Bobrow and Arbib Scan on Galois 7.12.91

Note: This is a book I found in Marriott. I copied one section, it follows. Title page is included, along with the call number. It is a pretty good book and helped me a lot.

My Xerox notes start at section 8-3.

It is noted that Z_p = GF(p) for p prime. Ring of integers modulo p.

Evariste Galois 1811-1832, lived 21 years.

Example 1: The • and + tables for GF(4), with $1 + x + x^2$ as f(x).

Definition 1: *irreducible* over a field K.

Theorem 1: The Ring K[x]/<p(x)> is a field iff p(x) is irreducible over K.

ground field, extension field.

Theorem 2: If K is a finite field, then order of K is p^m . Order is |K| .

This has a very long proof, I did not feel the need to include this theorem in my notes. I do quote it on the first page of my Chapter 1. After the proof, they note: we know that f(x) exists, so we know how to constuct R/I type fields of order p^m. So these must be all of them.

Definition 2: *root* of a polynomial. Relation to factor (x-a). Poly has at most n roots.

Example 3: For GF(2), they consider various polys and get 0, 1 or more roots in GF(2).

Notion of extending a poly from ground field to extension field is given.

Then come the m-tuples.

Example 4: GF(4) in m-tuple notation. They show for GF(4) that you can take $x^4 - 1$ and get the four elements of GF(4) as factors. This leads up to:

Theorem 3: Elements of GF(q) are roots of $x - x^q$.

This is my Big Theorem 2. I prove mine after knowledge of cyclic, so easy. They do proof before.

Example 5: Here they take some poly over GF(4) and show that it completely factors in GF(4).

Now begins the minimum polynomial discussion, a rather cold start. They ask: consider 010 in GF(8), construct all polys which have this as a factor. I do not see how they get their exhaustive list, but I know there is such a list. The point of doing this is that they happen to notice that all such polynomials seem

to be a multiple of $m(x) = 1 + x + x^3$. If this were the min poly as I would define it, then this is what we would expect.

Several things are noted about m(x), all of which I have noted in my list. You could use this as your f(x) , by the way, in the residue class ring thing. Not clear why you might do this yet.

Definition 3: the *minimum polynomial* m(x) of α.

Theorem 4: If the min pol of α is m(x), then is a root of f(x) iff m(x) divides f(x).

Proof both ways is very easy, I have not claimed this one yet.

Corollary 5: The min poly is unique.

If two different ones, then you know from Thm 4 that a divides b and b divides a so a(x) = b(x).

Note that there is no dicussion of conjugates, or how you might construct the min poly!

Theorem 6: Consider a *code* whose codewords are polynomials s(x) which have the property that $s(\alpha) = 0$, for α in $GF(2^m)$. We do not care how long the m-tuples are yet. Claim that:

(a) code is binary cyclic code
(b) code length is order of α { this is n, the bits in a code word }
(c) generator g(x) of the ideal is m(x) of α.

Aside having nothing to do with this theorem:

Right now I am a blank on cyclic codes and their relation to anything. But I agree with all A&B statements which follow, which are:

1. α is an element of $GF(2^m)$ and is a root of $x^{q-1} - 1$.
2. If α generates $(\alpha, n, \bullet)$, then α is also a root of $x^n - 1$.
3. We therefore know that m(x) divides $x^n - 1$.

We know from Theorem 4 that m(x) must divide any f(x) which has α as a root. Thus, it divides this thing which has n as the order of α. I have not noted this fact yet.

4. **Claim**: n is the *smallest* integer such that m(x) divides $x^n - 1$. How do we know this?

Proof: if there were a smaller m that worked, then since α is a root of m(x), it would be a root of $x^m - 1$, since we are claiming that $x^m - 1 = m(x)q(x)$. From my Fact 4, this would mean n must divide m, which is impossible. Thus, n = order of α is the smallest n for which m(x) divides $x^n - 1$.

Definition X: The smallest integer n such that m(x) of α divides $x^n - 1$ is called the *period* of m(x).

We have just seen that the period of m(x) is the order of α where α is any root of m(x).

Note on Rings: Suppose you do the residue thing with $f(x) = x^n - 1$. Your ideal is then all polys which are multiples of this, and the rows correspond to all the remainders. Aha! Consider this ring:

Ring2 = Polys[x,GF(2)]/ $(x^n - 1)$ = Ring1/Ideal1

Note in passing that the ring Ring1 is just a ring of polys over GF(2), it is not a field.

This f(x) can be reduced, so this Ring2 is not a field. There are 2^n elements in this ring. Each one is associated with a remainder poly of degree less than n -- a row. ! So I think we can consider these as binary numbers of length n bits. All bytes of length n are included.

Now, assume we can find some poly g(x) that divides $x^n - 1$. A candidate is certainly m(x). Suppose our g(x) is irreducible. Then what do we know? What might we do next? Try this:

$$\text{Ring3} = \text{Ring2}/(\ g(x)) \ = \ \text{Ring2/Ideal2} \quad = \quad GF(2^m).$$

Thus, out of all polys of degree less than n (all bytes of length n) (= Ring2), we consider only those that are a multiples of g(x). This thing (g(x)) is then an ideal. Since g(x) is irreducible, this thing looks like a field. Assume yes for the moment. What is the order of this field? Assume g(x) is of some order m, of course m < n. Then the new remainders are polys of degree less than m, so we are now talking $GF(2^m)$.

Quick Review of Cyclic Codes

Go back to the starting ring Ring1 of all binary polys of any degree. Now consider Ring2 which is enumerates as all remainders of degree less than n. This ring thus contains all n-bytes, no restrictions.

Fact: Consider multiplying polys of different rows. Select x from a row, and some n-byte. Go ahead and multiply them. So you have 01000000 x ABCD... in tuple notation. The claim is that you just cause a cyclic perm on the digits of your n-byte. Yes, the degree is too high, so you have to remainder the thing, you have to divide it by $x^n - 1$.

So all we know is this so far: multiply by x, and the n-byte multiplied undergoes a rotation. So what?

Consider out of the blue $x^n - 1 = h(x)g(x)$. Assume you have found some g(x) so this is true, maybe g(x) is reducible even. Assume g(x) has order n-k = m. We now have a Ring3 of 2^m polys of degree less than m. Suppose we have "data words" which are k-bytes. d(x) is poly order k-1. For each such d(x), we can make d(x)g(x) which is a poly of order less than n. So d(x)g(x) lies in the ring of 2^n elements. But as you vary d(x), you only get multiples of g(x). These multiples comprise Ideal2. So for all possible d(x), we get all possible elements in the Ideal2.

Ideal2 is an ideal (subring) of Ring2 which has 2^n elements. Thus, as you generate all the elements of Ideal2, you generate only some elements of Ring2 of n-bytes. Call these n-bytes "code words". Since there are 2^k possible d(x), there are 2^k codewords in the n-byte space.

Fact: you can easily show based on the $x^n - 1 = h(x)g(x)$ fact that if c(x) = d(x)g(x) is a codeword, then so are all cyclic perms of c(x). Fine.

Thus, we can describe an (n,k) block code in this way, and no need for g(x) to be irreducible.

Now back to the theorem which we repeat.

Theorem 6: Consider a *code* whose codewords are polynomials s(x) which have the property that $s(\alpha) = 0$, for α in $GF(2^m)$. Claim that:

(a) code is binary cyclic code
(b) length of the code words is n, the order of α
(c) generator g(x) of the ideal is m(x) of α.

Now try to interpret all this. Claim that these statements are the same:

1. Consider all polys s(x) such that $s(\alpha) = 0$.
2. Consider all polys s(x) which are multiples of m(x), the min poly of α.

We learn later that m(x) divides $x^n - 1$ where n is the order of α. Thus, if we say:

2. All polys c(x) = d(x)m(x) that are multiples of m(x).

We know that there exists some h(x) such that

$$h(x)m(x) = x^n - 1$$

Thus, finally we can identify m(x) as the generator g(x) of a cyclic code. Now, how can we connect with the standard numbers n and k?

g(x) has degree n-k	m(x) has degree n-k
c(x) have degree $\leq$ n	n is the order of α.

So here is the connection:

1) n = code length = the order of α in $GF(2^m)$
2) n-k = degree of m(x)

Thus, for any α, there is some order n, there is some m(x), and we get some mysterious cyclic code. I agree, we get some cyclic code. I do not know that it has any special properties.

Question: what role is played by the m of $GF(2^m)$? That is, $q = 2^m$. We certainly know that $n < q$. I now don't think m has any role other than specifying the field. m is *not* the length of the data words or of the code words, so in the above we had some red herring action.

How to leave this theorem: if just says that, given some m, you can consider $GF(2^m)$ on your plate. Then consider any element α of $GF(2^m)$. It has some m(x). If order of α is n, and if degree of m(x) is n-k, you can then define an (n,k) cyclic code. I agree, but I do not see any great significance yet to this. Is this a BCH code or something?

Lets move on in our review, we got stuck pretty long here on Theorem 6.

Example 6: Here he takes m=3, so we are talking α in GF(8). Pick α = 010. It has $m(x) = 1+x+x^3$. Since q-1 is prime = 7, we know that order of α = 7. Thus, n=7 for our code. And 3 = n-k, so k = 4. So we have a (7,4) code. It looks like maybe this is a Hamming code of max distance.

Definition 4: the exponent thing for abelian group

Lemma 7: The business that e' must divide e.

Theorem 8: GF(q) - 0 is cyclic.

Definition 5: An enumerator for this cyclic field is called a *primitive element*.

Example 7: Considers GF(16) and shows a nongenerator and a generator. I am by now quite familiar with this example/

Definition 6: I will restate this. If α is a primitive element of GF(q), ie, it generates all of GF(q), then its m(x) min pol is a *primitive polynomial*.

It follows that $m(\alpha) = 0$, and that m(x) is irreducible. I also know that m(x) divides $x^{q-1} - 1$. These authors are choosing not to stress m(x) too much I think.

Definition X: The smallest integer n such that m(x) of α divides x^n-1 is called the *period* of m(x).

Theorem 9: Suppose p(x) is irreducible over GF(p) and has degree m. Then p(x) is a primitive polynomial iff its period is q-1.

Proof: (1) If p(x) is a prim poly, then it is m(x) for a primitive element α, and $m(\alpha) = 0$. We know that m(x) divides $x^{q-1} - 1$. Is there are smaller n such that m(x) divides x^n-1? If so, then we have:

$$q(x)\, f(x) = (x^n - 1)$$

Since $m(\alpha) = 0$, this implies $\alpha^n = 1$ for $n < q-1$. But this would mean order of α divides n, but we know that order of α is q-1. Thus, if m(x) is a primitive polynomial, the period of m(x) is the full q-1.

(2) Suppose period is q-1 for some irreducible f(x) of degree m. We have $q(x)\, f(x) = (x^{q-1} - 1)$. Assume f(x) has some root α. If α is not a primitive element, then it has order < q-1, and α is a root of $x^n - 1$.

STOP. Whole thing is not clearly formulated. I think f(x) is always supposed to be a min poly.

I think the theorem is really this:

My version of Theorem 9:

Let m(x) be the min poly of α. Then α = primitive element and m(x) = primitive poly if and only if the period of m(x) is the full q-1.

Accept for now and see if we can see significance of the period.

Difference Equations: (from some earlier chapter).