

GEOMETRI BERHINGGA ATAS $GF(p^N)$ UNTUK MEMBENTUK ORTHOGONAL SERIES DESIGNS

Bambang Irawanto, Anisah
Jurusan Matematika FMIPA UNDIP

ABSTRACT---Galois Fields $GF(p^n)$ where p^n is a number of elements with p being a prime and n being an integer is used in creating Euclidean Geometry $EG(2, p^n)$, Projective Geometry $PG(2, p^n)$. $EG(2, p^n)$ can create a

BIB design which always results in an Orthogonal Series 1 (OS1) with parameters and $PG(2, p^n)$ can create a BIB

design which always results in an Orthogonal Series 2 (OS2) with parameters .

Keywords : Galois Field $GF(p^n)$, Euclidean Geometry $EG(2, p^n)$, Projective Geometry $PG(2, p^n)$.

1. PENDAHULUAN

Lapangan berhingga atau Galois Field adalah lapangan dengan elemen-elemennya berhingga. Elemen-elemen dalam Galois Field dapat digunakan untuk mengkonstruksi suatu geometri berhingga, yaitu geometri yang memiliki jumlah titik yang berhingga [4].

Rancangan Rangkaian Ortogonal merupakan salah satu Rancangan Blok Tidak Lengkap

Seimbang (RBTLS) dengan parameter-parameter $v = s^2$, $b = s^2 + s$, $r = s + 1$, $k = s$, yang dinamakan

dengan Rangkaian Ortogonal 1 (*Orthogonal Series 1 (OS1)*) dan $v = b = s^2 + s + 1$, $r = k = s + 1$, yang dinamakan dengan Rangkaian Ortogonal 2 (*Orthogonal Series 2 (OS2)*).

Dalam membentuk suatu Rancangan Rangkaian Ortogonal (*Orthogonal Series*) salah satunya dapat menggunakan geometri berhingga yaitu lapangan berhingga (*Finite fields*) atau disebut juga lapangan Galois (*Galois Fields*). Karena mempunyai manfaat yang cukup besar dalam aktifitas pendistribusian sejumlah objek maka untuk membentuk RBTLS dapat menggunakan banyak cara. Pada tulisan ini akan dibahas mengenai bagaimana cara membentuk Rancangan Rangkaian Ortogonal 1 dan 2 menggunakan konstruksi geometri berhingga atas *Galois Fields* $GF(p^n)$.

2. GEOMETRI EUCLID DAN GEOMETRI PROYEKTIF

Geometri Euclid berhingga (*Finite Euclidean Geometry*) dua dimensi atas lapangan $GF(p^n)$ dinotasikan dengan $EG(2, p^n)$ dan didefinisikan sebagai Geometri berhingga yang mempunyai dua

elemen yaitu titik dan garis, sebuah titik adalah pasangan (x, y) , dimana $x \in GF(p^n)$, $y \in GF(p^n)$. Jumlah x dan y adalah koordinat-koordinat titik. Garis adalah himpunan titik-titik yang memenuhi persamaan linier

$$ax + by = c$$

(1)

dimana $a, b, c \in GF(p^n)$ dan $(a, b) \neq (0, 0)$. Persamaan (1) kemudian dinamakan persamaan garis. Geometri berhingga $EG(2, p^n)$ memiliki s^2 titik dan $s^2 + s$ garis dan $s = p^n$ [2]. Sifat lain pada geometri berhingga adalah, setiap dua titik dari $EG(2, p^n)$ dihubungkan oleh tepat satu garis.[3]

Teorema 1.[2]

Terdapat tepat s titik di masing-masing garis dari $EG(2, p^n)$ dimana $s = p^n$.

Bukti :

Persamaan garis dapat ditulis sebagai

$$ax + by = c$$

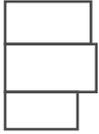
(i) atau sebagai

$$(ii) x = ?$$

Dalam kasus (i), untuk masing-masing nilai x , terdapat tepat satu nilai y . Karena x dianggap sebagai s sehingga x adalah nilai-nilai s . Oleh karena itu terdapat tepat s titik pada garis. Sedangkan untuk kasus (ii), x mempunyai sebuah nilai tetap $?$, tetapi $?$ dapat dipilih dalam s cara yang berbeda. Oleh karena itu terdapat s titik pada garis.

Dalam $EG(2, p^n)$, $s^2 + s$ garis dapat dibagi menjadi $s + 1$ himpunan-himpunan yang masing-masing terdiri dari s garis sedemikian sehingga setiap dua garis dari himpunan yang sama adalah paralel satu sama lain. Masing-masing himpunan ini dinamakan *parallel pencil*. [2]

Pandang geometri berhingga $EG(2, 2)$ berdasarkan lapangan $GF(2)$. Lapangan tersebut hanya terdiri dari dua



elemen yaitu 0 dan 1. Geometri berhingga $EG(2, p^n)$ mempunyai titik dan garis, dimana . Disini , sehingga $EG(2,2)$ mempunyai 4 titik, yaitu :

$(0,0), (0,1), (1,0), (1,1)$



Sedangkan jumlah garisnya adalah dan ditunjukkan dalam tabel berikut:

Tabel 1. Tabel garis-garis pada $EG(2,2)$

Persamaan Garis	Titik-titik yang dihubungkan
	$(0,0), (1,0)$
	$(0,1), (1,1)$
	$(0,0), (1,1)$
$y =$	$(1,0), (0,1)$
	$(0,0), (0,1)$
	$(1,0), (1,1)$

Geometri berhingga dari $EG(2,2)$ dapat disajikan

Gambar 1. EG (2,2)

Geometri Proyektif dinotasikan dengan $PG(2, p^n)$ dan didefinisikan sebagai perluasan dari $EG(2, p^n)$ dimana untuk setiap dua garis yang berbeda, berpotongan di sebuah titik yang berkorespondensi dengan masing-masing garis *parallel pencil* [2]. Titik baru ini disebut titik di tak hingga (*points at infinity*). Semua titik baru ini terdapat dalam sebuah garis yang disebut dengan garis di tak hingga (*line at infinity*). Berikut ini adalah sifat Geometri Proyektif,

Teorema 2. [2]

Geometri proyektif $PG(2, p^n)$ mempunyai $s^2 + s + 1$ titik dan $s^2 + s + 1$ garis. Setiap garis mengandung $s + 1$ titik, dan setiap titik terdapat di $s + 1$ garis. Setiap dua titik yang berbeda dihubungkan oleh satu garis yang unik dan setiap dua garis yang berbeda berpotongan di satu titik yang unik.

Bukti :

Terdapat s^2 titik dalam $EG(2, p^n)$ dan $s + 1$ titik di tak hingga (*points at infinity*) (Teorema 1). Oleh karena itu, terdapatlah $s^2 + s + 1$ titik.

Terdapat $s^2 + s$ garis dan satu garis di tak hingga (*line at infinity*). Oleh karena itu, terdapatlah $s^2 + s + 1$ garis.



Untuk setiap $m \in \text{GF}(p^n)$, didapat sebuah *parallel pencil* (dari bentuk (i) (Teorema 1.)) dengan kemiringan

m . Setiap garis dari *pencil* mempunyai persamaan, dimana m adalah sama untuk setiap garis dari *pencil* tetapi c berbeda untuk garis yang berbeda dari *pencil*. Titik di tak hingga berkorespondensi dengan *pencil* ini dan dikoordinatkan oleh (m) . Juga terdapat sebuah *parallel pencil* dari bentuk (ii) (Teorema 1.)

dengan kemiringan $-m$. Titik yang berkorespondensi dikoordinatkan oleh $(-m)$.

Garis di tak hingga dinotasikan oleh l . l mengandung $s + 1$ titik di tak hingga. Setiap garis di dalam $\text{EG}(2, p^n)$

mengandung s titik di tak hingga yang berkorespondensi dengan *pencil*. Maka garis mengandung titik (m) di tak hingga dan garis $x = c$ mengandung titik (m) . Jadi setiap garis dalam $\text{PG}(2, p^n)$ mengandung $s + 1$ titik. Juga setiap titik di dalam $\text{EG}(2, p^n)$ terkandung dalam $s + 1$ garis dalam $\text{EG}(2, p^n)$ dimana satu titiknya terletak di satu *parallel pencil*. Sebuah titik di tak hingga terkandung di setiap s garis dari *parallel pencil* yang saling berkorespondensi dan juga terkandung di garis tak hingga. Jadi setiap titik terkandung di tepat $s + 1$ garis.

Dua titik dalam $\text{EG}(2, p^n)$ dihubungkan oleh sebuah garis. Titik di tak hingga terletak di l . Misal sebuah

titik P dalam $\text{EG}(2, p^n)$ dan sebuah titik di tak hingga Q . P terletak tepat di garis dimana Q berada. Garis yang menghubungkan P dan Q adalah garis yang unik.

Dua garis yang tidak paralel dalam $\text{EG}(2, p^n)$ berpotongan di sebuah titik yang unik dalam $\text{EG}(2, p^n)$. Dua garis yang paralel dalam $\text{EG}(2, p^n)$ berpotongan di titik tak hingga yang berkorespondensi ke *parallel pencil* dimana kedua garis itu berada. Garis di tak hingga dan sebuah garis dalam $\text{EG}(2, p^n)$ berpotongan di titik tak hingga yang berkorespondensi ke *parallel pencil* dimana garis dalam $\text{EG}(2, p^n)$ berada. Maka, dua garis yang berbeda selalu berpotongan di sebuah titik yang unik.

Contoh 1

Geometri proyektif $\text{PG}(2, 2)$ atas lapangan GF_2 . Geometri proyektif $\text{PG}(2, p^n)$ mempunyai titik dan

garis, dimana $q = p^n$. Disini, gambar Geometri proyektif $\text{PG}(2, 2)$



Gambar.2 PG(2,2)

sehingga PG (2, 2) mempunyai 7 titik, yaitu :

(0), (1), (), (0,0), (0,1), (1,0), (1,1)

Sedangkan jumlah garisnya adalah dan ditunjukkan dalam tabel berikut:

Persamaan Garis	Titik-titik yang dihubungkan
	(0,0), (1,0), (0)
	(0,1), (1,1), (0)
	(0,0), (1,1), (1)
y =	(1,0), (0,1), (1)
	(0,0), (0,1), ()
	(1,0), (1,1), ()
	(0), (1), ()

Tabel .1 Jumlah garis dalam PG (2, 2)

**3 RANCANGAN RANGKAIAN ORTOGONAL
(ORTHOGONAL SERIES DESIGNS)**

Dalam beberapa penyusunan obyek yang digunakan untuk merancang suatu percobaan ada beberapa rancangan-rancangan salah satunya adalah Rancangan Rangkaian Ortogonal (Orthogonal Series Designs). Rancangan ini sebenarnya merupakan bentuk khusus dari Rancangan Blok Tidak Lengkap Seimbang

Suatu Rancangan Blok Tidak Lengkap Seimbang dengan parameter-parameter $(v, b, r, k, ())$ didefinisikan sebagai suatu penyusunan terhadap v objek yang berbeda a_1, \dots, a_v ke dalam b blok B_1, \dots, B_b sedemikian sehingga,memiliki bentuk dimana setiap blok B_j memuat tepat k objek yang berbeda, setiap objek a_i muncul di dalam tepat r blok yang berbeda dan setiap pasangan tak terurut a_i, a_j dari objek-objek yang berbeda, muncul bersama dalam tepat $($ blok , dimana

$v =$ Banyaknya objek yang akan dibagi ke dalam blok-blok B_1, \dots, B_b ,

$b =$ Banyaknya blok yang akan dihasilkan,

$r =$ Banyaknya blok yang memuat objek a_i ,

$k =$ Banyaknya objek dalam satu blok,

$(=$ Banyaknya blok yang memuat pasangan tak terurut a_i, a_j dari objek-objek yang berbeda.

Dengan parameter-parameter $v, b, r, k, ($ dari Rancangan Blok Tidak Lengkap Seimbang (RBTLS) memenuhi hubungan $bk = vr, ((v-1) = r(k-1)$ [2] Seperti pada teorema berikut ini

Teorema 3[2]

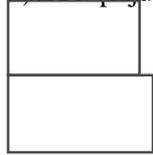
Parameter-parameter v, b, r, k , (dari RBTLS memenuhi hubungan $bk = vr, ((v-1) = r(k-1)$

Bukti :

Karena masing-masing blok mengandung k objek, jumlah objek yang terjadi di b blok adalah bk . Jumlah ini juga vr karena setiap v objek terjadi di r blok. Oleh karena itu $bk = vr$.



Terdapat r blok yang berbeda dimana sebuah objek muncul. Masing-masing blok mengandung $k - 1$ dari sisa $v - 1$ objek. Oleh karena itu jumlah objek yang lain dari muncul di blok ini adalah $r(k-1)$. Tetapi jumlah ini juga $((v-1) r)$ karena setiap $v-1$ objek harus muncul di (r) blok. Jadi $((v-1) r = r(k-1)$.



Akibatnya , merupakan bilangan bulat dan asli.

Karena banyaknya blok b tidak mungkin bilangan tak tercacah (*uncountable*) sehingga r pun harus bilangan bulat dan asli.

Suatu Rancangan Rangkaian Ortogonal dapat dibentuk secara langsung dari $EG(2, p^n)$, $PG(2, p^n)$.

Definisi 1



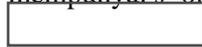
RBTLS dengan parameter-parameter disebut Rangkaian Ortogonal 1 (*Orthogonal series 1*) dinotasikan *OS1* dimana s prima atau pangkat prima.

Teorema 4

$EG(2, p^n)$ dapat membentuk RBTLS yang selalu menghasilkan *OS1*.

Bukti :

Karena $EG(2, p^n)$ mempunyai s^2 titik dan $s^2 + s$ garis yang berarti bahwa $EG(2, p^n)$ mempunyai s^2 objek dan $s^2 + s$ persamaan garis yang mengandung objek-objek dalam garis tersebut yang



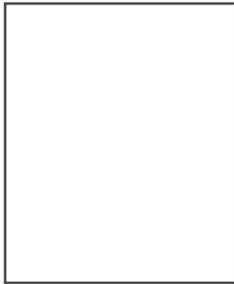
akan membentuk blok-blok. Hal ini berkorespondensi dengan parameter v dan b dari *OS1* dimana . Karena *OS1* merupakan sebuah RBTLS maka parameter-parameternya pun harus memenuhi persamaan dalam teorema 4. sebagai berikut

$$bk = vr, ((v-1) = r(k-1)$$

Sehingga



Atau



Diperoleh $r = (s+1)$ dan $k = s$.

Contoh 2



Membentuk OS1 dengan parameter . Geometri berhingga EG (2, 2) atas lapangan GF_2 terdiri dari dua elemen yaitu 0 dan 1. Disini $s = 2$ sehingga jumlah titiknya ada $s^2 = 4$ titik dan dapat diidentifikasi objek-objeknya yaitu :

Titik-titik dari EG	Objek
(2, 2)	
(0, 0)	1
(0, 1)	2
(1, 0)	3
(1, 1)	4

Tabel 2. objek-objek dalam

EG (2, 2)

Jumlah garisnya adalah $s^2 + s = 6$

Persamaan Garis	Titik-titik dihubungkan
<input type="text"/>	
<input type="text"/>	(0,0), (1,0)
<input type="text"/>	(0,1), (1,1)
<input type="text"/>	(0,0), (1,1)
$y =$ <input type="text"/>	(1,0), (0,1)
<input type="text"/>	(0,0), (0,1)
<input type="text"/>	(1,0), (1,1)

Tabel 3. Jumlah garis EG (2, 2)

Blok	Objek dalam setiap blok
1	(1, 3)
2	(2, 4)
3	(1, 4)
4	(3, 2)
5	(1, 2)
6	(3, 4)

Tabel 4. Rancangan blok OS1

Definisi 2

[Empty box]

RBTLS dengan parameter-parameter disebut Rangkaian Ortogonal 2 (*Orthogonal series 2* atau *OS2*) dimana s prima atau pangkat prima.

Teorema 5

$PG(2, p^n)$ dapat membentuk RBTLS yang selalu menghasilkan *OS2*.

Bukti :

Karena $PG(2, p^n)$ mempunyai $s^2 + s + 1$ titik dan garis yang berarti bahwa $PG(2, p^n)$ mempunyai $s^2 + s + 1$ objek dan persamaan garis yang mengandung objek-objek dalam garis tersebut yang

[Empty box]

akan membentuk blok-blok. Hal ini berkorespondensi dengan parameter v dan b dari *OS2* dimana . Karena banyaknya blok yang memuat pasangan tak terurut a_i, a_j dari objek-objek yang berbeda (?) pada *OS2* adalah 1 maka dari persamaan teorema 4 kita dapatkan

[Empty box]

Sehingga diperoleh $r = k = (s + 1)$.

Contoh 3

[Empty box]

Membentuk *OS2* dengan parameter .Geometri proyektif $PG(2, 2)$ atas lapangan GF_2 . Geometri proyektif

[Empty box]

$PG(2, p^n)$ mempunyai titik dan garis, dimana . Disini , sehingga $PG(2, 2)$ mempunyai 7 titik dan dapat diidentifikasi objek-objeknya yaitu :

Titik-titik dari $PG(2, 2)$	Objek
(0, 0)	1
(0, 1)	2
(1, 0)	3
(1, 1)	4

(0)	5	
(1)	6	
()	7	

Tabel 5. objek-objek PG (2, 2)



Sedangkan jumlah garisnya adalah sebagai berikut:

Persamaan Garis	Titik-titik yang dihubungkan
	(0,0), (1,0), (0)
	(0,1), (1,1), (0)
	(0,0), (1,1), (1)
y =	(1,0), (0,1), (1)
	(0,0), (0,1), ()
	(1,0), (1,1), ()
	(0), (1), ()

Tabel 6. Jumlah garis PG (2, 2)

Dari tabel 6. dapat dibuat rancangan blok-bloknya yaitu :

Blok	Objek dalam setiap blok
1	(1, 3, 5)
2	(2, 4, 5)
3	(1, 4, 6)
4	(3, 2, 6)
5	(1, 2, 7)
6	(3, 4, 7)
7	(5, 6, 7)

Tabel 7. Rancangan blok OS2

4. KESIMPULAN

Lapangan Hingga dengan elemen p dapat digunakan untuk membentuk Geometri Euclid dan Proyektif Geometri. Dari geometri Euclid dapat membentuk RBTLS yang selalu menghasilkan OS1 dan Proyektif Geometri dapat membentuk RBTLS yang selalu menghasilkan OS2.

5. DAFTAR PUSTAKA

- [1]. Bhattacharya, P.B, Jain, SR, Nagpaul, Basic Abstract Algebra, Cambridge University Press, USA, 1994
- [2] Bose R. C. & Manvel, B, *Introduction to Combinatorial Theory*, John Wiley & Sons, New York, 1984.
- [3]. Marshall Hall, Jr, *Combinatorial Theory*, Second Edition, John Wiley & Sons, New York, USA. P,

1986

[4]Raisinghania,M.D,Aggarwal,R.S,Modern Algebra, S Chand & Company Ltd,New Delhi, 1980

