CIRI-CIRI POLINOMIAL PERMUTASI ATAS FINITE FIELD

ABSTRAK

Polinomial atas finite field GF (q) memiliki aplikasi cukup luas yang mencakup area seperti coding theory, cryptography, combinatoric, konstruksi dari error-correcting codes maupun teknologi terkini seperti telepon seluler CDMA. Area-area tersebut sering menggunakan suatu polinomial dengan sifat khusus yang disebut polinomial permutasi. Polinomial f atas finite field GF (q) merupakan polinomial permutasi jika pemetaan f:GF (q)-GF (q)adalah pemetaan satu-satu. Penulisan ini membahas ciri-ciri dari suatu polinomial atas finite field GF (q) agar menjadi polinomial permutasi.

Kata kunci: Polinomial, polinomial permutasi, finite field

[1]Aini Suri Talita,
[2]Sri Mardiyati,
[3]Helen Burhan

[1,2] Pusat Studi Komputasi Matematika, Universitas Gunadarma
[3] Departemen Matematika FMIPA Universitas Indonesia

ainisuri@staff.gunadarma.ac.id,
sri_mardiyati@hotmail.com,
hnburhan@yahoo.com

PENDAHULUAN

Finite field maupun polinomial atas *finite field* memiliki aplikasi yang cukup luas sehingga menarik untuk dibahas. Aplikasi tersebut mencakup area seperti *coding theory*, *cryptography*, *combinatoric*, konstruksi dari *error-correcting codes* maupun teknologi terkini seperti telepon seluler CDMA (Blake et al. 1-4). Area-area tersebut sering melibatkan suatu polinomial atas *finite field* dengan sifat khusus yang disebut polinomial permutasi.

Polinomial f atas *finite field* $GF(q)$ merupakan polinomial permutasi jika pemetaan $f: GF(q) \rightarrow GF(q)$ adalah pemetaan satu-satu (Mollin and Small 535). Suatu polinomial yang merupakan polinomial permutasi di suatu *finite field* belum tentu merupakan polinomial permutasi di *finite field* yang lain. Sebagai contoh $f: (x) = x^2$, merupakan polinomial permutasi pada Z_z karena $f([0]_2) = [0]_2$ dan $f([1]_2) = ([1]_2)$. dan $f([1]_2) = ([1]_2)$ Namun $f(x) = x^2$, bukan polinomial permutasi pada Z_z , karena $f([1]_3) = [1]_3 = f([2]_3)$.

Polinomial permutasi atas *finite field* memiliki beberapa aplikasi khusus seperti *modular enciphering* dan *Imai-Matsumoto system* yang berkaitan dengan *cryptosystem*, *latin square* berkaitan dengan *combinatoric*, maupun pembentukan *key* berkaitan dengan *cryptography* (Lidl and Pilz 243, 252, 398; Koblitz 80).

Untuk menentukan apakah suatu polinomial atas *finite field* merupakan polinomial permutasi dapat digunakan cara yang paling sederhana yaitu dengan mendaftarkan semua hasil peta fungsi polinomial tersebut, kemudian memeriksa apakah himpunan peta yang didapat memuat semua anggota *finite field*. Akan tetapi, hal ini sulit dilakukan apabila jumlah anggota *finite field* besar. Karena itu, diperlukan suatu kriteria sederhana untuk memeriksa apakah suatu polinomial atas *finite field* merupakan polinomial permutasi atau bukan. Pada penulisan ini akan dibahas ciri-ciri dari beberapa polinomial atas *finite field* sebagai polinomial permutasi.

HASIL DAN PEMBAHASAN

Penulisan ini dimulai dengan membahas ciri-ciri dari suatu monomial $f(x) = x^m \in GF(q)[x]$, $m \in N, m < q$ agar menjadi polinomial permutasi atas $GF(q)$.

Teorema 1

$f: (x) = x^k \in GF(q)$ [x], $k <$ q, , adalah polinomial permutasi jika dan hanya jika $gcd(k, q - 1) = 1$.

Bukti

Jika $f(x) = x^k$ adalah polinomial permutasi maka akan dibuktikan $gcd(k, q - 1) = 1$. Pembuktian dilakukan dengan kontradiksi. Andaikan $gcd(k, q - 1) = 1 \neq 1$ maka terdapat bilangan prima p yang membagi $gcd(k, q - 1)$. Hal ini mengakibatkan $p|(q - 1)$. dan $p|k$ karena $p|k$ maka $k = pu$, untuk suatu bilangan bulat u karena $p|(q - 1)$ *maka terdapat* $a \neq 1$ *anggota* $GF(q) - \{0\}$ sedemikian sehingga $a^p = 1$. *maka* $a^k = a^{pu} = (a^p)^u = 1^u = 1 = 1^k$, *dimana* $a \neq 1$ *sehingga f bukan fungsi satu-satu. Hal ini kontradiksi dengan yang diketahui bahwa* $f(x)$ polinomial permutasi.

Sebaliknya, misalkan $gcd(q - 1) = 1$ maka terdapat bilangin bulat m dan n, *sedemikian sehingga* $nk+m(q-1) = 1$. *Untuk* x_1, x_2 *anggota* $GF(q)$, jika berlaku $f(x_1) = f(x_2)$ maka akan dibuktikan $x_1 = x_2$. *Pembuktian dibagi menjadi dua kasus yaitu jika* $f(x_1) = f(x_2) = 0$ dan jika $f(x_1) = f(x_2) \neq 0$

Jika $f(x_1) = f(x_2) = 0$ maka $x_1^k = x_2^k = 0$. Karena $GF(q)$ merupakan integral domain maka didapat $x_1 = 0 = x_2$

Jika $f(x_1) = f(x_2) \neq 0$. Jelas x_1 dan x_2 keduanya bukan 0. Karena berlaku $f(x_1) = f(x_2)$ maka $x_1^k = x_2^k$

$\Leftrightarrow x_{1n}^k = x_{2n}^k$

Karena x_1 , $x_2 \neq 0 \in GF(q) - \{0\}$ maka $x_1^{(q-1)} = 1 = x_2^{(q-1)}$ Sehingga $x_1^{m(q-1)} = 1 = x_2^{m(q-1)}$ di peroleh $x_1^{nk + m(q-1)} = x_2^{nk + m(q-1)}$ Karena $nk + m(q - 1) = 1$ *maka* $x_1 = x_2$ Sehingga f adalah fungsi satu-satu.

Berikut ini ditunjukkan suatu syarat yang harus dipenuhi oleh suatu polinomial berderajat m_n agar menjadi polonomial permutasi.

Teorema 2

Misalkan $f(x) = \sum_{i=1}^{n} c_i x^{mi}$

anggota dari $GF(q)[x]$ dimana $m_n > m_{n-1} > \ldots > m_1 \geq 1$

$\prod_{i=1}^{n} c_i \neq 0$ dan misalkan pula $e = \gcd\{m_i, 1 \leq i \leq n\}$

Maka $f(x)$ polinomial permutasi pada $GF(q)[x]$ jika dan hanya jika gcd (e,q-1) = 1 dan

$\sum_{i=1}^{n} c_i x^{\frac{m_i}{e}}$ adalah polinomial permutasi

Bukti

Bukti didapat dari fakta bahwa monomial x^e adalah polinomial permutasi atas $GF(q)$ jika dan hanya jika gcd (e,q-1) = 1 (Teorema 1).

Teorema 3

Misalkan k,j bilangan bulat positif sedemikian sehingga $q>k>j \geq 1$ dan gcd (k-j,q-1)=1. Maka $ax^k + bx^j + c$ dengan $a \neq 0$ adalah polinomial permutasi atas $GF(q)$ jika dan hanya jika gcd (k,q-1 dan b=0

Bukti

$ax^k + bx^j + c$ merupakan polinomial permutasi jika dan hanya jika $x^k + a^{-1}bx^j$ merupakan polinomial permutasi. Misalkan $g(x) = x^k + a^{-1}bx^j$. diketahui $\gcd(k,q-1) = 1$ dan b=0. berdasarkan teorema 1, $g(x)$ adalah polinomial permutasi.

Jika diketahui $g(x)$ adalah polinomial

permutasi akan ditunjukkan $gcd(k,q\text{-}1)=1$ dan b=0 Misal $gcd\ (k,q\text{-}1) \neq 1$. Pembuktian dibagi menjadi dua kasus yaitu jika b = 0 dan b ≠ 0. Untuk kasus b = 0, jelas berdasarkan Teorema 1 didapat $g(x)$ bukanlah polinomial permutasi. Untuk b ≠ 0, misalkan $a = -a^{-1}b \neq 0$ maka $g(x) = x^k - ax^j$, dengan a ∈ $GF(q)$. Dari premis diketahui bahwa $gcd\ (k\text{-}j,q\text{-}1)=1$ maka terdapat m,n ∈ z sedemikian sehingga $m(k\text{-}j) + n\ (q\text{-}1) = 1$ maka, am(k-j)+n(q-1)=a

Karena $a \in GF\ (q)$ - {0} maka $a^{n(q-1)} = 1$, sehingga $a^{m(k-j)} = a$ *sebut* $a^m=y \in GF(q)$. maka terdapat $y \in GF(q)$ sedemikian sehingga $a=y^{k-j}$,y≠0 Diketahui $g(x) = x^k - ax^j = x^j\ (x^{k-j} - a) = x^j\ (x^j$, maka $g(y) = 0 = g\ (0)$, padahal $y \neq 0$, *Sehingga g bukan fungsi satu-satu.*

Berdasarkan Teorema 3. diperoleh Akibat 4 dan Akibat 5 berikut ini.

Akibat 4

$ax^2 + bx + c$, $(a \neq 0)$ adalah polinomial permutasi atas $GF(q)$ jika dan hanya jika b=0 dan karakteristik dari $GF(q)$ adalah 2.

Bukti

Analog dengan Teorema 3 untuk k=2 dan j =1. Berdasarkan Teorema 3. ax^2+bx+c, dengan a ≠ 0, merupakan polinomial permutasi jika dan hanya jika b = 0 dan $gcd^{(2,q-1)}=1$. Haruslah q-1 ganjil. Maka karakteristik $GF\ (q)$ adalah 2.

Akibat 5

Misalkan q-1 tidak habis dibagi 3, 5 atau 7. Maka x^8 atau ax^t untuk t ganjil dan t < 8, adalah polinomial permutasi pada GF(q) jika dan hanya jika pada GF(q) dan GF(q) memiliki karakteristik 2.

Bukti

Berdasarkan Teorema 3. $x^8 + ax^t$ polinomial permutasi jika dan hanya jika $a = 0$ dan $gcd(8,q\text{-}1) = 1$ yaitu q-1 ganjil. Maka karakteristik $GF(q)$ adalah 2.

Pada teorema-teorema berikut akan dibahas ciri-ciri trimonial yang lain untuk menjadi polinomial permutasi.

Teorema 6

Misalkan $f(x) = ax^k + bx^j + c$ merupakan polinomial atas $GF(q)$ dengan a ≠ 0 dan $-ba^{-1}$ merupakan pangkat ke $(k\text{-}j)$ dari suatu anggota dalam $GF(q)$. Maka $f(x)$ polinomial permutasi jika dan hanya jika $b=0$ pada GF(q) dan $(k,q\text{-}1) = 1$

Bukti
Misalkan $g(x) = x^k + a^{-1}bx^j$, $f(x)$ merupakan polinomial permutasi jika dan hanya jika $g(x)$ merupakan polinomial permutasi. Jika diketahui $gcd(k,q\text{-}1)=1$ dan $b=0$ Berdasarkan Teorema 1, $g(x)$ adalah polinomial permutasi.

Jika diketahui $g(x)$ adalah polinomial permutasi. akan ditunjukkan $gcd(k,q\text{-}1)=1$ dan $b=0$

Misal $gcd\ (k,q\text{-}1) \neq 1$. terdapat 2 kasus yaitu jika $b=0$ dan $b \neq 0$. Untuk $b=0$, berdasarkan Teorema 1, didapat $g(x)$ bukanlah polinomial permutasi. Untuk $b \neq 0$. Misalkan $a=-ba^{-1} \neq 0$. maka $g(x) = x^k - ax^j$, dengan $a \in GF(q)$ dari premis diketahui bahwa $a=-ba^{-1}$ merupakan pangkat ke $(k\text{-}j)$ dari suatu anggota dalam $GF(q)$ Maka terdapat $y \in GF\ (q)$ sedemikian sehingga $a=y^{k-j}$, $y \neq 0$ Diketahui $g(x) = x^k - ax^j = x^j(x^{k-j}) - a) = xj\ (x^k$-. Jadi $g(y) = 0 = g\ (0)$. Padahal $y \neq 0$ jadi g bukanlah fungsi satu-satu. terdapat disimpulkan bahwa $g(x)$ bukan polinomial permutasi.

Berdasarkan Teorema 6, diperoleh Akibat 7 berikut ini.

Akibat 7 Misalkan $f(x) = ax^k + bx^j +$ c merupakan polinomial atas $GF(q)$ dengan a ≠ 0 dan $-ba^{-1}$ merupakan pangkat ke d dari suatu anggota dalam $GF(q)$ dimana $d=gcd(q\text{-}1, k\text{-}j)$, maka $f(x)$ merupakan polinomial permutasi jika dan hanya jika b=0 dan $gcd(k,q\text{-}1) = 1$

Bukti

Karena $-ba^{-1}$ merupakan pangkat ke d dari suatu anggota dalam $GF(q)$, dimana $d = gcd(q\text{-}1,k\text{-}j)$, maka terdapat $y \in GF(q)$ sedemikian sehingga $y^d = -ba^{-1}$. Pembuktian dibagi 2 kasus yaitu jika $y=0$ dan $y \neq 0$. Jika $y=0$. Didapat $-ba^{-1}=0$. Karena $a \neq 0$ dan $GF(q)$ integral domain maka $b=0$. Sehingga $f(x) = ax^k + c$ Namun $f(x)$ polinomial permutasi jika dan hanya jika x^k polinomial permutasi. Berdasarkan Teorema 1, $f(x)$ polinomial permutasi jika dan hanya jika $gcd\ (k,q\text{-}1) = 1$. Jika $y \neq 0$ Karena $d=gcd\ (q\text{-}1,k\text{-}j)$, maka terdapat bilangan bulat m,n sedemikian sehingga $d=m(q\text{-}1) + n$(k-j). Didapat

$-ba^{-1} = y^d$

$\Leftrightarrow -ba^{-1} = y^{m(q-1)\ +\ n\ (k-j)}$

Karena $y \in GF(q)$ - {0} maka $y^{(q-1)} = 1$ Sehingga $-ba^{-1} = [(y])^n)^{(k-j)}$ sebut $y^n=z \in GF(q)$. *Maka* $-ba^{-1}=z^{(k-j)}$, $z \in GF(q)$.

Berdasarkan Teorema 6, $f(x)$ polinomial permutasi jika dan hanya jika $b=0$ dan $gcd\ (k,q\text{-}1) = 1$

Teorema 8
Misalkan $f(x) = ax^k + bx^j + c \in GF(q)\ [x]$ dimana j membagi k, $a \neq 0$

$$gcd\left(\left(\frac{k}{j}\right) - 1,\ q\ -\ 1\ \right) = d$$

dan $gcd(j,q\text{-}1)=1$
Misalkan pula $-ba^{-1}\beta^{-1}$ merupakan pangkat ke d dari suatu anggota pada $GF(q)$, dimana

$\beta = z^{\left(\frac{k}{j}\right)\text{-}1} + z^{\left(\frac{k}{j}\right)\text{-}2} + \cdots + 1$ untuk suatu $z \in GF(q)$, $z \neq 1$ Maka $f(x)$ merupakan polinomial permutasi jika dan hanya jika b = 0 dan $gcd(k,q\text{-}1) = 1$

Bukti

Sebut $kg(x) = x^k + a^{-1}\ bx^j$ dan $h(x) = x^j + a^{-1}\ bx$

f(x) merupakan polinomial permutasi jika dan hanya jika $g(x)$ merupakan polinomial permutasi. Jika diketahui $gcd(k,q\text{-}1) = 1$ dan b = 0.

Berdasarkan Teorema 1, didapat $g(x)$ adalah polinomial permutasi.

Jika diketahui $g(x)$ adalah polinomial permutasi maka akan dibuktikan $gcd(k,q\text{-}1) = 1$ dan $b= 0$. Misal $gcd(k,q\text{-}1) \neq 1$. Terdapat dua kasus yaitu untuk $b=0$ dan $b \neq 0$. Jika $b=0$, berdasarkan Teorema 1, didapat bahwa $g(x)$ bukanlah polinomial permutasi.
Untuk b ≠ 0. $g\ (x)$ polinomial permutasi jika dan hanya jika h(x) polinomial permutasi . Misalkan $\frac{k}{j} = k'$ Dimana k' merupakan bilangan bulat karena dari premis diketahui bahwa j membagi k. Misalkan $a=-ba^{-1} \neq 0$. Maka didapat $a\beta^{-1}=y_1^d \neq 0$ untuk y_1 suatu anggota $GF(q)$ - {0} dan $d = gcd(k'\text{-}1,q\text{-}1)$. terdapat bilangan bulat m,n sedemikian sehingga m(k'-1) + n(q-1) = d .

Sehingga

$a\beta^{-1}=y_1^{\ m(k'-1)+n(q-1)}$

$\Leftrightarrow a\beta^{-1}=y_1^{\ m(k'-1)}y_1^{n(q-1)}$ Karena $y_1 \in GF(q)$ - {0} maka didapat $y_1^{n(q-1)} = 1$ Sehingga $a\beta^{-1} = y_1^{\ m(k'-1)}$

$\Leftrightarrow a\beta^{-1} = (y_1^m)\ (k'\text{-}1)$ Misalkan $y_1 = y \neq 0$ suatu anggota $GF(q)$. Sehingga $a = y^{k'-1}\ \beta$

Diketahui

$\beta = z^{k'-1}+z^{k'-2} + \ldots + 1$ Misalkan $x=yz$. (x ≠ y karena z ≠ 1), maka $a=y^{k'-1}\beta=x^{k'-1}+x^{k'-2}y+x^{k'-2}y^2 + \ldots +$

Didapat $a(x\text{-}y) = x^{k'} - y^{k'}$ Sehingga $y^{k'} - ay = x^{k'} - ax$ dengan $x \neq y$

Diperoleh $h(y) = h\ (x)$ padahal $x \neq y$ jadi h bukanlah fungsi satu-satu. Terbukti $h(x)$ bukan polinomial permutasi. Demikian pula dengan $g(x)$.

SIMPULAN DAN SARAN

Simpulan

Dengan belum diperolehnya ciri-ciri untuk polinomial atas *finite field* secara umum agar menjadi polinomial permutasi, pada penulisan ini hanya dibahas ciri-ciri dari beberapa jenis polinomial yang merupakan polinomial permutasi.

Untuk monomial $f(x) = xk \in GF(q)[x], k<q$, monomial tersebut akan menjadi polinomial permutasi atas $GF(q)$ jika dan hanya jika $gcd(k.q\text{-}1)=1$ seperti ditunjukkan pada Teorema 1, sedangkan untuk trinomial, dengan menambahkan syarat-syarat tertentu seperti yang ditunjukkan pada Teorema 3, Akibat 4, Teorema 6, Akibat 7, serta Teorema 8, trinomial tersebut akan menjadi polinomial permutasi.

Saran

Hingga saat ini, belum ditemukan syarat secara umum dari suatu polinomial atas *finite field* agar menjadi polinomial permutasi, hal ini dapat menjadi bahan penelitian untuk dikembangkan selanjutnya, mengingat banyaknya kegunaan dari polinomial permutasi atas *finite field*.

DAFTAR PUSTAKA

Blake, Ian F., et al. 2008. "Polynomials over Finite Fields and Applications". 19 Sept. 2008. <www.birs.ca/workshop/2006/06w5021/report06w5021.pdf>.

Herstein, I.N. 1975. *Topics in Algebra* (2nd ed.). United States of America: Wiley & Sons.

----------.1996. *Abstract Algebra* (3rd ed.). New Jersey: Prentice-Hall.

Koblitz, Neal. 1998. *Algebraic Aspects of Cryptography*. Vol.3. Germany: Springer-Verlag.

Lidl, Rudolf, and Gunter Pilz. *Applied Abstract Algebra* (2nd ed.). New York: Springer-Verlag, 1998.

Mollin, R.A., and C. Small. 1987. "On Permutation Polynomials over Finite Fields". *Internet. J. Math. & Math. Sci. Vol. 10, No. 3*. (1987). 535-543.