Chapter 22 Factoring P2(x, n) over a Finite Field

We start with a theorem:

Theorem 21-1 *The polynomial P2(x, n) of degree 3n which is generated by G(x) can be completely factored into polynomials of degree 1, modulo p, provided n|(p-1) and p is the discriminant of the irreducible polynomial G(x).*

The definitions of P2(x, n) and G(x) were given in the previous chapter. An example is given here:

Let $G(x) = x^3-2x^2-1$ be the irreducible polynomial of discriminant 59. The theorem states that P2(x,n) is generated for any n that is a factor of 59-1 = 58 = (2)*(29). It can be shown using *Mathematica* that for n = 2 the following 6^{th} degree polynomial is obtained;

[1] $P2(x, 2) = 1 + 4x^2 + 4x^4 - x^6 = -(x + 19)\,(x + 40)\,(x + 21)^2\,(x + 38)^2 \mod (59)$

where the negative sign replaces the value 58 = -1 mod (59).

A similar factoring into multiple factors of the form $(x + a_i)^r$ where r = 3 and $a_i \in 1, 2, \ldots..(p-1)$ can be shown for n = 29. For any n|(p-1), p divides the sum of all a_i (multiplicity not included). For any other value of n not a factor of (p-1), P2(x, n) cannot be completely factored into the form of a product $(x + a_i)^{ri}$.

In Chapter 20 we discussed the splitting of polynomials under modulo $x^2 + p*y^2$. Given in our case, p = 59 and choosing x=21, y = 2 the resulting prime 677 can completely split P2(x,2) as,

[2] $P2(x, 2) = -(x + 20)\,(x + 101)\,(x + 123)\,(x + 554)\,(x + 576)\,(x + 657) \mod (677)$

into monic factors of degree one. However, this is not true for P2(x, 29) since 677-1= 676 is not factored by 29. Searching for a prime p of the form $x^2 + 59*y^2$ where 29|(p-1), the resulting prime 5801 (x=45, y = 8) completely factors P2(x, 29).

Corollary 1: Let P2(x, n) be a polynomial generated from a cubic polynomial of discriminant p. Then P2(x, n) is completely factored modulo p and modulo $x^2 + p*y^2$ for values of n in which (p-1) and $x^2 + p*y^2$ -1 have n as a common factor.

Corollary 2: Let P2(x, n)/G(x) be the quotient (remainder free) polynomial generated from a cubic polynomial of discriminant p. Then P2(x, n)/G(x) is completely factored modulo p and modulo $x^2 + p*y^2$ for values of n in which (p-1) and $x^2 + p*y^2$ -1 have n as a common factor.

The Decomposition of an N-Dimensional Space[1]

We can use the complete factoring of P2(x, n) in a finite field to generate a characteristic equation of an operator (matrix) **A**. Define the coefficients a_i as the 3n eigenvalues (multiplicity is included). Then, P2(x, n) is the characteristic equation since the eigenvalues fall on a matrix diagonal as $(x + a_i)^{ri}$, and the determinant of this matrix is the characteristic equation. P2(x, n) is a polynomial of degree 3n and is a monic polynomial with coefficients in the field of a prime p. In general **A** can be any matrix such that

[1] Chapter II, Linear Vector Spaces in P. Dennery, A. Krzywicki, **Mathematics for Physicists**, Harper and Row, 1967.

[3] P2(λ, n) = det(λ**E** – **A**) = 0

with **E** the identity matrix. Since P2(λ, n) is derived from symmetry principles, the matrix **A** is a symmetric matrix.

The polynomial ϕ(λ) is generated from the negative a_i roots of the characteristic equation of **A** and r_i the multiplicity of the i [th] root modulo p.

[4] $\phi(\lambda) = -\prod_{i=1}^{L}(\lambda - (-a_i))^{r_i}$

where (i = 1, 2…. L).

It is possible to decompose the inverse of the characteristic polynomial as a sum;

[5] $\frac{1}{\phi(\lambda)} = -\sum_{i=1}^{L} f_i(\lambda) \Big/ (\lambda - (-a_i))^{r_i}$

Where $f_i(\lambda)$ is a polynomial of degree less than $r_i - 1$.

Multiply both sides by ϕ(λ) to obtain;

[6] $1 = -\sum_{i=1}^{L} f_i(\lambda) \prod_{i \neq k}(\lambda - (-a_k))^{r_k}$

And define the functions $\phi_\iota(\lambda)$ as

[7] $\phi_\iota(\lambda) = -f_i(\lambda) \prod_{i \neq k}(\lambda - (-a_k))^{r_k}$

In the above equations [4] to [7] the polynomials are reduced modulo p and ϕ(λ) = P2(λ, n).

As an example, calculate equation [5] for the polynomial P2(λ,2) in equation [1]. The eigenvalues are defined from the expansion as $(-a_i)$ = (-19, -40, -21, -21, -38, -38). Note that L = 4. *Mathematica* functions are used to find $f_i(\lambda)$.

Make the variable substitution λ→ x in the equations below. The expansion coefficients of the inverse series are obtained from the command;

[8] $\text{CoefficientList}[\text{Series}[-1/((19+x)(21+x)^2(38+x)^2(40+x)), \{x, 0, 20\}], x, \text{Modulus} \to 59]$

For the factors of the form $(x + a_i)^{r_i}$, the function $f_i(x)$ is a constant if $r_i = 1$ and a linear function (c +dx) if $r_i = 2$. The coefficient list command is then used with unknown constants a, b, c, d, e;

[9] $\text{CoefficientList}[\text{Series}[-a/(19+x) - b/(40+x) - (c+d*x)/(38+x)\text{^}2 - (e+f*x)/(21+x)\text{^}2 + 1/((19+x)(21+x)^2(38+x)^2(40+x)), \{x, 0, 20\}], x, \text{Modulus} \to 59]$

The first five of the resultant coefficients are then solved as simultaneous equations using the GroebnerBasis command:

[10] $\text{GroebnerBasis}[\{58 + 31a + 28b + 40c + 40e, 17a + 17b + c + 40d + 58e + 40f, 4 + 55a + 4b + 38c + d + 38e + 58f, 53a + 53b + 38c + 38d + 21e + 38f, 47 + 50a + 9b + 43c + 38d + 43e + 21f, 16a + 16b + 21c + 43d + 38e + 43f\}, \{f, e, d, c, b, a\}, \text{Modulus} \to 59]$

The resulting constants are immediately obtained,

[11] $\{30+a, 29+b, 35+c, 31+d, 35+e, 28+f\}$

Substituting the constants a, b, c, d, e in [9], equation [6] is verified as,

[12] 1 = $[-30*(21+x)^2(38+x)^2(40+x) - 29*(19+x)(21+x)^2(38+x)^2 - ((35)+(31)*x)*(19+x)(21+x)^2(40+x) - ((35)+(28)*x)*(19+x)(38+x)^2(40+x), \text{Modulus} \to 59]$

Since L = 4, the four polynomials $\phi_i(x)$ are extracted and expanded modulo 59 as in equation [7].

[13a] $\phi_1(x) = 14 + 21x + 58x^2 + 28x^3 + 39x^4 + 29x^5$

[13b] $\phi_2(x) = 14 + 38x + 58x^2 + 31x^3 + 39x^4 + 30x^5$

[13c] $\phi_3(x) = 16 + 23x + x^2 + 3x^3 + 20x^4 + 28x^5$

[13d] $\phi_4(x) = 16 + 36x + x^2 + 56x^3 + 20x^4 + 31x^5$

Such that $\phi_1(x) + \phi_2(x) + \phi_3(x) + \phi_4(x) = 1 \bmod (59)$.

The **Hamilton-Cayley** theorem states that we can replace x by the operator **A** in the characteristic equation. I have defined **A** as the 6x6 diagonal matrix of the eigenvalues.

[14] $\mathbf{A} = \begin{pmatrix} -19 & 0 & 0 & 0 & 0 & 0 \\ 0 & -40 & 0 & 0 & 0 & 0 \\ 0 & 0 & -21 & 0 & 0 & 0 \\ 0 & 0 & 0 & -21 & 0 & 0 \\ 0 & 0 & 0 & 0 & -38 & 0 \\ 0 & 0 & 0 & 0 & 0 & -38 \end{pmatrix}$

Then $\phi(\mathbf{A}) = 0$ and from the above verification $\sum_{i=1}^{L} \phi_i(\boldsymbol{A}) = \mathbf{E}$ where **E** is the identity matrix.

Lemma-1 *The operators* $\phi_i(\boldsymbol{A})$ *fulfill an orthogonality condition in the finite field p:*

$$\phi_i(\boldsymbol{A}) * \phi_k(\boldsymbol{A}) * \boldsymbol{v_{ek}} = \delta_{ik} * \phi_k(\boldsymbol{A}) * \boldsymbol{v_{ek}}$$

Where $\boldsymbol{v_{ek}}$ *is an eigenvector in the N dimensional space* S_N *of* $\phi_k(\mathbf{A})$ and δ_{ik} is the Kroecker delta function.

Lemma-2 *An arbitrary vector* $\boldsymbol{v}$ *in N space is decomposed by the sum of operators* $\phi_i(\boldsymbol{A})$ *such that*

$$\boldsymbol{v} = \sum_{i=1}^{L} \phi_i(\boldsymbol{A}) * \boldsymbol{v}$$

In addition, for a given eigenvalue λ_i *and associated eigenvector(s)* $\boldsymbol{v_{ei}}$ *the operators satisfy the following conditions:*

$$(\boldsymbol{A} - \lambda_i \boldsymbol{E})^{r_i} * \boldsymbol{v_{ei}} = 0 \text{ and } \quad (\boldsymbol{A} - \lambda_i \boldsymbol{E})^{r_i} * \phi_i(\boldsymbol{A}) * \boldsymbol{v_{ei}} = 0$$

Where r_i *is the multiplicity of the eigenvalue.*

Using the polynomial $\phi_4(x)$ which corresponds to $\lambda_i = -21$ of multiplicity 2, the eigenvector(s) and $\phi_4(\mathbf{A})$ are:

$\boldsymbol{v_e} = \{0,0,0,-1,0,0\}$ *and* $\{0,0,-1,0,0,0\}$

$\phi_4(\mathbf{A}) = 16 + 36\boldsymbol{A} + \boldsymbol{A}^2 + 56A^3 + 20\boldsymbol{A}^4 + 31\boldsymbol{A}^5$

Matrix powers are evaluated in *Mathematica* resulting in the matrices modulo 59,

$\phi_4(A) = \begin{bmatrix} 0. & 0. & 0. & 0. & 0. & 0. \\ 0. & 0. & 0. & 0. & 0. & 0. \\ 0. & 0. & 1. & 0. & 0. & 0. \\ 0. & 0. & 0. & 1. & 0. & 0. \\ 0. & 0. & 0. & 0. & 0. & 0. \\ 0. & 0. & 0. & 0. & 0. & 0. \end{bmatrix}$ $(\mathbf{A}- (-21)\ \mathbf{E})^2 = \begin{bmatrix} 4. & 0. & 0. & 0. & 0. & 0. \\ 0. & 7. & 0. & 0. & 0. & 0. \\ 0. & 0. & 0. & 0. & 0. & 0. \\ 0. & 0. & 0. & 0. & 0. & 0. \\ 0. & 0. & 0. & 0. & 53. & 0. \\ 0. & 0. & 0. & 0. & 0. & 53. \end{bmatrix}$

Choosing an arbitrary vector in N = 6 space, $\mathbf{v} = \{1, -1, 0, 1, -1, -1\}$,

$\phi_4(\mathbf{A})*\mathbf{v} = \{0., 0., 0., 1., 0., 0.\}$

$(\mathbf{A}- (-21)\ \mathbf{E})^2 * \phi_4(A)*\mathbf{v} = 0$

$(\mathbf{A}- (-21)\ \mathbf{E})^2 * \boldsymbol{v_e} = 0$

The complete expansion of **v** as $\sum_{i=1}^{L} \phi_i(\boldsymbol{A}) * \boldsymbol{v}$ is,

$\mathbf{v} = \{1., 0., 0., 0., 0., 0.\} + \{0., -1., 0., 0., 0., 0.\} + \{0., 0., 0., 0., -1., -1.\} + \{0., 0., 0., 1., 0., 0.\}$

The linear combination of vectors belonging to the L subspaces of the operator $\phi_i(\mathbf{A})$ allows for the expansion of an arbitrary vector in this space. We can find these operators for any characteristic polynomial P2(x, n) given the constraints described in **Theorem 1**. In addition, the operators $\phi_i(\mathbf{A})$ reduce the rank of an arbitrary matrix but the sum of the ranks of the sub matrices equals the rank of the original matrix.

Equivalence Relations

In this section, we find matrices equivalent to the diagonal matrix **A**. These matrices have the same following properties as **A**: (1) eigenvalues, (2) determinant and (3) characteristic polynomial. By definition, two square matrices **A** and **C** are similar if and only if,

[15] $\mathbf{C = P^{-1}AP}$

where **P** is a nonsingular matrix and has an inverse $\mathbf{P}^{-1}$.

The method of finding the diagonalization matrix **P** is normally used to diagonalize **C** such that

[16] $\mathbf{A = PC\ P^{-1}}$

Our analysis factors a polynomial in a finite field and we represent the complete factorization of P2(x,n) in the field as the diagonal matrix **A**.

I have developed a method for finding a matrix **C** by using the companion matrix **R** of the characteristic polynomial.

Let P2(x,n) be the minimal polynomial with coefficients c_i in the finite field p. Then **R** is defined as

[17] $\mathbf{R}= \begin{bmatrix} 0. & 1. & 0. & 0. & 0 \ldots . & 0. \\ 0. & 0. & 1. & 0. & 0 \ldots . & 0. \\ 0. & 0. & 0. & 1. & 0 \ldots . & 0. \\ 0. & 0. & 0. & 0. & 1 \ldots . & 0. \\ 0. & 0. & 0. & 0. & 0 \ldots . & 1. \\ c_1. & c_2. & c_3. & c_4. & c_5 \ldots . & c_k. \end{bmatrix}$

where k = 3n-1 and **R** is a 3n **x** 3n square matrix. The matrix **R** has the same characteristic polynomial as **A**.

(see D. Finkbeiner, **Introduction to Matrices and Linear Transformations**, W.H. Freeman and Co. 2nd Ed.)

Given the matrices A and R calculate the following matrices to obtain **P**.

[18a,b,c] $\mathbf{AO = R.A.R^{-1}.}$

$\mathbf{P = [AO^{-1}]^T.AO}$

$\mathbf{C= P^{-1}.A.P}$

Where the dot represents matrix multiplication, X^{-1} represents the inverse of a matrix X and X^T is the transpose of the matrix X.

The number of nonzero entries in **C** is related to the number of coefficients c_i in the characteristic polynomial. All calculations are completed in the finite field of modulo p.

The characteristic equation [1] and diagonal matrix [14] mod 59 is used as an example. Since the characteristic polynomial only has coefficients c_1, c_3 and c_5 the resulting matrix will be sparse.

$$\mathbf{R} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 4 & 0 & 4 & 0 \end{bmatrix}$$

$$\mathbf{R^{-1}} = \begin{bmatrix} 0 & 55 & 0 & 55 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\mathbf{AO} = \begin{bmatrix} 19 & 0 & 0 & 0 & 0 & 0 \\ 0 & 38 & 0 & 0 & 0 & 0 \\ 0 & 0 & 38 & 0 & 0 & 0 \\ 0 & 0 & 0 & 21 & 0 & 0 \\ 0 & 0 & 0 & 0 & 21 & 0 \\ 0 & 51 & 0 & 42 & 0 & 40 \end{bmatrix}$$

$$\mathbf{AO^{-1}} = \begin{bmatrix} 28 & 0 & 0 & 0 & 0 & 0 \\ 0 & 14 & 0 & 0 & 0 & 0 \\ 0 & 0 & 14 & 0 & 0 & 0 \\ 0 & 0 & 0 & 45 & 0 & 0 \\ 0 & 0 & 0 & 0 & 45 & 0 \\ 0 & 50 & 0 & 56 & 0 & 31 \end{bmatrix}$$

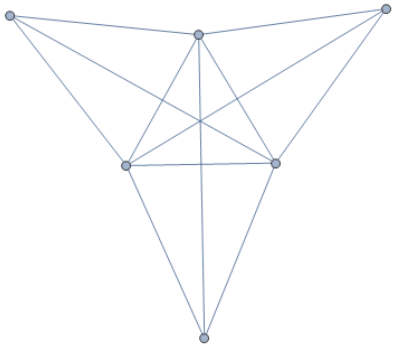
$$\mathbf{[AO^{-1}]^T.AO= P} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 14 & 0 & 35 & 0 & 53 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 24 & 0 & 52 & 0 & 57 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 47 & 0 & 4 & 0 & 1 \end{bmatrix}$$

$$\mathbf{P^{-1}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 6 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 12 & 0 & 55 & 0 & 6 \end{bmatrix}$$

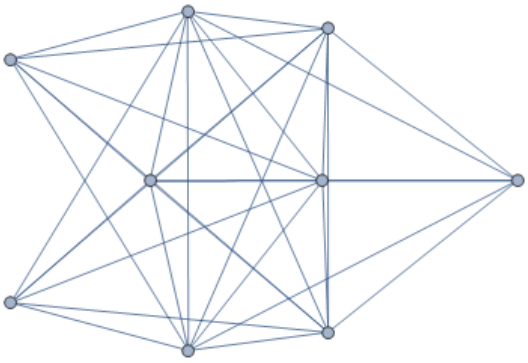
$$\mathbf{C} = \begin{bmatrix} 40 & 0 & 0 & 0 & 0 & 0 \\ 0 & 52 & 0 & 48 & 0 & 12 \\ 0 & 0 & 38 & 0 & 0 & 0 \\ 0 & 54 & 0 & 20 & 0 & 25 \\ 0 & 0 & 0 & 0 & 21 & 0 \\ 0 & 38 & 0 & 49 & 0 & 6 \end{bmatrix}$$

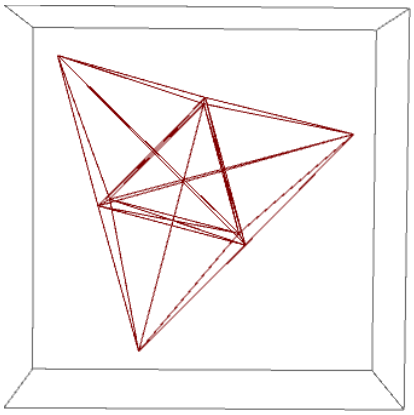
The determinant of **A** and **C** is 58 = -1 mod (59). Both matrices have characteristic polynomials $-1 - 4x^2 - 4x^4 + x^6 = 58 + 55x^2 + 55x^4 + x^6$ mod (59) and equal eigenvalues.

It is interesting to calculate the adjacency graph for matrix **C** assuming the 0's are edges (value 1) and the positive components are 0's. The resulting graph has 6 vertices and 12 edges and is shown below:



The symmetry of the figure is suggested from the symmetric functions used to derive P2(x,2)and the overall symmetry of **C**. The figure can be folded to reduce the outer three vertices to a single vertex forming a regular tetrahedron of 4 faces. A similar pattern occurs for all polynomials P2(x,2) independent of modulus. The adjacency graph for P2(x,3) with 33 edges is more complicated (see below left) but when rotated aligns as a regular tetrahedron (right).





Richard Turk

June 22, 2017