appendices. **DONE**.

Page headings: How should I do this? Just by Chapter. **DONE**

Ready for pagination.

But first, can I now **answer the question** posed below (3.5.4)? The long discussion regarding 2.3.2 always allows for the trivial solution, and we never eliminate this solution as a legal one of the p^k solutions.

OK, I did a half-baked argument and left it as a reader exercise, but I claim that the all zero's matrix element is not possible. Earlier I claimed no answer, now I do. I also did a few more Maple examples and found this to always be the case.

Next task: Once again, I want to look at all my **OTHER scrambler materials** and see if I have an error or left something out. I never mention pathological sequences for example.

Well, I did manage to add a small item at the very end on our **video tilt** problem. I now declare the subject matter closed! We can then start pagination any time now.

Sat Aug 31, 2013.

Starting pagination. TOC OK.

Overview and Summary. I will now start Summary on a separate page because that pushes the end onto a new page.

Chapter 1: First page is just the four drawings, OK.
OK through start of (c)
OK through start of 1.5
Ok through start of 1.6
Ok through start of 1.8
Ok through start of 1.10
done

I think I paginated Chapter 1 earlier, all those big division things are just fine.

Chapter 2: OK to page 61 where my chart of prim polys does not fit well, leaving me with a 40% blank page. Then repair on [p 63 bottom. Adjustment on p 65 to get last =0 on board. OK thru p 70. OK thru p 75. OK thru 78.

I start 2.5 on a new page, why is that? A totally new subject.

I made a lot of pagination changes in Section 2.4, including starting IT on a new page. Recall that this allows future changes to be more easily made.

Section 2.5: done, lots of changes made.

Pause: let's replace **Proof** by Proof everywhere. That took quite a while, all done.

Chapter 3 Pagination. OK through start of 3.7. OK through start of 3.9/ OK thru start of 3.11 on kill sequence.

App A: a long appendix, pagination now OK.
App B: made a change now OK
App C: OK a little ugly
App D: done
Refs: Done

Pagination is done! Updated TOC and saved.

Read through TOC. Done, seems all OK, did one lettering fix.

Let's now do a preliminary PDF shot to see if problems exist. Done, first time crapped out, then worked. Bookmarks all check OK. Blank pages search: OK, no blank pages.

Proofing: Will now proof the entire Overview and Summary section non-stop, using the doc directly. I rewrote the Overview to get the horses right at the start, it is better. Have now reviewed Chapter 1 summaries, various edits, done. Chapter 2 summaries now completed. It takes a long time, reading out loud. Chapter 3 done. Appendices done.

Do any equations look messed up in the PDF? (1.5.7) has arrow alignment problems.

Centering of pictures: done

I just cannot possibly proof the whole thing. Read the little CRC piece.

OK, it is time to push this baby out. But I suppose first I should clean up all my accumulated docs.

I just went through all the scrambler **doc files** and commented them at the start and filed into a few subfolders. Really there are just temp docs I used along the way. their results are all now contained either in FT, GA or Scrambler.

Created a Maple index as usual.

I just did the first ever web **release** of scrambler under its long name, and at the same time updated Galois to fix a few problems in it. The deed is done! Today is Aug 31, 2013.

Review of Scrambler Preparation

It is all above. I started on this May 23, just before the Torrey Mem Day trip. Then did the sink and the Samsung and resumed scrambler on June 12. So really June 11 was the effective start date. Did a full read through, then back to Chap 1. Redrew the pix. Another whole pass thru Chap 1on June 17. Did battle with my weird App A. How to name the figures: Start Chap 2 on Jun 21 or so. Rewrite 1.3. On June 25 am thru 2.3. June 27 another pass thru Ch 2. June 28 hit the code word rotation problem!

First debreak into Galois to handle this rotation of code words business, Sec 8k. This led to a full 12-day edit pass on Galois!! Added lots of new stuff, I claim.

July 12 and I resume scrambler. July 14 start using MLS buzzword. First time through 2.5. Revamp 2.5. July 16, realize I need a PSD for P-repeat sequence. Wrote Sec 1 overview on July 17. Another whole pass through Chap 1 and paginate it. July 18 overview thru 2.4. Added App F to FT for the P repeat thing. This used to be a reader exercise in Scrambler, rewrite App F on July 20. Think 2.5 but says hold the presses. Have to rewrite FT App F again. Realized there is a Z transform W-K on July 22. I then stop to update FT with all my new stuff. July 24 am back. Next, confused by "random variable" and Proakis. Whole question of what is a stat pulse train. Did July 31-Aug 8 entirely inside FT, release new FT. Did overview for 2.5. Aug 10 start into Chap 3. Aug 11 repair 2.5 and then Cod trip, back working on Aug 26, a huge gap of 15 days. Aug 27 working 3.8 and 3.9. Did App D for first time. Doing kill vectors. Review role of Galois theory. This leads to strange interpretation of the iterator, best I can do. Aug 30 I get Chap3 overview done, clean up Refs. Then section headings. Review other scrambler materials. Check TOC. Aug 31 various cosmetic edits, install summaries, release! Review doc and Maple files.

So here is a little time summary of this effort:

	S	GA	FT
June 11 start, go thru June 28.	17		
June 29-July 11 = 12 day edit pass on Galois, new GA released		12	
July 12 - July 20 scrambler	9		
July 21-23 update FT.			3
July 24-July 30 scrambler	7		
July 31 - Aug 8 edit pass on FT, new FT released.			9
Aug 12-Aug 25 Cod trip	nada		
Aug 26 - 31 finish scrambler	6		

So here is the cost:

update Galois	12 days	1/2- month
update Fourier	12 days	1/2- month
do scrambler	17+9+7+6 = 26+13 = 39 days	1 1/3 months
total	63 days, 2 months	

The calendar however ran from May 23 to Aug 31 which is 3 1/4 months. So I was only able to work about 70% of the time. So think of this as a 63 day effort. I never dreamed it would take anywhere near that long. I was planning a quick cleanup, thinking the GA and FT hard stuff was already done!